

Geswitchtes Netzwerk und Sicherheit?

Laboringenieur an der Hochschule Wismar

Studienrichtung Nachrichten und Kommunikationstechnik



Seit 2000 Netzwerkakademie Wismar

www.networking-academy.de

CCNA, Cisco Certified Academy Instructor

2001 CCNP- Instruktor

2004 FNS- Instruktor

2004 Gemeinschaftsinitiative

www.network-security-lab.de/

FNS- Instruktorausbildung

CCNP- Instruktorausbildung



Laut einer Studie der Gartner-Gruppe :

Erfolgen mehr als **70 Prozent** aller unberechtigten Zugriffe auf EDV-Systemen durch **autorisierte** Benutzer, seien es die eigenen Mitarbeiter oder Partner mehr als **95 Prozent** aller Angriffe führen zu einem signifikanten finanziellen Verlust

AGENDA

- Switch Mythos
- Gruppierung von Netzwerk Attacken
- Gebrauch von Sniffen Hub vs. Switch
- Vielfalt der Layer 2 Attacken (basic Attacken)
- Demonstration
 - MAC Flooding
 - ARP – spoofing
 - Man in the Middle Attack (DNS- Spoofing)
- Zusammenfassung

Switch Mythos

Switche (L2) nutzen MAC- Adresse zur Forwarding-Entscheidung

-> MAC- Adresse kann nicht verändert und gefälscht werden -> fest eingebrannt

Switche bauen direkte Verbindungen (Mikrosegmente) zum Ziel auf

-> Verhinderung des Mitlesens

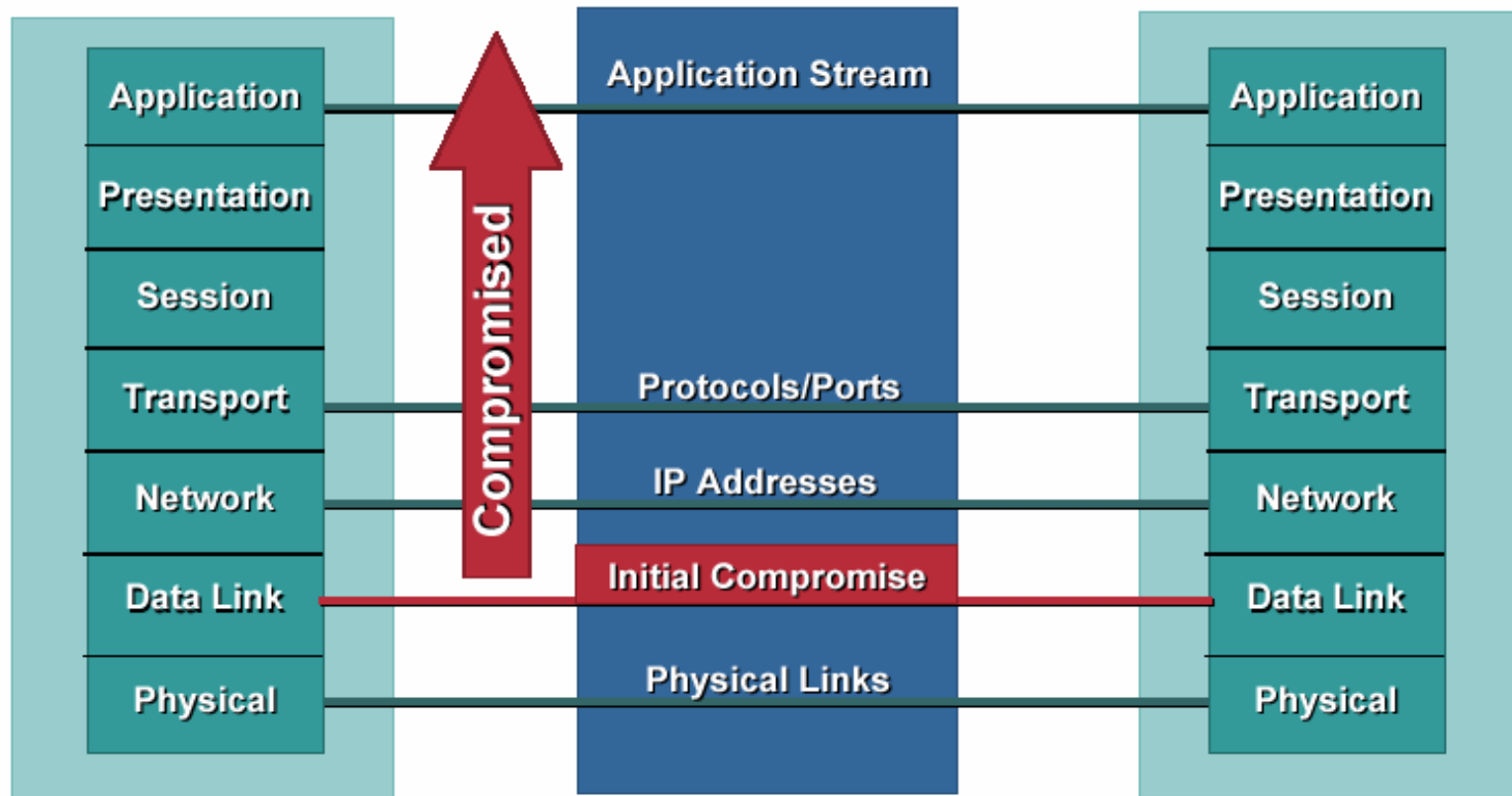
Switche teilen Broadcastdomänen auf

-> VLAN's sind völlig isoliert

The Domino Effect

Cisco.com

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- **Security is only as strong as your weakest link**
- When it comes to networking, layer 2 can be a **VERY** weak link



Gruppierung von Netzwerk Attacken

- **Passive Attacken**

- **Mitlesen von Informationen**
- **Analyse der fremden Informationen**

- **Aktive Attacken**

- **Denial of Service**
- **Spoofing**
- **Ändern und Missbrauch**
- **Viren, Würmer, Trojanische Pferde ...**

Gruppierung von Netzwerk Attacken (count.)

z. B. Mitlesen

- Nichterlaubtes Zuhören bei einer Netzkommunikation z.B Mailclient zum Mailserver , Öffnen von fremden Briefen

- Entsprechend des Netzmediums / Gerätes -> einfach oder schwer

-z.B. Layer1- Funktionalität:

Twisted-Pair und Coax	->	meist leicht
Glasfaser	->	relativ schwer
WLAN	->	sehr einfach
Hub	->	sehr einfach

-Layer2- Funktionalität:

Switch	->	schwieriger ?
Mitlesen im eigenen Netz	->	relativ einfach
Internet	->	schwieriger ?

