

Task 1: Scan Your Local Network for Open Ports

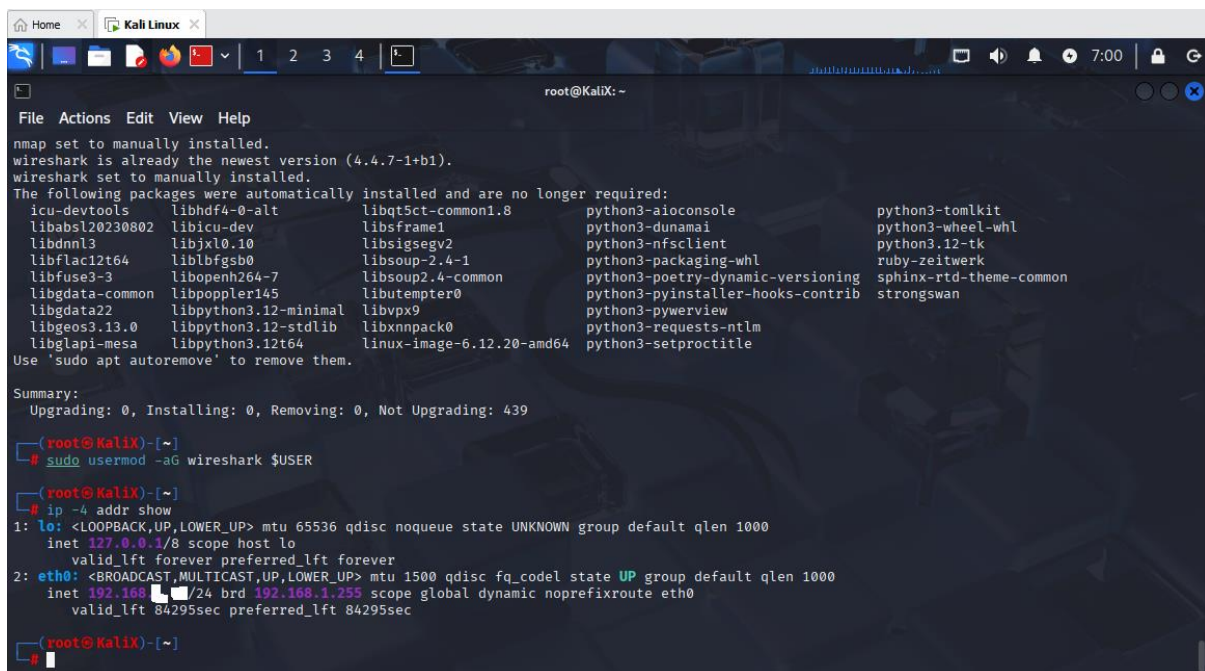
Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap

