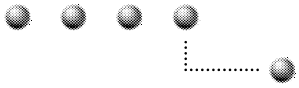


Berner Fachhochschule

Hochschule für
Technik und Architektur Bern

Enterprise Networking Architecture
Hacking und Auditing / Tools

Skript zum Unterricht

V 1.3
29.08.2002

Autor:
Martin Gafner
Aareweg 3c
3628 Uttigen

E-Mail: martin.gafner@networksfactory.com

Inhalt

1 Einführung

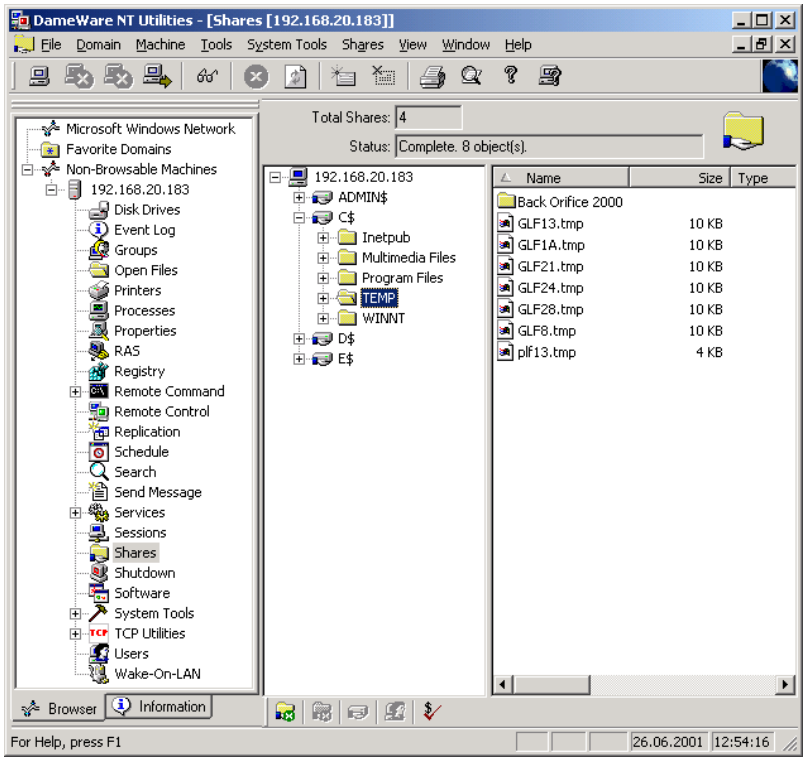
Seit den frühen 90er Jahren erfährt das Internet eine zunehmende Öffnung und Kommerzialisierung. Kaum ein Unternehmen, das nicht mindestens die Installation eines eigenen Servers plant. Kaum ein Anwender, der nicht mindestens einen Zugang zum Internet sucht. Diese Entwicklung hat natürlich auch Auswirkungen auf die Sicherheit im Internet, bzw. auf die Sicherheit der im Internet zusammengeschlossenen Informatiksysteme und Netze. Man hört und liest immer wieder von Viren, die über das Internet verteilt werden, von Hackern, die über das Internet an vertrauliche Daten gelangen oder von Anwendern, die aus Fahrlässigkeit oder Unwissenheit vertrauliche Informationen preisgeben. Immer wieder werden wir angefragt, ab wann sich denn ein Anwender einer bestimmten Gefahr aussetzt. Bin ich noch sicher, wenn ich Webseiten nur anschaue?

1.1 Ziel

Dieses Dokument gibt eine Übersicht über einige Tools, die potentielle Angreifer anwenden. Darauf basierend können Massnahmen abgeleitet werden, deren Umsetzung eine Erhöhung der Sicherheit von Rechnern am Internet bewirkt.

2 Windows NT Network Management

Mit den Dameware Utils (http://www.dameware.com) lässt sich ein Windows NT Netzwerk sehr nützlich administrieren. Das gleiche Tool kann jedoch auch ausgenutzt werden, um auf Rechner im Internet (z.B. bei einem Provider) zuzugreifen. Viele Benutzer gehen mit ihrem PC auf das Internet, ohne den Rechner zu sichern (z.B. kein Administrator-Passwort!).



