
w-jax 09
Konferenz für Java™, Enterprise Architekturen, SOA
Manu Carus
Ethical Hacking //
Looking at the
Dark Side of the Moon

Inhalt

- Hacking
- Ethical Hacking
- Gesetzgebung
- Malware
- Crimeware
- Professionelle Einbrüche
- IT-Sicherheit im Hier und Jetzt
- Software-Entwicklung

Hacking

Hacking

- Hacker sind „andersdenkende“ Spezialisten
- Welche Motivation treibt Hacker an?
  Neugier, Spieltrieb, Profilierung, Kriminalität...
- Welchen Schaden richten Hacker an?
  Finanzdaten, Wirtschaftsspionage, Raubkopien...
  Kreditkartendaten, digitale Identitäten, ...
  (D)DoS-Attacken...
- Black Hats Grey Hats White Hats

Cracker

?

Consultants?

Hacking

- 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?
- Was können Sie als Entwickler tun?
- Welche Gefahren bestehen außerhalb der im Netz eingesetzten Technik?

Ethical Hacking

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!

Ethical Hacking

Ausgangssituation

- expliziter Auftrag
- Sicherheitsprofil (Footprinting)
- Einbruch

Ziel

⇨ Schwachstellen finden

⇨ Sicherheitslücken beheben

⇨ Infrastruktur stärken

Methodik

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

Vorgaben

⇨ ethisches Verhalten
⇨ Integrität und Vertrauen

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

⇨ Auftragseinbruch!

Ethical Hacking

- 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?

Gesetzgebung

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...

⇨ August 2007:
Hackerparagraph, Bundestrojaner, Behördenabsicherung durch BSI

Hackerparagraph

- §202c: Vorbereiten des Ausspähens und Abfangens von Daten
- Bundesverfassungsgericht (BVerfG), 18.05.2009:

Nur die Absicht zählt:
Der Umgang mit eindeutig illegaler Software ist strafbar, wenn die Software zu kriminellen Zwecken eingesetzt wird oder der Anwender dies nachweisbar in Kauf nimmt.
Die Feststellung einer Straftat muss erkennbar sein.
(Beispiel: Wurde die Software für illegale Zwecke geschrieben?)

- Novelle Bundesdatenschutzgesetz (BDSG), 01.09.2009

⇨ §42: Meldepflicht für Datenverluste in Deutschland

Malware

„Die Welt ist schlecht!“

Malware

- Backdoor — Phishing
- Trojaner — Viren, Würmer
- Spam — Spyware

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

⇨ Cheats, Patches, Wallhacks
⇨ Internet-Cafés, WLANs
⇨ Handy-Spionage, Bluetooth FlexiSpy
⇨ Xing, monster.com, stayfriends.de
⇨ neue Technologien (AJAX, ...)

State of Internet Security

Report „State of Internet Security“,

Websense, September 2009

- Bis zu 95 Prozent der Kommentare in Blogs, Chat-Rooms und Message-Boards enthalten Malware-Links. Fokus: Web 2.0.
- Anstieg der Malware-verteilenden Seiten um 671 Prozent gegenüber 2008.
- 85 Prozent aller Spam-Mails verweisen auf verseuchte Web-Sites.
- Anstieg um über 600 Prozent allein in einem Monat (06/2009 ⇨ 05/2009).
- Knapp 70 Prozent aller Web-Sites aus den Kategorien Pornografie, Glücksspiel und Drogen enthalten mind. einen Link auf bösartige Web-Sites.
- 37 Prozent aller Web-Angriffe hat den Diebstahl von Passwörtern und Kreditkarteninformationen zum Ziel.

BSI Q3/2009

- Der Markt für Security-Lösungen und -Dienstleistungen wuchs zwischen 2006 und 2009 durchschnittlich um 12,7 Prozent pro Jahr.
- Marktvolumen: 4,4 Milliarden Euro (HW/SW/Dienstleistungen).
- Die Häufigkeit, mit der ein Betriebssystem bei Erscheinen eines Updates aktualisiert wird, liegt bei 74,1 Prozent.
- Für rund die Hälfte der neu gemeldeten Schwachstellen wurde von den Herstellern der Produkte kein Update zur Behebung des Sicherheitsproblems bereitgestellt.
- Angriffe erfolgen vermehrt auf Schwachstellen in weit verbreiteter Anwendungssoftware.
- Software verfügt häufig nicht über automatische Update-Mechanismen.

  Secunia CSI/PSI

- Von 100 empfangenen Mails sind im Durchschnitt gerade einmal 1,5 Mails gewünscht.

Wo liegt die Schmerzgrenze?

- IDC:

Weltweite Einkünfte aus Antiviren-Produkten (in Mio. US$)					
	2002	2003	2004	2005	2006
Privatkunden	659,0	821,3	972,3	1.097,8	1.200,1
Business-Kunden	1.559,2	1.870,3	2.220,2	2.544,9	2.881,8
Gesamt	**2.218,2**	**2.691,6**	**3.192,5**	**3.642,8**	**4.081,9**

Tabelle 1 Einnahmen der Hersteller von Antiviren-Software (für Privatanwender- und Firmenprodukte) [1]

- Computer Economics:

Finanzieller Schaden durch Virenangriffe 1995-2005	
Weltweiter Schaden (US $)	
2005	$ 14,2 Mrd.
2004	$ 17,5 Mrd.
2003	$ 13,0 Mrd.
2002	$ 11,1 Mrd.
2001	$ 13,2 Mrd.
2000	$ 17,1 Mrd.
1999	$ 13,0 Mrd.
1998	$ 6,1 Mrd.
1997	$ 3,3 Mrd.
1996	$ 1,8 Mrd.
1995	$ 500 Mio.

Tabelle 2 Weltweiter wirtschaftlicher Schaden durch Virenangriffe [2]

Crimeware

BSI Q3/2009

- Fast vier Mio. Deutsche sind bereits Opfer von Computerkriminalität geworden und erlitten einen finanziellen Schaden.
- Von Januar bis März 2008 wurden durchschnittlich 15.000 infizierte Web-Sites pro Tag entdeckt, 79% davon zu an sich harmlosen Internetangeboten.
- 90% aller Web-Sites weisen Schwachstellen auf.
  65% aller Web-Sites sind allein gegen XSS anfällig.
- Organisierte Kriminalität schöpft Gewinne in Milliardenhöhe ab.
- Professionell und international aufgestellte Schattenwirtschaft: Botnetze können gemietet werden, bspw. zwecks Spam-Versand.
- 2008: 503 Command-and-Control-Server im Jahresdurchschnitt.

