Juventus Technikerschule HF

Hacking Exposed

HE2: LAN-Security

Pascal Knecht

Video 0: Überblick

Die 3 allgemeinen IT-Schutzziele

- Vertraulichkeit / Confidentiality
- Integrität / Integrity
- Verfügbarkeit / Availability

Wichtiger Hinweis

- Dies ist eine Lehrveranstaltung.
- Die im Rahmen der Hacking-Exposed-Vorlesung vermittelten Kenntnisse sollen dazu beitragen, dass Sie Informationssicherheitsaspekte beachten und in Ihren Projekten berücksichtigen.
- Die HE-Vorlesung ist keineswegs als Anstiftung zum Hacken zu verstehen.

Inhalt heute Abend

- Network Scanning
- Machine-In-The-Middle Attacke
- ARP-Spoofing
- DNS-Spoofing
- Abwehrmassnahmen

Ziele

- Sie kennen die drei IT-Schutzziele und können Angriffe korrekt zuordnen.
- Sie kennen Techniken zur Netzwerk Scanning und Host Discovery
- Sie wissen was eine MITM-Attacke ist und können deren Eigenschaften beschreiben und diese im LAN durchführen.
- Sie kennen ARP- und DNS-Spoofing

#01 Network Scanning

Video 1: Network Scanning

Host Discovery

- Ein Port-Scan ist teuer und aufwendig und unnötig, wenn ein Zielsystem gar nicht online ist.
- Host Discovery erfüllt die Aufgabe, herauszufinden ob ein Zielsystem überhaupt erreichbar ist.
  - Findet vor dem Port-Scan statt.

Nmap Default Host Discovery – vor Port Scan

- Nmap führt standardmässig ein Host Discovery durch um Anzahl zu scannender Host auf interessante zu reduzieren:

  1) ICMP Echo Request (Ping)

  2) TCP SYN Paket auf Port 443

  3) TCP ACK Paket auf Port 80

  4) ICMP Timestamp Request

- Weitere Techniken und Informationen in der Manual Page:
  - `man nmap`

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
```

Host Discovery im LAN

- Schnell alle Geräte die Online sind im eigenen Netzwerk finden:
  - `$ sudo nmap -sn 192.168.1.0/24`
  - Ping Scan ohne Port Scan
  - Im lokalen Netzwerk wird ein ARP scan verwendet!

