

NMAP PORT SCANNING TECHNIQUES

This report provides a breakdown of multiple Nmap port scanning techniques performed in a controlled home lab environment. The objective is to understand how each scan works, interpret responses, and analyze packet level behavior using Wireshark.

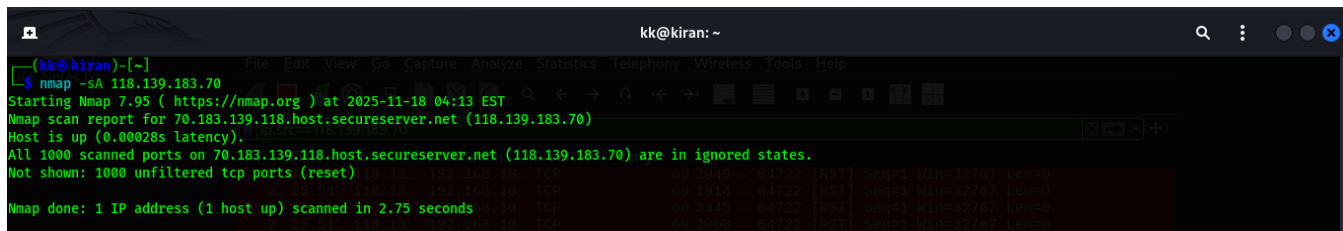
Introduction :

In this project, I performed multiple Nmap port scanning techniques in my home lab environment to understand how each scan works, how hosts respond, and how traffic appears in Wireshark.

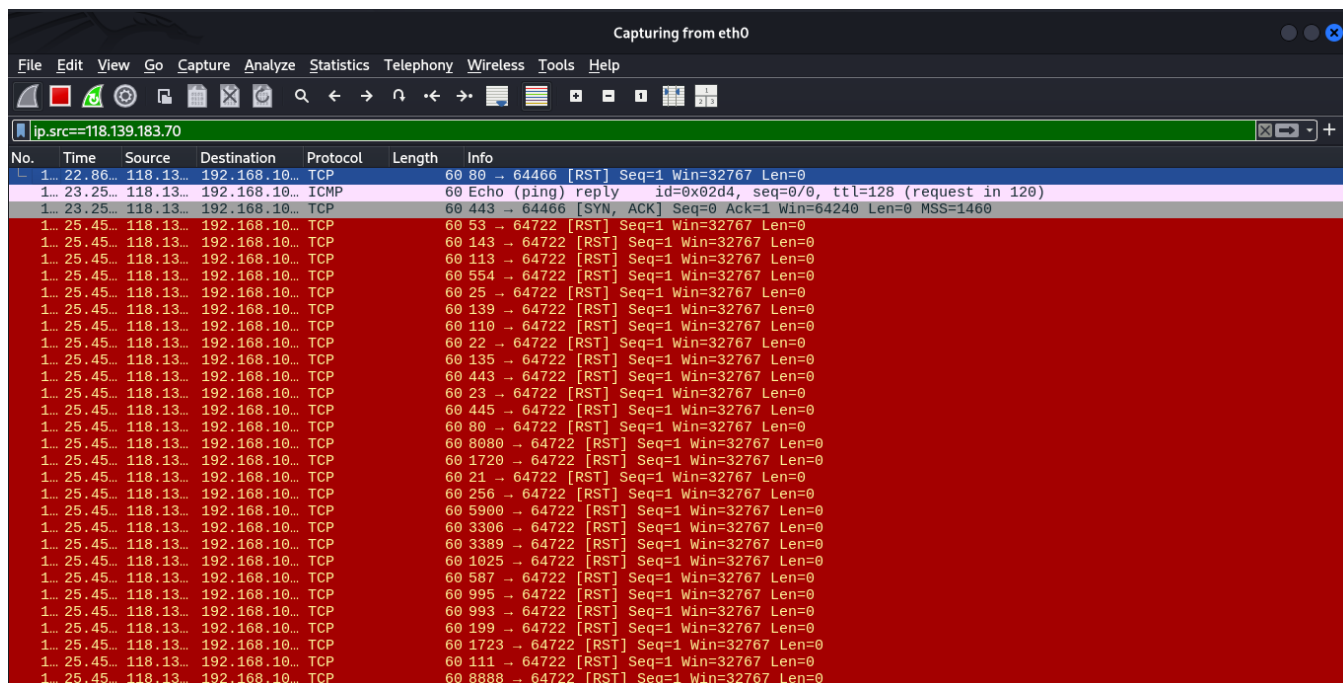
1) ACK Scan (-sA) :

ACK scan is used to identify firewall filtering rules. It helps determine whether ports are filtered or unfiltered.

