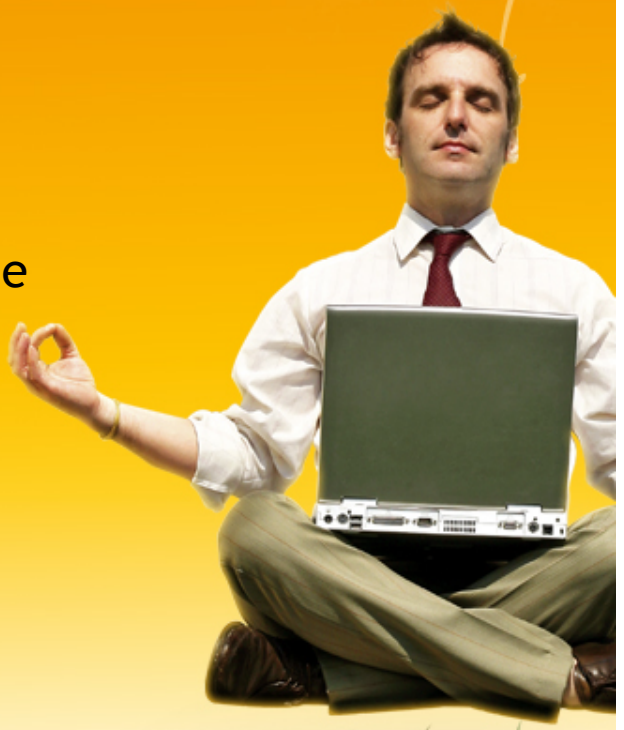
BASTA!

.NET, VISUAL STUDIO & MORE

Manu Carus | Manufaktur IT | www.ethical-hacking.de

Ethical Hacking für Fortgeschrittene

Night School



Inhalt

- Hacking
- Ethical Hacking
- Gesetzgebung
- „Die Welt ist schlecht!“
- Professionelle Einbrüche
- IT-Sicherheit im Hier und Jetzt
- Ausblick

Manu Carus

- Certified Ethical Hacker (EC Council, New York)
- Sicherheitsspezialist
  - Security Audits
  - Penetration Tests
  - Application Security Review
  - IT-Bedrohungs- und Risiko-Analyse
- Buchautor, CD-Verleger
- Initiative „Ethical Hacking – Die Netz Security“
  www.ethical-hacking.de

- manu.carus@ethical-hacking.de

Hacking

- „Hacker“ ~ „andersdenkende” Spezialisten
- Motivation?
  Neugier, Spieltrieb, Profilierung, Kriminalität...
- Schaden!
  Finanzdaten, Wirtschaftsspionage, Raubkopien...
  Kreditkarteninformationen, digitale Identitäten, (D)DoS-Attacken...
- Black Hats Gray Hats White Hats

„Cracker“

?

unabhängige
Security-Consultants

Schnellkurs

- Was treiben Hacker im Internet?
- Welcher Schaden entsteht durch ihr Tun?
- Welche Ziele nehmen Hacker ins Visier?
- Warum ist Hacking so einfach?
- Wo liegen die Schwächen des Internets?
- Wie kann man diesen Schwächen wirksam begegnen?

Ethical Hacking

Ausgangssituation
- expliziter Auftrag
- Sicherheitsprofil (Footprinting)
- Einbruch

Methodik
- Methoden und Techniken der Hacker-Community
- gleiche Werkzeuge
- gleiches Denken

⇨ höhere Sicherheit durch Erkundung und Einbruch von außen wie von anderen Hackern auch!

⇨ Auftragseinbruch!

Ziel
⇨ Schwachstellen finden
⇨ Sicherheitslücken beheben
⇨ Infrastruktur stärken

Vorgaben
⇨ ethisches Verhalten
⇨ Integrität und Vertrauen

Kann Hacking ethisch sein?

- gängige Sicherheitspraxis: Hamsterrad!
  Software-Version, Patch, und auf ein Neues...
- 1 Schwachstelle ⇔ n Lücken
- Spion gegen Spion
- Widerspruch?

⇨ Effektive Methode!

⇨ Wer sein Netzwerk wirksam absichern will, muss selbst wie ein Hacker denken!

Fragestellungen

- Was kann ein Eindringling auf dem Zielsystem sehen?
- Welche Server und Devices sind im Netzwerk sichtbar und erreichbar?
- Wie kann der Eindringling diese Information gegen das Unternehmen einsetzen?
- Sind die Versuche und Erfolge des Eindringlings in den Systemen nachvollziehbar?
- Welche Systeme sind im Unternehmen zu schützen?
- Gegen wen oder was muss geschützt werden?
- Welcher Schutz ist jeweils angemessen?
- Und welche Mittel ist das Unternehmen für ausreichenden Schutz bereit zu investieren?

Deutsches Strafgesetzbuch (StGB)

- § 202a: Ausspähen von Daten
- § 202b: Abfangen von Daten
- § 202c: Vorbereiten des Ausspähens und Abfangens von Daten
- § 303a: Datenveränderung
- § 303b: Computersabotage
- § 303c: Strafantrag

⇨ Wer Daten, die nicht für ihn selbst bestimmt sind, unbefugt ausspäht, unbrauchbar macht oder verändert, oder eine fremde Datenverarbeitung stört, macht sich mit einer Freiheitsstrafe von bis zu fünf Jahren oder unter Geldstrafe strafbar.

