
Techniken der Hacker

Angriffsmethoden und Abwehrstrategien

Dr. G. Weck

INFODAS GmbH

Köln

Inhalt

- Vorbereitung des Angriffs
 - Footprinting – Die Wahl des Angriffsziels
 - Scanning – erste Informationen
 - Auswertung und Angriffsplanung
- Angriffe auf gängige Betriebssysteme
 - Windows 95 / 98 / Me – Windows NT / 2000 / XP
 - Novell NetWare – Unix / Linux
- Angriffe auf Netzwerk-Komponenten
 - Einwahlknoten und RAS / VPN
 - Netzwerkgeräte und Firewalls
 - Denial-of-Service Angriffe
- Fortgeschrittene Angriffstechniken
 - TCP Hijacking
 - Hintertüren und Trojanische Pferde
 - Angriffe auf Web-Server

Die Wahl des Angriffsziels

- Footprinting:
 - Zusammenstellung leicht erhältlicher Informationen über das Angriffsziel
 - Namen / Telefonnummern von Personen
 - Rechnernamen / Domännennamen / IP-Adressen
 - Profil der vorhandenen / möglichen Schutzmaßnahmen
- Informationsquellen:
 - öffentlich verfügbare Informationen
 - Organigramme / Telefon- und E-Mail-Verzeichnisse
 - Social Engineering
 - Web-Seiten (HTML-Quelltext mit Kommentaren)
 - Internet-Verzeichnisse: InterNIC (www.arin.net)
 - DNS Informationen

Footprinting: Gegenmaßnahmen

- Einschränkung der veröffentlichten Informationen:
 - keine Organigramme mit Namen / Telefonnummern
 - keine E-Mail-Adressen mit Rechneradressen:
 - nicht: `G.Weck@mailserver.techdomain.infodas.de`
 - sondern: `G.Weck@infodas.de`
 - Kontrolle der an InterNIC übermittelten Informationen:
 - keine Namen / Adressen von Systemverwaltern
 - gesicherte Übermittlung von Daten an InterNIC (z.B. mit PGP)
 - Schutz von DNS
 - Verhinderung externer Zonen-Transfers
 - restriktive Firewall-Regeln und Network Address Translation (NAT)
- Schulung der Benutzer

Scanning – erste Informationen

- Auskundschaften der Netzstruktur
 - Suchläufe mit `ping`, `tracert` und Visualroute
 - ICMP-Abfragen (Uhrzeit, Teilnetz-Maske etc.)
- Auskundschaften einzelner Rechner
 - Port-Scans
 - erkennen extern zugängliche Dienste / Schnittstellen
 - erkennen potentiell unsichere Software
 - Erkennen des Betriebssystems
 - Analyse von Spezifika des TCP/IP-Protokoll-Stacks
- Zugriffe über ungenügend gesichertes SNMP

Beispiel für ping

```
C:\>ping holmes
```

```
Ping HOLMES [192.168.100.1] mit 32 Bytes Daten:
```

```
Antwort von 192.168.100.1: Bytes=32 Zeit<10ms TTL=128
```

```
Ping-Statistik für 192.168.100.1:
```

```
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
```

```
Ca. Zeitangaben in Millisek.:
```

```
  Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Beispiel für tracert

```
C:\>tracert www.altavista.com
```

```
Routenverfolgung zu altavista.com [209.73.164.93] über maximal 30 Abschnitte:
```

```
 1  141 ms   110 ms   120 ms   fra-tgn-oym-vty254.as.wcom.net [212.211.92.254]
 2  101 ms   110 ms   120 ms   fra-big1-eth01.wan.wcom.net [212.211.79.1]
 3  101 ms   100 ms   130 ms   fra-ppp1-fas0-1-0.wan.wcom.net [212.211.79.129]
 4  101 ms   100 ms   140 ms   fra-border1-fas6-1-0.wan.wcom.net [212.211.30.33]
 5  291 ms   180 ms   160 ms   POS0-1-0.gw8.Frankfurt.de.alter.net [139.4.45.145]
 6  100 ms   110 ms   120 ms   GE6-0.cr1.Frankfurt.de.alter.net [139.4.13.1]
 7  130 ms   120 ms   140 ms   102.at-6-1-0.CR1.Frankfurt1.de.alter.net [149.227.31.26]
 8  120 ms   130 ms   120 ms   114.ATM1-0-0.xr2.Frankfurt1.de.alter.net [149.227.31.34]
 9  131 ms   120 ms   130 ms   so-1-1-0.TR1.FFT1.Alter.Net [146.188.8.142]
10  190 ms   200 ms   190 ms   so-4-0-0.IR1.NYC12.Alter.Net [146.188.3.201]
11  190 ms   210 ms   191 ms   so-1-0-0.IR1.NYC9.ALTER.NET [152.63.23.61]
12  200 ms   211 ms   190 ms   0.so-0-0-0.TR2.NYC9.ALTER.NET [152.63.9.182]
13  191 ms   200 ms   200 ms   0.so-3-0-0.XR2.NYC9.ALTER.NET [152.63.22.93]
14  190 ms   200 ms   201 ms   0.so-3-1-0.XL1.NYC9.ALTER.NET [152.63.9.58]
15  210 ms   201 ms   200 ms   POS7-0.BR2.NYC9.ALTER.NET [152.63.22.229]
16  190 ms   200 ms   200 ms   atm4-0-1.core2.NewYork1.Level3.net [209.244.160.161]
17  190 ms   201 ms   200 ms   so-4-1-0.mp1.NewYork1.Level3.net [209.247.10.37]
18  290 ms   290 ms   291 ms   so-2-0-0.mp2.SanJose1.Level3.net [64.159.0.218]
19   *        280 ms   291 ms   gigabitethernet10-0.ipcolo3.SanJose1.Level3.net [64.159.2.41]
20  280 ms   281 ms   310 ms   unknown.Level3.net [64.152.64.6]
21  290 ms   280 ms   291 ms   10.28.2.9
22  291 ms   300 ms   310 ms   altavista.com [209.73.164.93]
```

