
Angriffsmethoden der Hacker

Dr. Gerhard Weck, INFODAS GmbH, Köln

25. DECUS Symposium 2002 in Bonn
Vortrag 1F01

Inhalt

- Vorbereitung des Angriffs
 - Footprinting – Die Wahl des Angriffsziels
 - Scanning – erste Informationen
 - Auswertung und Angriffsplanung
- Angriffe auf gängige Betriebssysteme
- Angriffe auf Netzwerk-Komponenten
- Fortgeschrittene Angriffstechniken
 - TCP Hijacking
 - Hintertüren und Trojanische Pferde
 - Angriffe auf Web-Server
 - Denial-of-Service Angriffe
- Statistiken

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

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 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]

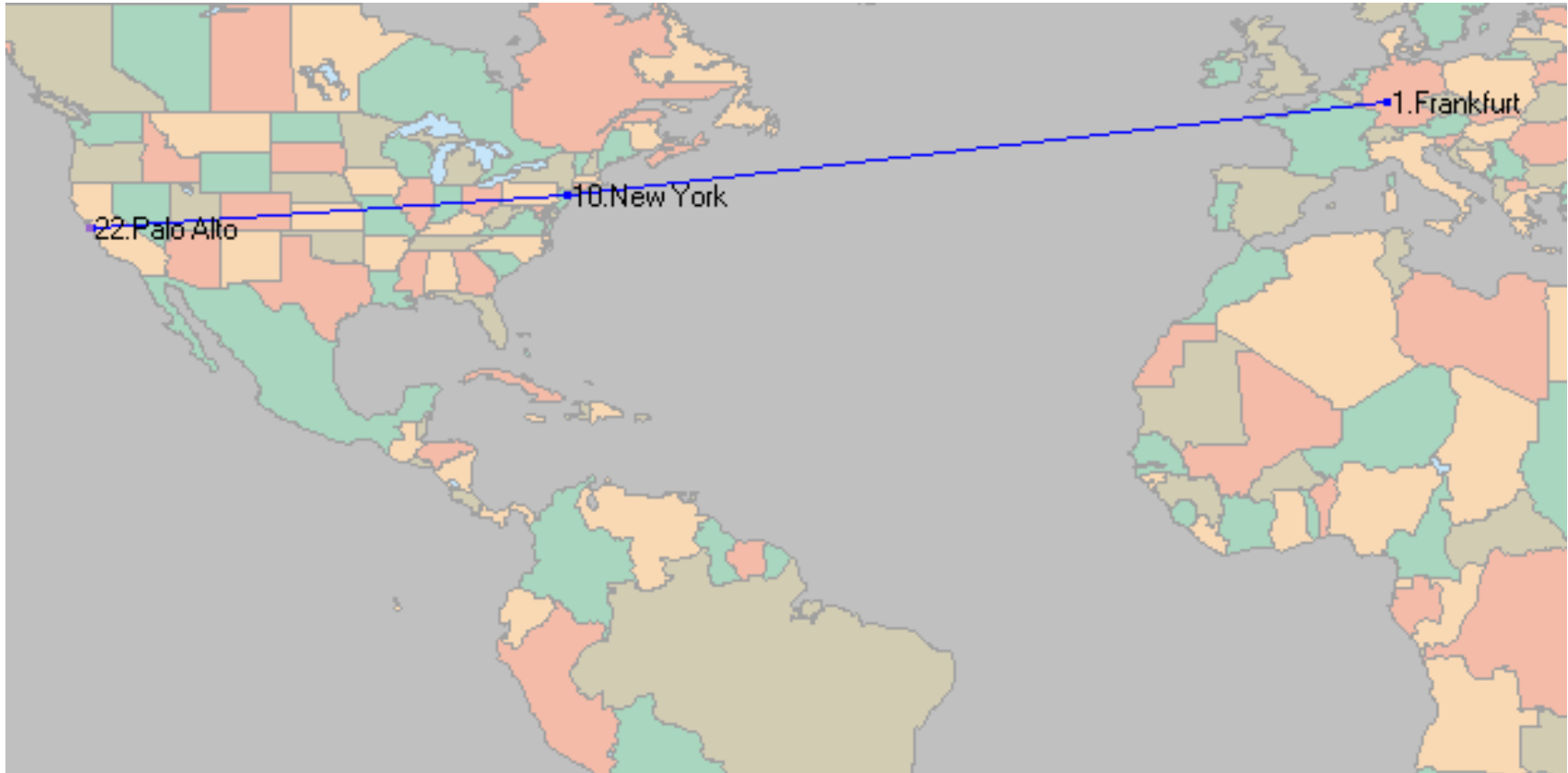


Analysis: 'www.altavista.com' was found in 22 hops (TTL=231). It is a HTTP server (running AW/1.0.1).