1. Nmap Installation:

\$sudo apt update

\$sudo apt install -y nmap wireshark



```
root@KaliX: ~
File Actions Edit View Help
nmap set to manually installed.
wireshark is already the newest version (4.4.7-1+b1).
wireshark set to manually installed.
The following packages were automatically installed and are no longer required:
icu-devtools libbdf4-0-alt libqt5ct-common1.8 python3-aioclient python3-tomlkit
libbabs120230802 libicu-dev libqt5ct-common1.8 python3-dunamai python3-wheel-whl
libbdl1 libbxc1.10 libsigsegv2 python3-nfsclient python3.12-tk
libbflac12t64 libbfgsb0 libsoup-2.4-1 python3-packaging-whl ruby-zeitwerk
libbfuse3-3 libopenh264-7 libsoup2.4-common python3-poetry-dynamic-versioning sphinx-rtd-theme-common
libbgeos3.13.0 libbpython3.12-minimal libutempter0 python3-pyinstaller-hooks-contrib strongswan
libbdata22 libbpython3.12-minimal libvpx9 python3-pyview python3-requests-ntlm
libbglapi-mesa libbpython3.12t64 linux-image-6.12.20-amd64 python3-setproctitle
Use 'sudo apt autoremove' to remove them.

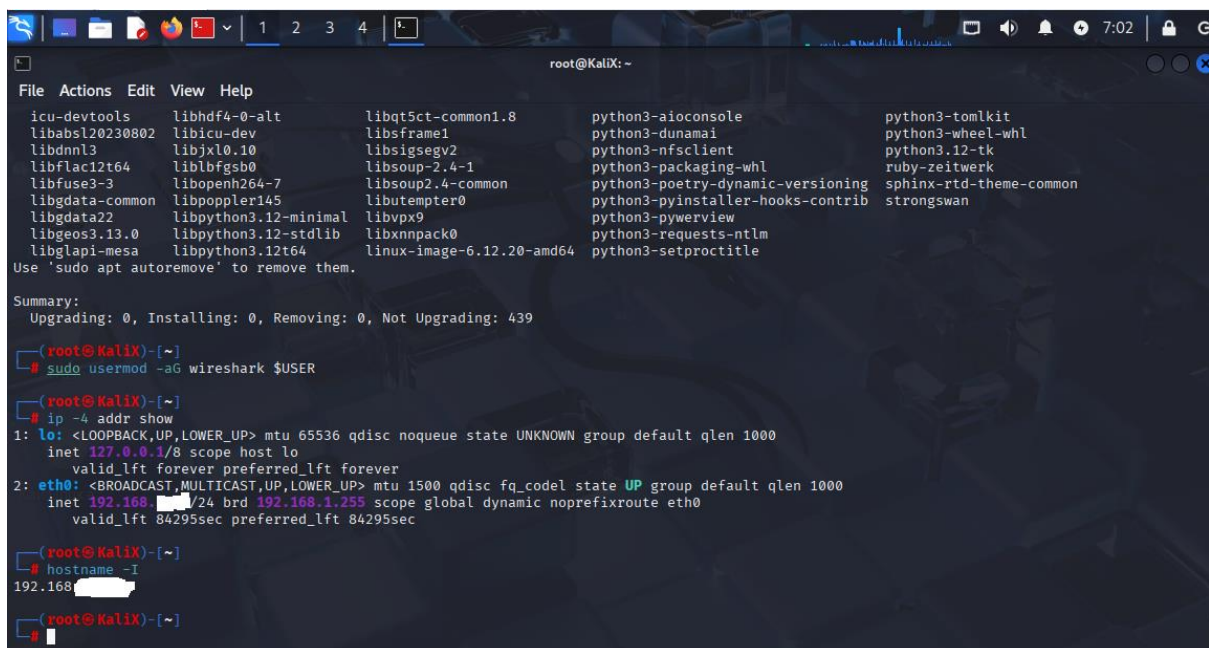
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 439
root@KaliX: ~
# sudo usermod -aG wireshark $USER
root@KaliX: ~
# ip -4 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.1.255/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 84295sec preferred_lft 84295sec
root@KaliX: ~
#
```

- 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



```
root@KaliX: ~  
File Actions Edit View Help  
icu-devtools      libhdf5-0-alt      libqt5ct-common1.8  python3-aioconsole  python3-tomlkit  
libabsl20230802   libicu-dev         libsqlite3           python3-dunamai      python3-wheel-whl  
libbrotli1        libjxl0.10         libsigsegv2          python3-nfsclient    python3.12-tk  
libflac12t64      liblbfgsb0         libsoup-2.4-1        python3-packaging-whl  ruby-zeitwerk  
libfuse3-3        libopenh264-7      libsoup2.4-common    python3-poetry-dynamic-versioning  sphinx-rtd-theme-common  
libgdata-common   libpoppler145      libutempter0         python3-pyinstaller-hooks-contrib  strongswan  
libgdata22        libpython3.12-minimal  libvpx9             python3-pyviewview  
libgeos3.13.0     libpython3.12-stdlib  libxnnpack0          python3-requests-ntlm  
libglapi-mesa     libpython3.12t64    linux-image-6.12.20-amd64  python3-setproctitle  
Use 'sudo apt autoremove' to remove them.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 439  
(root@KaliX)~  
# sudo usermod -aG wireshark $USER  
(root@KaliX)~  
# ip -4 addr show  
1: 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 192.168.1.255/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0  
valid_lft 84295sec preferred_lft 84295sec  
(root@KaliX)~  
# hostname -I  
192.168.1.255  
(root@KaliX)~  
#
```

