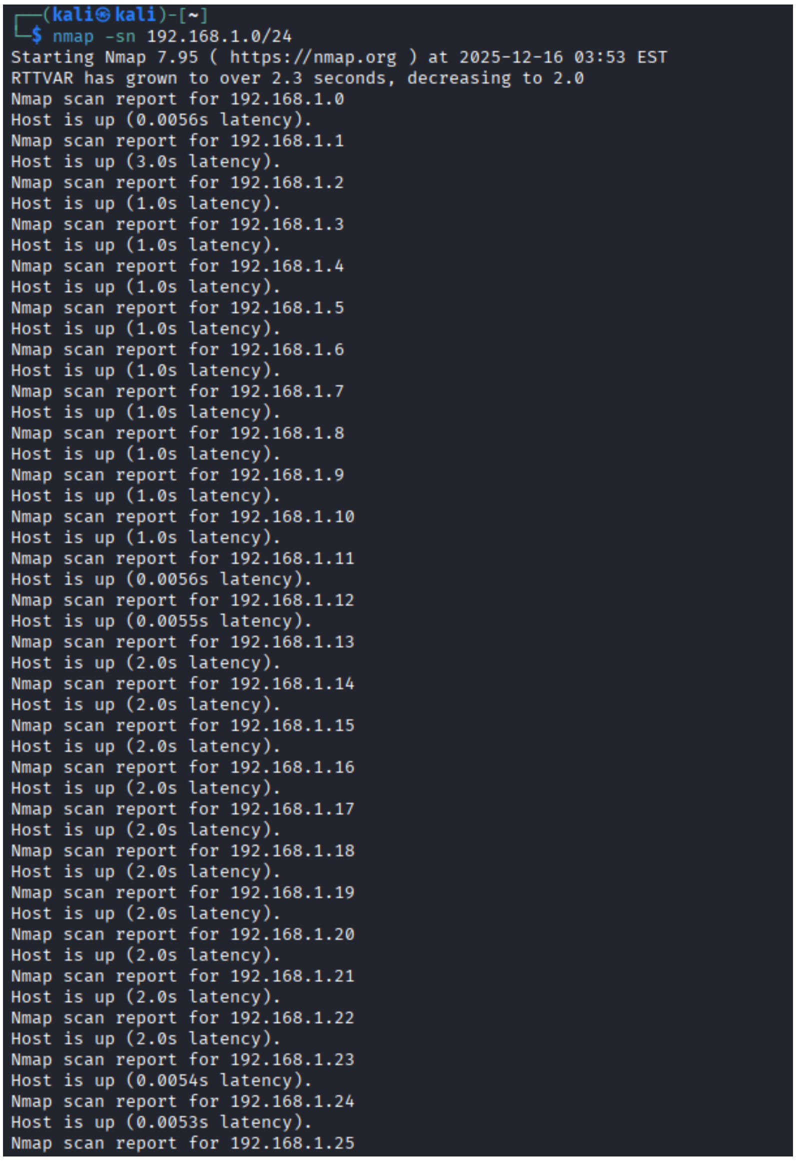
TASK 1:

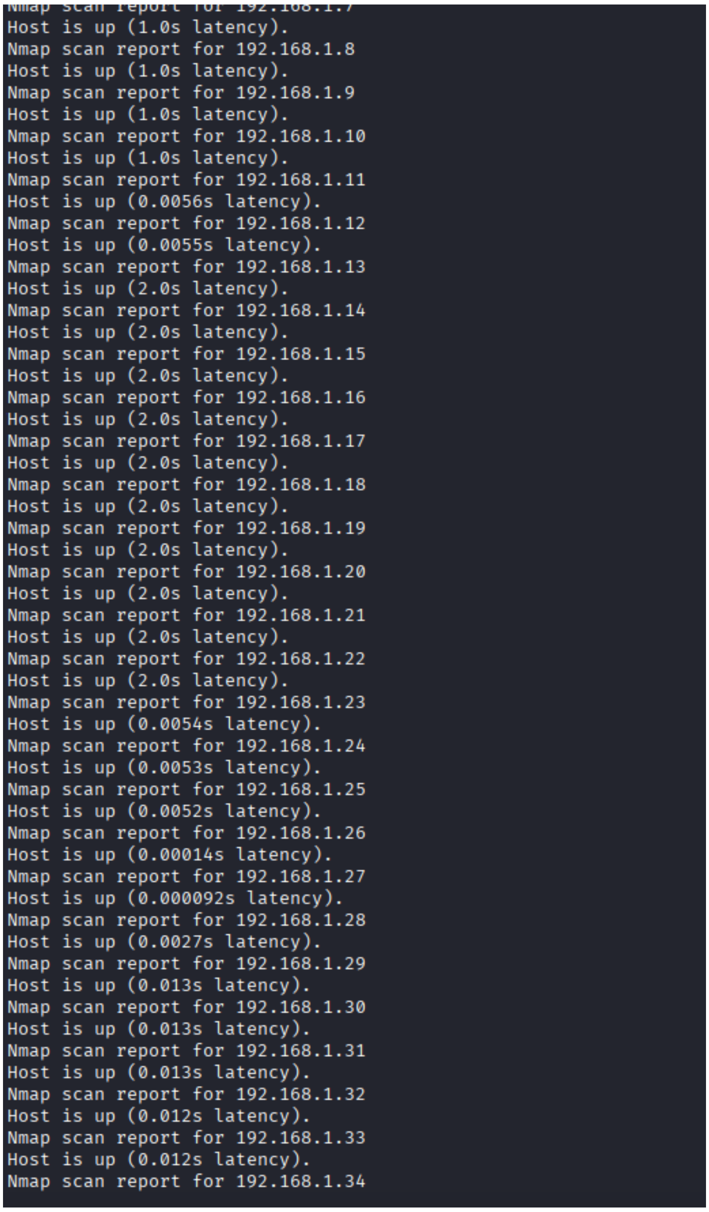
NMAP COMMANDS:

1.nmap -sn 192.168.1.0/24

Scans Entire subnet for hosts.



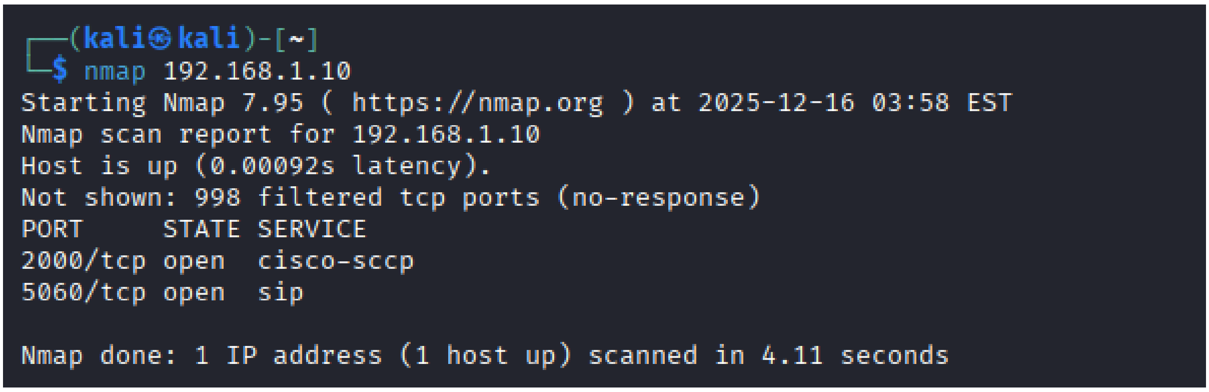
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 03:53 EST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.1.0
Host is up (0.0056s latency).
Nmap scan report for 192.168.1.1
Host is up (3.0s latency).
Nmap scan report for 192.168.1.2
Host is up (1.0s latency).
Nmap scan report for 192.168.1.3
Host is up (1.0s latency).
Nmap scan report for 192.168.1.4
Host is up (1.0s latency).
Nmap scan report for 192.168.1.5
Host is up (1.0s latency).
Nmap scan report for 192.168.1.6
Host is up (1.0s latency).
Nmap scan report for 192.168.1.7
Host is up (1.0s latency).
Nmap scan report for 192.168.1.8
Host is up (1.0s latency).
Nmap scan report for 192.168.1.9
Host is up (1.0s latency).
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).
Nmap scan report for 192.168.1.11
Host is up (0.0056s latency).
Nmap scan report for 192.168.1.12
Host is up (0.0055s latency).
Nmap scan report for 192.168.1.13
Host is up (2.0s latency).
Nmap scan report for 192.168.1.14
Host is up (2.0s latency).
Nmap scan report for 192.168.1.15
Host is up (2.0s latency).
Nmap scan report for 192.168.1.16
Host is up (2.0s latency).
Nmap scan report for 192.168.1.17
Host is up (2.0s latency).
Nmap scan report for 192.168.1.18
Host is up (2.0s latency).
Nmap scan report for 192.168.1.19
Host is up (2.0s latency).
Nmap scan report for 192.168.1.20
Host is up (2.0s latency).
Nmap scan report for 192.168.1.21
Host is up (2.0s latency).
Nmap scan report for 192.168.1.22
Host is up (2.0s latency).
Nmap scan report for 192.168.1.23
Host is up (0.0054s latency).
Nmap scan report for 192.168.1.24
Host is up (0.0053s latency).
Nmap scan report for 192.168.1.25
```



