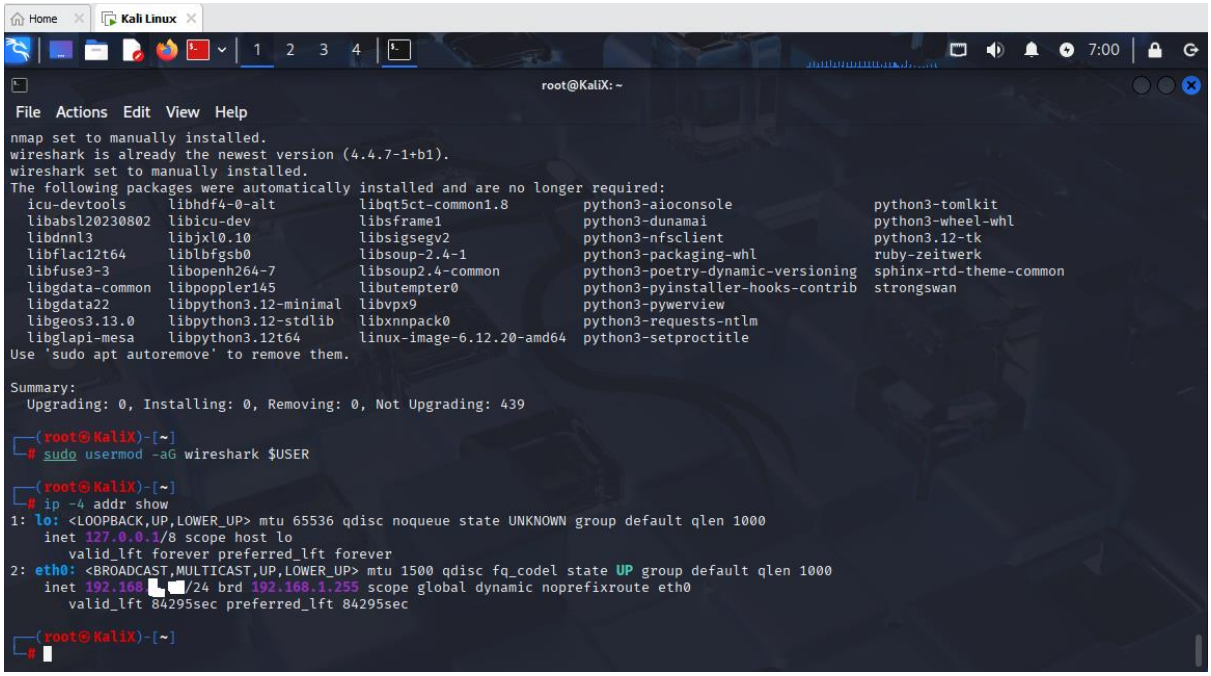
Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap

---

1. **Nmap Installation:**
   $sudo apt update
   $sudo apt install -y nmap wireshark