Gebrauch von Sniffen Hub vs. Switch

- Schnüfflerprogramme „Sniffer“

meist im „Negativen“ betrachtet

Eigentliche Funktion:

Protokollanalyse entsprechend des OSI-Modells,

Testung Überwachung, Monitoring des eigenen Netzes,

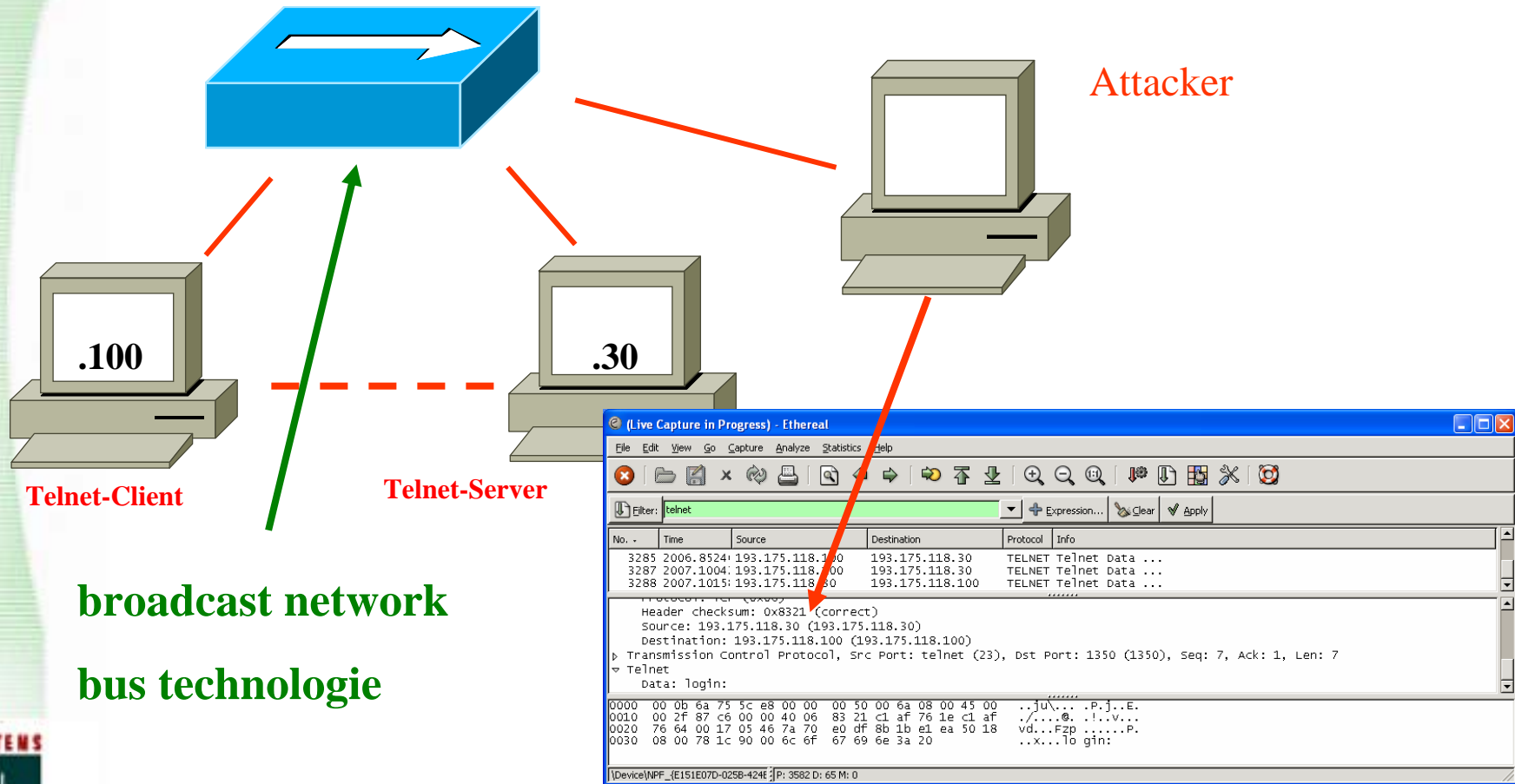
Applikationsentwicklung

Funktionsweise

Netzwerkkarte leitet normalerweise nur an sie gerichtete Daten weiter, andere Daten werden ignoriert

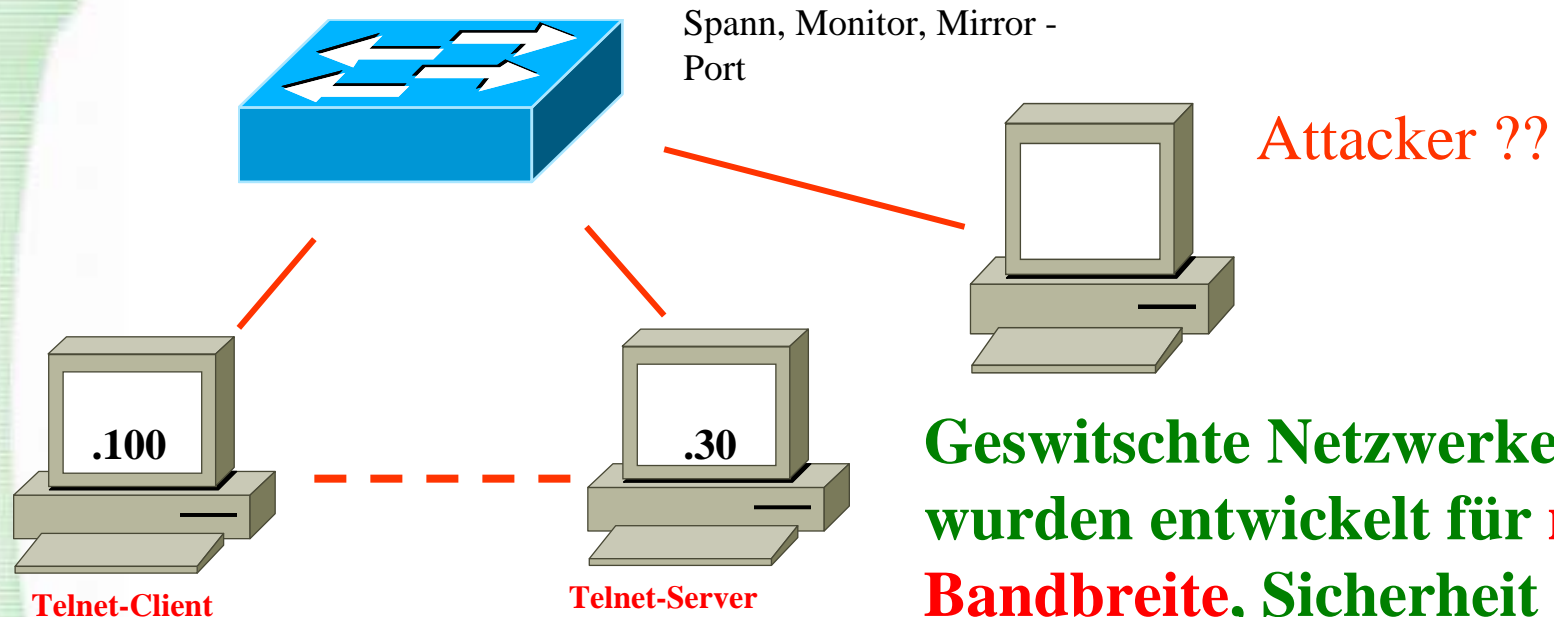
Sniffer schalten die NIC in den Monitor bzw. promiscuous-mode

Gebrauch von Sniffern Hub vs. Switch (count)



**broadcast network
bus technologie**

Gebrauch von Sniffern Hub vs. Switch (count)



Geswitschte Netzwerke wurden entwickelt für **mehr Bandbreite, Sicherheit ?**

Zugriff auf Switch-Konfig.

