

Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Port Scanning

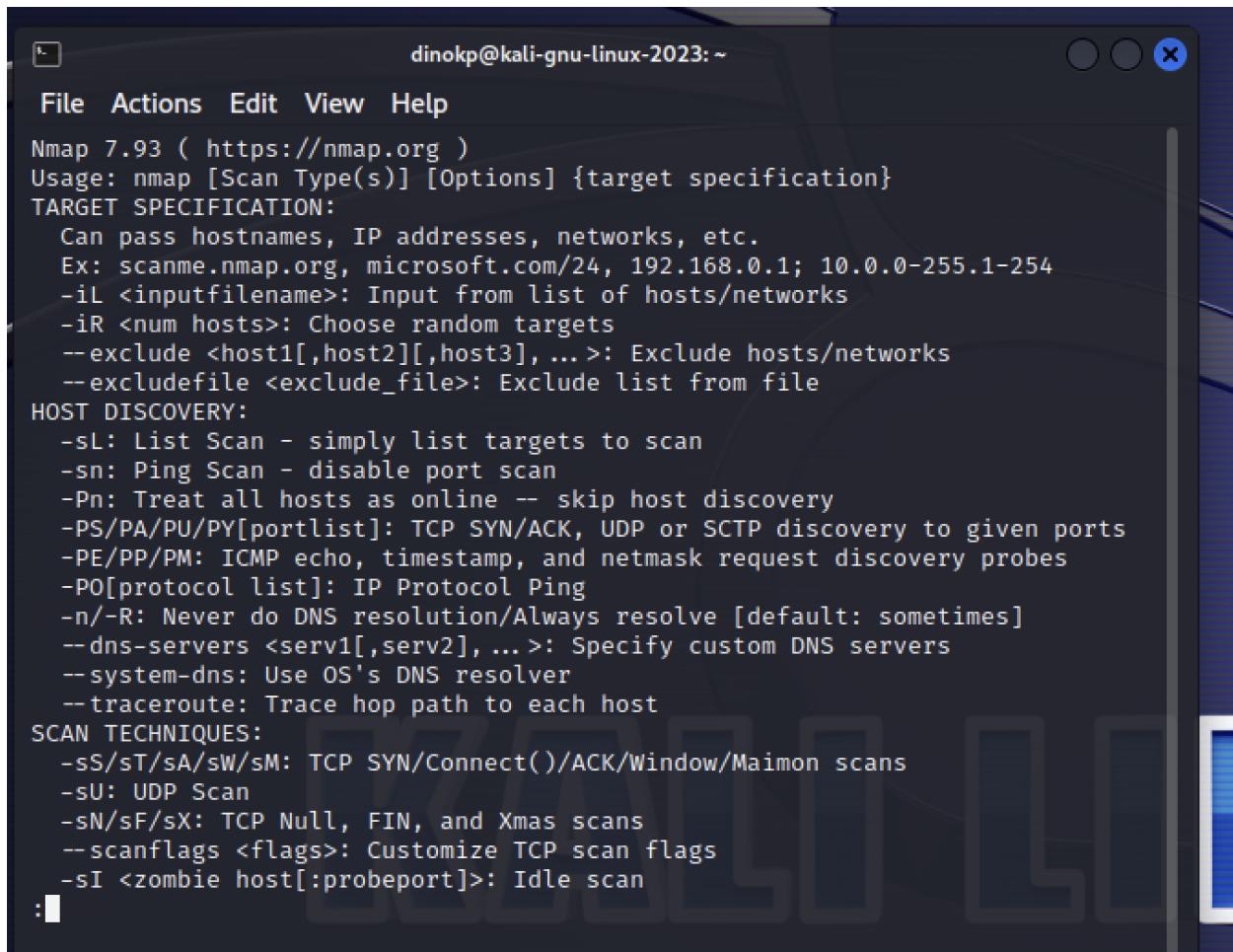
Lab : 11

Chapter : 16 (Port Scanning with Nmap)

Exercise : 16. 1

Step 1 :

A.



