Sicherheit durch Penetrationstests

Hacking im Auftrag –
oder echte Sicherheitsanalyse?

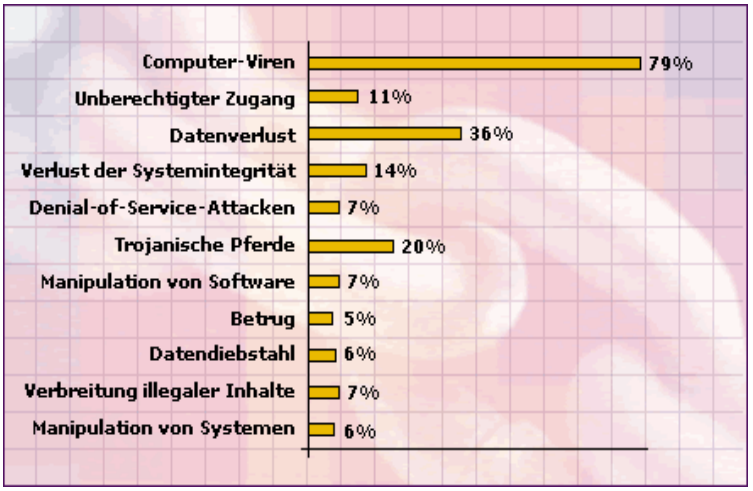
Dr. G. Weck
INFODAS GmbH
Köln

infodas

Inhalt

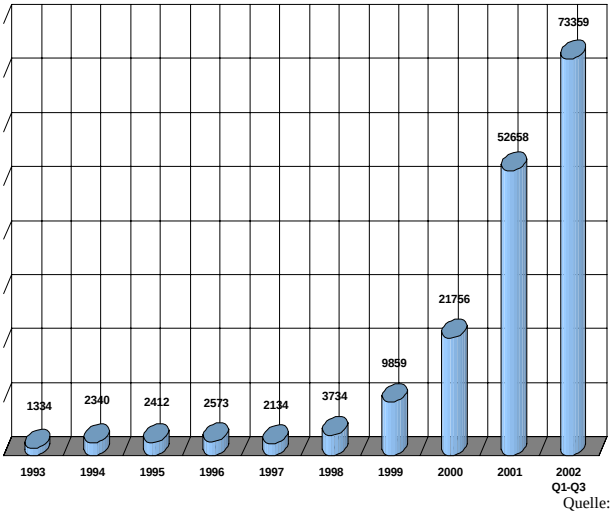
- Motivation: Wozu braucht man IT-Sicherheit?
- Schwachstellen
- Sicherheitskonzepte und Penetrationstests – Widerspruch oder Ergänzung?
- Vor- und Randbedingungen der Penetrationstests
- Simulierte / kontrollierte Hackerangriffe
- Vorgehensweise
- Werkzeuge
- Empfehlungen und Ausblick

Aktuelle Sicherheitsprobleme



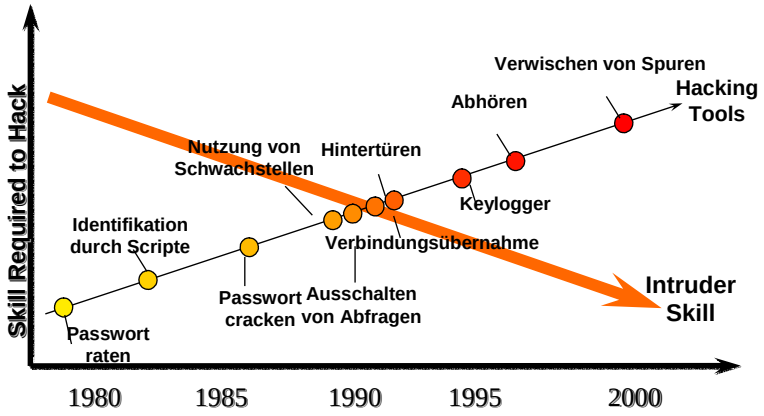
Quelle: Computer Crime and Security Survey 2001