- console –telnet, ssh

Vielfalt der Layer 2 Attacken

Übersicht

-MAC Attacken

-ARP Attacken

-VLAN „Hopping“

-Spanning Tree Attacken

- DHCP, VTP

Vielfalt der Layer 2 Attacken

MAC Attacken

z.B. MAC Flooding (Überfluten des Switchs mit MAC's)

- **Attacker- Rechner sendet Frames mit vielen zufälligen MAC- Sourceadressen zum Switch**

- **Switche lernen an Hand der Source- Mac, -> Switch füllt (begrenzte) MAC-zu- Port Tabelle**

(**CAM** Content Addressable Memory)

- **Wenn der Switch keinen Pufferspeichererplatz mehr hat, (fail open) -> Funktion Hub**

- **Attacke seit 1999 bekannt und genutzt -> siehe Demo**

Vielfalt der Layer 2 Attacken

MAC Attacken

z.B. **MAC Duplicating** oder „**Switch Port Stealing**“

Voraussetzung: man kennt MAC-Adresse des Opferrechners,

– dann senden eines Frames mit Opfer-Quelladresse und Attacker Destination

ändern „spooft“ der eigenen MAC- Adresse „*Mac MakeUp*“; *ifconfig eth0 down hw ether 00:11:22:33:44:55*

ifconfig eth0 up

Es erfolgt kein physikalischer Adresswechsel; es ist eine gespoofte Adresse oder „fake address“

– Der Switch lernt, das an einem zweiten Port die gleiche MAC- Adresse existiert, überschreibt CAM -> Attacker kann Frames für das Opfer lesen

- Wechselseitiges Senden mit OpferMAC

Vielfalt der Layer 2 Attacken

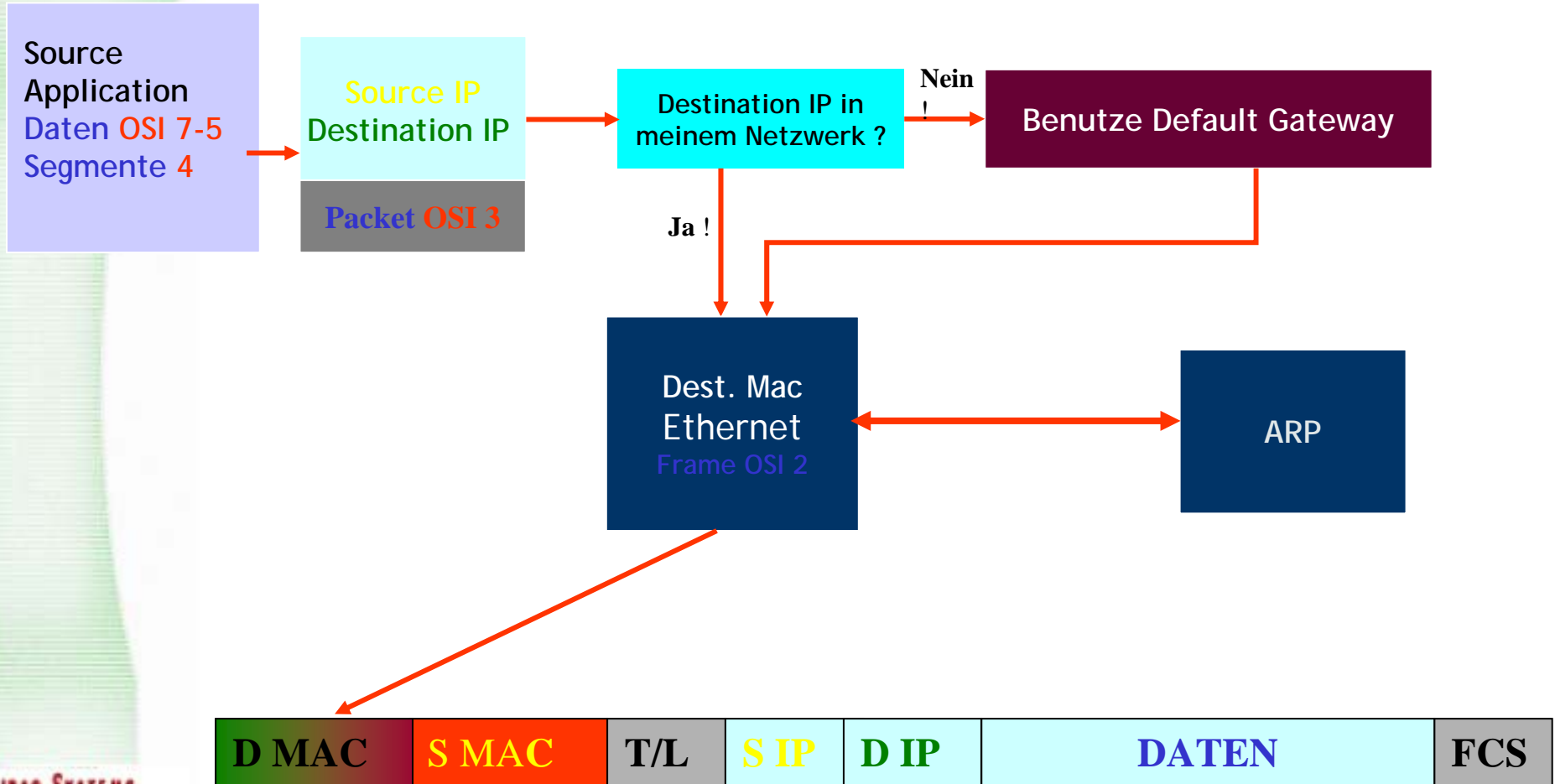
MAC Attacken - Verminderung

Port- Security:

- Plattform und herstellerabhängig
- Spezifizierung von Mac- Adressen am Port
 - Verletzungen -> Port shutdown
 - verhindert Mac- Flooding