The screenshot shows a terminal window titled "dinokp@kali-gnu-linux-2023: ~". The window contains the usage information for Nmap 7.93. The text is as follows:

```
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ... >: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
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/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
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ... >: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
:|
```

B.

```
dinokp@kali-gnu-linux-2023: ~
File Actions Edit View Help
NMAP(1) Nmap Reference Guide NMAP(1)
NAME
nmap - Network exploration tool and security / port scanner
SYNOPSIS
nmap [Scan Type ...] [Options] {target specification}
DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network
exploration and security auditing. It was designed to rapidly scan
large networks, although it works fine against single hosts. Nmap
uses raw IP packets in novel ways to determine what hosts are
available on the network, what services (application name and
version) those hosts are offering, what operating systems (and OS
versions) they are running, what type of packet filters/firewalls
are in use, and dozens of other characteristics. While Nmap is
commonly used for security audits, many systems and network
administrators find it useful for routine tasks such as network
inventory, managing service upgrade schedules, and monitoring host
or service uptime.

The output from Nmap is a list of scanned targets, with supplemental
information on each depending on the options used. Key among that
information is the "interesting ports table". That table lists the
Manual page nmap(1) line 1 (press h for help or q to quit)
```

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 .

No.	Time	Source	Destination	Protocol	Length	Info
135..	2946.875282	192.168.1.123	192.168.1.153	TCP	58	63552 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877924	192.168.1.123	192.168.1.153	TCP	58	63552 → 3801 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877966	192.168.1.123	192.168.1.153	TCP	58	63552 → 901 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877977	192.168.1.123	192.168.1.153	TCP	58	63552 → 1233 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877985	192.168.1.123	192.168.1.153	TCP	58	63552 → 5009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877992	192.168.1.123	192.168.1.153	TCP	58	63552 → 16012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.877998	192.168.1.123	192.168.1.153	TCP	58	63552 → 50800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.878005	192.168.1.123	192.168.1.153	TCP	58	63552 → 3007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.880795	192.168.1.123	192.168.1.153	TCP	58	63552 → 3689 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.880862	192.168.1.123	192.168.1.153	TCP	58	63552 → 13 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.880877	192.168.1.123	192.168.1.153	TCP	58	63552 → 1131 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2946.971784	192.168.1.123	192.168.1.153	TCP	58	63554 → 23502 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976025	192.168.1.123	192.168.1.153	TCP	58	63554 → 1247 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976250	192.168.1.123	192.168.1.153	TCP	58	63554 → 9943 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976613	192.168.1.123	192.168.1.153	TCP	58	63554 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976660	192.168.1.123	192.168.1.153	TCP	58	63558 → 41511 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976674	192.168.1.123	192.168.1.153	TCP	58	63558 → 2065 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976812	192.168.1.123	192.168.1.153	TCP	58	63558 → 3370 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976833	192.168.1.123	192.168.1.153	TCP	58	63556 → 10626 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976843	192.168.1.123	192.168.1.153	TCP	58	63556 → 10025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.976984	192.168.1.123	192.168.1.153	TCP	58	63556 → 3986 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135..	2947.977011	192.168.1.123	192.168.1.153	TCP	58	63556 → 30718 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```

> Frame 33363: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0x0000
> 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: 192.168.1.123, Dst: 8.8.8.8
> Internet Control Message Protocol

```

