Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

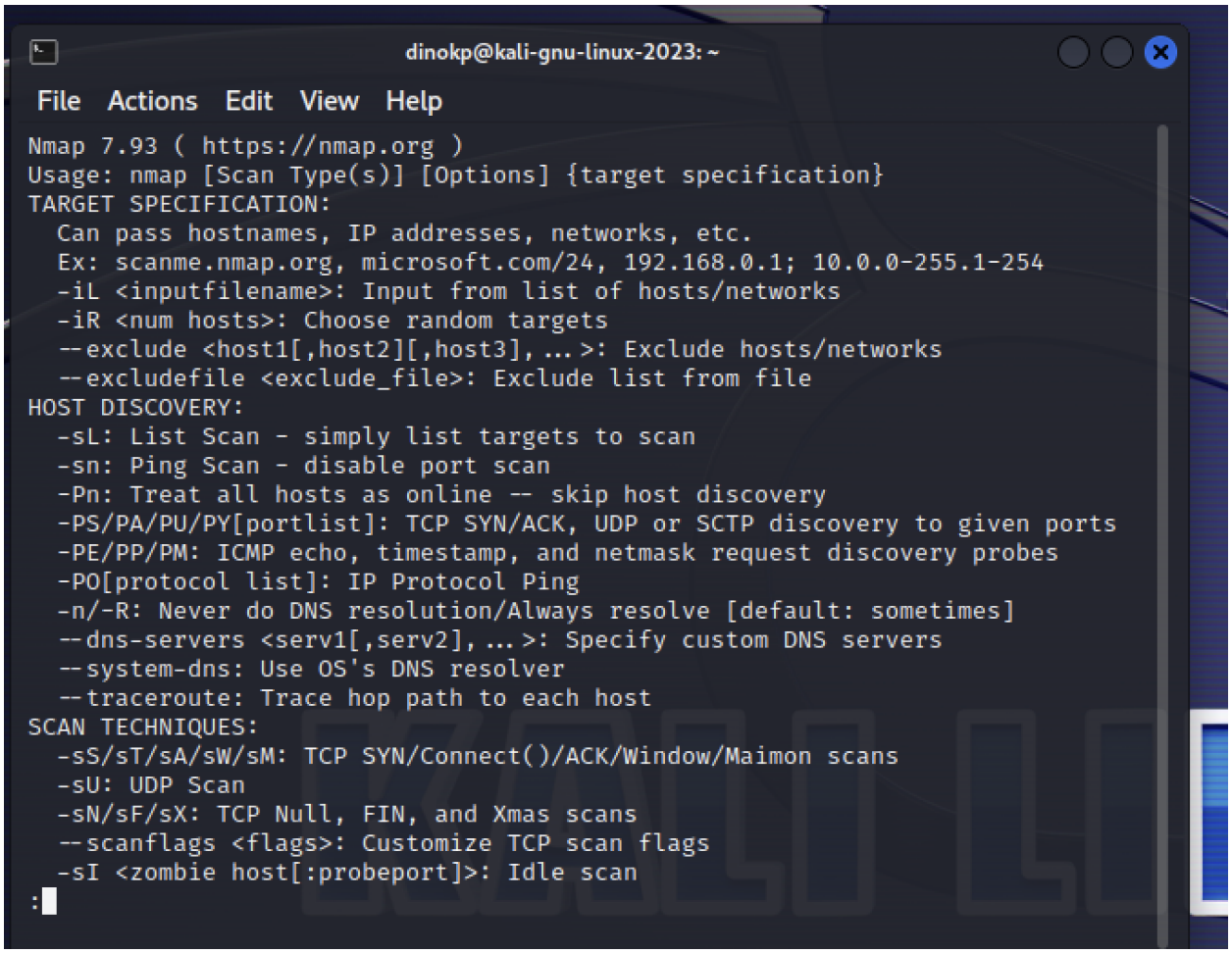
Title : Port Scanning

Lab : 11

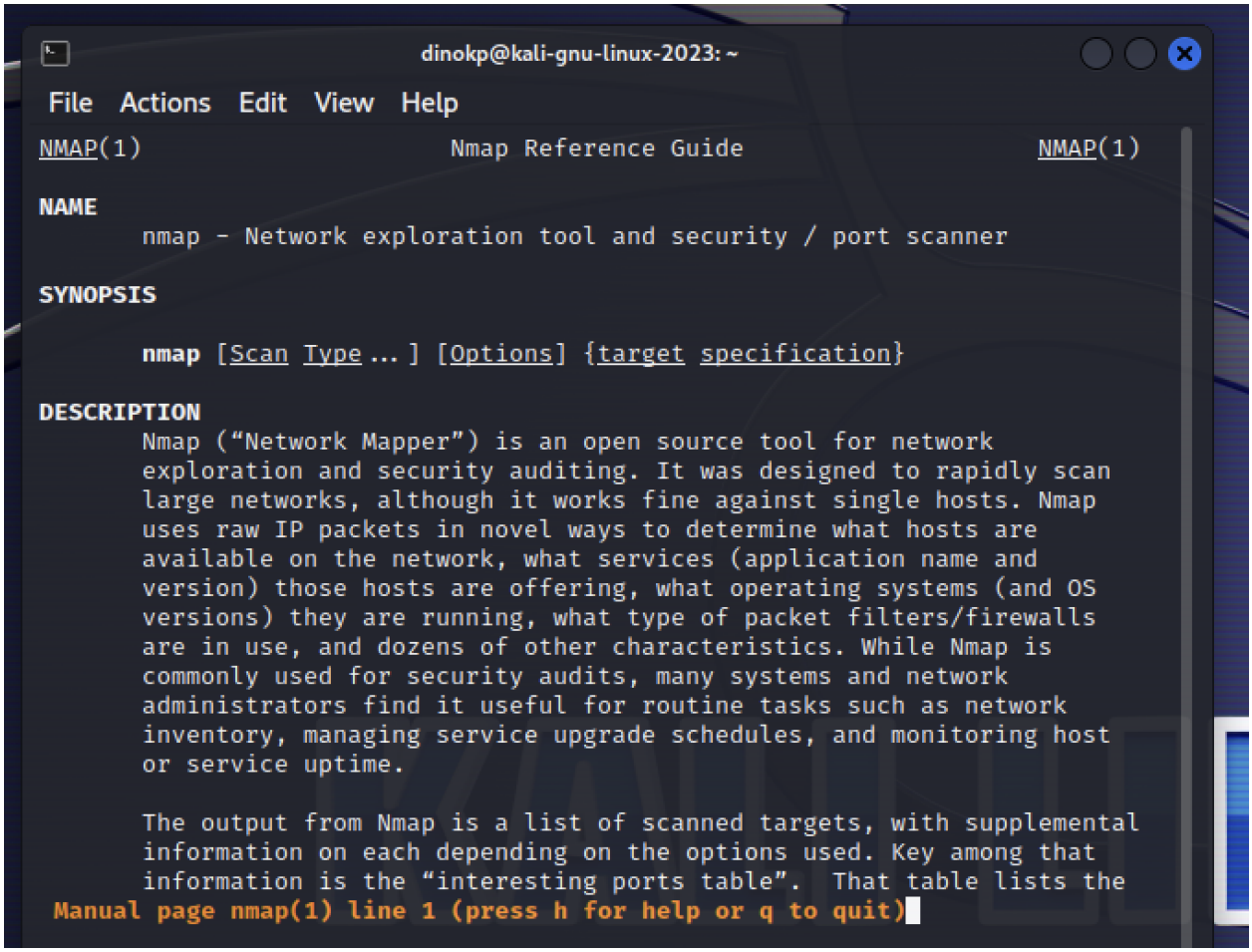
Chapter : 16 (Port Scanning with Nmap)

Exercise : 16. 1

Step 1 :
A.