Black Market

GENERAL	TOPICS	POSTS	LAST POST
Announcements Info about what's going on...	18	258	
Introductions Introduce yourselfs here.	209	1422	
Chat / Off Topic General Chat and off topic chat.	215	2137	
Suggestions I can't run this site by myself, so suggestions are welcome	49	399	
Help General Help	177	1088	
Show Off Show us your skills here...	144	1332	
Trusted Apply to be a Trusted Member Here...	116	729	
HACKING/CRACKING MARKET	**TOPICS**	**POSTS**	
Bot Bin/Sources + Bots Sell Bots - HTTP/IRC etc here...	36	466	
Stealers / Keyloggers / Rats Sell Firefox/Steam etc Stealers here...	27	172	
Accounts Sell Cpanels/WHM's etc here...	209	584	
Crypters/Downloaders Sell Packers/Crypters/Binders here...	28	151	
Servers and Hosting Sell Servers/Roots/VPS's/Hosting/Shells ect here...	55	219	
Other Sell Other stuff here, which doesn't fit in other categories, eg. Databases	109	611	
Exploits Sell 0day Exploits here...	10	196	
CARDING MARKET	**TOPICS**	**POSTS**	
CC's Sell CC's , Specify Country , Price, Minimum Amount	271	2524	
Gift Cards Sell Any Gift Cards in here	102	685	
Cardable Post Sites you've carded here & Chat...	70	525	
PHISHING/BANKING MARKET	**TOPICS**	**POSTS**	
Bank Logins Sell Any Bank Login here...	151	902	
Phising Kits Post Free Phishing Kits + Sell em...	22	146	
Emails / Spamming Sell Fresh Email Lists / Mailers	68	202	
OTHER	**TOPICS**	**POSTS**	
Want to Buy Can't find what ur looking to buy, Post it here	359	1399	
Proxies / VPN's Socks, HTTP Proxies, VPN's etc sell here...	33	162	
Scammers Post Evidence and name and shame here...	49	424	
Tutorials Post some useful info here...	118	636	
Services Specify details...	125	638	

Underground Economy [GDATA 2009]

E-Mail-Adressen	30 – 250 €	je eine Mio. Adressen
Spam-Mails an Zielgruppe	300 – 800 €	je eine Mio. Mails
Stealer	5 – 40 €	Zugangsdaten ausspähen
E-Mail-Account	1 – 5 €	Username / Password
Kreditkartendatensatz	2 – 300 €	je nach Datenumfang/qualität
Bot-Datei	20 – 100 €	Rechner kapern
Bot-Quellcode	200 – 800 €	individuell anpassbar
Bot-Install	50 – 250 €	je 1.000 Rechner
Web-Hosting	5 – 9.999 €	illegale Inhalte
FUD-Service	10 – 40 €	Fully Undetectable Signaturen
DDoS-Angriff	10 – 150 €	je Stunde
DHL-PackStation-Konto	50 – 150 €	gestohlen / gefaked
PayPal-Account	1 – 25 €	Username / Password
GSM Skimmer Device	4.000 €	Bankautomatenaufsatz
Ausweise / Führerscheine	50 – 2.500 €	gefälschte Papiere

Organisierte Kriminalität

- Hauptplattformen der Szene sind sog. Boards (Diskussionsforen).
- Verhandlung zwischen Käufer und Verkäufer erfolgt anonym via Instant Messaging (MSN, ICQ, Yahoo Messenger, Jabber, ...).
- Bezahlung erfolgt über Online-Bezahldienste.
- Webshops verbergen sich hinter IPs, in denen die Käufer Schadcode einkaufen können (Warenkorbfunktionalität!).
- Bulletproof Hosting ~ Server-Standorte, die sicher vor dem Zugriff internationaler Ermittler sind (z.B. Russian Business Network):
  - Drop Zone für die Daten der eigenen Botnetze
  - illegale Shops
  - Command & Control-Server
  - whois: Daten von Strohmännern im Ausland (Afrika, Asien, ...)
- Gefälschte Ausweise und Führerscheine werden für Kontoeröffnungen benötigt (Auszahlungsort für Diebesgut).

- Versand von 1 Mio. Spam-Mails:
  - 250 – 700 $ für kleines Botnetz (ca. 20.000 Zombies)
  - 25 Sekunden Dauer bei 2 Mails / Sek. und aktiven Bots

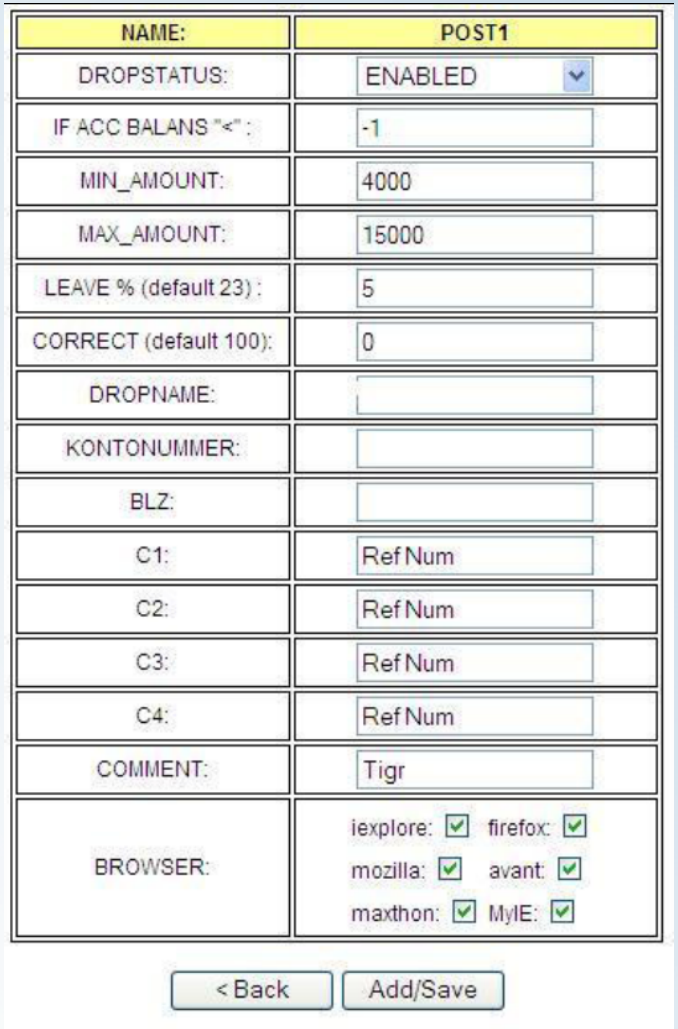
It‘s Cash-Time!

- **Cashout:** Umwandlung von virtuellem Geld in echtes Geld.
- Lieferung eingekaufter Waren an **Dropzones.**
- Mittelsmänner leiten als Kuriere die Ware weiter (Anwerbung via Spam-Mail und Provision).
  - Lieferung der Ware an eine Adresse in Russland.
  - Mittelsmann holt die Ware an der Post ab und leitet an die Zieladresse.
  - Nebeneinkommen (1 2)!
- **Housedrop:** Lieferung an leerstehende Häuser und Wohnungen. Adressänderungen erfolgen online.
- **DHL Packstation:** anonymer Zugang mit gefälschten Dokumenten.
- **Geld verschieben:**
  - Einzahlung in einem Online-Casino mit gestohlenem PayPal-Account.
  - Verschieben des Geldes von dort auf einen *Bankdrop* (Konto, auf das man Zugriff hat, das aber nicht auf den eigenen Namen ausgestellt ist) oder an einen Mittelsmann (*Geldwäsche*).
  - Anleitungen zum Erlangen eines anonymen Kontos verfügbar (hoher Preis!)

Mai 2009

- Cybergang mit dem Ziel: Zugriff auf deutsche Bankkonten.
- Infektion zahlreicher Web-Sites via Crimeware Toolkit (ca. 300 $).
- Verseuchte Web-Sites infizieren die Browser (Drive-by-Download) und installieren ein Trojaner-Toolkit auf den betroffenen Rechnern.
  - ⇨ ca. 6.400 verseuchte PCs bei insgesamt 90.000 Besuchern
- Der Trojaner späht die Zugangsdaten aus und kommuniziert mit einem C&C-Server in der Ukraine. Letzterer steuert die Geldüberweisungen von dem Opfer über sog. *Money Mules* an die *Cybergang*:
  - Umgehung der Anti-Fraud-Systeme der Banken
  - Verdeckung der „ungewöhnlichen" Geldtransfers
  - diverse Parameter steuern die Überweisung
- Money Mule Konten sind legitime Bankkonten im Zugriff von Mittelsmännern, die eingehende Beträge nach Abzug einer Provision an die Cybergang weiterleitet.