`nmap -sA <Target ipaddress>`



```
kk@kiran: ~  
[kk@kiran]~  
$ nmap -sA 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:13 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.00028s latency).  
All 1000 scanned ports on 70.183.139.118.host.secureserver.net (118.139.183.70) are in ignored states.  
Not shown: 1000 unfiltered tcp ports (reset)  
Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```

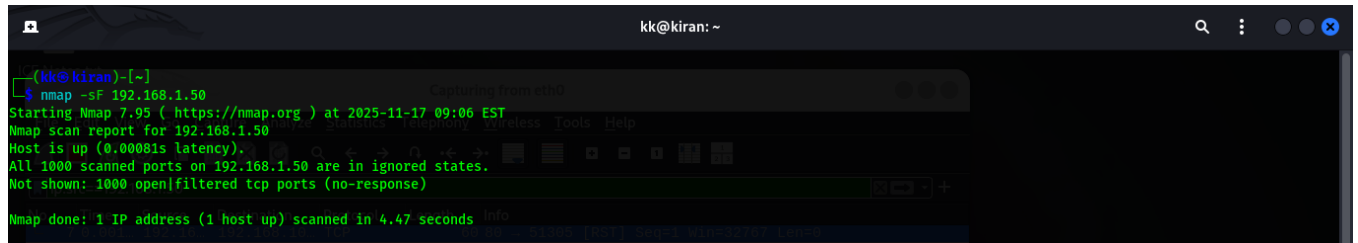


No.	Time	Source	Destination	Protocol	Length	Info
1...	22.86...	118.13...	192.168.10...	TCP	60	80 → 64466 [RST] Seq=1 Win=32767 Len=0
1...	23.25...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0x02d4, seq=0/0, ttl=128 (request in 120)
1...	23.25...	118.13...	192.168.10...	TCP	60	443 → 64466 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1...	25.45...	118.13...	192.168.10...	TCP	60	53 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	143 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	113 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	554 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	25 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	139 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	110 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	22 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	135 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	443 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	23 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	445 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	80 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	8080 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	1720 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	21 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	256 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	5900 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	3306 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	3389 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	1025 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	587 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	995 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	993 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	199 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	1723 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	111 → 64722 [RST] Seq=1 Win=32767 Len=0
1...	25.45...	118.13...	192.168.10...	TCP	60	8888 → 64722 [RST] Seq=1 Win=32767 Len=0

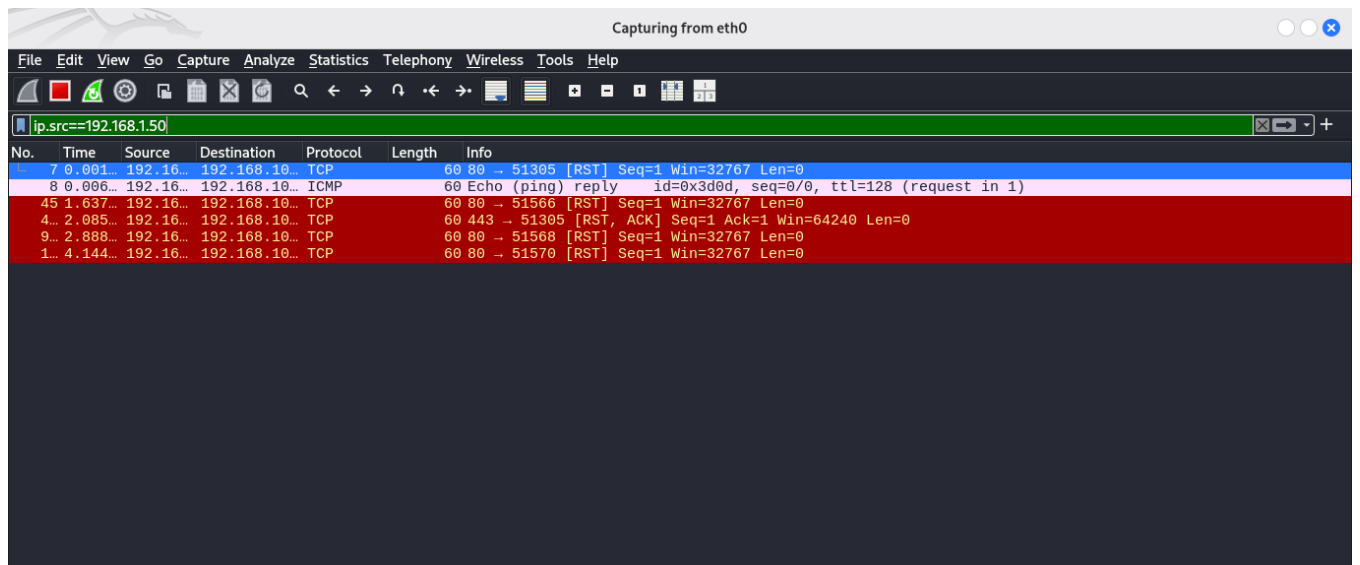
2) FIN Scan :

- Stealth scanning (avoids detection on some systems)
- Discovering **open vs closed ports** based on response behavior
- Testing systems that follow RFC 793 behavior

Command - `nmap -sF <Target ipaddress>`



```
kk@kiran: ~  
[~]  
$ nmap -sF 192.168.1.50  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 09:06 EST  
Nmap scan report for 192.168.1.50  
Host is up (0.00081s latency).  
All 1000 scanned ports on 192.168.1.50 are in ignored states.  
Not shown: 1000 open|filtered tcp ports (no-response)  
Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
```



No.	Time	Source	Destination	Protocol	Length	Info
7	0.001...	192.16...	192.168.10...	TCP	60	80 → 51305 [RST] Seq=1 Win=32767 Len=0
8	0.006...	192.16...	192.168.10...	ICMP	60	Echo (ping) reply id=0x3d0d, seq=0/0, ttl=128 (request in 1)
45	1.637...	192.16...	192.168.10...	TCP	60	80 → 51566 [RST] Seq=1 Win=32767 Len=0
4...	2.085...	192.16...	192.168.10...	TCP	60	443 → 51305 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
9...	2.888...	192.16...	192.168.10...	TCP	60	80 → 51568 [RST] Seq=1 Win=32767 Len=0
1...	4.144...	192.16...	192.168.10...	TCP	60	80 → 51570 [RST] Seq=1 Win=32767 Len=0

3) NULL Scan :

- Stealth scanning
- Identifying how targets respond to packets with **no flags**
- Detecting open ports on systems that ignore malformed packets

Command - `nmap -sN <Target ipaddress>`

