Hacker-Tools

Christian J Dietrich
Benjamin Fabricius

FH, Gelsenkirchen, Informatik, Netzwerksicherheit
Dozent: Prof. Dr. Norbert Pohlmann

Teil 1

Christian Dietrich

Übersicht

- Angriffe gegen Betriebssysteme
  - Kryptographische Tools
  - Pufferüberläufe – Exploits
  - „Denial of Service“-Angriffe
- Security Scanner, Vulnerability Scanner
- Backdoors, trojanische Pferde, Rootkits
- Zusammenfassung

Kryptographische Tools

- Identifikation/Authentisierung durch Kryptographie realisiert
- symmetrische Verschlüsselung abhängig von der Qualität des Schlüssels
- Passwort-Knack-Programme
- Wörterbuch-Attacken können schwache Passwörter relativ schnell entschlüsseln
- Brute-Force-Angriffe probieren den gesamten Schlüsselraum aus
- Beispiele: john, Brutus

Beispiel: john (http://www.openwall.com/john/)

- Eingabe: UNIX-Passwortdatei
- Unterstützt verschiedene Ciphertext Formate (DES, MD5)
- Bietet Wörterbuch-Angriff, Wörterbücher können ausgetauscht und erweitert werden
- Brute-Force-Attacke
- Algorithmen in Assembler optimiert, daher sehr performant
- Folgende Beispielpasswörter:
  - maria27 94.47 Sekunden (Wörterbuch)
  - F9,Q2vY1 nach 20 Min abgebrochen
- Auf 1.8 GHz Rechner: Standard DES (64 Bit): 183.116 Pw/Sek => ~3.194.381 Jahre (365 d/a)

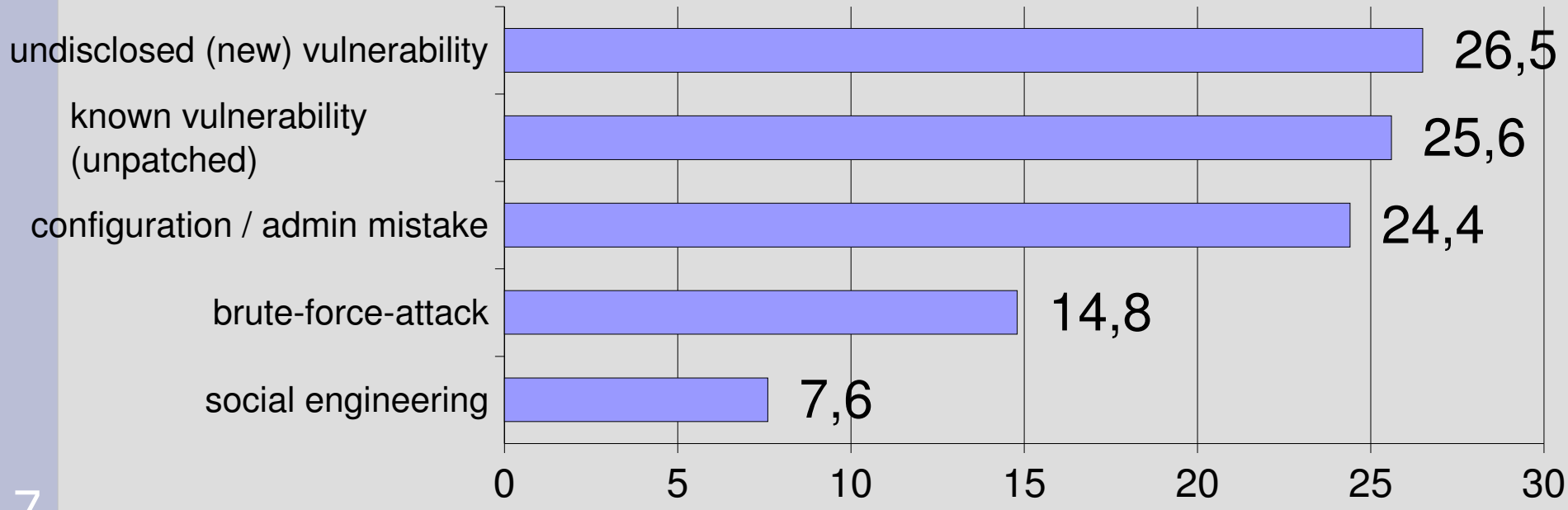
Pufferüberlauf – Buffer overflow

- Versuch mehr Daten an Speicherstelle zu schreiben als vorher reserviert
- Überschreiben fremder Speicherbereiche
  - Absturz
  - Gezielt Assemblercode einschleusen und ausführen (Exploit)
- Nur eingeschränkt generische Programme, da
  - Pufferüberläufe individuell für jedes Programm, Version und meist sogar Kompilat sind
  - Exploits Speicherstellen (oft) absolut adressieren