DameWare NT Utilities

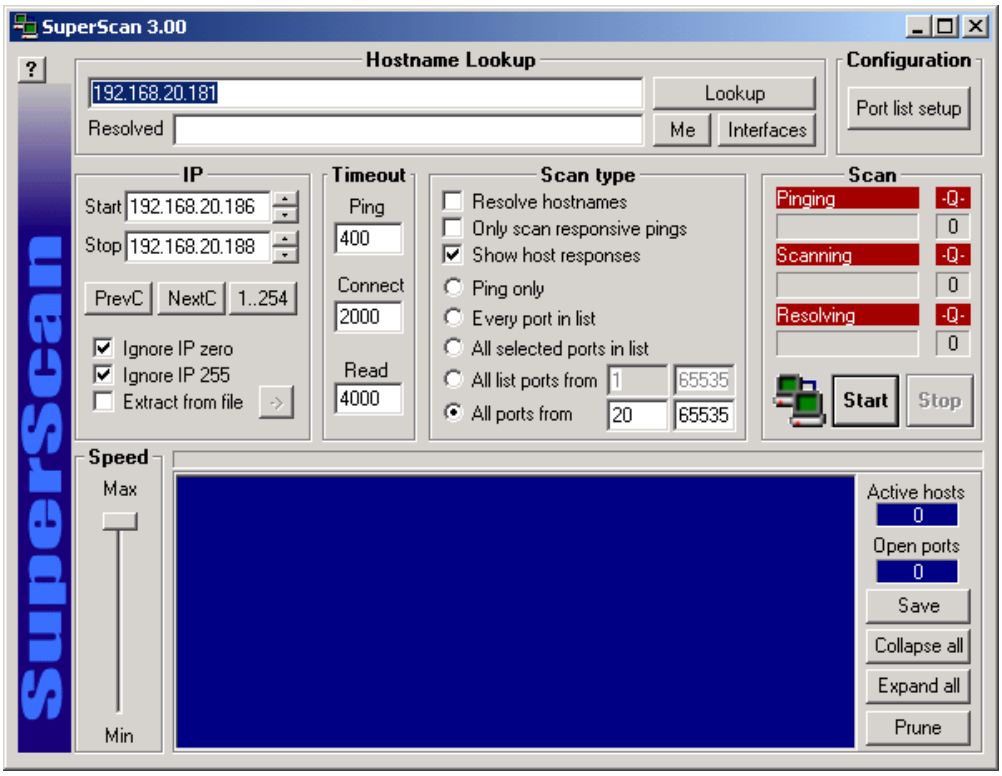
3 Portscanning

Anhand eines systematischen Scans auf einen Bereich von TCP oder UDP Portnummern auf einem oder mehreren Systemen kann ein Angreifer feststellen, welche Internet-Anwendungen (Dienste) auf den Zielsystemen aktiv sind und für einen möglichen Angriff verwendet werden könnten.

Portscanning kann wie folgt verglichen werden:
Ein potentieller Einbrecher streicht um die ihn interessierenden Häuser herum und prüft durch drücken der Türfallen, ob irgendeine Türe nicht geschlossen ist. Dabei notiert er sich auch, welche Schliesssysteme verwendet werden, damit er später nachschlagen kann, welches Schliesssystem welche Sicherheitslücken hat. Diese Information könnte er später nutzen, um die entsprechenden Werkzeuge mitzunehmen, wenn er in eines der Häuser eindringen will. Genauso macht es auch der Hacker. Er prüft die Angriffsziele und verwendet die Informationen, um sich auf mögliche Angriffe mit entsprechender Software und dem nötigen Wissen über die Software auszurüsten.

Im Labor testen wir einige Portscanning-Tools:

- FScan v1.12 - Command line port scanner. (http://www.foundstone.com)
- Hoppa Portscanner 2.0 (http://www.surf.to/hoppa)
- Nmap (Unix/Linux) (http://www.insecure.org/nmap)
- Nmap NT (Portierung auf Windows NT) (http://www.eEye.com)
- Nscan (http://nscan.hypermart.net)
- NTO Portscanner (http://www.ntobjectives.com)
- Scanport 1.1 (http://www.dataset.fr/eng/scanport.html)
- Superscan 3.00 (http://www.foundstone.com)



SuperScan 3.00

4 Security Vulnerabilities

Nach dem Portscan und den damit verfügbaren Informationen über Anwendungen informiert sich der Angreifer über die Sicherheitslücken der gefundenen Anwendungen. Diese Informationen kann er sich auch direkt aus dem Internet holen. Einerseits bieten viele Softwarehersteller auf ihrer Website Informationen über Sicherheitslücken und natürlich dazugehöriger Patches ihrer Software, andererseits gibt es aber auch Websites, auf denen diese Informationen zusammengefasst und suchbar zur Verfügung stellen.

Einige Beispiele:

Allgemeine/Zusammenfassend

- http://xforce.iss.net
- http://neworder.box.sk
- http://www.guninski.com

Hersteller

- http://www.microsoft.com/security

5 Sniffer

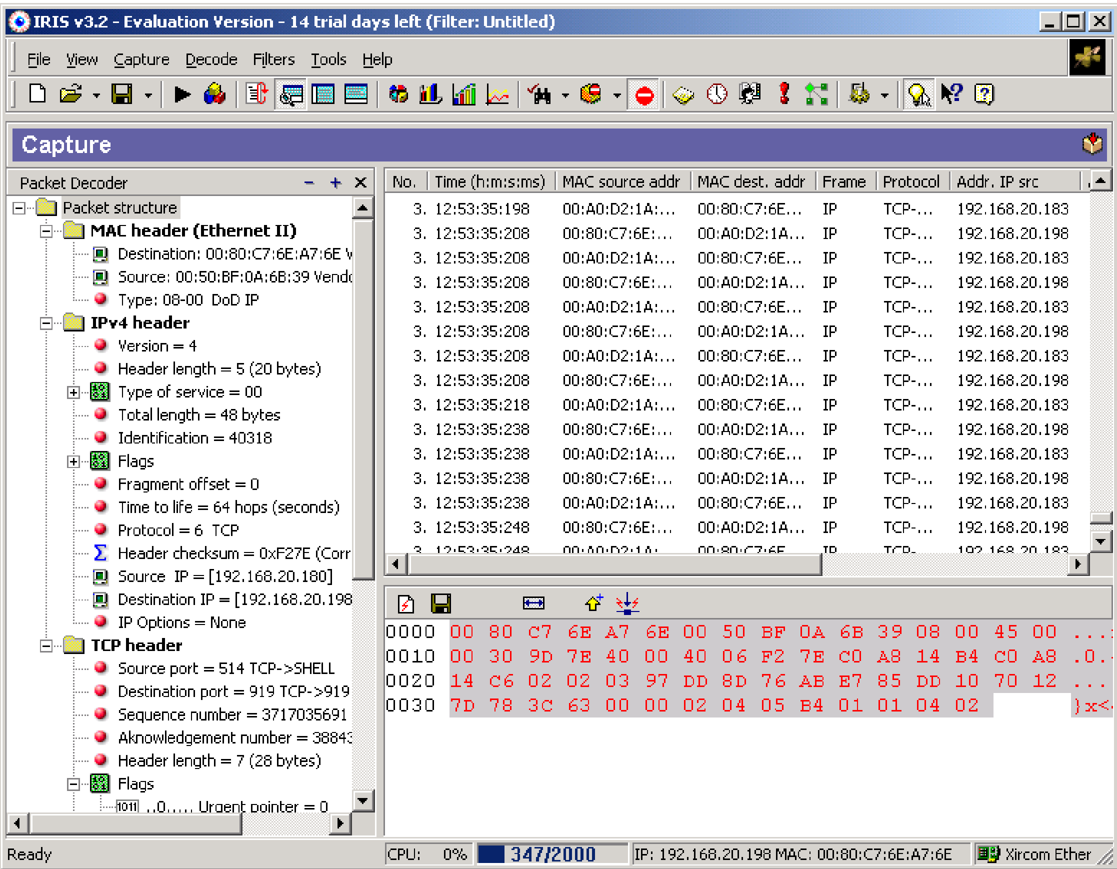
Mit einem Sniffer kann ein Netzwerkverwalter den Datenverkehr auf seinem Netzwerk "abhören". Dies kann sehr nützlich sein für die Fehlersuche.
Angreifer verwenden Sniffer, um Informationen über Netzwerke herauszufinden. Interessante Informationen sind:

- Netzstruktur
- IP-Adressen
- Verwendete Dienste
- Daten

Im Labor setzen wir folgende Sniffer ein:

- IRIS (http://www.eeye.com) , unter Windows NT/2000
- Ethereal (www.ethereal.com)

Um die Funktionsweise des Sniffers kennenzulernen und um Daten auf dem Netzwerk zu generieren, werden nochmals einige Portscans durchgeführt.
Der Sniffer wird bei den folgenden Uebungen immer wieder eingesetzt. Damit kann auf Netzwerkbasis sehr genau analysiert werden, was die Angriffstools bewirken.



IRIS Version 3.2

6 Angriffstools

Nuking oder attacking… Begriffe, die viele „kleine“ Hacker gerne verwenden. Man sieht es auch der Software an, die Programmierer der Tools dazu sind meistens eher jüngerer Generation.
Nicht alle Tools sind gleich gefährlich. Sie zeigen aber, dass durchaus das Potential da ist, für bekannte Sicherheitslücken auch die entsprechende Software, die die Sicherheitslücken ausnutzt, zu programmieren.

6.1 Mail Spoofing

Mail Spoofing Tools ermöglichen es auf bestimmten Mailservern unter fremder Mail-Adresse Mails zu versenden.

- AnonyMail 1.0
- Ghost Mail v.5.1 by Albert Yale ay@aci.qc.ca (http://ay.home.ml.org/)

6.2 Mail Bombing

Mit Mail Bombing Tools kann man innert kürzester Zeit eine grosse Menge Mails erzeugen. Dadurch können Mailserver überbelastet und Postfächer überfüllt werden.

- HakTek v1.1 (http://www.clubnexus.com/haktek)
- UnaBomber
- Up Yours!

6.3 Nukeing

Unter Nukeing versteht man das “Stören” von Netz-Verbindungen und ausgewählten Endsystemen. Häufig werden solche Tools von Hackern im IRC (Internet Relay Chat) verwendet um andere Chatter aus dem Chat-Network zu „entfernen“ (vom Netz zu trennen). Es können aber auch andere Client-Server Verbindungen mit solchen Tools getrennt werden.

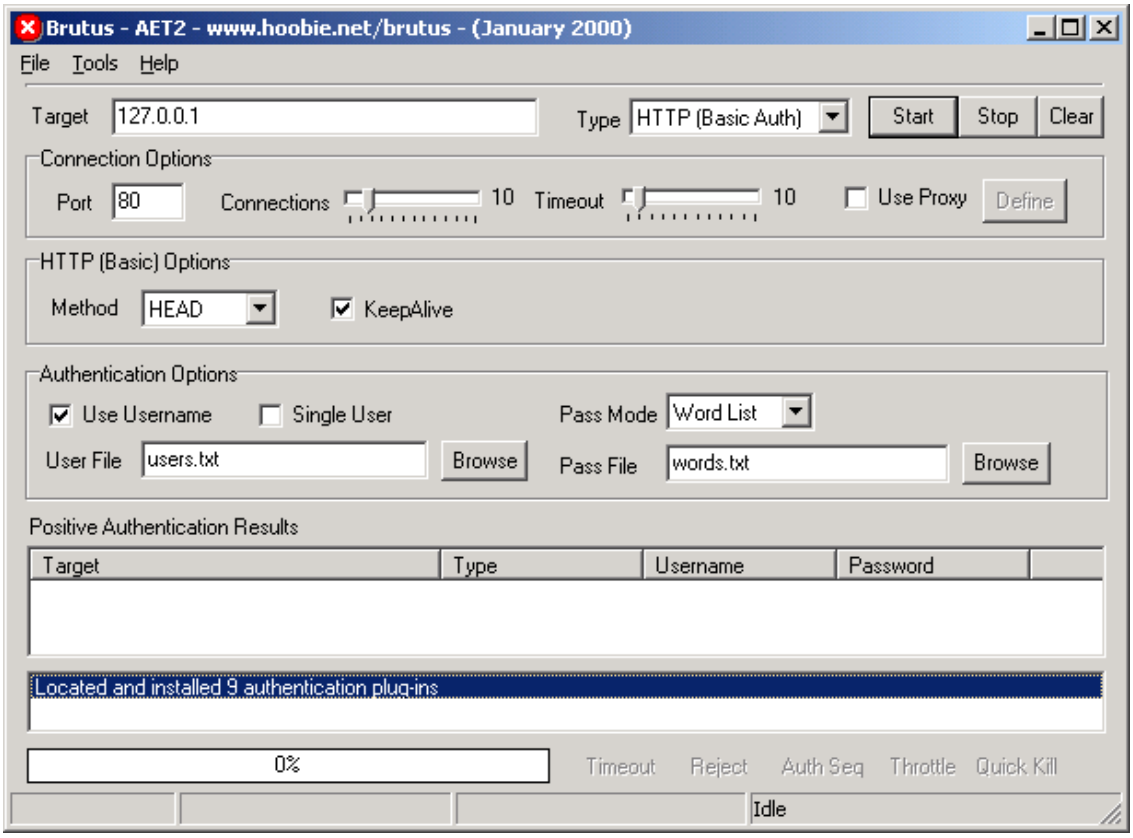
- Battle Pong (http://www.technophoria.com)
- Click V2.2
- Death n Destruction (http://www.hack101.com)
- Final Fortune 2.4
- Hnuke V2.23
- Panther 2

Folgende Tools nutzen eine Sicherheitslücke von Windows NT 4.0 < SP3. Diese Sicherheitslücke (Out of Band) hat die Auswirkung, dass der Rechner vom Netz getrennt wird und die Netzwerkkonfiguration wiederhergestellt werden muss.