Weltweit gemeldete IT-Sicherheitsvorfälle



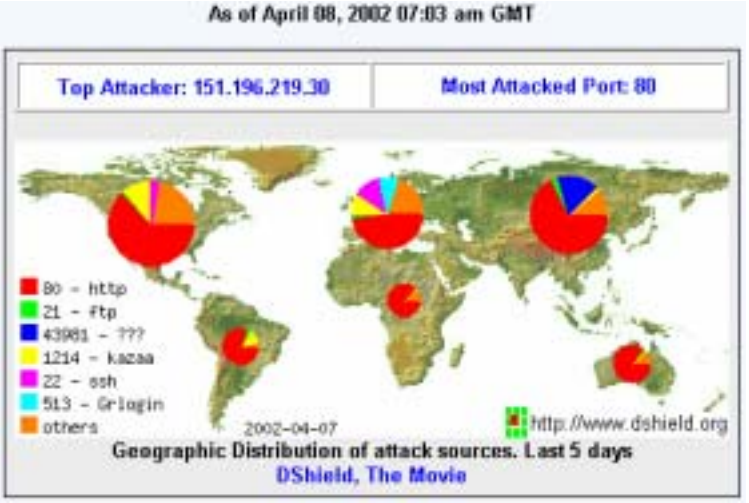
Quelle: www.cert.org, 2002

Hacking wird immer einfacher



infodas

Verteilung der Angriffe



infodas

Häufigste Angreifer

IP Address	Host Name
152.66.208.66 191686/96319	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 78963/78963	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 35375/35375	dolphin.mbay.net
130.104.56.130 31264/31261	130.104.56.130
62.243.88.196 46820/30492	psych0dad.webspeed.dk
195.145.52.5 54961/30107	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	191686
Number of targets	96318
Date Range	2002-01-11 to 2002-01-11

Ports Attacked (up to 10)

Port	Attacks
22	191686

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

Schwachstellen

- Angriffpunkte in Rechnern:
  - fehlerhafte / ungeschützte Software
    - Dienste: SMB / NFS / SMTP / FTP
    - Anwendungen: Web-Server / Browser / E-Mail
  - Übertragung von Paßwörtern im Klartext
    - Telnet / FTP / POP3
    - Zugriff auf Anwendungen
  - ungenügende Verschlüsselung
    - LAN Manager Verschlüsselung bei Windows
    - Zugriff auf Anwendungen

Schwachstellen

- Angriffsmöglichkeiten im Netz:
  - Abhören
    - von Daten
    - von Authentisierungen (Paßwörtern etc.)
    - von Kommunikationsbeziehungen
  - Maskerade / Impersonation
  - Verfälschung von Daten
  - „Man-in-the-Middle“ Angriffe
  - Leugnen der Kommunikationsbeziehung
  - Datenüberflutung / Denial of Service

Schwachstellen

- Organisatorische Mängel:
  - ungenügende Paßwortverwaltung
  - permissive Zugriffskontrolle
  - Verzicht auf Überwachung / Protokollierung
  - Einsatz fehlerhafter Software
    - ungeeignete Betriebssysteme
    - schlampig programmierte Web-Dienste
  - Anbieten überflüssiger Dienste
  - ungesicherte Zugänge zum Netz
  - zu späte / ungenügende Übernahme von Sicherheitspatches

Verfahren zur Absicherung

- IT-Sicherheitskonzepte als konstruktive Sicherheit
  - Analyse der Sicherheitsanforderungen
  - Risiko- und Schwachstellenanalyse
  - Maßnahmenempfehlungen

⇒ systematische Bestimmung notwendiger Aktionen
⇒ Gefahr des Übersehens „untypischer“ Angriffe

- Penetrationstests als Analyse potentieller Lücken

⇒ Mittel zum Auffinden technischer Lücken
⇒ bieten keine Gesamtsicht der Sicherheit

