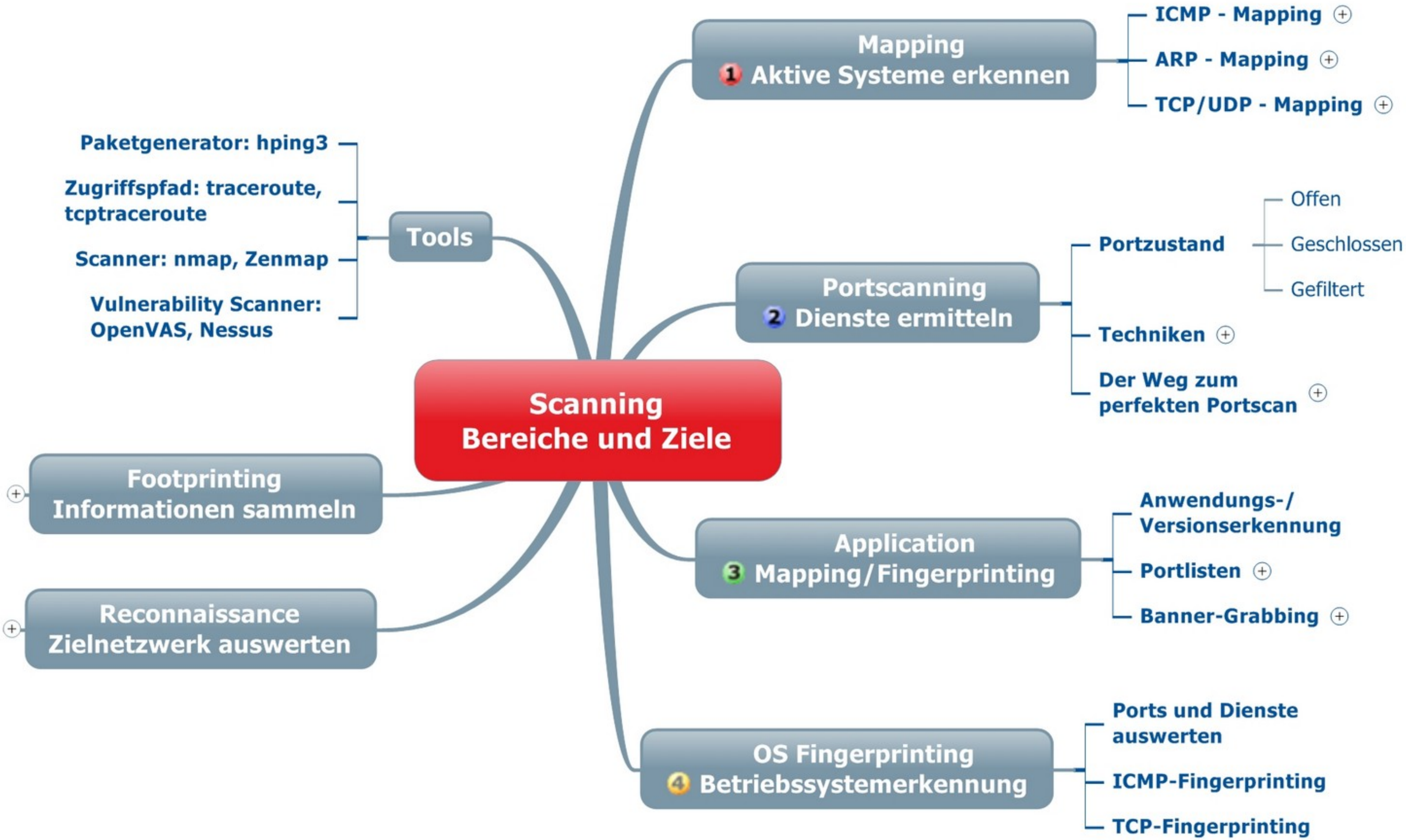
ZE(NMAP)

Network-/Hostscanning

gds2
Gottlieb-Daimler-Schule 2
Technisches Schulzentrum Sindelfingen
mit Abteilung Akademie für Datenverarbeitung



Scanning Bereiche und Ziele

- Mapping
  1 Aktive Systeme erkennen
  - ICMP - Mapping ⊕
  - ARP - Mapping ⊕
  - TCP/UDP - Mapping ⊕
- Portscanning
  2 Dienste ermitteln
  - Portzustand
    - Offen
    - Geschlossen
    - Gefiltert
  - Techniken ⊕
  - Der Weg zum perfekten Portscan ⊕
- Application
  3 Mapping/Fingerprinting
  - Anwendungs-/ Versionserkennung
  - Portlisten ⊕
  - Banner-Grabbing ⊕
- OS Fingerprinting
  4 Betriebssystemerkennung
  - Ports und Dienste auswerten
  - ICMP-Fingerprinting
  - TCP-Fingerprinting
- Tools
  - Paketgenerator: hping3
  - Zugriffspfad: traceroute, tcptraceroute
  - Scanner: nmap, Zenmap
  - Vulnerability Scanner: OpenVAS, Nessus
- ⊕ Footprinting Informationen sammeln
- ⊕ Reconnaissance Zielnetzwerk auswerten

