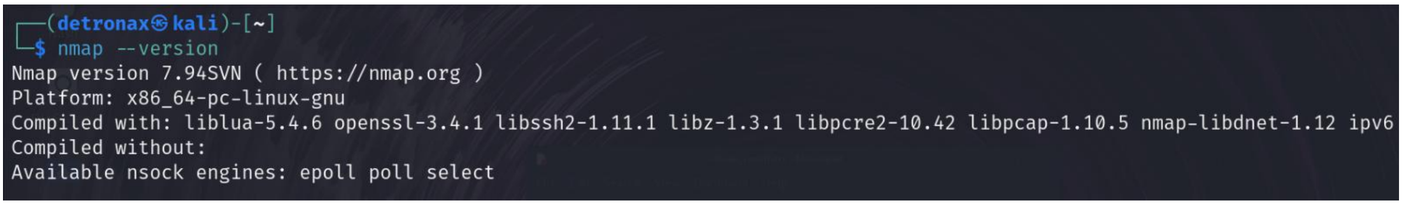
Task – 1

Task 1: Scan Your Local Network for Open Ports

>>> Solution: -

Step 1: - Checked the Nmap installed or not and the version of Nmap

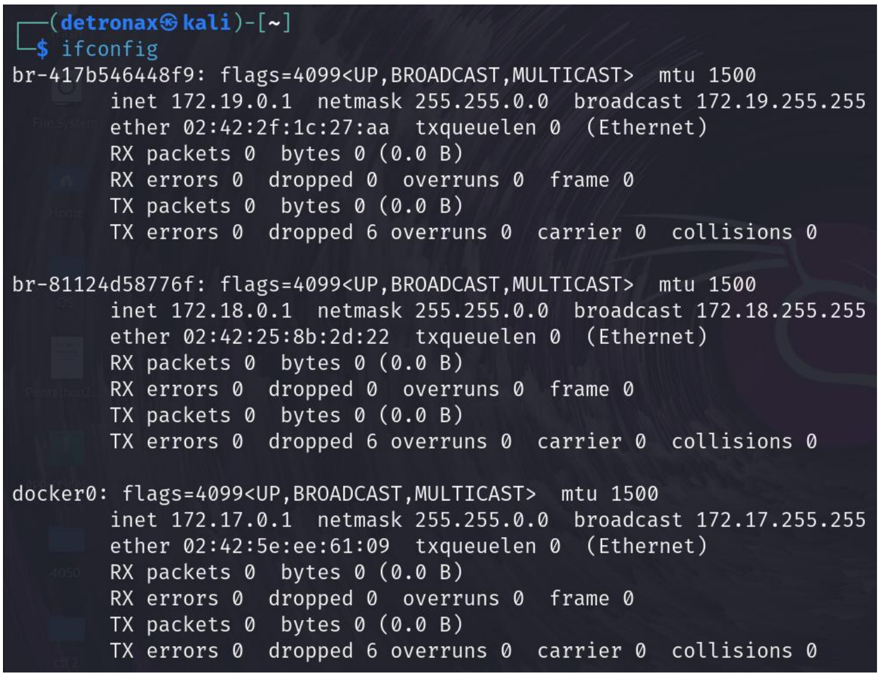
>>> nmap –version



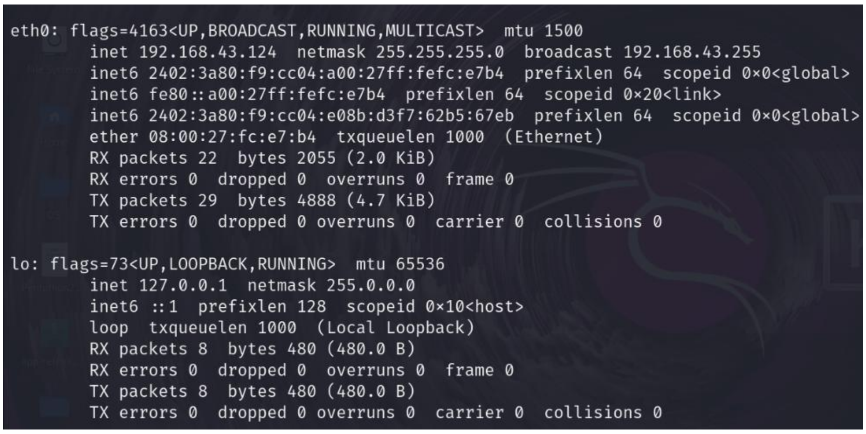
```
┌──(detronax㉿kali)-[~]