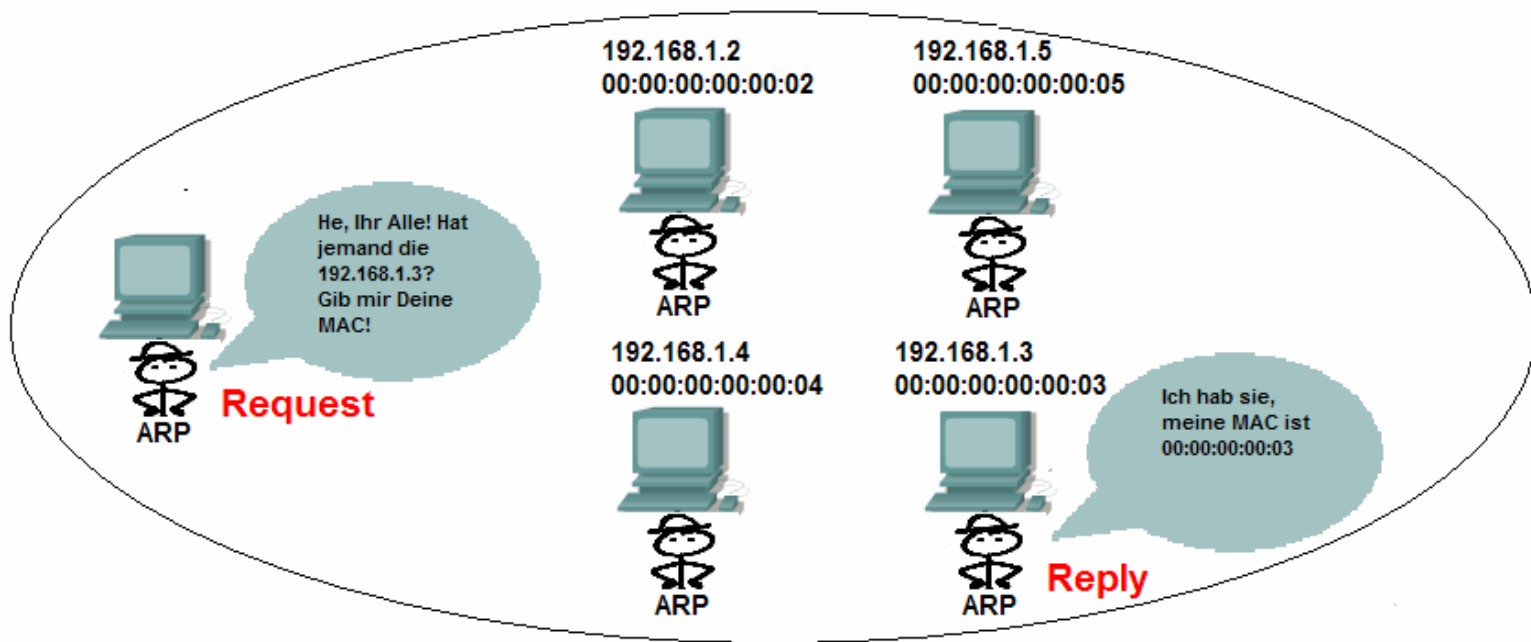
Vielfalt der Layer 2 Attacken

Normaler Encapsulation Prozess



Vielfalt der Layer 2 Attacken

ARP Attacken



-Speichern der IP/MAC- Zuordnung lokal im ARP -Cache

--> minimiert Broadcast

-Cache wird mit jedem neuem ARP- Reply

-ARP ist ein „stateless“ Protokoll und erfordert keine Authentication

Vielfalt der Layer 2 Attacken

ARP- Spoofing (Schwindeln)

Ich bin ein Anderer!

Kenntnis über die beiden Adressen eines Hosts/Gerätes:

- Mac/Ethernet Adresse -> Hardwareadresse der NIC
- die IP- Adresse -> logische Adresse Software konfiguriert

Herausfinden durch z.B. Ping an das Netz!

ARP- Spoofing als Voraussetzung für „Man in the Middle“ im geschwichten Netzwerk

ARP- Spoofing:

-Nutzt falsche ARP- Replies mit der Updatefähigkeit des ARP- Caches, ungeachtet der eigenen gesendeten Requests

-Falsche ARP- Replies haben meist nur Erfolg, wenn ein Eintrag MAC/IP vorhanden ist (OS abhängig)

-Der Prozess der Verfälschung des ARP- Caches wird als „Poisoning“ bezeichnet.

Vielfalt der Layer 2 Attacken

ARP- Attacken - Verminderung

Verwendung von Intusion Detection / Prevention Systemen

-> Erkennen erhöhten ARP- Traffic

Verwendung von Software zur Überwachung der MAC/IP-
Paare (ARPWatch *Linux*, WinARP)

Statische ARP für wichtige Netzgeräte

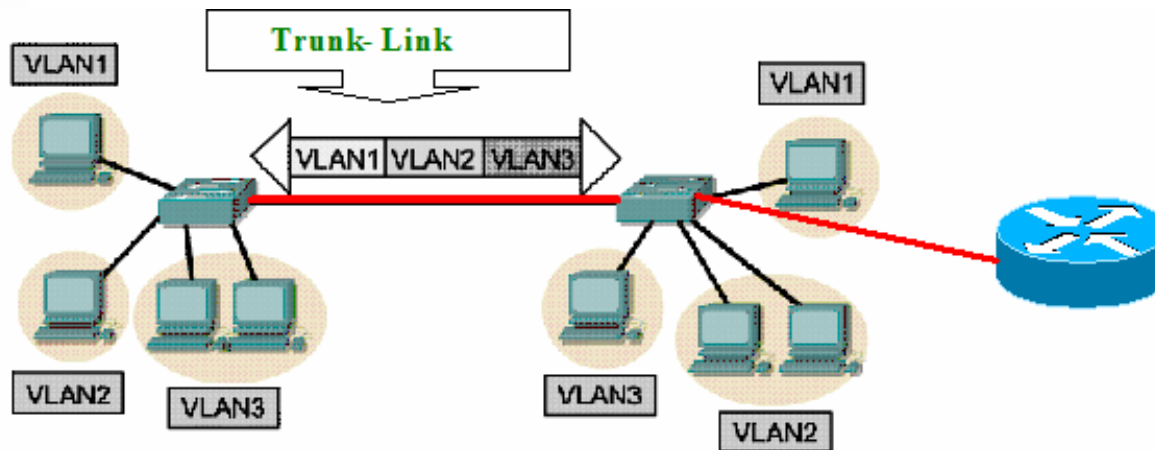
ARP- Firewalls , professionelle Firewalls mit ARP-Spoofing
Erkennung

Einrichten von Privaten VLAN's

Kommunikation zwischen Host's meist nicht möglich

Vielfalt der Layer 2 Attacken

VLAN „Hopping“ Basics



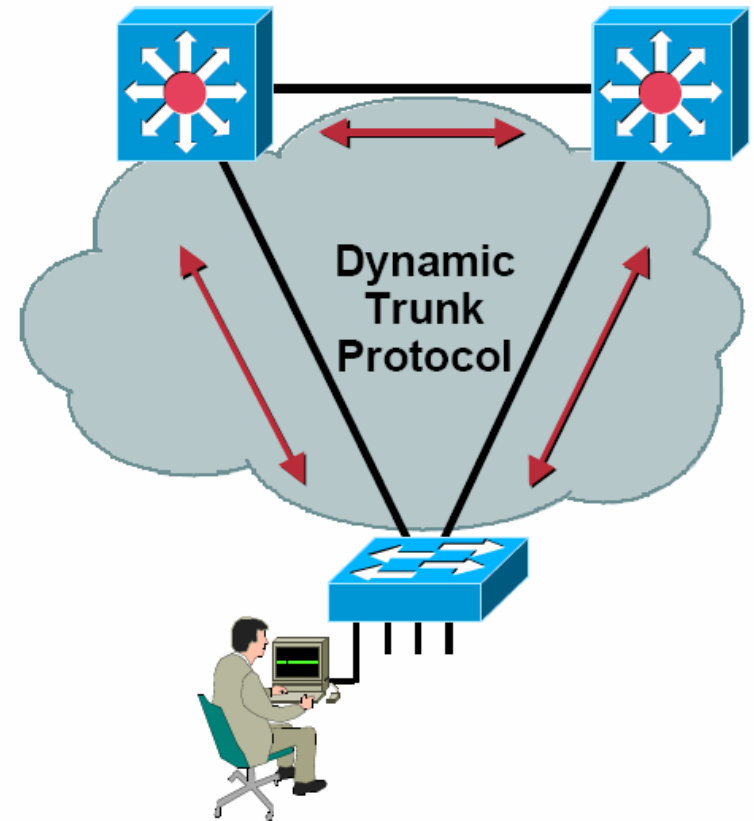
- Trunk Ports transportieren bei einer Standard Konfiguration alle VLAN's zwischen Switchen und/oder Routern auf dem selben physikalischen Link
- Verwendung von automatischer Trunk- Synchronisation mit DTP (Dynamic Trunk Protocol)