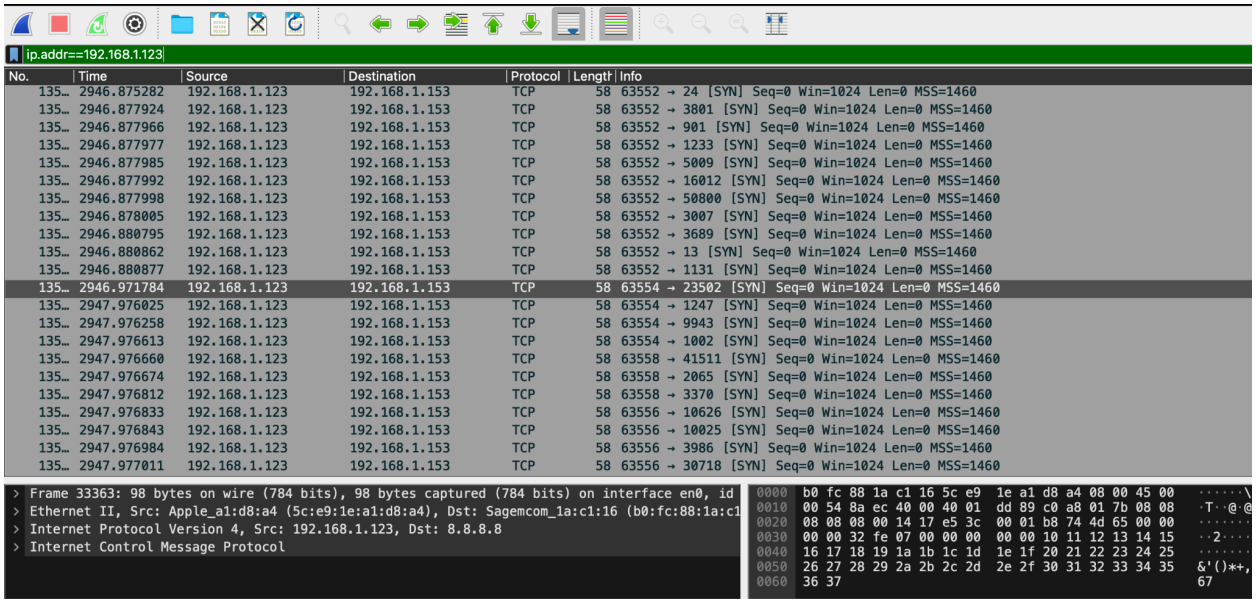
B.



C.

```
┌──(parallels㉿kali-gnu-linux-2023)-[/home/dinokp]
└─$ sudo nmap 192.168.1.153
[sudo] password for parallels:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-09 19:51 EST
Nmap scan report for MacBook-Pro-6.lan (192.168.1.153)
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 5C:E9:1E:A1:D8:A4 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds
```

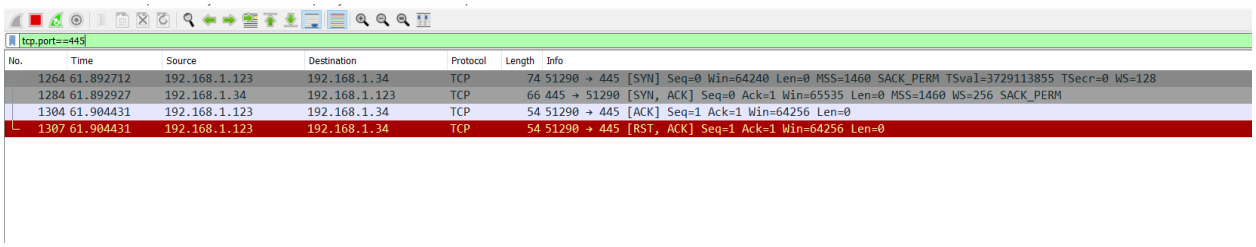
D, E .



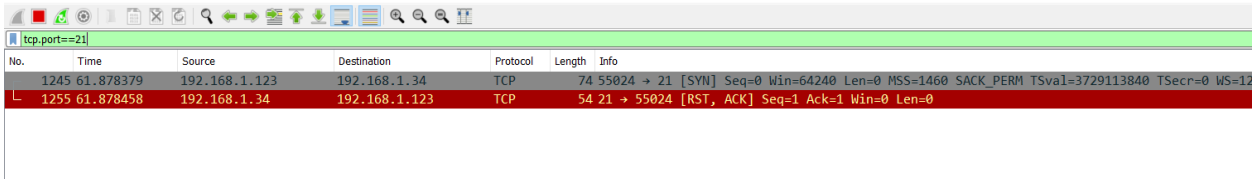
Sent a SYN

I used a different computer for Step 1 and Step 2 later, as I was having trouble in bridged mode.

Thanks

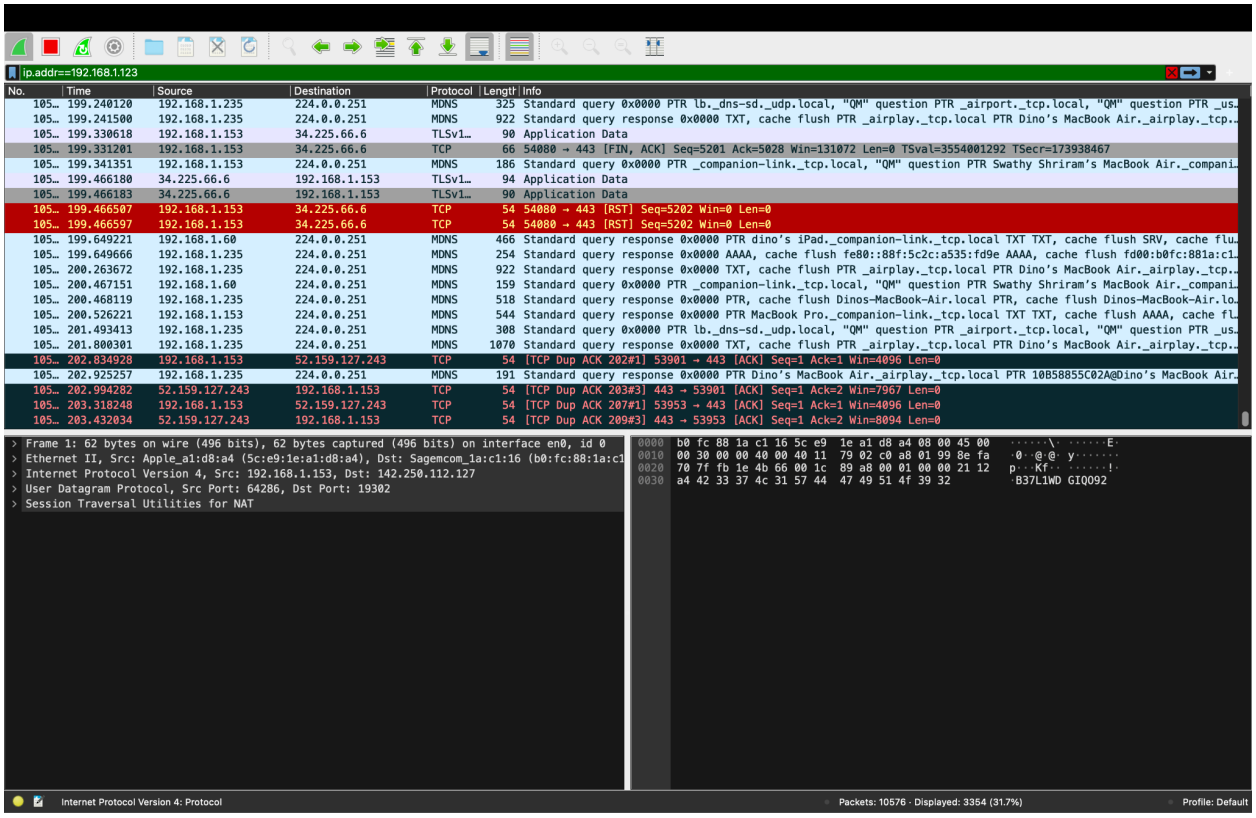


F.

