Task1 Report

Overall Status: **Complete**

Project Name: **Scan Your Local Network for Open Ports**

Date: 26/05/25

Target IP Address: 192.168.x.x

Scan Tool: nmap

Observation: Following ports were found open:

```
Host is up (0.0083s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
```

Summary of the ports

135/tcp – MSRPC (Microsoft RPC)

- **Service:** Microsoft Remote Procedure Call (MSRPC)
- **Purpose:** Used for RPC-based communication, such as DCOM and administrative tasks (e.g., remote services management, WMI).
- **Common Use Case:** Allows Windows applications to communicate over a network.
- **Security Note:** Often targeted in Windows exploits; should be restricted on firewalled systems.

139/tcp – NetBIOS Session Service

- **Service:** NetBIOS Session Service (NetBIOS over TCP/IP)
- **Purpose:** Supports file and printer sharing over NetBIOS on older Windows systems.
- **Common Use Case:** Legacy SMB file sharing (pre-Windows 2000).
- **Security Note:** Largely obsolete; should be disabled if not needed.

445/tcp – Microsoft-DS (Direct SMB)

- **Service:** Microsoft Directory Services (SMB over TCP)
- **Purpose:** Used for modern Windows file sharing and Active Directory.
- **Common Use Case:** SMB (Server Message Block) for file, printer, and network resource sharing.
- **Security Note:** Commonly targeted in ransomware and malware attacks (e.g., WannaCry).

3306/tcp – MySQL

- **Service:** MySQL Database Server
- **Purpose:** Default port for MySQL database service.
- **Common Use Case:** Database operations for web and application backends.
- **Security Note:** Should be firewalled or tunneled; avoid exposing it directly to the internet.

5357/tcp – WSDAPI (Web Services on Devices)

- **Service:** Web Services for Devices API (WSDAPI)
- **Purpose:** Enables device discovery and communication (like printers or scanners) on local networks using SOAP over HTTP.
- **Common Use Case:** Plug-and-play device discovery in Windows environments.
- **Security Note:** Typically used only on trusted local networks.

Potential Risks

Port	Service	Potential Risks	Common Exploits / Threats	Mitigation
135/tcp	MSRPC	- Remote code execution (RCE) - Lateral movement - Service enumeration	MS08-067, WannaCry, Conficker	Block externally, restrict access, patch regularly
139/tcp	NetBIOS-SSN	- Information leakage - NTLM relay attacks - Legacy SMB vulnerabilities	SMB Relay, name/share enumeration	Disable if unused, block externally, enforce modern SMB protocols
445/tcp	Microsoft-DS (SMB)	- RCE via SMB vulnerabilities - Malware propagation - Data leakage	EternalBlue, WannaCry, NotPetya	Disable SMBv1, patch frequently, block externally, use strong access controls
3306/tcp	MySQL	- Brute-force login attempts - Unauthorized data access - SQL injection	Credential guessing, app-layer SQLi	Never expose to internet, strong creds, use firewalls/VPN
5357/tcp	WSDAPI	- Uncontrolled device discovery - Local attack surface expansion - Recon	SOAP-based enumeration	Disable if unused, restrict to trusted subnets, monitor traffic