Task 1 – Local Network Port Scan Report

Name: Pratiksha Baviskar

Task: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools Used: Nmap (free)

---

1. Tools and Setup

✅ Tool Installed:

- **Nmap**: Installed via

  sudo apt install nmap

  (Linux)
  or downloaded **Nmap Windows installer** from nmap.org.

✅ Optional Tool:

- **Wireshark** (for packet capture analysis if required).

---

2. Scanning Commands Performed

A. Identify Devices on Local Network

nmap -sn 192.168.1.0/24

🔹 **Purpose:** Finds all live hosts in the subnet 192.168.1.0/24.

B. Scan Open Ports on a Specific Device

nmap -sV 192.168.1.10

🔹 **Purpose:**

- Scans **192.168.1.10** (example IP)
- Lists open ports and services running on them.

C. Aggressive Scan (Optional)

nmap -A 192.168.1.10

🔹 **Purpose:**

- Enables OS detection, version detection, script scanning, and traceroute for detailed analysis.

---

3. Sample Scan Output

Starting Nmap 7.80 (https://nmap.org) at 2025-06-29 19:00 IST
Nmap scan report for 192.168.1.10
Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

---

4. Findings

✅ **Device IP:** 192.168.1.10
✅ **Open Ports:**

- **22/tcp – SSH** (Remote login access)
- **80/tcp – HTTP** (Web server)
- **139/tcp & 445/tcp – Samba SMB** (File sharing)

---

5. Conclusion

✓ Key Learnings:

- Identified devices on the local network using Nmap.
- Discovered open ports and running services on each device.
- Understood potential **network exposure risks** (e.g. if SSH is open with weak passwords or if file sharing is exposed).