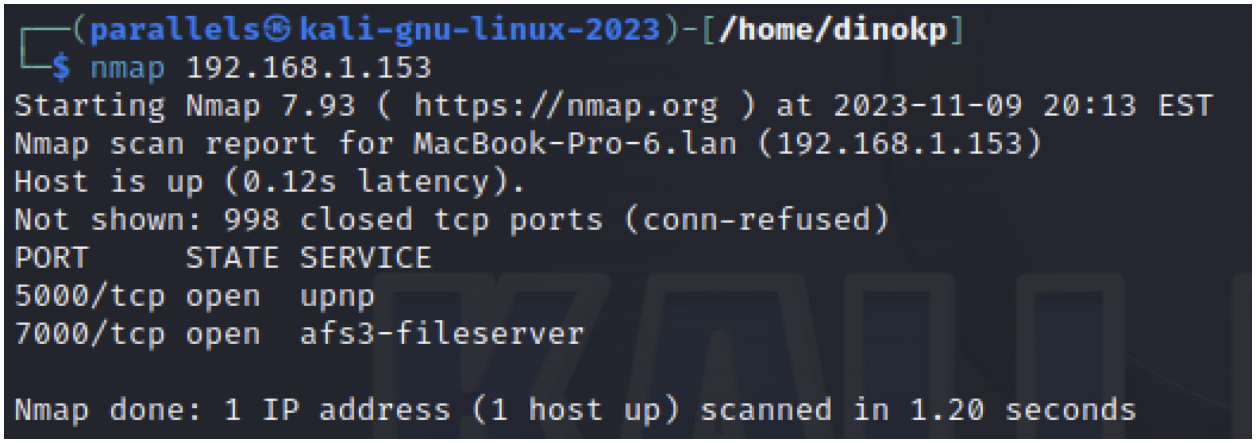


Step 2 :

A.


ip.addr==192.168.1.123
No. Time Source Destination Protocol Length Info
105… 199.240120 192.168.1.235 224.0.0.251 MDNS 325 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question PTR _us…
105… 199.241500 192.168.1.235 224.0.0.251 MDNS 922 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Dino's MacBook Air._airplay._tcp…
105… 199.330618 192.168.1.153 34.225.66.6 TLSv1… 90 Application Data
105… 199.331201 192.168.1.153 34.225.66.6 TCP 66 54080 → 443 [FIN, ACK] Seq=5201 Ack=5028 Win=131072 Len=0 TSval=3554001292 TSecr=173938467
105… 199.341351 192.168.1.153 224.0.0.251 MDNS 186 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR Swathy Shriram's MacBook Air._compani…
105… 199.466180 34.225.66.6 192.168.1.153 TLSv1… 94 Application Data
105… 199.466183 34.225.66.6 192.168.1.153 TLSv1… 90 Application Data
105… 199.466507 192.168.1.153 34.225.66.6 TCP 54 54080 → 443 [RST] Seq=5202 Win=0 Len=0
105… 199.466597 192.168.1.153 34.225.66.6 TCP 54 54080 → 443 [RST] Seq=5202 Win=0 Len=0
105… 199.649221 192.168.1.60 224.0.0.251 MDNS 466 Standard query response 0x0000 PTR dino's iPad._companion-link._tcp.local TXT TXT, cache flush SRV, cache flu…
105… 199.649666 192.168.1.235 224.0.0.251 MDNS 254 Standard query response 0x0000 AAAA, cache flush fe80::88f:5c2c:a535:fd9e AAAA, cache flush fd00:b0fc:881a:c1…
105… 200.263672 192.168.1.235 224.0.0.251 MDNS 922 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Dino's MacBook Air._airplay._tcp…
105… 200.467151 192.168.1.60 224.0.0.251 MDNS 159 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR Swathy Shriram's MacBook Air._compani…
105… 200.468119 192.168.1.235 224.0.0.251 MDNS 518 Standard query response 0x0000 PTR, cache flush Dinos-MacBook-Air.local PTR, cache flush Dinos-MacBook-Air.lo…
105… 200.526221 192.168.1.153 224.0.0.251 MDNS 544 Standard query response 0x0000 PTR MacBook Pro._companion-link._tcp.local TXT TXT, cache flush AAAA, cache fl…
105… 201.493413 192.168.1.235 224.0.0.251 MDNS 308 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question PTR _us…
105… 201.800301 192.168.1.235 224.0.0.251 MDNS 1070 Standard query response 0x0000 TXT, cache flush PTR _airplay._tcp.local PTR Dino's MacBook Air._airplay._tcp…
105… 202.834928 192.168.1.153 52.159.127.243 TCP 54 [TCP Dup ACK 202#1] 53901 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
105… 202.925257 192.168.1.235 224.0.0.251 MDNS 191 Standard query response 0x0000 PTR Dino's MacBook Air._airplay._tcp.local PTR 10B58855C02A@Dino's MacBook Air…
105… 202.994282 52.159.127.243 192.168.1.153 TCP 54 [TCP Dup ACK 203#3] 443 → 53901 [ACK] Seq=1 Ack=2 Win=7967 Len=0
105… 203.318248 192.168.1.153 52.159.127.243 TCP 54 [TCP Dup ACK 207#1] 53953 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
105… 203.432034 52.159.127.243 192.168.1.153 TCP 54 [TCP Dup ACK 209#3] 443 → 53953 [ACK] Seq=1 Ack=2 Win=8094 Len=0
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface en0, id 0
Ethernet II, Src: Apple_a1:d8:a4 (5c:e9:1e:a1:d8:a4), Dst: Sagemcom_1a:c1:16 (b0:fc:88:1a:c1
Internet Protocol Version 4, Src: 192.168.1.153, Dst: 142.250.112.127
User Datagram Protocol, Src Port: 64286, Dst Port: 19302
Session Traversal Utilities for NAT
0000 b0 fc 88 1a c1 16 5c e9 1e a1 d8 a4 08 00 45 00
0010 00 30 00 00 40 00 40 11 79 02 c0 a8 01 99 8e fa
0020 70 7f fb 1e 4b 66 00 1c 89 a8 00 01 00 00 21 12
0030 a4 42 33 37 4c 31 57 44 47 49 51 4f 39 32
B37L1WD GIQO92
Internet Protocol Version 4: Protocol
Packets: 10576 · Displayed: 3354 (31.7%)
Profile: Default

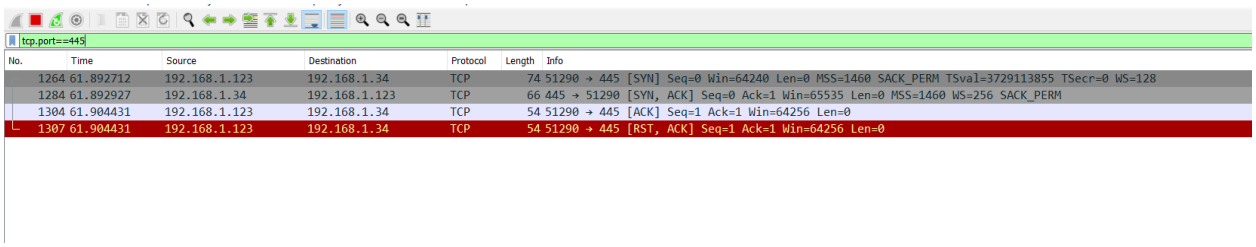
B,


┌──(parallels㉿kali-gnu-linux-2023)-[/home/dinokp]
└─$ nmap 192.168.1.153
Starting Nmap 7.93 (https://nmap.org) at 2023-11-09 20:13 EST
Nmap scan report for MacBook-Pro-6.lan (192.168.1.153)
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
5000/tcp open upnp
7000/tcp open afs3-fileserver
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

C.

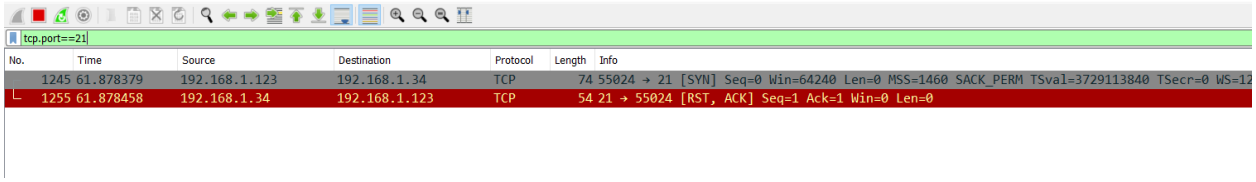
```
┌──(parallels㉿kali-gnu-linux-2023)-[/home/dinokp]
└─$ nmap -sT 192.168.1.153
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-09 20:15 EST
Nmap scan report for MacBook-Pro-6.lan (192.168.1.153)
Host is up (0.37s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
5000/tcp open  upnp
7000/tcp open  afs3-fileserver

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
```

D.