Vielfalt der Layer 2 Attacken

VLAN „Hopping“ Basics

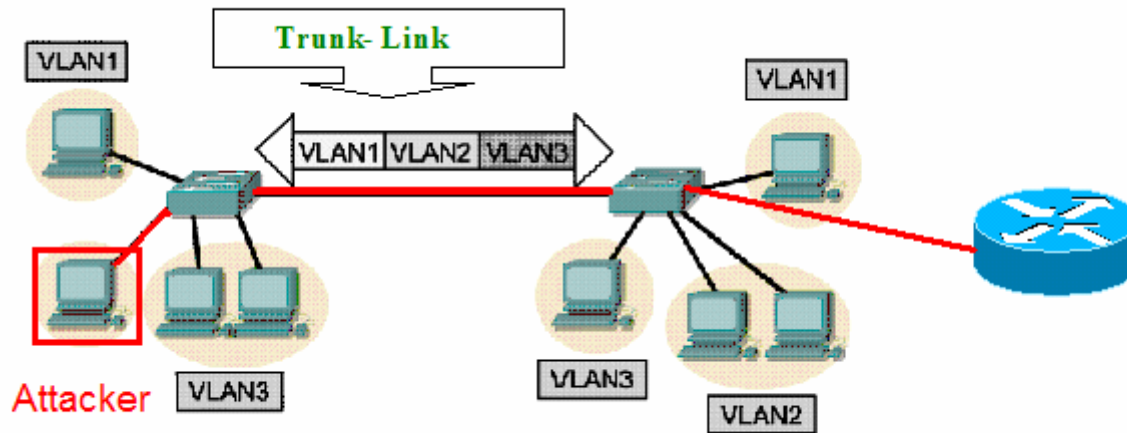
Was ist DTP?

- automatisiert 802.1Q/ISL Trunk-Konfiguration
- arbeitet nur bei Switchen
- synchronisiert Port- Mode
- DTP Status kann sein.
- „Auto, ON, OFF, Desirable, Non-Negotiate“



Vielfalt der Layer 2 Attacken

VLAN „Hopping“ Basics



Standardmäßig ist ein Switchport auf Trunk Mode auto ->

- senden von gefälschten DTP- Frames (Packetgenerator)
- Attacker schaltet Switchport in Trunk- Mode um
- Zugriff auf alle transportierten VLAN- Daten möglich

Vielfalt der Layer 2 Attacken

VLAN Attacken - Verminderung

- Ausschalten von ungenutzten Ports
- Ausschalten von DTP an User- Ports

Demonstration

MAC Flooding

ARP Spoofing

MiM DNS-Spoofing

Demonstration

Verwendete Tools: Linux Tool „dsniff“ <http://www.monkey.org/~dugsong/dsniff>

- Was ist „dsniff“ ?

Freies Tool für:

capturing von Authentifizierungsdaten mit Anwendung von ARP-Spoofing

Anwendung der libpcap library (capture und process von Frames/Packeten)

kann mehrere Authentifizierungsprotokolle decodieren:

**PC Anywhere, NNTP (Network News Transfer Protocol)
AOL Instant Messenger, ICQ, HTTP, FTP, IMAP
POP, Napster, SNMP, Oracle, RPC mount Requests,
LDAP, Telnet, SQL, RIP, rlogin, OSPF, IRC, Citrix , ssh-1 .**

Demonstration

Tools im dsniff Packet:

- Arpspoof:** abfangen einer Ziel-MAC und spoofen einer falschen MAC
- TCPnice:** verlangsamen laufender TCP-Sessions
- FindGW:** FindGW passives sniffing zum Bestimmen des lokalen Gateways
- Macof:** Macof flutet das lokale LAN mit zufälligen gefälschten MAC's
- TCPKill:** beendet active TCP –Verbindungen
- Mailsnarf:** capturing und Ausgabe von SMTP
- WebSpy:** captures und sendet URL Informationen zu einem Web- Client in Echtzeit
- UrlSnarf:** aufzeichnen und ausgeben von URL's im CLF

Demonstration

MAC- Flooding

The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No. .	Time	Source	Destination	Protocol	Info
195986	617.292441	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
196533	618.792356	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
197068	620.292506	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
197594	621.792468	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
198131	623.292598	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
198656	624.792476	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
199174	626.292596	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
199712	627.792610	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
200246	629.292750	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
200773	630.792673	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
201305	632.292780	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
201844	633.792738	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
202382	635.292761	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
202928	636.792781	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
203455	638.292894	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
203972	639.792759	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request
204530	641.292933	192.168.1.4	192.168.1.1	ICMP	Echo (ping) request

```

0000  00 08 a3 d1 9a 81 00 10 dc 11 93 2c 08 00 45 00  .....E.
0010  00 3c 08 ff 00 00 40 01 ee 6c c0 a8 01 04 c0 a8  .<....@. .l.....
0020  01 01 08 00 41 5c 04 00 08 00 61 62 63 64 65 66  ....A\.. .abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
    
```