C&C-Server



NAME:	POST1
DROPSTATUS:	ENABLED
IF ACC BALANS "<" :	-1
MIN_AMOUNT:	4000
MAX_AMOUNT:	15000
LEAVE % (default 23) :	5
CORRECT (default 100):	0
DROPNAME:	
KONTONUMMER:	
BLZ:	
C1:	Ref Num
C2:	Ref Num
C3:	Ref Num
C4:	Ref Num
COMMENT:	Tigr
BROWSER:	iexplore: ☑ firefox: ☑ mozilla: ☑ avant: ☑ maxthon: ☑ MyIE: ☑

< Back | Add/Save

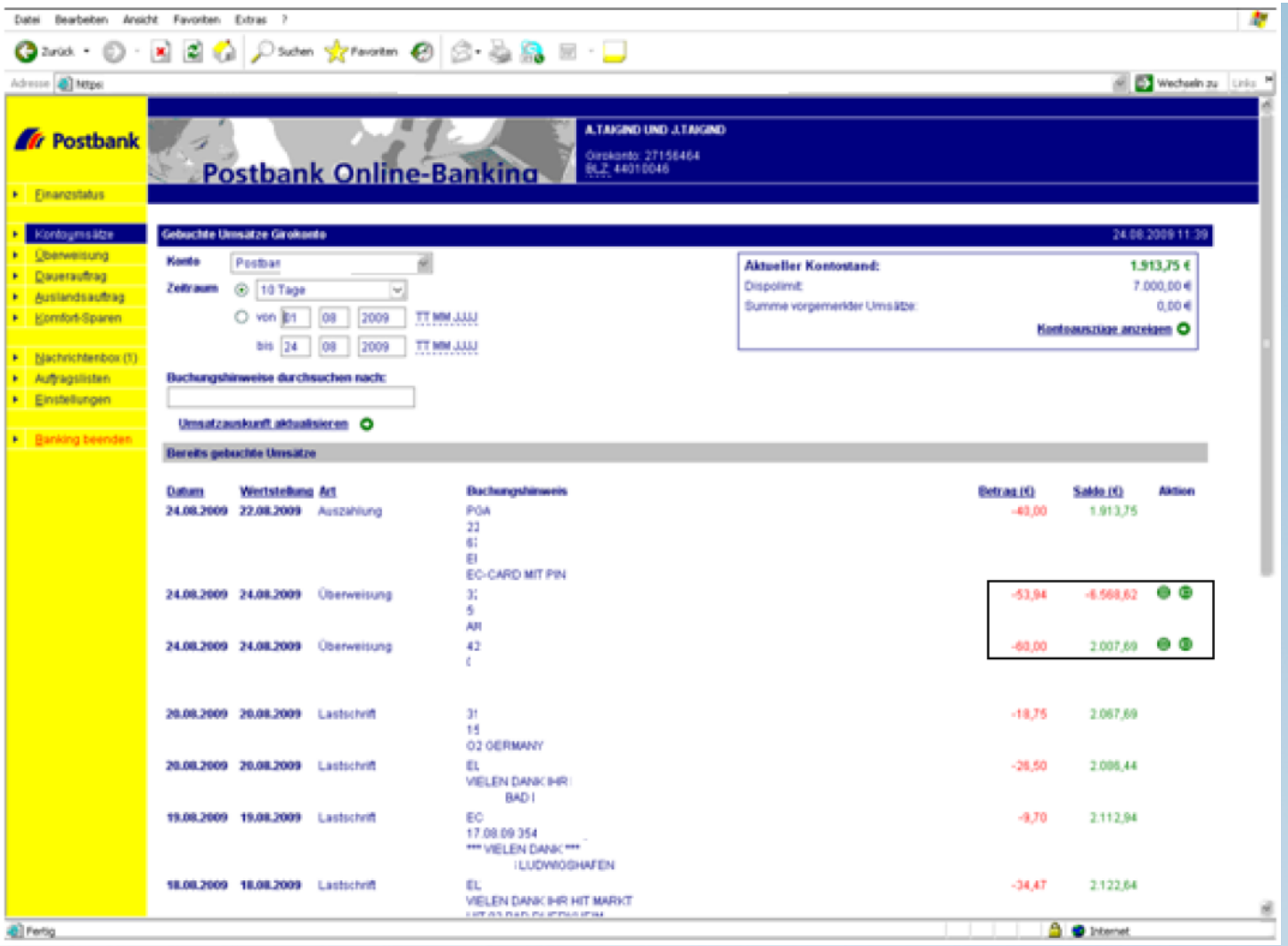
Die Parameter stellen sicher, dass

- der Kontostand des Opfers positiv bleibt.
- der gestohlene Betrag nicht zu hoch ist.
- jede Transaktion einen anderen, zufälligen Betrag überweist.

Der C&C

- überweist den Betrag an einen anderen Account als online vom Benutzer angegeben!
- täuscht das Opfer durch Injektion in die laufende Online-Banking-Anwendung!

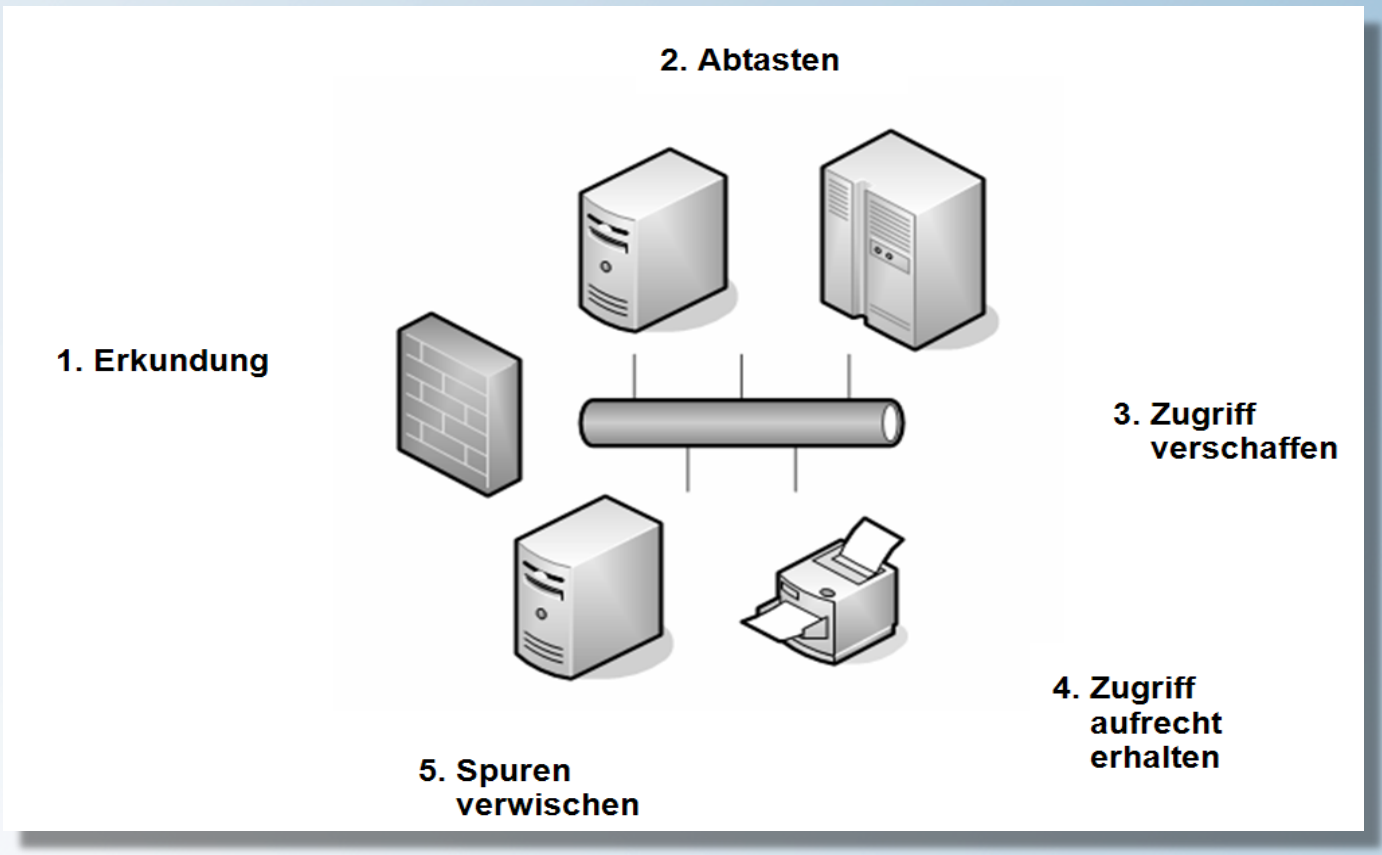
Nach der Eingabe einer iTAN...