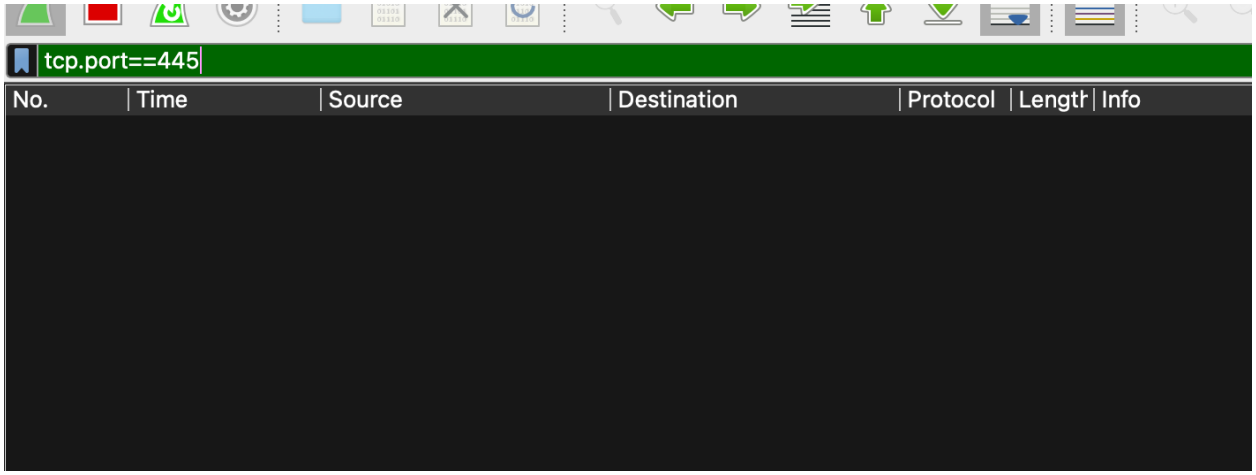
E.

Ip.port == 21



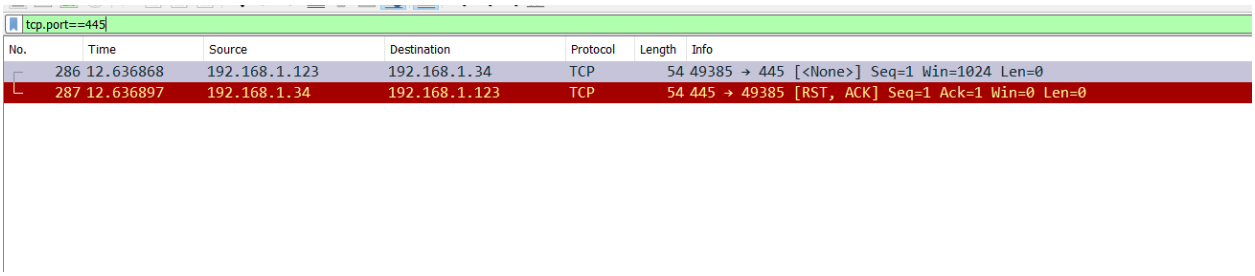
Step 3 :

A.



B.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sN -p 445 192.168.1.34
[sudo] password for parallels:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 11:56 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.18s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```



C.

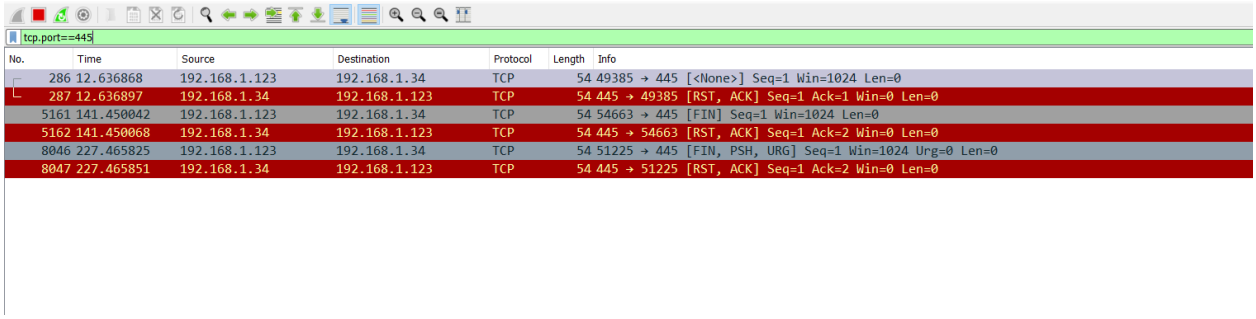
Yeah I got RST for NULL scan, lets try for fin, and Xmas.

D.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sF -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 11:58 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.12s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

E.