└─$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.4.1 libssh2-1.11.1 libz-1.3.1 libpcre2-10.42 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Step 2: - Checked the system IP

>>> ifconfig



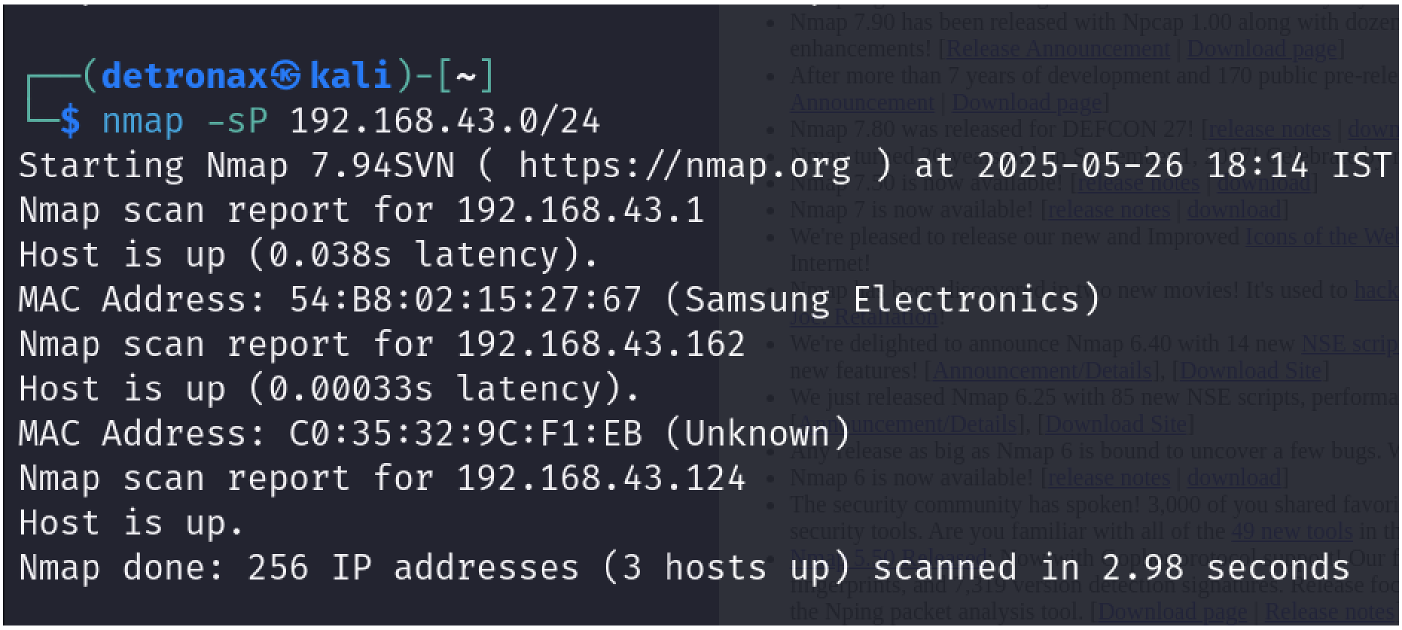
```
┌──(detronax㉿kali)-[~]
└─$ ifconfig
br-417b546448f9: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:2f:1c:27:aa  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0