Quelle: www.finjan.com Cybercrime Intelligence Report 3/2009

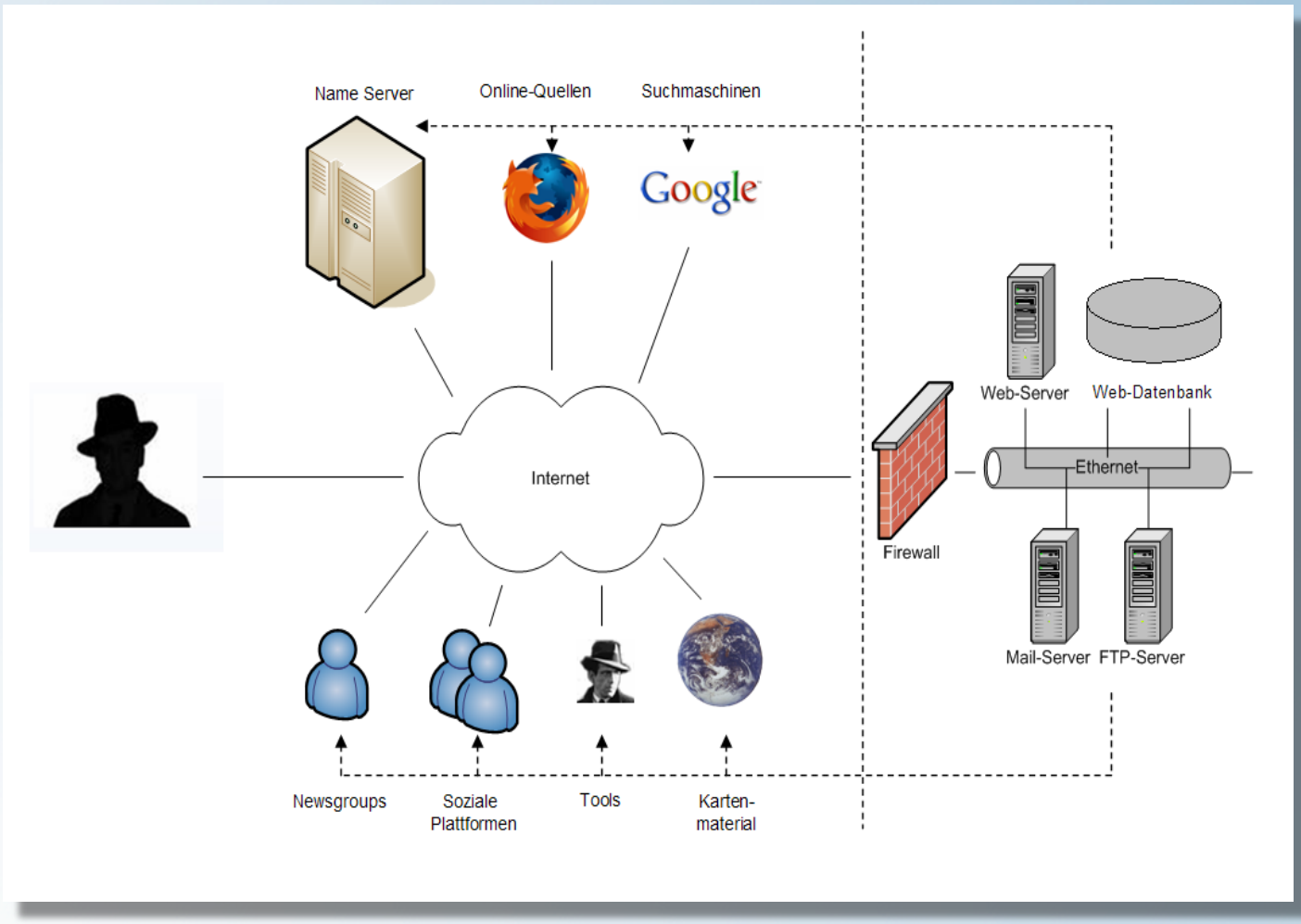
Professionelle Einbrüche

Professionelle Einbrüche



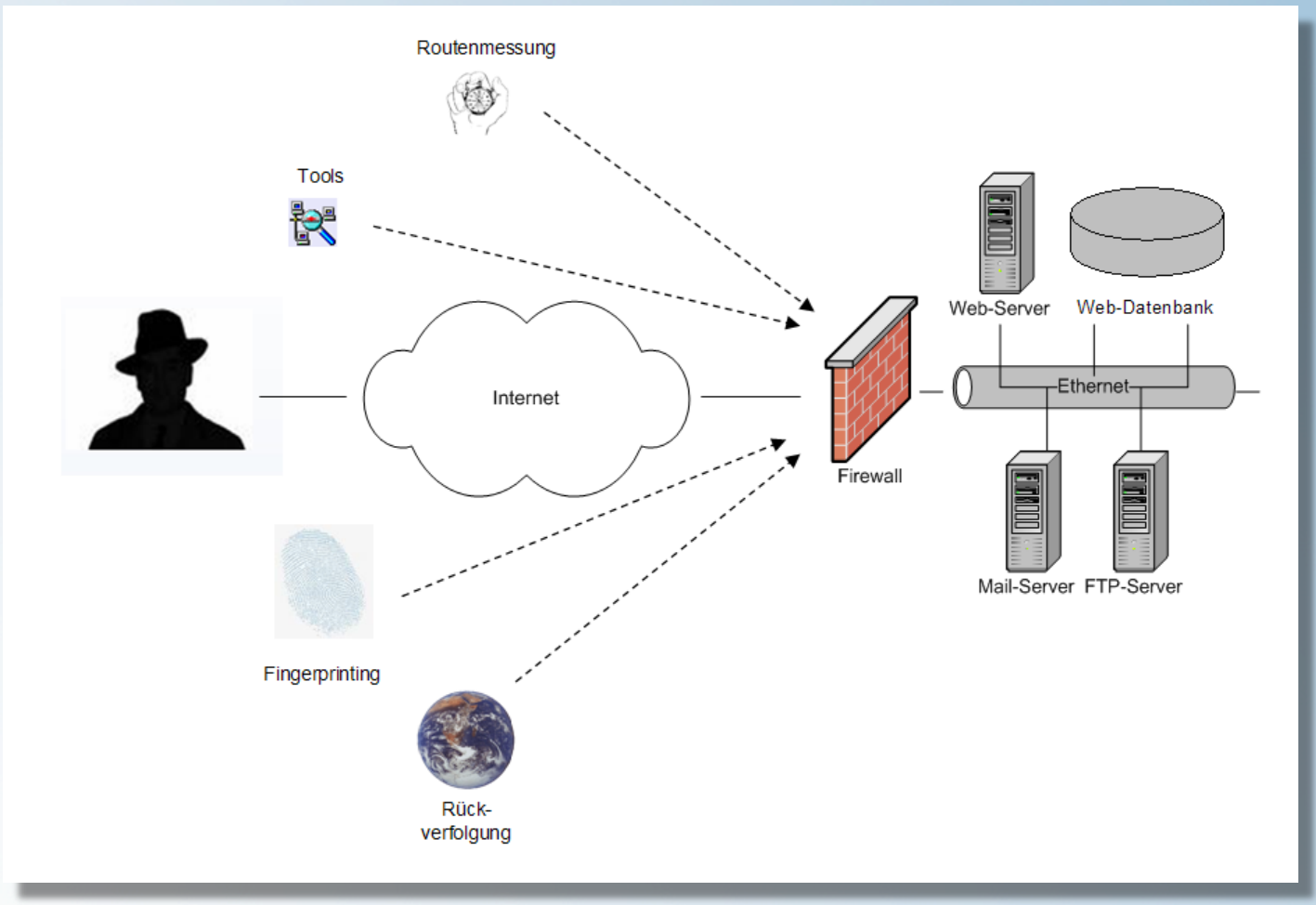
Erstellung eines Sicherheitsprofils: 90% der Zeit