⇨ Bereits der Versuch ist strafbar...

⇨ Gesetzentwurf August 2007:
Hackerparagraph 202c, Bundestrojaner, BSI

⇨ Computer Ethics Institute: *http://www.brook.edu/its/cei/cei_hp.htm*

„Die Welt ist schlecht!“

Malware

- Backdoors
- Trojaner
- Spam

Phishing

Viren, Würmer

Spyware

⇨ Cheats, Patches, Wallhacks

⇨ Internet-Cafés, WLANs

⇨ Handy-Spionage, Bluetooth

⇨ Xing, monster.com, stayfriends.de

⇨ neue Technologien (AJAX, ...)

FlexiSpy

Backdoors

- Script Kiddies: Construction Kit (Beast 1 2 3)
- Cracker: Spyware (Keylogger 1 2 3 4 5)
- Profis: DSL auf TCP-Listener (Server | Client | DSL)

- Festsetzen:
  - Spam, Web-Sites, Multimedia, Games, ...
- Tarnen:
  - Rootkits

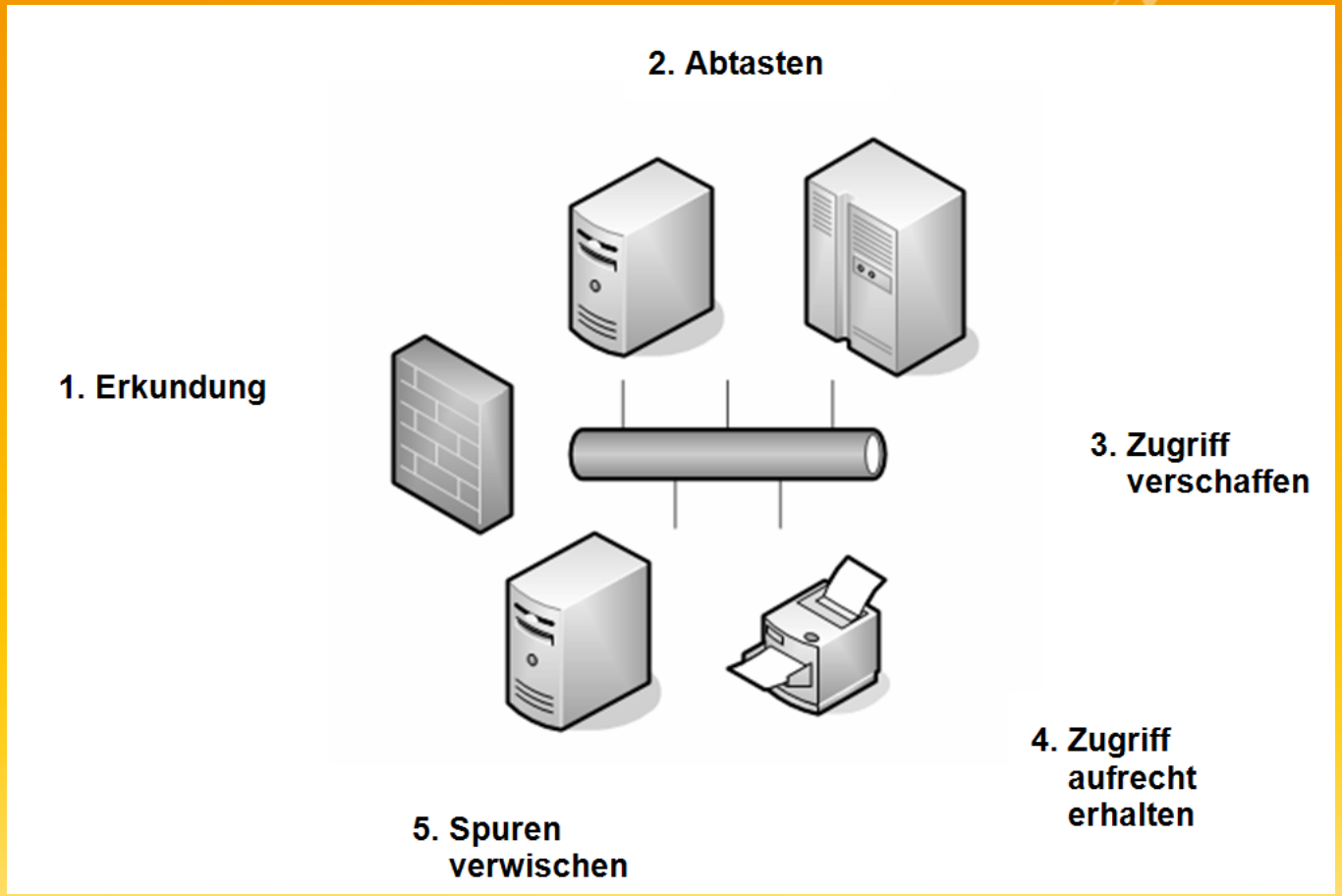
Spam

- Backdoor erstellen
- als Trojaner tarnen (CreateExt 1 2)
- Mail anonym versenden (SMTP 1 | 2)