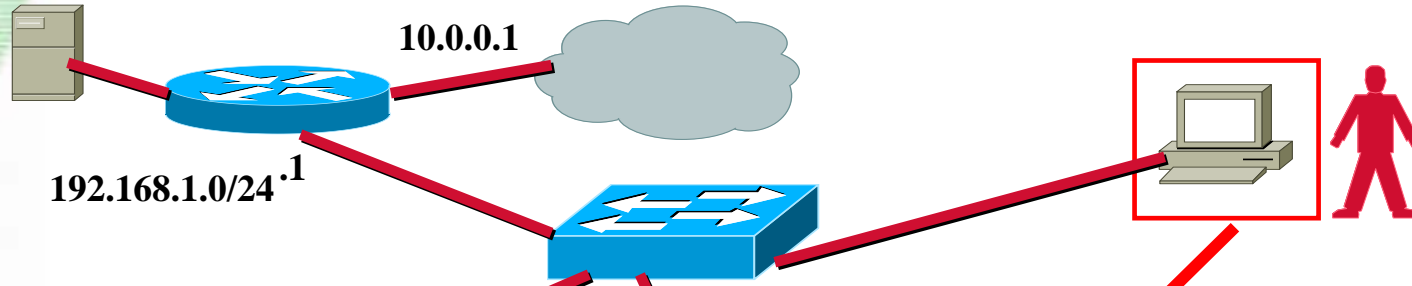
Filter: icmp [Reset] [Apply] <live capture in progress>

```

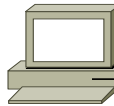
de:8c:32:32:22:d2 9d:de:eb:71:10:0 0.0.0.0.59862 > 0.0.0.0.48673: S 1203977039:1203977039(0) win 512
b8:45:d5:74:3b:1a 13:6c:9f:1d:d6:8c 0.0.0.0.4679 > 0.0.0.0.34772: S 516384785:516384785(0) win 512
d7:cf:fd:35:b9:dc 54:3b:cb:a:76:dd 0.0.0.0.51230 > 0.0.0.0.13722: S 992689145:992689145(0) win 512
af:1:e7:6d:35:36 5f:27:dd:26:1f:40 0.0.0.0.31891 > 0.0.0.0.40987: S 1679285814:1679285814(0) win 512
25:79:de:78:db:7c e2:2a:ff:6e:b6:fb 0.0.0.0.11460 > 0.0.0.0.39928: S 1384755877:1384755877(0) win 512
3:ac:66:50:4:8b 24:db:31:35:80:4b 0.0.0.0.13767 > 0.0.0.0.45200: S 1141826386:1141826386(0) win 512
    
```

Demonstration ARP-Spoofing

Topologie:



.3



```

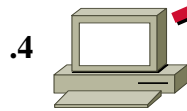
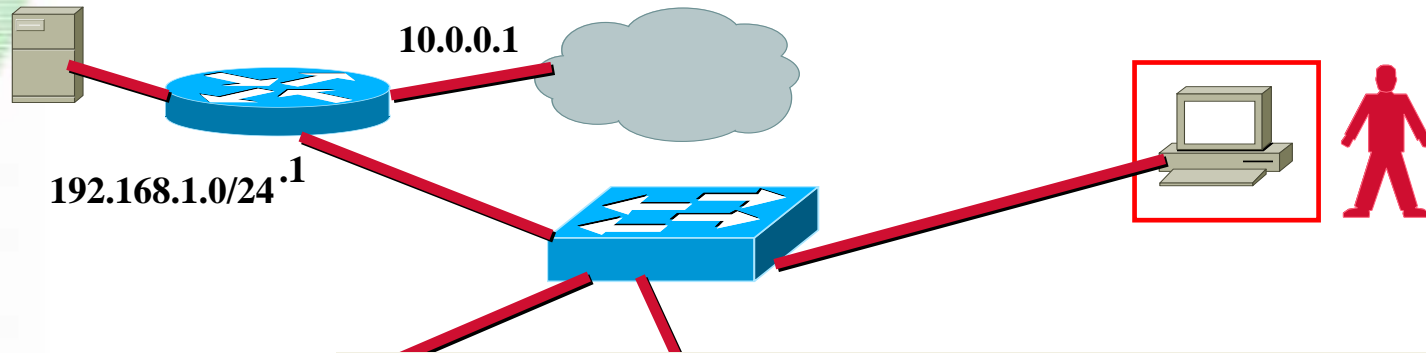
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@1[~]# ifconfig
eth0    Link encap:Ethernet  HWaddr 00:0C:29:45:23:84
        inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:49 errors:0 dropped:0 overruns:0 frame:0
        TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6130 (5.9 KiB)  TX bytes:3490 (3.4 KiB)
        Interrupt:18 Base address:0x1000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:400 (400.0 b)  TX bytes:400 (400.0 b)

root@1[~]# arp
Address          Hwtype  Hwaddress      Flags Mask      Iface
192.168.1.4     ether   00:10:DC:11:93:2C  C        eth0
192.168.1.1     ether   00:08:A3:D1:9A:81  C        eth0
root@1[~]# arpspoof -i eth0 - t 192.168.1.4 192.168.1.1
    
```

Demonstration ARP-Spoofing

Topologie:



```

C:\Eingabeaufforderung
C:\Dokumente und Einstellungen\Uwe1>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:

Antwort von 192.168.1.1: Bytes=32 Zeit=9ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=4ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=4ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=4ms TTL=255

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 4ms, Maximum = 9ms, Mittelwert = 5ms

C:\Dokumente und Einstellungen\Uwe1>arp -a

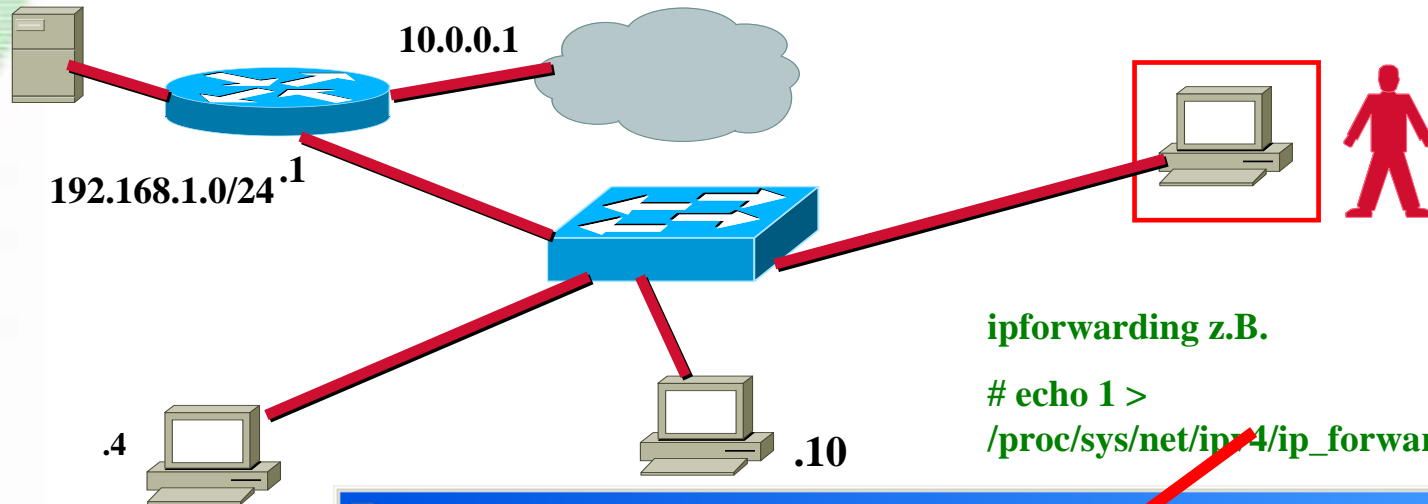
Schnittstelle: 192.168.1.3 --- 0x10006
    Internetadresse           Physikal. Adresse           Typ
    192.168.1.1                00-08-a3-d1-9a-81          dynamisch

C:\Dokumente und Einstellungen\Uwe1>
    
```

Ungespooftes Standard Gateway

Demonstration ARP-Spoofing

Topologie:



ipforwarding z.B.