Angriff: 10% der Zeit

Passive Reconnaissance

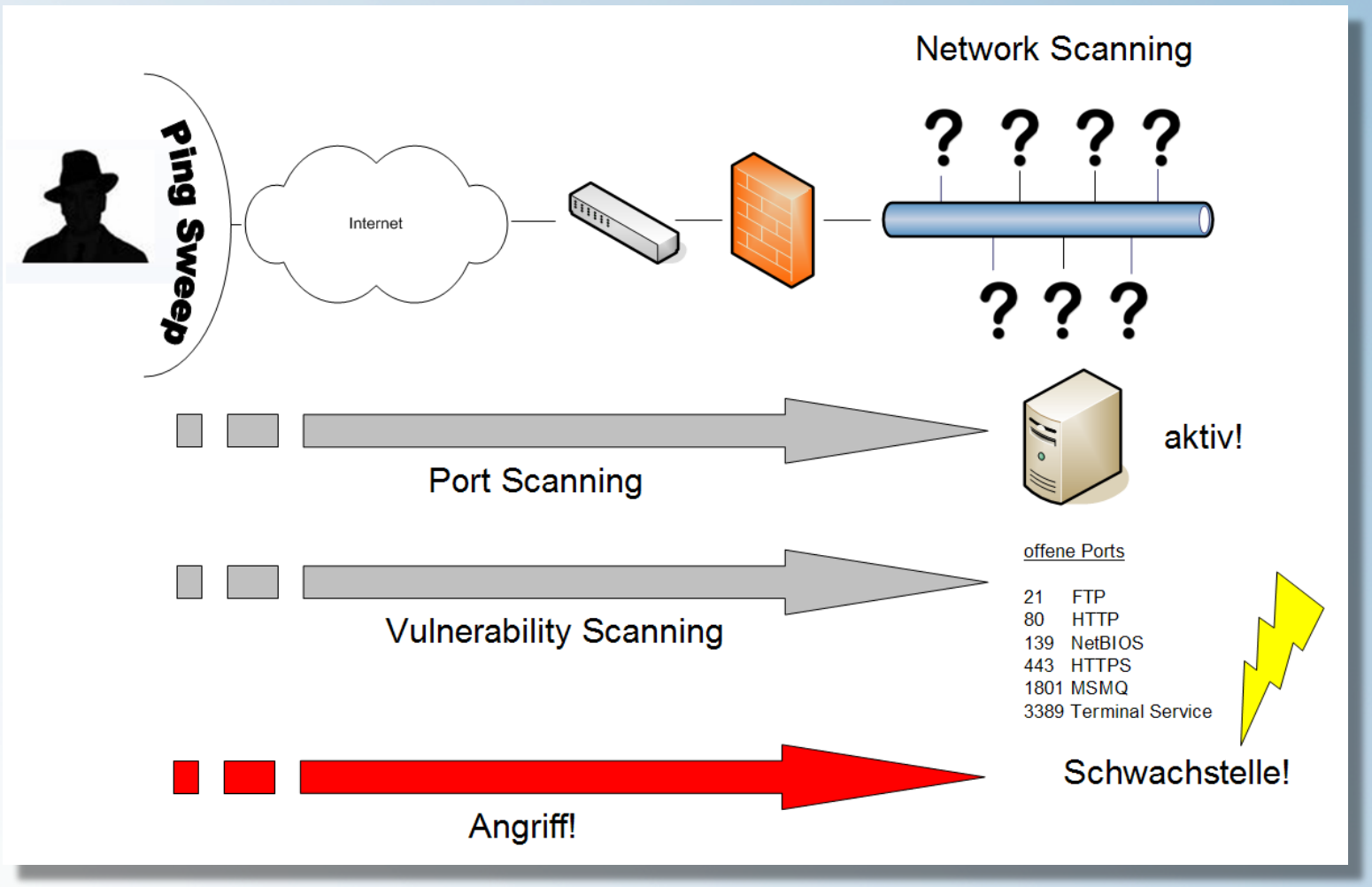


www.who.is
www.netcraft.com
www.dnsstuff.com
www.google.de
www.archive.org
www.utrace.de
maps.google.de
www.123people.de
www.xing.com