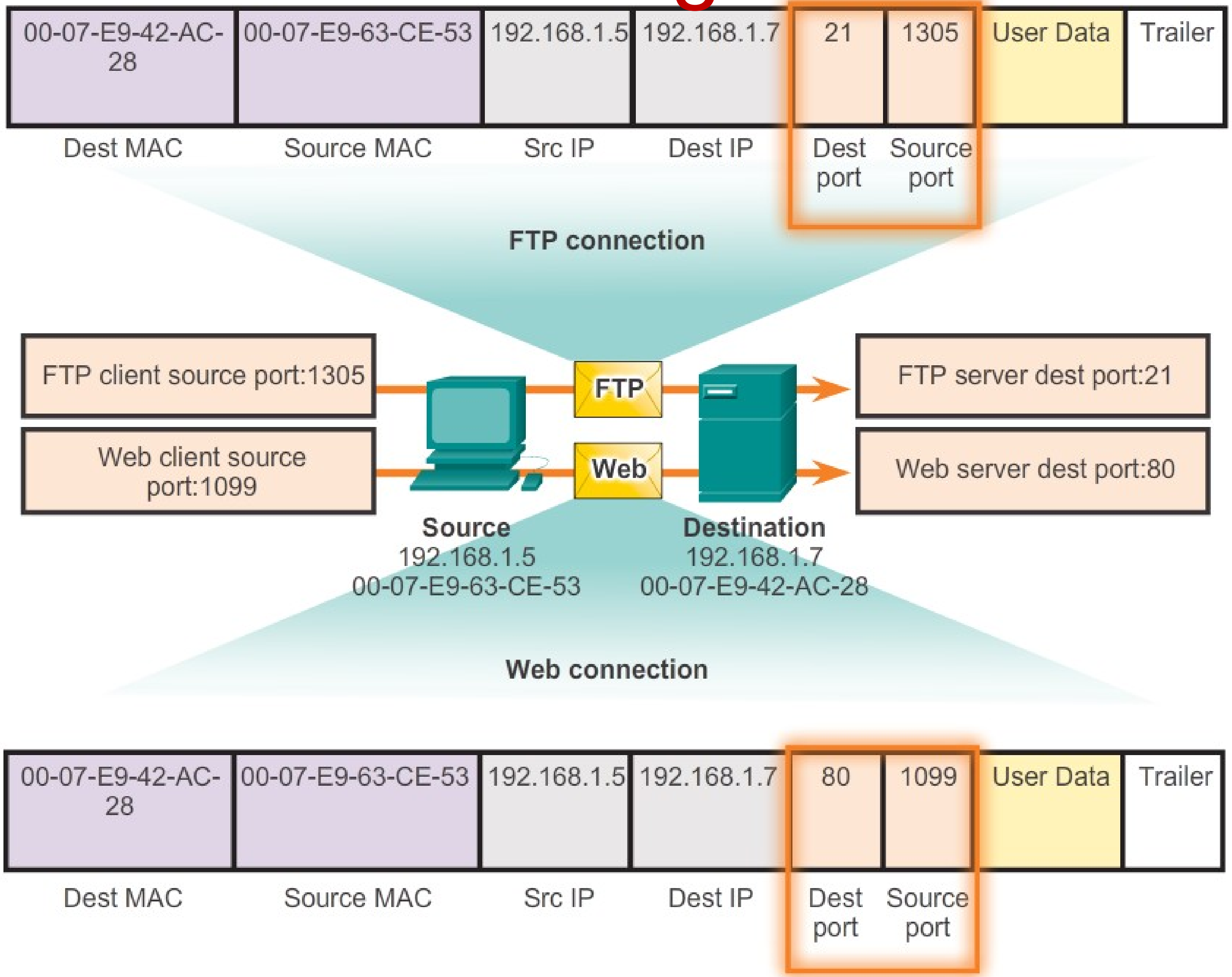
Basics !?

- Netzwerkprotokolle
  - ARP Address Resolution Protocol
  - IP Internet Protocol
  - TCP/UDP Transmission Control Protocol / User Datagram Protocol
  - ICMP Internet Control Message Protocol

- TCP-Verbindungsauf-/abbau: SYN, ACK, FIN

- Portnummern – Zuordnung Dienste/Anwendungen

Netzwerkverbindungen



00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.5	192.168.1.7	21	1305	User Data	Trailer
Dest MAC	Source MAC	Src IP	Dest IP	Dest port	Source port		

FTP connection

FTP client source port:1305

Web client source port:1099

FTP server dest port:21

Web server dest port:80

Source
192.168.1.5
00-07-E9-63-CE-53

Destination
192.168.1.7
00-07-E9-42-AC-28

Web connection

00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.5	192.168.1.7	80	1099	User Data	Trailer
Dest MAC	Source MAC	Src IP	Dest IP	Dest port	Source port		

Scans zur Informationsgewinnung

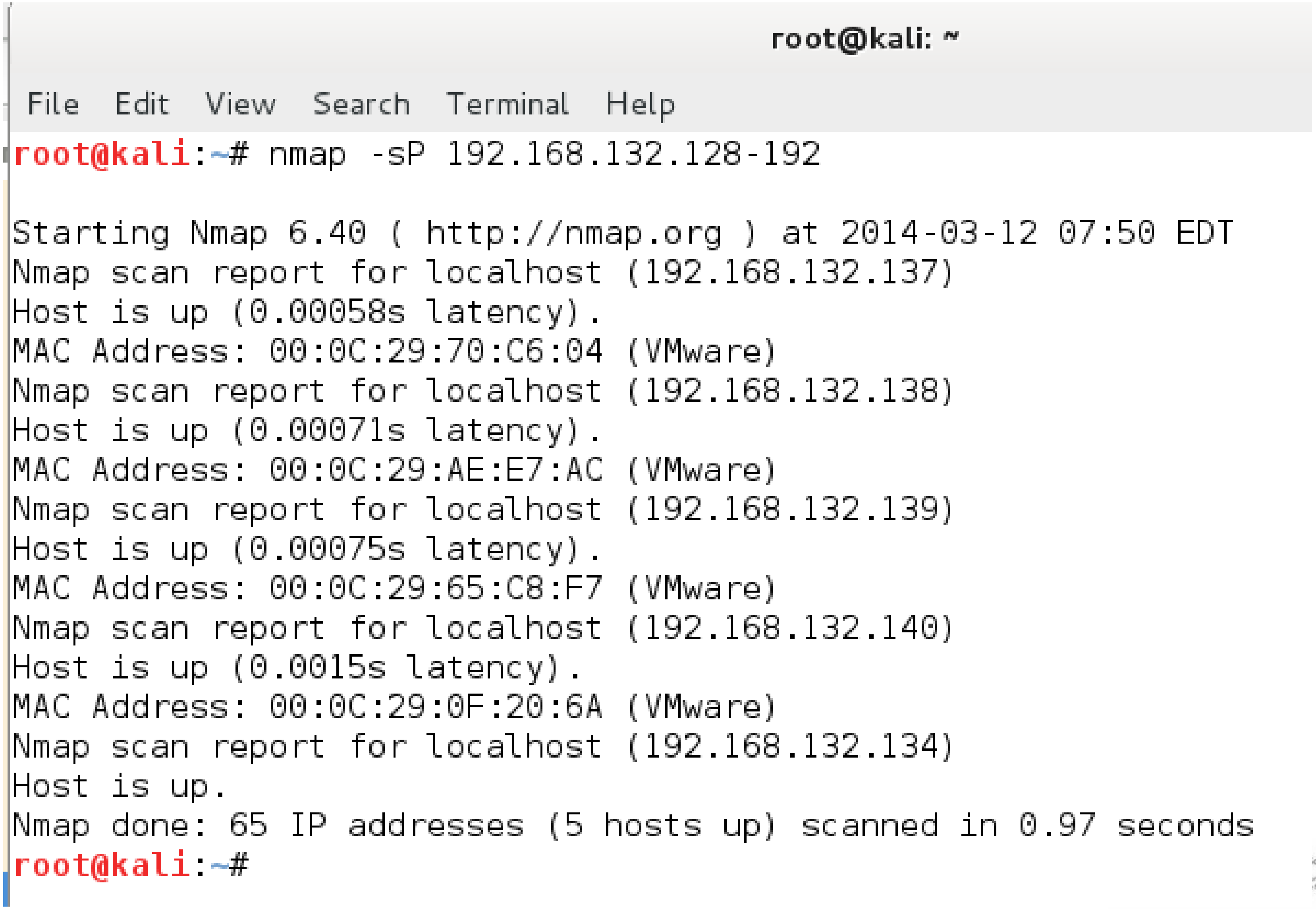
- Aktive Hosts erkennen `nmap –sP <IP>`
- Basic Portscan `nmap <IP>`
- UDP-Ports scannen `nmap –sU <IP>`
- Versionserkennung `nmap –sV <IP>`
- Betriebssystemerkennung `nmap –O <IP>`