Beide Verfahren ergänzen sich notwendigerweise

Vor- und Randbedingungen

- Juristische Absicherung
  - Angriffe gegen fremde Rechner sind strafbar !!!
  - Penetrationstests erfordern daher
    - einen klaren Auftrag des Systembetreibers
    - eine genaue Abgrenzung von Umfang und Ziel der Tests
    - explizite, schriftliche Beauftragung durch den Verantwortlichen
- Abgrenzung des Angriffsziels und der Methoden
  - keine Angriffe gegen zusätzliche Ziele
  - definitive Beschränkung auf vereinbarte Methoden
- Ausführliche, detaillierte Dokumentation
  - zur Gewährleistung der Nachvollziehbarkeit
  - zur Absicherung gegen Nebeneffekte

Simulierte / kontrollierte Hackerangriffe

- Interne Angriffe
  - sind angekündigt und der Systemverwaltung bekannt
  - testen die Sicherheit des technischen Systems
  - verwenden interne Informationen (“white box”)
  - sind ggf. wegen temporärer Korrekturen unrealistisch
- Externe Angriffe
  - sind nur dem Management des Auftraggebers bekannt
  - testen zusätzlich die Sicherheit des operationellen Umfelds
  - verwenden nur allgemein zugängliche Informationen (“black box”)
  - können ggf. als echte Angriffe aufgefaßt und behandelt werden

Vorgehensweise von Hackern

- Vorbereitung
  - Footprinting – Die Wahl des Angriffsziels
  - Scanning – erste Informationen
  - Auswertung und Angriffsplanung
- Angriffstechniken
  - Pufferüberlaufprobleme
  - Angriffe auf gängige Betriebssysteme
  - Denial-of-Service Angriffe
- Komplexere Techniken
  - TCP Hijacking
  - Hintertüren und Trojanische Pferde
  - Angriffe auf Web-Server

Schritte eines Penetrationstests

- Festlegung der Teststruktur
  - Art des Tests: intern / extern
  - Angriffsziele und Methoden
  - Art und Umfang der Dokumentation
- Auskundschaften des Testobjekts
  - Footprinting: Sammeln allgemein verfügbarer Information
  - Scanning: Analyse der Netzstruktur
- Verwundbarkeitsanalyse: Suchen nach Lücken
- Penetration: Ausnutzen der gefundenen Lücken

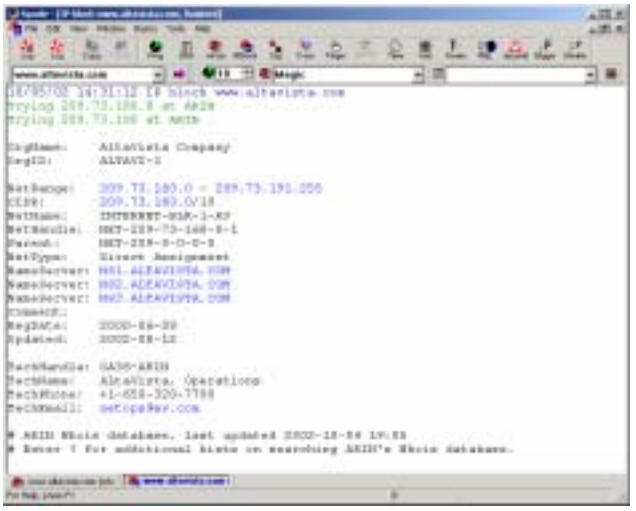
Werkzeuge zur Analyse der Netzstruktur

- Discovery Tools
  - WS-Ping ProPack (umfangreiche Tool-Box)
  - NetScanTools (umfangreiche Tool-Box)
  - Sam Spade (zur Routen- und DNS-Analyse)
  - Rhino9 Pinger (zum schnellen Durchsuchen mit Ping)
  - VisualRoute (geographische Analyse von Routen)
  - What's running (Laden von Programm-Identifikationen)
- Port Scanner
  - Nmap (äußerst leistungsfähiger Port-Scanner)
  - 7th Sphere Port Scanner (liest auch Banner)
  - Super Scan (gibt auch Zuordnung Dienste ↔ Ports aus)

