**1. Install Nmap from Official Website**

* from: https://nmap.org/download.html
* Downloaded the appropriate version for my OS (Windows Installer)
* Installed it with default settings (includes a GUI version called **Zenmap**, but we’re using CMD).

**2. Find Your Local IP Range**

Using ipconfig, I found my IP details:

* **IPv4 Address**: 192.168.29.153
* **Subnet Mask**: 255.255.255.0  
  → This means my local IP range is:

192.168.29.0/24

This range includes **all 256 devices (from .1 to .254)** that could be on my Wi-Fi.

**3. Run Nmap TCP SYN Scan**

Open **Command Prompt**, and run:

nmap -sS 192.168.29.0/24

This performs a **stealthy TCP SYN scan** of all devices in network, checking for **open ports**.

**4. Note Down IP Addresses and Open Ports Found**

The scan discovered 4 active devices:

**192.168.29.1 → (Router - Reliance Jio)**

Open Ports:

* 80/tcp → HTTP
* 443/tcp → HTTPS
* 8080/tcp → HTTP Proxy
* 8200/tcp → Trivnet1 (custom)
* 8443/tcp → HTTPS-alt
* 7000/tcp, 7443/tcp → Oracle services

**192.168.29.21 → (Realme Mobile)**

* All ports closed

**192.168.29.24 → (Smart Device - Earda)**

* 2869/tcp → ICSLAP (UPnP related)

**192.168.29.153 → (My PC)**

Open Ports:

* 135/tcp → MSRPC
* 139/tcp → NetBIOS
* 445/tcp → Microsoft-DS
* 1521/tcp → Oracle DB Listener
* 8080/tcp → HTTP Proxy
* 903/tcp → ISS console (possibly VMware)

**5. Optionally Analyze with Wireshark** *(Skipped in my case)*

**6. Research Common Services Running on Those Ports**

| **Port** | **Service** | **Description** |
| --- | --- | --- |
| 80 | HTTP | Unsecured web service |
| 443 | HTTPS | Secure web communication |
| 135 | MSRPC | Remote procedure call (Windows system) |
| 139 | NetBIOS | File/printer sharing |
| 445 | Microsoft-DS | SMB file sharing |
| 8080 | HTTP Proxy | Alt HTTP port (sometimes used by devs) |
| 1521 | Oracle DB | Database listener port |
| 2869 | ICSLAP | Part of UPnP, media streaming |

**7. Identify Potential Security Risks from Open Ports**

**My PC (192.168.29.153) Security Risks:**

* **135/139/445**: High risk — commonly exploited in ransomware and malware.
* **1521**: Sensitive Oracle DB port — should be closed if not in use.
* **8080**: Often targeted by bots — should be monitored or closed if unused.
* **903**: VMware remote console — not needed unless running VMs.

I closed these ports using:

* **Windows Firewall rules**
* **Disabling File and Printer Sharing**
* **Identifying & stopping background services.**

**8. Save Scan Results as a Text File**

To save the scan:

nmap -sS 192.168.29.0/24 -oN scan\_results.txt

This creates a text file named scan\_results.txt in current CMD directory.

I then uploaded this file to **GitHub** along with a report.md and README.md.

**Outcome of the Task**

* Learned to use **Nmap** to scan a local network
* Discovered **active devices and their ports**
* Understood how to **research services**
* Identified and **closed risky ports**
* Practiced **network hardening**
* Uploaded a clean report to **GitHub**