Zielangabe:

- Einzelne IP `192.168.1.1`
- Bereich `192.168.1.1-10`
- Netz `192.168.1.0/24`

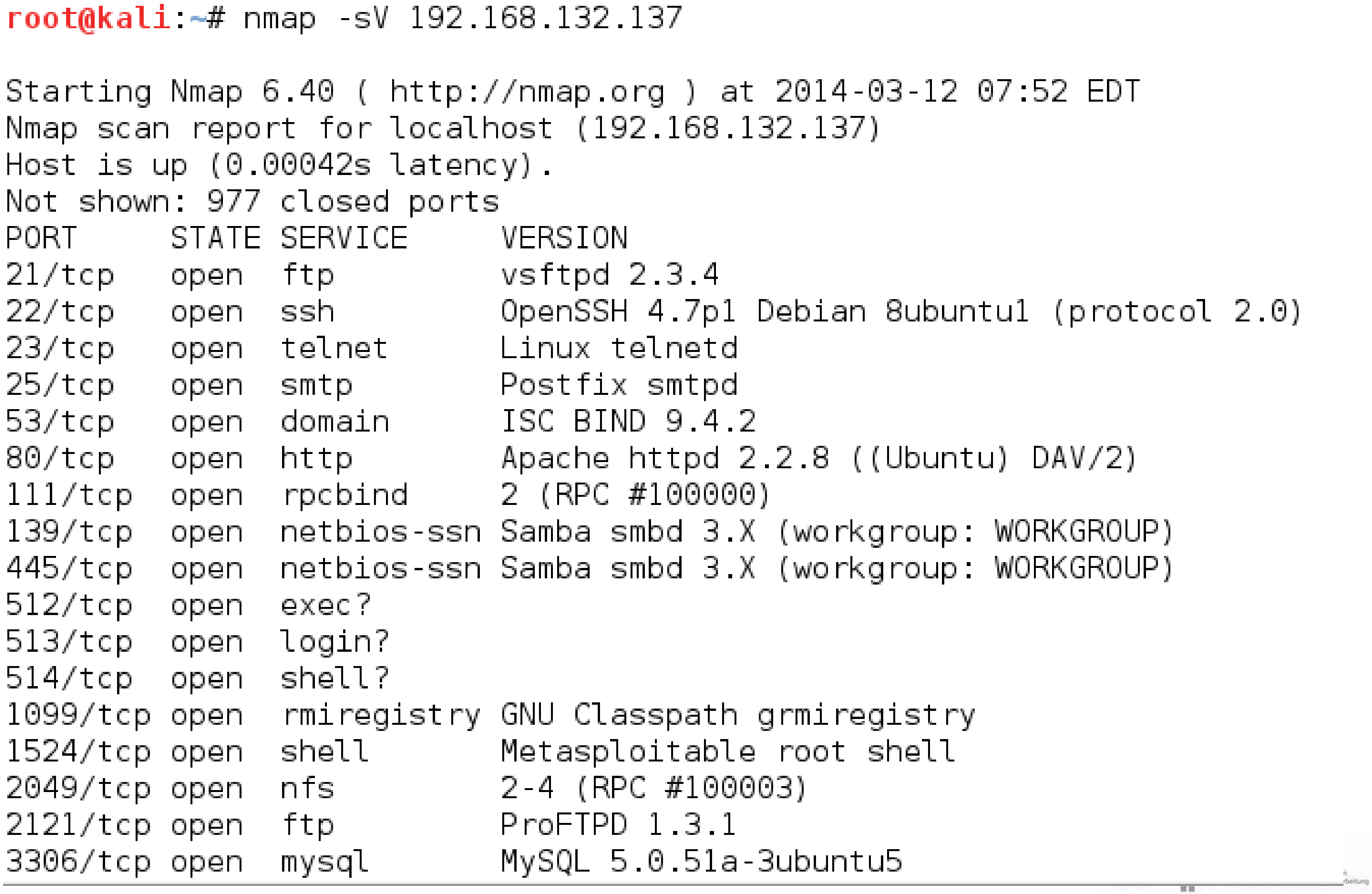
NMAP berherscht eine Fülle an weiteren Optionen für verschiedene Scantechniken.
Referenzhandbuch : Projektseite http://nmap.org/man/de/

