Task 1: Scan Your Local Network for Open Ports

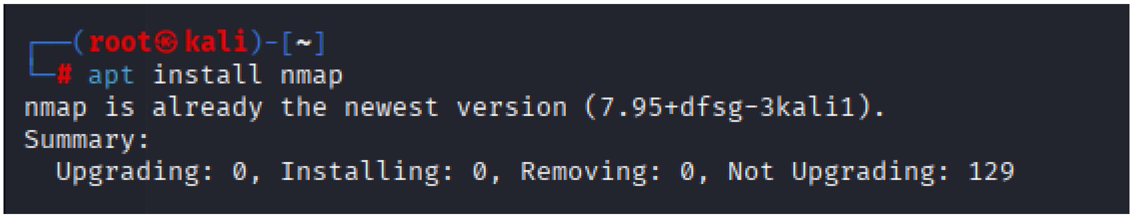
- **Objective**: Learn to discover open ports on devices in your local network to understand network exposure.
- **Tools**: Nmap (free), Wireshark (optional).

What is Nmap

Nmap (Network Mapper) is a free and open-source tool used to scan networks, discover devices, and detect open ports and running services. It helps identify security risks and monitor network health.

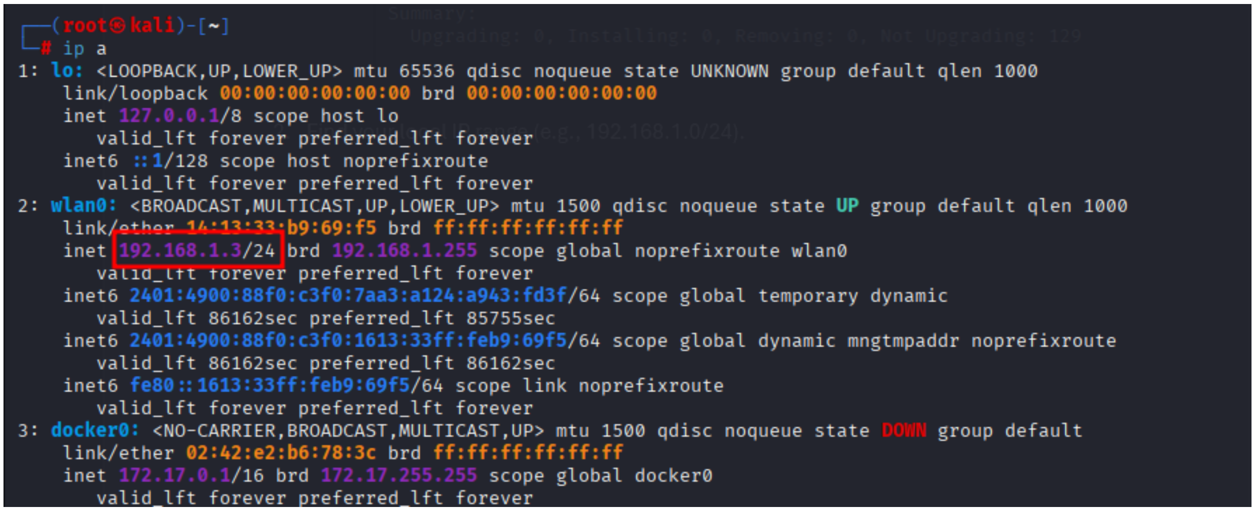
1. Installation of Nmap in Linux (Kali)