```
Ablaufverfolgung beendet.
```

Zugriffsweganzeige von Visualroute

Report for www.altavista.com [209.73.164.90]

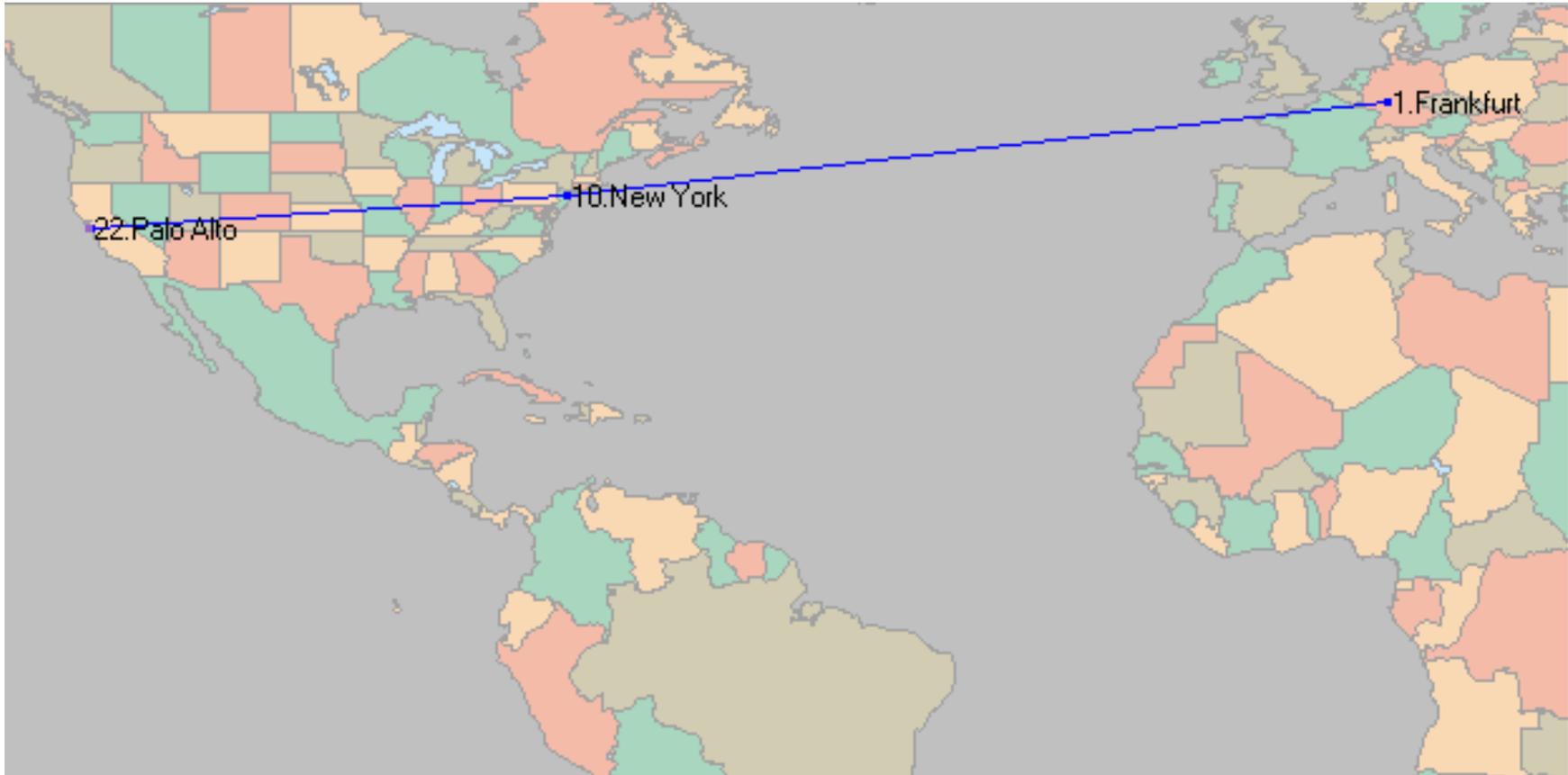


Analysis: 'www.altavista.com' was found in 22 hops (TTL=231). It is a HTTP server (running AW/1.0.1).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		192.168.100.3	doyle	...			0	(private use)
1		195.232.57.254	fra-tgn-oyv-vty254.as.wcor	Frankfurt, Germany	+1.0	127		Frankfurt PPP Client Pool
2		212.211.79.33	fra-big2-eth01.wan.wcom	Frankfurt, Germany	+1.0	137		Frankfurt PPP Infrastructure
3		212.211.79.133	fra-ppp2-fas0-1-0.wan.wc	Frankfurt, Germany	+1.0	141		Frankfurt PPP Infrastructure
4		212.211.30.29	fra-border1-fas0-1-0.wan.	Frankfurt, Germany	+1.0	136		European PPP Infrastructure
5		139.4.45.145	POS0-1-0.gw8.Frankfurt.d	Frankfurt, Germany	+1.0	139		EUNET Deutschland GmbH
6		139.4.13.1	GE6-0.cr1.Frankfurt.de.alt	Frankfurt, Germany	+1.0	106		EUNET Deutschland GmbH
7		149.227.30.230	102.ATM0-0.cr1.Frankfurt1	Frankfurt, Germany	+1.0	129		UUNET Deutschland GmbH
8		149.227.19.102	114.ATM2-0-0.xr1.Frankfu	Frankfurt, Germany	+1.0	135		UUNET Deutschland GmbH
9		146.188.8.138	so-0-1-0.TR2.FFT1.Alter.N	Frankfurt, Germany	+1.0	123		UUNET PIPEX
10		146.188.3.201	so-4-0-0.IR1.NYC12.Alter.	New York, NY, USA	-5.0	191		UUNET PIPEX
