**Task 1: Scan Your Local Network for Open Ports**

**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

**Tools:** Nmap (free), Wireshark (optional)

**Hints/Mini Guide:**

1.Install Nmap from official website.

2.Find your local IP range (e.g., 192.168.1.0/24).

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

4.Note down IP addresses and open ports found.

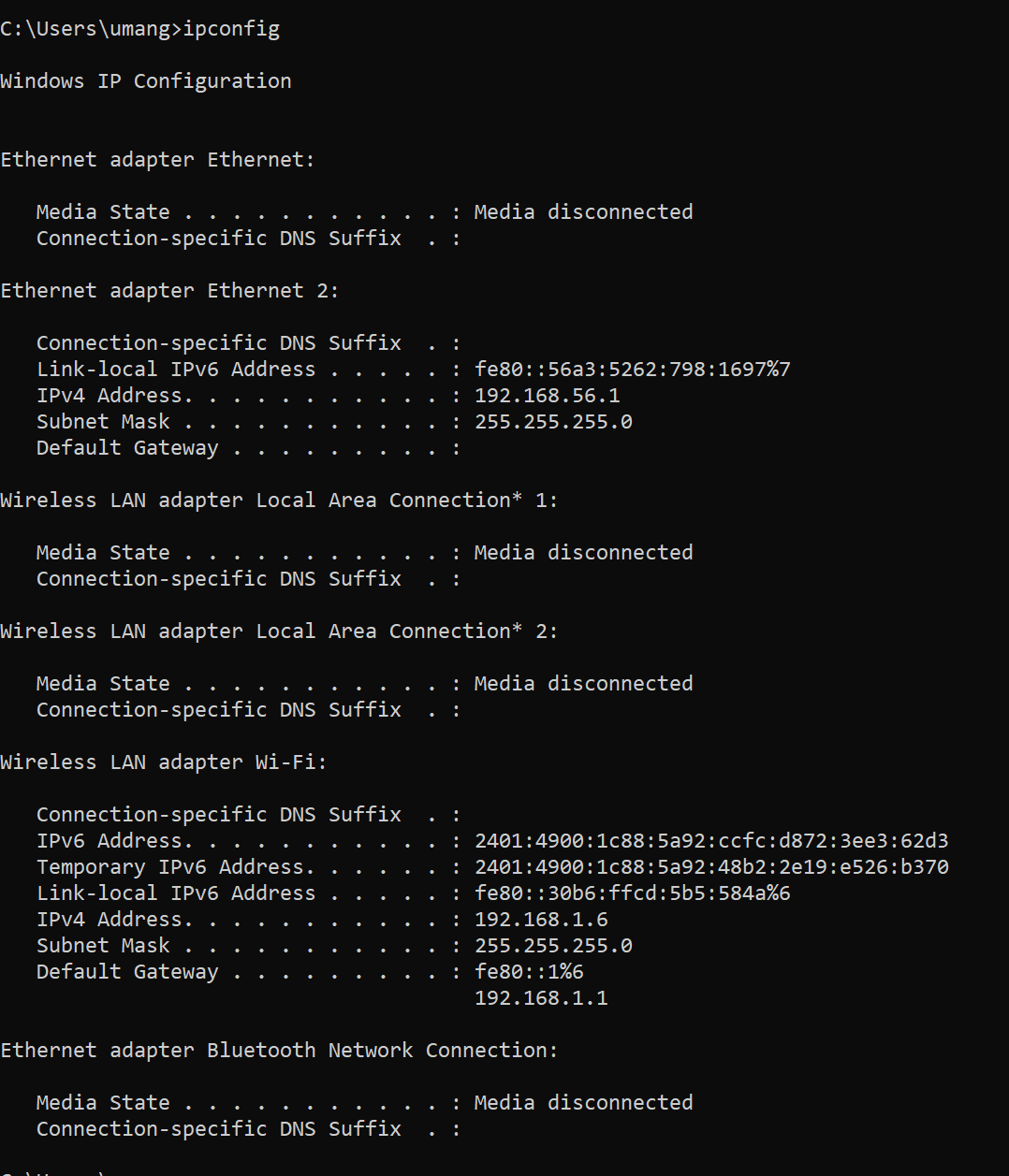
5.Optionally analyze packet capture with Wireshark.