```

0000 b0 fc 88 1a c1 16 5c e9 1e a1 d8 a4 08 00 45 00 ...
0010 00 54 8a ec 40 00 40 01 dd 89 c0 a8 01 7b 08 08 T @ ...
0020 08 00 08 00 14 17 e5 3c 00 01 b8 74 4d 65 00 00
0030 00 00 32 fe 07 00 00 00 00 00 10 11 12 13 14 15 - 2 -
0040 16 17 18 19 1a 1b 1c 1d 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()**,
0060 36 37 67

```

Sent a SYN

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

No.	Time	Source	Destination	Protocol	Length	Info
1264	61.892712	192.168.1.123	192.168.1.34	TCP	74	51290 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3729113855 TSeср=0 WS=128
1284	61.892927	192.168.1.34	192.168.1.123	TCP	66	445 → 51290 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1304	61.904431	192.168.1.123	192.168.1.34	TCP	54	51290 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
1307	61.904431	192.168.1.123	192.168.1.34	TCP	54	51290 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0

F.

No.	Time	Source	Destination	Protocol	Length	Info
1245	61.878379	192.168.1.123	192.168.1.34	TCP	74	55024 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3729113840 TSeср=0 WS=128
1255	61.878458	192.168.1.34	192.168.1.123	TCP	54	21 → 55024 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Step 2 :

A.

No.	Time	Source	Destination	Protocol	[Length]	Info
105..	199.2401280	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..	199.2415000	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	540888 → 443 [FIN, ACK] Seq=5201 Ack=5028 Win=131072 Len=0 TSval=3554001292 TSeср=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..	199.466188	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	540888 → 443 [RST] Seq=5202 Win=0 Len=0
105..	199.466597	192.168.1.153	34.225.66.6	TCP	54	540888 → 443 [RST] Seq=5202 Win=0 Len=0
105..	199.649221	192.168.1.235	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::8bf5:c2ca:55: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	380	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question PTR _us...
105..	201.880301	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..	203.432834	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:ef:1e:a1:d8:a4), Dst: Sagemcom_la: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

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.

No.	Time	Source	Destination	Protocol	Length	Info
1264	61.892712	192.168.1.123	192.168.1.34	TCP	74	51290 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3729113855 TSectr=0 WS=128
1284	61.892927	192.168.1.34	192.168.1.123	TCP	66	445 → 51290 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1304	61.904431	192.168.1.123	192.168.1.34	TCP	54	51290 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
1307	61.904431	192.168.1.123	192.168.1.34	TCP	54	51290 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0

E.

Ip.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
1245	61.878379	192.168.1.123	192.168.1.34	TCP	74	55024 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3729113840 TSectr=0 WS=128
1255	61.878458	192.168.1.34	192.168.1.123	TCP	54	21 → 55024 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Step 3 :

A.

No.	Time	Source	Destination	Protocol	Length	Info

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
```