11		152.63.23.61	so-1-0-0.IR1.NYC9.ALTEF	New York, NY, USA	-5.0	200		UUNET Technologies, Inc.
12		152.63.15.185	119.at-6-1-0.TR1.NYC9.AI	New York, NY, USA	-5.0	196		UUNET Technologies, Inc.
13		152.63.22.97	0.so-3-0-0.XR1.NYC9.ALT	New York, NY, USA	-5.0	210		UUNET Technologies, Inc.
14		152.63.9.58	0.so-3-1-0.XL1.NYC9.ALT	New York, NY, USA	-5.0	208		UUNET Technologies, Inc.
15		152.63.22.225	POS6-0.BR2.NYC9.ALTEF	New York, NY, USA	-5.0	200		UUNET Technologies, Inc.
16		209.244.160.161	atm4-0-1.core2.NewYork1	New York, NY, USA	-5.0	202		Level 3 Communications, Inc.
17		209.247.10.37	so-4-1-0.mp1.NewYork1.l	New York, NY, USA	-5.0	201		Level 3 Communications, Inc.
18		64.159.0.218	so-2-0-0.mp2.SanJose1.l	San Jose, CA, USA	-8.0	280		Level 3 Communications, Inc.
19		64.159.2.169	gigabitethernet10-2.ipcolc	San Jose, CA, USA	-8.0	274		Level 3 Communications, Inc.
20		64.152.64.6	unknown.Level3.net	-		283		Level 3 Communications, Inc.
21		10.28.2.9	-	...		288		(private use)
22		209.73.164.90	www.altavista.com	Palo Alto, CA 94301		283		AltaVista Company

Roundtrip time to www.altavista.com, average = 283ms, min = 280ms, max = 360ms -- 9.9.2001 12:39:40

Zugriffsweganzeige von Visualroute



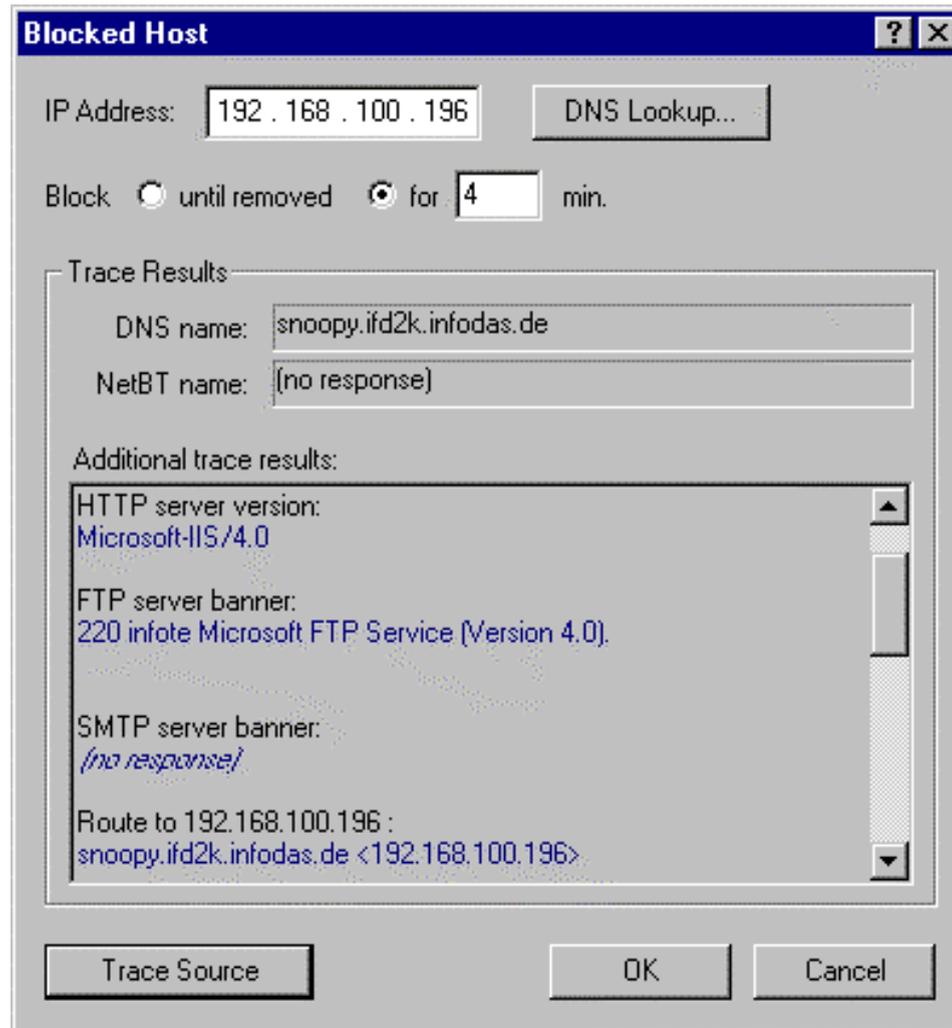
Port-Scan eines Windows NT Servers