br-81124d58776f: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:25:8b:2d:22  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:5e:ee:61:09  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0
```



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.124  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2402:3a80:f9:cc04:a00:27ff:fefc:e7b4  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fefc:e7b4  prefixlen 64  scopeid 0x20<link>
        inet6 2402:3a80:f9:cc04:e08b:d3f7:62b5:67eb  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:fc:e7:b4  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 2055 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 4888 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 3: - Perform a Basic Scan with the help of Nmap

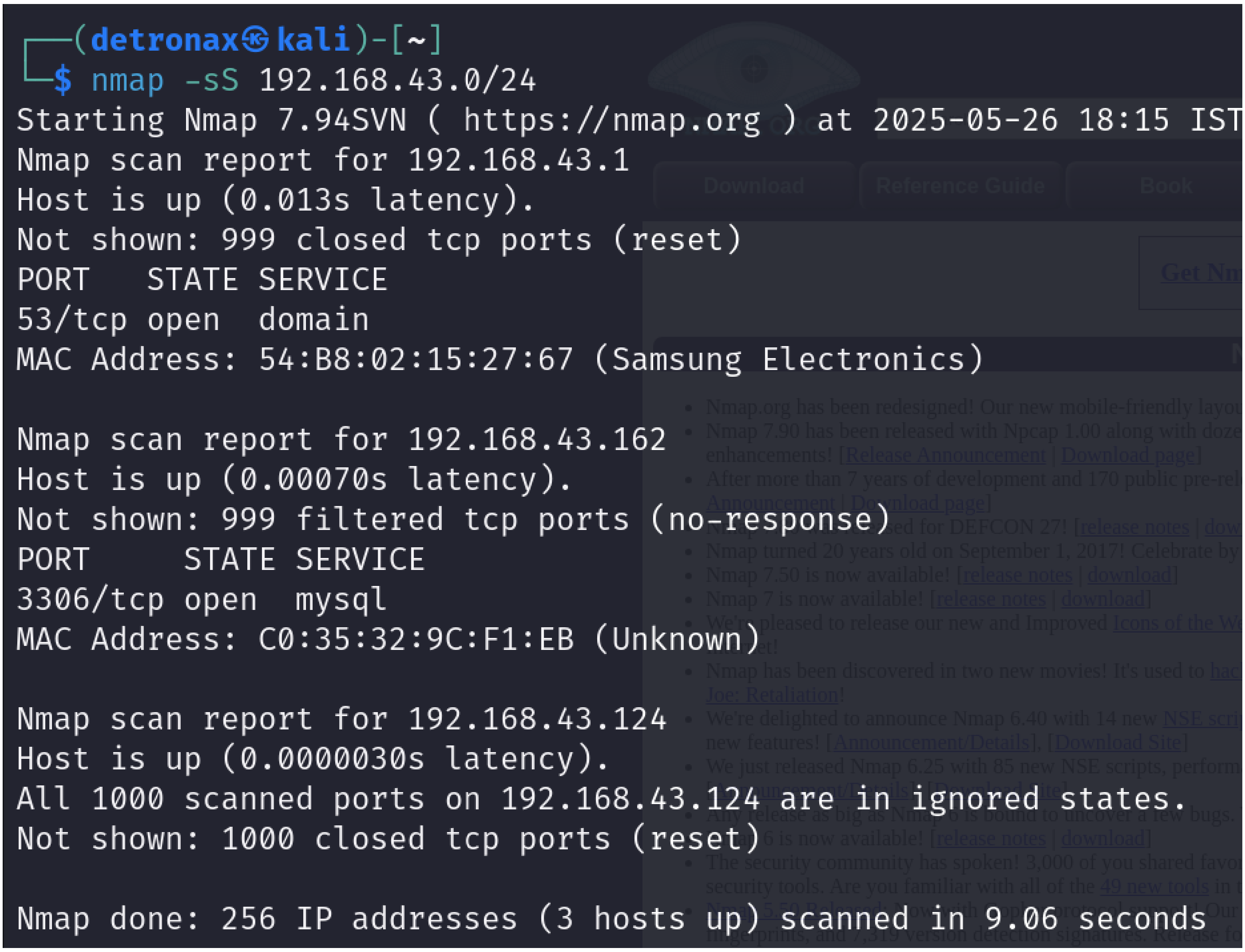
>>>nmap -sP 1*2.1*8.4*.0/24



