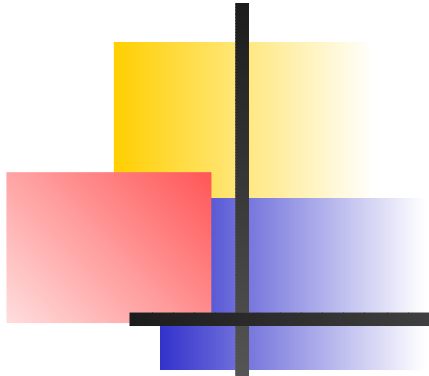


Entfernte Analyse von Netzen

- ich weiss was du weisst -

Torsten Höfler

htor@unixer.de

TU-Chemnitz

Motivation

TECHNISCHE UNIVERSITÄT CHEMNITZ

- Spionage
- Faszination der Macht
- Begeisterung für technische Möglichkeiten
- Geltungsdrang - “sportlicher Ehrgeiz“
- Zerstörungswille
- Rachsucht (ehemalige Mitarbeiter)
- ...

typische Angriffsziele

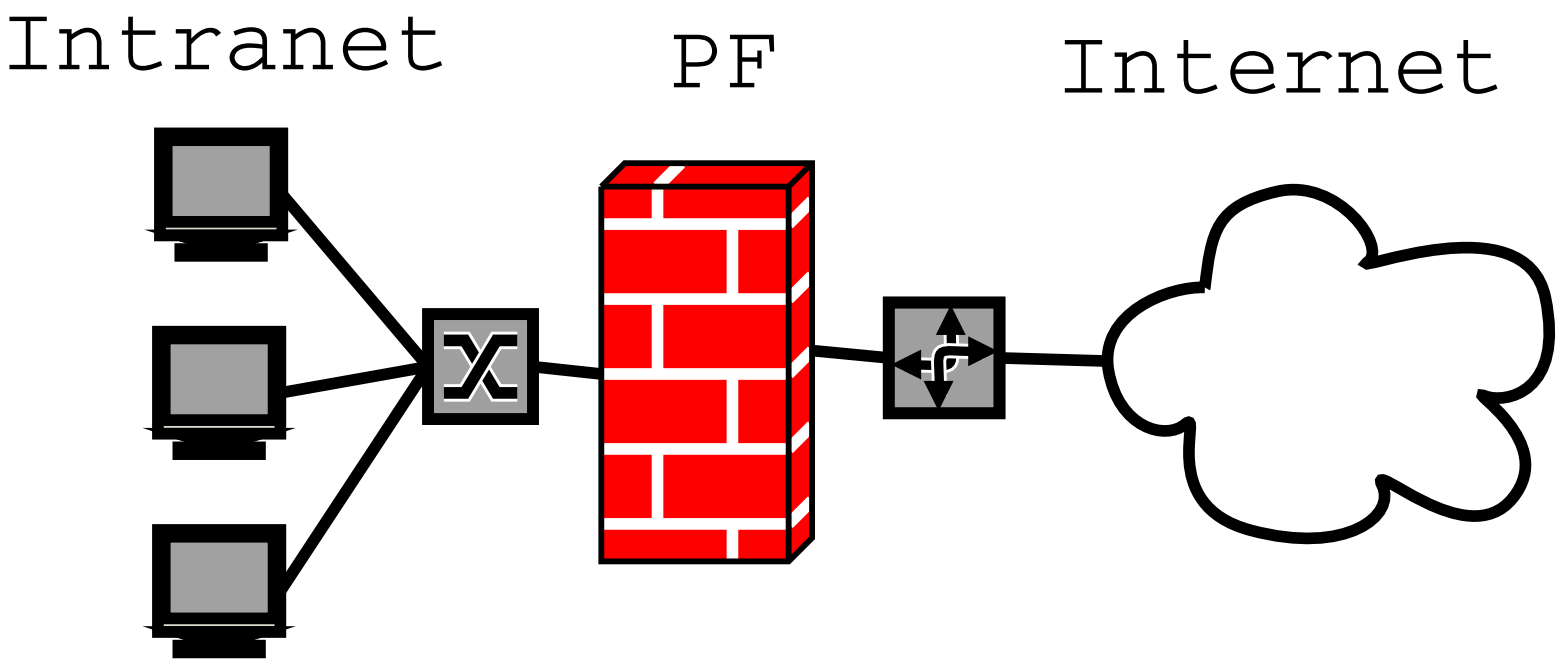
TECHNISCHE UNIVERSITÄT CHEMNITZ

- Router / Firewalls / Packetfilter
- Intrusion Detection Systeme
- Loghosts (um Spuren zu verwischen)
- nach aussen erreichbare Server (DMZ?)
- Clientsysteme
- Hardwaresysteme (z.B. Access Points ...)

Allgemeiner Aufbau eines Firewallsystems

TECHNISCHE UNIVERSITÄT CHEMNITZ

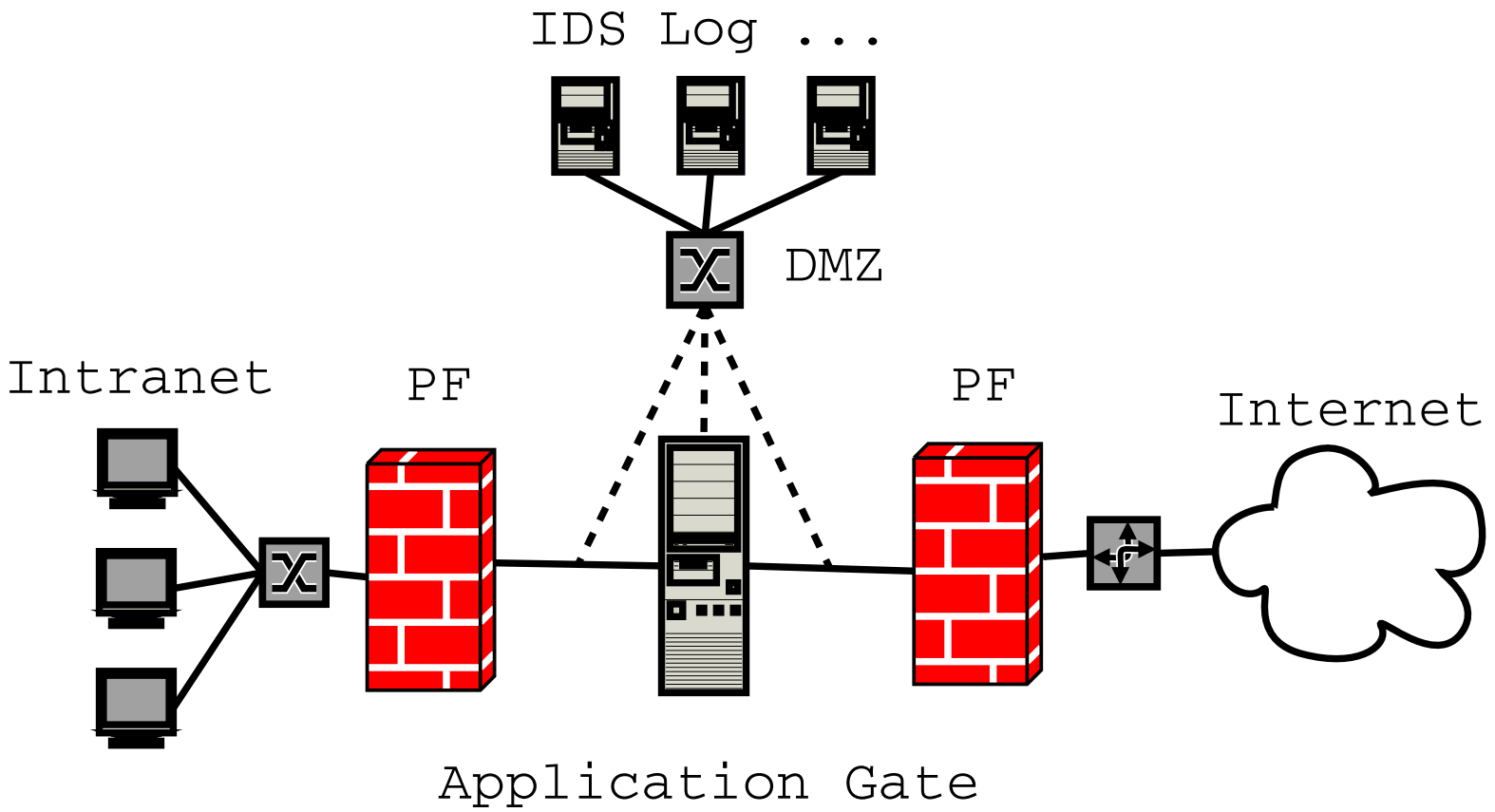
einfache Variante:



Allgemeiner Aufbau eines Firewallsystems

TECHNISCHE UNIVERSITÄT CHEMNITZ

komplexere Varianten:



Angriffsvektoren aus dem Internet

TECHNISCHE UNIVERSITÄT CHEMNITZ

$\Rightarrow$ Angreifer (wir) im Internet

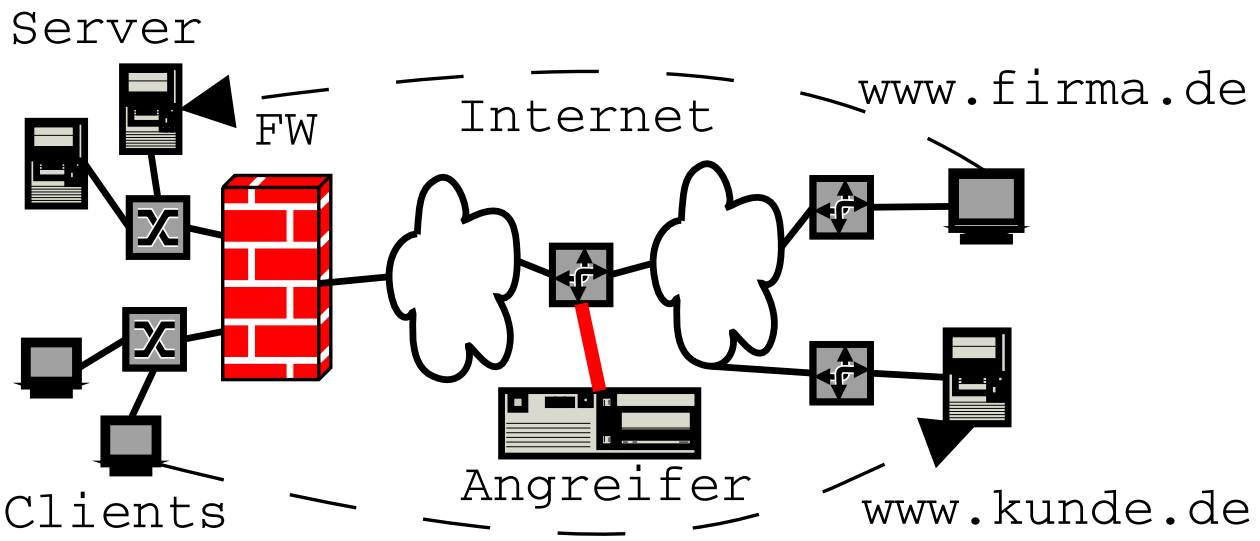
- passive remote Analyse (z.B. sniffing)
- aktive remote Anaylse (z.B. scanning)
- Analyse aktiver Komponenten (z.B. fingerprinting)
- Topologieanalyse (z.B. firewalking, tracing)
- social engineering

passive Analyse

TECHNISCHE UNIVERSITÄT CHEMNITZ

⇒ verscheidene Möglichkeiten:

- sniffi ng
  - Headeranalyse
  - passive fi ngerprinting
  - payload Analyse (z.B. Softwareversionen)



passive Analyse - Headeranalyse

TECHNISCHE UNIVERSITÄT CHEMNITZ

- bringt Verständnis der Topologie z.B.:
  - TTL: OS generiert normalerweise „runden“ Startwert (255, 128, 64 ...) -> Abweichung bestimmt Hopcount
  - Ausnahmen (z.B. traceroute) beachten!
- angebotene bzw. genutzte Dienste z.B.:
  - Source- bzw. Dest.-Ports auswerten

passive Analyse - Headeranalyse

TECHNISCHE UNIVERSITÄT CHEMNITZ

aus Headerfeldern ist einiges ableitbar:

Feld	Ort	Tools?	Was?
TTL	IP	x	OS + Topologie
Fragmentation	IP	x	OS
Header Length	IP	x	OS
TOS	IP	-	OS
ID	IP	-	OS + Traffi c
Source Port	TCP	-	OS + Traffi c
Window Size	TCP/Opt	x	OS
Max. Segmentgr.	TCP/Opt	x	OS
...	...	-	OS

passive Analyse - passive fingerprinting

TECHNISCHE UNIVERSITÄT CHEMNITZ

fingerprinting ohne den Versand von Paketen

- beruht auf Abweichungen des OS vom Standard (RFC)
- kumulative Analyse verschiedener Headerfelder
- von Hand fast unmöglich, da umfangreiche Datenbanken („Signaturen“)
- $\Rightarrow$ automatisierte Tools (siphon, p0f)
- ABER: sehr langsam! $\Rightarrow$ aktive Analyse

passive Analyse - passive fingerprinting

TECHNISCHE UNIVERSITÄT CHEMNITZ

Beispiele (p0f - SYN/ACK Auswertung):

- www.tu-chemnitz.de:80 - Linux recent 2.4 (1) (up: 866 hrs)
- gulliver.hrz.tu-chemnitz.de:22 - UNKNOWN (up: 4760 hrs)
- rotuma.informatik.tuc.de:22 - Linux older 2.04 (up: 703 hrs)
- www.microsoft.de:80 - Windows 2000 (SP1+) (fi rewall!)
- www.openbsd.org:80 - Solaris 7 (up: 2533 hrs)
- www.mcafee.com:80 - Windows 2000 SP4
- www.georgewbush.com:80 - Windows 2000 SP4
- www.nsa.gov:80 - Linux recent 2.4 (1) (up: 5664 hrs)
- www.bundeskanzler.de:80 - Linux recent 2.4 (1) (up: 11405 hrs)
- ...

aktive Analyse - active fingerprinting

TECHNISCHE UNIVERSITÄT CHEMNITZ

fingerprinting mit Paketversand und Analyse der Antwort

- zwei Hauptnachteile:
  - leicht festzustellen (vgl. Portscan)
  - Packetfilter kann Ergebnisse blocken bzw. verfälschen
- quasi-Standard: nmap von Fyodor
- $\Rightarrow$ wird von IDS oder Packetfilter als „Standard-Tool“ erkannt und kann gefiltert werden

fingerprinting - neue Ansätze

TECHNISCHE UNIVERSITÄT CHEMNITZ

- nmap braucht 1 offenen und geschlossenen TCP-Port + 1 geschl. UDP-Port (praktisch nicht anzufinden wegen firewall)
- man muss andere Metriken finden
- $\Rightarrow$ RING (**R**emote **I**dentification **N**ext **G**eneration)
- TCP Retransmissioncount und -time wird verwendet!
  (Sendet Anfrage an offenen Port und dann nichts mehr)

advanced scanning

TECHNISCHE UNIVERSITÄT CHEMNITZ

Inverse Mapping

- normale „unauffällige“ Pakete an verschiedene IP-Adressen
- z.B. FIN, ACK, DNS-Reply
- nicht existierende Rechner: Router generiert ICMP host unreachable -> Angreifer schlussfolgert Netzstruktur/belegte IP Bereiche