- Update and Install nmap and Wireshark

2. **IP Scan - Discover your local IP range**

   $ip -4 addr show

- : lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

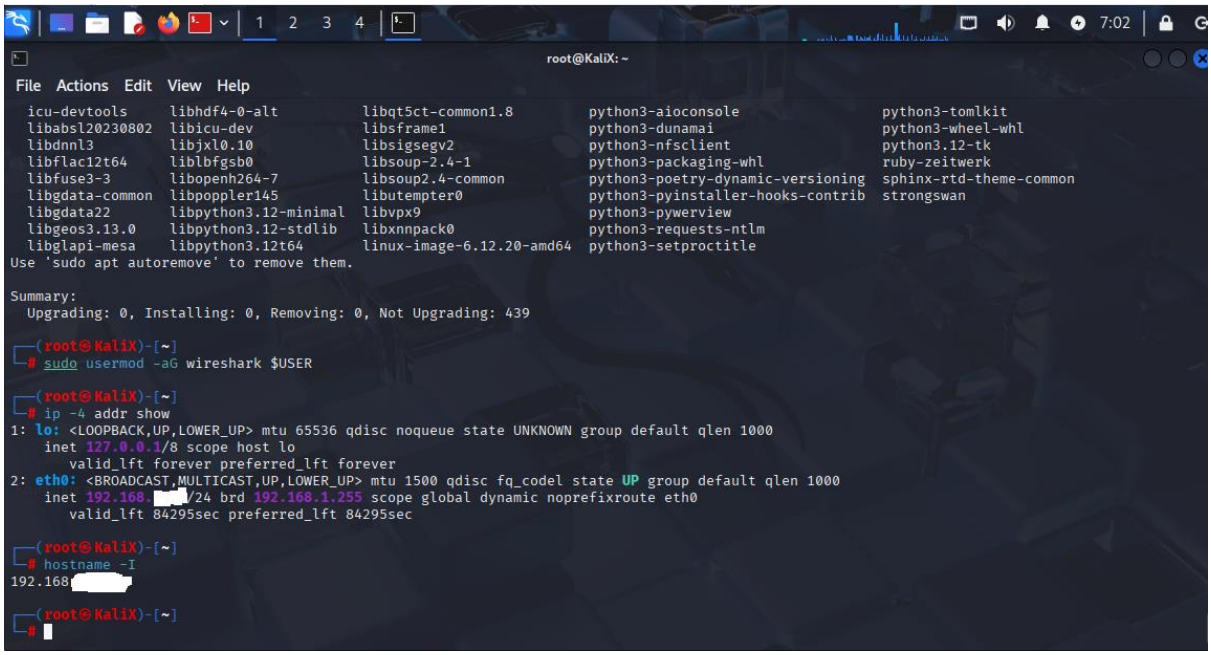
  inet 127.0.0.1/8 scope host lo

  valid_lft forever preferred_lft forever

  2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

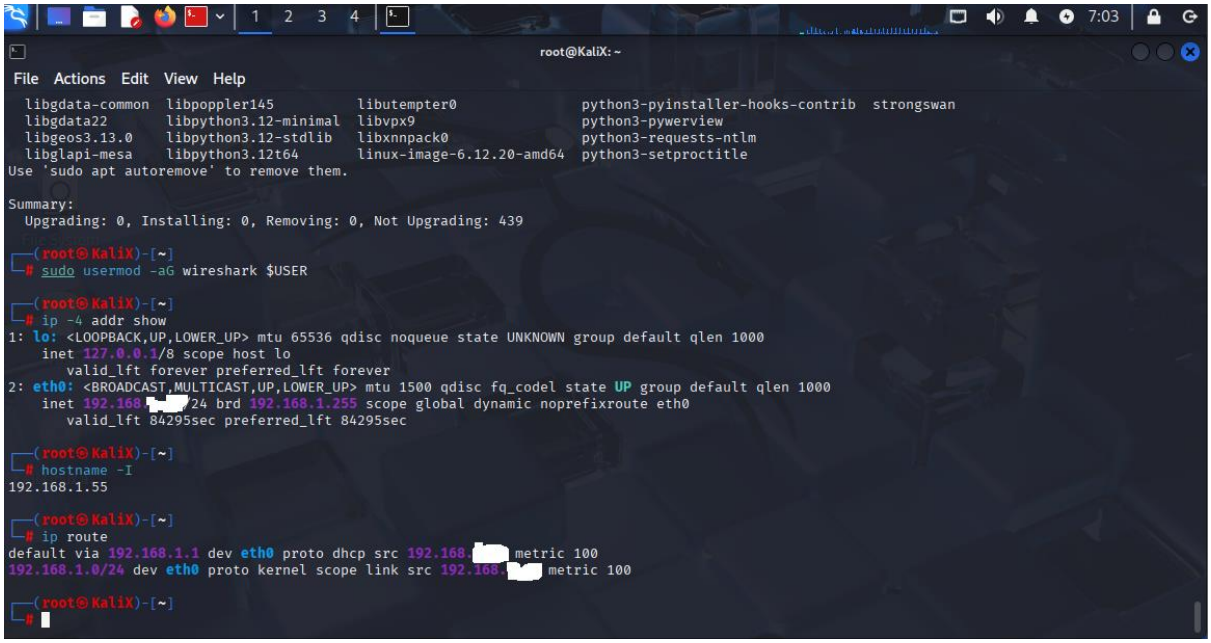
  inet 192.168.--.--/24 brd 192.168.--.-- scope global dynamic noprefixroute eth0