Aktive Hosts erkennen



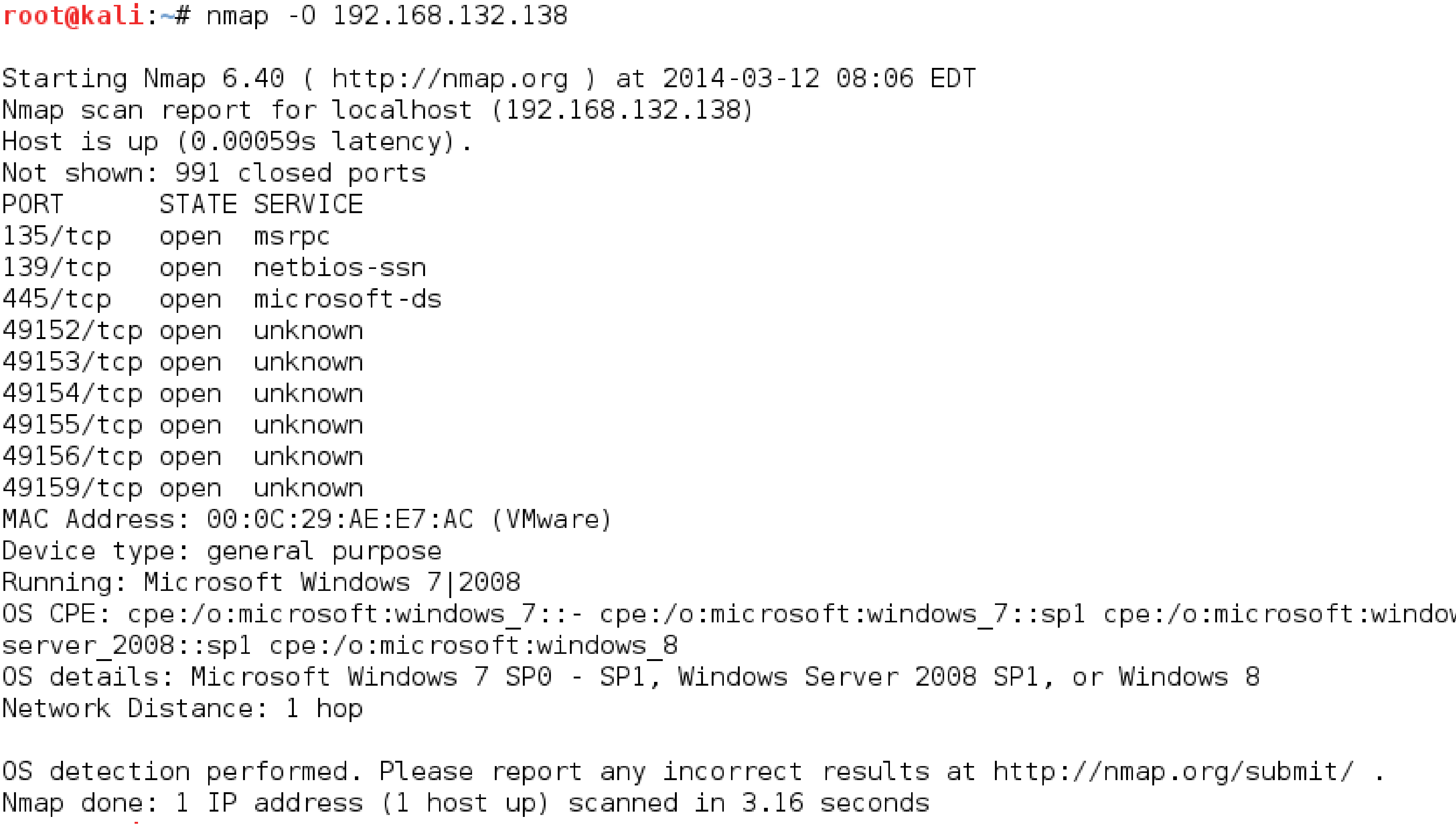
```
root@kali:~# nmap -sP 192.168.132.128-192

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-12 07:50 EDT
Nmap scan report for localhost (192.168.132.137)
Host is up (0.00058s latency).
MAC Address: 00:0C:29:70:C6:04 (VMware)
Nmap scan report for localhost (192.168.132.138)
Host is up (0.00071s latency).
MAC Address: 00:0C:29:AE:E7:AC (VMware)
Nmap scan report for localhost (192.168.132.139)
Host is up (0.00075s latency).
MAC Address: 00:0C:29:65:C8:F7 (VMware)
Nmap scan report for localhost (192.168.132.140)
Host is up (0.0015s latency).
MAC Address: 00:0C:29:0F:20:6A (VMware)
Nmap scan report for localhost (192.168.132.134)
Host is up.
Nmap done: 65 IP addresses (5 hosts up) scanned in 0.97 seconds
root@kali:~#
```

Versionserkennung



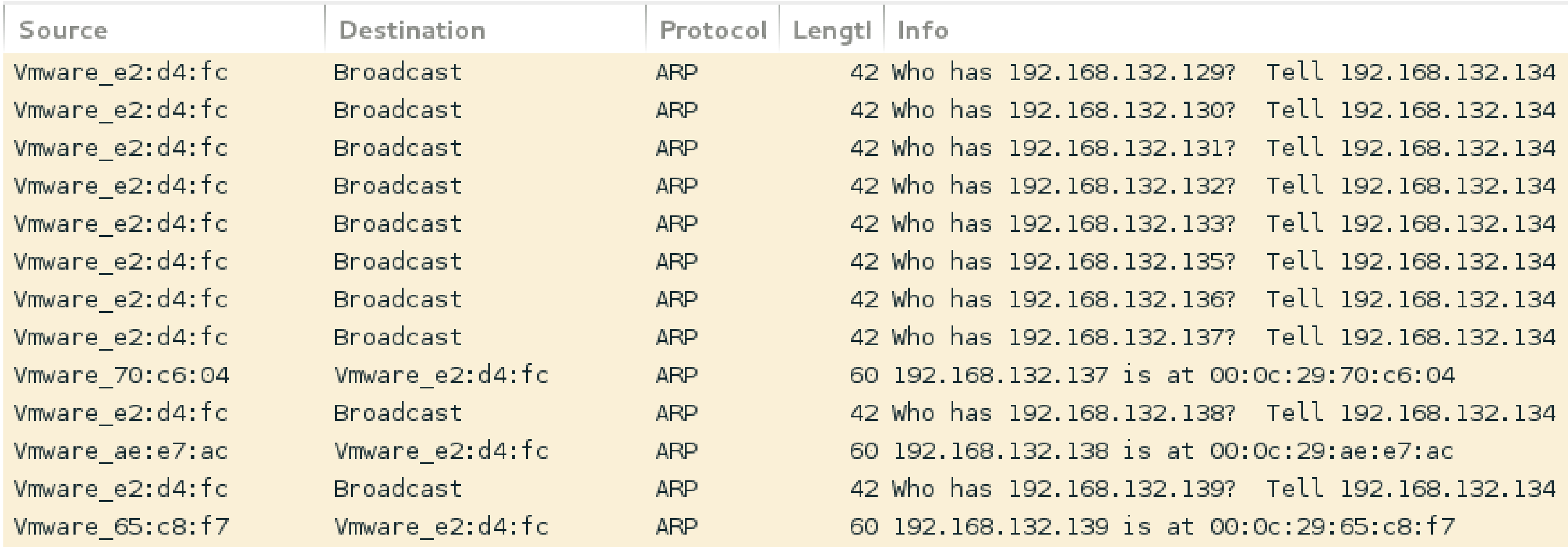
```
root@kali:~# nmap -sV 192.168.132.137

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-12 07:52 EDT
Nmap scan report for localhost (192.168.132.137)
Host is up (0.00042s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

Betriebssystemerkennung



