Task 1: Local Network Port Scan (Nmap)

Author: CHETAN M
Date: 2025-10-20
Tool(s): Nmap 7.98

---

1. Objective

Perform a basic TCP port scan on a local host to identify open services and assess network exposure.

---

2. What I did

1. Identified my local host IP and target for scanning.
2. Used **Nmap** to scan for open TCP ports on this host.
3. Saved the scan output and captured a screenshot of the terminal output.
4. Analyzed open ports and corresponding services.
5. Assessed potential risks and suggested mitigations.
6. Sanitized output and screenshot before publishing for privacy.

---

3. Commands Used

Basic SYN scan (single host)

nmap -sS <TARGET_IP> -oN scan_results.txt

Optional detailed scan with service and OS detection

nmap -T4 -A -v <TARGET_IP> -oX results.xml

xsltproc results.xml -o results.html # optional: convert XML to HTML

Replace <TARGET_IP> with your own target host when reproducing.

---

4. Scan Output (Screenshot)

The screenshot of the scan result is included in the repository as screenshot_redacted.png.

---

5. Sanitized Scan Output

Starting Nmap 7.98 (https://nmap.org) at 2025-10-20 20:13 +0530

Nmap scan report for REDACTED_IP

Host is up (0.00012s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 3.63 seconds

---

6. Findings & Analysis

Open Ports Identified

Port	Service	Description
135/tcp	msrpc	Windows RPC service used for remote management.
139/tcp	netbios-ssn	NetBIOS Session Service (used for file sharing).
445/tcp	microsoft-ds	SMB over TCP (file and printer sharing).
3306/tcp	mysql	MySQL database service (requires authentication).

Summary:
These ports indicate common Windows services (RPC, NetBIOS, SMB) and a MySQL database running on the host. While these are normal for internal networks, leaving them open unnecessarily increases potential attack surfaces.

---

7. Risk Assessment

- **RPC/SMB (135, 139, 445):** Frequently targeted by malware and exploits. Should be firewalled or disabled if not needed.
- **MySQL (3306):** Exposing a database port externally can allow attackers to attempt brute-force logins or exploit unpatched vulnerabilities.
- **General:** Multiple open ports increase attack surface; all unnecessary services should be disabled or restricted.

---

8. Recommendations

1. **Disable Unused Services** — Turn off MySQL, SMB, or RPC if not required.
2. **Enable Firewall Rules** — Allow only trusted IPs to access essential services.
3. **Restrict MySQL Access** — Bind MySQL to localhost if remote connections are not needed.

4. **Update and Patch Regularly** — Keep OS and applications updated to prevent exploitation.
5. **Use Strong Authentication** — Require complex passwords for all services.
6. **Segment Networks** — Isolate VMs, IoT, or test devices from production systems.
7. **Monitor Traffic** — Use security monitoring tools to detect unusual access patterns.

9.RESULT SCREENSHOT