- CG OOB
- Bit Slap

6.4 Diverse

- Web Check 1.1beta (damit lassen sich Webserver auf bekannte Sicherheitslücken prüfen)
- Brutus AET2 (http://www.hoobie.net/brutus) (damit können Passwörter über das Netzwerk auf einem entfernten System mittels Brute Force Attack erraten werden)



Brutus AET2

7 Trojanische Pferde und Back Doors

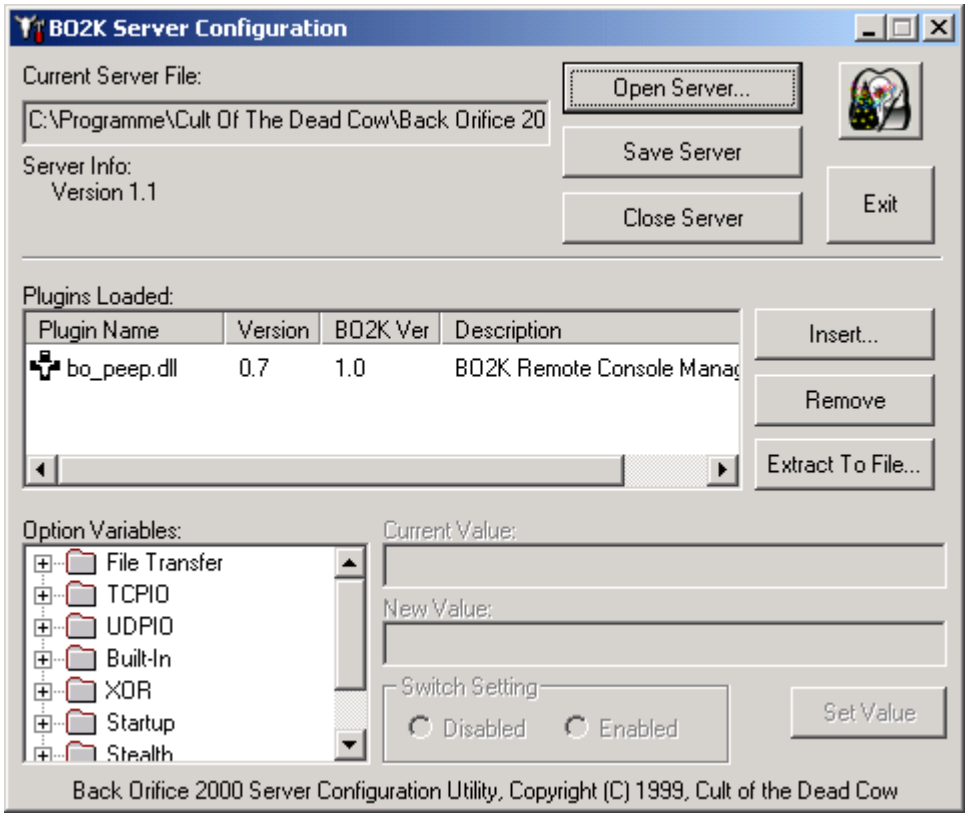
Trojanische Pferde sind Programme, die auf der Ebene eines normalen Benutzers Legalität vortäuschen und die gewünschten Funktionen scheinbar korrekt ausführen, die aber darüber hinaus noch eine erweiterte Funktionalität aufweisen, die demjenigen, der das Trojanische Pferde installiert hat, die Möglichkeit zu unerlaubten Handlungen eröffnet.

Eine Backdoor ist die Realisierung eines nicht autorisierten Zugangs zu einem IT-System, mit dem man die Zugangs- und Rechteprüfung umgehen kann. Konkret handelt es sich bei einer Backdoor meistens um einen nicht dokumentierten, geheimen Entry-Point in ein Programmodul.

Im Labor wird Back Orifice 2000 getestet:

- Back Orifice 2000 (http://www.bo2k.de)

Auf http://www.bo2k.de unter Tutorial ist eine Schritt für Schritt Anleitung (BO2K BASIC Tutorial v.1-1), wie dieses Tool in der Praxis eingesetzt wird.



Back Orifice 2000 Server Configuration

Weitere verbreitete Back Doors:

- Net Bus Pro
- SubSeven

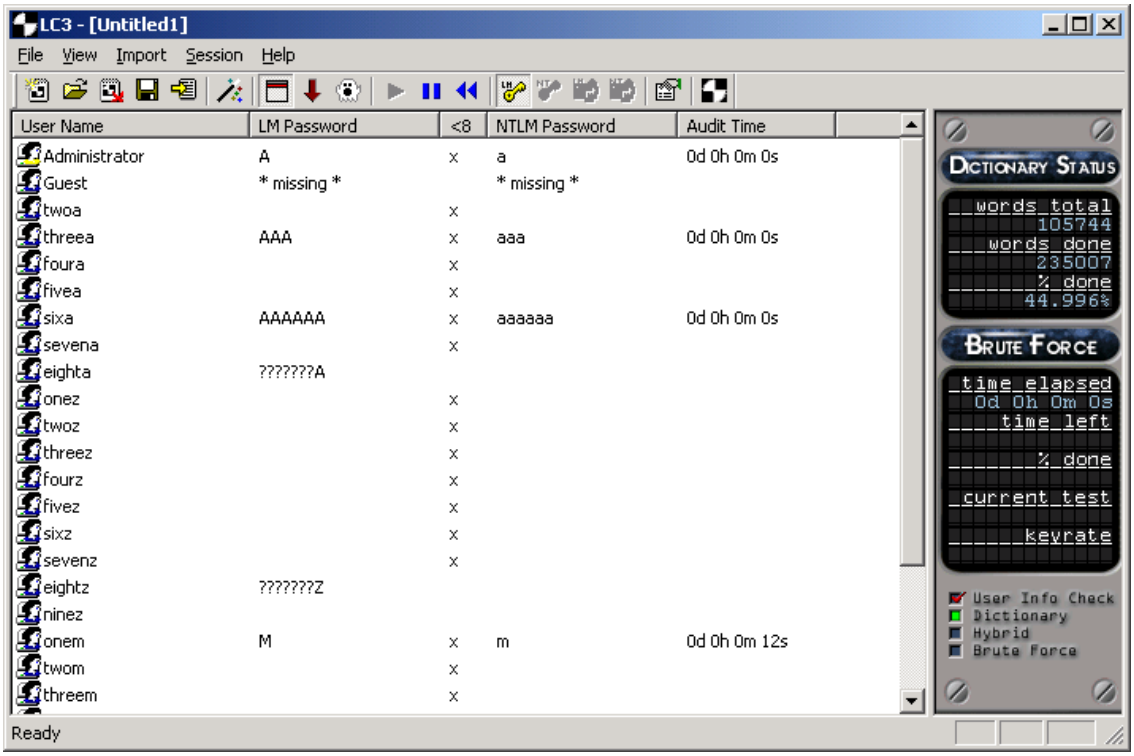
8 Passwort Cracker

Passwort Cracker werden verwendet, um die Passwort Qualität (Zusammensetzung des Passwortes, Alphabetisch, Zahlen, Sonderzeichen) zu prüfen.
Von Angreifern werden Passwort Cracker verwendet, um Passwörter von Benutzern herauszufinden und anschliessend deren Benutzeraccount auszunutzen.

Im Labor wird das L0phtCrack 2.52 eingesetzt:

- L0phtCrack 2.52
  (neueste Version unter http://www.atstake.com/research/lc3/index.html)

L0phtCrack ermöglicht es, die Passwörter auch aus dem Netzwerk zu sniffen. Bedingung ist, dass man sich mit dem Tool im entsprechenden Netzsegment befindet und das Netzwerk mittels Hubs (nicht Switches) vernetzt ist.



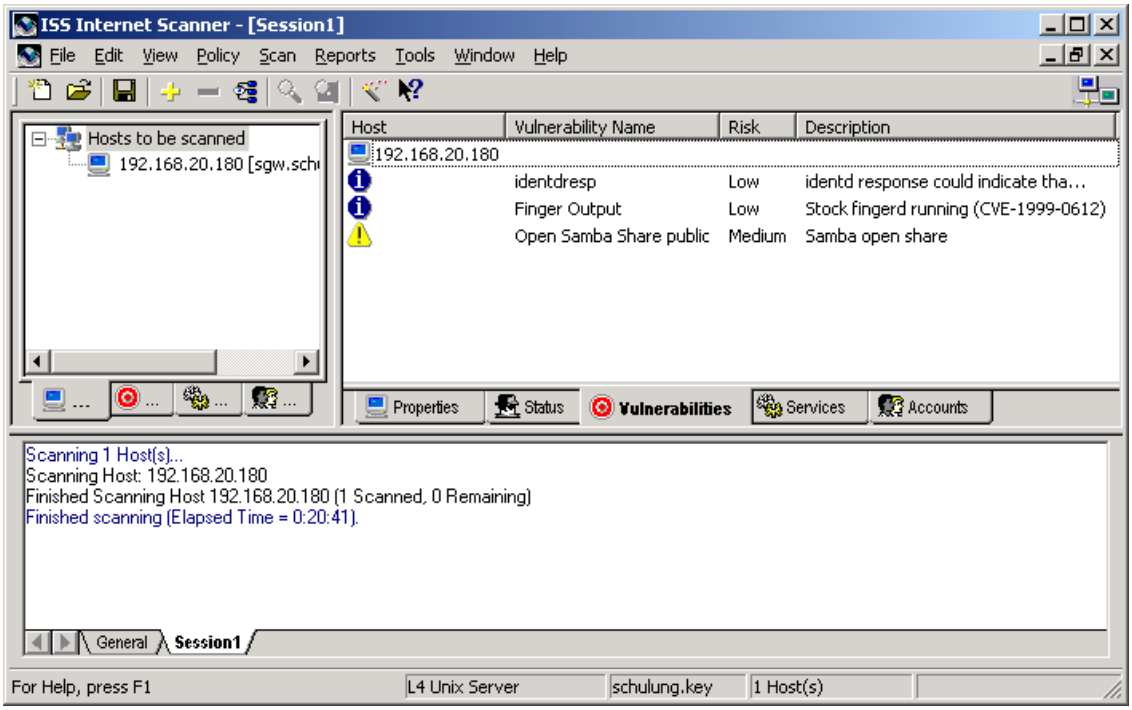
L0phtCrack Version 3

Unter Unix sind folgende vergleichbare Tools bekannt:

- John the ripper (http://www.openwall.com/john)
- Crack

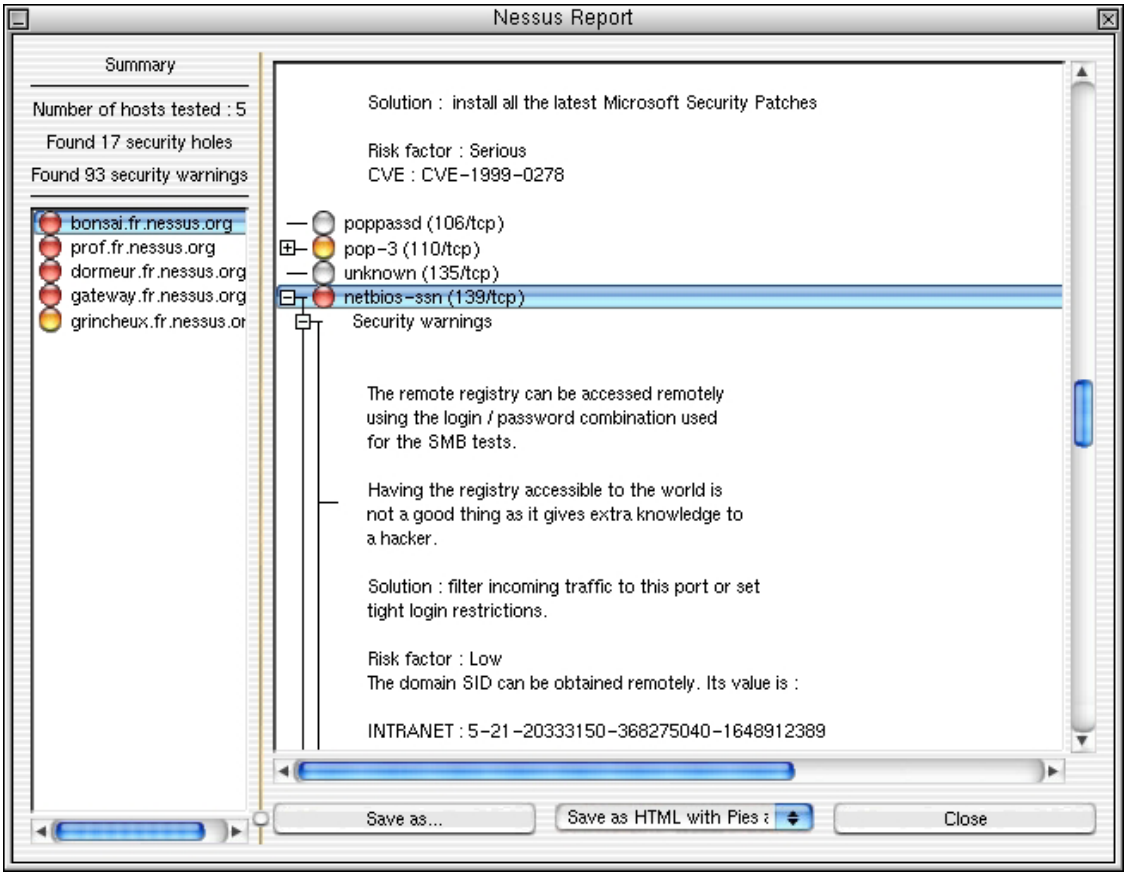
9 Auditing Software

Auditing Software wird verwendet, um auf Systemen nach bekannten Sicherheitslücken zu suchen. Normalerweise sollten solche Tools von Systemadministratoren zur Überprüfung ihrer Server und Workstations verwendet werden.
Eine der am weitesten verbreiteten Auditing Software ist der Internet Security Scanner von Internet Security Systems (http://www.iss.net).



Internet Scanner Version 6.1

Unter Unix ist mehr und mehr der NESSUS verbreitet (http://www.nessus.org)

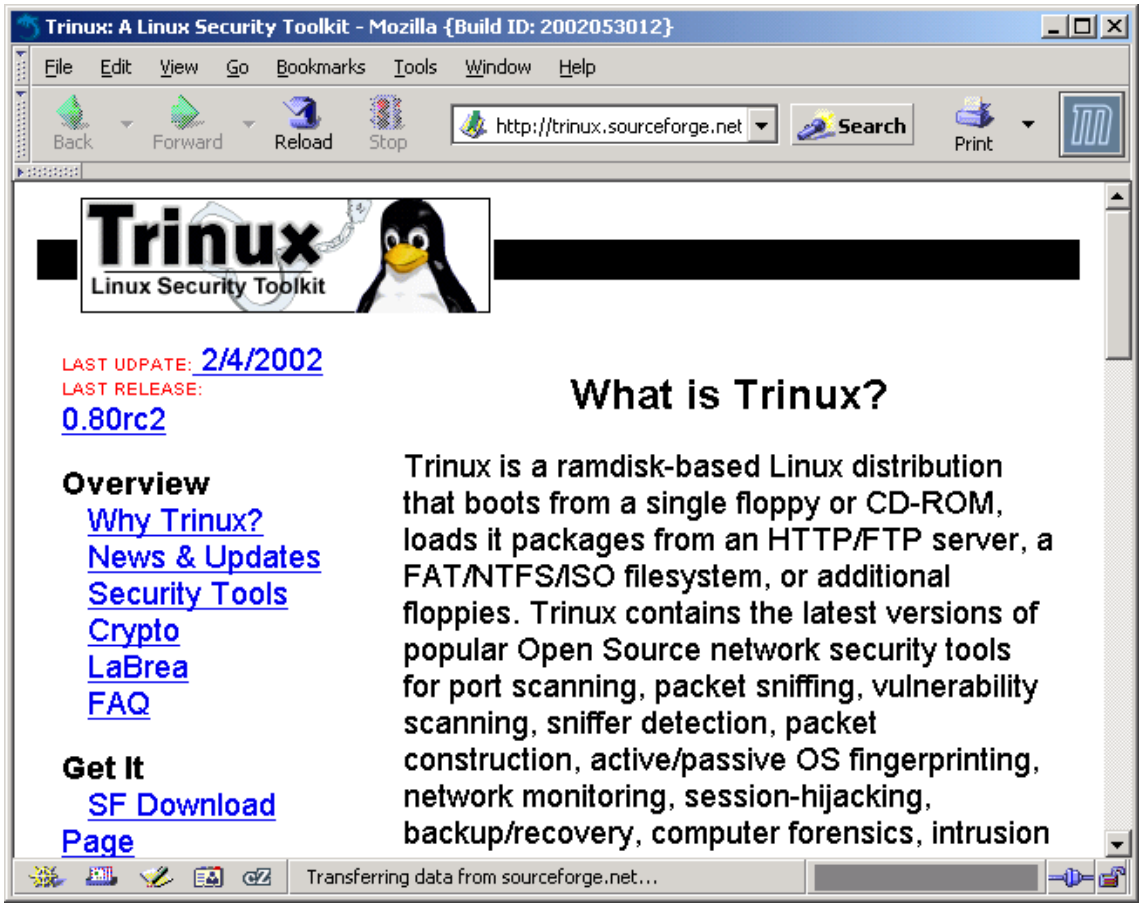


Nessus

10 Trinux Toolkit

Tiefergehende Tools bietet der Trinux Toolkit (http://www.trinux.org).

