DAY 1 - TASK 1

**Objective**: Learn to discover open ports on devices in your local network to understand network exposure.
**Tools**: Nmap (free), Wireshark (optional).

Network Scanning Report

1. Installation of NMAP

   I downloaded and installed Nmap from the official nmap.org website, ensuring I had the latest version (7.94SVN).

2. Finding my local IP range

   I identified my local IP address and determined that my network falls within the **192.168.56.0/24** range. This helped scope the Nmap scan properly.

3. Scanning using command

   I ran a TCP SYN scan (`-sS`) on the local subnet to discover live hosts and open ports without making full TCP connections.

   **A) Command** : nmap -sS 192.168.56.0

   **Purpose:** Performs a basic scan on the target IP `192.168.56.1` to discover open ports and services.

   **Result:**
   **-** Host is **up** (reachable).
   - **Port 3306/tcp** is **open**, running the **MySQL** service.
   - All other 999 ports are filtered (no response).
   - MAC Address is detected: `0A:00:27:00:00:03` (vendor unknown).
   - Scan duration: ~17.69 seconds.

   **B) Command** : nmap -sV -p 3306 192.168.56.1

   **Purpose:**
   **-** `-sV` enables **version detection** to identify the software and version running on an open port.
   - `-p 3306` limits the scan to **port 3306** only.

**Result:**
**-** Host is again confirmed as **up**.
- Port **3306/tcp** is **open**, running **MySQL**.
- The service responded with version info: `MySQL (unauthorized)`, indicating access is restricted without credentials.
- Same MAC address is detected.
- Scan duration: ~13.47 seconds.

4. Noting down IP addresses and open ports found

   **Discovered Host:** `192.168.56.1`
   **Open Port:** `3306/tcp`
   **Service:** `MySQL` (version detection showed "unauthorized" access status)

5. Optionally analyzing packet capture with Wireshark

   While I did not include a full Wireshark packet capture for this submission due to an installation error, I understand that analyzing traffic to/from port 3306 could reveal plaintext SQL traffic or authentication attempts, which is useful in detecting security misconfigurations.

6. Research common services running on those ports

   Port **3306** is used by **MySQL**, a widely used relational database system. By default, MySQL does not encrypt traffic, and if exposed to the network, it can be vulnerable to brute-force attacks, unauthorized access, and data leaks.

7. Identify potential security risks from open ports

   **Unauthorized access** - if MySQL is not properly secured
   **Plaintext data transmission** (no SSL/TLS)
   **Brute-force and dictionary attacks**
   **SQL injection risks** - if exposed via web apps

8. Save scan results as a text or HTML file

   # Nmap 7.94SVN scan initiated at 2025-08-04 15:54 IST
   Nmap scan report for 192.168.56.1
   Host is up (0.000060s latency).
   Not shown: 999 filtered tcp ports (no-response)
   PORT     STATE SERVICE
   3306/tcp open  mysql

MAC Address: 0A:00:27:00:00:03 (Unknown)

# Nmap done at 2025-08-04 15:54 IST -- 1 IP address (1 host up) scanned in 17.69 seconds

# Nmap 7.94SVN scan initiated at 2025-08-04 15:55 IST
Nmap scan report for 192.168.56.1
Host is up (0.000052s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 0A:00:27:00:00:03 (Unknown)

# Nmap done at 2025-08-04 15:55 IST -- 1 IP address (1 host up) scanned in 13.47 seconds