\$hostname -I

- displays network/mask

```
root@Kalix:~  
File Actions Edit View Help  
libgdata-common libpoppler145 libutempter0 python3-pyinstaller-hooks-contrib strongswan  
libgdata22 libpython3.12-minimal libvpx9 python3-pywebview  
libgeos3.13.0 libpython3.12-stdlib libxnnpack0 python3-requests-ntlm  
libglapi-mesa libpython3.12t64 linux-image-6.12.20-amd64 python3-setproctitle  
Use 'sudo apt autoremove' to remove them.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 439  
  
(root@Kalix)~#  
# sudo usermod -aG wireshark $USER  
  
(root@Kalix)~#  
# ip -4 addr show  
1: 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 192.168.1.0/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0  
        valid_lft 84295sec preferred_lft 84295sec  
  
(root@Kalix)~#  
# hostname -i  
192.168.1.55  
  
(root@Kalix)~#  
# ip route  
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.0/24 metric 100  
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.0 metric 100  
  
(root@Kalix)~#  
#
```

\$ip route

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

3. Basic TCP SYN network scan

```
root@Kalix:~  
File Actions Edit View Help  
  
(root@Kalix)~#  
# nmap -sS 192.168.1.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 08:23 EDT  
Nmap scan report for 192.168.1.0/24  
Host is up (0.0035s latency).  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    filtered ftp  
22/tcp    filtered ssh  
23/tcp    filtered telnet  
53/tcp    open  domain  
80/tcp    open  http  
139/tcp   filtered netbios-ssn  
443/tcp   open  https  
445/tcp   filtered microsoft-ds  
1119/tcp  open  bnetgame  
8888/tcp  open  sun-answerbook  
MAC Address: 54:47:16:00:00:00 (Syrotech Networks.)  
  
Nmap scan report for 192.168.1.0/24  
Host is up (0.0020s latency).  
All 1000 scanned ports on 192.168.1.0/24 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 8C:90:1E:00:00:00 (Unknown)  
  
Nmap scan report for 192.168.1.0/24  
Host is up (0.0085s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    filtered domain  
MAC Address: 2A:5A:16:00:00:00 (Unknown)
```

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 192.168.1.0/24

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)

```
root@kaliX: ~  
File Actions Edit View Help  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 8C:90: [redacted] (Unknown)  
  
Nmap scan report for 192.168. [redacted]  
Host is up (0.0085s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE    SERVICE  
53/tcp    filtered domain  
MAC Address: 2A:5A: [redacted] (Unknown)  
  
Nmap scan report for 192.168. [redacted]  
Host is up (0.0011s latency).  
All 1000 scanned ports on 192.168. [redacted] are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 28:16:AD:0A:DC:0A (Intel Corporate)  
  
Nmap scan report for 192.168. [redacted]  
Host is up (0.0070s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE    SERVICE  
5060/tcp  filtered sip  
MAC Address: E2:C3: [redacted] (Unknown)  
  
Nmap scan report for 192.168. [redacted]  
Host is up (0.0000060s latency).  
All 1000 scanned ports on 192.168. [redacted] are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (6 hosts up) scanned in 11.88 seconds  
root@kaliX: ~
```