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
```

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`)
- Auswertung von Novell NetWare Netzen
 - Abfrage des Windows Netzwerk Browsers
 - Abfragen mit On-Site-Admin (ohne Anmeldung!)
- Auswertung von Unix-Netzen
 - Bestimmung von Netzwerk-Ressourcen / NIS
 - Suchen von Benutzer-Informationen (`finger`)
 - Auswertung von Anwendungen / Bannern (`rpcinfo`)

Angriffe auf Windows NT/2000/XP

- Auslesen von Informationen
 - aus Dateien / aus der Registry / über Netzanfragen
 - Abfragen über nicht authentifizierte „Null-Sessions“
- Erlangen von Administratorrechten über **getadmin**
 - Ausführen zusätzlichen Codes in privilegierten Prozessen durch „DLL-Injektion“
 - Lücke wurde mit Service Pack 4 geschlossen und ist inzwischen wieder geöffnet
- Installation automatisch ausgeführter Programme
 - in der Autostart-Gruppe
 - in den Run-Schlüsseln der Registry

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 columns: User Name, LM Password, <8, NTLM Password, and Audit Time. The table lists 19 users, with 'Administrator' and 'Gast' having 'x' in the '<8' column, and 'Krey' having 'x' in the 'NTLM Password' column. The 'Audit Time' column shows "0d 0h 0m 0s". To the right is a "DICTIONARY STATUS" panel showing "words total: 29156" and "words done: 29156", with "% done" at "100.000%". Below it is a "BRUTE FORCE" panel showing "time elapsed" and "time left" as "0d 0h 0m 0s", and "% done" as empty. At the bottom right are checkboxes for "User Info Check", "Dictionary", "Hybrid", and "Brute Force", all of which are checked. The status bar at the bottom left says "Exported 159 accounts".

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\$				

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)
XXXXXX  (Heilmann)
XXXXXX  (Atik)
XXXXXX  (b1)
XXXXXX  (Ming)
XXXXXXXX (Install)
XXXXXX  (cspecht)
XXXXXX  (hmeise)
XXXXXX  (hadler)
XXXXXXXX (Maier)
XXXXXXXX (boeffgen:1)
XXXXXX  (klaus)
XXXXXX  (bo)
XXXXXXXX (Test:1)
X        (Henschke:2)
XXXXXXXX (jg:1)
XXXXXX  (Klinge)
XXXXXX  (Backup)
XXXXXX  (je)
XXXXXXXX (Henschke:1)
guesses: 44  time: 0:00:00:01 42% (1)  c/s: 14957056  trying: `KOERSF - `DER
```

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	*:*	

Angriffe auf Unix / Linux

- Einschleusen eigenen Codes durch Pufferüberlauf
 - ungenügende Absicherung von Parameterübergaben
 - Standardverfahren zur Ausnutzung der Fehler
 - funktioniert auch bei Windows
- 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)
- Auslesen beliebiger Dateien über `tftp`

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
- Fernsteuerung über Back Orifice 2000 oder NetBus

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

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
- 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

