# Task 1

Scan Your Local Network for Open Ports.

1. Local IP range found and ran nmap, performed TCP SYN Scan.
2. Noted down the Open ports found and listed below
3. Accessed and analysed the potential risks and vulnerabilities.
4. Saved results are attached in the Task submission sheet.
5. Interview questions prepared.

|  |  |
| --- | --- |
| Scan Tool | Nmap |
| Scan Type | TCP SYN Scan (-sS) |
| Target Network | 192.168.\*.1/24 |
|  |  |
|  |  |

TCP SYN Results:

PS C:\Users\Ram> nmap -sS 192.168.\*.1/24

Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-23 14:32 +0530

Nmap scan report for 192.168.\*.1 (192.168.\*.1)

Host is up (0.00035s latency).

Not shown: 991 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

3306/tcp open mysql

6881/tcp open bittorrent-tracker

7070/tcp open realserver

Nmap done: 256 IP addresses (1 host up) scanned in 62.26 seconds

Discovered host with 9 open ports.

Scan Results:

| Port | Service : | Description : |
| --- | --- | --- |
| 80 | HTTP | Unencrypted web service |
| 135 | MSRPC | Windows RPC – used by DCOM |
| 139 | NetBIOS-SSN | File/printer sharing (legacy) |
| 443 | HTTPS | Secure web service |
| 445 | Microsoft-DS | SMB over TCP |
| 1025 | NFS-or-IIS | Could be dynamic Windows port or web |
| 3306 | MySQL | Database port |
| 6881 | BitTorrent Tracker | Peer-to-peer file sharing |
| 7070 | RealServer | RealAudio streaming |

* I am running a web server, file share, torrent app, or database intentionally and are updated to patch vulnerabilities.
* Blocked unused ports using:Windows Defender Firewall**.**
* **netstat -ano** used as a command to view active network connections and identify which processes (via PID) are using which ports.