```
kk@kiran: ~  
--(kk@kiran)-[~]  
$ nmap -sN 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:23 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.00009s latency).  
All 1000 scanned ports on 70.183.139.118.host.secureserver.net (118.139.183.70) are in ignored states.  
Not shown: 1000 open|filtered tcp ports (no-response)  
Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==118.139.183.70

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000...	118.13...	192.168.10...	TCP	60	80 → 59309 [RST] Seq=1 Win=32767 Len=0
18	0.361...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0x82d7, seq=0/0, ttl=128 (request in 1)
19	0.365...	118.13...	192.168.10...	TCP	60	443 → 59309 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
45	1.372...	118.13...	192.168.10...	TCP	60	80 → 59570 [RST] Seq=1 Win=32767 Len=0
9...	2.624...	118.13...	192.168.10...	TCP	60	80 → 59572 [RST] Seq=1 Win=32767 Len=0
1...	3.877...	118.13...	192.168.10...	TCP	60	80 → 59574 [RST] Seq=1 Win=32767 Len=0

3) Protocol Scan :

- Host discovery (checking if a machine is up)
- Network mapping and live host scanning

`nmap -sO <Target ipaddress>`

```
kk@kiran: ~  
$ nmap -sO 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:25 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.044s latency).  
Not shown: 252 filtered n/a protocols (proto-unreach)  
PROTOCOL STATE SERVICE  
1 open icmp  
6 open tcp  
17 open|filtered udp  
47 open|filtered gre  
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

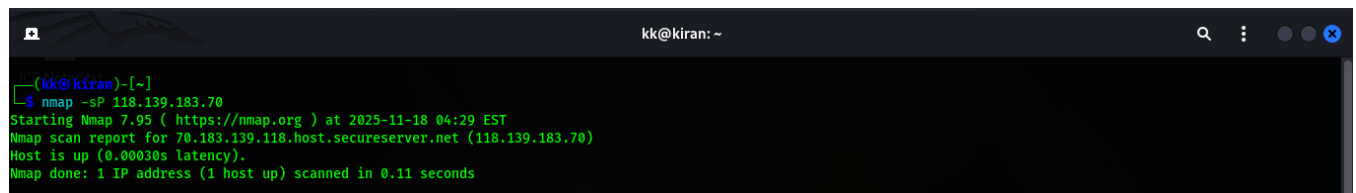
ip.src==118.139.183.70

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000...	118.13...	192.168.10...	TCP	60	80 → 34932 [RST] Seq=1 Win=32767 Len=0
1...	0.115...	118.13...	192.168.10...	TCP	60	80 → 35188 [RST] Seq=1 Win=32767 Len=0
5...	0.357...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0x5d6e, seq=0/0, ttl=128 (request in 1)
5...	0.367...	118.13...	192.168.10...	TCP	60	443 → 34932 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5...	0.442...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0x8bfc, seq=0/0, ttl=128 (request in 22)

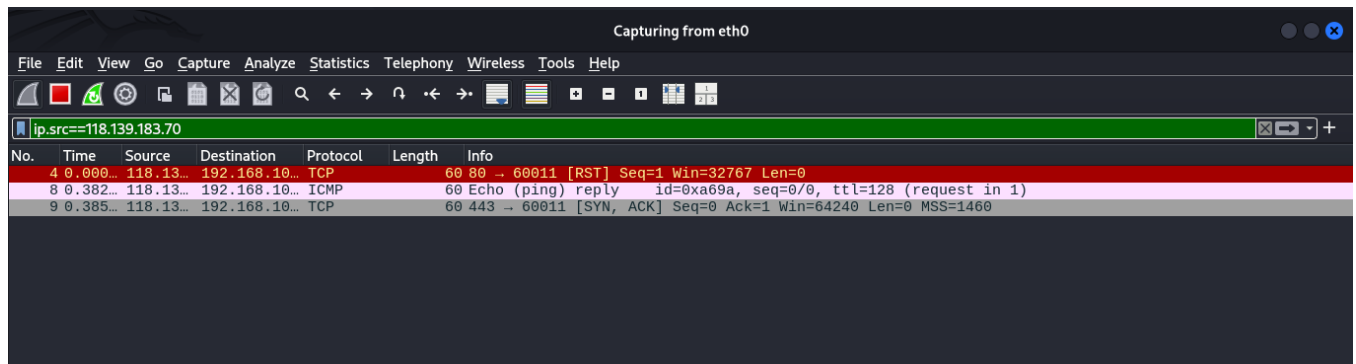
4) Ping Scan :

- Host discovery (checking if a machine is up)
- Network mapping and live host scanning

Command - `nmap -sP <Target ipaddress>`



```
kk@kiran: ~  
$ nmap -sP 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:29 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.00030s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```



Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==118.139.183.70

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000...	118.13...	192.168.10...	TCP	60	80 → 60011 [RST] Seq=1 Win=32767 Len=0
8	0.382...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0xa69a, seq=0/0, ttl=128 (request in 1)
9	0.385...	118.13...	192.168.10...	TCP	60	443 → 60011 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

6) SYN Scan :

- Fast, stealthy port scanning
- Half-open scan avoids completing TCP handshake
- Identifying **open/closed/filtered** ports accurately