```
┌──(detronax㉿kali)-[~]
└─$ nmap -sP 192.168.43.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 18:14 IST
Nmap scan report for 192.168.43.1
Host is up (0.038s latency).
MAC Address: 54:B8:02:15:27:67 (Samsung Electronics)
Nmap scan report for 192.168.43.162
Host is up (0.00033s latency).
MAC Address: C0:35:32:9C:F1:EB (Unknown)
Nmap scan report for 192.168.43.124
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.98 seconds
```

Step 4: - Perform a TCP SYN Scan (Stealth Scan)

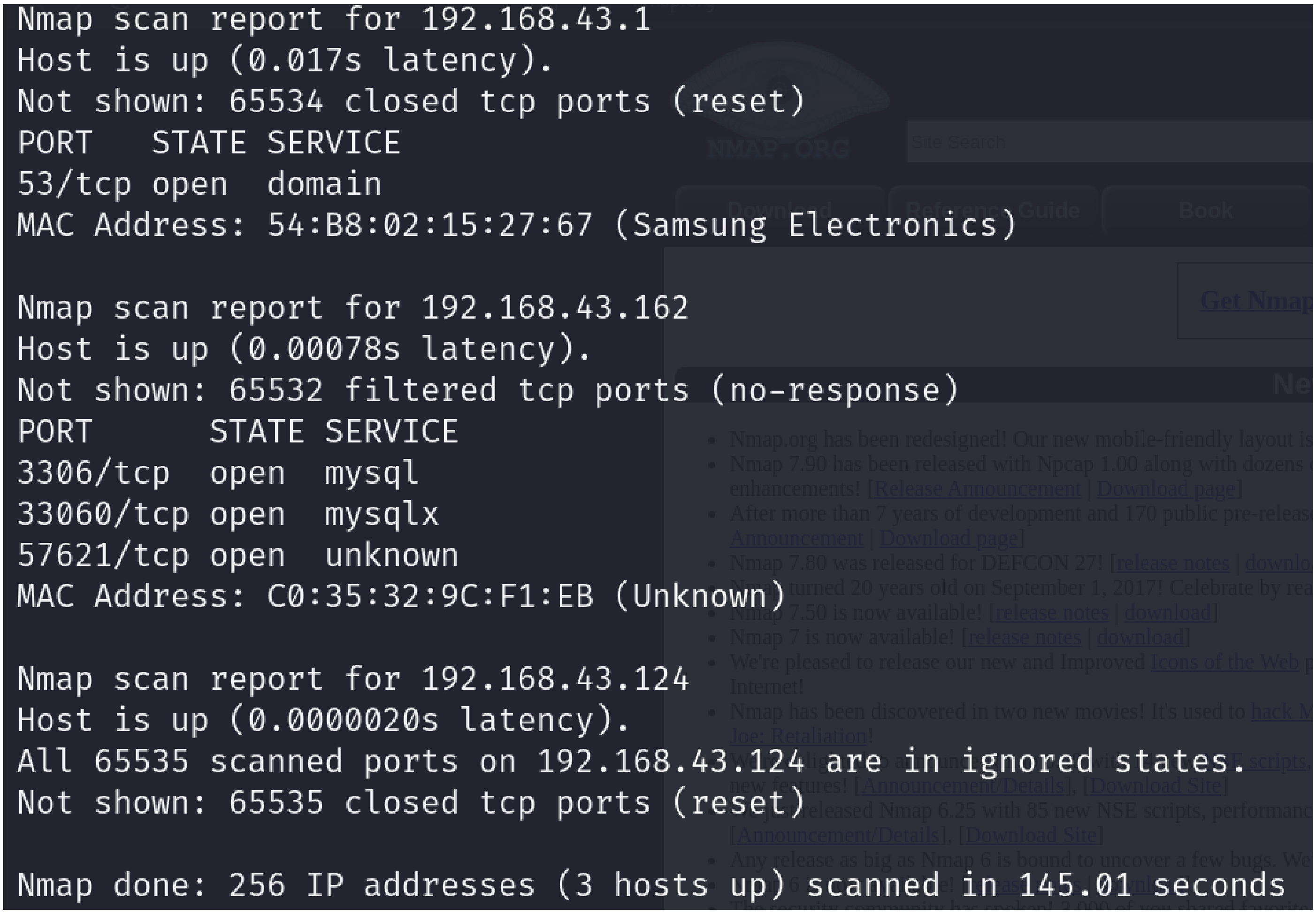
>>> nmap -sS 1*2.1*8.4*.0/24