  valid_lft 84295sec preferred_lft 84295sec



   $hostname -I

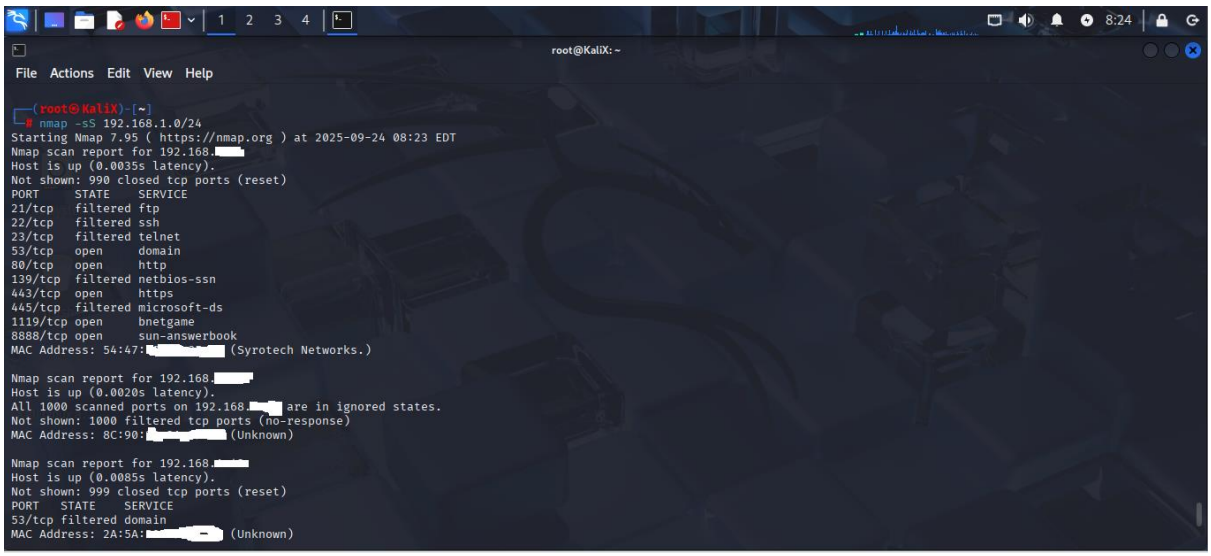
- displays network/mask



$ip route

- default via 192.168.1.1 dev eth0 proto dhcp src 192.168.--.-- metric 100
  192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.--.-- metric 100

3. Basic TCP SYN network scan



nmap -sS 192.168.1.0/24

-sS : TCP SYN

Result:

Starting Nmap 7.95 (https://nmap.org) at 2025-09-24 08:23 EDT

Nmap scan report for 192.168.1.--

Host is up (0.0035s latency).

Not shown: 990 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

1119/tcp open bnetgame

8888/tcp open sun-answerbook

MAC Address: 54:47:--:--:--:-- (Syrotech Networks.)

Nmap scan report for 192.168.1.--

Host is up (0.0020s latency).

All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 8C:90:--:--:--:-- (Unknown)

Nmap scan report for 192.168.1.--

Host is up (0.0085s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp filtered domain

MAC Address: 2A:5A:--:--:--:-- (Unknown)

