Steps Followed for Task 1 – Port Scanning Using Nmap

⚙️ 1. Environment Setup

- **OS Used:** Kali Linux
- Verified active network interface using:
- **Local IP:** 192.168.76.8
- **Subnet:** 255.255.255.0 → **CIDR:** 192.168.76.0/24

🛠️ 2. Installed Tools

- Installed **Nmap** (already available in Kali Linux) and checked it's version.
- Opened **Wireshark** for optional network packet analysis (already available in Kali Linux).

🔍 3. Performed Nmap TCP SYN Scan

Ran the following command in the terminal:

bash

- This scanned 256 IPs in the local network for open TCP ports.

💾 4. Saved Scan Results

Saved the output using:

nmap -sS 192.168.76.0/24 -oN nmapScanResult.txt

- This saved the scan result in a file for documentation.

📊 5. Interpreted Nmap Results

Found 3 hosts:

1. **192.168.76.122** – Open port 3306/tcp → MySQL
2. **192.168.76.184** – Open port 53/tcp → DNS
3. **192.168.76.8** (My own machine) – All ports closed

🔐 6. Security Risk Analysis

- Identified services and possible security risks (e.g., exposed MySQL or DNS ports).
- Documented findings in a table.

🧪 7. Captured Packets Using Wireshark

- Opened Wireshark and started a capture on eth0
- Ran the Nmap scan while capturing
- Applied filters like:
  ip.addr == 192.168.76.122 || ip.addr == 192.168.76.184
  tcp.flags.syn == 1 && tcp.flags.ack == 0
- Observed:
  - **SYN** packets from my host
  - **SYN-ACK** replies from target open ports
  - **RST** responses from closed ports
- Saved capture as wiresharkResult.pcapng

🧠 8. Answered Interview Questions

Prepared answers for:

- Open ports
- TCP vs UDP scanning
- Nmap's SYN scan method
- Risks and security measures
- Role of firewall
- Use of Wireshark in recon

📁 9. Created GitHub Repository

- Repository structure:

ElevateLabs_Task1 /

```
├── README.md
├──nmapScanResult.txt
├── stepsForTask1.pdf
├── nmapResultSummary.pdf
├── wiresharkResult.pcapng
└── 📁 screenshots/
      ├──ifconfigResult.png
      ├──nmapAvailabilityCheck.png
      ├── wiresharkCapturedPacketAnalysis.png
      └── nmapResult.png
```

- Added all task artifacts
- Wrote README.md including:
    - Objective
    - Tools
    - Steps
    - Results
    - Risk Analysis
    - Wireshark analysis