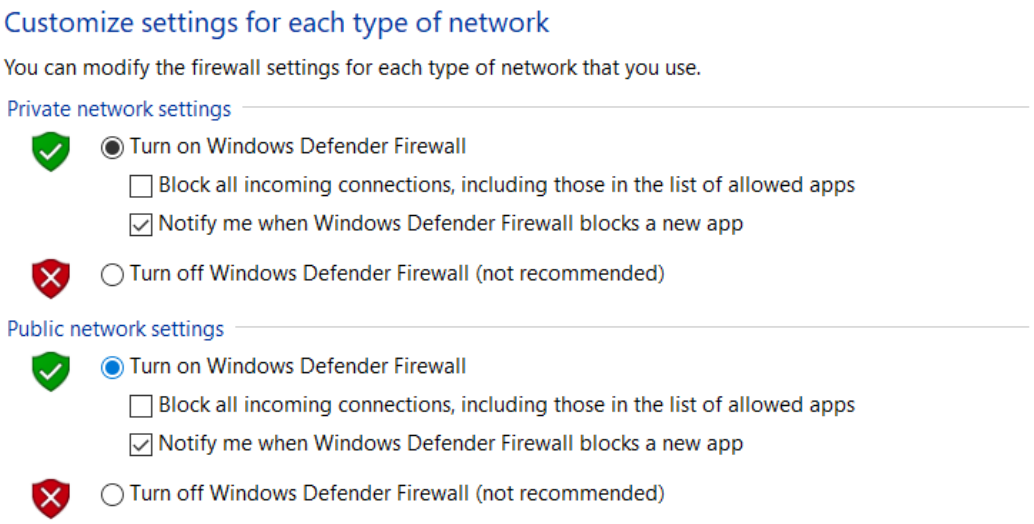
```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sX -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:00 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.14s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```



tcp.port==445

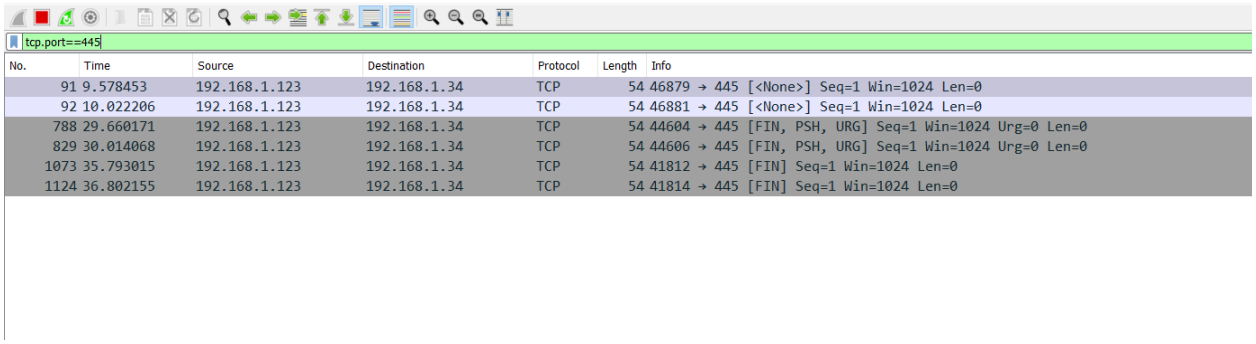
No.	Time	Source	Destination	Protocol	Length	Info
286	12.636868	192.168.1.123	192.168.1.34	TCP	54	49385 → 445 [<None>] Seq=1 Win=1024 Len=0
287	12.636897	192.168.1.34	192.168.1.123	TCP	54	445 → 49385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5161	141.450042	192.168.1.123	192.168.1.34	TCP	54	54663 → 445 [FIN] Seq=1 Win=1024 Len=0
5162	141.450068	192.168.1.34	192.168.1.123	TCP	54	445 → 54663 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
8046	227.465825	192.168.1.123	192.168.1.34	TCP	54	51225 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
8047	227.465851	192.168.1.34	192.168.1.123	TCP	54	445 → 51225 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

F.

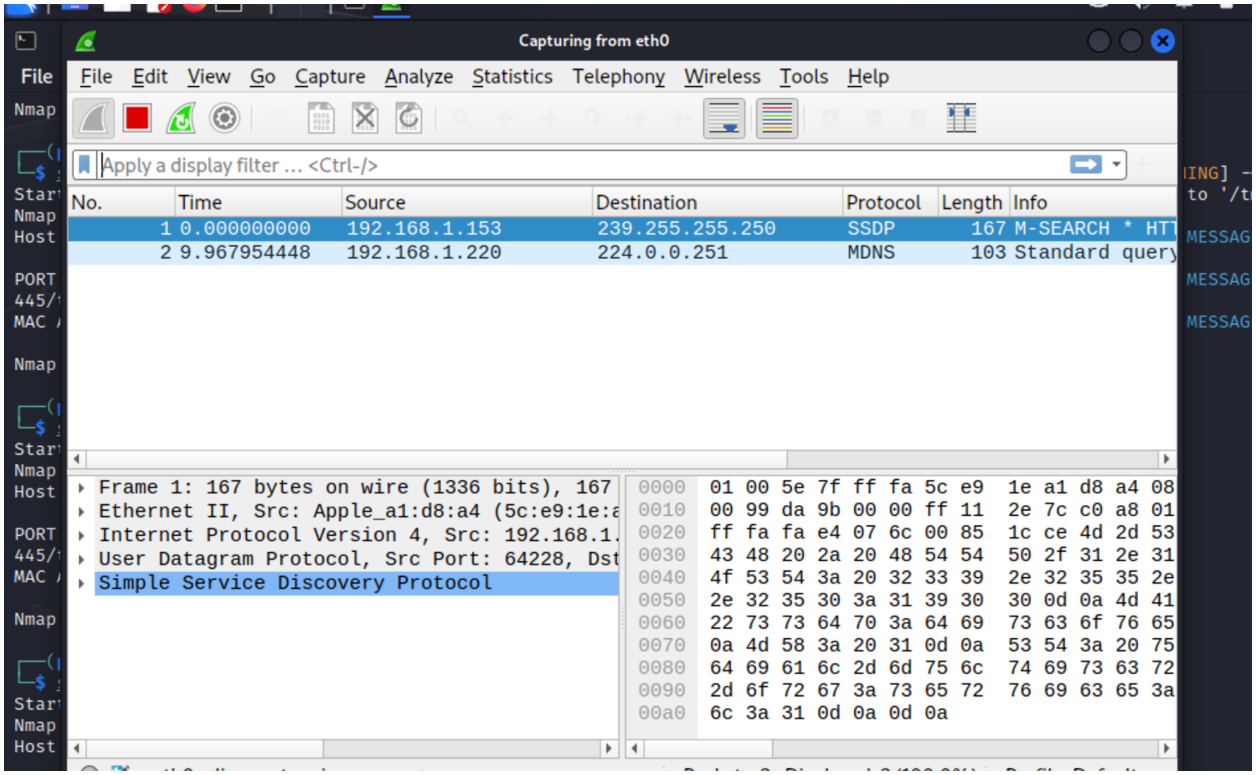


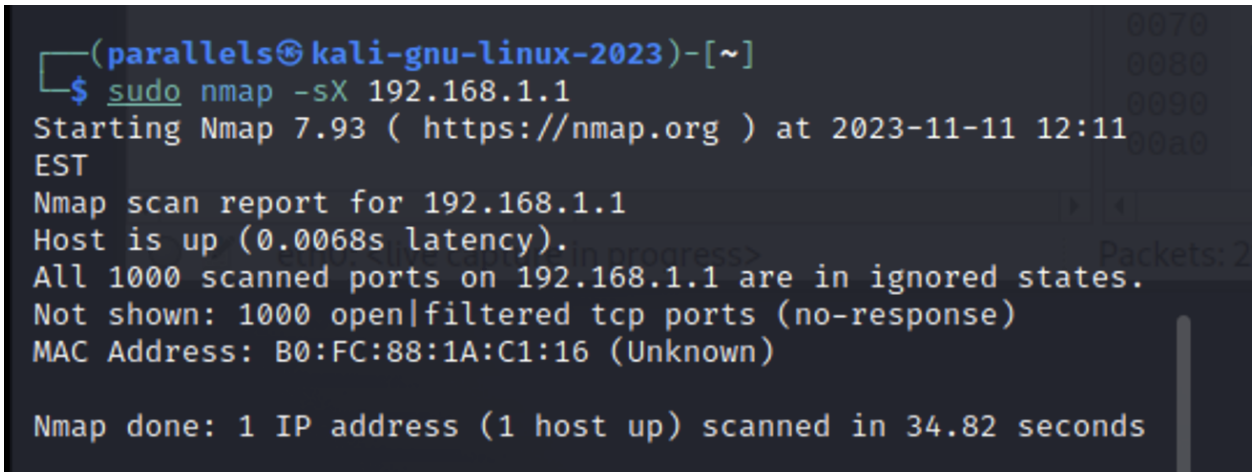
G.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sN -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:06 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.087s latency).

PORT    STATE         SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds

┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sX -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:06 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.069s latency).

PORT    STATE         SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds

┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sF -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:06 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.20s latency).

PORT    STATE         SERVICE
445/tcp open|filtered microsoft-ds
MAC Address: 38:00:25:A4:BA:28 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
```

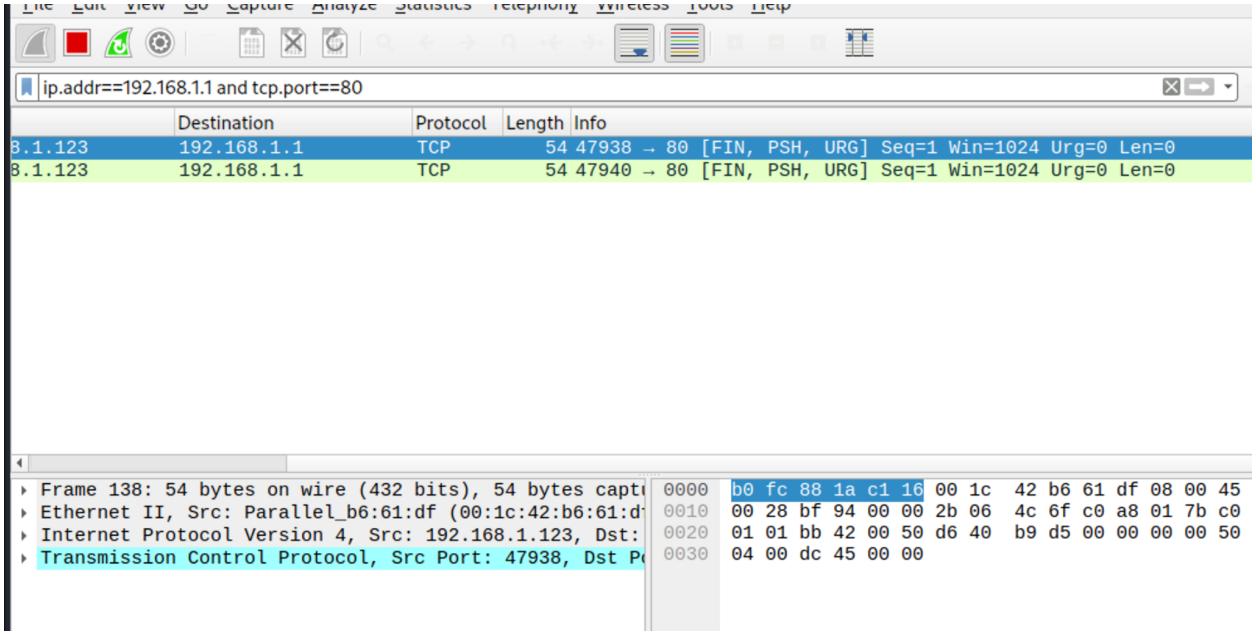


H.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.1.153 239.255.255.250 SSDP 167 M-SEARCH * HT
2 9.967954448 192.168.1.220 224.0.0.251 MDNS 103 Standard query
Frame 1: 167 bytes on wire (1336 bits), 167
Ethernet II, Src: Apple_a1:d8:a4 (5c:e9:1e:a
Internet Protocol Version 4, Src: 192.168.1.
User Datagram Protocol, Src Port: 64228, Dst
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 5c e9 1e a1 d8 a4 08
0010 00 99 da 9b 00 00 ff 11 2e 7c c0 a8 01
0020 ff fa fa e4 07 6c 00 85 1c ce 4d 2d 53
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a
00a0 6c 3a 31 0d 0a 0d 0a