```
┌──(detronax㉿kali)-[~]
└─$ nmap -sS 192.168.43.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 18:15 IST
Nmap scan report for 192.168.43.1
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 54:B8:02:15:27:67 (Samsung Electronics)

Nmap scan report for 192.168.43.162
Host is up (0.00070s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: C0:35:32:9C:F1:EB (Unknown)

Nmap scan report for 192.168.43.124
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.43.124 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.06 seconds
```

Step 5: - List All Open Ports on Each Device

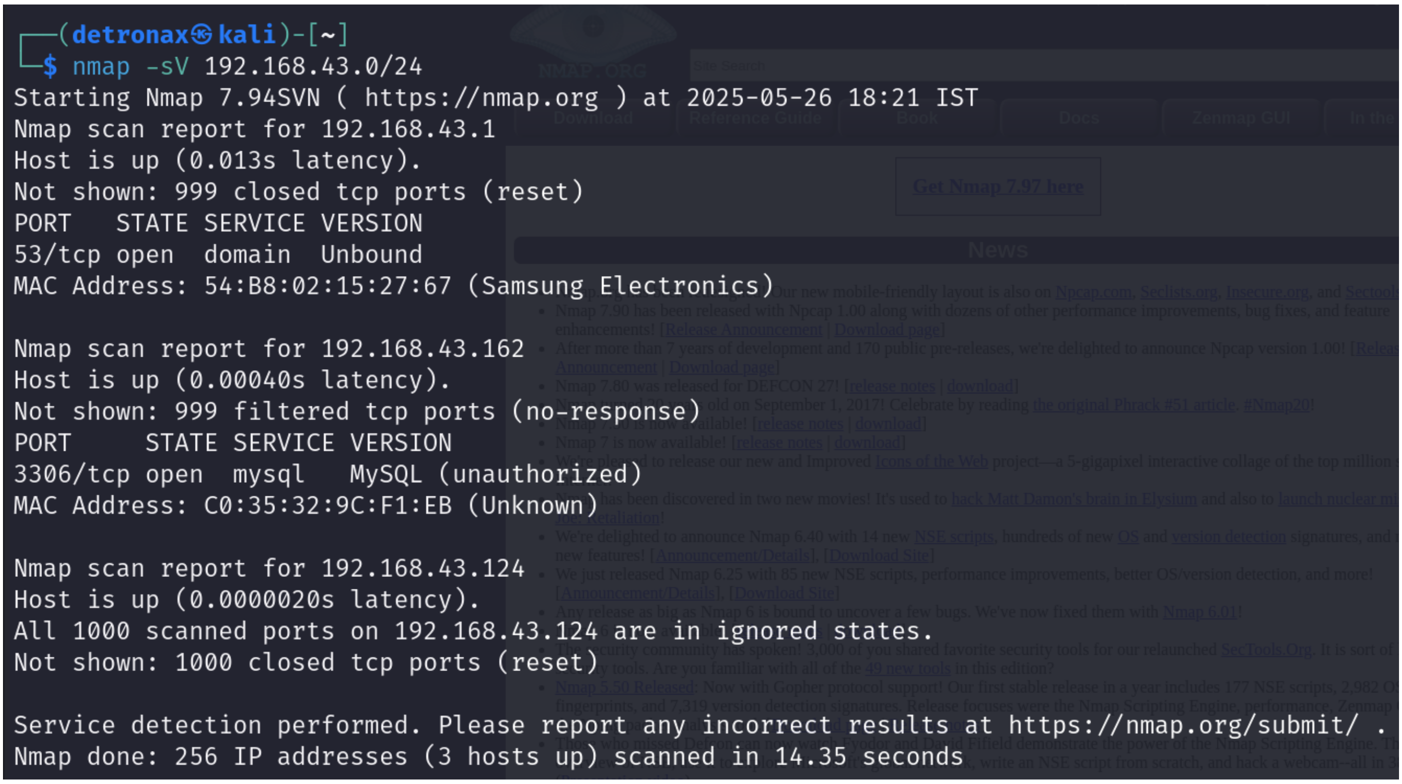
```
>>>nmap -p- 1*2.1*8.4*.0/24
```