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.--

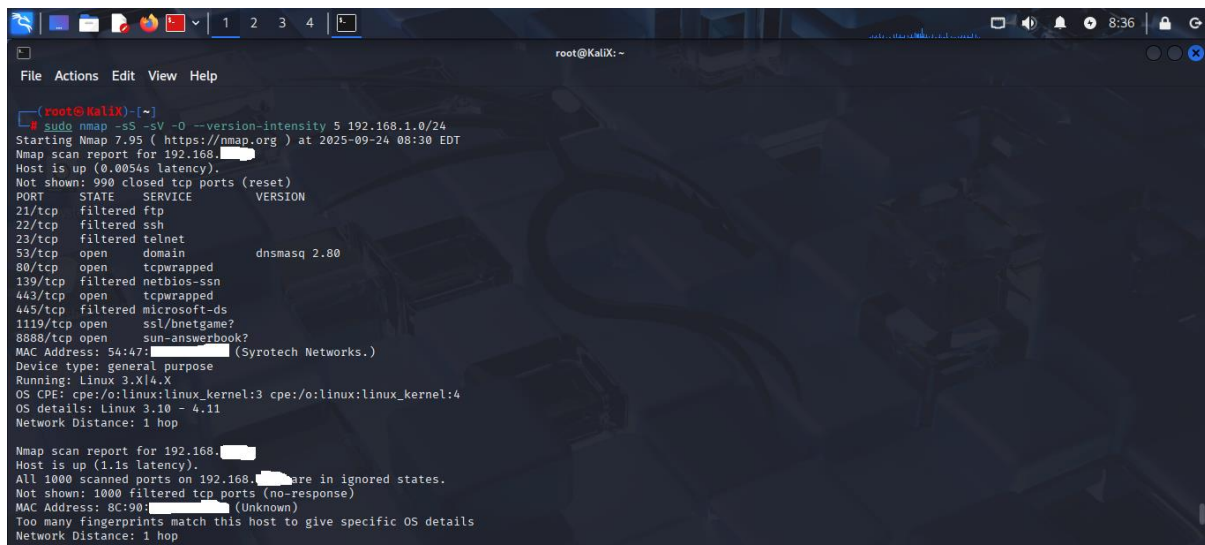
Host is up (0.0000060s latency).

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)



```
root@kaliX: ~  
File Actions Edit View Help  
root@kaliX:~# sudo nmap -sS -sV -O --version-intensity 5 192.168.1.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 08:30 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0054s latency).  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    filtered ftp  
22/tcp    filtered ssh  
23/tcp    filtered telnet  
53/tcp    open  domain       dnsmasq 2.80  
80/tcp    open  tcpwrapped  
139/tcp   filtered netbios-ssn  
443/tcp   open  tcpwrapped  
445/tcp   filtered microsoft-ds  
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 192.168.1.1  
Host is up (1.1s latency).  
All 1000 scanned ports on 192.168.1.1 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
```

\$ 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).

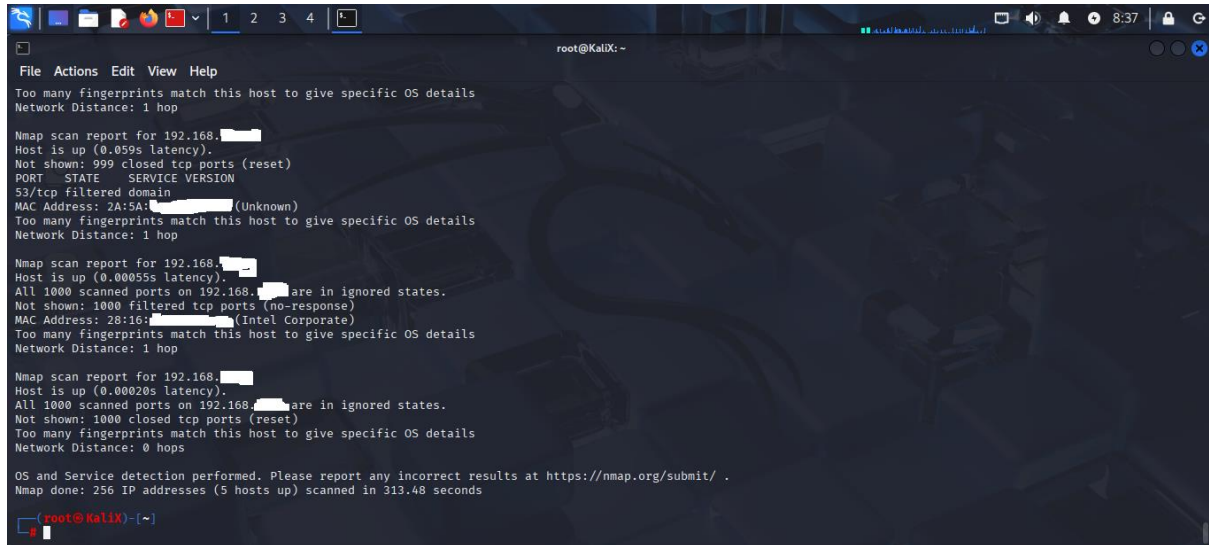
All 1000 scanned ports on 192.168.1.-- are in ignored states.