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

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
```

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.

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

- Turn on Windows Defender Firewall
 Block all incoming connections, including those in the list of allowed apps
 Notify me when Windows Defender Firewall blocks a new app

- Turn off Windows Defender Firewall (not recommended)

Public network settings

- Turn on Windows Defender Firewall
 Block all incoming connections, including those in the list of allowed apps
 Notify me when Windows Defender Firewall blocks a new app

- Turn off Windows Defender Firewall (not recommended)

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

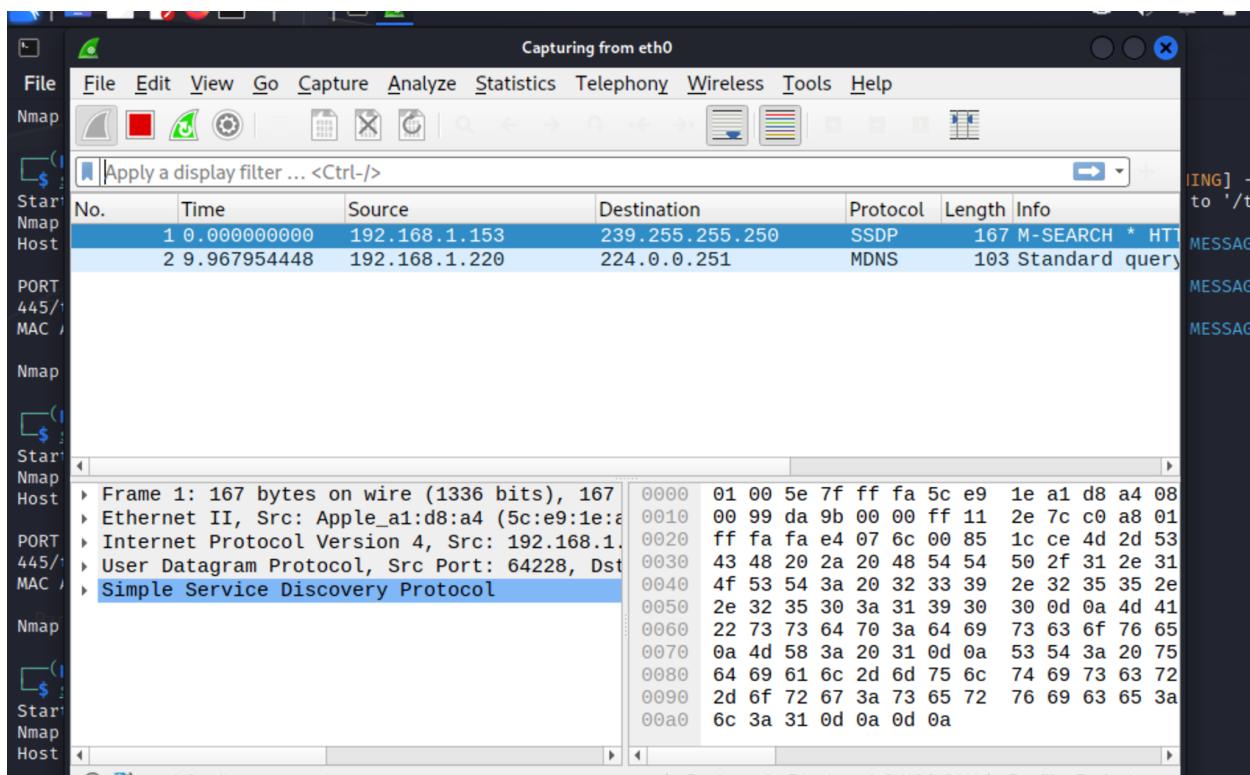
└─(parallels㉿kali-gnu-linux-2023)~] $ sudo nmap -sF -p 445 192.168.1.34
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:06 EST
Nmap scan report for DESKTOP-SMM9I0Q.lan (192.168.1.34)
Host is up (0.20s latency).

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
```

No.	Time	Source	Destination	Protocol	Length	Info
91	9.578453	192.168.1.123	192.168.1.34	TCP	54	46879 → 445 [None] Seq=1 Win=1024 Len=0
92	10.022206	192.168.1.123	192.168.1.34	TCP	54	46881 → 445 [None] Seq=1 Win=1024 Len=0
788	29.660171	192.168.1.123	192.168.1.34	TCP	54	44604 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
829	30.014068	192.168.1.123	192.168.1.34	TCP	54	44606 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1073	35.793015	192.168.1.123	192.168.1.34	TCP	54	41812 → 445 [FIN] Seq=1 Win=1024 Len=0
1124	36.802155	192.168.1.123	192.168.1.34	TCP	54	41814 → 445 [FIN] Seq=1 Win=1024 Len=0

H.

