**Cybersecurity Internship Task Report**

**Task Name:** Local Network Port Scanning using Nmap  
**Intern:** Sakshi Shetti  
**Date of Scan:** August 4, 2025 at 07:01 PM  
**Tool Used:** Nmap 7.95 (Zenmap GUI)  
**System Used:** Windows  
**IP Scanned:** 192.168.0.122  
**Scan Command:** nmap -T4 -A -v 192.168.0.122

**Objective**

The goal of this task was to perform a local network reconnaissance scan to identify open ports and services running on a device within the same local Wi-Fi network. This helps assess exposure to potential security threats.

**Scan Results**

* **Host Status:** Online
* **Latency:** 0.00071s
* **Open Ports and Services:**

| **Port** | **State** | **Service** | **Description** |
| --- | --- | --- | --- |
| 135 | Open | Microsoft RPC | Used for remote procedure calls |
| 139 | Open | NetBIOS-SSN | Used for Windows file sharing |
| 445 | Open | Microsoft-DS (SMB) | Used for file sharing; high risk |

* **Operating System Detected:** Microsoft Windows (exact version not confirmed)
* **Uptime Guess:** ~1.17 days
* **Network Distance:** 0 hops (same LAN)

**Security Analysis**

1. **Port 445 (SMB):** High-risk port often targeted in ransomware attacks like WannaCry.
2. **Port 139 (NetBIOS):** Allows enumeration of shared files and users; outdated protocol.
3. **Port 135 (RPC):** Can be used for DCOM exploitation or lateral movement.
4. **SMB Signing:** Enabled but not required — this allows for potential Man-in-the-Middle attacks.

**Skills Demonstrated**

* Network scanning with Nmap
* Service detection and port analysis
* Basic network enumeration
* Risk assessment based on open ports

**Outcome**

I have successfully completed a real-world cybersecurity reconnaissance task by scanning a device on my local network. I discovered 3 critical open ports, analyzed their services, and assessed the associated risks.

This task demonstrates strong foundational knowledge of network security tools and vulnerability exposure.