Task 1: Scan Your Local Network for Open Ports Using Nmap and Wireshark

---

1. Objective

To discover open ports on devices within the local network to understand network exposure and identify potential security risks.

---

2. Tools Used

- **Nmap** – For scanning open ports.
- **Wireshark** – For analyzing network traffic (optional, used in this task).

---

3. Key Concepts Covered

- Network Reconnaissance
- Port Scanning
- TCP SYN Scan (-sS)
- IP Addressing and Subnet Ranges
- Identifying Common Services
- Network Security Awareness

---

4. Procedure

4.1 Determine Local IP Range

- Run ipconfig (Windows) or ifconfig (Linux/macOS).
- Identify IP range, e.g., 192.168.1.0/24.

4.2 Perform TCP SYN Scan with Nmap

```
bash
CopyEdit
nmap -sS 192.168.1.0/24
```

- This performs a stealth SYN scan to discover open ports without completing TCP handshakes.

4.3 Save Scan Results

```
bash
CopyEdit
nmap -sS 192.168.1.0/24 -oN scan_results.txt
```

4.4 Analyze Network Packets with Wireshark

- Open Wireshark.
- Start capture on the active interface.
- Apply display filter: tcp.flags.syn==1 && tcp.flags.ack==0 (for SYN packets).
- Observe network discovery and Nmap activity.

5. Findings

IP Address	Open Ports	Common Services	Notes
192.168.1.1	80, 443	HTTP, HTTPS	Router interface
192.168.1.10	22, 139, 445	SSH, SMB	Likely a Linux/Windows machine
192.168.1.12	3389	Remote Desktop	Windows system

6. Common Services and Risk Analysis

Port	Service	Description	Risk
22	SSH	Remote shell	Brute force attacks if open to external network
80	HTTP	Web server	Susceptible to web vulnerabilities
445	SMB	Windows File Sharing	Can expose file system if misconfigured

7. Security Implications

- Open ports reveal active services; attackers can exploit vulnerabilities in these services.
- Reducing the number of open ports and enforcing firewalls strengthens the network perimeter.
- Intrusion Detection Systems (IDS) should monitor unusual scanning activity.

---

8. Conclusion

This task helped in:

- Gaining practical experience with **Nmap** and **Wireshark**.
- Understanding how devices expose services over the network.
- Identifying potential vulnerabilities due to open ports.