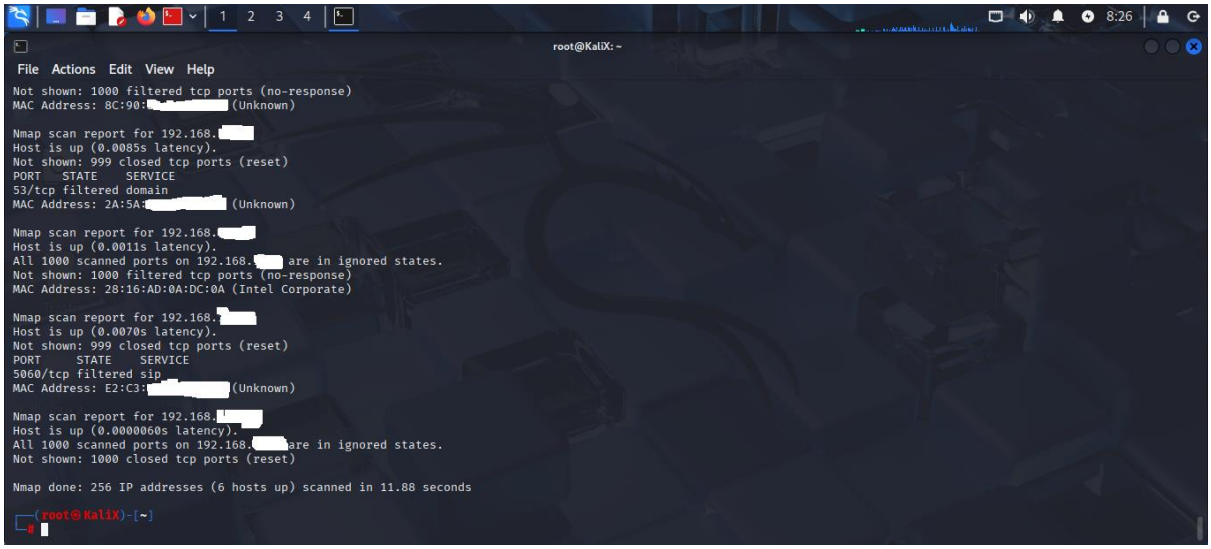
Nmap scan report for 192.168.1.--

Host is up (0.0011s latency).

All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 28:16:--:--:--:-- (Intel Corporate)



Nmap scan report for 192.168.1.--

Host is up (0.0070s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

5060/tcp filtered sip

MAC Address: E2:C3:--:--:--:-- (Unknown)

Nmap scan report for 192.168.1.--

Host is up (0.0000060s latency).

All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 11.88 seconds

4. **Service & version detection + OS detection (more intrusive)**

$ sudo nmap -sS -sV -O --version-intensity 5 192.168.1.0/24

- `-sV` : service/version detection
- `-O` : OS detection (requires root/admin)
- `--version-intensity` : tweak how aggressive version detection is

tarting Nmap 7.95 (https://nmap.org) at 2025-09-24 08:30 EDT

Nmap scan report for 192.168.1.--

Host is up (0.0054s latency).

Not shown: 990 closed tcp ports (reset)

PORT STATE SERVICE VERSION

53/tcp open domain dnsmasq 2.80

80/tcp open tcpwrapped

443/tcp open tcpwrapped

1119/tcp open ssl/bnetgame?

8888/tcp open sun-answerbook?

MAC Address: 54:47:--:--:--:-- (Syrotech Networks.)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.10 - 4.11

Network Distance: 1 hop

Nmap scan report for 192.168.1.--

Host is up (1.1s latency).

All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 8C:90:--:--:--:-- (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 192.168.1.--

Host is up (0.059s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE VERSION

53/tcp filtered domain

MAC Address: 2A:5A:--:--:--:-- (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 192.168.1.--

Host is up (0.00055s latency).

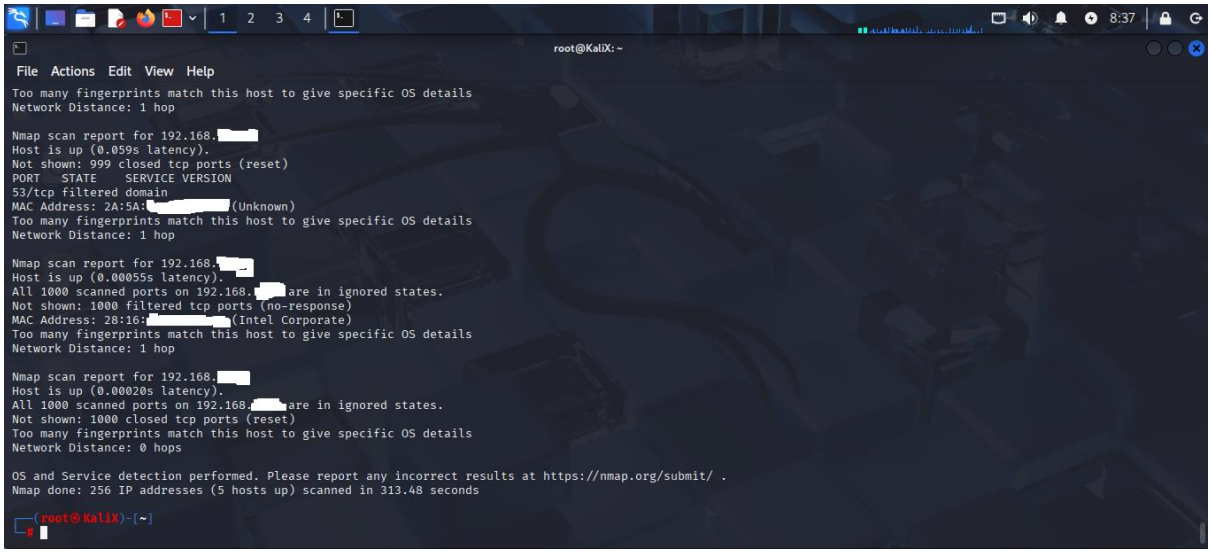
All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 28:16:--:--:--:-- (Intel Corporate)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop



Nmap scan report for 192.168.1.--

Host is up (0.00020s latency).