6.Research common services running on those ports.

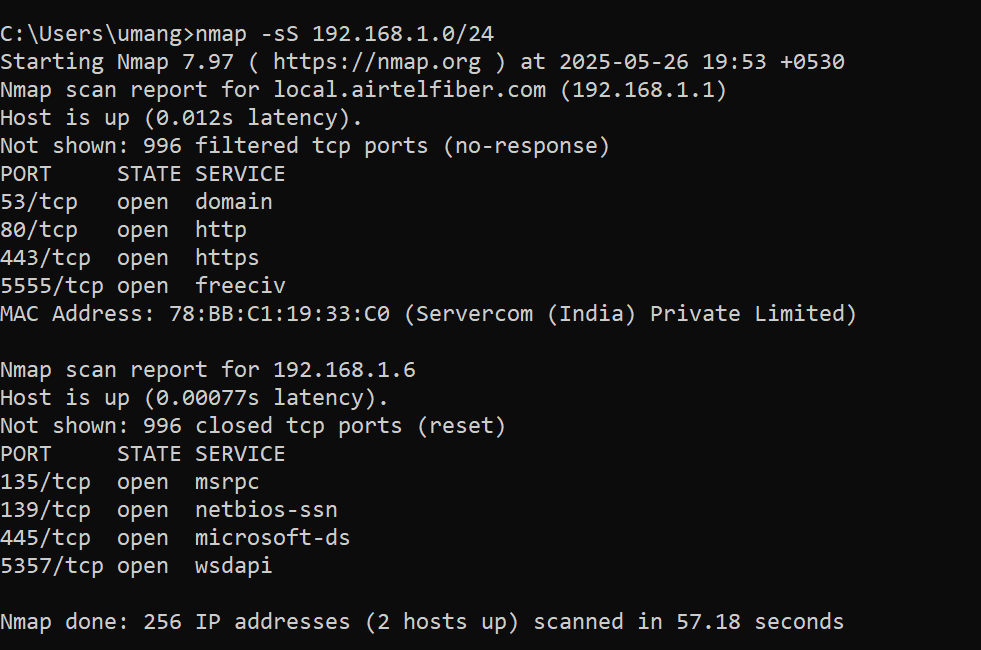
7.Identify potential security risks from open ports.

8.Save scan results as a text or HTML file.

Performing steps as per the guide/hints:



Below are the ports open for the given ip range



**Device 1: 192.168.1.X**

Host is up (0.012s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

5555/tcp open freeciv

MAC Address: 78:BB:C1:19:33:C0 (Servercom (India) Private Limited)

**Port Breakdown**

| **Port** | **Service** | **Description** |
| --- | --- | --- |
| **53** | **domain** | DNS service – used to resolve domain names to IPs. Usually on routers or DNS servers. |
| **80** | **http** | Standard web traffic – might be hosting a web admin page or web service. |
| **443** | **https** | Secure web traffic – typically used for encrypted communications. |
| **5555** | **freeciv** | This is non-standard. Could be: • An Android Debug Bridge (ADB) port• A game like FreeCiv• A backdoor/malware in some cases |

**Risk Analysis**

* **53**: Only risky if it's exposed externally or misconfigured.
* **80 & 443**: Check what web service is running. If no authentication or outdated software is found, it could be a risk.
* **5555**: 🚨 **Potential red flag.** If this is ADB over TCP (common on Android TVs, devices), it can allow remote shell access without a password if not secured. Needs immediate investigation.

**Recommendations**

* Check what device this is (router, smart TV, etc.).
* Try visiting http://192.168.1.X in a browser to see if there's a web interface.
* If port 5555 is ADB, **disable ADB over network** or **firewall it**.