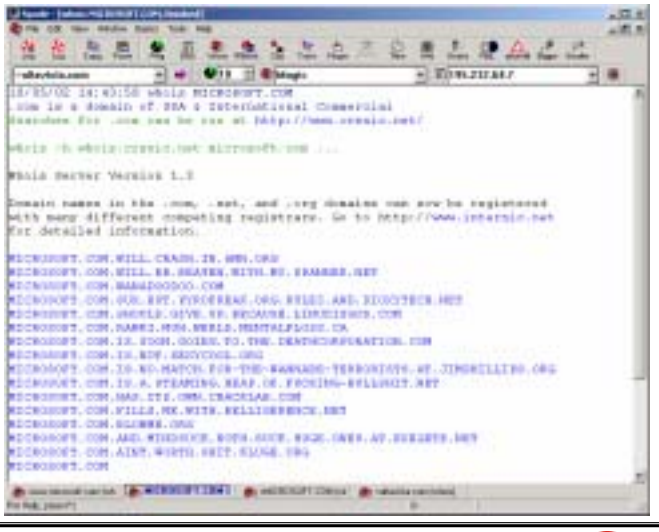
Erste Analyse des Angriffsziels

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

Abfrage der arin-Datenbank



whois-Abfrage



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

Suche nach angreifbaren Rechnern

Analyse der Netzstruktur

Beispiel für `tracert`

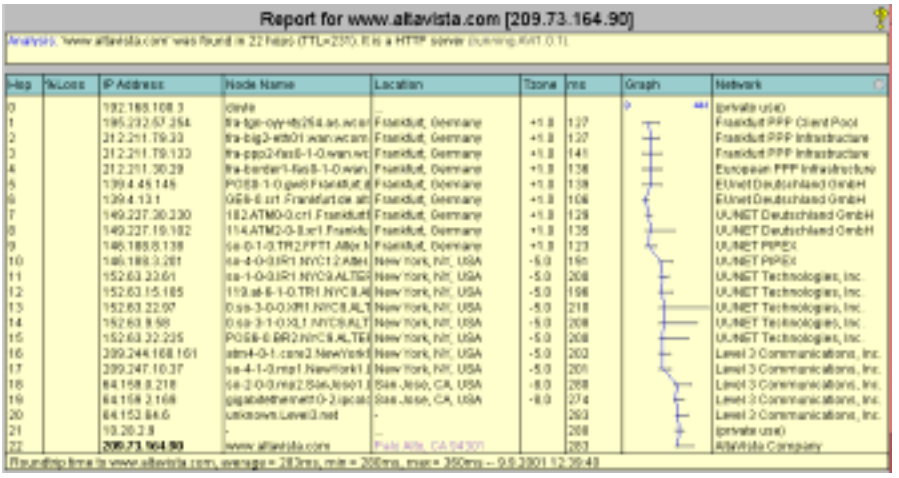
```
C:\>tracert www.altavista.com

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

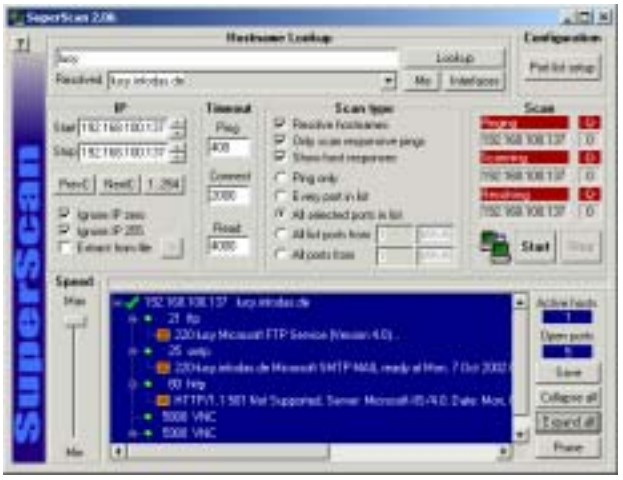


Zugriffsweganzeige von Visualroute

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
```