Die Trinux Tools erfordern jedoch tiefe Unix und TCP/IP-Protokoll-Kenntnisse. Die Programme können nur auf der Kommandozeile unter Angabe von Parametern ausgeführt werden.



Trinux Linux Security Toolkit

11 Anhang: Liste bekannter Portnummern von Back Doors

Port	Name des Trojaners	Protokoll
21	Back Construction	
21	Blade Runner	
21	Doly Trojan 1.1	
21	Fore	
21	FTP trojan	
21	Invisible FTP	
21	Larva	
21	WebEx	
21	WinCrash	
23	Tiny Telnet Server (= TTS)	
25	Ajan	
25	Antigen	
25	Email Password Sender	
25	Haebu Coceda (= Naebi)	
25	Happy 99	
25	Kuang2	
25	ProMail Trojan	
25	Shtrilitz	
25	Stealth	
25	Tapiras	
25	Terminator	
25	WinPC	
25	WinSpy	
31	Agent 31	TCP
31	Hackers Paradise	TCP
31	Masters Paradise	
41	DeepThroat	TCP
58	DMSetup	TCP
59	DMSetup	
79	Firehotcker	TCP
80	Executor	TCP
80	RingZero	
99	Hidden Port V2.0	
110	ProMail Trojan	TCP
113	Kazimas	TCP
119	Happy 99	TCP
121	BO JammerKillah	TCP
129	Password Generator Protocol	TCP
137	Netbios name (DoS attacks)	TCP/UDP
139	Netbios session (DoS attacks)	TCP/UDP
421	TCP Wrappers	TCP
456	Hackers Paradise	TCP
531	Rasmin	TCP
555	Ini-Killer	
555	NeTAdmin	
555	Phase Zero	TCP
555	Stealth Spy	TCP
666	Attack FTP	TCP
666	Back Construction	
666	Cain & Abel	
666	Peur de Rien FTP	
666	Satanz Backdoor	
666	ServeU	
666	Shadow Phyre	
667	DeepThroat 2.0	TCP
677	DeepThroat 2.0	TCP
777	AimSpy	
911	Dark Shadow	TCP
999	DeepThroat	TCP
999	WinSatan	
1000	Der Spaeher 3	
1001	Silencer	TCP
1001	WebEx	TCP
1010	Doly Trojan 1.30	
1010	Doly Trojan 1.35	
1011	Doly Trojan 1.1+1.2	TCP
1012	Doly Trojan	TCP
1015	Doly Trojan 1.5	TCP
1015	Doly Trojan 1.5	TCP
1016	Doly Trojan 1.6	
1024	Bla 1.1	
1024	NetSpy	TCP
1024	Psyber Streaming Server	
1033	NetSpy	
1042	Bla	TCP
1045	Rasmin	TCP
1090	Xtreme	TCP
1170	Psyber Streaming Server	
1170	Streaming Audio Trojan	TCP
1170	Voice	TCP
1207	SoftWar	
1243	BackDoor-G	
1243	SubSeven	TCP
1243	SubSeven Apocalypse	
1243	Ultors Trojan	
1245	VooDoo Doll	TCP
1269	Mavericks Matrix	TCP
1349	Back Orifice (BO) DLL	UDP
1492	FTP99CMP	TCP
1509	Nikhil G.	
1509	Psyber Streaming Server	TCP
1600	Shiva-Burka	TCP
1807	Nikhil G.	
1807	SpySender	TCP
1981	ShockRave	TCP
1999	BackDoor	TCP