echo 1 >

/proc/sys/net/ipv4/ip_forward

```

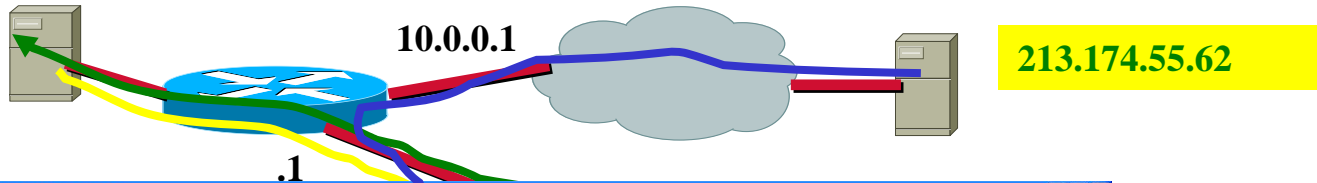
c:\ Eingabeaufforderung
C:\Dokumente und Einstellungen\Uwe1>ping 192.168.1.1 -t
Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:

Antwort von 192.168.1.1: Bytes=32 Zeit=12ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=5ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=6ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=7ms TTL=255
    
```

„Man in the Middle“ Topologie

DNS-Spoofing

DNS- Server 192.76.157.4



213.174.55.62
www.edunetwork.de

EduNetwork 05 -- 10.+11. Juni 2005

Home
Partner
Agenda
Bildungsmarkt
Organisation
Anmeldung
Impressum / Kontakt

MINT-EC
Der Verein MINT-EC ist eine Arbeitgeberinitiative unter deren Dach sich derzeit 83 überdurchschnittlich engagierte und zertifizierte Schulen mit Sek. II vereinen. Diese MINT-Excellence-Center sind in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik herausragend und werden durch das MINT-EC-Netzwerk vielfältig gefördert.

Porta Quadra
Porta Quadra, Ausrichter von EduNetwork 05 vor Ort, ist ein kleines Netzwerk - eigentlich eines in der Art unseres Weltalls ganz kurz nach dem "Big Bang" so interpretieren wir, alle an Porta Quadra und Schulporte Interessierten, es jedenfalls voller Hoffnung.

Science on Stage

213.174.55.62

„Man in the Middle“ DNS-Spoofing

Web- Seitenumleitung/Modifizierung

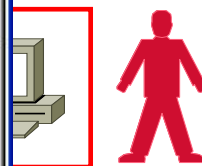
DNS- Server 192.76.157.4

The screenshot shows a VMware Workstation window titled "Auditor - VMware Workstation". Inside, there is a Linux virtual machine named "Auditor". A terminal window titled "Shell - Konsole <2>" is open, showing the following commands and output:

```

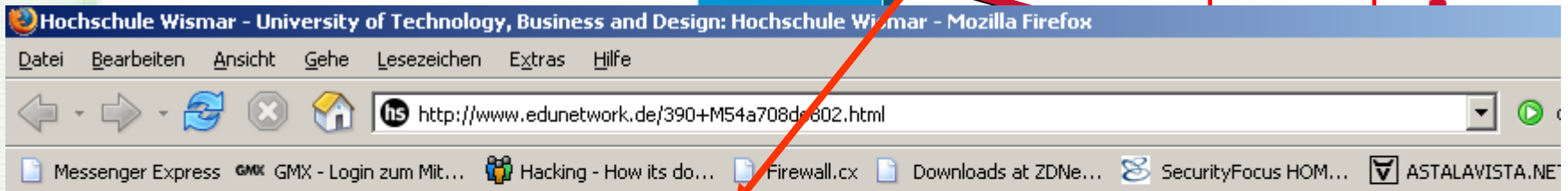
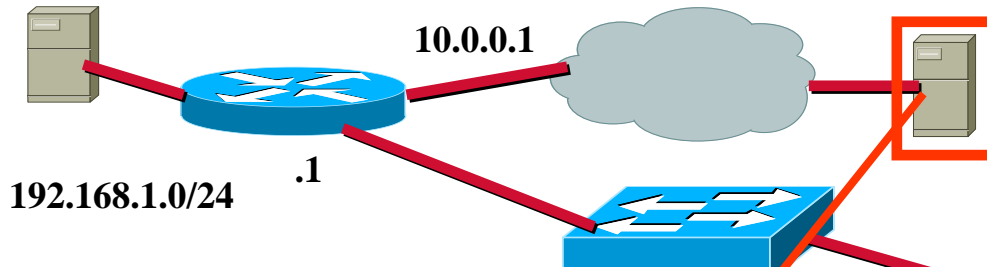
root@2[~]# dnsspoof -f /edunetwork
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.5]
192.168.1.4.1492 > 192.76.157.4.53: 57644+ A? www.edunetwork.de
192.168.1.4.1492 > 192.76.157.4.53: 57644+ A? www.edunetwork.de
192.168.1.4.1500 > 192.76.157.4.53: 40482+ A? www.edunetwork.de
192.168.1.4.1500 > 192.76.157.4.53: 40482+ A? www.edunetwork.de
root@2[~]# dnsspoof -f /edunetwork
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.5]
192.168.1.4.1532 > 192.76.157.4.53: 35878+ A? www.edunetwork.de
192.168.1.4.1532 > 192.76.157.4.53: 35878+ A? www.edunetwork.de
    
```

Other windows visible include "edunetwork - KWrite" with the address bar showing "192.76.157.26 www.edunetwork.de".



„Man in the Middle“ DNS-Spoofing

DNS- Server 192.76.157.4



Ganz oben.



Hochschule Wismar

University of Technology, Business and Design

Rheinlandarchitekt zu Gast und Seifenkistenrennen

Detailinformationen zum traditionellen Seifenkistenrennen können den Aushängen in Haus 7 entnommen werden.
Zum letztem Vortrag im Rahmen der [WismarerArchitekturGespräche](#) in diesem Semester lädt Prof. Frank Werner.

[mehr]

10.06.2005 BIS 11.06.2005

Die Studiengänge

- Design
- Innenarchitektur
- Kommunikationsdesign und Medien
- Architectural Lighting Design, Master
- Architektur, Bachelor
- Architektur, Master
- Bauingenieurwesen, Bachelor
- Bauingenieurwesen, Master
- Pflege des Bauerbes, Master
- Betriebswirtschaft
- Binationaler deutsch-polnischer Bachelorstudiengang
- Wirtschaftsinformatik
- Binationaler deutsch-polnischer Masterstudiengang Wirtschaftsinformatik

Home • Sitemap • Kontakt

- Hochschule
- Studium
- Organisation
- Forschung
- Service
- Partner & Freunde
- Finden