Port-Scan eines Windows NT Servers



Port-Scan eines Linux-Systems

Erkennen des Betriebssystems

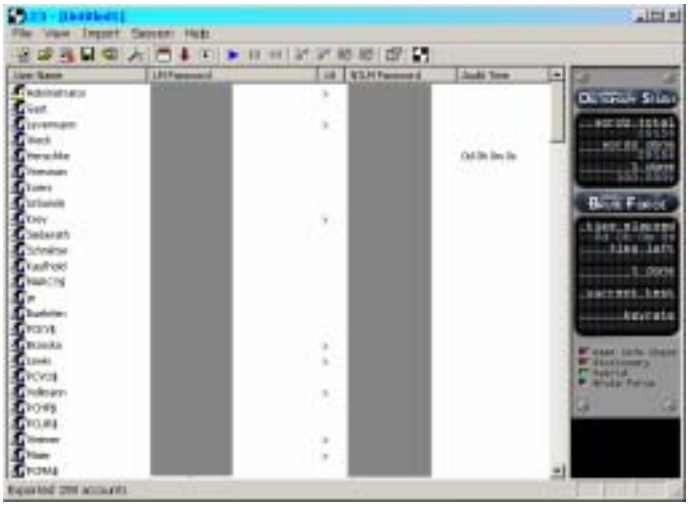
Werkzeuge zur Informationsbeschaffung

- Lesen der übertragenen Daten mit Sniffern
  - Dsniff (Zugriff auf Paßwörter, E-Mail, Web-Daten)
  - Linsniff (liest den Anfang jeder TCP-Verbindung)
  - Tcpdump / WinDump (liest / filtert den Netzverkehr)
- Password Cracker
  - L0phtCrack: entschlüsselt NT Paßwörter
  - pwdump2: entschlüsselt auch mit SYSKEY doppelt verschlüsselte Paßwörter
  - John the Ripper: skriptgesteuertes Crack-Programm für Unix und Windows NT

Cracken von Paßwörtern

- Windows NT / 2000 / XP
  - 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 **`l0pthcrack`** / **`LC3`** oder **`john`** (the ripper)
- Unix / Linux
  - Auslesen der Paßwort-Datei **`/etc/passwd`**
    - Datei ist für alle Benutzer lesbar
    - versteckte Abspeicherung in Shadow-Paßwort-Dateien

Cracken von Paßwörtern



Cracken von Paßwörtern

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

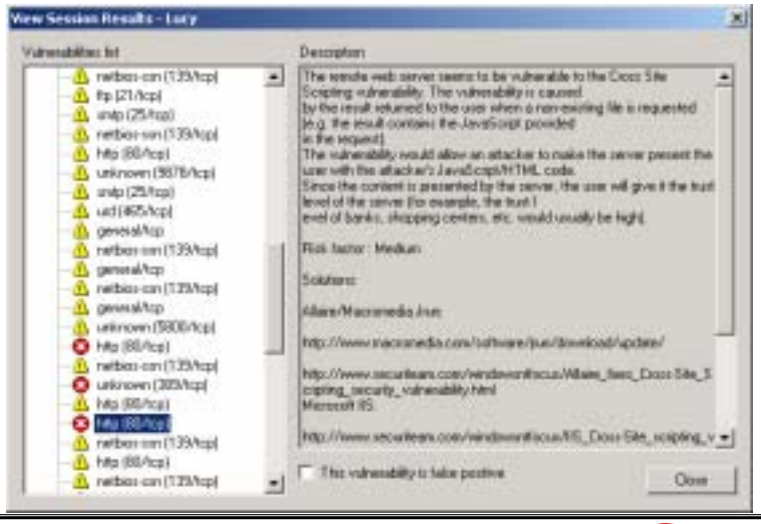

Password-Spoofer

- Programm setzt READ auf Terminal auf
- Spiegelt Login („Username: “, „Password: “) vor
- Simuliert Paßwort-Fehler („User authorization failure“)
- Schreibt gelesenes Paßwort in private Datei
- Gibt Terminal für echtes Login frei