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

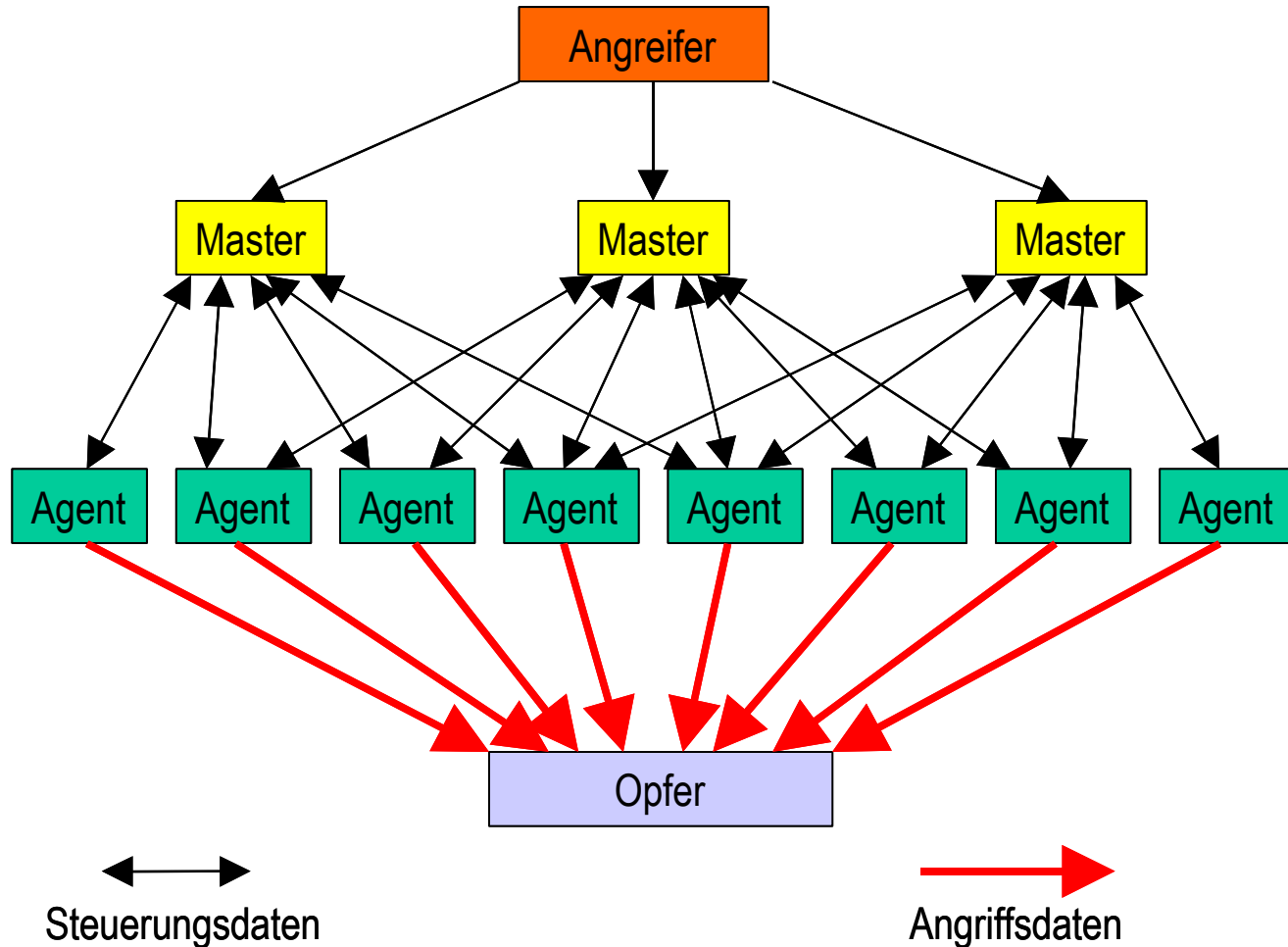
Verteilte Denial-of-Service Angriffe

- 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

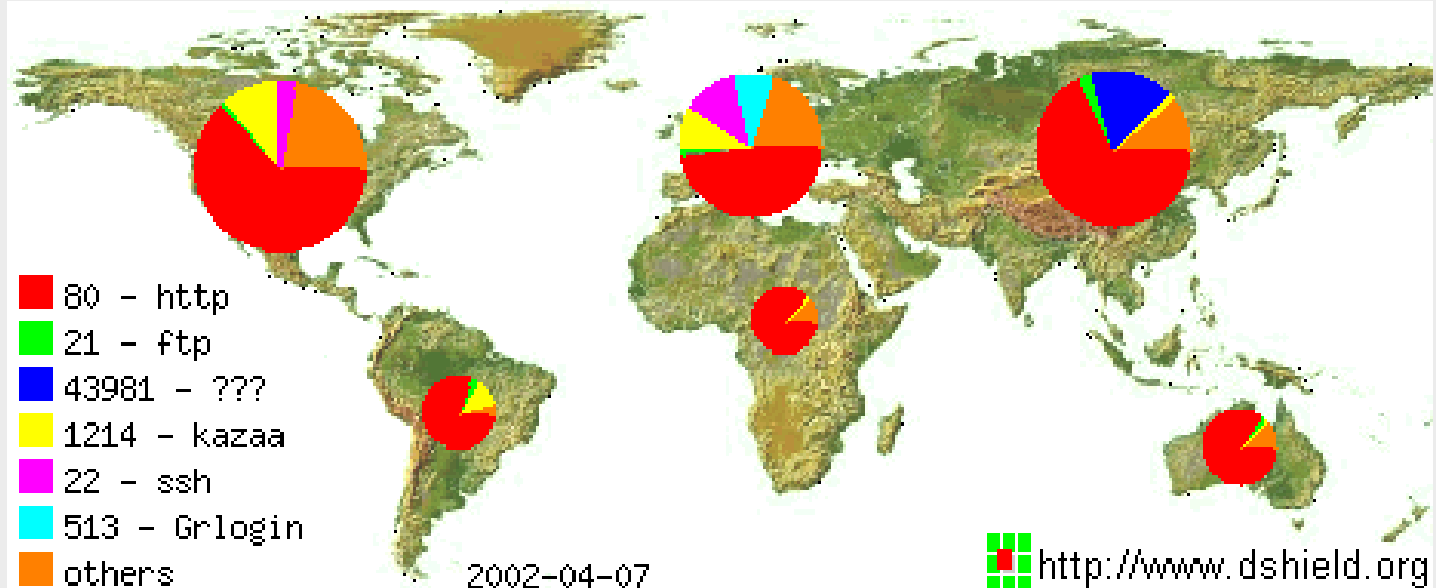


Verteilung der Angriffe

As of April 08, 2002 07:03 am GMT

Top Attacker: 151.196.219.30




Most Attacked Port: 80



Geographic Distribution of attack sources. Last 5 days

DSShield, The Movie

Häufigste Angreifer

IP Address	Host Name
152.66.208.66 ^{191666/} ₉₆₃₁₈	gigant.sch.bme.hu
128.104.182.159 ^{92024/} ₉₂₀₂₃ 	pc614.bme.wisc.edu
141.217.86.26 ^{89621/} ₈₉₆₂₀ 	spawn.iog.wayne.edu
134.2.62.152 ^{78953/} ₇₈₉₅₃	tuna.biol.biologie.uni-tuebingen.de
63.175.111.67 ^{57948/} ₃	63.175.111.67
166.114.182.76 ^{56318/} ₅₆₂₅₀	166.114.182.76
206.55.237.6 ^{35376/} ₃₅₃₇₅	dolphin.mbay.net
130.104.56.130 ^{31264/} ₃₁₂₆₁	130.104.56.130
62.243.88.196 ^{46828/} ₃₀₄₉₂ 	psych0dad.webspeed.dk
195.145.52.5 ^{54951/} ₃₀₁₀₇	195.145.52.5

Charakteristika eines Angreifers

IP
Address: 152.66.208.66

HostName: gigant.sch.bme.hu

DShield
Profile:

Country:	HU
Contact E-mail:	remzso@eik.bme.hu
Total Records against IP:	191666
Number of targets:	96318
Date Range:	2002-01-11 to 2002-01-11

Ports Attacked (up to 10):

Port	Attacks
22	191666

Whois: Technical University of Budapest Centre of
Information Systems (NET-HUNGARNET-B01)
Muegyetem rkp. 9. R. III. 310.
BUDAPEST, H-1111 HU

Netname: HUNGARNET-B01

Netblock: 152.66.0.0 - 152.66.255.255

Coordinator: Technical University of Budapest(BME) Centre of
Information Systems (EISzK)
(ZT9-ARIN) remzso@eik.bme.hu +36 1 4631821

Domain System inverse mapping provided by:
NIC.BME.HU 152.66.115.1
NS.BME.HU 152.66.116.1

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>