   apt install nmap



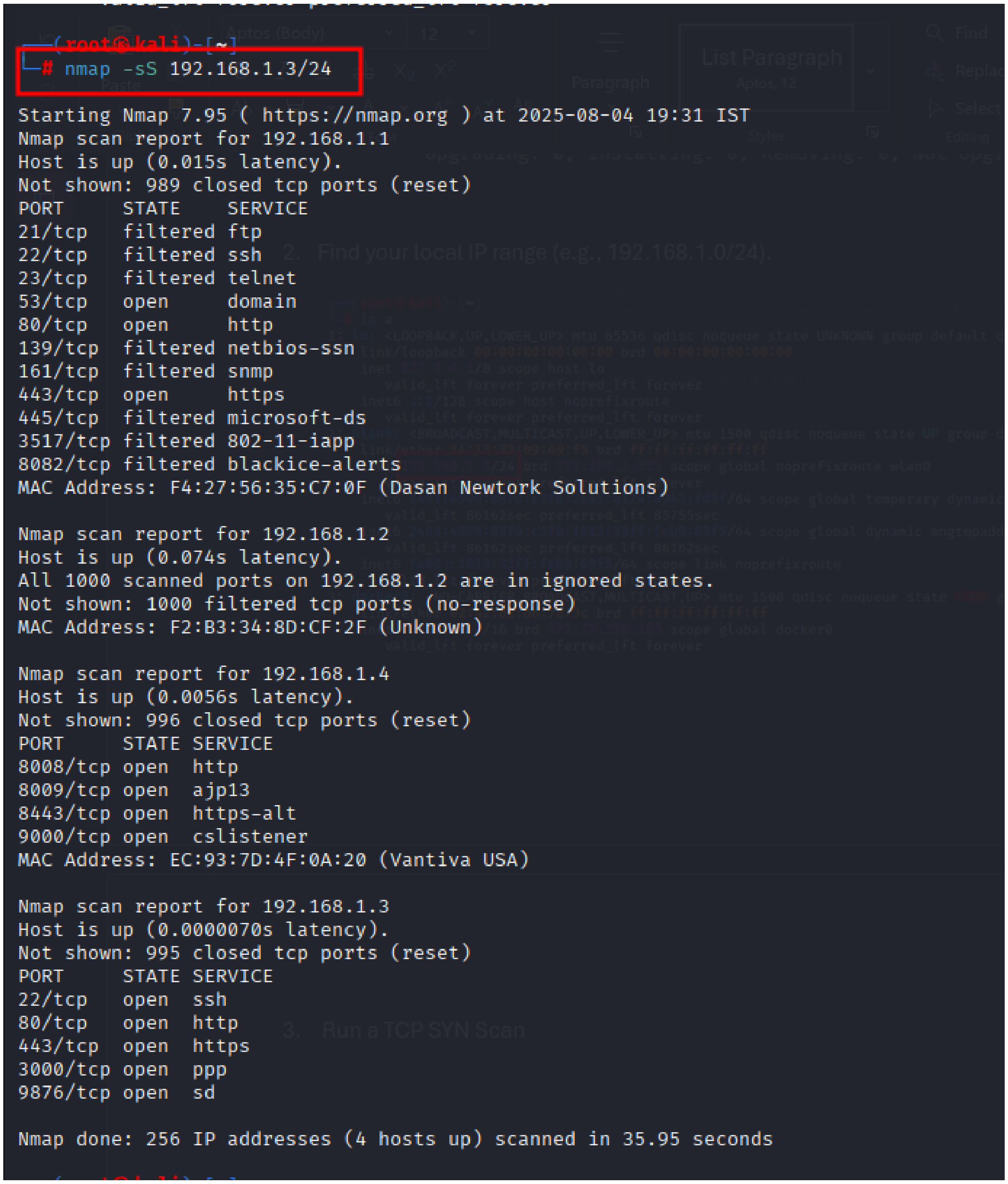
```
┌──(root㉿kali)-[~]
└─# apt install nmap
nmap is already the newest version (7.95+dfsg-3kali1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 129
```

2. Find your local IP range (e.g., 192.168.1.0/24).



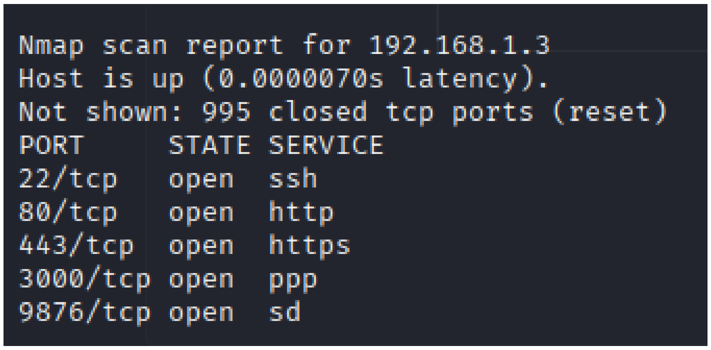
```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 14:13:33:b9:69:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global noprefixroute wlan0
       valid_lft forever preferred_lft forever
    inet6 2401:4900:88f0:c3f0:7aa3:a124:a943:fd3f/64 scope global temporary dynamic
       valid_lft 86162sec preferred_lft 85755sec
    inet6 2401:4900:88f0:c3f0:1613:33ff:feb9:69f5/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86162sec preferred_lft 86162sec
    inet6 fe80::1613:33ff:feb9:69f5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:e2:b6:78:3c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

3. Run a TCP SYN Scan