```
pascal@0x470:~$ nmap -sn 192.168.105.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-23 21:25 CEST
Nmap scan report for _gateway (192.168.105.1)
Host is up (0.0034s latency).
Nmap scan report for pihole (192.168.105.53)
Host is up (0.0084s latency).
Nmap scan report for 192.168.105.114
Host is up (0.11s latency).
Nmap scan report for 0x470.home (192.168.105.118)
Host is up (0.00013s latency).
Nmap scan report for sonos_wohnzimmer.home (192.168.105.150)
Host is up (0.0037s latency).
Nmap scan report for sonos_buero.home (192.168.105.151)
Host is up (0.059s latency).
Nmap scan report for sonos_bad.home (192.168.105.152)
Host is up (0.057s latency).
Nmap scan report for sonos_kueche.home (192.168.105.153)
Host is up (0.061s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 4.78 seconds
```

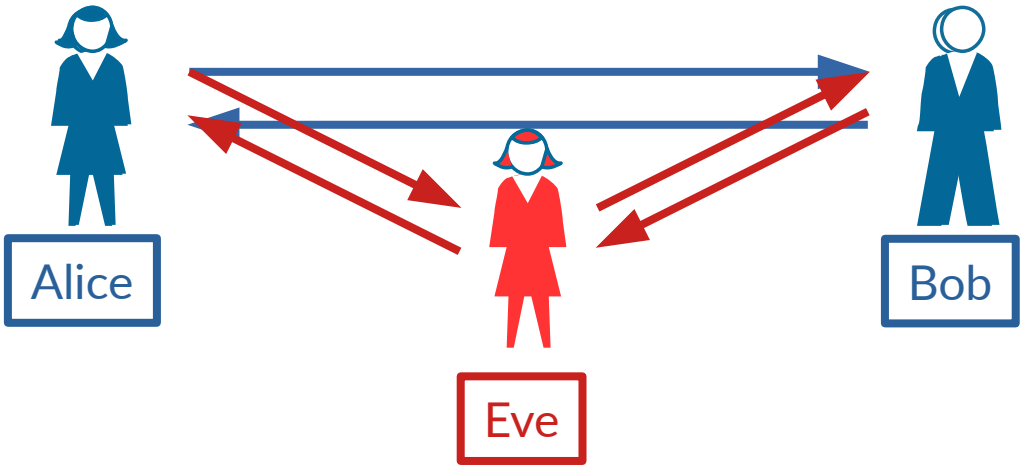
#02 MITM-Attacke

Machine-in-the-Middle

Video 2: MITM-Attacke

MITM

- Jede Form von Angriff, in der Netzwerkverkehr zwischen Alice und Bob von Eve mitgelesen und/oder verändert werden kann.



Alice, Bob, Eve und Mallory

- Alice und Bob sind zwei Personen die miteinander kommunizieren.
- Eve ist eine dritte Person, welche die Kommunikation zwischen Alice und Bob passiv belauscht. (engl. eavesdropper)
- Mallory ist wie Eve, verändert aber aktiv die Kommunikation. (engl. malicious)

https://de.wikipedia.org/wiki/Alice_und_Bob

#03 ARP-Spoofing

Video 3: ARP-Spoofing

Recap: MAC-Adresse

- Rechneradressierung auf Sicherungsschicht (OSI Layer 2)