VIST



Zusammenfassung und Verbesserung der Netzsicherheit

**Geswitchte LAN's für mehr Effizienz und Bandbreite aber
nicht für mehr Sicherheit !**

Mitlesen „Sniffen“ schwieriger -> aber möglich

**verschiedene andere Attacken möglich (MAC, ARP, VLAN, STP ..)
nicht alle Linux-basierend**

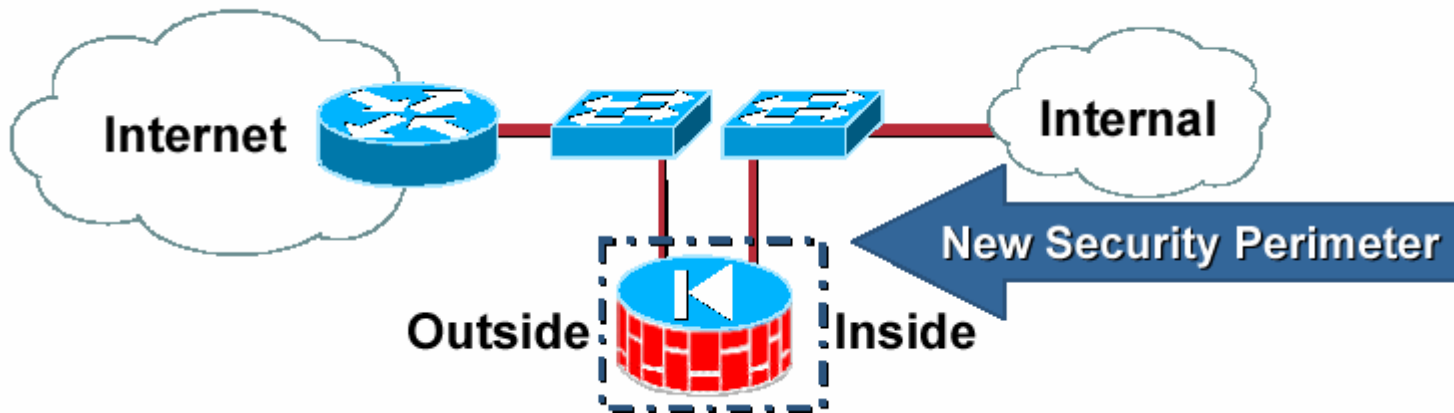
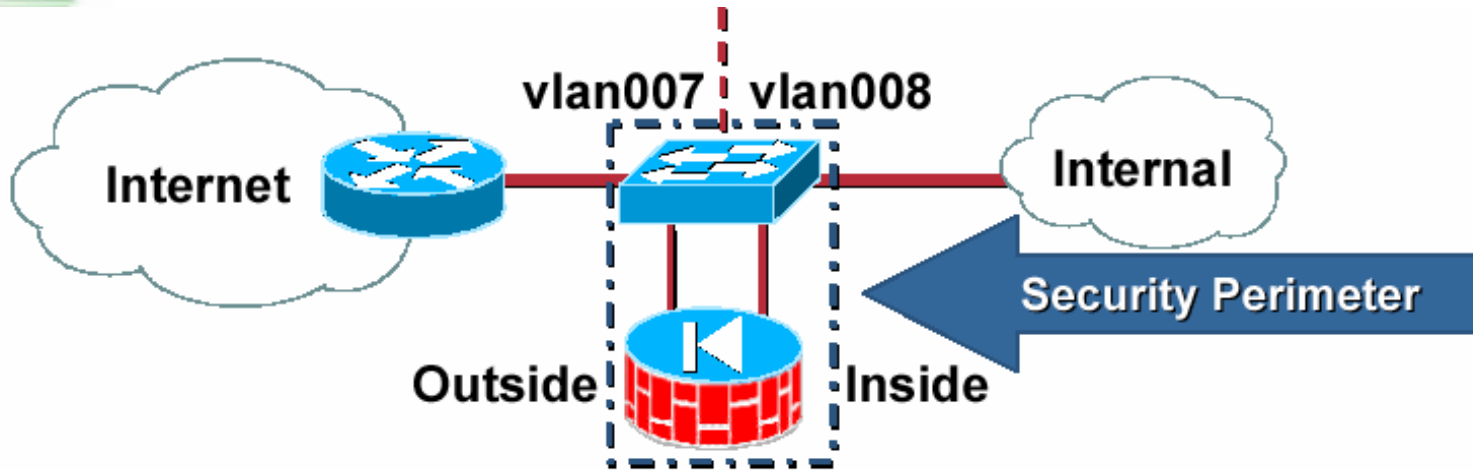
**Portsecurity- Mechanismen abhängig vom Hersteller
verwendbar und praktikabel in Abhängigkeit der LAN- Größe**

Ausschalten ungenutzter Ports bzw. von Default- Einstellungen

**Überwachung des ARP- Caches / Traffic -> PC, Netzwerk ->
ARPWatch, IDS, MAC- Firewall's**

Zusammenfassung und Verbesserung der Netzsicherheit

Physische Topologie Verbesserungen:



Quellen und Links:

<http://www.cisco.com/go/save>

Curricula CNAP *Cisco*

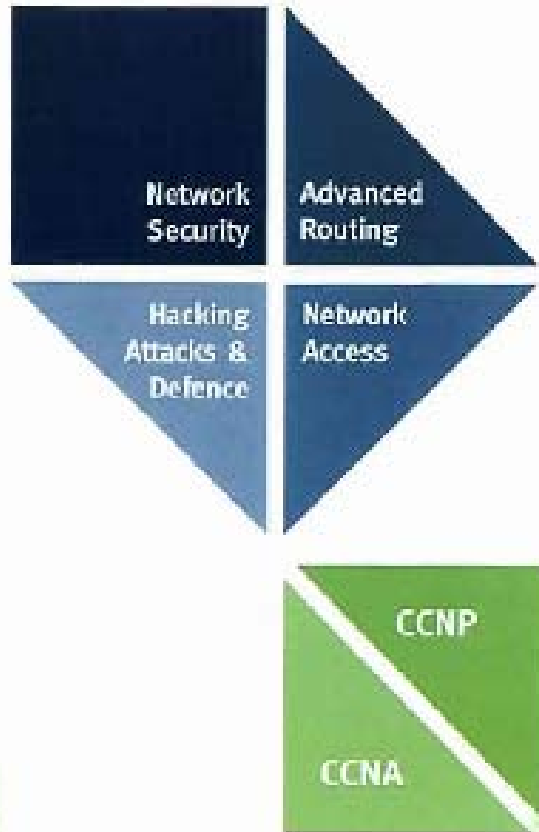
„Fun with Ethernet Switches“ *Sean Convery*

dsniff <http://www.monkey.org>

„Hacker Attack and Defence - Kurs“

Hochschule Wismar

Kursangebote der Netzwerkakademie an der Hochschule Wismar



Anmeldung und Informationen:

Hochschule Wismar, University of
Technology, Business and Design
Network Academy

Philipp-Mueller-Strasse

Postfach 1210

D-23952 Wismar

Phone: +49 3841 75 33 75

Fax: +49 3841 753130

www.networking-academy.de

networking-academy@hs-wismar.de

u.starke@et.hs-wismar.de

Kurse: Fundamentals of Network Security

(Instructorausbildung)

Termine

Gesamtzeit	online	Präsent vor Ort
04.10. – 28.10.05	04.10. – 07.10.05 17.10. – 21.10.05	10.10. - 14.10.05 24.10. - 28.10.05
21.11. – 16.12.05	21.11. - 02.12.05	05.12. – 16.12.05

Universität Rostock

Institut für Nachrichtentechnik und Informationselektronik

ComLab – Labor für Kommunikationssysteme

Richard-Wagner-Str. 31

18119 Rostock (Warnemünde)

www.network-security-lab.de



Danke für die Aufmerksamkeit!

Fragen ?