```
root@kali:~# nmap -O 192.168.132.138

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-12 08:06 EDT
Nmap scan report for localhost (192.168.132.138)
Host is up (0.00059s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:0C:29:AE:E7:AC (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windo
server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
```

Aktive Hosts erkennen - Was macht NMAP da eigentlich!? Ein Livemitschnitt



Source	Destination	Protocol	Lengtl	Info
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.129? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.130? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.131? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.132? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.133? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.135? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.136? Tell 192.168.132.134
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.137? Tell 192.168.132.134
Vmware_70:c6:04	Vmware_e2:d4:fc	ARP	60	192.168.132.137 is at 00:0c:29:70:c6:04
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.138? Tell 192.168.132.134
Vmware_ae:e7:ac	Vmware_e2:d4:fc	ARP	60	192.168.132.138 is at 00:0c:29:ae:e7:ac
Vmware_e2:d4:fc	Broadcast	ARP	42	Who has 192.168.132.139? Tell 192.168.132.134
Vmware_65:c8:f7	Vmware_e2:d4:fc	ARP	60	192.168.132.139 is at 00:0c:29:65:c8:f7

Vielfältige Specials □ - 3 Beispiele

- Geschindigkeit `nmap –T[0..5] <IP>`
  langsame bis agressive Scans um einem IDS nicht aufzufallen

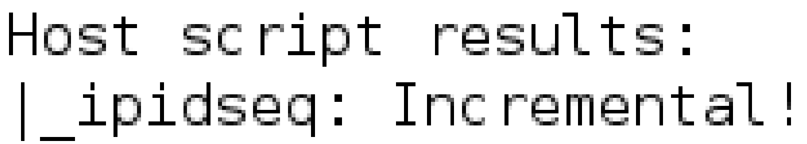
- Fragmentierung `nmap –f <IP>`
  fragmentierte Pakete um Firewall/IDS zu täuschen

- Idle-Scan `ping –sI <IP>`
  Scan mit einem Zombie-Host um selbst nicht aufzufallen
  http://nmap.org/book/idlescan.html

- …

Idle Scan

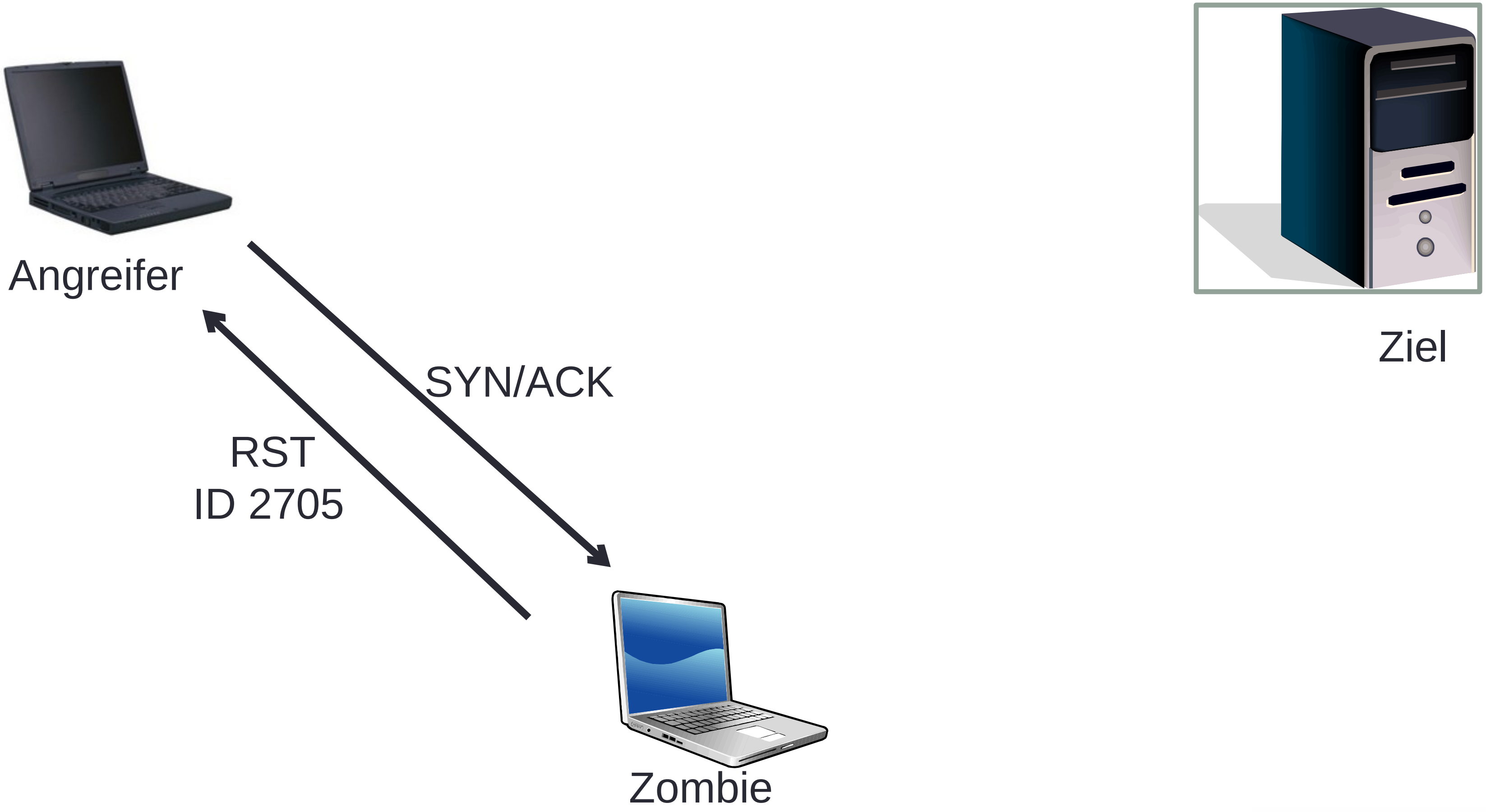
- Verwendung eines unschuldigen PC‘s (Zombie) zum Scannen
- Zombie PC muß Identifikations Nummer (16 Bit Feld) im IP Header immer ums 1 erhöhen (inkrement)
- Testen ob für Zombie geeignet
- nmap --script ipidseq IP
- Wenn Ergebnis ->