- Besteht aus 6 Oktetts à 8 Bit (48 Bit)
  - Organisationally Unique Identifier (OUI) Byte 0 bis 2
    - https://www.wireshark.org/tools/oui-lookup.html
  - Network Interface Controller (NIC) Byte 3 bis 5

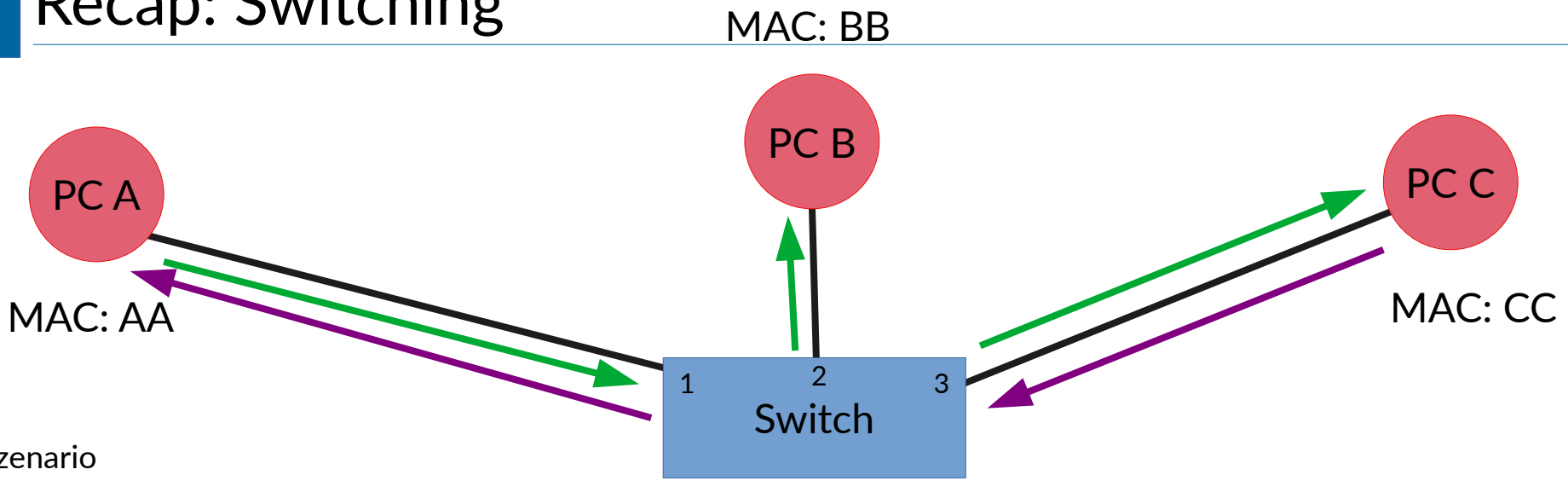
Recap: Kommunikation im LAN

- Client IP
  - `192.168.42.23/24`
- Subnetz
  - `255.255.255.0`
- Server IP
  - `192.168.42.45`
- Sind erste 24 Bit identisch?

- Client IP
  - `11000000.10101000.00101010.00010111`
- Subnetz
  - `11111111.11111111.11111111.00000000`
- Server IP
  - `11000000.10101000.00101010.00101101`

IP Routing Explained:
https://www.youtube.com/watch?v=8qtKpZGoNdI (11 min.)

Recap: Switching



Szenario
Alle PCs neu an Switch gehängt und diesen neu gestartet

1) PC A sendet PC C eine Nachricht:
MAC Src: AA | MAC Dst: CC

2) Switch weiss nicht wo MAC Dst: CC ist und schickt Message an alle Ports

3) PC B prüft MAC Dst der Message mit eigener MAC und verwirft

4) PC C prüft MAC Dst der Message mit eigener MAC und antwortet
MAC Src: CC | MAC Dst: AA

5) Switch prüft Tabelle, findet MAC Dst auf Port 1 und stellt Message an PC A zu

Port	MAC
1	AA
3	CC

https://www.youtube.com/watch?v=chlBlRfsnq0 (8 Min.)

Woher weiss PC A die MAC-Adresse von PC B?

- Über eine flüchtige Tabelle die IP-Adressen auf MAC-Adressen mappt.
- Das ARP-Protokoll löst IP-Adressen nach MAC-Adressen auf
- Damit diese Namensauflösung nicht immer neu gemacht werden muss, werden die Ergebnisse in der ARP-Tabelle des PCs gecached

Beispiel 1 ARP via Ping im lokalen Netz