```
C:\Programme\Tools\NetCat>nc -v -z -w2 192.168.100.137 1-140
lucy.infodas.de [192.168.100.137] 139 (netbios-ssn) open
lucy.infodas.de [192.168.100.137] 135 (epmap) open
lucy.infodas.de [192.168.100.137] 122 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 100 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 99 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 85 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 80 (http) open
lucy.infodas.de [192.168.100.137] 79 (finger): TIMEDOUT
lucy.infodas.de [192.168.100.137] 75 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 62 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 58 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 42 (nameserver): TIMEDOUT
lucy.infodas.de [192.168.100.137] 35 (?): TIMEDOUT
lucy.infodas.de [192.168.100.137] 25 (smtp) open
lucy.infodas.de [192.168.100.137] 21 (ftp) open
lucy.infodas.de [192.168.100.137] 13 (daytime): TIMEDOUT
lucy.infodas.de [192.168.100.137] 12 (?): TIMEDOUT
```

Scanning: Gegenmaßnahmen

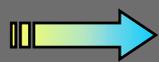
- Schutz gegen **ping** und ICMP-Abfragen:
 - Abblocken geeigneter ICMP Nachrichten im Firewall
 - Intrusion Detection Systeme (IDS)
 - Network Address Translation (NAT)
 - Verwendung privater Adressen im internen Netz
 - 10.0.0.0/8 (d.h. 10.x.y.z) für A-Subnetze
 - 172.160.0.0/12 (d.h. 172.16.x.y bis 172.31.x.y) für B-Subnetze
 - 192.168.0.0/16 (d.h. 192.168.x.y) für C-Subnetze
- Schutz gegen Port-Scans und Betriebssystem-Erkennung
 - Intrusion Detection Systeme (IDS)
 - gezielte Überwachung von Port-Abfragen im Firewall

Rückverfolgung eines Angreifers



Auswertung und Angriffsplanung

- Auswertung von Windows NT / 2000 Netzen
 - Bestimmung der Netz-Ressourcen (`net view`)
 - Bestimmung von Benutzerkonten / Gruppen (`nbtstat`)
 - Abfragen über das SNMP-Protokoll
 - Auswertung von Anwendungen und Bannern (`telnet`)



Gegenmaßnahmen:

- Einschränken des anonymen Zugriffs
- Abblocken der NetBIOS-Ports (135 – 139)
- Ausschalten des SNMP-Dienstes
- Abschalten unnötiger Banner in Anwendungen
- Schutz der Registry gegen Fernzugriff

Auswertung und Angriffsplanung

- Auswertung von Novell NetWare Netzen
 - Abfrage des Windows Netzwerk Browsers
 - Abfragen mit On-Site-Admin (ohne Anmeldung!)

 Gegenmaßnahme: Einschränkungen durch Filter im NDS-Baum

- Auswertung von Unix-Netzen
 - Bestimmung von Netzwerk-Ressourcen / NIS
 - Suchen von Benutzer-Informationen (`finger`)
 - Auswertung von Anwendungen und Bannern (`rpcinfo`)

 Gegenmaßnahme: Abschalten / Filtern aller überflüssigen Dienste

Windows 95 / 98 / Me

- Zugriff auf Datei-Freigaben
 - Auffinden über TCP/IP- oder NetBIOS-Scanning
 - Zugriff über erratene / geknackte Paßwörter

 **Gegenmaßnahme: Freigaben abschalten**

- Nutzung von Hintertüren zur Systemkontrolle
 - Back Orifice ermöglicht komplette Fernsteuerung
 - Verteilung des Clients über Viren / aktive Inhalte
- Direkte Zugriffe von der „Konsole“
 - Windows 9x Paßwörter sind wirkungslos !!!
 - Paßwort-Verschlüsselung ist zu schwach

 **Bester Schutz: Verzicht auf Windows 9x !**

Windows NT / 2000 / XP

- Erraten / Knacken von Paßwörtern
 - Auslesen aus der Kopie der SAM-Datenbank
 - ungeschützte Kopie liegt oft unter `%systemroot%\repair`
 - Auslesen mit `pwdump` oder `samdump`
 - Abgreifen über Logon-Schnittstelle mit `pwdump2`
 - Abgreifen im Netz über SMB Packet Capture
 - Erraten zu schwacher Paßwörter
 - Analyse mit `10pthcrack` / `LC3` oder `john` (the ripper)



Gegenmaßnahmen:

- nur Administratorzugriff auf `%systemroot%\repair`
- Paßwort-Management („Kennwortrichtlinien“)
- Überterschlüsselung der Paßwörter mit `syskey`
- Abschalten der LAN Manager Authentisierung

Cracken von Paßwörtern

The screenshot shows a software window titled "LC3 - [Untitled1]" with a menu bar (File, View, Import, Session, Help) and a toolbar. The main area is a table with the following columns: User Name, LM Password, <8, NTLM Password, and Audit Time. The table lists 20 users, with 'x' marks in the '<8' and 'NTLM Password' columns for Administrator, Levermann, Krey, Brzoska, Lewis, Wollmann, Weimer, and Maier. The 'Audit Time' column shows "0d 0h 0m 0s".

User Name	LM Password	<8	NTLM Password	Audit Time
Administrator		x		
Gast				
Levermann		x		
Weck				
Henschke				0d 0h 0m 0s
Wriesman				
Koers				
Urbanski				
Krey		x		
Sieberath				
Schmitter				
Kaufhold				
MARCY\$				
je				
Buehrlen				
PCKY\$				
Brzoska		x		
Lewis		x		
PCVO\$				
Wollmann		x		
PCHP\$				
PCUR\$				
Weimer		x		
Maier		x		
PCMA\$				

Exported 159 accounts

DICTIONARY STATUS

words total	29156
words done	29156
% done	100.000%

BRUTE FORCE

time elapsed	0d 0h 0m 0s
time left	
% done	
current test	
keyrate	

- User Info Check
- Dictionary
- Hybrid
- Brute Force

Cracken von Paßwörtern