Exploits

- Obwohl sehr spezifisch, große Gefahr, da in oft kurzer Zeit bereits verfügbar
- Leute mit wenig Erfahrung (sog. Script-Kiddies) können vorgefertigte Exploits herunterladen und ungeschützte Ziele angreifen
- Statistik

Angriffsmethoden (Quelle: http://www.zone-h.org)



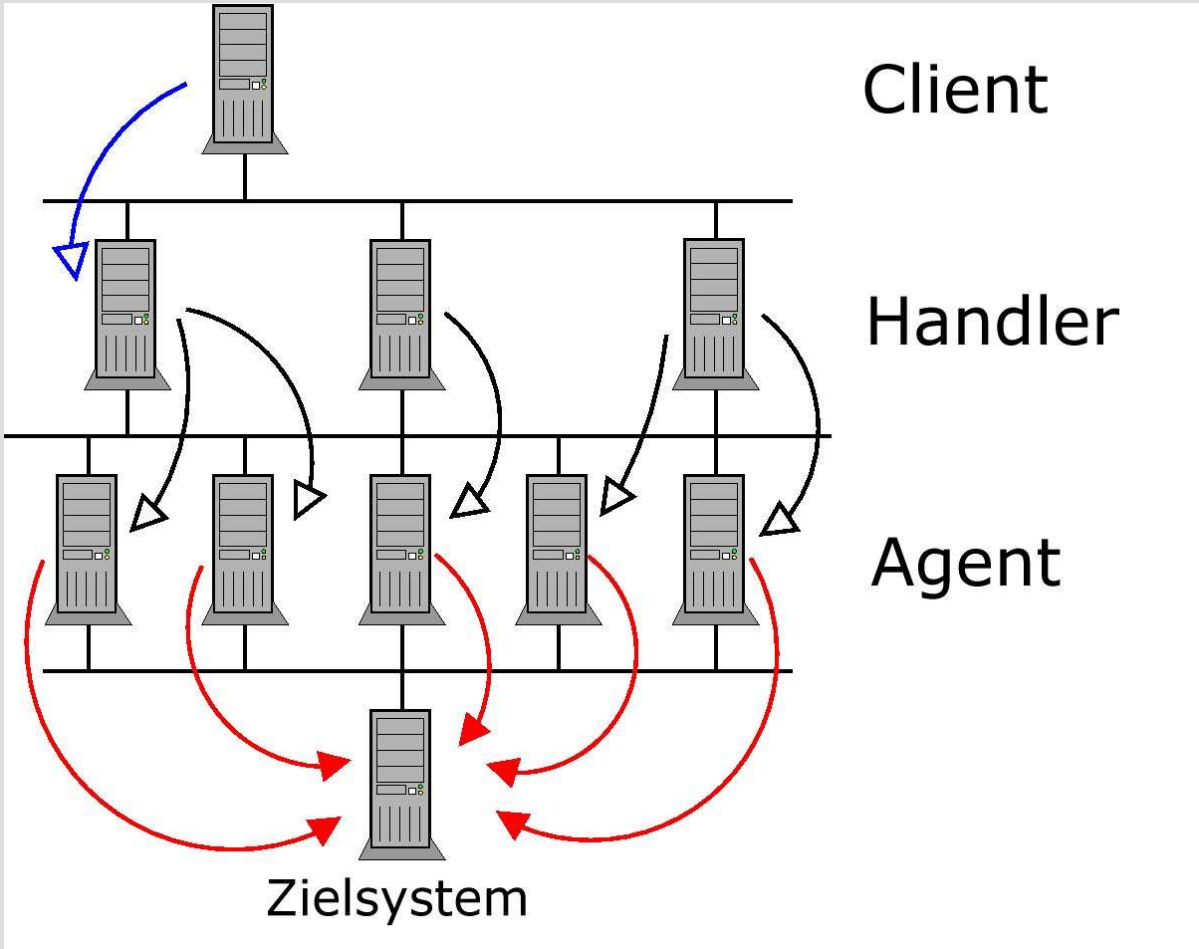
Screenshot – Exploit-Suche

Denial of Service – Angriffe (DoS)