```
pascal@0x470:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.105.1            ether   d8:58:d7:00:8f:ca   C                     wlp4s0
192.168.105.53           ether   f2:c2:f4:12:ef:d8   C                     wlp4s0
```

```
pascal@0x470:~$ ping 192.168.105.151 -c 1
PING 192.168.105.151 (192.168.105.151) 56(84) bytes of data.
64 bytes from 192.168.105.151: icmp_seq=1 ttl=64 time=5.39 ms

--- 192.168.105.151 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 5.391/5.391/5.391/0.000 ms
```

```
pascal@0x470:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.105.1            ether   d8:58:d7:00:8f:ca   C                     wlp4s0
192.168.105.53           ether   f2:c2:f4:12:ef:d8   C                     wlp4s0
192.168.105.151          ether   48:a6:b8:12:22:50   C                     wlp4s0
```

Beispiel 2 ARP via Ping ins Internet

```
pascal@0x470:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.105.1            ether   d8:58:d7:00:8f:ca   C                     wlp4s0
192.168.105.53           ether   f2:c2:f4:12:ef:d8   C                     wlp4s0
192.168.105.151          ether   48:a6:b8:12:22:50   C                     wlp4s0
```

```
pascal@0x470:~$ ping 8.8.8.8 -c 1
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=2.47 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.466/2.466/2.466/0.000 ms
```

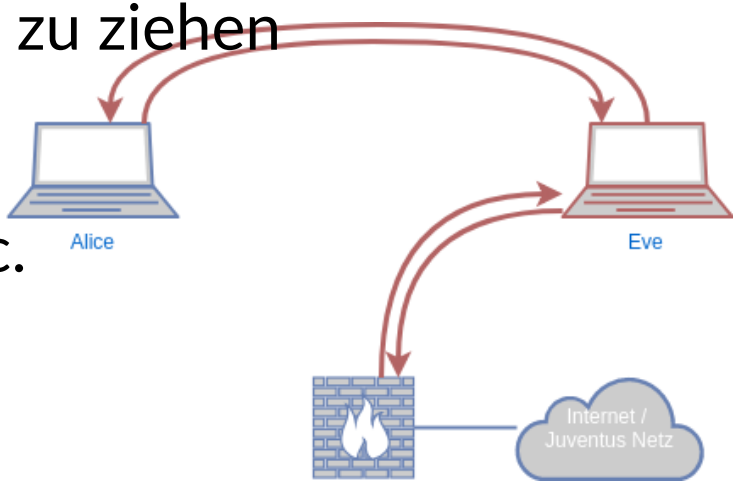
```
pascal@0x470:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.105.1            ether   d8:58:d7:00:8f:ca   C                     wlp4s0
192.168.105.53           ether   f2:c2:f4:12:ef:d8   C                     wlp4s0
192.168.105.151          ether   48:a6:b8:12:22:50   C                     wlp4s0
```

ARP Protokoll – im eigenen Subnetz

- ARP ist ein Broadcasting Namenssystem
  - Self-Managed: kein Master-Node notwendig
  - Einfach zu implementieren
  - Lokationsunabhängig
  - Skaliert nicht: Kommunikation wächst mit der Anzahl Teilnehmer
  - Einfach auszunutzen
- Broadcast Nachricht: «Was ist die MAC-Adresse zu der IP-Adresse x? Antwort bitte an y»

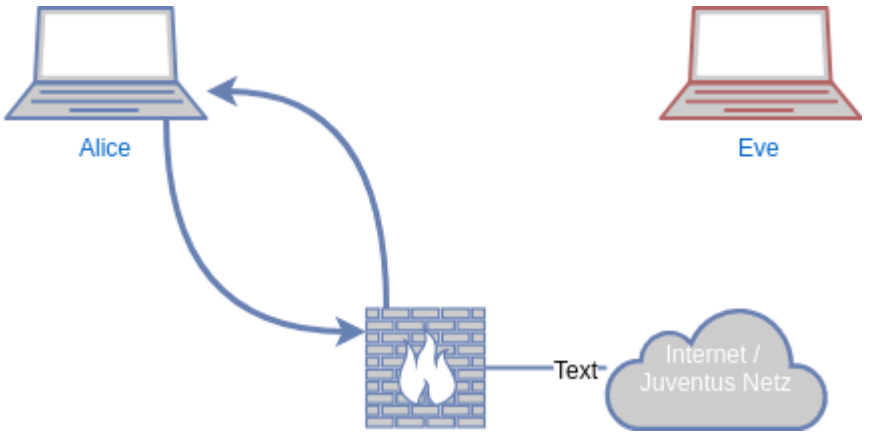
ARP Spoofing