E-Mail-Adressen sammeln:

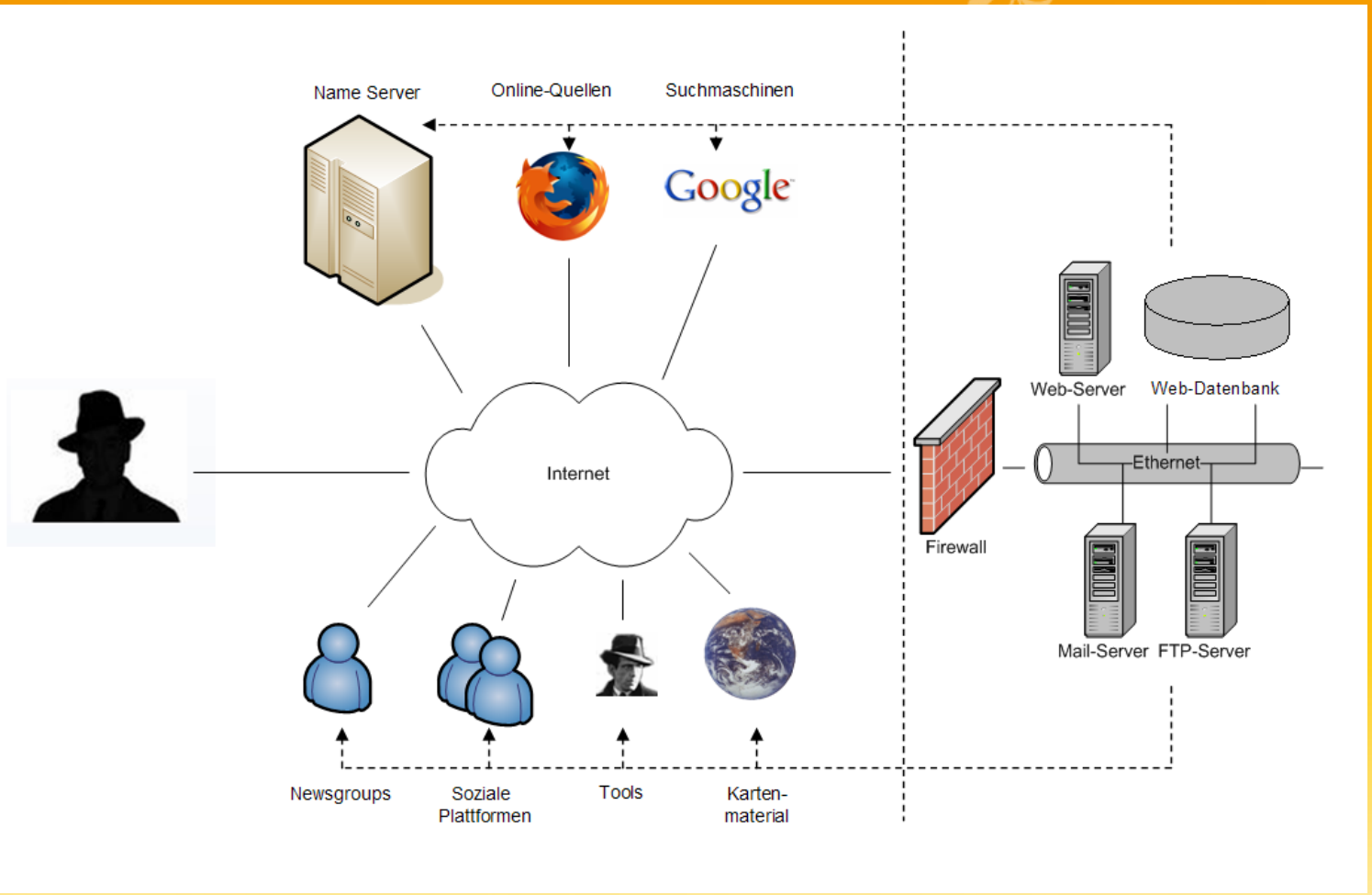
- Google Hacking (\w+([-+.']\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*)
- 1st Email Address Spider
- Kauf (20 – 100$)