(parallels㉿kali-gnu-linux-2023)-[~]
$ sudo nmap -sX 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-11-11 12:11
EST
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: B0:FC:88:1A:C1:16 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 34.82 seconds

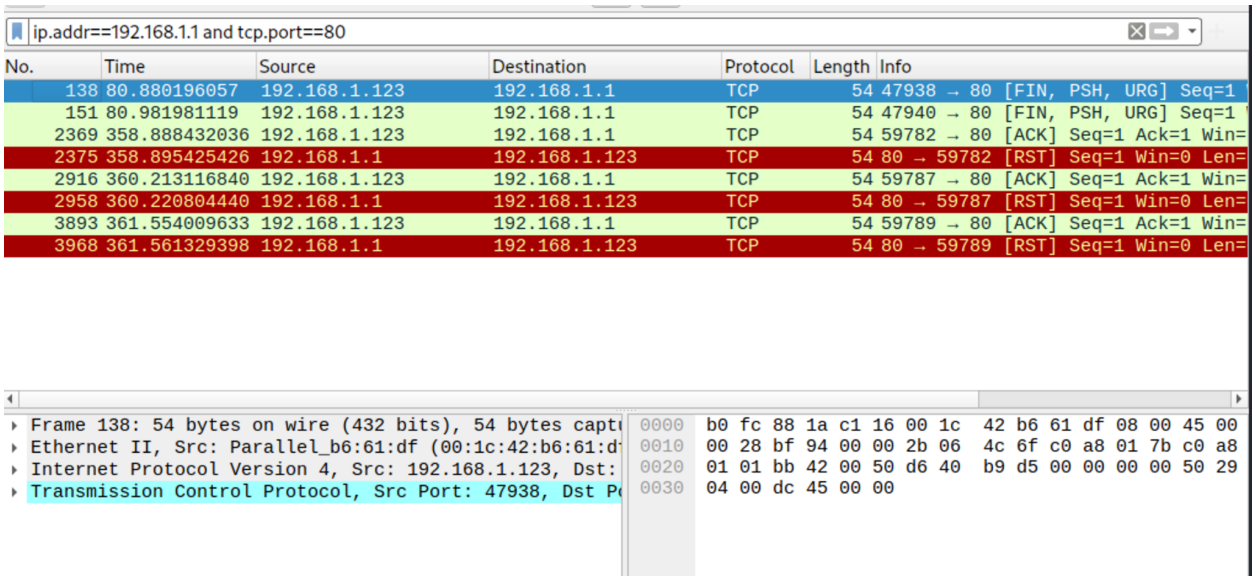
```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sX 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:11
EST
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: B0:FC:88:1A:C1:16 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 34.82 seconds
```



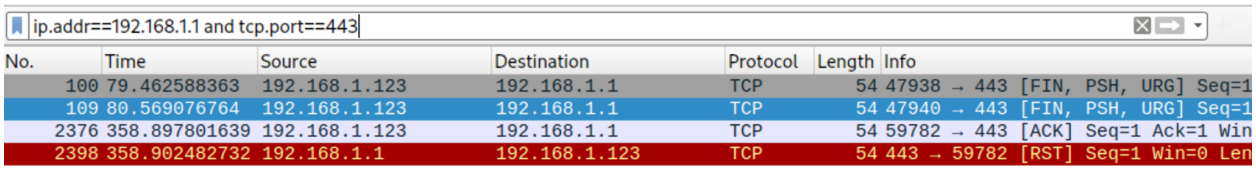
Yes it didn’t return any RST

J.

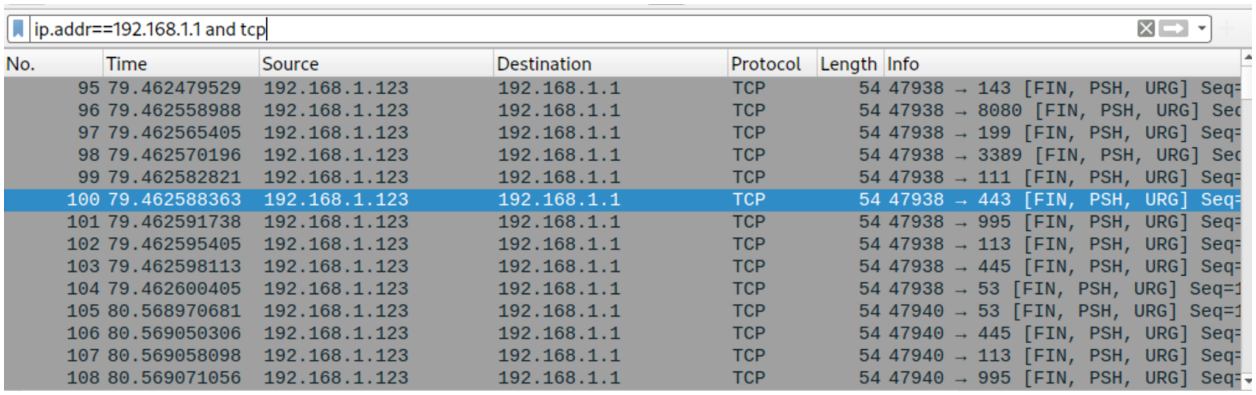
```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sA 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:15
EST
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE      SERVICE
80/tcp  unfiltered http
443/tcp unfiltered https
MAC Address: B0:FC:88:1A:C1:16 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
```



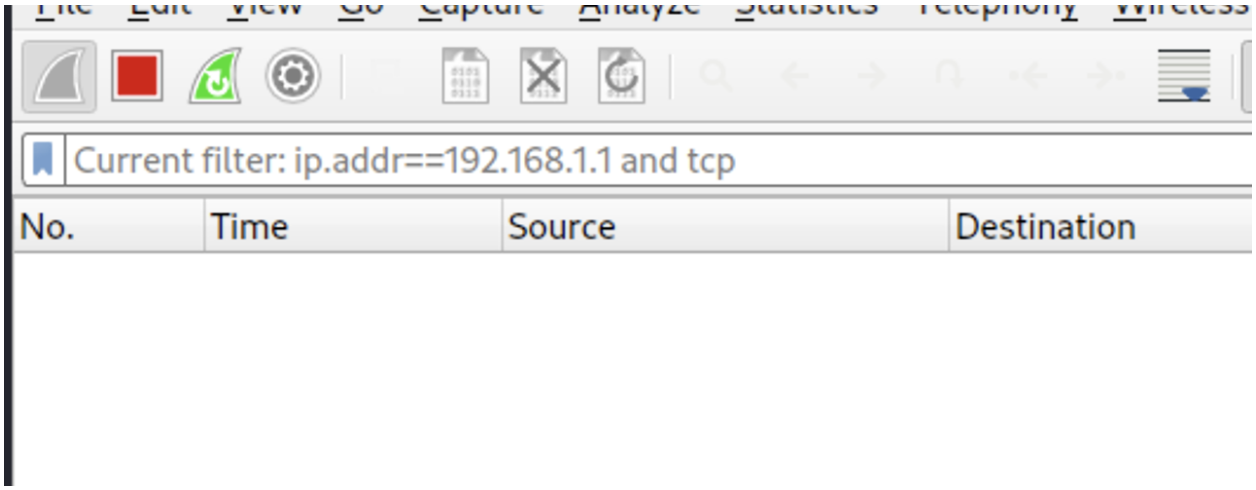
Now I can see the RST from my windows machine which is connected in my default router.