- MITM durch Vergiften von ARP Einträgen bei zwei oder mehreren Rechnersystemen
- Auch ARP-Poisoning genannt
- Ziel ist sämtlichen Datenverkehr an sich zu ziehen
- Einsatzort: LAN
  - Café, Bibliothek, Schule, Zuhause etc.



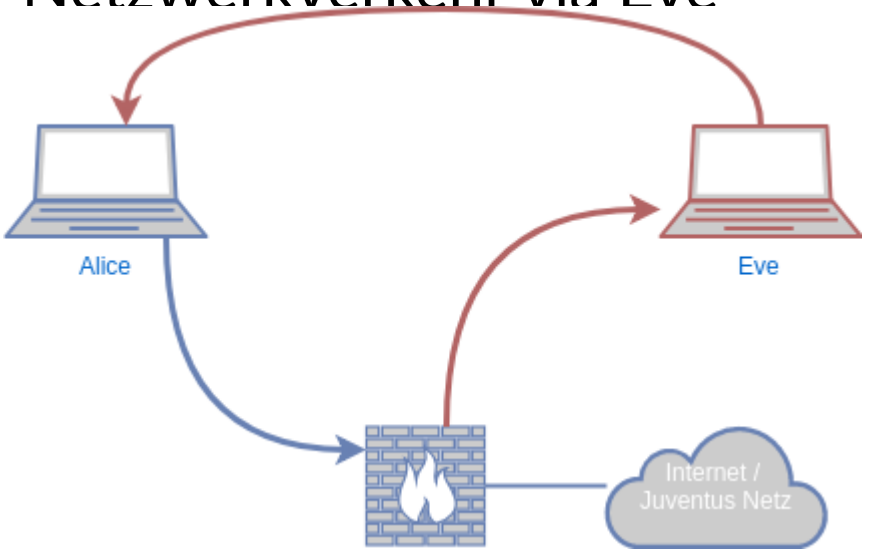
ARP Poisoning

- Angreifer sendet gefälschte ARP-Pakete an Alice und Bob und leitet so den Netzwerkverkehr über sich



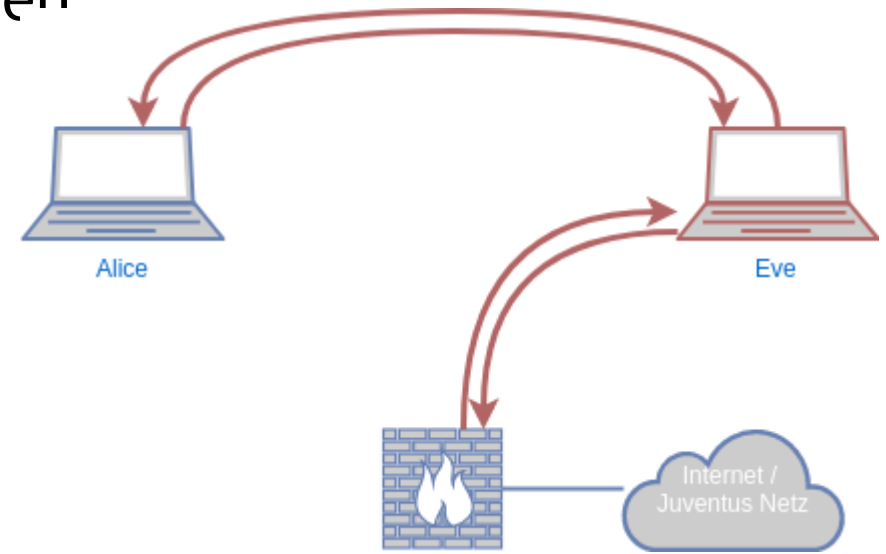
ARP Poisoning Phase 1

- Eve teilt dem Gateway per ARP-Reply die eigene MAC-Adresse für die IP von Alice mit
  - Asynchroner Netzwerkverkehr via Eve



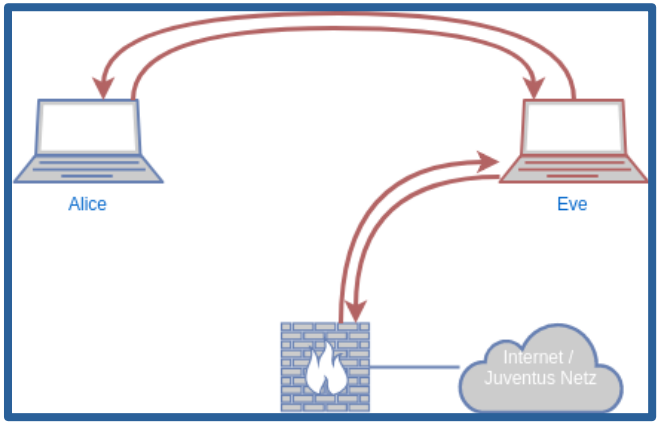
ARP Poisoning Phase 2

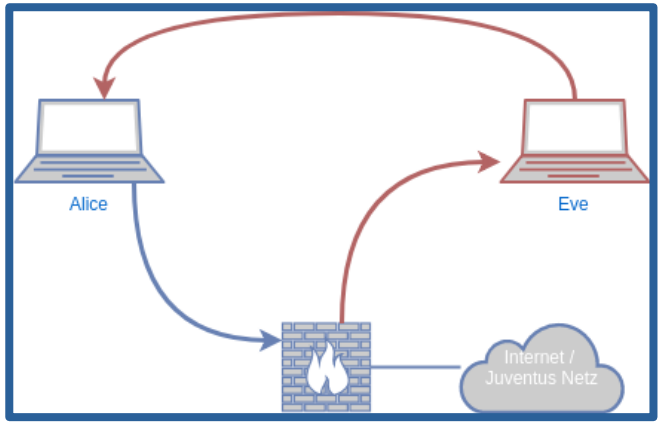
- Eve teilt Alice per ARP-Replay die eigene MAC-Adresse für die IP vom Default-Gateway mit.
  - Synchroner Netzwerkverkehr über Eve → MITM abgeschlossen

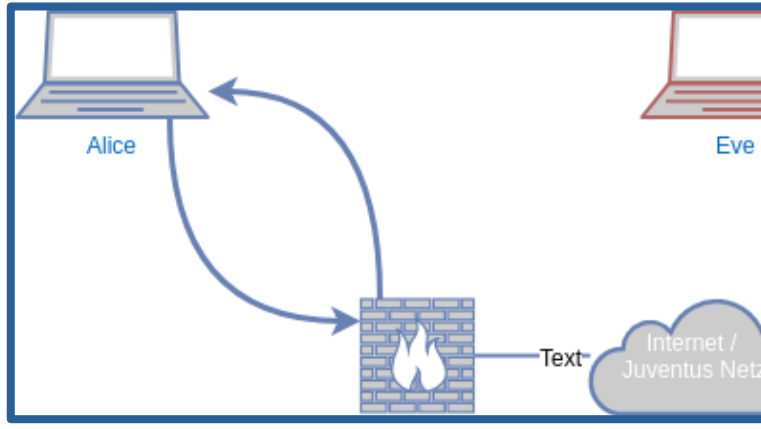


ARP Detoxing

- Um möglichst unbemerkt zu bleiben, die ursprüngliche ARP Tabelle wiederherstellen.







ARP Spoofing erkennen

- Manuell lässt sich ARP Spoofing anhand der ARP-Tabelle erkennen.
  - `$ arp -n`

