# Task 1: Local Network Port Scan Report

Name: RACHANA J

Date: 20/10/2025

Objective: Discover open ports in the local network and identify potential security risks.

## 1. Scope

Network scanned: 10.XXX.XX.0/24  
Tool used: Nmap (-sS TCP SYN scan)  
Optional tools: Wireshark (not used)

## 2. Hosts Found and Open Ports

### Host 1: 10.1XX.XX.XXX

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Service | Risk | Notes / Recommendations |
| 53/tcp | DNS | Low | Likely router or DNS server. No action required. |

### Host 2: XX.XXX.XX.XXX

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Service | Risk | Notes / Recommendations |
| 135/tcp | MSRPC | Medium | Windows RPC service; ensure firewall is enabled. |
| 139/tcp | NetBIOS-SSN | High | File sharing; disabled on this machine. |
| 445/tcp | Microsoft-DS | High | File sharing; disabled on this machine. |
| 3306/tcp | MySQL | High | Database service in use by the user. |

## 3. Potential Security Risks

1. Open file-sharing ports (139, 445) could allow unauthorized access if misconfigured.  
2. Open database port (3306) may expose sensitive data if not securely configured.  
3. MSRPC (135) could be leveraged if the host is unpatched.

## 4. Recommended Actions

**Immediate actions taken:**

- File and printer sharing: Disabled (confirmed by user).

- MySQL: In use by the user (do not stop); apply hardening steps below.

MySQL hardening recommendations:

1. Bind MySQL to localhost if remote access is not required: set `bind-address = 127.0.0.1` in my.cnf/my.ini.

2. Use strong passwords for all MySQL accounts and remove anonymous accounts.

3. Run the MySQL secure installation utility (`mysql\_secure\_installation`) to enforce secure settings.

4. Ensure MySQL runs under a dedicated, limited-permission user account.

5. If remote access is required, restrict access by firewall to specific IP addresses and use TLS for encryption.

General network hardening:

- Ensure Windows Firewall is enabled and inbound rules block SMB (139/445) and MySQL (3306) from the LAN/WAN except where needed.

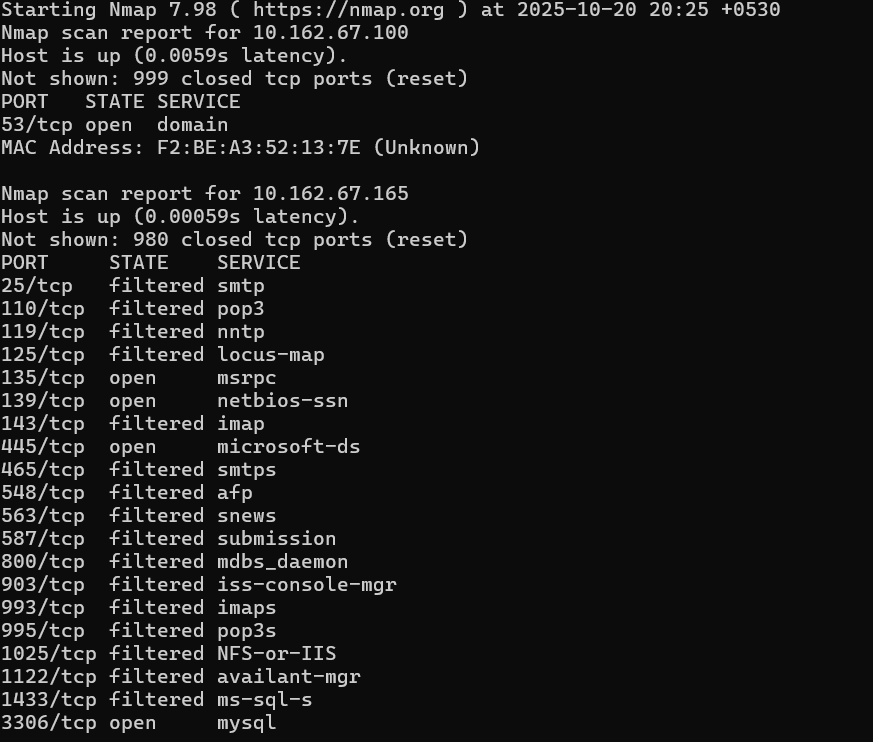
- Keep Windows and all device firmware up to date.

- Change default passwords on routers and IoT devices and disable unused services.

- Remove unnecessary port forwarding on the router.

- Schedule periodic Nmap scans to monitor the network.

## 5. Evidence / Attachments

Nmap scan output saved as: local\_scan\_results.txt .

## Task Completion Status

All mandatory steps for Task 1 completed. Optional packet capture and intrusive vulnerability scanning were skipped.