Werkzeuge zur Schwachstellenanalyse

- Netzorientierte Verwundbarkeits-Scanner
  - Network Associates CyberCop Scanner
  - ISS Internet Scanner
  - Nessus (unter GNU-Lizenz)
  - Symantec NetRecon (analysiert auch NetWare)
  - Bindview HackerShield
- Host-Basierte Scanner
  - Symantec Enterprise Security Manager (ESM)
  - Pentasafe VigilEnt (auch für IBM AS/400)
  - NetIQ (auch für netzweites Sicherheitsmanagement)

Nessus: Verwundbarkeitsanalyse



Windows NT / 2000 Werkzeuge

- Bordmittel von Windows:
  - NET USE / Null Connection: Aufbau von Verbindungen
  - NET VIEW: Namen von Domänen, Rechnern, Shares
  - Getmac: bestimmt die Hardware-Adresse
- Werkzeuge anderer Anbieter:
  - DumpSec: Auslesen der Benutzer-Informationen
  - user2Sid / sid2User: Umsetzung Namen ↔ SIDs
  - NetBIOS Auditing Tool (NAT): Erraten von Paßwörtern
  - SMBGrind: Ausprobieren von Paßwortlisten
  - DumpReg: Auslesen von Registry-Informationen
  - Netcat (NC): „Schweizer Taschenmesser“ des Hackers
  - FPipe: Umleiten von Ports

Werkzeuge des Windows Resource Kits

- Informationsdienste:
  - NLTEST / NETDOM: Identifikation von Servern
  - Local Administrators / Global (“Domain Admins”)
  - Usrstat: Benutzerinformationen eines PDC / BDC / DC
  - SRVCHECK / SRVINFO: Informationen über Server
  - REGDMP: Auslesen von Informationen aus der Registry
- Steuerung von Systemen über das Netz:
  - AuditPol: Auslesen / Ein-/Ausschalten der Überwachung
  - Remote: Fernzugriff auf die Kommandozeile
  - SC / AT: Kontrolle / Verwendung des Schedulers

Angriffe auf 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

Unix-Werkzeuge

- Zugriff auf Dienste
  - Netcat (NC): Verbinden von Ports mit stdin / stdout
  - Auswertung von Konfigurations-Dateien:
    - **`/etc/hosts.equiv`** und **`.rhosts`** (Login ohne Paßwort)
    - **`/etc/inetd.conf`** (Bestimmung der gestarteten Dienste)
    - **`/etc/exports`** (Zugriff auf NFS-Dateistrukturen)
    - **`/etc/passwd`** (Benutzernamen und ggf. auch Paßwörter)
  - Schwachstellen in NFS, X-Windows, **`sendmail`**, ...
- Ausnutzen von Pufferüberlauf
- Falsche Zugriffsrechte auf Dateien
- Fehler in Anwendungen (Apache, BIND, ...)

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`**

Spezielle Werkzeuge

- Web-Testing Tools
  - Whisker: Perl-basierter CGI-Scanner
  - SiteScan: Tests für Schwachstellen von Servern
  - THC Happy Browser: Penetrationstests von Servern
  - wwwhack / Web Cracker / Brutus:
    Paßwort-Cracker für Web-Server
- Remote Control
  - pcAnywhere / Virtual Network Computing (VNC):
    Fernzugriff auf Windows NT / 2000
  - NetBus / Back Orifice 2000:
    Hacker-Tools mit Einbau von Hintertüren zur
    Fernsteuerung von Windows NT / 2000

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!