Command - Nmap -sS <Target ipaddress>

```
kk@kiran: ~  
$ nmap -sS 10.216.136.193  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:32 EST  
Nmap scan report for 10.216.136.193  
Host is up (0.0014s latency).  
Not shown: 995 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realservice  
912/tcp   open  apex-mesh  
  
Nmap done: 1 IP address (1 host up) scanned in 6.24 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.216.136.193

No.	Time	Source	Destination	Protocol	Length	Info
8...	116.6...	10.216...	192.168.10...	TCP	60	1 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	1 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	100 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	100 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	1000 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	1000 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10000 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10000 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10001 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10001 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	10002 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	10002 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
6...	112.5...	10.216...	192.168.10...	TCP	60	10003 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
5...	110.2...	10.216...	192.168.10...	TCP	60	10004 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
5...	110.3...	10.216...	192.168.10...	TCP	60	10004 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10009 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10009 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	114.5...	10.216...	192.168.10...	TCP	60	1001 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	116.6...	10.216...	192.168.10...	TCP	60	1001 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
6...	112.5...	10.216...	192.168.10...	TCP	60	10010 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
6...	112.5...	10.216...	192.168.10...	TCP	60	10010 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	10012 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	10012 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	1002 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	1002 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	114.5...	10.216...	192.168.10...	TCP	60	10024 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	116.6...	10.216...	192.168.10...	TCP	60	10024 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10025 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7...	112.5...	10.216...	192.168.10...	TCP	60	10025 → 53923 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
8...	116.6...	10.216...	192.168.10...	TCP	60	1007 → 53921 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

7) TCP Scan :

- Scanning when SYN scan is **not allowed** or requires privileges
- Fully completes TCP handshake to identify open ports
- Reliable but less stealthy

Command - `nmap -sT <Target ipaddress>`

```
Host is up (0.00070s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

(kk@kiran)-[~]
$ nmap -sT 192.168.1.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:55 EST
Nmap scan report for 192.168.1.50
Host is up (0.022s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
50002/tcp open  iiimfsf

Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

```
Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.50

No. Time Source Destination Protocol Length Info
4... 87.73... 192.16... 192.168.10... TCP 60 1197 → 56706 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.73... 192.16... 192.168.10... TCP 60 1190 → 52542 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.73... 192.16... 192.168.10... TCP 60 8085 → 55722 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.73... 192.16... 192.168.10... TCP 60 2040 → 58072 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.75... 192.16... 192.168.10... TCP 60 3766 → 37220 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.75... 192.16... 192.168.10... TCP 60 3800 → 37880 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.75... 192.16... 192.168.10... TCP 60 4279 → 49604 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.75... 192.16... 192.168.10... TCP 60 10010 → 56058 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.75... 192.16... 192.168.10... TCP 60 28201 → 43078 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 1113 → 42918 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 6346 → 38642 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 7676 → 42326 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 49154 → 39182 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 5822 → 34058 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 65000 → 60578 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 3325 → 55918 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 1309 → 59746 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 3878 → 33579 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 10628 → 44454 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 1059 → 44652 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 61532 → 59826 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 5226 → 38462 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 1032 → 41454 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 3301 → 45960 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.79... 192.16... 192.168.10... TCP 60 1192 → 49440 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.80... 192.16... 192.168.10... TCP 60 8800 → 49142 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.80... 192.16... 192.168.10... TCP 60 16016 → 50538 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.80... 192.16... 192.168.10... TCP 60 787 → 37998 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.81... 192.16... 192.168.10... TCP 60 389 → 42378 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.81... 192.16... 192.168.10... TCP 60 6901 → 33690 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4... 87.81... 192.16... 192.168.10... TCP 60 5950 → 55518 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
```

8) UDP Scan :

- Discovering opened **UDP-based services** (DNS, DHCP, SNMP)
- Finding services not detected by TCP scans
- Network enumeration

