==========

INTERNSHIP REPORT – TASK 1

==========

Student Name: Solanki Bhumirajsinh
Date: 08 December 2025
Task: Local Network Scan Using Nmap

---

1. Objective

The objective of this task was to scan the local network using Nmap to identify open ports on devices, analyze running services, and evaluate potential security risks. This helps in understanding network exposure and basic network reconnaissance skills.

---

2. Tools Used

- Nmap (Network Mapper)
- Windows Command Prompt
- Wireshark (Optional)

---

3. Local IP & Network Range

- IPv4 Address: 192.168.43.177
- Subnet Mask: 255.255.255.0
- Network Range: 192.168.43.0/24

---

4. Scan Commands

- Full network scan:
  nmap -sS 192.168.43.0/24
- Scan own device:
  nmap -sV 192.168.43.177

---

5. Scan Output

Nmap scan report for 192.168.43.177

Host is up (0.000082s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

---

6. Open Ports & Services

Port	Service	Purpose
135	MSRPC	Windows Remote Procedure Call (internal communication)
139	NetBIOS	Old LAN file sharing protocol
445	SMB	Modern Windows file sharing protocol

---

7. Risk Analysis

Port	Risk Level	Potential Threat
135	Medium	May allow remote commands if exploited
139	Medium-High	Can leak system information on local network
445	High	Vulnerable to ransomware attacks

Mitigation Steps Taken:

- Network discovery turned OFF
- File & Printer Sharing turned OFF
- SMBv1 disabled
- Firewall rules configured to block unnecessary ports

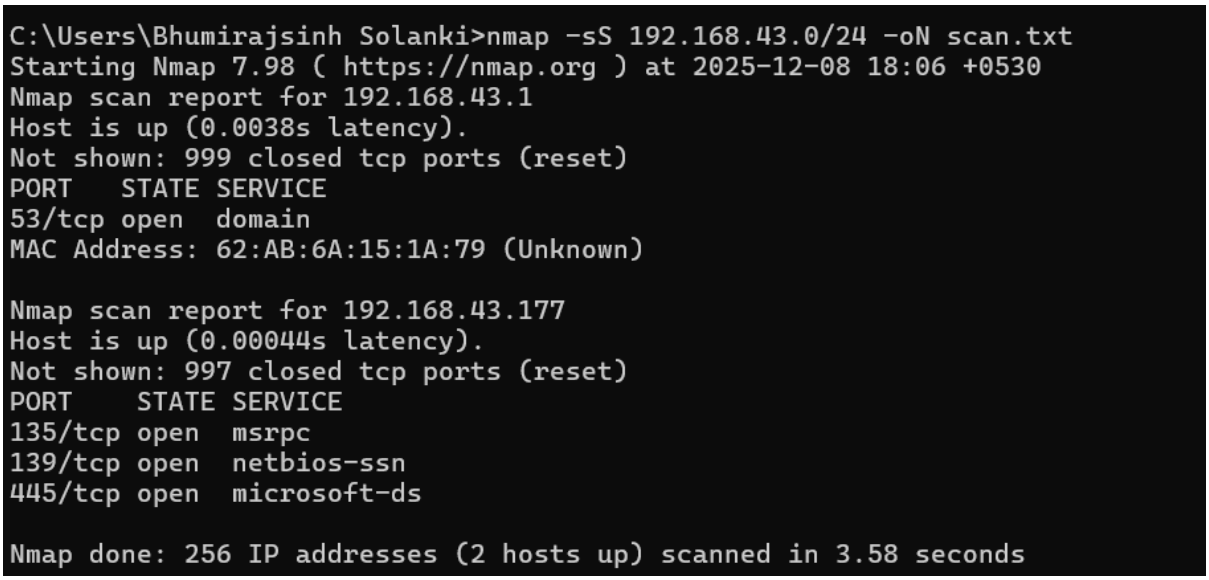
---

8. Conclusion

The network scan successfully identified open ports and their services. Potential security risks were analyzed and mitigated. This task helped in understanding basic network reconnaissance and network exposure assessment.

Attachments:

- **Scan result file:** "C:\Users\Bhumirajsinh Solanki\scan.txt"
- **Optional:** Screenshot of scan output



```
C:\Users\Bhumirajsinh Solanki>nmap -sS 192.168.43.0/24 -oN scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-08 18:06 +0530
Nmap scan report for 192.168.43.1
Host is up (0.0038s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 62:AB:6A:15:1A:79 (Unknown)

Nmap scan report for 192.168.43.177
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.58 seconds
```