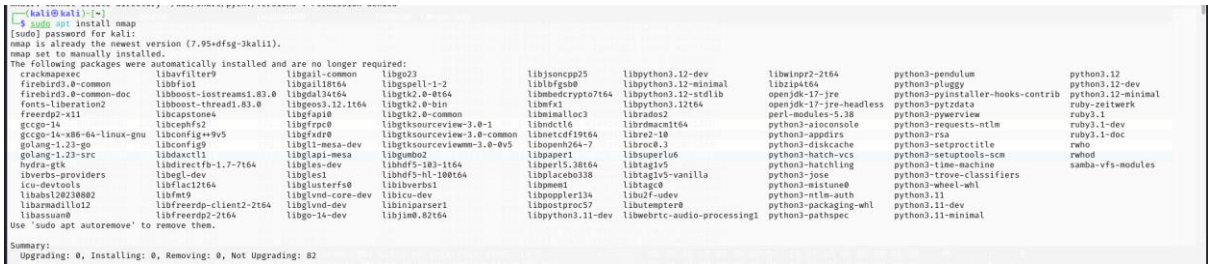
CYBER SECURITY INTERNSHIP TASK -1

1. Install Nmap from Official Website

- Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing.
- On Kali Linux, it is pre-installed. If not:

Command:

```
sudo apt update
sudo apt install nmap -y
```

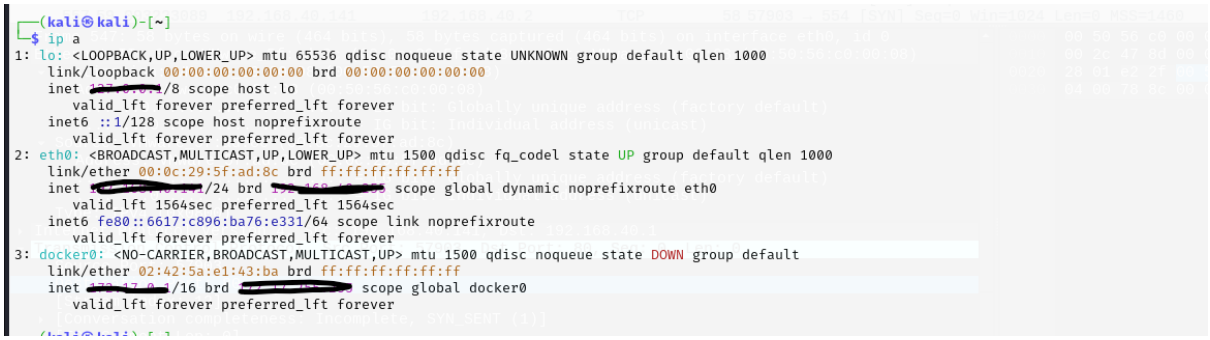


2. Find Your Local IP Range

- You need to identify the **subnet** (range of IPs) to scan.
- Run:

Command:

```
ip a
```

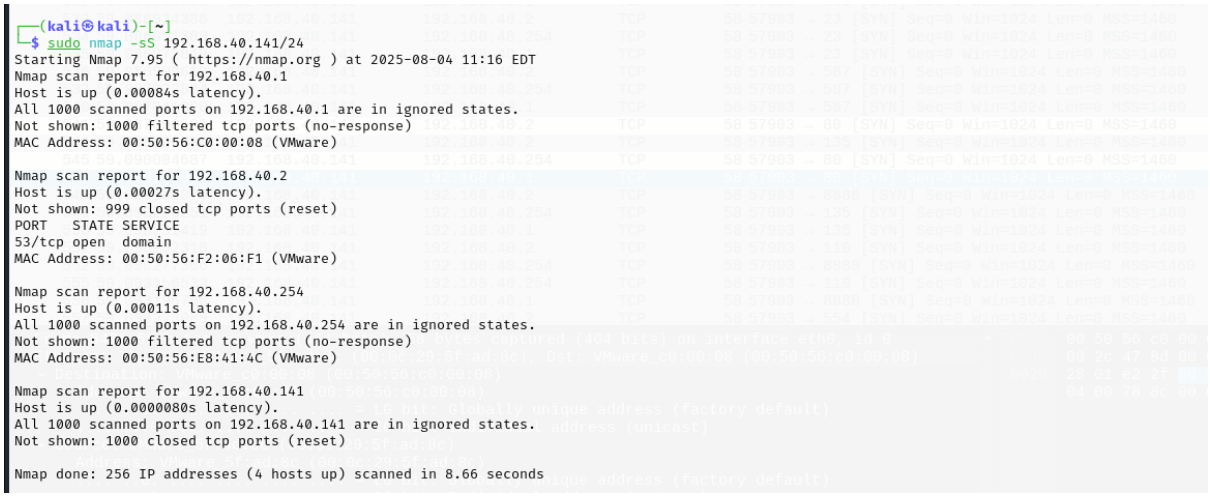


3. Run: `nmap -sS 192.168.1.0/24` to Perform a TCP SYN Scan

- This is a stealth scan (also known as half-open scan).
- It sends TCP SYN packets to all ports on each host in the subnet.

Command:

```
sudo nmap -sS 192.168.40.0/24
```



4: Note IP Addresses and Open Ports

- **IP addresses**
- **Open ports**
- **Service names**

Command:

```
sudo nmap -sS -T4 -v 192.168.1.0/24
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 -v 192.168.40.141/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 11:17 EDT
Initiating ARP Ping Scan at 11:17
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 11:17, 1.87s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 11:17
Completed Parallel DNS resolution of 3 hosts. at 11:17, 0.01s elapsed
Nmap scan report for 192.168.40.0 [host down]
Nmap scan report for 192.168.40.3 [host down]
Nmap scan report for 192.168.40.4 [host down]
Nmap scan report for 192.168.40.5 [host down]
Nmap scan report for 192.168.40.6 [host down]
Nmap scan report for 192.168.40.7 [host down]
Nmap scan report for 192.168.40.8 [host down]
Nmap scan report for 192.168.40.9 [host down]
Nmap scan report for 192.168.40.10 [host down]
Nmap scan report for 192.168.40.11 [host down]
Nmap scan report for 192.168.40.12 [host down]
Nmap scan report for 192.168.40.13 [host down]
Nmap scan report for 192.168.40.14 [host down]
Nmap scan report for 192.168.40.15 [host down]
Nmap scan report for 192.168.40.16 [host down]
Nmap scan report for 192.168.40.17 [host down]
Nmap scan report for 192.168.40.18 [host down]
Nmap scan report for 192.168.40.19 [host down]
Nmap scan report for 192.168.40.20 [host down]
Nmap scan report for 192.168.40.21 [host down]
Nmap scan report for 192.168.40.22 [host down]
Nmap scan report for 192.168.40.23 [host down]
Nmap scan report for 192.168.40.24 [host down]
Nmap scan report for 192.168.40.25 [host down]
Nmap scan report for 192.168.40.26 [host down]
Nmap scan report for 192.168.40.27 [host down]
Nmap scan report for 192.168.40.28 [host down]
Nmap scan report for 192.168.40.29 [host down]
Nmap scan report for 192.168.40.30 [host down]
Nmap scan report for 192.168.40.31 [host down]
Nmap scan report for 192.168.40.32 [host down]
Nmap scan report for 192.168.40.33 [host down]
Nmap scan report for 192.168.40.34 [host down]
Nmap scan report for 192.168.40.35 [host down]
Nmap scan report for 192.168.40.36 [host down]
Nmap scan report for 192.168.40.37 [host down]
Nmap scan report for 192.168.40.38 [host down]
Nmap scan report for 192.168.40.39 [host down]
Nmap scan report for 192.168.40.40 [host down]
Nmap scan report for 192.168.40.41 [host down]
Nmap scan report for 192.168.40.42 [host down]
```

```
Nmap scan report for 192.168.40.2
Host is up (0.00074s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F2:06:F1 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E8:41:4C (VMware)

Initiating SYN Stealth Scan at 11:17
Scanning 192.168.40.141 [1000 ports]
Completed SYN Stealth Scan at 11:17, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.40.141
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.40.141 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.01 seconds
           Raw packets sent: 6516 (278.512KB) | Rcvd: 3012 (124.388KB)
```

5. Optionally Analyze Packet Capture with Wireshark

- Open Wireshark:

  `sudo wireshark`

- Select your network interface (e.g., `wlan0`, `eth0`)
- Start capture.

- While Wireshark is running, perform your Nmap scan.
- Use this filter to see SYN packets:

Search this in the `wireshark` filter:

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```