```
Host script results:
|_ipidseq: Incremental!
```

- Geeignet!
- Funktionsweise am Beispiel

Schritt 1 ID abfragen



Angreifer

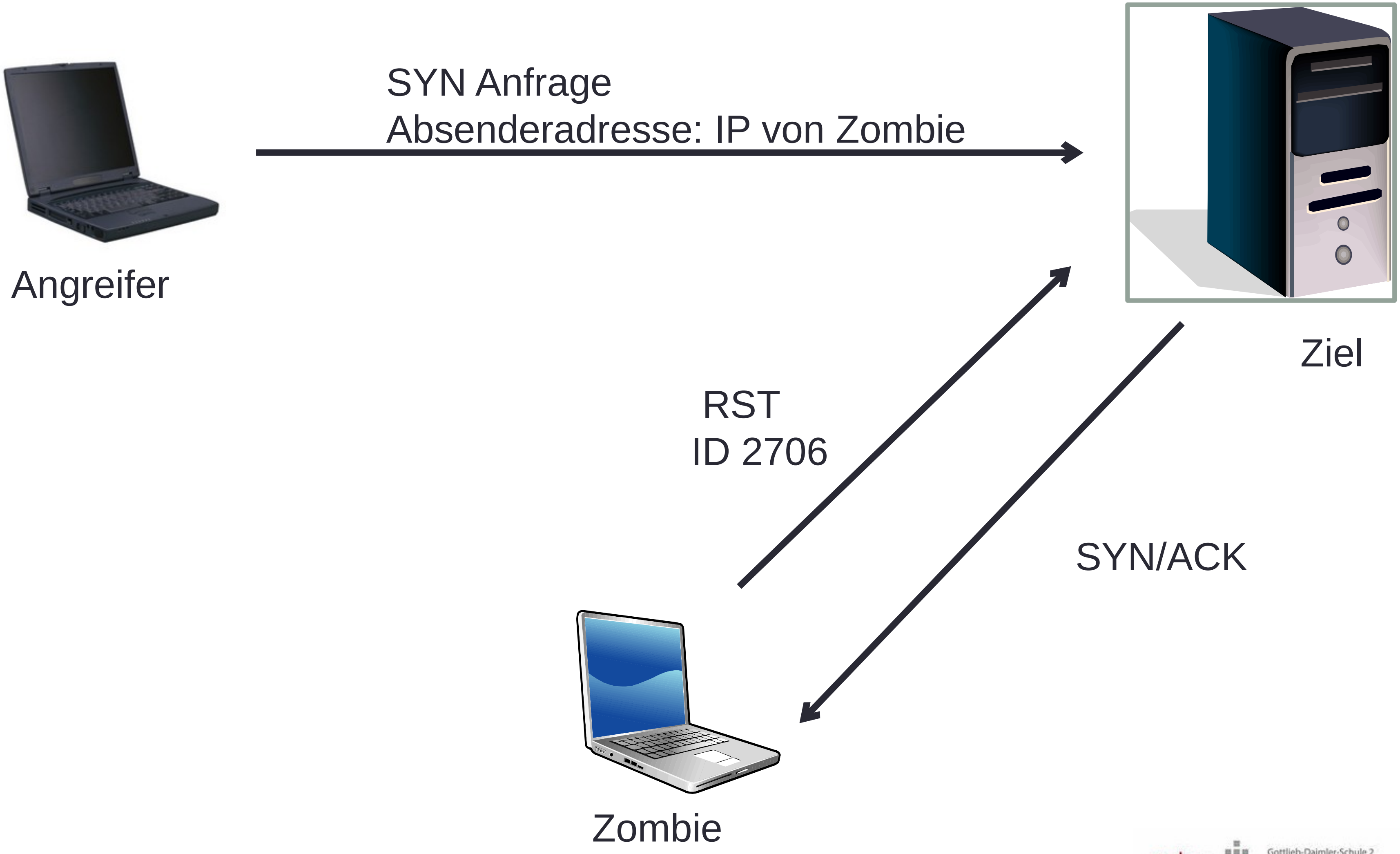
Ziel

SYN/ACK

RST
ID 2705

Zombie

Schritt 2 Gefälschte SYN Anfrage



SYN Anfrage
Absenderadresse: IP von Zombie

Angreifer

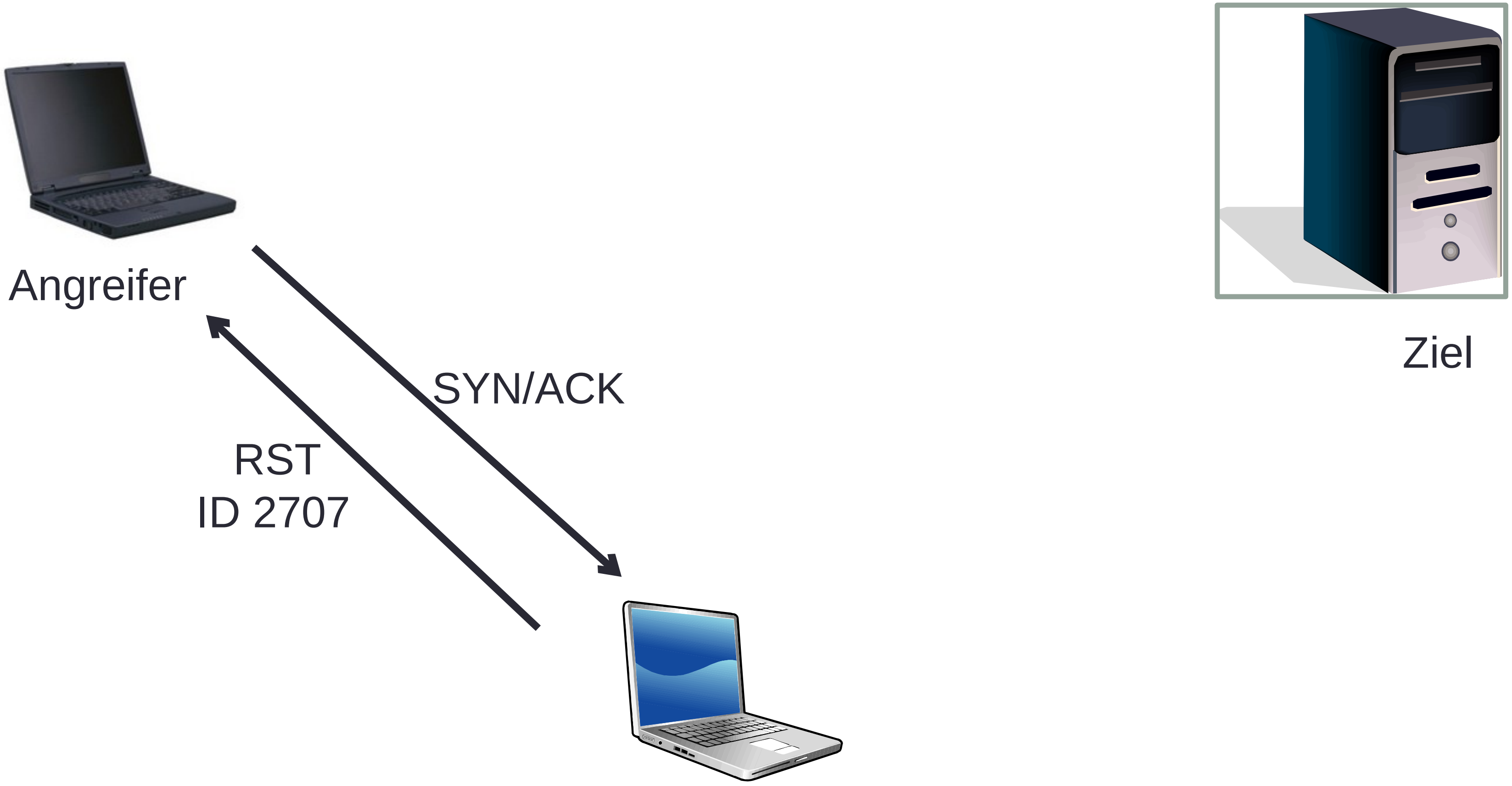
Ziel

RST
ID 2706

SYN/ACK

Zombie

Schritt 3 ID erneut abfragen



Angreifer

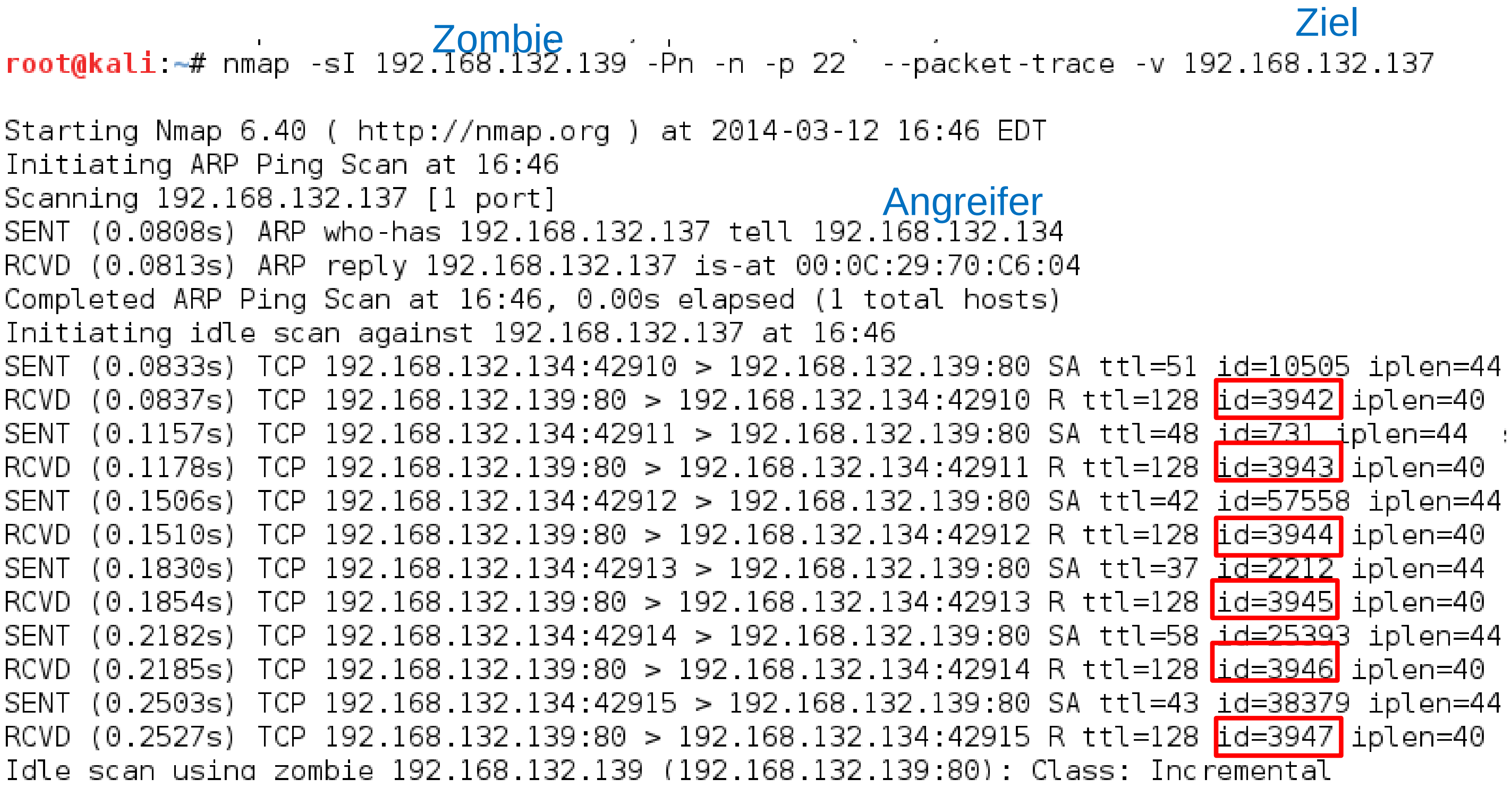
SYN/ACK

RST
ID 2707

Ziel

Wenn ID sich um 2 erhöht hat ist der abgefragte Port offen

IDLE SCAN starten



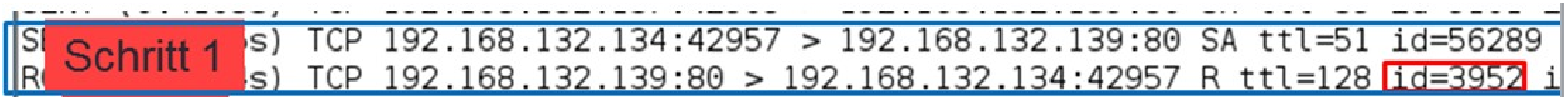
```
root@kali:~# nmap -sI 192.168.132.139 -Pn -n -p 22  --packet-trace -v 192.168.132.137

Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-12 16:46 EDT
Initiating ARP Ping Scan at 16:46
Scanning 192.168.132.137 [1 port]
SENT (0.0808s) ARP who-has 192.168.132.137 tell 192.168.132.134
RCVD (0.0813s) ARP reply 192.168.132.137 is-at 00:0C:29:70:C6:04
Completed ARP Ping Scan at 16:46, 0.00s elapsed (1 total hosts)
Initiating idle scan against 192.168.132.137 at 16:46
SENT (0.0833s) TCP 192.168.132.134:42910 > 192.168.132.139:80 SA ttl=51 id=10505 iplen=44
RCVD (0.0837s) TCP 192.168.132.139:80 > 192.168.132.134:42910 R ttl=128 id=3942 iplen=40
SENT (0.1157s) TCP 192.168.132.134:42911 > 192.168.132.139:80 SA ttl=48 id=731 iplen=44
RCVD (0.1178s) TCP 192.168.132.139:80 > 192.168.132.134:42911 R ttl=128 id=3943 iplen=40
SENT (0.1506s) TCP 192.168.132.134:42912 > 192.168.132.139:80 SA ttl=42 id=57558 iplen=44
RCVD (0.1510s) TCP 192.168.132.139:80 > 192.168.132.134:42912 R ttl=128 id=3944 iplen=40
SENT (0.1830s) TCP 192.168.132.134:42913 > 192.168.132.139:80 SA ttl=37 id=2212 iplen=44
RCVD (0.1854s) TCP 192.168.132.139:80 > 192.168.132.134:42913 R ttl=128 id=3945 iplen=40
SENT (0.2182s) TCP 192.168.132.134:42914 > 192.168.132.139:80 SA ttl=58 id=25393 iplen=44
RCVD (0.2185s) TCP 192.168.132.139:80 > 192.168.132.134:42914 R ttl=128 id=3946 iplen=40
SENT (0.2503s) TCP 192.168.132.134:42915 > 192.168.132.139:80 SA ttl=43 id=38379 iplen=44
RCVD (0.2527s) TCP 192.168.132.139:80 > 192.168.132.134:42915 R ttl=128 id=3947 iplen=40
Idle scan using zombie 192.168.132.139 (192.168.132.139:80): Class: Incremental
```

- Nochmal testen, ob IP um 1 erhöht wird

IDLE SCAN es wird ernst

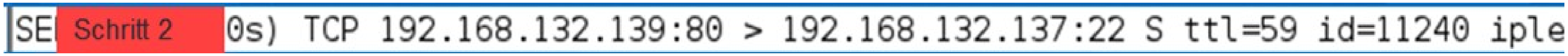
Angreifer 134 Zombie 139 Ziel 137

1. Momentane ID des Zombies feststellen



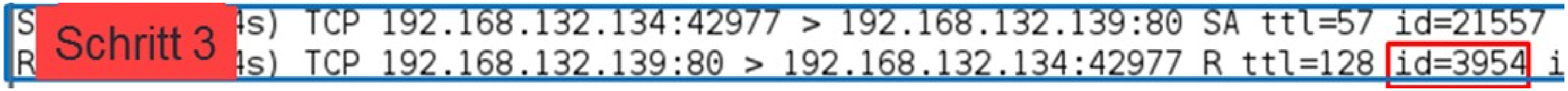
```
SE Schritt 1 s) TCP 192.168.132.134:42957 > 192.168.132.139:80 SA ttl=51 id=56289
R           s) TCP 192.168.132.139:80 > 192.168.132.134:42957 R ttl=128 id=3952 i
```

2. Gefälschte Anfrage an Ziel abschicken



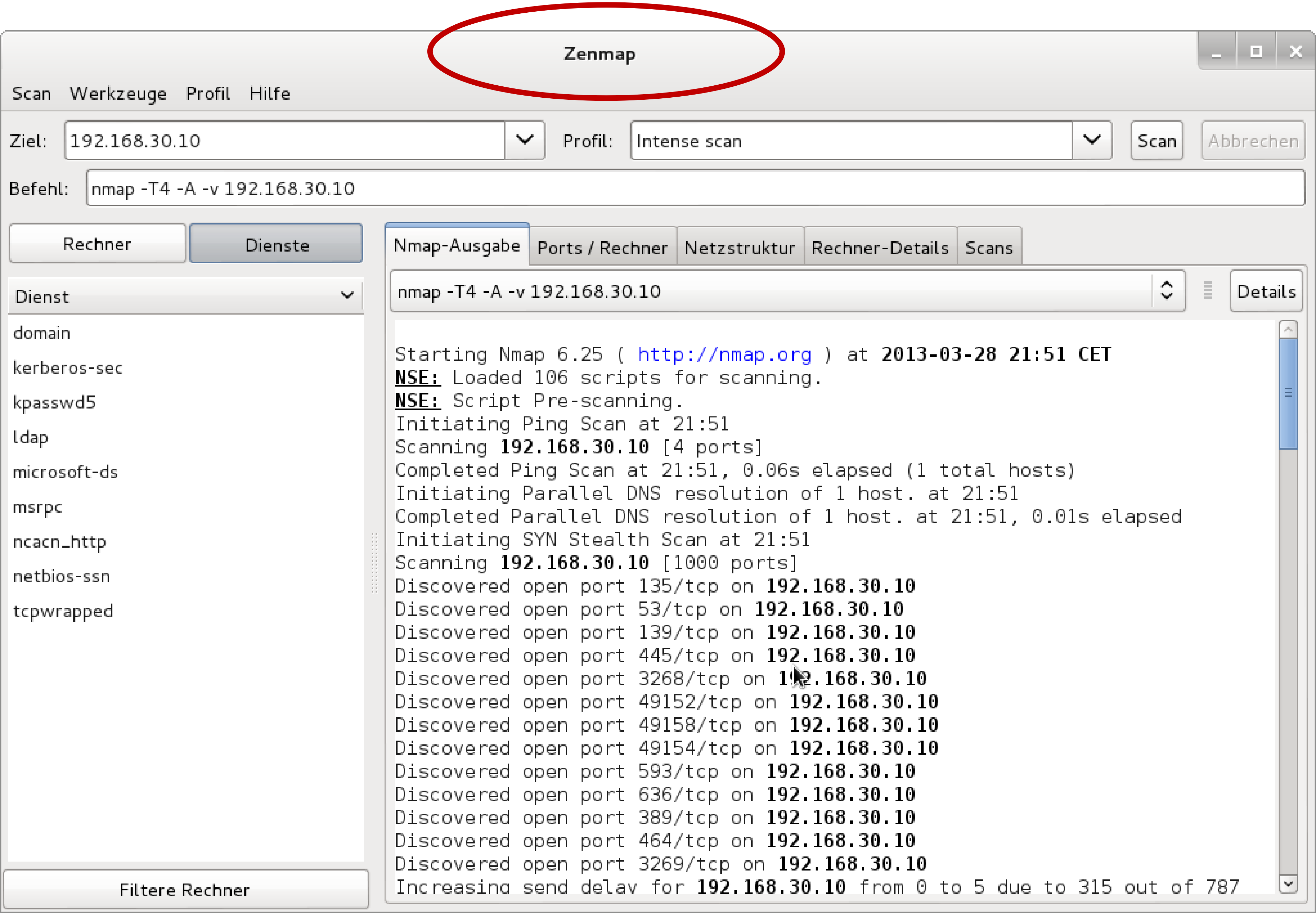
```
SE Schritt 2 0s) TCP 192.168.132.139:80 > 192.168.132.137:22 S ttl=59 id=11240 iple
```

3. ID des Zombies erneut abfragen



