

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)

✓ Step 1: Install Nmap

Most Kali Linux systems come with Nmap pre-installed. If not, run:

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

To verify installation:

```
nmap --version
```

🔍 Step 2: Identify Your Local IP and Subnet Range

To discover your IP address and subnet:

```
ip a
```

Look for something like `inet 192.168.1.5/24` under your active interface (`eth0`, `wlan0`, etc.).

This tells you your subnet is `192.168.1.0/24`.

```
(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.94 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.4 openssl-3.0.10 libssh2-1.10.0 libz-1.2.13 libpcap-1.10.4 nmap-libdnet-
1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

(kali㉿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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:17:a5:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.129/24 brd 192.168.40.255 scope global dynamic noprefixroute eth0
        valid_lft 1432sec preferred_lft 1432sec
```



Step 3: Perform a TCP SYN Scan on Local Network

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

This command:

- -sS = Stealthy TCP SYN scan
- Scans all 256 addresses in the subnet for open TCP ports

You can also save the results:

```
sudo nmap -sS 192.168.40.0/24 -oN scan_results.txt
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.40.0/24

[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-27 04:36 EDT
Nmap scan report for 192.168.40.1
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.40.2
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F7:5F:69 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
```



Step 4: Research Discovered Ports and Services

Use Nmap's service detection:

```
sudo nmap -sV 192.168.1.X
```

- Common ports:
 - 22 – SSH
 - 80 – HTTP

- 443 – HTTPS
- 21 – FTP
- 23 – Telnet
- 3389 – RDP

Use online resources like <https://www.speedguide.net/port.php> to understand each port.

Step 5: Identify Potential Security Risks

Open ports can expose:

- Unsecured web interfaces
 - Outdated or vulnerable services
 - Remote login ports (e.g., SSH, RDP)
-

Step 6: Save Results

You can store your scans for documentation:

```
sudo nmap -sS 192.168.40.0/24 -oN my_scan.txt
```

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.40.0/24

[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-27 04:36 EDT
Nmap scan report for 192.168.40.1
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.40.2
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F7:5F:69 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
```

Outcome

- You understand how to identify and analyze open ports.
- You can assess potential security exposure on a local network.