```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.3/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 19:31 IST
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
Not shown: 989 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
161/tcp  filtered snmp
443/tcp  open     https
445/tcp  filtered microsoft-ds
3517/tcp filtered 802-11-iapp
8082/tcp filtered blackice-alerts
MAC Address: F4:27:56:35:C7:0F (Dasan Newtork Solutions)

Nmap scan report for 192.168.1.2
Host is up (0.074s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F2:B3:34:8D:CF:2F (Unknown)

Nmap scan report for 192.168.1.4
Host is up (0.0056s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
8008/tcp open  http
8009/tcp open  ajp13
8443/tcp open  https-alt
9000/tcp open  cslistener
MAC Address: EC:93:7D:4F:0A:20 (Vantiva USA)

Nmap scan report for 192.168.1.3
Host is up (0.0000070s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3000/tcp open  ppp
9876/tcp open  sd

Nmap done: 256 IP addresses (4 hosts up) scanned in 35.95 seconds
```

4. Note Down Open IPs and Ports



```
Nmap scan report for 192.168.1.3
Host is up (0.0000070s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3000/tcp open  ppp
9876/tcp open  sd
```

Nmap Interview Questions

1. What is an open port?

An **open port** is a network port on a device that is actively **listening for connections**. It means a service or application is running on that port and can accept incoming traffic.

- Example:
  Port 80 open = HTTP web server is running.
  Port 22 open = SSH remote access service is available.

Risk: If unnecessary ports are open, attackers can exploit vulnerabilities in the services running on them.

2. How does Nmap perform a TCP SYN scan?

A **TCP SYN scan** is one of the most common and stealthy scans in Nmap, using the -sS option.

Steps:

1. Nmap sends a **SYN** packet (like a "hello") to the target port.
2. If the port is open, the target replies with a **SYN-ACK**.
3. Instead of completing the connection, Nmap sends an **RST** (reset) packet to avoid full handshake.

This way, Nmap identifies open ports **without establishing a full TCP connection**, making it fast and harder to detect.

3. What risks are associated with open ports?

Open ports can expose:

- **Vulnerable services** (e.g., outdated SSH, FTP, etc.)
- **Sensitive data** if misconfigured
- **Entry points** for unauthorized access or malware
- **Denial of Service (DoS)** attack targets

Even one exposed, unnecessary, or weakly protected port can give attackers a way into the system.

4. Difference between TCP and UDP scanning?

Feature	TCP Scan	UDP Scan
Protocol Used	TCP (connection-oriented)	UDP (connectionless)
Response Type	SYN-ACK (open), RST (closed)	No response = possibly open
Detection	Easier to detect (logs exist)	Harder to detect
Speed	Faster and more reliable	Slower and less reliable
Usage	Common services like HTTP, SSH	Services like DNS, SNMP, DHCP

5. How can open ports be secured?

✅ **Steps to secure open ports:**

- **Close unnecessary ports/services**
- **Use firewalls** to control traffic
- **Apply service authentication and encryption**
- **Regularly update and patch** services
- **Use port knocking** or **VPN access** to restrict exposure

6. What is a firewall's role regarding ports?

A **firewall** monitors and controls incoming/outgoing network traffic. It decides which ports and services are allowed or blocked.

Functions:

- **Blocks unwanted ports**
- **Prevents unauthorized access**

- **Enforces access control policies**
- **Logs suspicious activity**

Firewalls are essential for reducing attack surface and protecting network boundaries.

7. Why do attackers perform port scans?

Attackers use **port scanning** to:

- **Discover live hosts** on a network
- **Identify open ports** and running services
- **Find vulnerable applications**
- **Map the network structure**

It’s the first step in **reconnaissance** — gathering information before launching a real attack.

8. How does Wireshark complement port scanning?

Wireshark is a **packet sniffer** — it captures and analyzes the actual data packets.

Together with Nmap:

- Nmap finds **open ports and services**
- Wireshark shows **detailed traffic** and **packet behavior**
- Helps detect **suspicious responses**, **hidden ports**, or **misconfigurations**

Useful for learning how a system behaves during a scan or when analyzing attacks.