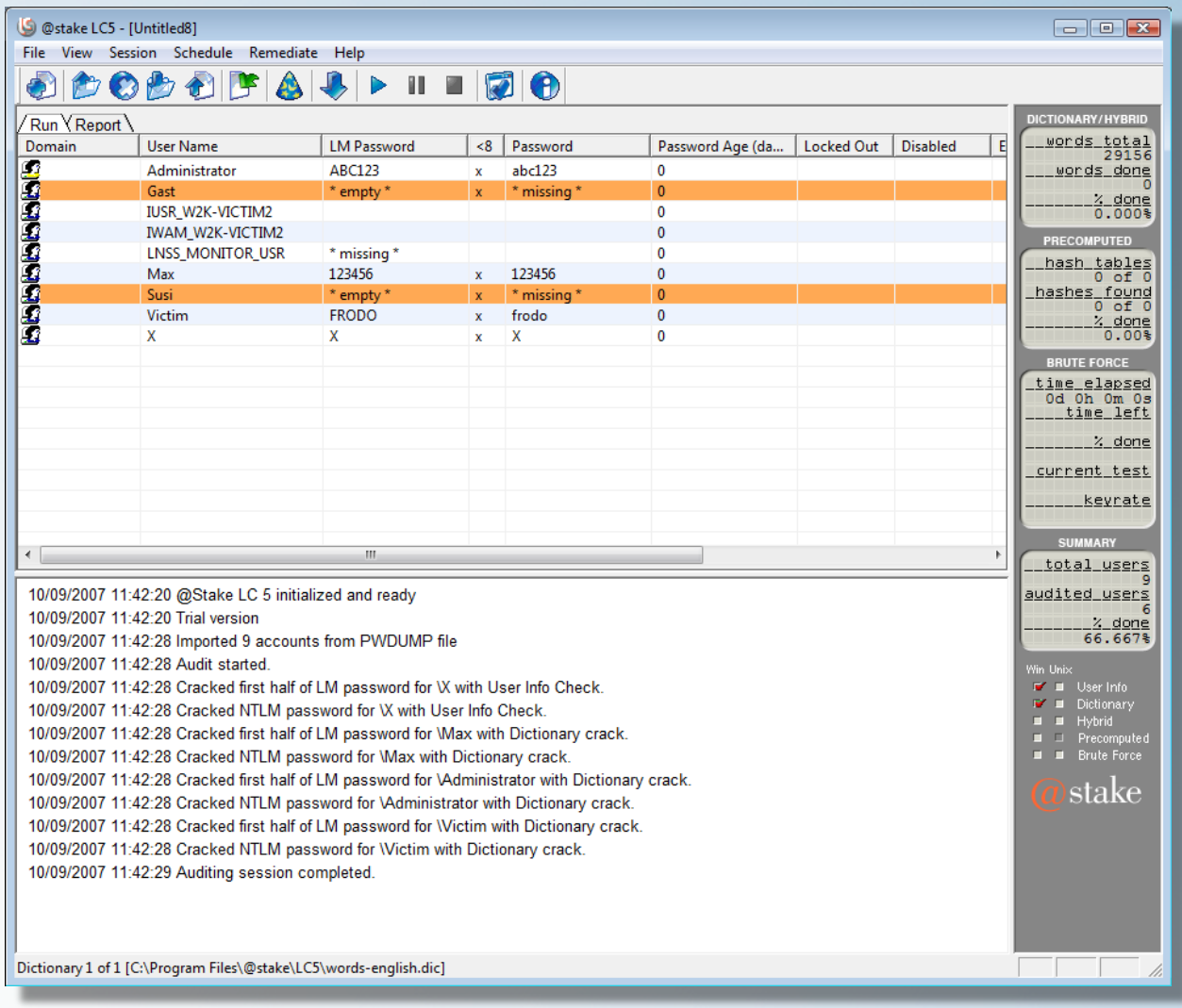
Aktive Reconnaissance



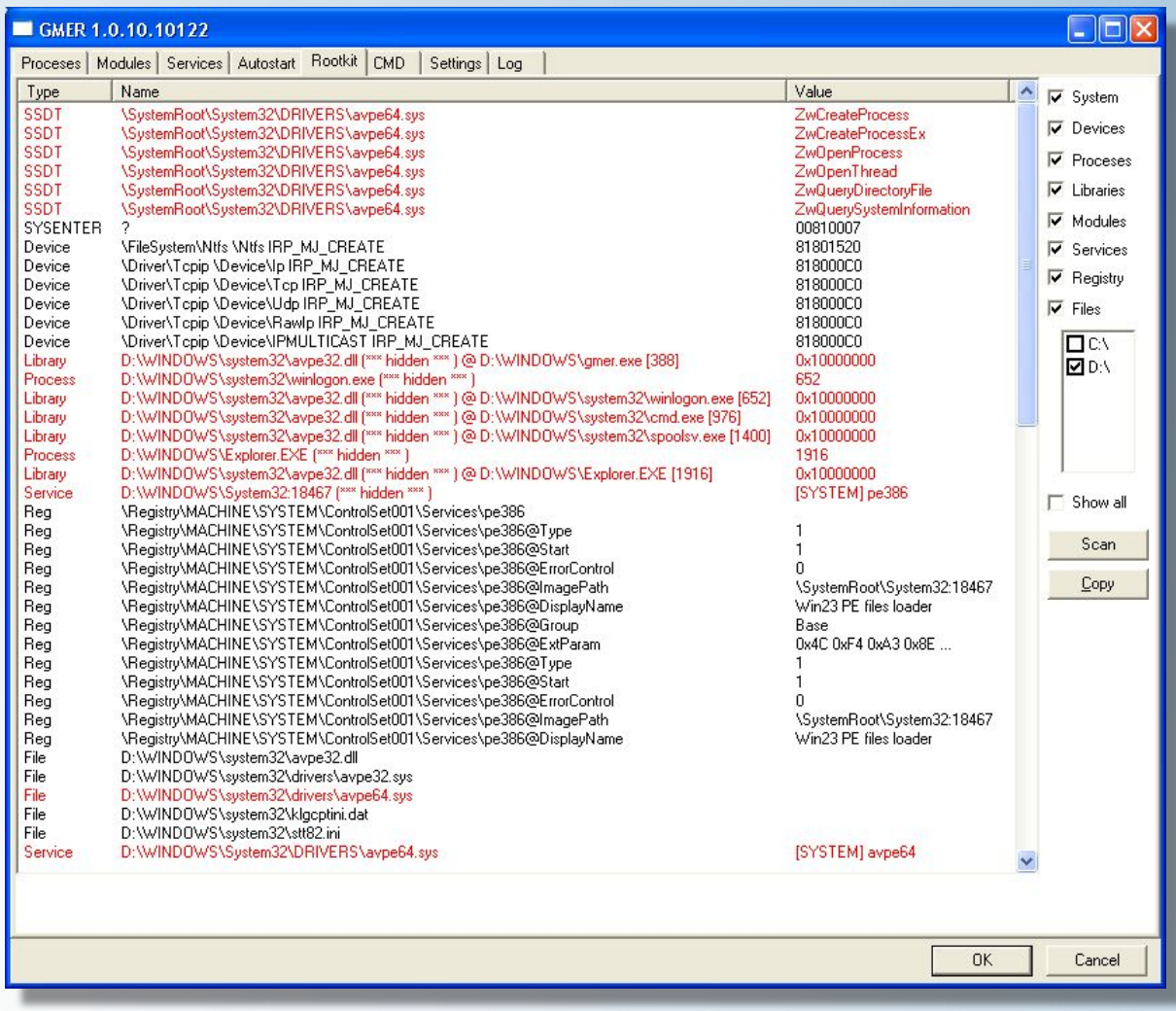
Scanning


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

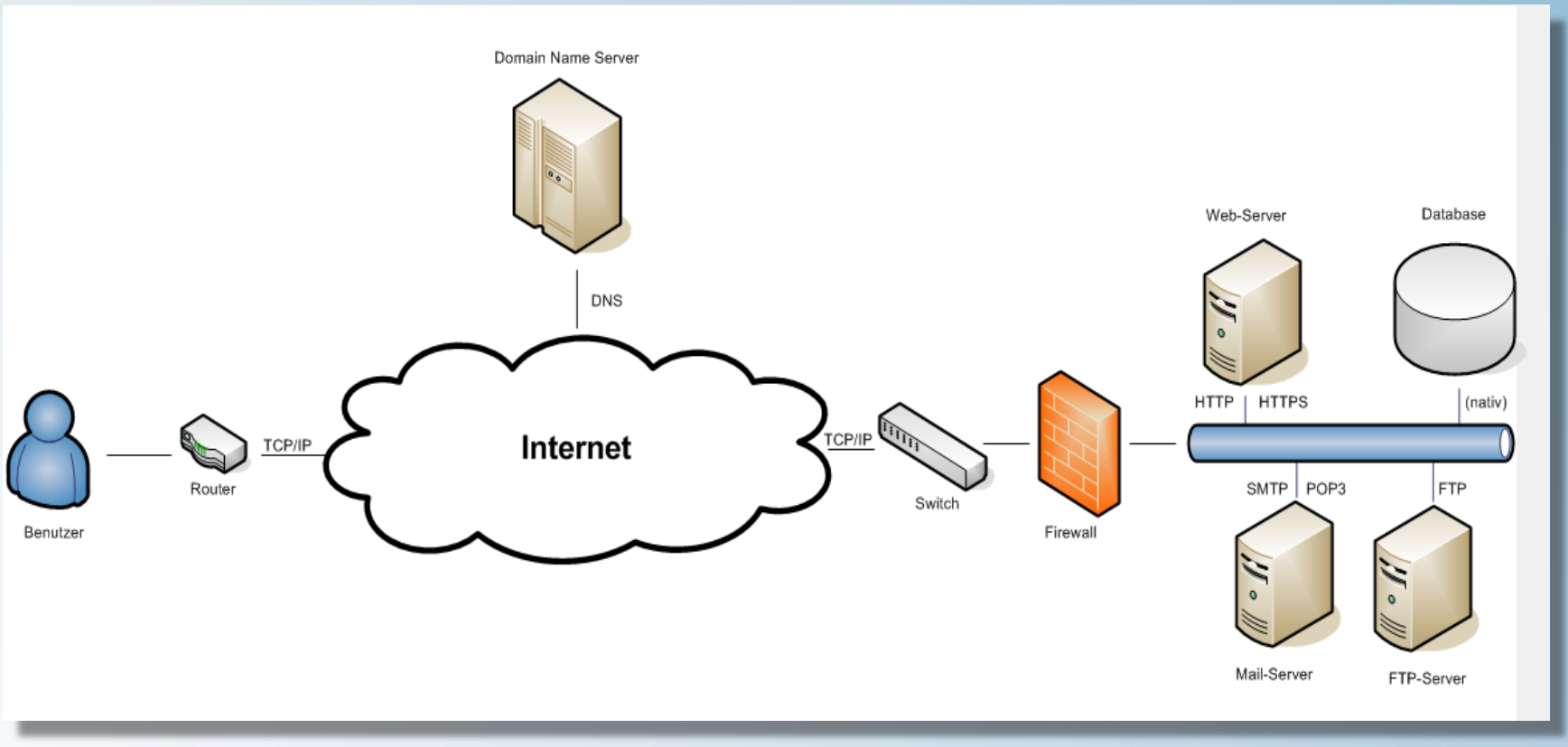

@stake LC5 - [Untitled8]
File View Session Schedule Remediate Help
Run Report
Domain | User Name | LM Password | <8 | Password | Password Age (da... | Locked Out | Disabled
Administrator | ABC123 | x | abc123 | 0
Gast | * empty * | x | * missing * | 0
IUSR_W2K-VICTIM2 | 0
IWAM_W2K-VICTIM2 | 0
LNSS_MONITOR_USR | * 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

Rootkit


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