```
Nmap scan report for 192.168.1.7
Host is up (1.0s latency).
Nmap scan report for 192.168.1.8
Host is up (1.0s latency).
Nmap scan report for 192.168.1.9
Host is up (1.0s latency).
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).
Nmap scan report for 192.168.1.11
Host is up (0.0056s latency).
Nmap scan report for 192.168.1.12
Host is up (0.0055s latency).
Nmap scan report for 192.168.1.13
Host is up (2.0s latency).
Nmap scan report for 192.168.1.14
Host is up (2.0s latency).
Nmap scan report for 192.168.1.15
Host is up (2.0s latency).
Nmap scan report for 192.168.1.16
Host is up (2.0s latency).
Nmap scan report for 192.168.1.17
Host is up (2.0s latency).
Nmap scan report for 192.168.1.18
Host is up (2.0s latency).
Nmap scan report for 192.168.1.19
Host is up (2.0s latency).
Nmap scan report for 192.168.1.20
Host is up (2.0s latency).
Nmap scan report for 192.168.1.21
Host is up (2.0s latency).
Nmap scan report for 192.168.1.22
Host is up (2.0s latency).
Nmap scan report for 192.168.1.23
Host is up (0.0054s latency).
Nmap scan report for 192.168.1.24
Host is up (0.0053s latency).
Nmap scan report for 192.168.1.25
Host is up (0.0052s latency).
Nmap scan report for 192.168.1.26
Host is up (0.00014s latency).
Nmap scan report for 192.168.1.27
Host is up (0.000092s latency).
Nmap scan report for 192.168.1.28
Host is up (0.0027s latency).
Nmap scan report for 192.168.1.29
Host is up (0.013s latency).
Nmap scan report for 192.168.1.30
Host is up (0.013s latency).
Nmap scan report for 192.168.1.31
Host is up (0.013s latency).
Nmap scan report for 192.168.1.32
Host is up (0.012s latency).
Nmap scan report for 192.168.1.33
Host is up (0.012s latency).
Nmap scan report for 192.168.1.34
```

2. nmap 192.168.1.10

Scan top 1000 TCP ports

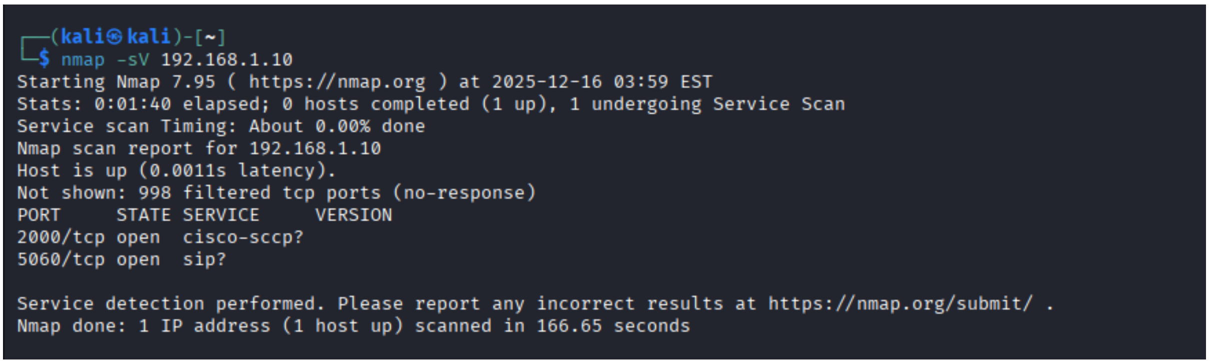


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 03:58 EST
Nmap scan report for 192.168.1.10
Host is up (0.00092s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
2000/tcp open  cisco-sccp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 4.11 seconds
```

3. nmap -sV 192.168.1.10

Detects running services and versions.