All 1000 scanned ports on 192.168.1.-- are in ignored states.

Not shown: 1000 closed tcp ports (reset)

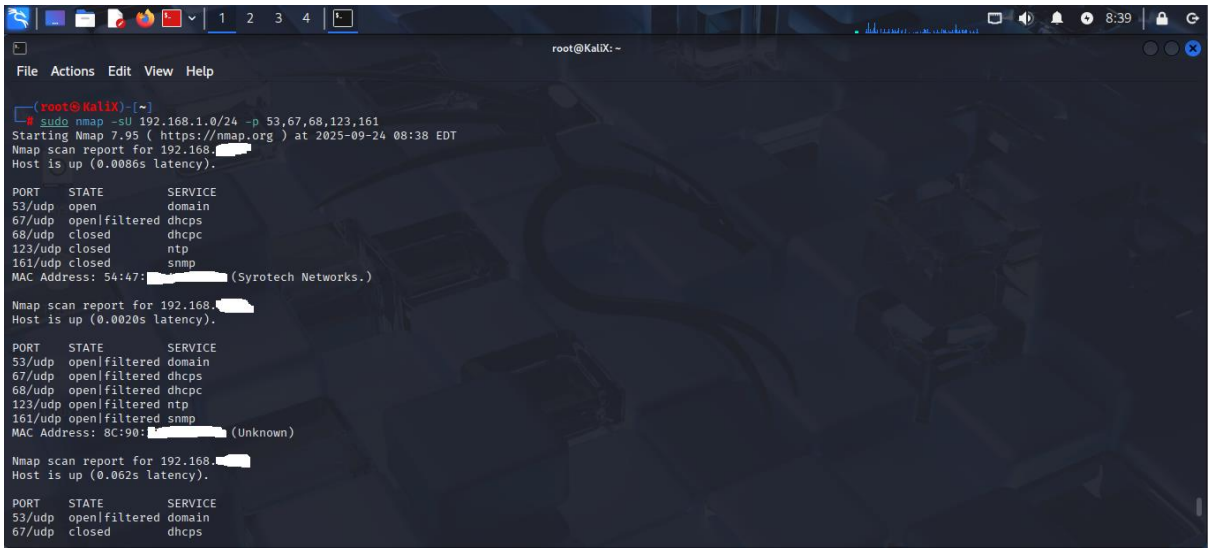
Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (5 hosts up) scanned in 313.48 seconds

5. **UDP scan**



$sudo nmap -sU 192.168.1.0/24 -p 53,67,68,123,161

focus on common UDP ports first (53 DNS, 67/68 DHCP, 123 NTP, 161 SNMP).

Result:

Starting Nmap 7.95 (https://nmap.org) at 2025-09-24 08:38 EDT

Nmap scan report for 192.168.1.--

Host is up (0.0086s latency).

PORT STATE SERVICE

53/udp open domain

MAC Address: 54:47:--:--:--:-- (Syrotech Networks.)

Nmap scan report for 192.168.1.--

Host is up (0.0020s latency).

PORT STATE SERVICE

53/udp open|filtered domain

67/udp open|filtered dhcps

68/udp open|filtered dhcpc

123/udp open|filtered ntp

161/udp open|filtered snmp

MAC Address: 8C:90:--:--:--:-- (Unknown)