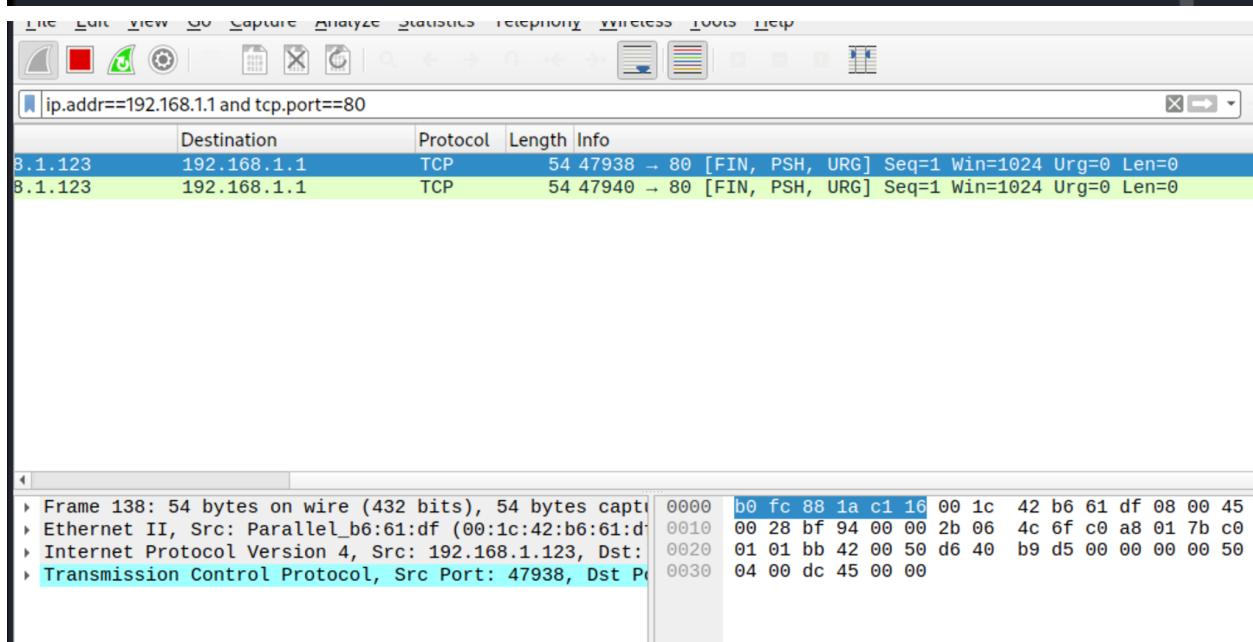


```
(parallels@kali-gnu-linux-2023) [~]
$ sudo nmap -sX 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:11 EST
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
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
```

ip.addr==192.168.1.1 and tcp.port==80						
No.	Time	Source	Destination	Protocol	Length	Info
138	80.880196057	192.168.1.123	192.168.1.1	TCP	54	47938 → 80 [FIN, PSH, URG] Seq=1
151	80.981981119	192.168.1.123	192.168.1.1	TCP	54	47940 → 80 [FIN, PSH, URG] Seq=1
2369	358.888432036	192.168.1.123	192.168.1.1	TCP	54	59782 → 80 [ACK] Seq=1 Ack=1 Win=
2375	358.895425426	192.168.1.1	192.168.1.123	TCP	54	80 → 59782 [RST] Seq=1 Win=0 Len=
2916	360.213116840	192.168.1.123	192.168.1.1	TCP	54	59787 → 80 [ACK] Seq=1 Ack=1 Win=
2958	360.220804440	192.168.1.1	192.168.1.123	TCP	54	80 → 59787 [RST] Seq=1 Win=0 Len=
3893	361.554009633	192.168.1.123	192.168.1.1	TCP	54	59789 → 80 [ACK] Seq=1 Ack=1 Win=
3968	361.561329398	192.168.1.1	192.168.1.123	TCP	54	80 → 59789 [RST] Seq=1 Win=0 Len=

Frame 138: 54 bytes on wire (432 bits), 54 bytes captured	
► Ethernet II, Src: Parallel_b6:61:df (00:1c:42:b6:61:d)	0000 b0 fc 88 1a c1 16 00 1c 42 b6 61 df 08 00 45 00
► Internet Protocol Version 4, Src: 192.168.1.123, Dst:	0010 00 28 bf 94 00 00 2b 06 4c 6f c0 a8 01 7b c0 a8
► Transmission Control Protocol, Src Port: 47938, Dst Port:	0020 01 01 bb 42 00 50 d6 40 b9 d5 00 00 00 00 50 29
►	0030 04 00 dc 45 00 00

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

ip.addr==192.168.1.1 and tcp.port==443						
No.	Time	Source	Destination	Protocol	Length	Info
100	79.462588363	192.168.1.123	192.168.1.1	TCP	54	47938 → 443 [FIN, PSH, URG] Seq=1
109	80.569076764	192.168.1.123	192.168.1.1	TCP	54	47940 → 443 [FIN, PSH, URG] Seq=1
2376	358.897801639	192.168.1.123	192.168.1.1	TCP	54	59782 → 443 [ACK] Seq=1 Ack=1 Win=
2398	358.902482732	192.168.1.1	192.168.1.123	TCP	54	443 → 59782 [RST] Seq=1 Win=0 Len=

This is for the port 443.