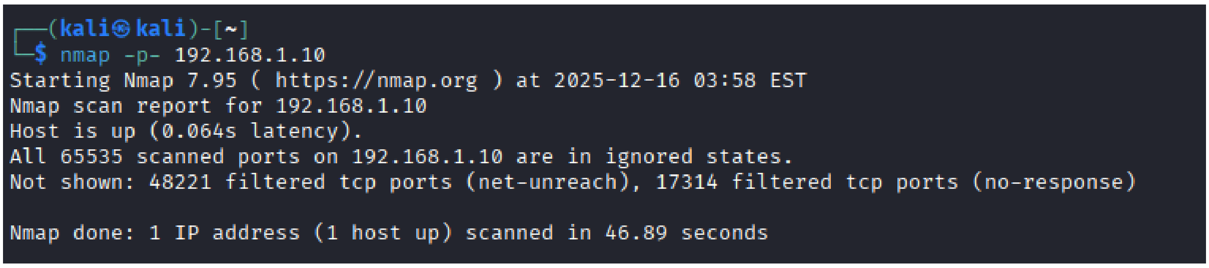


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 03:59 EST
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.1.10
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
2000/tcp open  cisco-sccp?
5060/tcp open  sip?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.65 seconds
```

4. nmap -p- 192.168.1.10

Scans all 65535 TCP ports

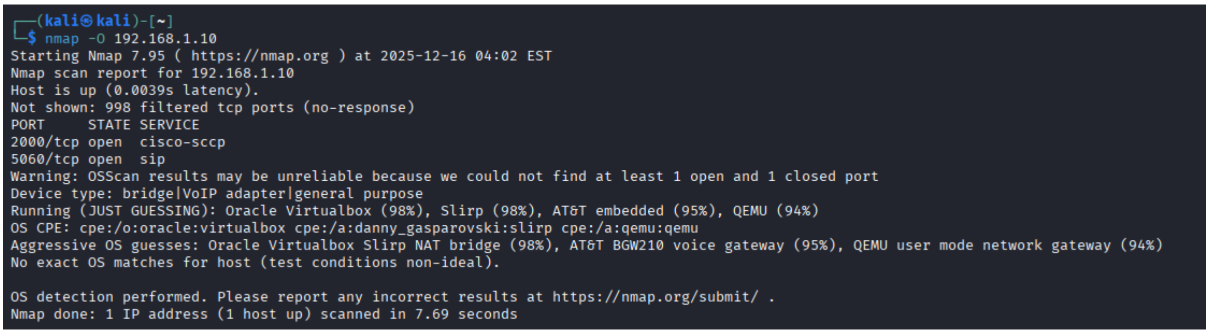


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 03:58 EST
Nmap scan report for 192.168.1.10
Host is up (0.064s latency).
All 65535 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 48221 filtered tcp ports (net-unreach), 17314 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 46.89 seconds
```

5. nmap -O 192.168.1.10

Detects OS details

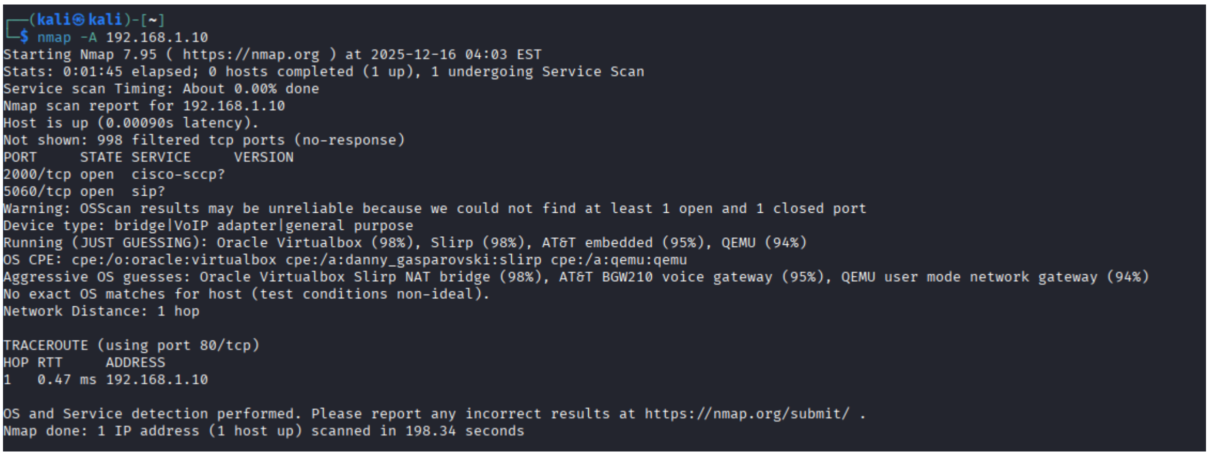


```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 04:02 EST
Nmap scan report for 192.168.1.10
Host is up (0.0039s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
2000/tcp open  cisco-sccp
5060/tcp open  sip
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
```