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



```
root@kali: ~  
File Actions Edit View Help  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
Nmap scan report for 192.168.1.1  
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:00:00:00:00 (Unknown)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
Nmap scan report for 192.168.1.1  
Host is up (0.00055s latency).  
All 1000 scanned ports on 192.168.1.1 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 192.168.1.1  
Host is up (0.00020s latency).  
All 1000 scanned ports on 192.168.1.1 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  
root@kali: ~
```

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)

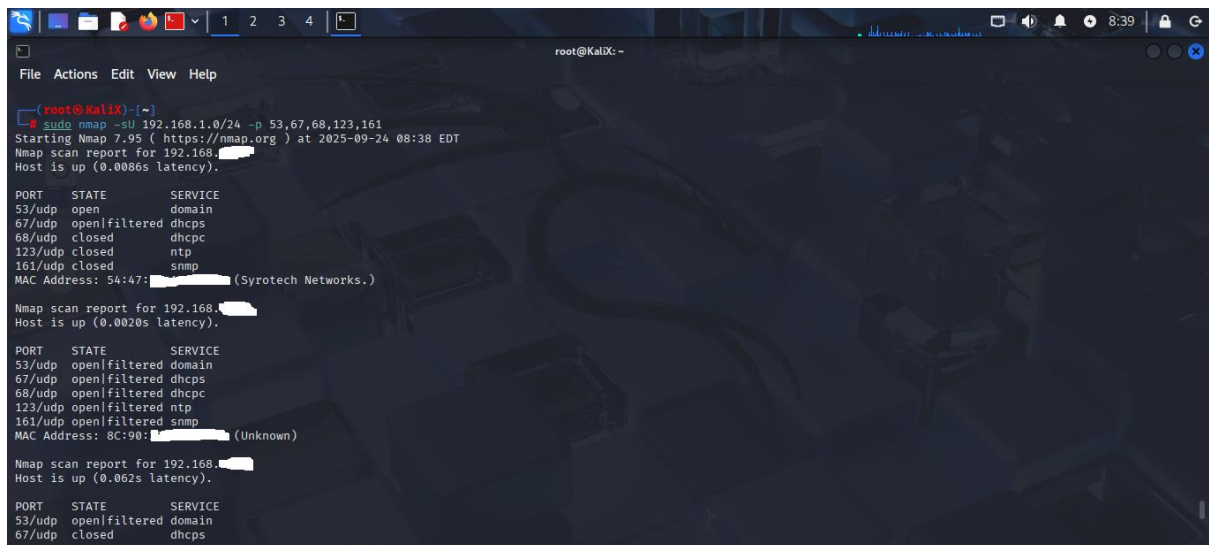
Too many fingerprints match this host to give specific OS details

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



```
root@kaliX: ~  
File Actions Edit View Help  
root@kaliX:~# sudo nmap -sU 192.168.1.0/24 -p 53,67,68,123,161  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 08:38 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0086s latency).  


| PORT    | STATE         | SERVICE |
|---------|---------------|---------|
| 53/udp  | open          | domain  |
| 67/udp  | open filtered | dhcps   |
| 68/udp  | closed        | dhcpc   |
| 123/udp | closed        | ntp     |
| 161/udp | closed        | snmp    |

  
MAC Address: 54:47: [redacted] (Syrotech Networks.)  
  
Nmap scan report for 192.168.1.2  
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: [redacted] (Unknown)  
  
Nmap scan report for 192.168.1.3  
Host is up (0.062s latency).  


| PORT   | STATE         | SERVICE |
|--------|---------------|---------|
| 53/udp | open filtered | domain  |
| 67/udp | closed        | dhcps   |