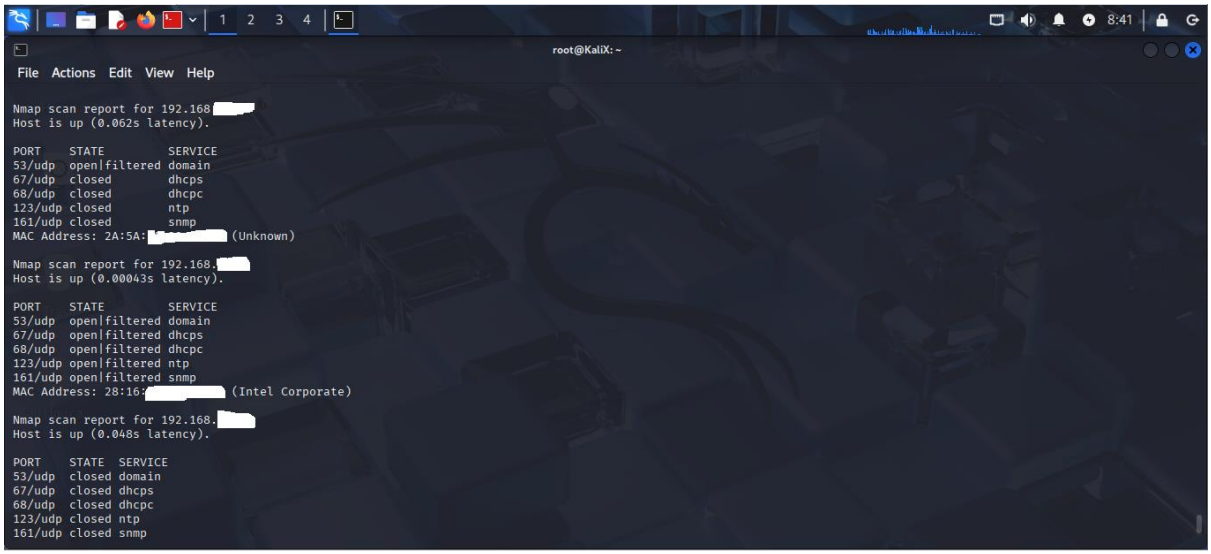
Nmap scan report for 192.168.1.--

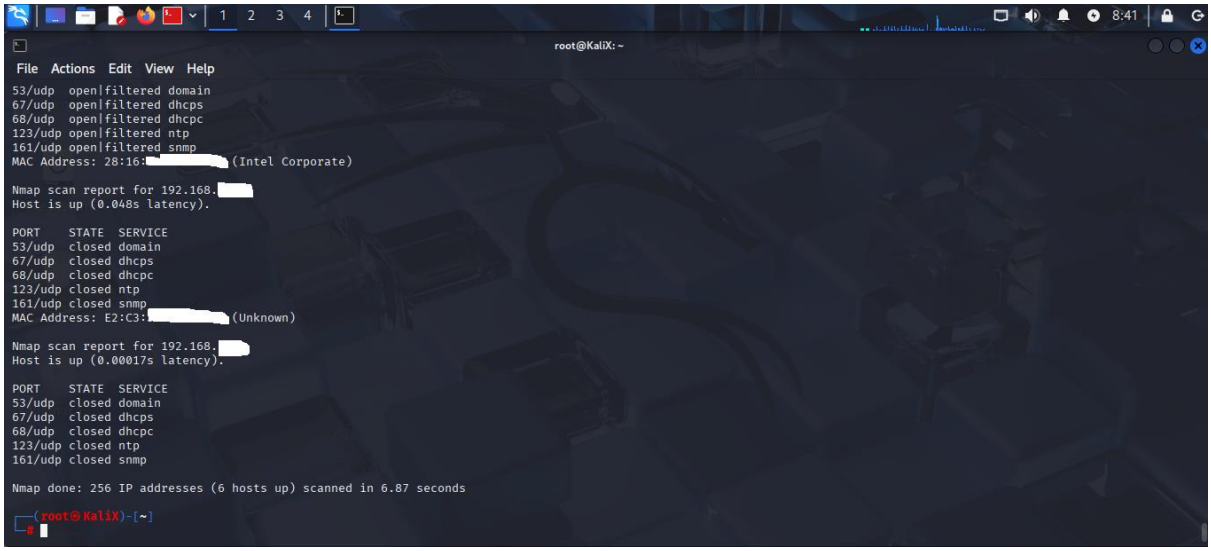
Host is up (0.062s latency).

PORT STATE SERVICE

53/udp open|filtered domain

MAC Address: 2A:5A:--:--:--:-- (Unknown)





Nmap scan report for 192.168.1.--

Host is up (0.00043s latency).

PORT STATE SERVICE

53/udp open|filtered domain

67/udp open|filtered dhcps

68/udp open|filtered dhcpc

123/udp open|filtered ntp

161/udp open|filtered snmp

MAC Address: 28:16:--:--:--:-- (Intel Corporate)

Nmap scan report for 192.168.1.--

Host is up (0.048s latency).

PORT STATE SERVICE

MAC Address: E2:C3:--:--:--:-- (Unknown)

Nmap scan report for 192.168.1.--

Host is up (0.00017s latency).

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.87 seconds