**Day 1 Internship Report — Cyber Security**

**Task: Local Network Port Scanning Using Nmap**

**Intern Name: Konakalla Trishul**

**Date: 04 August 2025**

**Task Title: Port Scanning on Local Network (TCP SYN Scan)**

**Tools Used:**

* Nmap 7.97
* Command Prompt (Windows 10)
* Subnet Mask Analysis
* CIDR Notation
* GitHub for Documentation

**Objective**

To explore and analyze the exposure of devices on my local network by performing a TCP SYN scan using Nmap, thereby identifying open ports and understanding the basic risks of exposed services.

**Network Environment Details**

| **Parameter** | **Value** |
| --- | --- |
| IPv4 Address | 192.168.1.45 |
| Subnet Mask | 255.255.255.0 |
| CIDR Notation | /24 |
| Scanned IP Range | 192.168.1.0/24 |
| Total IPs Scanned | 256 |

**Command Used**

bash

CopyEdit

nmap -sS 192.168.1.0/24 -oN result.txt

* -sS : TCP SYN (Stealth) Scan
* /24 : Full local subnet
* -oN : Output saved in normal text format (result.txt)

**Scan Summary**

| **IP Address** | **Host Info / MAC** | **Open Ports / Services** |
| --- | --- | --- |
| 192.168.1.1 | ZTE Router | 53 (DNS), 80 (HTTP), 443 (HTTPS), 23 (Telnet\*) |
| 192.168.1.21 | Unknown | 7 (Echo - filtered) |
| 192.168.1.45 | My Machine | 135 (MSRPC), 139 (NetBIOS), 445 (SMB), 903 (VMware), 3306 (MySQL), 5432 (PostgreSQL) |
| Others (1.6, 1.13, etc.) | Xiaomi, Samsung, Unknown | All 1000 ports closed or reset (safe) |

Telnet (Port 23) is outdated and unencrypted — should be disabled.  
 Port 445 is vulnerable to SMB exploits (e.g., EternalBlue used by WannaCry).  
 Ports 3306 & 5432 expose databases and should be protected by firewalls.

**Analysis & Insights**

1. **My Router (192.168.1.1)**:
   * Exposed HTTP and Telnet services.
   * Suggestion: Disable Telnet and use HTTPS for management.
2. **My System (192.168.1.45)**:
   * MySQL and PostgreSQL ports are open. Should be restricted to localhost or protected by a firewall.
   * File sharing services (SMB) like port 445 are frequently targeted in cyber attacks — ensure only needed services are allowed.
3. **Other Devices**:
   * Several smartphones and smart devices showed no open ports — which is good.
   * One device responded on port 7 (Echo), which is mostly harmless but filtered.

**What I Learned**

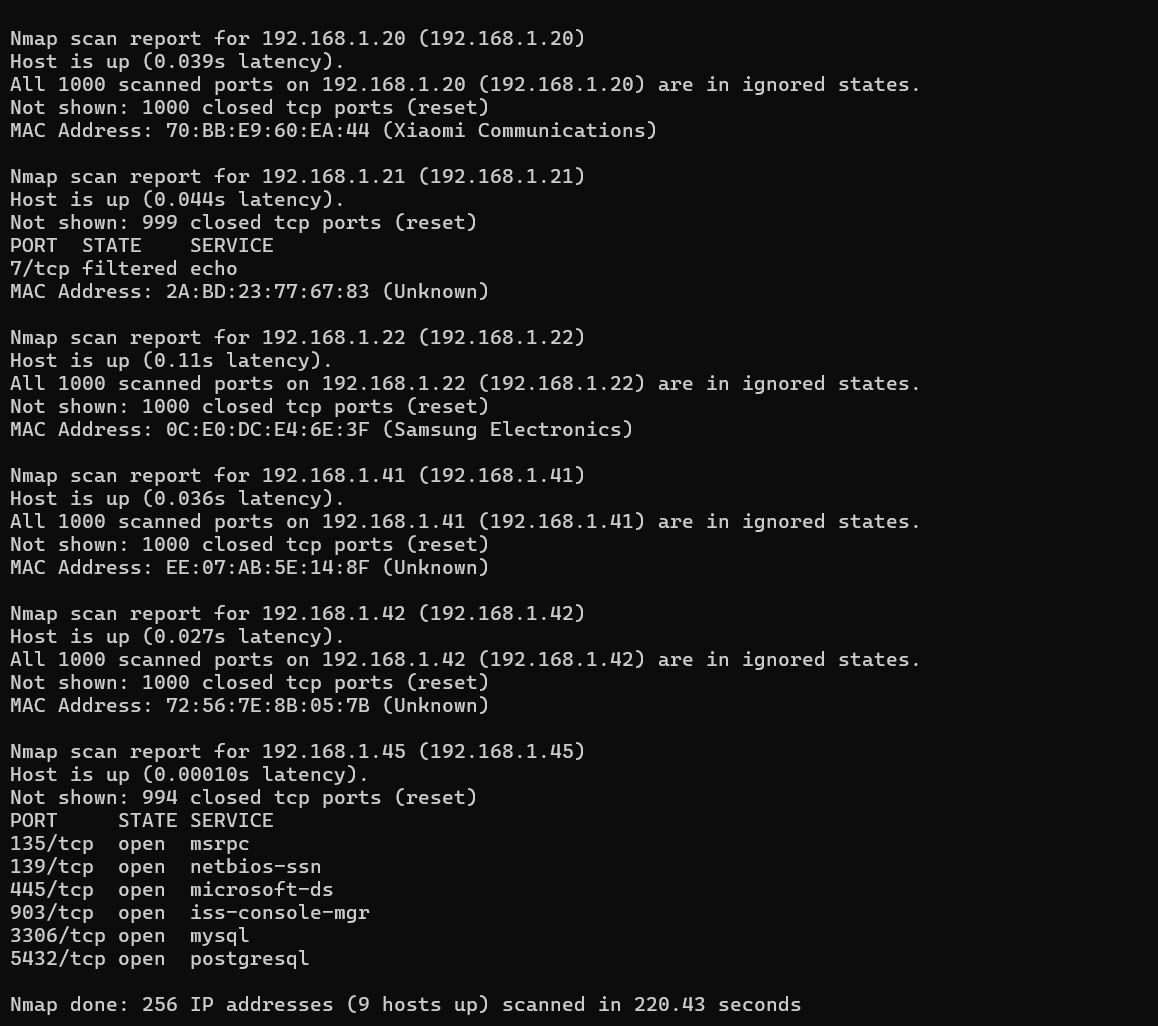
* How to find CIDR from Subnet Mask (255.255.255.0 → /24)
* How Nmap performs stealthy SYN scans to detect services
* Importance of port exposure in cybersecurity
* How open ports can lead to real-world exploits
* How to document cybersecurity tasks for real-world reporting

**Files in This Repository**

| **File Name** | **Description** |
| --- | --- |
| result.txt | Full raw output of the Nmap scan |
| README.md | This report with summary, analysis & insights |
| screenshot.png | Terminal snapshot of the scan |

**Conclusion**

This task gave me real-world insight into how attackers perform reconnaissance on a network. It also showed me how exposed ports can reveal sensitive services, even in a simple home Wi-Fi network. Closing unnecessary ports and configuring firewalls are crucial for security.

A screenshot of a computer program

AI-generated content may be incorrect.