```
Nmap scan report for 192.168.43.1
Host is up (0.017s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 54:B8:02:15:27:67 (Samsung Electronics)

Nmap scan report for 192.168.43.162
Host is up (0.00078s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
3306/tcp  open  mysql
33060/tcp open  mysqlx
57621/tcp open  unknown
MAC Address: C0:35:32:9C:F1:EB (Unknown)

Nmap scan report for 192.168.43.124
Host is up (0.0000020s latency).
All 65535 scanned ports on 192.168.43.124 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 145.01 seconds
```

Step 6: - Identify Running Services

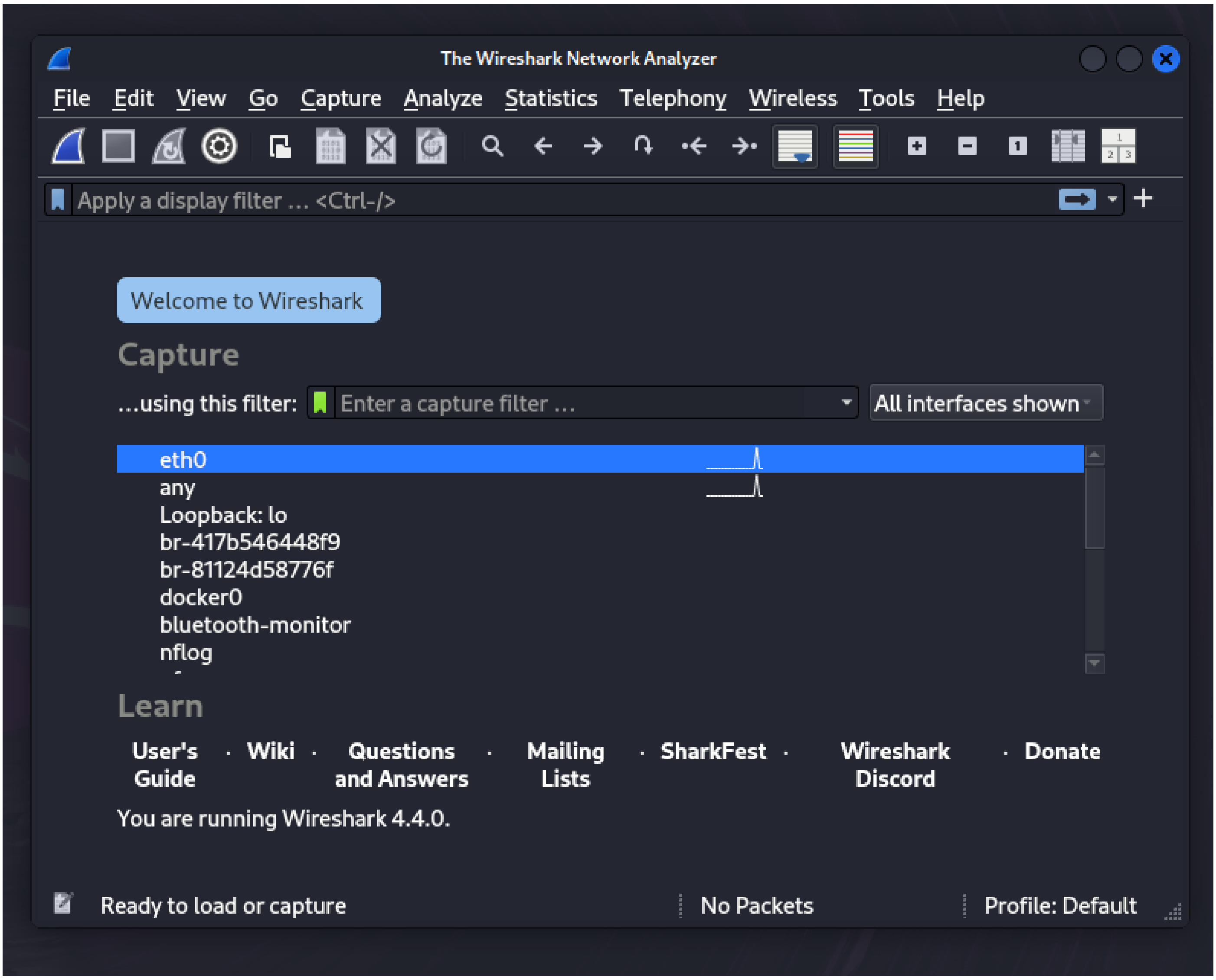
```
>>> nmap -sV 1$2.1$8.4*.0/24
```