Command - `nmap -sU <Target ipaddress>`

```
kk@kiran: ~  
$ nmap -sU 192.168.1.50  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 08:58 EST  
Nmap scan report for 192.168.1.50  
Host is up (0.0043s latency).  
Not shown: 997 open|filtered udp ports (no-response)  
PORT      STATE SERVICE  
53/udp    open  domain  
111/udp   open  rpcbind  
2049/udp  open  nfs  
  
Nmap done: 1 IP address (1 host up) scanned in 4.57 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.50

No.	Time	Source	Destination	Protocol	Length	Info
1...	3.585...	192.16...	192.168.10...	TFTP	379	Unknown (0x80f0)
1...	3.585...	192.16...	192.168.10...	TFTP	271	Unknown (0x0191)
1...	3.585...	192.16...	192.168.1...	ICMP	407	Destination unreachable (Port unreachable)
1...	3.585...	192.16...	192.168.1...	ICMP	299	Destination unreachable (Port unreachable)
1...	3.587...	192.16...	192.168.10...	TFTP	379	Unknown (0x0191)
1...	3.587...	192.16...	192.168.1...	ICMP	407	Destination unreachable (Port unreachable)
1...	3.594...	192.16...	192.168.10...	TFTP	104	Option Acknowledgement, 0=, \001=\001, \001=, \aversion\004bind=, \020=\0030\, \020=\003, =, =, \...
1...	3.594...	192.16...	192.168.1...	ICMP	132	Destination unreachable (Port unreachable)
1...	3.595...	192.16...	192.168.10...	TFTP	60	Unknown (0x0000)
1...	3.595...	192.16...	192.168.10...	TFTP	299	Unknown (0x0000)
1...	4.190...	192.16...	192.168.10...	TFTP	74	Unknown (0x72fe)
1...	4.190...	192.16...	192.168.1...	ICMP	102	Destination unreachable (Port unreachable)
1...	4.194...	192.16...	192.168.10...	TFTP	66	Unknown (0x3eec)
2...	52.69...	192.16...	192.168.10...	TCP	60	80 -> 44235 [RST] Seq=1 Win=32767 Len=0
2...	52.70...	192.16...	192.168.10...	ICMP	60	Echo (ping) reply id=0x1ada, seq=0/0, ttl=128 (request in 2117)
2...	54.39...	192.16...	192.168.10...	TCP	60	80 -> 44496 [RST] Seq=1 Win=32767 Len=0
2...	54.41...	192.16...	192.168.10...	UDP	66	2049 -> 44491 Len=24
2...	54.41...	192.16...	192.168.1...	ICMP	94	Destination unreachable (Port unreachable)
2...	54.41...	192.16...	192.168.10...	NFS	66	V2 NULL Reply (Call In 2197)
2...	54.41...	192.16...	192.168.1...	ICMP	94	Destination unreachable (Port unreachable)
2...	54.63...	192.16...	192.168.10...	Portmap	74	V104316 proc=0 Reply (Call In 2324)
2...	54.63...	192.16...	192.168.10...	RPC	66	Continuation
2...	54.63...	192.16...	192.168.1...	ICMP	102	Destination unreachable (Port unreachable)
2...	54.64...	192.16...	192.168.1...	ICMP	94	Destination unreachable (Port unreachable)
2...	54.75...	192.16...	192.168.10...	TCP	60	443 -> 44235 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2...	55.22...	192.16...	192.168.10...	DNS	104	Standard query response 0x0006 TXT version.bind TXT NS version.bind
2...	55.22...	192.16...	192.168.1...	ICMP	132	Destination unreachable (Port unreachable)
2...	55.22...	192.16...	192.168.10...	DNS	60	Server status request response 0x0000 Not implemented
2...	55.22...	192.16...	192.168.1...	ICMP	82	Destination unreachable (Port unreachable)
2...	55.22...	192.16...	192.168.10...	DNS	299	Standard query response 0x0000 PTR _services._udp.local NS F.ROOT-SERVERS.NET NS J.ROOT-SER...
3...	56.47...	192.16...	192.168.10...	TCP	60	80 -> 44498 [RST] Seq=1 Win=32767 Len=0

9) Windows Scan :

- Detecting open ports using TCP window size differences
- Works well on **Windows-based systems**
- Alternative to SYN/FIN/NULL scans

Command - `nmap -sW <Target ipaddress>`

```
kk@kiran: ~  
[kk@kiran]~  
$ nmap -sW 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:36 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.00025s latency).  
  
PORT      STATE SERVICE  
1/tcp     open  tcpmux  
3/tcp     open  compressnet  
4/tcp     open  unknown  
6/tcp     open  unknown  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
20/tcp    open  ftp-data  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
24/tcp    open  priv-mail  
25/tcp    open  smtp  
26/tcp    open  rsftp  
30/tcp    open  unknown  
32/tcp    open  unknown  
33/tcp    open  dsp  
37/tcp    open  time  
42/tcp    open  nameserver  
43/tcp    open  whois  
49/tcp    open  tacacs  
53/tcp    open  domain  
70/tcp    open  gopher  
79/tcp    open  finger  
80/tcp    open  http  
81/tcp    open  hosts2-ns  
82/tcp    open  xfer  
83/tcp    open  mit-ml-dev
```

```
Capturing from eth0  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
ip.src==118.139.183.70  
No. Time Source Destination Protocol Length Info  
1.. 0.307.. 118.13.. 192.168.10.. TCP 60 20031 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 1080 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 8443 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 1248 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 3369 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 5903 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.308.. 118.13.. 192.168.10.. TCP 60 1047 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.309.. 118.13.. 192.168.10.. TCP 60 10001 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.309.. 118.13.. 192.168.10.. TCP 60 8090 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.309.. 118.13.. 192.168.10.. TCP 60 4900 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.309.. 118.13.. 192.168.10.. TCP 60 1152 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 6901 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 40193 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 49160 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 5100 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 4003 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.310.. 118.13.. 192.168.10.. TCP 60 888 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.311.. 118.13.. 192.168.10.. TCP 60 6001 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.311.. 118.13.. 192.168.10.. TCP 60 42 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.311.. 118.13.. 192.168.10.. TCP 60 13 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.311.. 118.13.. 192.168.10.. TCP 60 9103 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.312.. 118.13.. 192.168.10.. TCP 60 5815 -> 43465 [RST] Seq=1 Win=32767 Len=0  
1.. 0.312.. 118.13.. 192.168.10.. TCP 60 8333 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.312.. 118.13.. 192.168.10.. TCP 60 31038 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.312.. 118.13.. 192.168.10.. TCP 60 992 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.313.. 118.13.. 192.168.10.. TCP 60 1600 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.313.. 118.13.. 192.168.10.. TCP 60 9876 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.313.. 118.13.. 192.168.10.. TCP 60 42510 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.313.. 118.13.. 192.168.10.. TCP 60 44443 -> 43465 [RST] Seq=1 Win=32767 Len=0  
2.. 0.358.. 118.13.. 192.168.10.. ICMP 60 Echo (ping) reply id=0x89ae, seq=0/0, ttl=128 (request in 1)  
2.. 0.360.. 118.13.. 192.168.10.. TCP 60 443 -> 43209 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```