6. nmap -A 192.168.1.10

Aggressive Scan – OS detection, Service detection, Script Scanning and Traceroute



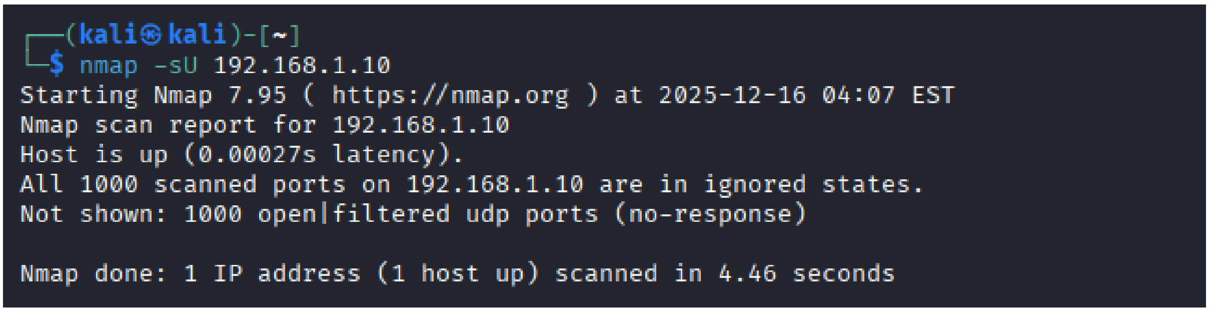
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 04:03 EST
Stats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.1.10
Host is up (0.00090s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
2000/tcp open  cisco-sccp?
5060/tcp open  sip?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.47 ms 192.168.1.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 198.34 seconds
```

7. nmap -sU 192.168.1.10

UDP port scan.

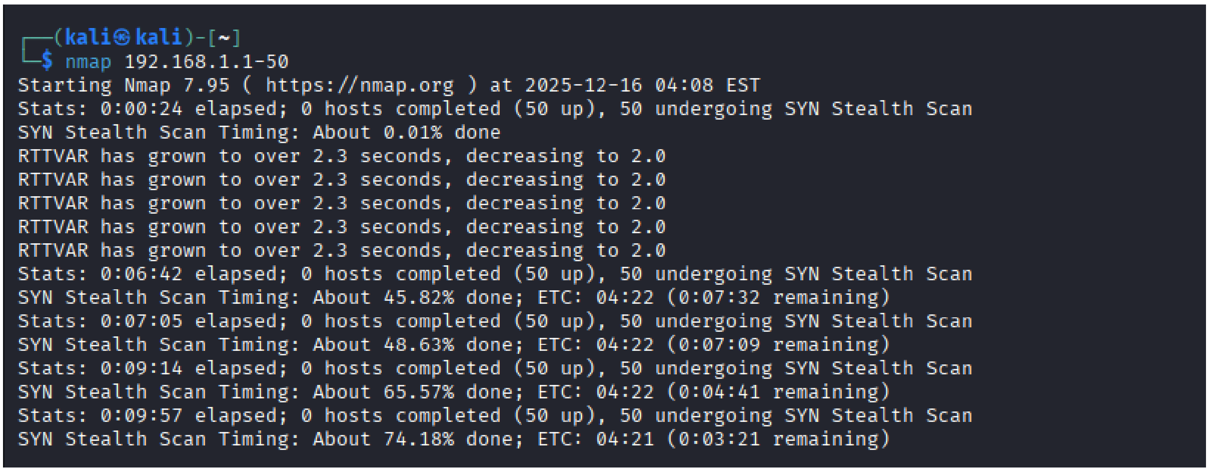


```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 04:07 EST
Nmap scan report for 192.168.1.10
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

8. nmap 192.168.1.1-50

Scans multiple targets (Works like angry IP scanner)



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.1-50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 04:08 EST
Stats: 0:00:24 elapsed; 0 hosts completed (50 up), 50 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.01% done
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:06:42 elapsed; 0 hosts completed (50 up), 50 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.82% done; ETC: 04:22 (0:07:32 remaining)
Stats: 0:07:05 elapsed; 0 hosts completed (50 up), 50 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.63% done; ETC: 04:22 (0:07:09 remaining)
Stats: 0:09:14 elapsed; 0 hosts completed (50 up), 50 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.57% done; ETC: 04:22 (0:04:41 remaining)
Stats: 0:09:57 elapsed; 0 hosts completed (50 up), 50 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.18% done; ETC: 04:21 (0:03:21 remaining)
```