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.

📡 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
```

🧠 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- Outdated or vulnerable services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
```

📘 Outcome

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