11 Anhang: Liste bekannter Portnummern von Back Doors

1999	TransScout		5400	Back Construction 1.2+1.5	
2000	Remote Explorer	TCP	5400	Blade Runner	TCP
2000	TransScout		5401	Back Construction	
2001	TransScout		5401	Blade Runner	TCP
2001	Trojan Cow	TCP	5402	Back Construction	
2002	TransScout	TCP	5402	Blade Runner	TCP
2003	TransScout	TCP	5512	Illusion Mailer	
2004	TransScout	TCP	5512	Xtcp	TCP
2005	TransScout	TCP	5521	Illusion Mailer	
2023	Hack City Ripper Pro		5550	Xtcp	TCP
2023	Pass Ripper	TCP	5555	ServeMe	TCP
2086	Netscape/Corba exploit	TCP	5556	BO Facil	TCP
2115	Bugs	TCP	5557	BO Facil	TCP
2140	Deep Throat	TCP/UDP	5569	Robo-Hack	TCP
2140	Nikhil G.		5714	WinCrash	
2140	The Invasor		5741	WinCrash	
2155	Illusion Mailer	TCP	5742	WinCrash	TCP
2283	HVL Rat5	TCP	6000	The tHing 1.6	
2565	Striker	TCP	6400	The tHing	TCP
2583	WinCrash 2	TCP	6669	Vampyre 1.0	TCP
2600	Digital RootBeer		6711	SubSeven	TCP
2801	Nikhil G.		6712	SubSeven	TCP
2801	Phineas Phucker	TCP	6713	SubSeven	TCP
2989	RAT	UDP	6776	BackDoor-G	
3024	WinCrash	TCP	6776	SubSeven	TCP
3028	RingZero	TCP	6883	DeltaSource (DarkStar)	
3128	RingZero		6912	Danny	
3129	Masters Paradise	TCP	6912	Shit Heep	TCP
3150	Deep Throat 1.0	TCP/UDP	6939	Indoctrination	TCP
3150	The Invasor		6969	GateCrasher	TCP
3459	Eclipse 2000	TCP	6969	IRC 3	
3700	Portal of Doom	TCP	6969	Priority	TCP
3791	Total Eclypse 1.0 (FTP)	TCP	6970	GateCrasher	TCP
3801	Eclypse	UDP	7000	Kazimas	
4000	Psyber Streaming Server		7000	Remote Grab	TCP
4092	WinCrash	TCP	7300	NetMonitor	TCP
4321	BoBo		7301	NetMonitor	TCP
4321	School Bus 1.6	TCP	7306	NetMonitor	TCP
4321	Schoolbus 1.0		7307	NetMonitor	TCP
4567	Danny		7308	NetMonitor	TCP
4567	File Nail	TCP	7789	Back Door Setup	
4590	ICQTrojan	TCP	7789	ICKiller	TCP
4950	IcqTrojan		8080	RingZero	TCP
5000	Back Door Setup		8787	Back Orifice 2000	
5000	Bubbel		8879	Hack Office Armageddon	
5000	Socket23		9400	InCommand	
5000	Sockets de Troie v1	TCP	9872	Portal of Doom	TCP
5001	Back Door Setup		9873	Portal of Doom	TCP
5001	Sockets de Troie v1	TCP	9874	Portal of Doom	TCP
5011	One of the Last Trojans		9875	Portal of Doom	TCP
5032	NetMetropolitan 1.04		9876	Cyber Attacker	TCP
5321	Firehotcker	TCP	9878	TransScout	TCP

11 Anhang: Liste bekannter Portnummern von Back Doors

9989	iNi-Killer	TCP
10067	Portal of Doom	TCP/UDP
10101	BrainSpy	
10167	Portal of Doom	TCP
10167	Portal of Doom	UDP
10520	Acid Shivers	TCP
10607	Coma	TCP
10607	Danny	
10666	Ambush	
11000	Senna Spy	TCP
11223	ProgenicTrojan	TCP
12076	GJamer	TCP
12223	Hack'99	TCP
12223	KeyLogger	TCP
12345	GabanBus	
12345	NetBus	TCP
12345	Pie Bill Gates	
12345	Ultor's Trojan	TCP
12345	X-bill	
12346	GabanBus	
12346	NetBus 1.x avoiding Netbuster	TCP
12346	X-bill	
12361	Whack-a-mole	TCP
12362	Whack-a-mole	TCP
12456	NetBus	TCP
12631	WhackJob	TCP
12701	Eclipse 2000	
13000	Senna Spy	TCP
13700	Kuang2 The Virus	
16969	Priority	TCP
17300	Kuang2 The Virus	TCP
20000	Millennium	TCP
20001	Millennium	TCP
20034	NetBus 2 Pro	TCP
20203	Chupacabra	
20203	Logged!	
20331	Bla	
21544	Schwindler 1.82	
21554	GirlFriend	TCP
22222	Prosiak 0.47	TCP
23456	Evil FTP	TCP
23456	Ugly FTP	TCP
23456	Whack Job	
23476	Donald Dick	TCP
23477	Donald Dick	TCP
26274	Delta Source	TCP/UDP
27374	SubSeven 2.1	
27573	SubSeven 2.1	UDP
27573	SubSeven 2.1	TCP
27665	Trin00 DoS Attack	TCP
29891	The Unexplained	TCP/UDP
30029	AOL Trojan 1.1	TCP
30100	NetSphere	TCP
30101	NetSphere	TCP
30102	NetSphere	TCP
30133	Netsphere Final	
30133	Trojan Spirit 2001a	
30303	Socket 25	
30303	Sockets de Troie	TCP
30999	Kuang 2	TCP
31335	Trin00 DoS Attack	UDP
31336	Bo Whack	TCP
31337	Back Orifice	
31337	BackFire	UDP
31337	Backorifice (BO)	UDP
31337	Baron Night	TCP
31337	BO client	
31337	Bo Facil	
31337	BO2	
31337	DeepBO	
31337	Netpatch	TCP
31338	Back Orifice	UDP
31338	DeepBO	UDP
31338	NetSpy DK	TCP
31339	NetSpy DK	TCP
31666	BOWhack	TCP
31785	Hack'a'Tack	TCP
31787	Hack'a'Tack	UDP
31788	Hack'a'Tack	UDP
31789	Hack'a'Tack	UDP
31790	Hack'a'Tack	UDP
31791	Hack'a'Tack	UDP
31792	Hack'a'Tack	
32418	Acid Battery 1.0	
33333	Prosiak	TCP
33390	Unknown Trojan	UDP
33911	Trojan Spirit 2001a	TCP
34324	BigGluck	TCP
34324	Tiny Telnet Server	
34324	TN	TCP
40412	The Spy	TCP
40421	Agent 40421	TCP
40421	Masters Paradise	TCP
40422	Masters Paradise	TCP
40423	Masters Paradise	TCP
40425	Masters Paradise	TCP
40426	Masters Paradise	TCP
43210	Schoolbus 1.6	
47252	Delta Source	TCP
47262	Delta Source	UDP
49301	Online Keylogger	
50505	Sockets de Troie v2	TCP
50766	Fore	TCP
50766	Schwindler	

11 Anhang: Liste bekannter Portnummern von Back Doors

53001	Remote Windows Shutdown	TCP	60000	Deep Throat 2.0 & 3.0	TCP
54320	Back Orifice	UDP	61466	Telecommando	TCP
54320	Back Orifice 2000	TCP	65000	Devil 1.03	TCP
54321	Back Orifice	TCP			
54321	Back Orifice 2000	UDP			

[Quelle: http://home.t-online.de/home/TschiTschi/well_known_trojaner_ports.htm]