Slow Scan

- Scanrate < 1 Paket/Stunde
- sind automatisiert nur schwer erkennbar

advanced scanning

TECHNISCHE UNIVERSITÄT CHEMNITZ

Idle Scan

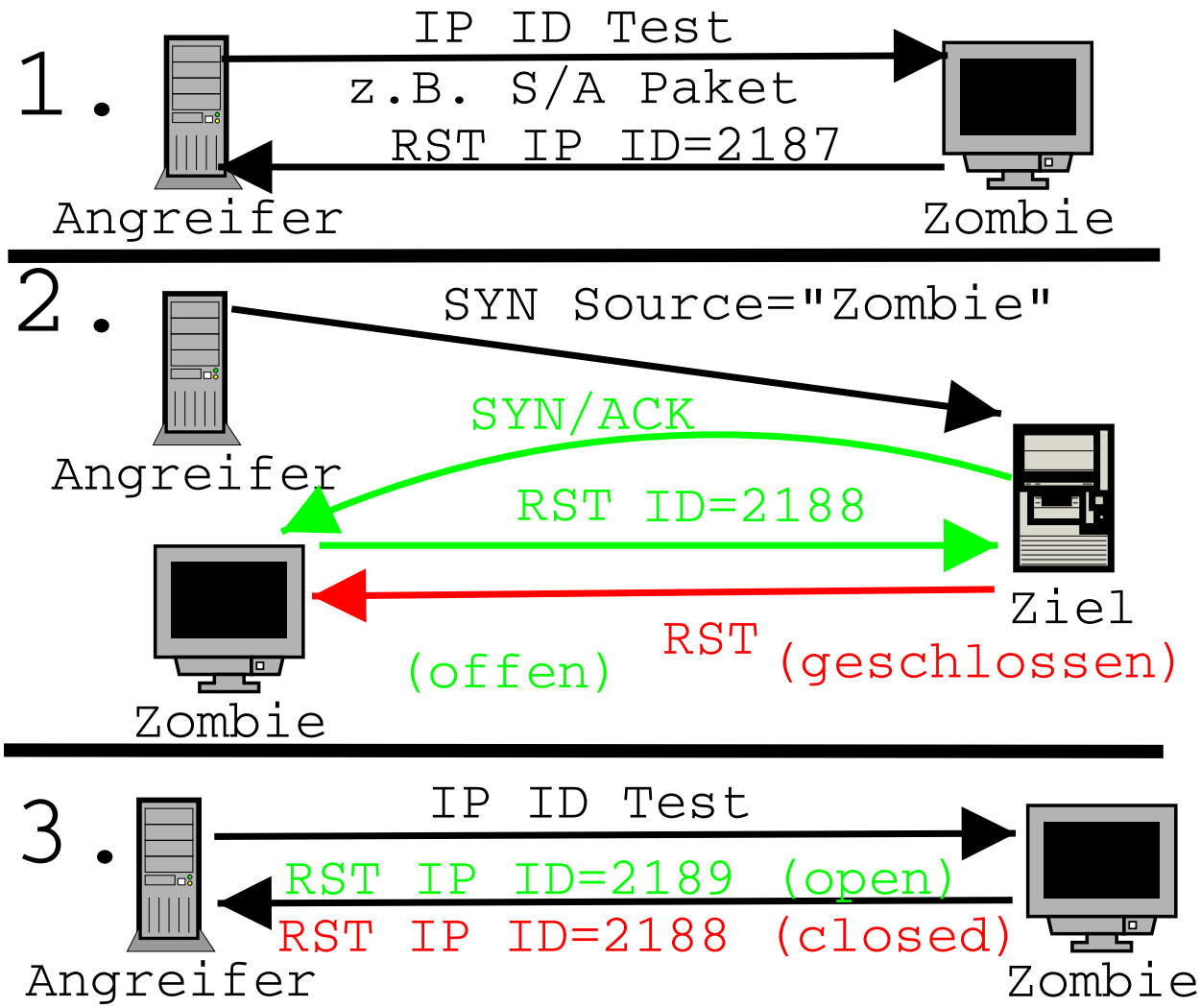
- kein Paket direkt → Versand über „Zombie“ Hosts
- Ausnutzung der vorhersagbaren Fragmentnummer im IP-Paket
- auch zum Test von IP-basierten Filtern
- IDS meldet den „Zombie“ als Angreifer

Gegenmaßnahmen:

- eingehende Pakete von unlogischen Adressen droppen (z.B. internes Netz)
- stateful fi rewall
- OS mit schwer vorhersagbaren IP IDs

advanced scanning

TECHNISCHE UNIVERSITÄT CHEMNITZ



advanced scanning

TECHNISCHE UNIVERSITÄT CHEMNITZ

Gefahr als Zombie genutzt zu werden ist gross!
z.B. an der TUC verfügbare Zombies (von extern):

- gulliver.hrz.tu-chemnitz.de (Solaris)
- pontius.hrz.tu-chemnitz.de (HP-UX)
- sunnyboy.informatik.tu-chemnitz.de (Solaris)
- rotuma.informatik.tu-chemnitz.de (Linux)
- sogar geschützte Rechner sind nutzbar:
- zucker.informatik.tu-chemnitz.de (134.109.184.191)
- ...

firewalking

TECHNISCHE UNIVERSITÄT CHEMNITZ

= Analyse des Netzes einer Firewall (packetfilter)
z.B. Testen ob IP erreichbar:

- SYN-Pakete werden von FW verworfen
- SYN/ACK nicht (nur stateful FWs)
- mittels SYN/ACK Paketen kann man IPs (hinter FW) scannen
- ruleset der FW kann ermittelt werden

firewalking

TECHNISCHE UNIVERSITÄT CHEMNITZ

z.B. Portscan auf wald.informatik.tu-chemnitz.de (134.109.184.40) von extern:
archimedes: # hping2 wald.informatik.tu-chemnitz.de -p 22 -A
HPING wald.informatik.tu-chemnitz.de (eth0 134.109.184.40): A set ...
len=46 ip=134.109.184.40 ttl=55 DF id=0 sport=22 flags=R seq=0 win=0 rtt=64.3 ms
len=46 ip=134.109.184.40 ttl=55 DF id=0 sport=22 flags=R seq=1 win=0 rtt=64.8 ms
$\Rightarrow$ Port 22 (ssh) offen

archimedes: # hping2 wald.informatik.tu-chemnitz.de -p 81 -A
HPING wald.informatik.tu-chemnitz.de (eth0 134.109.184.40): A set ...
ICMP Port Unreachable from ip=134.109.184.40 name=wald
ICMP Port Unreachable from ip=134.109.184.40 name=wald
$\Rightarrow$ Port 81 closed

Laufen die Poolrechner am Wochenende?
HPING donau.hrz.tu-chemnitz.de (eth0 134.109.72.177): SA set ...
len=46 ip=134.109.72.177 ttl=55 DF id=0 sport=82 flags=R seq=0 win=0 rtt=62.5 ms
len=46 ip=134.109.72.177 ttl=55 DF id=0 sport=82 flags=R seq=1 win=0 rtt=65.4 ms
$\Rightarrow$ ja ;o)

firewalking

TECHNISCHE UNIVERSITÄT CHEMNITZ

lt. Cambridge Technology Partners: „A Traceroute-Like Analysis of IP Packet Responses to determine Gateway Access Control Lists.“

- neuere Entwicklung
- 1. Phase: Hopcount bis FW (Gateway) wird ermittelt = HC(FW)
- 2. Phase: Pakete mit TTL=HC(GW)+1 zum SYN Scan
- wenn HC(target) > HC(GW)+2 $\rightarrow$ kein Paket erreicht target
- offener Port: ICMP Time exceed
- geschl. Port: keine Antwort (Timeout)
- Abhilfe:
  - ausgehende ICMP Time exceed verwerfen
  - application proxy

Abhilfe (Client)

TECHNISCHE UNIVERSITÄT CHEMNITZ

auf Linux bezogen (Anpassen von Kernel-Parametern):

- /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts = 1
- /proc/sys/net/ipv4/conf/*/accept_source_route = 0
- /proc/sys/net/ipv4/conf/*/rp_fi lter = 1 (Pakete für lokal die auf einem Interface reinkommen und auf einem anderen rausgehen werden gedroppt → spoofi ng)
- /proc/sys/net/ipv4/ipfrag_high_thresh = ? (ab diesem Wert werden Fragmente verworfen - Rose Attacks?)
- /proc/sys/net/ipv4/ipfrag_low_thresh = ? (ab diesem Wert werden Fragmente wieder akzeptiert)
- /proc/sys/net/ipv4/conf/*/log_martians (Pakete mit illegalen Adressen werden geloggt)
- /proc/sys/net/ipv4/ip_default_ttl = ? (verwirrt OS detection)