```
C:\Programme\Tools\NetCat>john pwlist.1
Loaded 158 passwords with no different salts (NT LM DES [24/32 4K])
XXXXXXXX (nh)
X (Koers:2)
XXXXXXXX (amor98)
XXXXXXXX (amor1)
XXXXXXXX (INFODAS$)
XXXXXXXX (IFD2K$)
XXXXXXXX (GEFSTDA$)
XXXXXXXX (RECHENZENTRUM$)
XXXXXXXX (sc:1)
XXXXXXXX (Schmidt)
XXXXX (Heilmann)
XXXXX (Atik)
XXXX (b1)
XXXXXX (Ming)
XXXXXXXX (Install)
XXXXX (cspecht)
XXXXX (hmeise)
XXXXX (hadler)
XXXXXXXX (Maier)
XXXXXXXX (boeffgen:1)
XXXXXX (klaus)
XXXXXX (bo)
XXXXXXXX (Test:1)
X (Henschke:2)
XXXXXXXX (jg:1)
XXXXXX (Klinge)
XXXXXX (Backup)
XXXX (je)
XXXXXXXX (Henschke:1)
guesses: 44 time: 0:00:00:01 42% (1) c/s: 14957056 trying: `KOERSF - `DER
```

Windows NT / 2000 / XP

- Auslesen von Informationen
 - aus Dateien
 - aus der Registry
 - über Netzanfragen
- Erlangen von Administratorrechten über **getadmin**
 - Ausführen zusätzlichen Codes in privilegierten Prozessen durch „DLL-Injektion“
 - Lücke ist seit Service Pack 4 geschlossen
- Installation automatisch ausgeführter Programme
 - in der Autostart-Gruppe
 - in den Run-Schlüsseln der Registry
- Fernsteuerung über Back Orifice 2000 oder NetBus

Scannen einer Windows NT Domäne