K.

ip.addr==192.168.1.1 and tcp						
No.	Time	Source	Destination	Protocol	Length	Info
95	79.462479529	192.168.1.123	192.168.1.1	TCP	54	47938 → 143 [FIN, PSH, URG] Seq=
96	79.462558988	192.168.1.123	192.168.1.1	TCP	54	47938 → 8080 [FIN, PSH, URG] Seq=
97	79.462565405	192.168.1.123	192.168.1.1	TCP	54	47938 → 199 [FIN, PSH, URG] Seq=
98	79.462570196	192.168.1.123	192.168.1.1	TCP	54	47938 → 3389 [FIN, PSH, URG] Seq=
99	79.462582821	192.168.1.123	192.168.1.1	TCP	54	47938 → 111 [FIN, PSH, URG] Seq=
100	79.462588363	192.168.1.123	192.168.1.1	TCP	54	47938 → 443 [FIN, PSH, URG] Seq=
101	79.462591738	192.168.1.123	192.168.1.1	TCP	54	47938 → 995 [FIN, PSH, URG] Seq=
102	79.462595405	192.168.1.123	192.168.1.1	TCP	54	47938 → 113 [FIN, PSH, URG] Seq=
103	79.462598113	192.168.1.123	192.168.1.1	TCP	54	47938 → 445 [FIN, PSH, URG] Seq=
104	79.462600405	192.168.1.123	192.168.1.1	TCP	54	47938 → 53 [FIN, PSH, URG] Seq=
105	80.568970681	192.168.1.123	192.168.1.1	TCP	54	47940 → 53 [FIN, PSH, URG] Seq=
106	80.569050306	192.168.1.123	192.168.1.1	TCP	54	47940 → 445 [FIN, PSH, URG] Seq=
107	80.569058098	192.168.1.123	192.168.1.1	TCP	54	47940 → 113 [FIN, PSH, URG] Seq=
108	80.569071056	192.168.1.123	192.168.1.1	TCP	54	47940 → 995 [FIN, PSH, URG] Seq=

Step 4 :

A.

Current filter: ip.addr==192.168.1.1 and tcp			
No.	Time	Source	Destination

B.

```
(parallels@kali-gnu-linux-2023)-[~]
$ sudo nmap -sU -p 99 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-11 12:26
EST
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).

PORT      STATE      SERVICE
99/udp    closed    metagram
MAC Address: B0:FC:88:1A:C1:16 (Unknown)

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

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 unreach)

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)~] 53, Dst Port: 3524
$ 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)
  ▶ Domain Name System (response)
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 1.1.168
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
219	272.234540525	192.168.1.123	192.168.1.1	DNS	84	Standard query 0x8c87 PTR 1.1.168
220	272.246764438	192.168.1.1	192.168.1.123	DNS	125	Standard query response 0x8c87 PT

UDP payload (83 bytes)

Domain Name System (response)

- Transaction ID: 0x05cc
- Flags: 0x8580 Standard query response, No error
- Questions: 1
- Answer RRs: 2
- Authority RRs: 0

E.

```
[parallel@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)
Additional RRs: 0
Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

ip.addr==192.168.1.123 and udp.port==67						
No.	Time	Source	Destination	Protocol	Length	Info
373	433.679662096	192.168.1.123	192.168.1.1	DHCP	286	DHCP Inform - Transaction ID 0x
374	433.691281628	192.168.1.1	192.168.1.123	DHCP	342	DHCP ACK - Transaction ID 0x

Step 5 :

A.

```
(parallels㉿kali-gnu-linux-2023) [~] 192.168.1.123
$ nmap -v scanme.nmap.org 192.168.1.1
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
                  client IP address: 255.255.255.255
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 details

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 details

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 details

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 details

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 details

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 details

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 details
```