```
S Schritt 3 4s) TCP 192.168.132.134:42977 > 192.168.132.139:80 SA ttl=57 id=21557
R           4s) TCP 192.168.132.139:80 > 192.168.132.134:42977 R ttl=128 id=3954 i
```

Noch besser in Wireshark, da man dort
auch die Antwort von Ziel auf Zombie sieht



Ziel: 192.168.30.10

Profil: Intense scan

Befehl: nmap -T4 -A -v 192.168.30.10

Dienst
- domain
- kerberos-sec
- kpasswd5
- ldap
- microsoft-ds
- msrpc
- ncacn_http
- netbios-ssn
- tcpwrapped

nmap -T4 -A -v 192.168.30.10

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-28 21:51 CET
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 21:51
Scanning 192.168.30.10 [4 ports]
Completed Ping Scan at 21:51, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:51
Completed Parallel DNS resolution of 1 host. at 21:51, 0.01s elapsed
Initiating SYN Stealth Scan at 21:51
Scanning 192.168.30.10 [1000 ports]
Discovered open port 135/tcp on 192.168.30.10
Discovered open port 53/tcp on 192.168.30.10
Discovered open port 139/tcp on 192.168.30.10
Discovered open port 445/tcp on 192.168.30.10
Discovered open port 3268/tcp on 192.168.30.10
Discovered open port 49152/tcp on 192.168.30.10
Discovered open port 49158/tcp on 192.168.30.10
Discovered open port 49154/tcp on 192.168.30.10
Discovered open port 593/tcp on 192.168.30.10
Discovered open port 636/tcp on 192.168.30.10
Discovered open port 389/tcp on 192.168.30.10
Discovered open port 464/tcp on 192.168.30.10
Discovered open port 3269/tcp on 192.168.30.10
Increasing send delay for 192.168.30.10 from 0 to 5 due to 315 out of 787
```

Workshop

- nmap mit Optionen testen
- IP Adressen der virtuellen Maschinen feststellen
- Informationen zu virtuellen Maschinen sammeln (Offene Ports Dienste, OS)
- IDLE Scan