- engl. etwa Dienstverweigerung
- Zielsystem mit sinnlosen Anfragen zu beschäftigen, sodass es nicht mehr seiner eigentlichen Aufgabe nachkommen kann
- Ein Quellsystem -> ein Zielsystem:
  - Derjenige mit der höheren Bandbreite gewinnt
  - Relativ einfach zu unterbinden
- Daher: Distributed Denial of Service (DDoS)
  - Durch verteilte Arbeitsweise Angriff mehrerer Quellsysteme auf ein Zielsystem
  - Schwierig abzuwehren
- Überflutung mit Netzwerkpaketen (UDP, ICMP, TCP-SYN)

DDoS-Tools Struktur

- DDoS Tools haben eine charakteristische Struktur bestehend aus Client, Handler und Agent



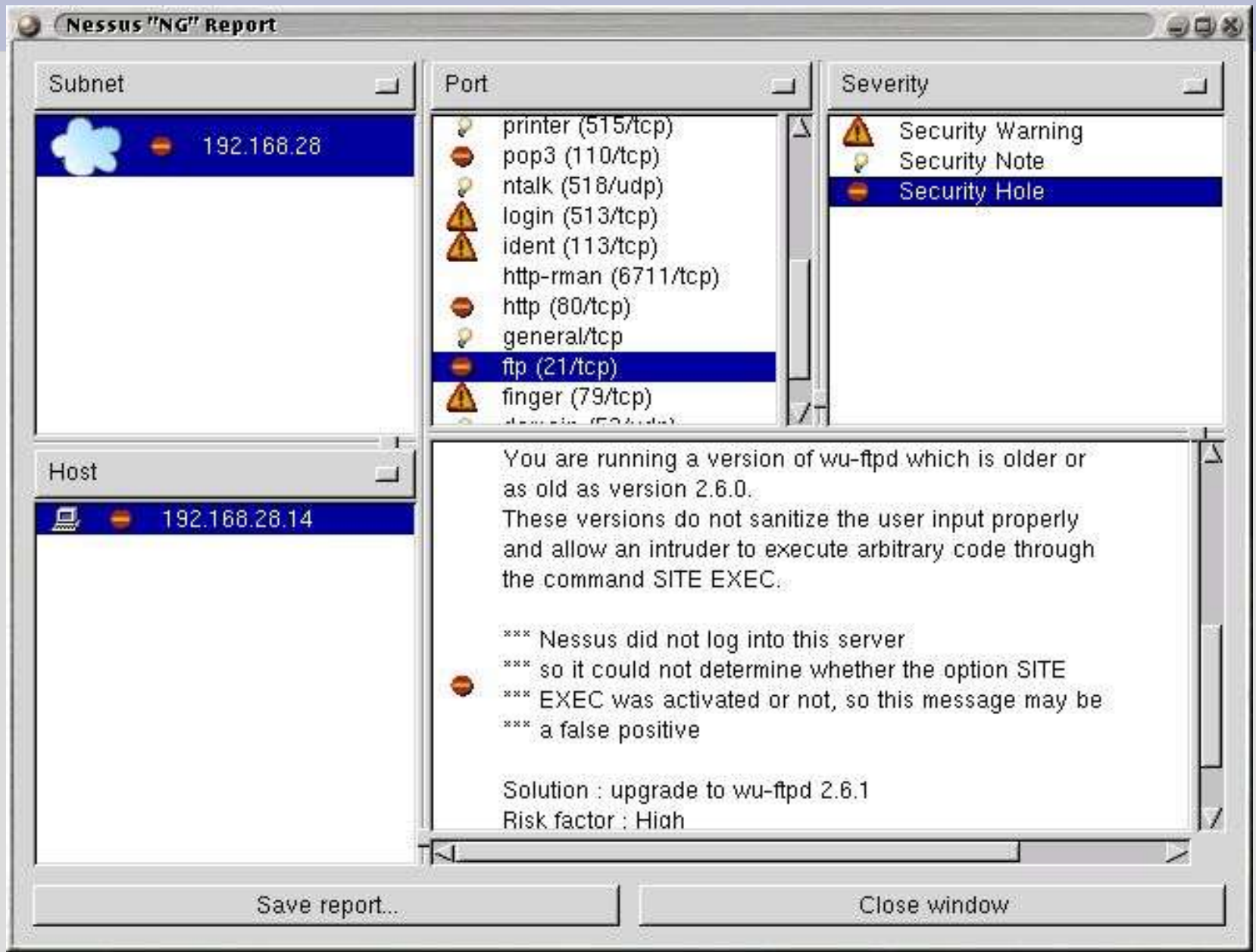
Stacheldraht

- Blowfish-verschlüsselte Kommunikation zwischen Client und Handler
- Kommunikation zwischen Handler und Agent wird durch ICMP-Pakete oder UDP-Datagramme getarnt
- Sehr schwierig zu unterbinden, da ICMP oft nicht als Datenträger vermutet wird und notfalls auf UDP gewechselt werden kann
- Mittlerweile Tools verfügbar, die Stacheldraht aufspüren

Security Scanner

- Traditionell: sobald Verbindung mit Daemon aufgebaut ist, wird Begrüßungsbanner mit Angabe der Software und Version ausgegeben
- Nachteil: verwendete Software und Version sofort erkennbar
- Security Scanner nutzen diese Information, um Schwachstellen oder Sicherheitslücken aufzuzeigen
- Praktisch für die Systemadministration
- Leider auch praktisch für den Hacker
- Beispiel Nessus

Security Scanner: Beispiel Nessus



Rootkits

- Teil des Kernels
- Vollkommen versteckt im System, sobald aktiv
  - Beispielsweise Verzeichnis-Listings ändern und somit Existenz von Dateien verschleiern
  - Netzwerkverbindungen verschleiern
  - Von der Tastatur mitloggen (sog. Key-logging)
  - Andere Systeme angreifen