```
C:\Programme\Tools\NetCat>netviewx -x
IGNAZ NT-serv 4.0 dom-bakctrl bak-brows Sicherungsdomänencontroller BDC
LINUS NT-serv 5.0 afp bak-brows
LUCY NT-serv 4.0 dom-ctrl print bak-brows mast-brows Domänencontroller PDC
MARCY NT-ws 4.0
PATTY NT-ws 4.0 CD-Brenner-PC 2.Stock
PCAT NT-ws 4.0
PCBA NT-ws 4.0 print
PCBAPS NT-ws 4.0
PCBC1 NT-serv 4.0
PCBO NT-ws 4.0
PCDA1 NT-ws 4.0 Bührlen PC 2.Stock
PCEL1 NT-ws 4.0
PCEXCH NT-serv 4.0
PCGN NT-ws 4.0
PCHF NT-ws 4.0 print
PCHL NT-ws 4.0
PCHP NT-ws 4.0
PCINTRA NT-serv 5.0 afp bak-brows
PCJE NT-ws 4.0
PCJG1 NT-ws 4.0
PCKG1 NT-ws 4.0
PCKH1 NT-ws 4.0
PCKHLA win95 4.0 Laptop Kh
```

Bestimmen offener Ports

```
C:\Programme\Tools\NetCat>netstat -an
```

Aktive Verbindungen

Proto	Lokale Adresse	Remoteadresse	Status
TCP	0.0.0.0:135	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:389	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:443	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:445	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:636	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:1025	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:1029	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:6000	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:11371	0.0.0.0:0	ABHÖREN
TCP	127.0.0.1:8080	0.0.0.0:0	ABHÖREN
TCP	192.168.100.86:139	0.0.0.0:0	ABHÖREN
TCP	192.168.100.86:2163	0.0.0.0:0	ABHÖREN
TCP	192.168.100.86:2163	192.168.100.190:139	HERGESTELLT
TCP	192.168.100.86:2350	192.168.100.86:389	WARTEND
TCP	192.168.100.86:2352	161.69.2.21:389	WARTEND
TCP	192.168.100.86:2354	194.171.167.2:11370	WARTEND
TCP	192.168.100.86:2355	192.168.100.196:389	WARTEND
TCP	192.168.100.86:2356	192.168.100.164:389	WARTEND
TCP	192.168.100.86:2357	161.69.2.21:389	WARTEND
TCP	192.168.100.86:2359	194.171.167.2:11370	WARTEND
TCP	192.168.100.86:2360	192.168.100.196:389	WARTEND
TCP	192.168.100.86:2361	192.168.100.164:389	WARTEND
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	127.0.0.1:10000	*:*	
UDP	192.168.100.86:137	*:*	
UDP	192.168.100.86:138	*:*	

Novell NetWare

- Aufbau anonymer Verbindungen
 - On-Site-Admin: Novell-Tool zur Remote Administration
 - Bestimmung von Adressen über `snlist` und `nslist`
 - ermöglicht Analyse der Netzstruktur
- Auswertung von Bindery und NDS-Baum
 - Bestimmung von Benutzernamen und Objekten
 - durch Zugriffsfiler kontrollierbar
- Suchen von Benutzern ohne Paßwort mit `chknull`
- Knacken von Paßwörtern mit `Nwpcrack`
- Suchen von Admin-Äquivalenten mit Pandora
- Zugriff auf den Server mit `rconsole`

Unix / Linux

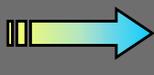
- Auslesen der Paßwort-Datei `/etc/passwd`
 - Datei ist für alle Benutzer lesbar
 - versteckte Abspeicherung in Shadow-Paßwort-Dateien
- Einschleusen eigenen Codes durch Pufferüberlauf
 - ungenügende Absicherung von Parameterübergaben
 - Standardverfahren zur Ausnutzung der Fehler
- Reverse Telnet durch Firewall hindurch
 - Starten ausgehender Verbindungen auf dem Zielsystem
 - Kopplung über `netcat` auf dem Angriffsrechner
 - Kommunikation über unverdächtige Ports (z.B. 80 / 25)

Unix / Linux

- Auslesen beliebiger Dateien über `tftp`
- Zugriff über falsch konfiguriertes anonymes `ftp`
- Ausnutzen von Fehlern in `sendmail`
- Nicht authentisierter Zugriff über Vertrauensbeziehungen
 - vertrauenswürdige Rechner in `/etc/hosts`
 - vertrauenswürdige Benutzer in `.rhosts`
 - unterläuft globale Sicherheitsvorgaben
- Normalerweise keine (wirksame) Authentikation von RPC-Nachrichten

Unix / Linux