```
Address                  HWtype  HWaddress           Flags Mask            Iface
35.222.85.5                      (incomplete)                              enp0s31f6
192.168.1.100            ether   88:1f:a1:40:c8:18   C                     wlp4s0
192.168.1.1              ether   08:00:27:1c:ef:3e   C                     wlp4s0
192.168.1.116            ether   08:00:27:1c:ef:3e   C                     wlp4s0
35.224.99.156                    (incomplete)                              enp0s31f6
```

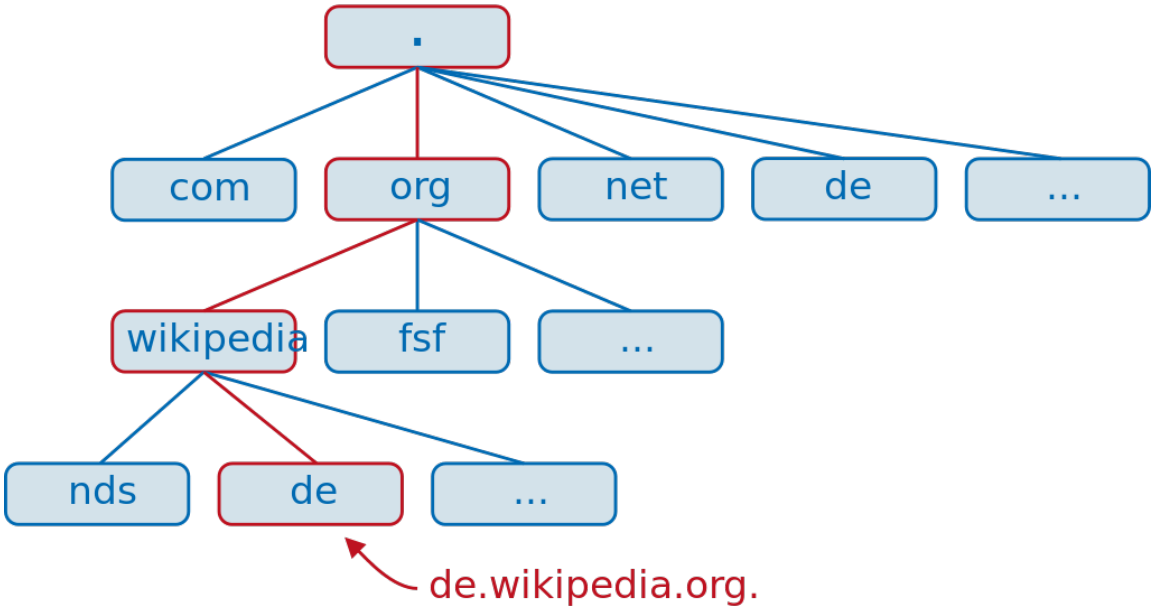
#04 DNS Spoofing

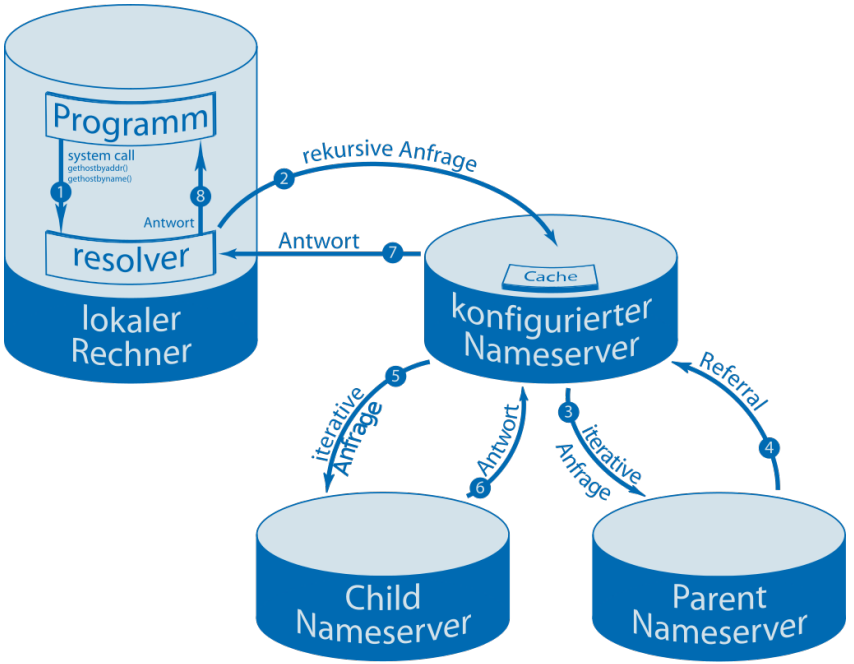
Weitere Attacken im LAN

Video 4: DNS-Spoofing

Namensauflösung im Internet

- DNS hierarchische Namensauflösung





DNS Protokoll

- UDP basiertes Protokoll
  - Kein Verbindungsaufbau → anfällig für Spoofing-Attacken
- Client erhält via DHCP die IP-Adresse des lokalen DNS-Resolvers
- Sobald ein Domainname in eine IP übersetzt werden muss, wird eine Anfrage an den Resolver geschickt

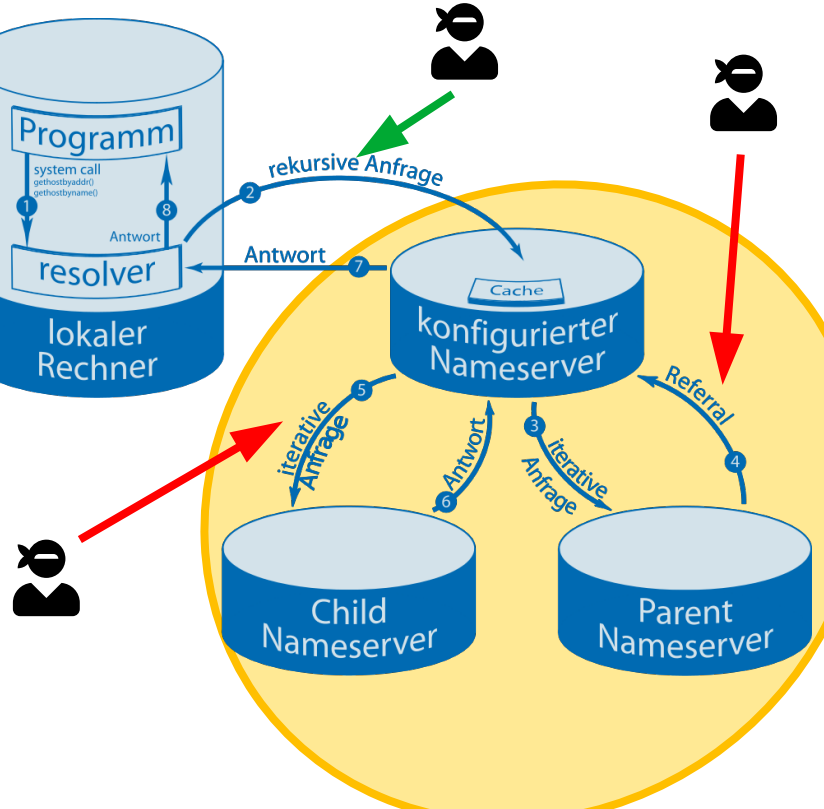
Source	Destination	Protocol	Info
192.168.100.100	8.8.8.8	DNS	Standard query 0x18b2 A www.heise.de OPT