- Meistens Realisierung als Kernel-Modul
- Schutz durch sog. monolithischen Kernel (keine Module, gesamte Funktionalität im Kernel-Binary)
- Beispiel: LKM

Zusammenfassung Teil 1 (1/2)

- Kryptografische Tools
  - Passwort-Knacker: einfach, aber keine Chance bei guten Passwörtern
- Pufferüberläufe
  - Gefährlich, da oft Exploits im Internet verfügbar
- „Denial of Service“-Angriffe
  - Verteile Arbeitsweise (Distributed Denial of Service)
  - Überflutung des Zielsystems mit sinnlosen Anfragen
- Security Scanner
  - Analysieren Daemons eines Zielsystems und erkennen mögliche Sicherheitslücken
  - Geben Tipps zur Behebung der Schwachstellen

Zusammenfassung Teil 1 (2/2)

- Rootkits
  - Verstecken sich im Kernel
  - Haben (auf gängigen Betriebssystemen) die komplette Macht über das System
  - Können wiederum Angriffe auf andere Systeme starten, z.B. DoS

Teil 2

Benjamin Fabricius

Hackertools Teil 2

Übersicht

- Remote Access Angriffe
  - War Dialing
  - VPN Cracking
- ISO / OSI Schicht 1-3 Angriffe
  - MITM Switch Sniffing I (OSI Schicht 2)
  - MITM Switch Sniffing II (OSI Schicht 3)
  - Firewalls
- Web Hacking
  - Cross Site Scripting und „Defacements“

Remote Access Angriffe (1/2)

War Dialing

-> Motivation und Verletzlichkeit:

- Komprommitieren von jeglichen Netzwerk Hosts oder Komponenten
- Ausnutzen von schwach geschützten Remote Access Servern, Zugangsleitungen oder Tk-Anlagen

-> Angriff:

- Nummern Blöcke suchen und mit War Dialern prüfen
- Trägersignal und Banner erkennen
- Bekannte Schwächen ausnutzen, Fallobst abgreifen oder Brute-Force Attacke starten um Zugang zu bekommen

-> Gegenmaßnahme:

- Genaue Buchhaltung aller Remote Access Zugänge und standfeste Sicherung dieser durch doppelte Authentifizierung z.B.