IT-Sicherheit im Hier und Jetzt

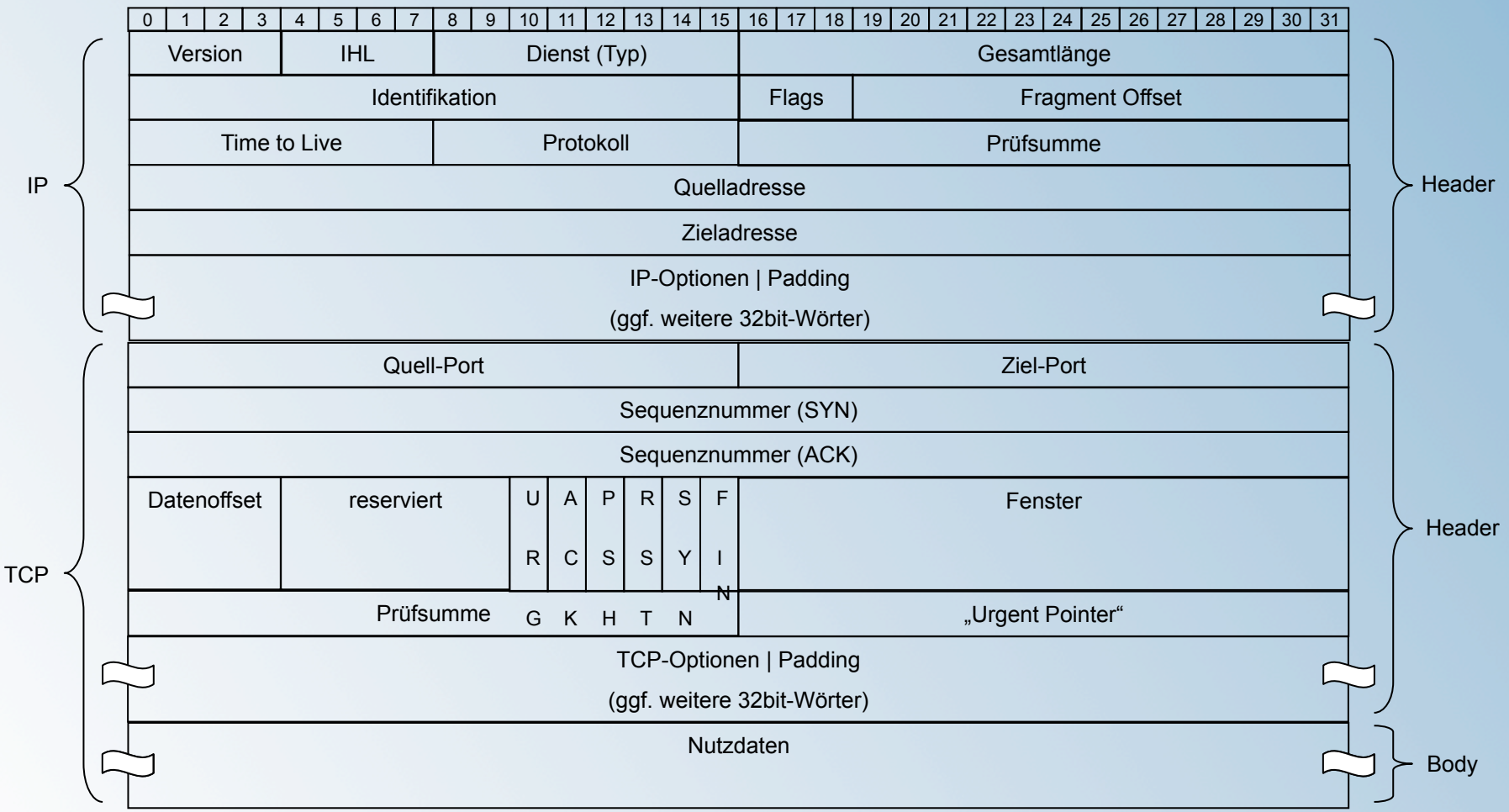


Protokolle

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

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

TCP/IP


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
IHL
Dienst (Typ)
Gesamtlänge
Identifikation
Flags
Fragment Offset
Time to Live
Protokoll
Prüfsumme
Quelladresse
Zieladresse
IP-Optionen | Padding
(ggf. weitere 32bit-Wörter)
IP
Header
Quell-Port
Ziel-Port
Sequenznummer (SYN)
Sequenznummer (ACK)
Datenoffset
reserviert
U R
A C
P S
R S
S Y
F I N
Fenster
Prüfsumme
G K H T N
„Urgent Pointer“
TCP-Optionen | Padding
(ggf. weitere 32bit-Wörter)
TCP
Header
Nutzdaten
Body