8.8.8.8	192.168.100.100	DNS	Standard query response 0x18b2 A www.heise.de A 193.99.144.85 OPT

DNS Spoofing

- IP-Adresse im DNS-Response wird gefälscht
- Voraussetzung: DNS-Anfragen kommen bei Angreifer vorbei (MITM)
  - ARP-Spoofing
  - DHCP-Spoofing

DNSSEC

- Ist DNSSEC eine Schutzmassnahme gegen DNS-Spoofing-Attacken?
- DNSSEC ist eine wichtige Technologie zur Absicherung von Web- und Internetservices



DNSSEC in der Schweiz
https://www.youtube.com/watch?v=_rSWTQ9LGCE

#05 Abwehrmassnamen

Video 5: Abwehrmassnamen

Juventus
Technikerschule HF

Abwehrmassnamen im LAN

- Einfachste Massnahme ist, den Datenverkehr zu verschlüsseln
- Thema der nächsten Vorlesung!
  - Transportverschlüsselung
    - TLS, VPN, SSH, Tor, moderne Messenger wie Threema, Signal
  - Ende-zu-Ende-Verschlüsselung
    - Passwort-ZIP, S/MIME und PGP, moderne Messenger wie Threema, Signal

Übungen & Labor

Übungen: HE2

Labor: github.com/ryru/HackingExposed

Videoempfehlungen fürs Selbststudium

- Du kannst alles hacken – du darfst dich nur nicht erwischen lass en.
  (57 Min)

CC BY-SA 4.0