Professionelle Einbrüche

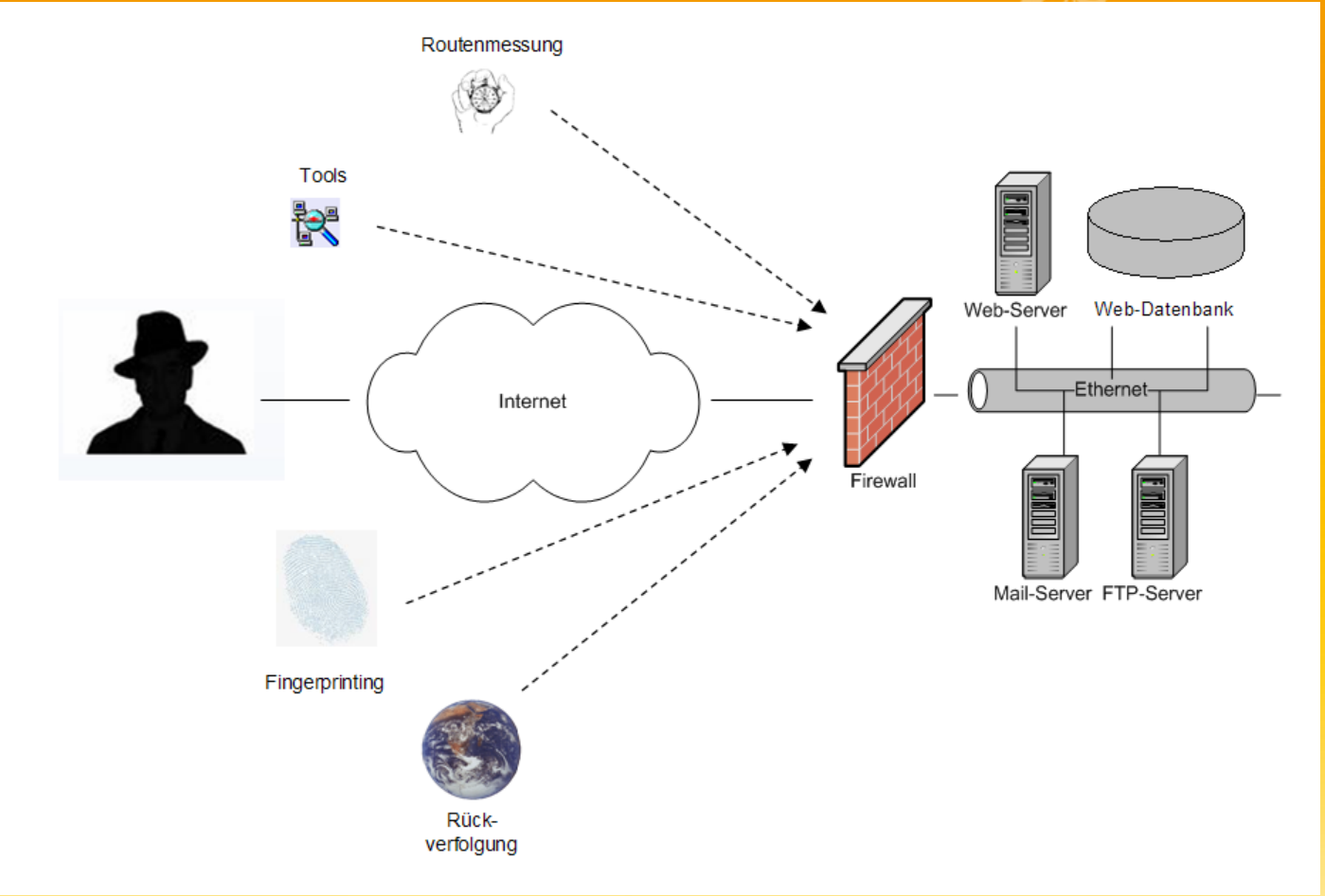


- Erstellung eines Sicherheitsprofils: 90% der Zeit
- Angriff: 10% der Zeit

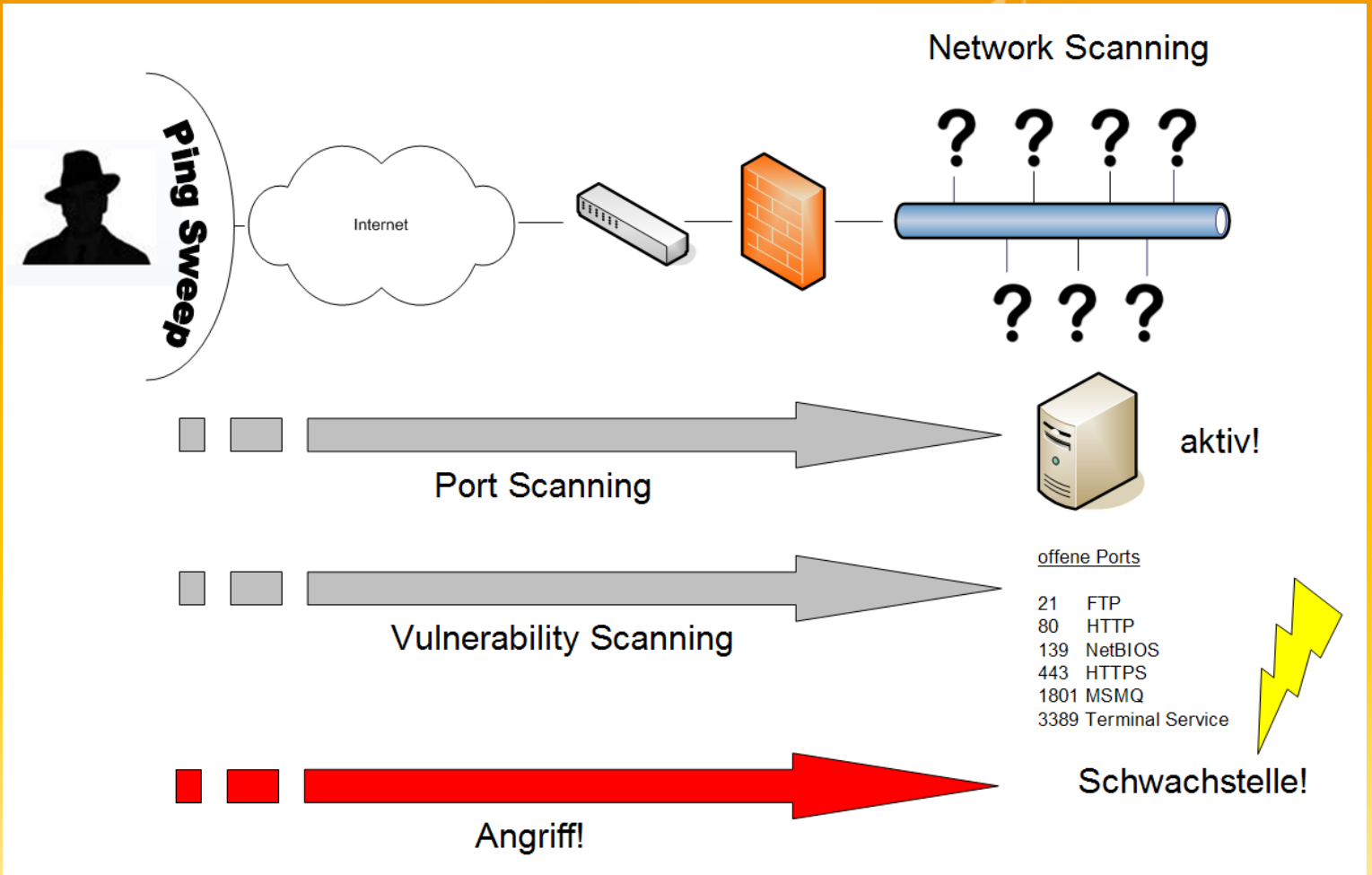