- **r**-Kommandos (**rlogin** etc.) verwenden die (fälschbare) IP-Adresse als Authentisierung
- Einschleusen Trojanischer Pferde
 - durch Installation von **setuid**-Dateien („root shell“)
 - durch Austausch existierender Dateien
 - erfordert nur Schreibzugriff auf das übergeordnete Verzeichnis
 - kein Zugriffsrecht auf die Datei selbst erforderlich
- Zugriff über falsch konfiguriertes NFS
- Austricksen der shell über manipulierte IFS-Variable

 **Gegenmaßnahmen erfordern genaue Kenntnisse**

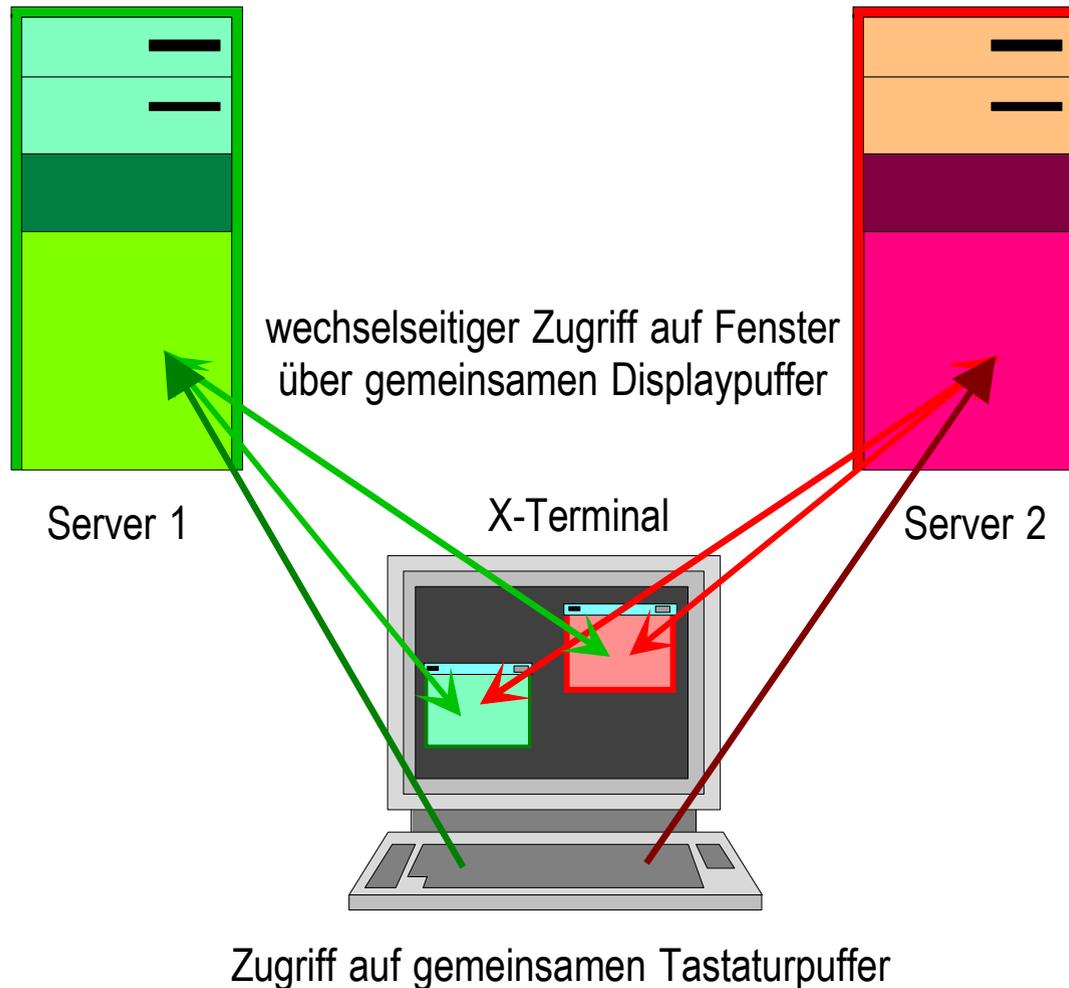
Lücken im X-Windows-System

- Nur sehr schwache Authentifikations-Mechanismen
 - Vergleich der Netzadresse des Auftraggebers mit einer Liste erlaubter Adressen
 - keine benutzerabhängige Kontrolle
 - Schlüsselverteilung für kryptographische Authentifikationsverfahren (und auch Verteilung der „magic cookies“) weitgehend ungelöst / in Standard-Implementierungen nicht enthalten

Lücken im X-Windows-System

- X-Window-Anwendungen mit Zugriff auf den Display-Puffer haben auch Zugriff auf:
 - den Inhalt anderer Fenster auf demselben X-Server
 - Gefahr des Diebstahls von Informationen aus fremden Anwendungen
 - Gefahr der Manipulation der Darstellung fremder Anwendungen
 - den Tastaturpuffer anderer Anwendungen, die Fenster auf demselben X-Server darstellen
 - Gefahr des Diebstahls von Informationen aus fremden Anwendungen
 - Gefahr der Manipulation von Benutzer-Eingaben

Lücken im X-Window-System



Einwahlknoten und RAS / VPN

- Herausfinden der Einwahlnummern
 - Bestimmen „interessanter“ Telephonnummernbereiche
 - systematisches Anrufen mit Wardialern (ToneLoc, THC-Scan, PhoneSweep)
- Testen, was dahinter liegt

 **Gegenmaßnahmen: Call-Back und Kontrollen**

- Ausnutzen von Schwächen der Technik:
 - Schwächen des Protokolls CHAP
 - Implementierungsfehler im Protokoll PPTP

 **Gegenmaßnahme: Einsatz von IPsec**

Firewalls

- Bestimmen des Firewall-Typs
 - Bestimmen typischer Ports durch Port-Scan
 - Abfragen von Dienst-Bannern

 **Gegenmaßnahme: Informationen im Firewall bzw. im Router davor blockieren**

- Durchgriff durch das Firewall-System:
 - Firewalking: Abfragen von Ports hinter dem Firewall
 - Tunneling: Verpacken in DNS- / ICMP- / UDP-Paketen
 - Ausnutzen falsch konfigurierter Proxies / von DCOM

 **Gegenmaßnahme: restriktive Konfiguration**

Denial-of-Service Angriffe

- Einfache Angriffe reduzieren die Netzbandbreite durch permanente Übermittlung großer Datenmengen (z.B. UDP Flooding)
- Komplexe Angriffe nutzen Schwachstellen der verwendeten Protokolle aus, um einen Zusammenbruch einzelner Rechner / des Gesamtnetzes zu provozieren:
 - „Ping of Death“: ICMP Echo Request mit Pufferüberlauf
 - „Smurf“: ICMP Echo Request an Broadcast Adresse mit gefälschtem Absender

Denial-of-Service Angriffe

- Spezifisch: SYN-Attacke in TCP/IP-Netzen
 - TCP/IP baut Verbindungen in mehreren Schritten auf:
 - Sender meldet Verbindungswunsch durch ein SYN-Paket
 - Empfänger quittiert den Wunsch und signalisiert damit seine Empfangsbereitschaft
 - Sender quittiert diese Quittung - damit steht die Verbindung
 - Angriff durch Überflutung eines Rechners mit SYN-Paketen mit verschiedenen (gefälschten) Absendern
 - Empfänger baut für jedes SYN-Paket eine Verbindung auf und wartet auf die 2. Quittung
 - irgendwann sind die Ressourcen des Empfängers erschöpft
 Deadlock / Crash!
 - Time-out der aufgebauten Verbindungen ist wirkungslos, wenn die SYN-Pakete zu schnell ankommen

Verteilte Denial-of-Service Angriffe