10) XMAS Scan :

- Stealth scanning with FIN + PSH + URG flags
- Detecting open/closed ports on RFC-compliant systems
- Avoiding some IDS/IPS detection methods

Command - `nmap -sX <Target ipaddress>`

```
kk@kiran: ~  
[kk@kiran]~  
$ nmap -sX 118.139.183.70  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 04:40 EST  
Nmap scan report for 70.183.139.118.host.secureserver.net (118.139.183.70)  
Host is up (0.00059s latency).  
All 1000 scanned ports on 70.183.139.118.host.secureserver.net (118.139.183.70) are in ignored states.  
Not shown: 1000 open|filtered tcp ports (no-response)  
Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==118.139.183.70

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000...	118.13...	192.168.10...	TCP	60	80 → 64981 [RST] Seq=1 Win=32767 Len=0
18	0.401...	118.13...	192.168.10...	TCP	60	443 → 64981 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
20	0.406...	118.13...	192.168.10...	ICMP	60	Echo (ping) reply id=0xc725, seq=0/0, ttl=128 (request in 1)
42	1.396...	118.13...	192.168.10...	TCP	60	80 → 65162 [RST] Seq=1 Win=32767 Len=0
9...	2.651...	118.13...	192.168.10...	TCP	60	80 → 65164 [RST] Seq=1 Win=32767 Len=0
1...	3.905...	118.13...	192.168.10...	TCP	60	80 → 65166 [RST] Seq=1 Win=32767 Len=0

11) ICMP Ping :

- Host discovery using **ICMP Echo Request**
- Detecting reachable hosts in a network
- Network reconnaissance

Command - `nmap -PI <Target ip address>`

```
kk@kiran: ~  
--(kk@kiran)~[~]-- Capture Analyze Statistics Telephony Wireless Tools Help  
$ nmap -PI 10.216.136.93  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 01:36 EST  
Nmap scan report for 10.216.136.93  
Host is up (0.035s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
5060/tcp  filtered sip  
MAC Address: 16:C9:BE:37:6F:1A (Unknown)  
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src==10.216.136.93						
No.	Time	Source	Destination	Protocol	Length	Info
35	5.971...	10.216...	10.216.136...	TCP	60	135 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	5.975...	10.216...	10.216.136...	TCP	60	995 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39	5.976...	10.216...	10.216.136...	TCP	60	199 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	5.979...	10.216...	10.216.136...	TCP	60	256 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41	5.979...	10.216...	10.216.136...	TCP	60	554 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	5.979...	10.216...	10.216.136...	TCP	60	445 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	5.979...	10.216...	10.216.136...	TCP	60	587 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	5.979...	10.216...	10.216.136...	TCP	60	3389 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	5.979...	10.216...	10.216.136...	TCP	60	5900 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	5.979...	10.216...	10.216.136...	TCP	60	993 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	5.980...	10.216...	10.216.136...	TCP	60	113 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	5.985...	10.216...	10.216.136...	TCP	60	53 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
71	5.991...	10.216...	10.216.136...	TCP	60	139 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72	5.991...	10.216...	10.216.136...	TCP	60	8080 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	5.991...	10.216...	10.216.136...	TCP	60	1720 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74	5.991...	10.216...	10.216.136...	TCP	60	23 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
77	5.995...	10.216...	10.216.136...	TCP	60	111 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	5.995...	10.216...	10.216.136...	TCP	60	1723 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	5.995...	10.216...	10.216.136...	TCP	60	443 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	5.995...	10.216...	10.216.136...	TCP	60	3306 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
81	5.995...	10.216...	10.216.136...	TCP	60	21 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
88	5.998...	10.216...	10.216.136...	TCP	60	80 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89	5.998...	10.216...	10.216.136...	TCP	60	22 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
90	6.000...	10.216...	10.216.136...	TCP	60	25 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91	6.000...	10.216...	10.216.136...	TCP	60	110 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
92	6.000...	10.216...	10.216.136...	TCP	60	16080 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
93	6.001...	10.216...	10.216.136...	TCP	60	27356 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	6.001...	10.216...	10.216.136...	TCP	60	8888 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	6.001...	10.216...	10.216.136...	TCP	60	143 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	6.002...	10.216...	10.216.136...	TCP	60	1025 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
97	6.003...	10.216...	10.216.136...	TCP	60	84 → 60029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

12) SYN Ping :

- Host discovery using SYN packets
- Useful when ICMP is blocked
- Detecting active hosts behind firewalls

Command - `nmap -PS <Target ip address>`

```
kk@kiran: ~  
$ nmap -PS 10.216.136.93  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 01:38 EST  
Nmap scan report for 10.216.136.93  
Host is up (0.012s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE      SERVICE  
5060/tcp  filtered  sip  
MAC Address: 16:C9:BE:37:6F:1A (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
```

