Task 1 Elevate Labs

Task 1: Scan Your Local Network for Open Ports

🎯 Objective

The goal of this task is to explore which devices are active on your local network and which ports (or "doors") are open on them. Open ports tell us which services or programs are available — and whether they might pose a security risk.

🛠️ Tools Used

- **Nmap** – a free and powerful tool used to scan networks.
- **Wireshark (optional)** – helps you dig deeper into network traffic, like a magnifying glass for internet data.

🔧 Steps I Followed

1. Installed Nmap

I downloaded Nmap from the official website and installed it on my system. It also comes with a tool called **Zenmap** (the graphical version), which can be helpful if you prefer not to use command-line tools.

---

2. Found My Local IP Range

I used the command below to check my IP address:

```
ipconfig   (on Windows)
```

My IP was something like `192.168.1.5`, so I figured the network range to scan would be `192.168.1.0/24` — which covers all devices connected to the same router.

---

3. Scanned the Network with Nmap

I ran the following command to perform a basic scan:

```
nmap -sS 192.168.1.0/24
```

This scanned all devices on my local network and showed me which ports were open on each one.

---

4. Noted Down the Results

I looked at each device Nmap found and made note of:

- The IP address
- Which ports were open
- What service was running on each port

For example:

```
192.168.1.10
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
445/tcp  open  microsoft-ds
```

---

5. (Optional) Analyzed Packets with Wireshark

To get more insight, I opened Wireshark and watched the traffic during the scan. It helped me see how Nmap was communicating with each device and which protocols were in use.

---

6. Looked Up the Services

I looked up what the common ports mean:

- **22 (SSH)** – Secure login to remote devices
- **80 (HTTP)** – Regular websites (not encrypted)
- **445 (SMB)** – Windows file sharing

Some of these, like **SMB (445)**, are known to be risky if exposed outside the network.

---

7. Identified Security Risks

I asked myself:

- Do these services really need to be running?
- Are they up to date?
- Could someone from outside the network access them?

For example, SMB on port 445 is commonly targeted by ransomware, so it's something to keep an eye on.

---

8. Saved the Scan Results

To keep a record, I saved my scan like this:

```
nmap -sS 192.168.1.0/24 -oN my_scan_results.txt
```

This gave me a clean text file I could use for reporting or further analysis.

📝 Final Summary

IP Address	Open Ports	Services	Risk Level
192.168.1.1	80, 443	HTTP, HTTPS	Low
192.168.1.5	139, 445, 3389	NetBIOS, SMB, RDP	High
192.168.1.10	22, 3306	SSH, MySQL	Medium

✅ What I Learned

- How to scan a local network using Nmap
- How to identify which services are running on each device
- How to recognize which ports could be potential security risks
- How to document findings for future reference

Let me know if you'd like this in PDF format, or if you'd like help creating a security recommendation based on your results.