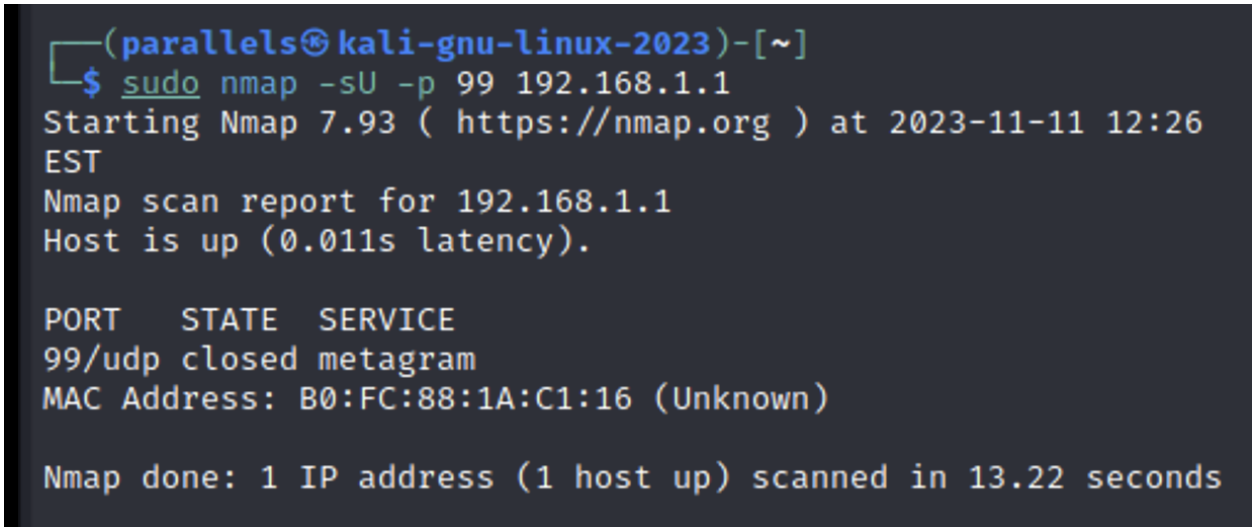
This is for the port 443.
K.

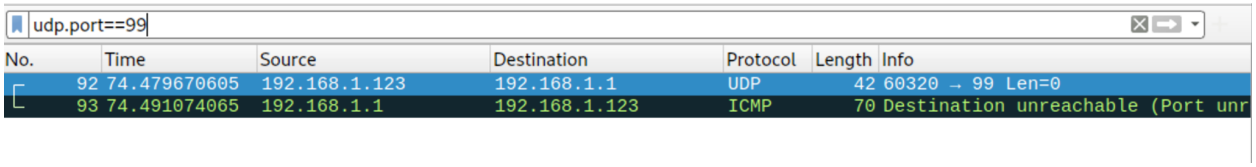


Step 4 :
A.

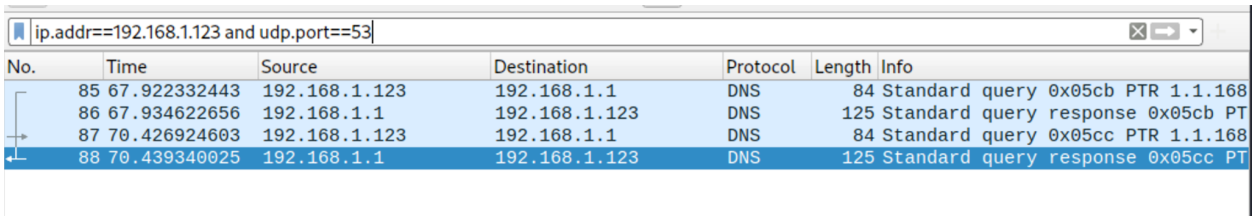


B.

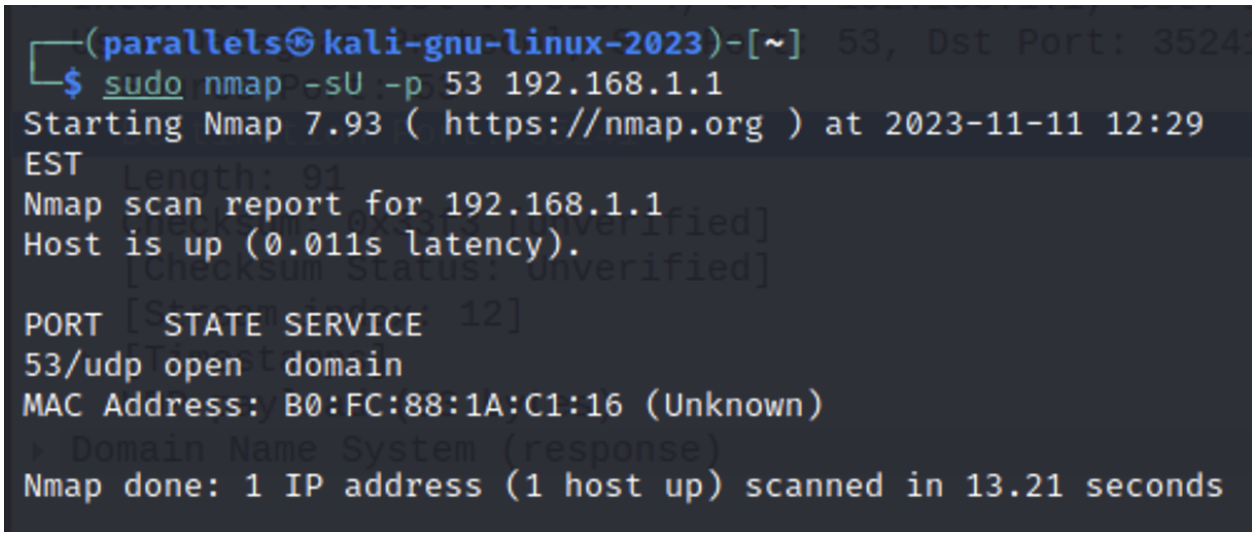


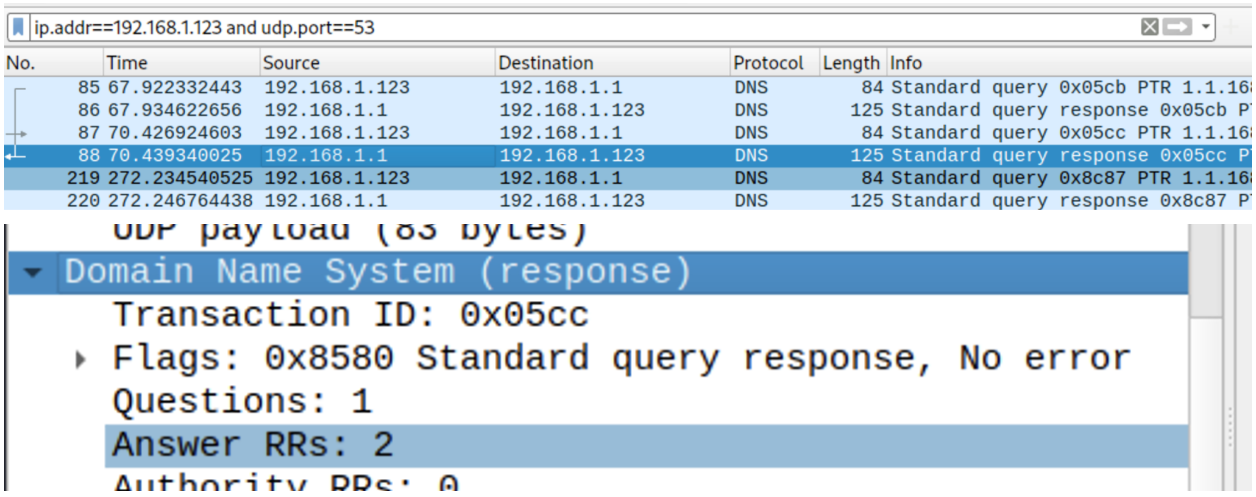

udp.port==99
No. Time Source Destination Protocol Length Info
92 74.479670605 192.168.1.123 192.168.1.1 UDP 42 60320 → 99 Len=0
93 74.491074065 192.168.1.1 192.168.1.123 ICMP 70 Destination unreachable (Port unr

C.


ip.addr==192.168.1.123 and udp.port==53
No. Time Source Destination Protocol Length Info
85 67.922332443 192.168.1.123 192.168.1.1 DNS 84 Standard query 0x05cb PTR 1.1.168
86 67.934622656 192.168.1.1 192.168.1.123 DNS 125 Standard query response 0x05cb PT
87 70.426924603 192.168.1.123 192.168.1.1 DNS 84 Standard query 0x05cc PTR 1.1.168
88 70.439340025 192.168.1.1 192.168.1.123 DNS 125 Standard query response 0x05cc PT

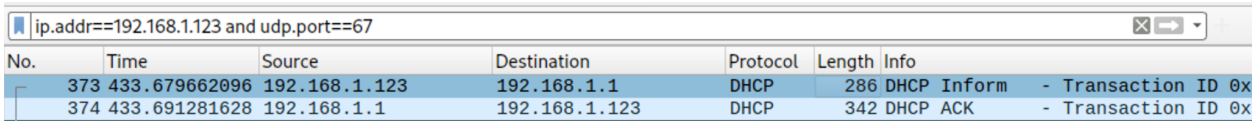
D.