Passive Reconnaissance



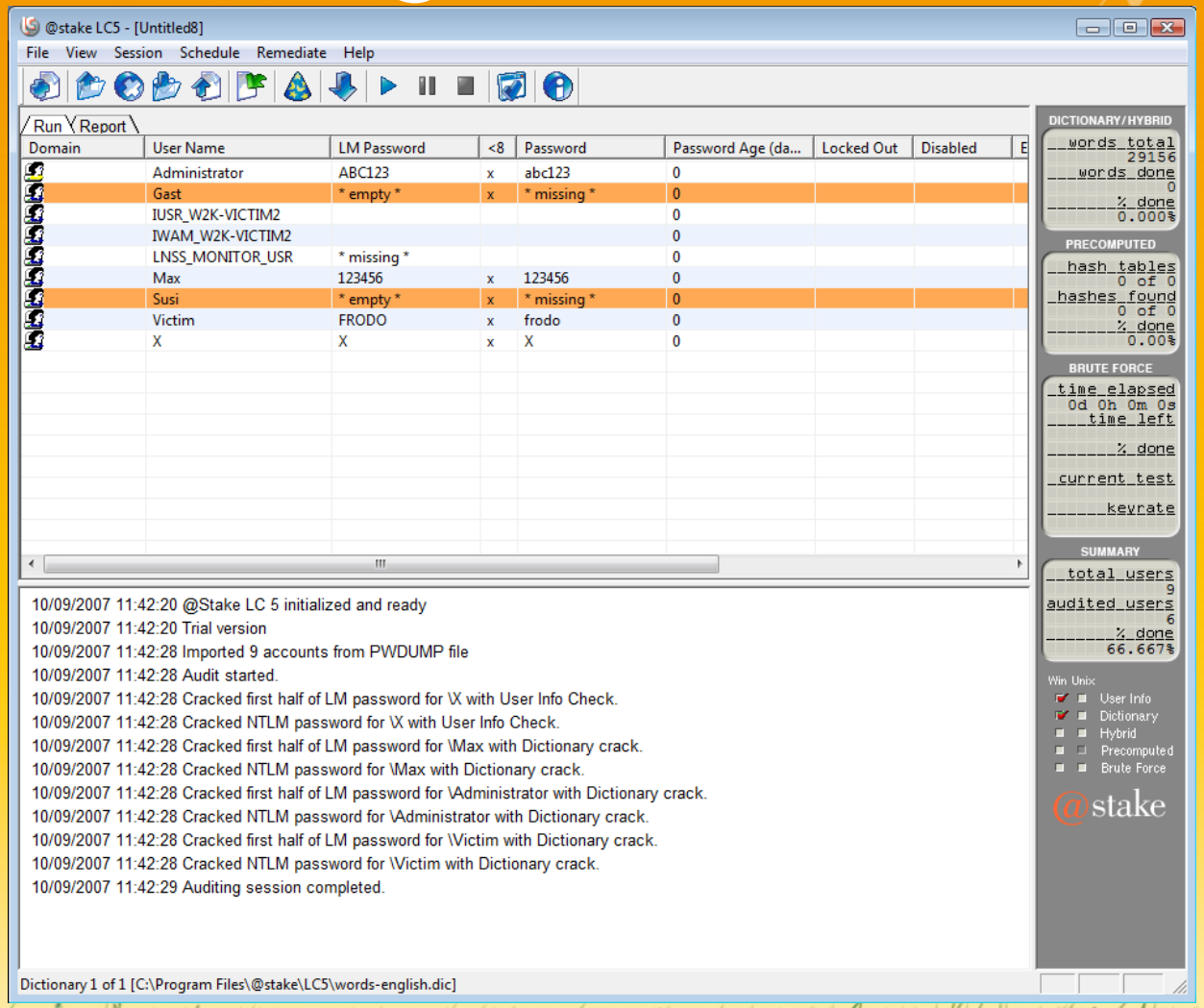
Aktive Reconnaissance



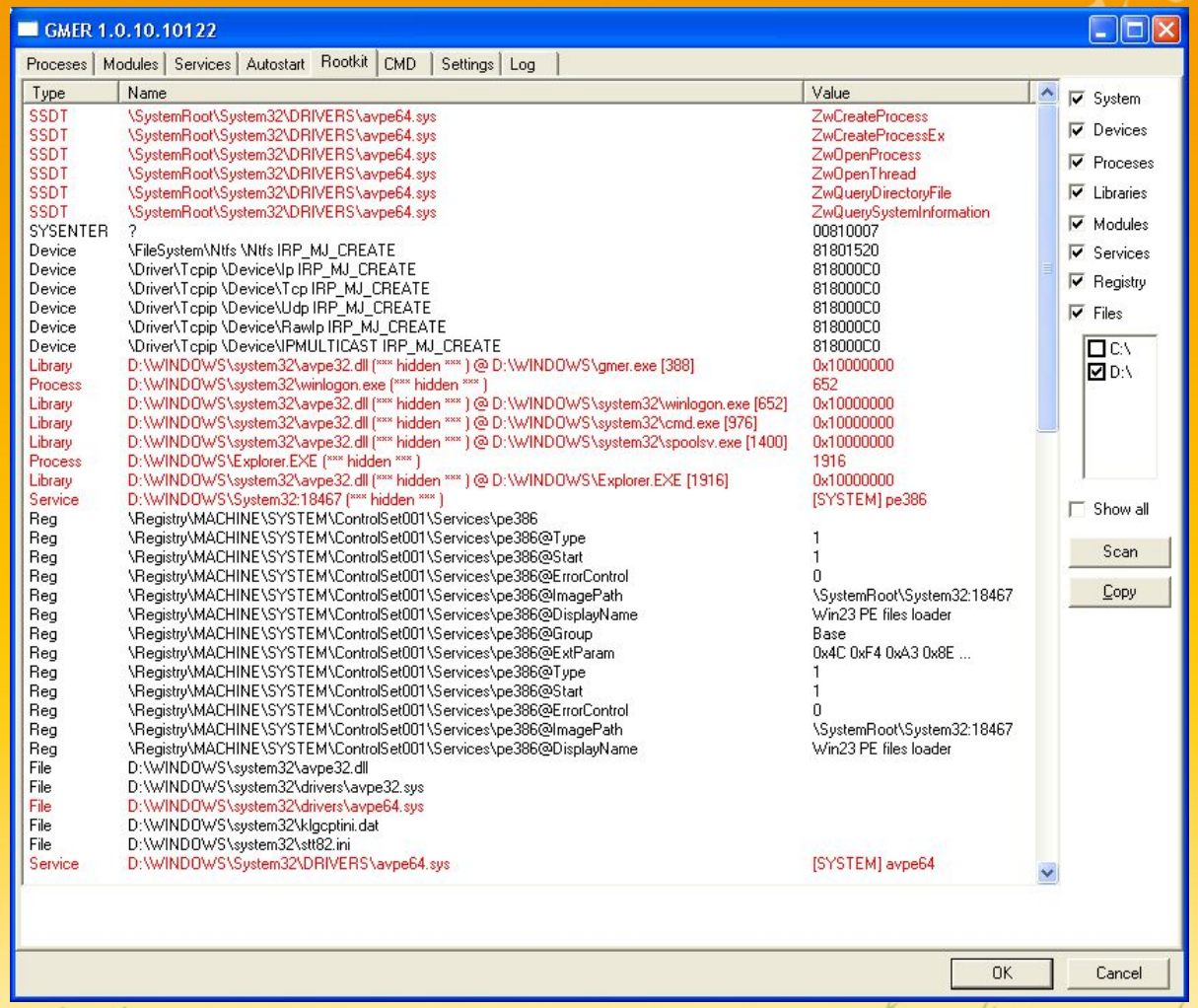
Scanning


Network Scanning
Ping Sweep
Internet
Port Scanning
aktiv!
Vulnerability Scanning
offene Ports
21 FTP
80 HTTP
139 NetBIOS
443 HTTPS
1801 MSMQ
3389 Terminal Service
Schwachstelle!
Angriff!