- Zielrechner wird durch systematische Datenüberflutung zum Zusammenbruch gebracht
 - Überflutung mit UDP-Nachrichten / SYN-Attacken / ICMP Echo Request
 - Überflutung mit über ICMP gesteuerten Broadcasts

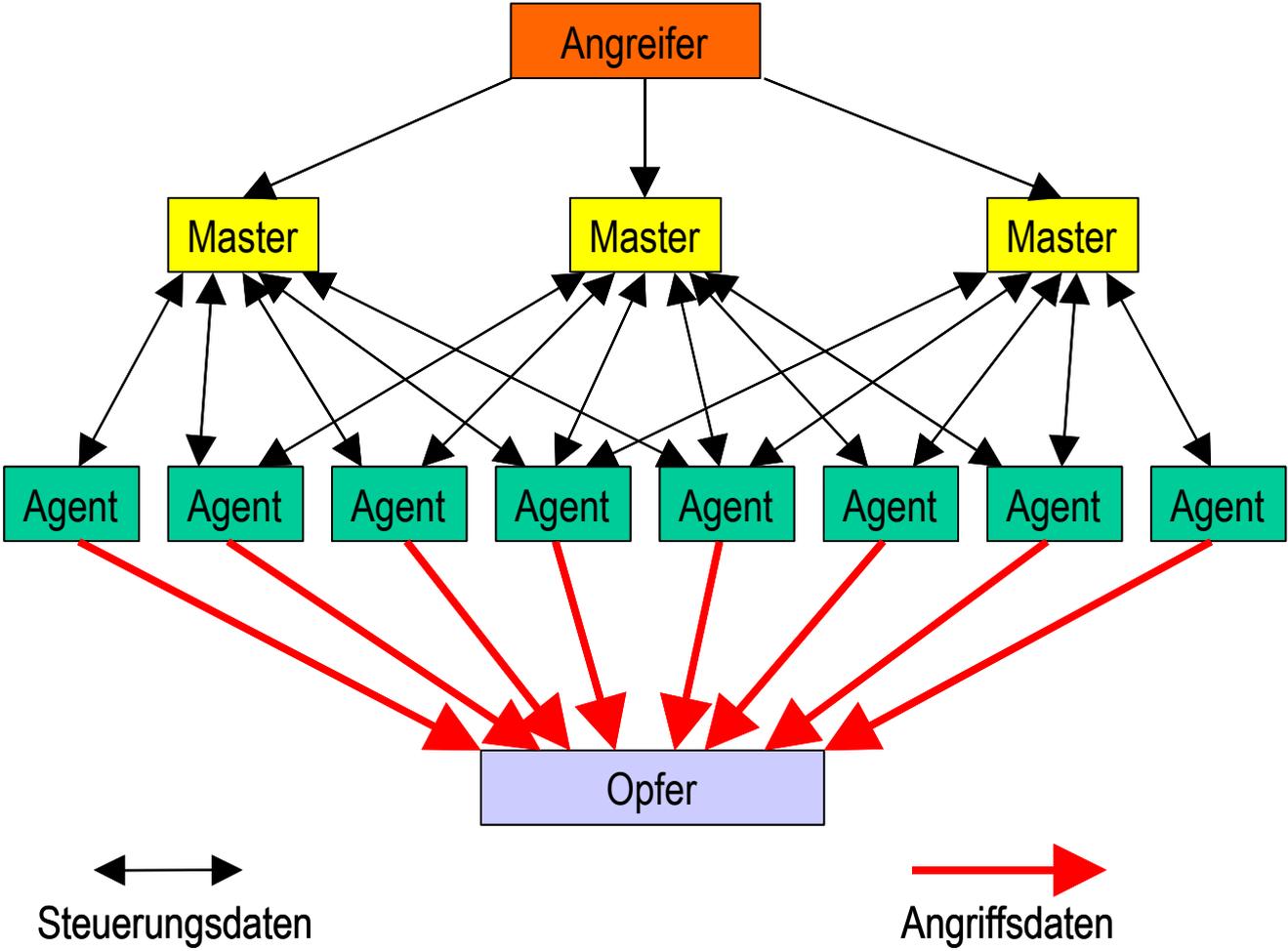
Verteilte Denial-of-Service Angriffe

- Angriff erfolgt über Rechner, auf denen fernsteuerbare Angriffsprogramme („Agenten“, „Daemons“) installiert werden
 - Installation auf beliebigen, ungeschützten Rechnern möglich
 - Installation über Upload oder durch Einschleppen von Viren
 - Betreiber weiß oft nicht, daß sein System für den Angriff mißbraucht wird
 - Angriffsrechner können die Datenmenge vervielfachen (besonders MacOS 9)

Verteilte Denial-of-Service Angriffe

- Angriffsprogramme werden über ferngesteuerte, verteilte Steuerungsprogramme („Master“) mit Aufgaben versorgt
 - Installation ebenfalls auf ungeschützten Rechnern ohne Wissen der Betreiber
 - geschützte, z.T. verschlüsselte Kommunikation mit den Agenten sowie mit dem Steuerprogramm auf dem Rechner des Hackers
- Mehrere Tools im Netz verbreitet (trin00, TFN, TFN2k, Stacheldraht)

Verteilte Denial-of-Service Angriffe



Ausnutzen von Remote Control

- Erlaubt volle Kontrolle über das Zielsystem
- Ausnutzen bekannter Schwachstellen
 - Übertragen von Benutzernamen / Paßwort im Klartext
 - Verwendung schwacher Verschlüsselung
 - Abspeichern von Paßwörtern in Dateien / der Registry
 - Auslesen verdeckt eingegebener Paßwörter
 - Kopieren von Profilen auf das Zielsystem



Gegenmaßnahmen:

- Paßwortmanagement / alternative Beglaubigungen
- Zugriffsschutz auf Profile und Setup-Dateien

TCP Hijacking und Hintertüren

- Ausnutzen von Schwächen in der Erzeugung der Sequenznummern für TCP
 - Erraten der nächsten legalen Nummer
 - Senden von Nachrichten mit der erratenen Nummer
 - Angriff erfolgt mit Tool-Unterstützung (Juggernaut, Hunt)

 **Gegenmaßnahme: Switching-Technik**

- Einbau von Hintertüren:
 - Installation von Benutzern / Programmen / Cron-Jobs
 - Einträge in Start-Dateien / Autostart-Gruppe / Registry
 - Installation von Remote Control Software

 **Gegenmaßnahme: Überwachung des Systems**

Trojanische Pferde

- „Timeo Danaos et dona ferentes“:

Vertrauen Sie keiner kostenlosen Software,
die Ihnen angeboten wird!

- an der Oberfläche nützlich / angenehm
(Bildschirmschoner, Spiel, Utility)
- im Hintergrund Installation einer Hintertür etc.

- Typische Beispiele:

- Whack-A-Mole: Spiel mit NetBus-Installation
- BoSniffer: Installiert Back Orifice, statt es zu entfernen
- eLiTeWarp: Packer zur Installation von Trojanern
- FPWNTCLNT.DLL: Abfangen von Paßwörtern

Angriffe auf Web-Server

- Web-Diebe: Durchsuchen von HTML-Seiten nach Code / Fehlern / Paßwörtern / Telephonnummern
- Automatische Suche nach angreifbaren Seiten:
 - Pufferüberläufe im Server
 - erlauben Ausführen eigenen Codes auf dem Server
 - Durchgriff auf die Kommando-Schnittstelle
 - ungenügende Überprüfung von Benutzereingaben
 - im Phone Book Skript (PHF)
 - in schlecht programmierten CGI-Skripten
 - durch Auslesen von Active Server Pages (ASP)
- Ausnutzen schlechter Web-Programmierung

 Gegenmaßnahmen: Sorgfalt und Kontrolle

Weitere Informationen

- George Kurtz, Stuart McClure, Joel Scambray:
Das Anti-Hacker-Buch; MITP-Verlag, Bonn, 2000
- Web-Adressen:
 - <http://www.cert.org>
 - <http://www.nmrc.org>
 - <http://www.securityfocus.com>
 - <http://www.microsoft.com/security/>
 - <http://www.ntbugtraq.com>
 - <http://www.w3.org/Security/Faq/wwwsf4.html>
 - <http://www.hackingexposed.com>