(parallels㉿kali-gnu-linux-2023)-[~]
$ sudo nmap -sU -p 53 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-11-11 12:29
EST
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
PORT STATE SERVICE
53/udp open domain
MAC Address: B0:FC:88:1A:C1:16 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds

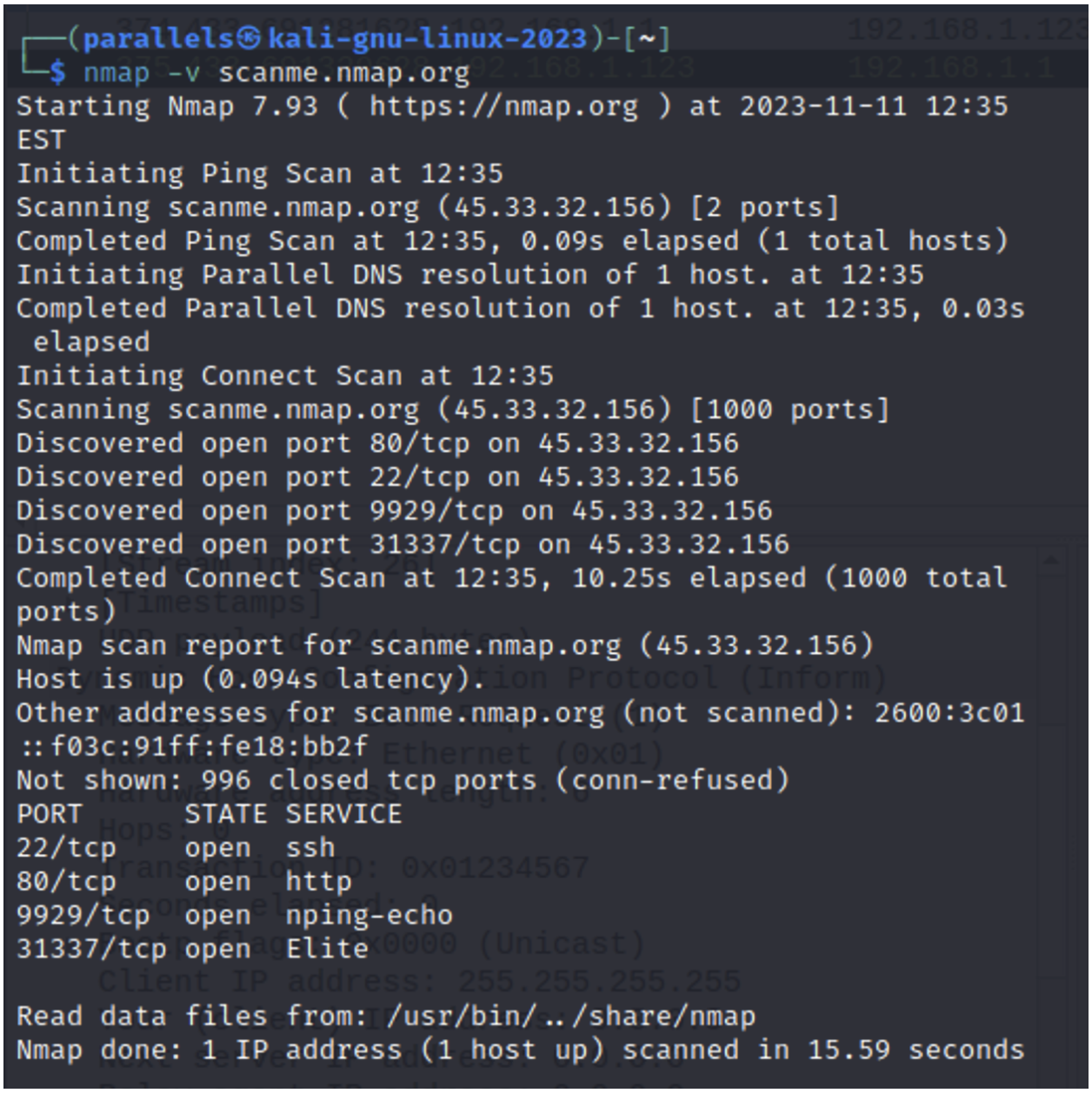

ip.addr==192.168.1.123 and udp.port==53
No. Time Source Destination Protocol Length Info
85 67.922332443 192.168.1.123 192.168.1.1 DNS 84 Standard query 0x05cb PTR 1.1.16
86 67.934622656 192.168.1.1 192.168.1.123 DNS 125 Standard query response 0x05cb P
87 70.426924603 192.168.1.123 192.168.1.1 DNS 84 Standard query 0x05cc PTR 1.1.16
88 70.439340025 192.168.1.1 192.168.1.123 DNS 125 Standard query response 0x05cc P
219 272.234540525 192.168.1.123 192.168.1.1 DNS 84 Standard query 0x8c87 PTR 1.1.16
220 272.246764438 192.168.1.1 192.168.1.123 DNS 125 Standard query response 0x8c87 P
Domain Name System (response)
Transaction ID: 0x05cc
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 2

E.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sU -p 67 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:32
EST
Nmap scan report for 192.168.1.1
Host is up (0.0098s latency).

PORT   STATE SERVICE
67/udp open  dhcps
MAC Address: B0:FC:88:1A:C1:16 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```



Step 5 :
A.


(parallels㉿kali-gnu-linux-2023)-[~]
$ nmap -v scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-11-11 12:35
EST
Initiating Ping Scan at 12:35
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 12:35, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:35
Completed Parallel DNS resolution of 1 host. at 12:35, 0.03s
elapsed
Initiating Connect Scan at 12:35
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 12:35, 10.25s elapsed (1000 total
ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.094s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01
::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.59 seconds

B.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~]
└─$ sudo nmap -sS -O scanme.nmap.org/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:39 EST
Nmap scan report for 45.33.32.0
Host is up (0.0052s latency).
All 1000 scanned ports on 45.33.32.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for gw-li982.linode.com (45.33.32.1)
Host is up (0.0054s latency).
All 1000 scanned ports on gw-li982.linode.com (45.33.32.1) are
in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for 45.33.32.2
Host is up (0.0056s latency).
All 1000 scanned ports on 45.33.32.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for 45.33.32.3
Host is up (0.0057s latency).
All 1000 scanned ports on 45.33.32.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for business-software.shop (45.33.32.4)
Host is up (0.083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
```

```
Nmap scan report for 45-33-32-12.ip.linodeusercontent.com (45.3
3.32.12)
Host is up (0.0051s latency).
All 1000 scanned ports on 45-33-32-12.ip.linodeusercontent.com
(45.33.32.12) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for 45-33-32-13.ip.linodeusercontent.com (45.3
3.32.13)
Host is up (0.0061s latency).
All 1000 scanned ports on 45-33-32-13.ip.linodeusercontent.com
(45.33.32.13) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls

Nmap scan report for 45-33-32-14.ip.linodeusercontent.com (45.3
3.32.14)
Host is up (0.0064s latency).
All 1000 scanned ports on 45-33-32-14.ip.linodeusercontent.com
(45.33.32.14) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS detai
ls
```