**Intern Name:** Swapnil Dixit  
**Date:** 22/09/2025  
**Tool Used:** Nmap (with Npcap on Windows)

**1. 🎯 Objective**

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

**2. 🖥️ Environment Details**

| **Parameter** | **Value** |
| --- | --- |
| Operating System | Windows 10 |
| Scanner Tool | Nmap v7.98 |
| Packet Driver | Npcap |
| Network Range | 192.168.1.0/2 |

*Use ipconfig to confirm your IP and subnet mask.*

**3. ⚙️ Scan Configuration**

**Command Used:**

nmap -sS 192.168.1.0/24 -T4 -v -oN scan\_results.txt

**Scan Type:**

* TCP SYN (Stealth) Scan
* Verbose Mode
* Saved Output to Text File

**4. 📋 Scan Results Summary**

| **IP Address** | **Status** | **Open Ports** | **Services Detected** |
| --- | --- | --- | --- |
| 192.168.1.1 | Up | 80, 443 | HTTP, HTTPS |
| 192.168.1.5 | Up | 22 | SSH |
| 192.168.1.09 | Up | 3306 | MySQL Database |
| 192.168.1.13 | Up | 139, 445 | SMB (Windows File Share) |
|  |  |  |  |

Full scan file saved as: scan\_results.txt

**5. 🔍 Service and Port Analysis**

| **Port** | **Common Service** | **Description** | **Risk Level** | **Notes** |
| --- | --- | --- | --- | --- |
| 22 | SSH | Remote Shell Access | Medium | Ensure strong password or key-only auth |
| 80 | HTTP | Web Server | Low | No HTTPS on some hosts |
| 3306 | | MySQL | Database | High | Should not be exposed to LAN unless needed |
| 139, 445 | SMB | File Sharing | High | Often vulnerable to exploits (e.g., EternalBlue) |
|  |  |  |  |  |

**6. 🛡️ Security Observations**

* Several hosts expose critical services like **SMB** and **MySQL** to the local network.
* No evidence of firewalls blocking unused ports on some machines.
* At least one host does not redirect HTTP to HTTPS — possible unencrypted login risk.
* No detected IDS/IPS responses to the scan — low alerting/monitoring observed.

**7. 📝 Recommendations**

* **Disable unnecessary services** on non-server hosts.
* **Restrict SSH/MySQL** access to specific IPs using firewall rules.
* **Update SMB servers** and ensure patches are applied.
* **Enforce HTTPS** across all web services.
* Consider using an IDS/IPS (e.g., Snort, Suricata) for scan detection.

**✅ Conclusion**

The Nmap scan provided valuable insight into live hosts and exposed services in the local network. Based on the open ports and service detection, several moderate to high-risk issues were identified. Appropriate hardening and monitoring measures are recommended.