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src==10.216.136.93						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000...	10.216...	224.0.0.251	MDNS	191	Standard query 0x0000 ANY Android.local, "QU" question ANY Android.local, "QU" question ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local
3	0.215...	10.216...	224.0.0.251	MDNS	191	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local
6	0.414...	10.216...	224.0.0.251	MDNS	191	Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local
21	0.555...	10.216...	10.216.136...	TCP	60	554 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	0.555...	10.216...	10.216.136...	TCP	60	1025 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.557...	10.216...	10.216.136...	TCP	60	256 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	0.558...	10.216...	10.216.136...	TCP	60	110 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.558...	10.216...	10.216.136...	TCP	60	445 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.560...	10.216...	10.216.136...	TCP	60	443 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.560...	10.216...	10.216.136...	TCP	60	25 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.561...	10.216...	10.216.136...	TCP	60	1723 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.562...	10.216...	10.216.136...	TCP	60	8080 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	0.562...	10.216...	10.216.136...	TCP	60	995 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51	0.570...	10.216...	10.216.136...	TCP	60	993 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
52	0.570...	10.216...	10.216.136...	TCP	60	113 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53	0.570...	10.216...	10.216.136...	TCP	60	587 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	0.570...	10.216...	10.216.136...	TCP	60	1720 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	0.573...	10.216...	10.216.136...	TCP	60	80 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	0.573...	10.216...	10.216.136...	TCP	60	135 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	0.573...	10.216...	10.216.136...	TCP	60	3306 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	0.573...	10.216...	10.216.136...	TCP	60	53 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	0.573...	10.216...	10.216.136...	TCP	60	22 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	0.573...	10.216...	10.216.136...	TCP	60	199 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	0.573...	10.216...	10.216.136...	TCP	60	8888 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	0.574...	10.216...	10.216.136...	TCP	60	111 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	0.574...	10.216...	10.216.136...	TCP	60	143 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64	0.574...	10.216...	10.216.136...	TCP	60	21 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	0.575...	10.216...	10.216.136...	TCP	60	5900 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66	0.576...	10.216...	10.216.136...	TCP	60	3389 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
67	0.576...	10.216...	10.216.136...	TCP	60	139 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68	0.578...	10.216...	10.216.136...	TCP	60	23 → 44036 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

13) TCP Ping :

- Host discovery using TCP ACK packets
- Works even when ICMP is filtered
- Identifying ALIVE hosts without scanning ports