```

```
$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)

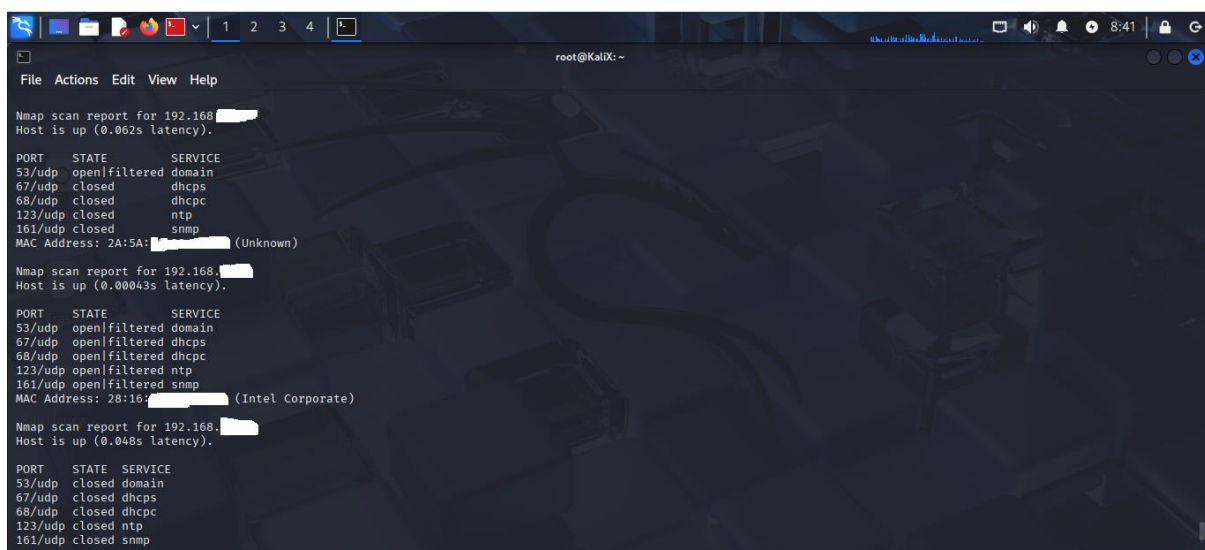
Nmap scan report for 192.168.1.--

Host is up (0.062s latency).

PORT	STATE	SERVICE
------	-------	---------

53/udp	open filtered	domain
--------	---------------	--------

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



```
root@KaliX: ~  
File Actions Edit View Help  
Nmap scan report for 192.168.1.1  
Host is up (0.062s latency).  
  
PORT      STATE      SERVICE  
53/udp    open|filtered domain  
67/udp    closed     dhcpcs  
68/udp    closed     dhcpc  
123/udp   closed     ntp  
161/udp   closed     snmp  
MAC Address: 2A:5A:00:00:00:00 (Unknown)  
  
Nmap scan report for 192.168.1.2  
Host is up (0.00043s latency).  
  
PORT      STATE      SERVICE  
53/udp    open|filtered domain  
67/udp    open|filtered dhcpcs  
68/udp    open|filtered dhcpc  
123/udp   open|filtered ntp  
161/udp   open|filtered snmp  
MAC Address: 28:16:00:00:00:00 (Intel Corporate)  
  
Nmap scan report for 192.168.1.3  
Host is up (0.048s latency).  
  
PORT      STATE      SERVICE  
53/udp    closed     domain  
67/udp    closed     dhcpcs  
68/udp    closed     dhcpc  
123/udp   closed     ntp  
161/udp   closed     snmp
```

```
root@kaliX: ~  
File Actions Edit View Help  
53/udp open|filtered domain  
67/udp open|filtered dhcp  
68/udp open|filtered dhcp  
123/udp open|filtered ntp  
161/udp open|filtered snmp  
MAC Address: 28:16: (Intel Corporate)  
  
Nmap scan report for 192.168.  
Host is up (0.048s latency).  
  
PORT STATE SERVICE  
53/udp closed domain  
67/udp closed dhcp  
68/udp closed dhcp  
123/udp closed ntp  
161/udp closed snmp  
MAC Address: E2:C3: (Unknown)  
  
Nmap scan report for 192.168.  
Host is up (0.00017s latency).  
  
PORT STATE SERVICE  
53/udp closed domain  
67/udp closed dhcp  
68/udp closed dhcp  
123/udp closed ntp  
161/udp closed snmp  
  
Nmap done: 256 IP addresses (6 hosts up) scanned in 6.87 seconds  
root@kaliX: ~
```

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 dhcp

68/udp open|filtered dhcp

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