Abhilfe (Client)

TECHNISCHE UNIVERSITÄT CHEMNITZ

auf Linux bezogen (www.grsecurity.org - features):

- Larger entropy pools (bessere Zufallszahlen)
- Randomized TCP Initial Sequence Numbers (erschwert OS detection)
- Randomized IP IDs (verhindert „Zombie“-Scan)
- Randomized TCP source ports (erschwert OS detection)

$\Rightarrow$ eigene Anpassungen im Sourcecode

- z.B. keine Antwort auf illegale Pakete: /usr/src/linux/net/ipv4/*
- ändern der Window Size: /usr/src/linux/include/net/tcp.h (MAX_TCP_WINDOW)
- ...

deep packet inspection

TECHNISCHE UNIVERSITÄT CHEMNITZ

Firewall Evolution

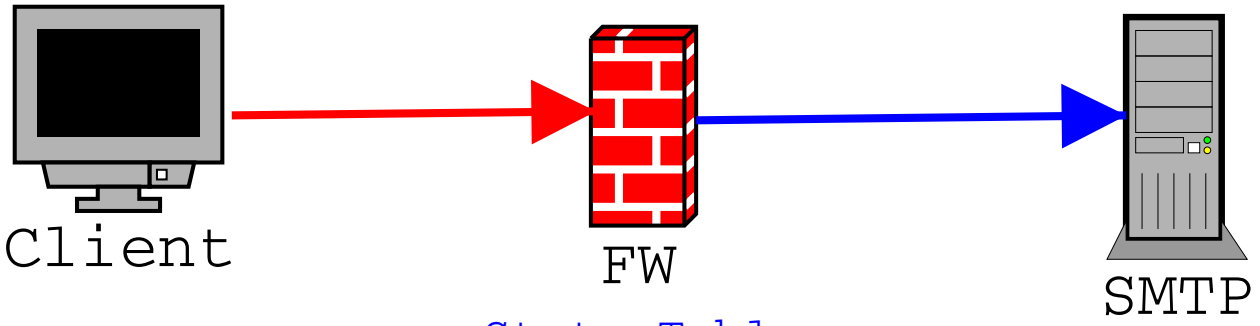
- Firewall - Schutzfunktion
- IDS - Überwachungsfunktion
- derzeit: manuelles Einschreiten notwendig
- Problem: schnelle Attacken (Code Red, Nimda)
- $\rightarrow$ deep packet inspection = FW + IDS
- Exploits können beim Versuch (automatisch) verhindert werden

z.B. Überwachung auch auf Applikationsebene

(vgl. PIX „fi xup“ Befehl) $\Rightarrow$ nächste Folie

deep packet inspection

TECHNISCHE UNIVERSITÄT CHEMNITZ



State Table:
SMTP: client:1025 - SMTP:25

Protokoll (SMTP):

Fragen?

TECHNISCHE UNIVERSITÄT CHEMNITZ

Vielen Dank
für Ihre
Aufmerksamkeit!

Torsten Höfler
<htor@unixer.de>

Quellen

TECHNISCHE UNIVERSITÄT CHEMNITZ

- eigene Erfahrung :o)
- Laurent Joncheray: Simple Active Attack Against TCP, 1995
- Kevin Timm: Passive Network Traffi c Analysis, 2003
- Lance Spitzner: Passive Fingerprinting, 2000
- Fyodor: Remote OS detection via TCP/IP Stack FingerPrinting, 1998
- Intranode Research: RING - Full Paper, 2002
- Synnergy Networks: Advanced Host Detection, 2001
- Cambridge Technology Partners: Firewalking, 1998
- Ido Dubrawsky: Firewall Evolution - Deep Packet Inspection, 2003