Command - `nmap -PT <Target ip address>`

```
kk@kiran: ~  
$ nmap -PT 10.216.136.93  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 01:31 EST  
Nmap scan report for 10.216.136.93  
Host is up (0.036s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
5060/tcp  filtered sip  
MAC Address: 16:C9:BE:37:6F:1A (Unknown)  
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

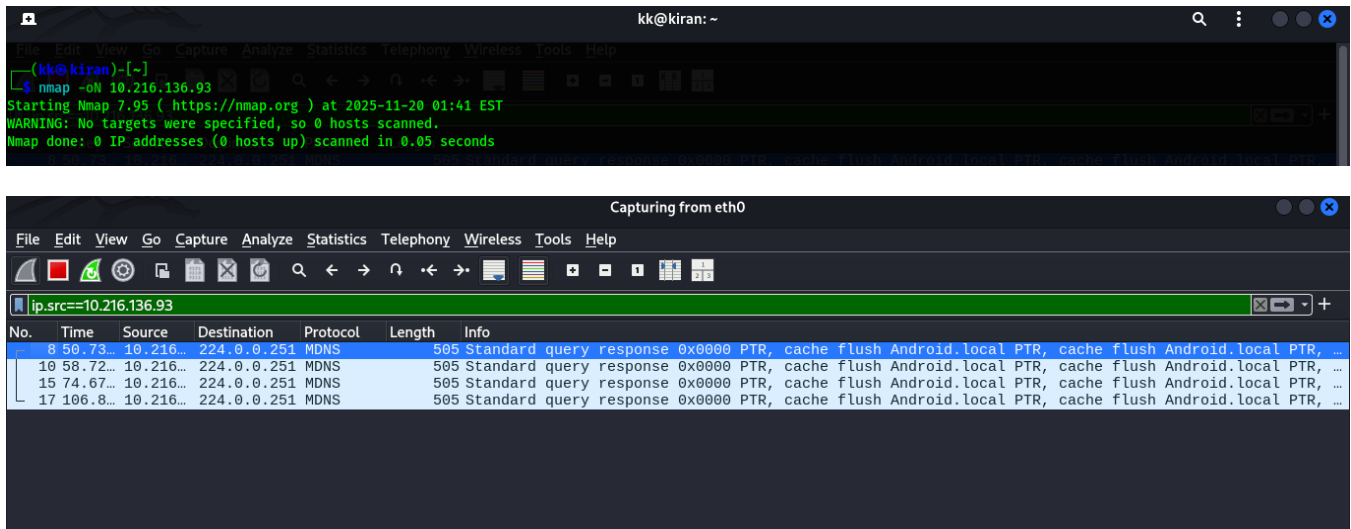
ip.src==10.216.136.93

No.	Time	Source	Destination	Protocol	Length	Info
2...	10.01...	10.216...	10.216.136...	TCP	60	1 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.49...	10.216...	10.216.136...	TCP	60	100 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.35...	10.216...	10.216.136...	TCP	60	1000 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.43...	10.216...	10.216.136...	TCP	60	10000 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4...	10.08...	10.216...	10.216.136...	TCP	60	10001 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.25...	10.216...	10.216.136...	TCP	60	10002 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.36...	10.216...	10.216.136...	TCP	60	10003 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.50...	10.216...	10.216.136...	TCP	60	10004 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.51...	10.216...	10.216.136...	TCP	60	10009 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4...	10.07...	10.216...	10.216.136...	TCP	60	1001 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8...	10.18...	10.216...	10.216.136...	TCP	60	10010 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6...	10.14...	10.216...	10.216.136...	TCP	60	10012 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.57...	10.216...	10.216.136...	TCP	60	1002 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5...	10.11...	10.216...	10.216.136...	TCP	60	10024 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.48...	10.216...	10.216.136...	TCP	60	10025 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.44...	10.216...	10.216.136...	TCP	60	1007 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5...	10.10...	10.216...	10.216.136...	TCP	60	10082 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.46...	10.216...	10.216.136...	TCP	60	1009 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4...	10.09...	10.216...	10.216.136...	TCP	60	1010 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9...	10.20...	10.216...	10.216.136...	TCP	60	1011 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.51...	10.216...	10.216.136...	TCP	60	10180 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9...	10.20...	10.216...	10.216.136...	TCP	60	1021 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9...	10.23...	10.216...	10.216.136...	TCP	60	10215 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9...	10.20...	10.216...	10.216.136...	TCP	60	1022 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.44...	10.216...	10.216.136...	TCP	60	1023 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.35...	10.216...	10.216.136...	TCP	60	1024 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2...	10.01...	10.216...	10.216.136...	TCP	60	10243 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	9.948...	10.216...	10.216.136...	TCP	60	1025 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2...	10.01...	10.216...	10.216.136...	TCP	60	1026 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.50...	10.216...	10.216.136...	TCP	60	1027 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1...	11.30...	10.216...	10.216.136...	TCP	60	1028 → 42554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

14) Normal Output :

- Saving scan results in **human-readable format**
- Good for reports and documentation
- Easily readable in text editors

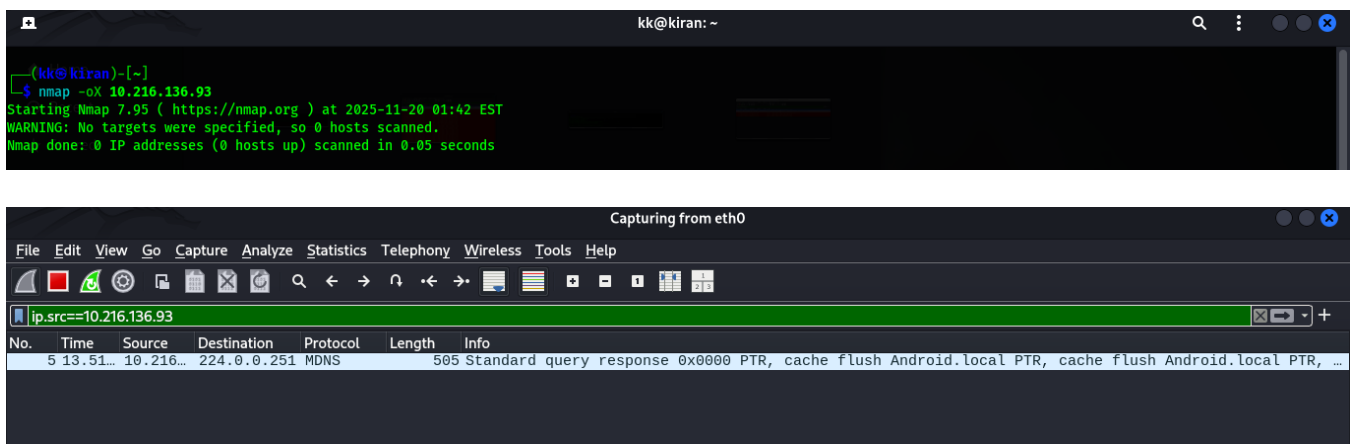
Command - `nmap -oN <Target ip address>`



15) XML Output :

- Saving scan results in XML format
- Automation, scripting, and log parsing
- Importing results into security tools (e.g., Nessus, OpenVAS dashboards)

Command - `nmap -oX <Target ip address>`



Summary Table :

Scan Type	Purpose	Typical Response / Behavior
ACK Scan (-sA)	Detect firewall filtering rules	RST = unfiltered, No response = filtered
FIN Scan (-sF)	Stealth scan; identify open/closed ports	No response = open/filtered, RST = closed
NULL Scan (-sN)	Stealth scan with no flags	No response = open/filtered, RST = closed
Protocol Scan (-sO)	Discover supported IP protocols	ICMP unreachable or protocol responses
Ping Scan (-sP)	Check if host is up	ICMP echo reply = host alive
SYN Scan (-sS)	Fast, stealthy half-open scan	SYN/ACK = open, RST = closed
TCP Connect Scan (-sT)	Full connection scan (3-way handshake)	Full connect = open, RST = closed
UDP Scan (-sU)	Identify UDP services	No response = open/filtered, ICMP unreachable = closed
Windows Scan (-sW)	Detect open/closed ports using Windows TCP	Closed ports send RST with specific window size
XMAS Scan (-sX)	FIN+PSH+URG stealth scan	No response = open/filtered, RST = closed
ICMP Ping (-PI)	Host discovery using ICMP	ICMP echo reply = host reachable
SYN Ping (-PS)	Host discovery with SYN packets	SYN/ACK or RST = host alive
TCP Ping (-PT)	Host discovery with TCP ACK packets	RST = host alive
Normal Output (-oN)	Save human-readable scan output	Stores readable results in .txt file
XML Output (-oX)	Save output in XML format	Used for automation, scripts, parsing tools

Conclusion : This project helped me understand how different port scanning techniques work, how firewalls respond, and how traffic appears inside Wireshark. This knowledge is essential for both offensive and defensive cybersecurity roles.