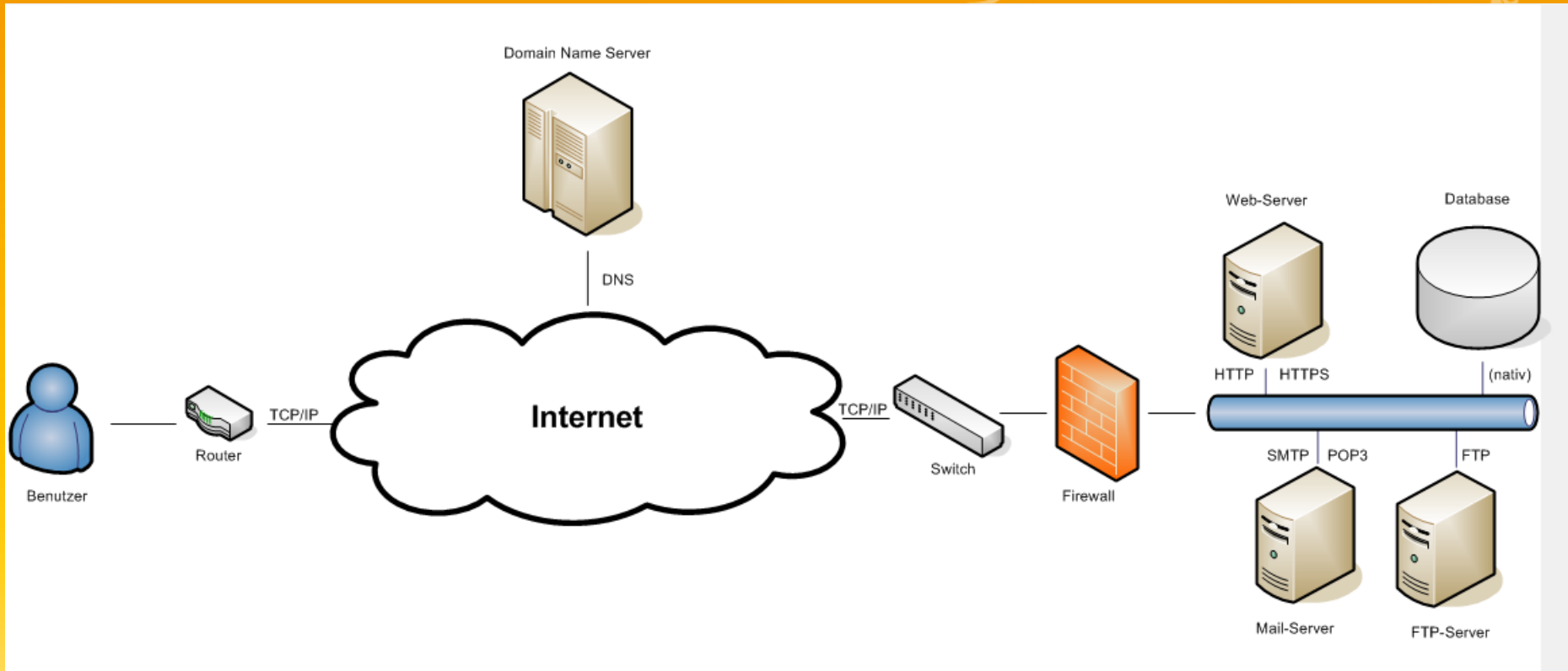
Cracking


@stake LC5 - [Untitled8]
File View Session Schedule Remediate Help
Run Report
Domain | User Name | LM Password | <8 | Password | Password Age (da... | Locked Out | Disabled
Administrator | ABC123 | x | abc123 | 0
Gast | * empty * | x | * missing * | 0
IUSR_W2K-VICTIM2 | 0
IWAM_W2K-VICTIM2 | 0
LNSS_MONITOR_USR | * missing * | 0
Max | 123456 | x | 123456 | 0
Susi | * empty * | x | * missing * | 0
Victim | FRODO | x | frodo | 0
X | X | x | X | 0
10/09/2007 11:42:20 @Stake LC 5 initialized and ready
10/09/2007 11:42:20 Trial version
10/09/2007 11:42:28 Imported 9 accounts from PWDUMP file
10/09/2007 11:42:28 Audit started.
10/09/2007 11:42:28 Cracked first half of LM password for \X with User Info Check.
10/09/2007 11:42:28 Cracked NTLM password for \X with User Info Check.
10/09/2007 11:42:28 Cracked first half of LM password for \Max with Dictionary crack.
10/09/2007 11:42:28 Cracked NTLM password for \Max with Dictionary crack.
10/09/2007 11:42:28 Cracked first half of LM password for \Administrator with Dictionary crack.
10/09/2007 11:42:28 Cracked NTLM password for \Administrator with Dictionary crack.
10/09/2007 11:42:28 Cracked first half of LM password for \Victim with Dictionary crack.
10/09/2007 11:42:28 Cracked NTLM password for \Victim with Dictionary crack.
10/09/2007 11:42:29 Auditing session completed.
Dictionary 1 of 1 [C:\Program Files\@stake\LC5\words-english.dic]
DICTIONARY/HYBRID
words total 29156
words done 0
% done 0.000%
PRECOMPUTED
hash tables 0 of 0
hashes found 0 of 0
% done 0.00%
BRUTE FORCE
time elapsed 0d 0h 0m 0s
time left
% done
current test
keyrate
SUMMARY
total users 9
audited users 6
% done 66.667%
Win Unix
User Info
Dictionary
Hybrid
Precomputed
Brute Force
@stake