```
┌──(detronax㉿kali)-[~]
└─$ nmap -sV 192.168.43.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 18:21 IST
Nmap scan report for 192.168.43.1
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
MAC Address: 54:B8:02:15:27:67 (Samsung Electronics)

Nmap scan report for 192.168.43.162
Host is up (0.00040s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: C0:35:32:9C:F1:EB (Unknown)

Nmap scan report for 192.168.43.124
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.43.124 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 14.35 seconds
```

Step 7: - Analysis the packet with Wireshark

```
>>> sudo wireshark
```

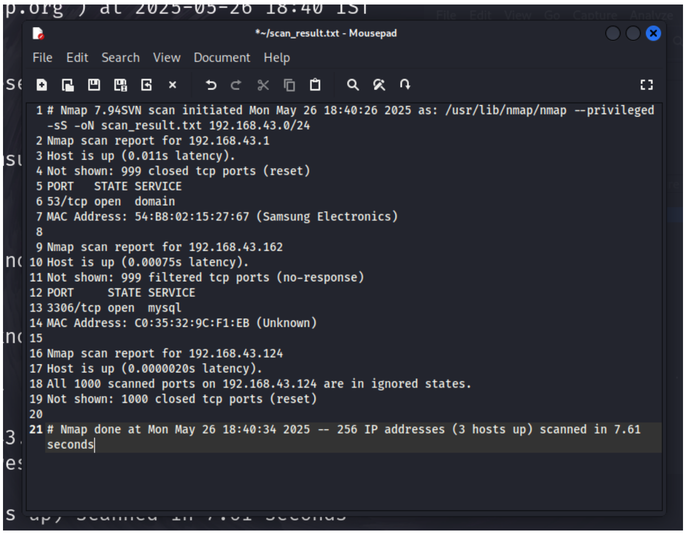


```
eth0
any
Loopback: lo
br-417b546448f9
br-81124d58776f
docker0
bluetooth-monitor
nflog
```

You are running Wireshark 4.4.0.

Ready to load or capture | No Packets | Profile: Default

This is the report



```
# Nmap 7.94SVN scan initiated Mon May 26 18:40:26 2025 as: /usr/lib/nmap/nmap --privileged
 -sS -oN scan_result.txt 192.168.43.0/24
Nmap scan report for 192.168.43.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 54:B8:02:15:27:67 (Samsung Electronics)

Nmap scan report for 192.168.43.162
Host is up (0.00075s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: C0:35:32:9C:F1:EB (Unknown)

Nmap scan report for 192.168.43.124
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.43.124 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

# Nmap done at Mon May 26 18:40:34 2025 -- 256 IP addresses (3 hosts up) scanned in 7.61
seconds
```