Anwendungen

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

⇨ Mehr als die Hälfte der Anwender nutzt das Internet..., um einzukaufen und um Bankgeschäfte zu erledigen. [BSI Q3/2009]

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

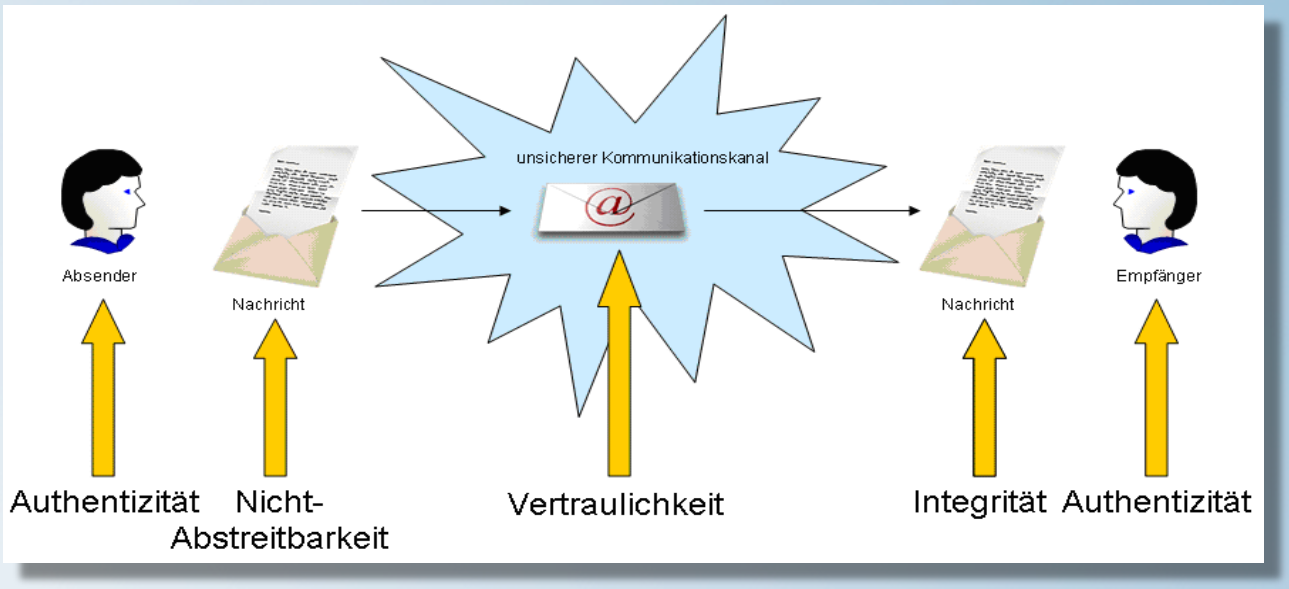
⇨ Jeder Internet-User kann zu 100% anonym bleiben.

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

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

Software Entwicklung

Kryptographische Ziele



- Hashing
- Salted Hashing
- Message Authentication Codes
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Zufallszahlen

- Digitale Signatur
- Schlüsselaustauschverfahren
- In-Memory-Verschlüsselung

➢ BSI Technische Richtlinie TR-02102
Kryptographische Verfahren -
Empfehlungen und Schlüssellängen

Guides

- OWASP Top 10 Most Criminal Web Application Vulnerabilities (2007)
- CWE/SANS Top 25 Most Dangerous Programming Errors
- BSI: Die Lage der IT-Sicherheit in Deutschland (Q3/2009)
- Common Weaknesses Enumeration (CWE)
- OWASP Development Guide v2 (2005)
- OWASP Code Review Guide v1.1
- OWASP Testing Guide v3

Frameworks

- OWASP ESAPI Validation API
- OWASP ESAPI Encoding API
- OWASP ESAPI AccessReferenceMap
- OWASP ESAPI Encryption
- OWASP ESAPI Canonicalization Control
- OWASP ESAPI Session Management Control
- OWASP PHP Anti-XSS Library
- OWASP CSRFGuard
- OWASP CSRFTester
- ...

http://www.owasp.org/

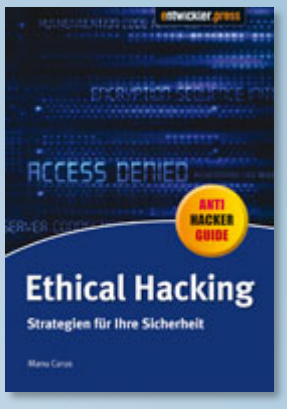
OWASP ESAPI Encoding API

Beispiel: Es gibt 50 unterschiedliche Darstellungsweisen des Zeichens „<".

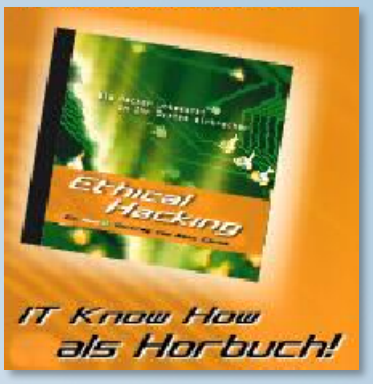
<	<	<	&#x3C	&#X003C
%3C	<	<	&#x03C	&#X0003C
&lt	<	&#X3c	&#x003C	&#X00003C
<	<	&#X03c	&#x0003C	&#X000003C
&LT	&#x3c	&#X003c	&#x00003C	<
<	&#x03c	&#X0003c	&#x000003C	<
&#60	&#x003c	&#X00003c	<	<
&#060	&#x0003c	&#X000003c	<	<
&#0060	&#x00003c	<	<	<
&#00060	&#x000003c	<	<	<
&#000060	<	<	<	\x3c
&#0000060	<	<	<	\x3C
<	<	<	&#X3C	\u003c
<	<	<	&#X03C	\u003C

Empfehlungen

- Buch „Ethical Hacking“
  erschienen bei entwickler.press



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

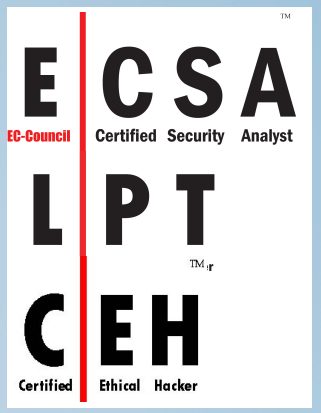


- „Ethical Hacking – Die Netz Security“

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

Manu Carus

- manu.carus@ethical-hacking.de
- IT-Sicherheitsbeauftragter
  - Certified Security Analyst (E|CSA)
  - Licensed Penetration Tester (LPT)
  - Certified Ethical Hacker (CEH)
- Buchautor, CD-Verleger
- „Ethical Hacking – Ihre Netz Security“



www.ethical-hacking.de

Manu Carus

Vielen Dank für Ihr Interesse!