Remote Access Angriffe (2/2)

VPN Cracking

-> Motivation und Verletzlichkeit
- Netzwerk-Zugang erobern oder verschlüsselte Daten mitlesen
- VPN Gateways mit dynamischem Zugang, die sich in den IKE Aggressive Mode zwingen lassen, ausnutzen

-> Angriff:
- VPN Gateway in IKE Aggressive Mode zwingen (PGPNet Client)
- Authentifizierungs-Hash abfangen, knacken, entschlüsseln und PSK „bergen“ (Cain & Abel)
- Tarnung als trusted user oder MITM Attacke gegen VPN User

-> Gegenmaßnahme:
- Starke Hashverschlüsselung (128Bit)
- Nur starke PSKs bei der Authentifizierung benutzen
- Keine dynamischen IP Addressen in VPNs / kein dynamic crypto map
- Aggressive Mode bei Bedarf deaktivieren

ISO/OSI Schicht Angriffe (1/3)

MITM Switch Sniffing I (OSI Schicht 2)

-> Motivation und Verletzlichkeit
- Mitlesen jeglicher Daten in einem geswitchten Segment
- ARP Schwächen und IP-Forwarding ausnutzen

-> Angriff:
- Angreifer fälscht ARP Pakete und forciert Änderung des ARP Caches seines Opfers (arpredirect)
- Sämtlicher Netzverkehr geht erst über das angreifend System und wird dann mittels IP-Forwarding weitergeleitet (fragrouter)
- Netzverkehr wird ausgelesen (linsniff, tcpdump, ethereal)

-> Gegenmaßnahme:
- statische ARP Routen
- monitoring Tools (arpmonitor)

ISO/OSI Schicht Attacken (2/3)

MITM Switch Sniffing II (OSI Schicht 3)

-> Motivation und Verletzlichkeit
- Mitlesen von (verschlüsselten) Daten, Auslesen von Klartextpasswörtern
- Keine Verschlüsselung bei Protokollen / inkompetenter Umgang mit SSH / SSL

-> Angriff:
- mit MITM Switch Sniffing Realisierung Klartextpasswörter auslesen, POP/SMTP oder HTTP Verkehr abfangen etc. (dsniff, mailsnarf, webspy, ettercap)
- SSH / SSL Verkehr intervenierieren und MITM Attacke fahren (sshmitm, webmitm)
- Durch DNS Spoof vertrautes System vorgaukeln (dnsspoof)

-> Gegenmaßnahmen:
- SSH Kapselung von Protokollen ohne Authentikationsmethodik
- allerdings nur mit grundlegender Kenntnis zu SSH / SSL

ISO/OSI Schicht Attacken (3/3)

Firewalls

-> Motivation und Verletzlichkeit
- Überwinden der Firewall und komprommitieren von Netzressourcen
- Non-Stateful Paketfilter, Mangelnde FW-Regeln und IP-Schwächen ausnutzen

-> Angriff
- Scanning und Banner abgreifen (nmap, firewalk)
- Quellport – Angriff
- ICMP oder UDP Kapselung von von Echtdaten (loki)
- IP Fragment Angriffe

-> Gegenmaßnahme
- Stateful Firewalls / Proxy Firewall
- grundlegende ACL Kenntnisse
- IP-Fragmentierung bei Bedarf durch FW-Regeln unterbinden

Web Hacking (1/1)

Cross Site Scripting (XSS) und „Defacements“

-> Motivation und Verletzlichkeit

- Vandalismus, persönliche Interessen, politische Meinungsmache
- Schlecht programmierte Skripte und „exploit“bare Dienste ausnutzen

-> Angriff

- Sichten von fehlerhaften Skripten und Erkennung von unsicheren Diensten
- Injizieren von schädlichem Code
- unter Umständen Eroberung des Opfersystems mit User- oder Root-Rechten
- Verändern der eigentlichen Homepage mittels Ersetzung durch die des Angreifers

-> Gegenmaßnahme

- Gründliche Datenprüfung in Skripten
- Regelmäßige Prüfung der Sicherheit angebotener Dienste

Quellen

- Kurtz, G. / McClure, S. / Scambray, J.: „Das Anti-Hacker-Buch“, 4.Aufl. 2003, MITP-Verlag
- http://www.zone-h.org
- http://www.securityfocus.com
- http://packetstormsecurity.nl
- http://www.nessus.org
- http://ettercap.sourceforge.net
- http://www.insecure.org
- http://www.attrition.org
- http://www.vulnwatch.org
- http://www.atstake.org
- Weitere Quellen entnehmen Sie bitte der Ausarbeitung