Tarnen


GMER 1.0.10.10122
Proceses | Modules | Services | Autostart | Rootkit | CMD | Settings | Log
Type | Name | Value
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwCreateProcess
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwCreateProcessEx
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwOpenProcess
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwOpenThread
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwQueryDirectoryFile
SSDT | \SystemRoot\System32\DRIVERS\avpe64.sys | ZwQuerySystemInformation
SYSENTER | ? | 00810007
Device | \FileSystem\Ntfs \Ntfs IRP_MJ_CREATE | 81801520
Device | \Driver\Tcpip \Device\Ip IRP_MJ_CREATE | 818000C0
Device | \Driver\Tcpip \Device\Tcp IRP_MJ_CREATE | 818000C0
Device | \Driver\Tcpip \Device\Udp IRP_MJ_CREATE | 818000C0
Device | \Driver\Tcpip \Device\RawIp IRP_MJ_CREATE | 818000C0
Device | \Driver\Tcpip \Device\IPMULTICAST IRP_MJ_CREATE | 818000C0
Library | D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\gmer.exe [388] | 0x10000000
Process | D:\WINDOWS\system32\winlogon.exe (*** hidden ***) | 652
Library | D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\winlogon.exe [652] | 0x10000000
Library | D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\cmd.exe [976] | 0x10000000
Library | D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\system32\spoolsv.exe [1400] | 0x10000000
Process | D:\WINDOWS\Explorer.EXE (*** hidden ***) | 1916
Library | D:\WINDOWS\system32\avpe32.dll (*** hidden ***) @ D:\WINDOWS\Explorer.EXE [1916] | 0x10000000
Service | D:\WINDOWS\System32:18467 (*** hidden ***) | [SYSTEM] pe386
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Type | 1
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Start | 1
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ErrorControl | 0
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ImagePath | \SystemRoot\System32:18467
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@DisplayName | Win23 PE files loader
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Group | Base
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ExtParam | 0x4C 0xF4 0xA3 0x8E ...
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Type | 1
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@Start | 1
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ErrorControl | 0
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@ImagePath | \SystemRoot\System32:18467
Reg | \Registry\MACHINE\SYSTEM\ControlSet001\Services\pe386@DisplayName | Win23 PE files loader
File | D:\WINDOWS\system32\avpe32.dll
File | D:\WINDOWS\system32\drivers\avpe32.sys
File | D:\WINDOWS\system32\drivers\avpe64.sys
File | D:\WINDOWS\system32\klgcptini.dat
File | D:\WINDOWS\system32\stt82.ini
Service | D:\WINDOWS\System32\DRIVERS\avpe64.sys | [SYSTEM] avpe64
System
Devices
Proceses
Libraries
Modules
Services
Registry
Files
C:\
D:\
Show all
Scan
Copy
OK
Cancel

IT-Sicherheit im Hier und Jetzt



Internet-Protokolle

- 1969: ARPANET, ein Projekt der *Advanced Research Project Agency* (ARPA) des US-Verteidigungsministeriums
- 1970 ff: TCP/IP, Telnet, FTP
- 1980 ff: SMTP, HTTP, POP, DNS
- 1990 ff: erste visuelle Web-Browser
- 1994: SSL
- 1994 ff: HTTPS, Secure FTP, POP3S, STARTTLS, PGP, S/MIME

⇨ veraltete Protokolle, die seit über 20 Jahren nicht auf unsere heutigen Sicherheitsbedürfnisse angepasst wurden

Anwendungen

- Online-Banking
- Shopping
- Auktionen
- ...

⇨ Verlagerung der (Sicherheits-)Verantwortung auf Sie! (Firewall-Regeln | Passwörter | Schadensabwicklung)

⇨ Jeder Internet-User kann zu 100% anonym bleiben.

⇨ Fast jede Information kann gefälscht, abgefangen, abgehört, umgeleitet werden.

⇨ Das Internet in der uns heute vorliegenden Form ist nicht gesellschaftsfähig!

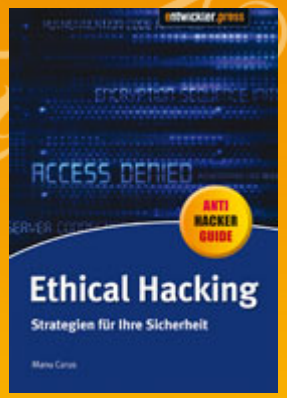
Goldene Regeln

- http://www.ethical-hacking.de/

- Nehmen Sie nichts von Fremden an!
- Nichts ist so wie es scheint!
- Seien Sie misstrauisch!
- Geben Sie nichts von sich preis!
- Speichern Sie niemals vertrauliche Daten auf Ihrem Computer!
- Halten Sie sich fern von Internet-Cafés und WLAN-HotSpots!
- Schotten Sie Ihren Rechner ab!
- Entziehen Sie sich selbst Ihre Admin Rechte!
- Vermeiden Sie die Registrierung Ihres Namens im Internet! Machen Sie sich unsichtbar!
- Verpflichten und sensibilisieren Sie Ihre Mitarbeiter!
- Hacken Sie sich selbst!
- Schalten Sie alles ab, was Sie nicht zwingend benötigen!
- Bewahren Sie Passwörter niemals dort auf, wo Sie sie benötigen!
- Verwenden Sie ausschließlich starke Passwörter!

Empfehlungen

- Buch „Ethical Hacking“
  erschienen bei entwickler.press



- AudIT-CD „Ethical Hacking“
  erschienen bei Manufaktur IT

- „Ethical Hacking – Die Netz Security“
  http://www.ethical-hacking.de/