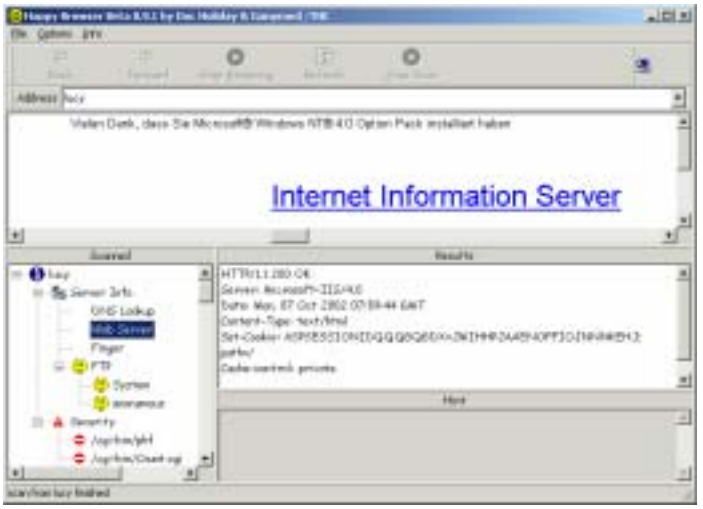
- an der Oberfläche nützlich / angenehm (Bildschirmschoner, Spiel, Utility)
  - im Hintergrund Installation einer Hintertür etc.
- Typische Beispiele:
  - Whack-A-Mole: Spiel mit NetBus-Installation
  - BoSniffer: Installiert Back Orifice, statt es zu entfernen
  - eLiTeWrap: Packer zur Installation von Trojanern
  - FPWNTCLNT.DLL: Abfangen von Paßwörtern

Angriffe auf Web-Server

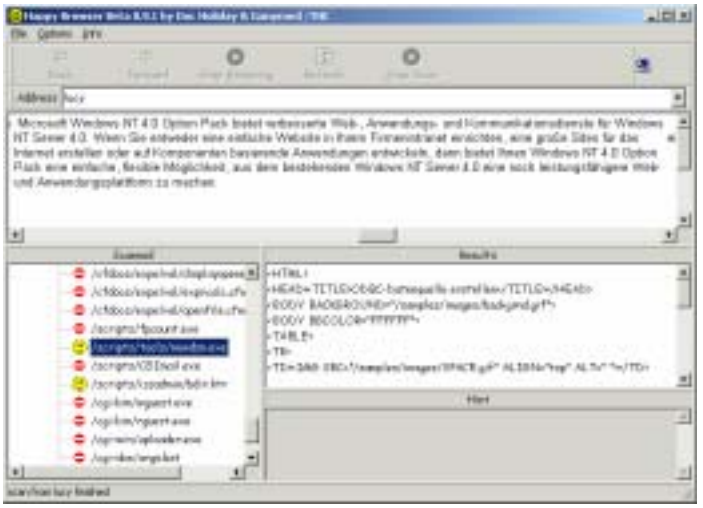
- Web-Diebe: Durchsuchen von HTML-Seiten
  - nach Code / Fehlern / Paßwörtern / Telephonnummern
- Suche nach angreifbaren Seiten:
  - Pufferüberläufe im Server
    - erlauben Ausführen eigenen Codes auf dem Server
    - Durchgriff auf die Kommando-Schnittstelle
  - ungenügende Überprüfung von Benutzereingaben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

Lesen der Anwendungs-Identifikation

Suchen nach Lücken in Web-Servern



Suchen nach Lücken in Web-Servern



Empfehlungen und Ausblick

- Einsatz zusätzlicher Schutzmaßnahmen
  - verbesserte Authentifikation
    - Single Sign-on über zentralen Dienst im Netz (z.B. Kerberos)
    - Einsatz mehrerer Komponenten (Besitz + Wissen / Chipkarte)
  - einheitliche Verwaltung durch Verzeichnisdienste
  - Verschlüsselung sensitiver Daten
- Timesharing statt Client/Server
  - zentralisierte, einheitliche Verwaltung
  - Verzicht auf unsichere Desktop-Systeme
- Einsatz von Analyse- und Nachweis-Systemen
- Versicherung gegen Schäden

Weiterführende Informationen

- T. J. Klevinsky, S. Laliberte, A. Gupta:
  Hack I.T. – Security Through Penetration Testing;
  Addison-Wesley/Pearson Education, Boston, 2002
- Web-Adressen:
  - **http://www.cert.org**
  - **http://www.nmrc.org**
  - **http://www.l0pht.com**
  - **http://www.netsecurity.net**
  - **http://www.packetstormsecurity.com**
  - **http://www.sans.org**
  - **http://www.securityfocus.com**