**Device 2: 192.168.1.6**

Host is up (0.00077s 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

5357/tcp open wsdapi

**🔎 Port Breakdown**

| **Port** | **Service** | **Description** |
| --- | --- | --- |
| **135** | **msrpc** | Microsoft RPC – used for DCOM services and remote management. |
| **139** | **netbios-ssn** | File and printer sharing (NetBIOS). |
| **445** | **microsoft-ds** | Windows file sharing (SMB). |
| **5357** | **wsdapi** | Web Services for Devices – used for device discovery on LAN (like printers). |

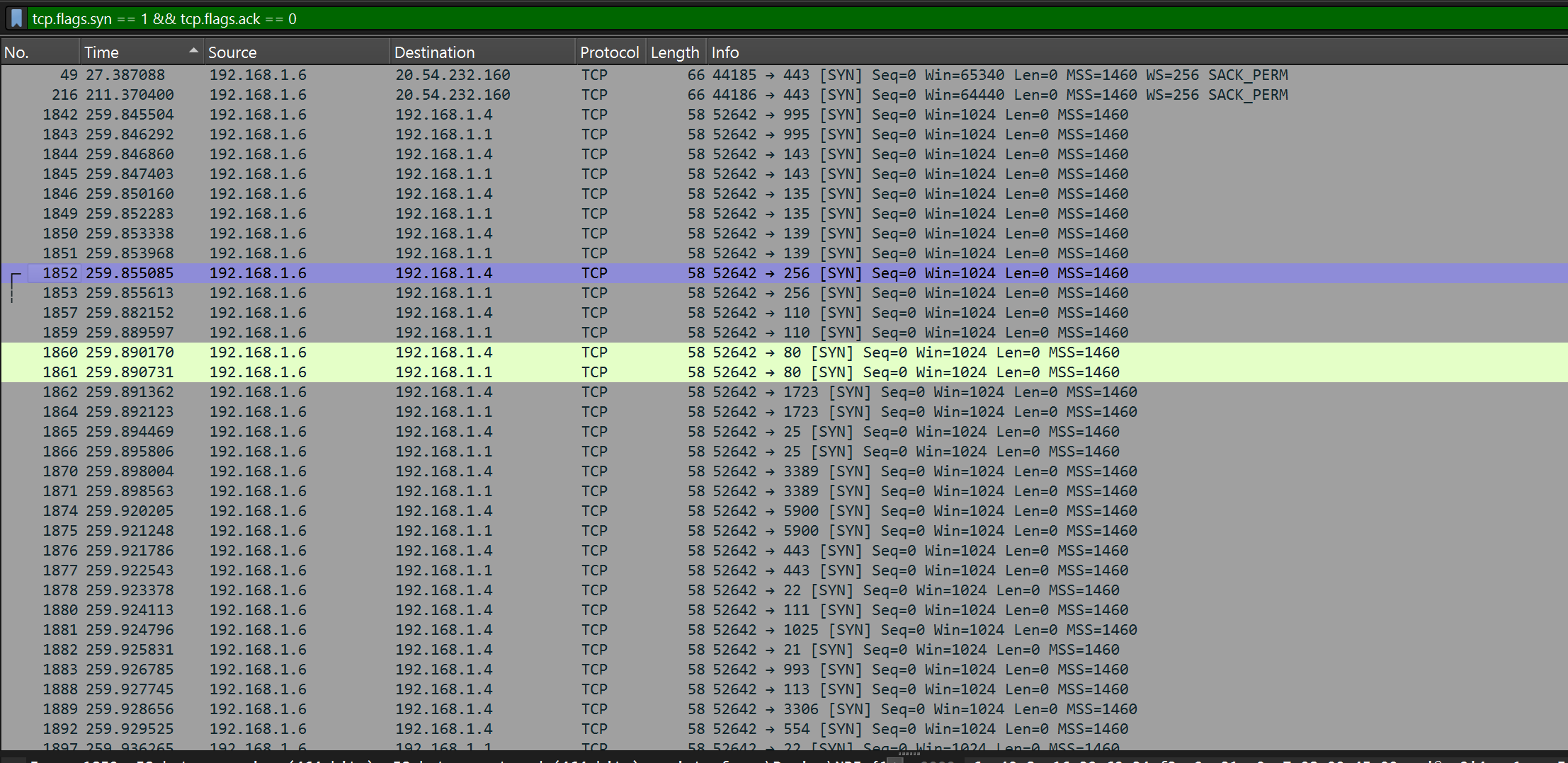
**Risk Analysis**

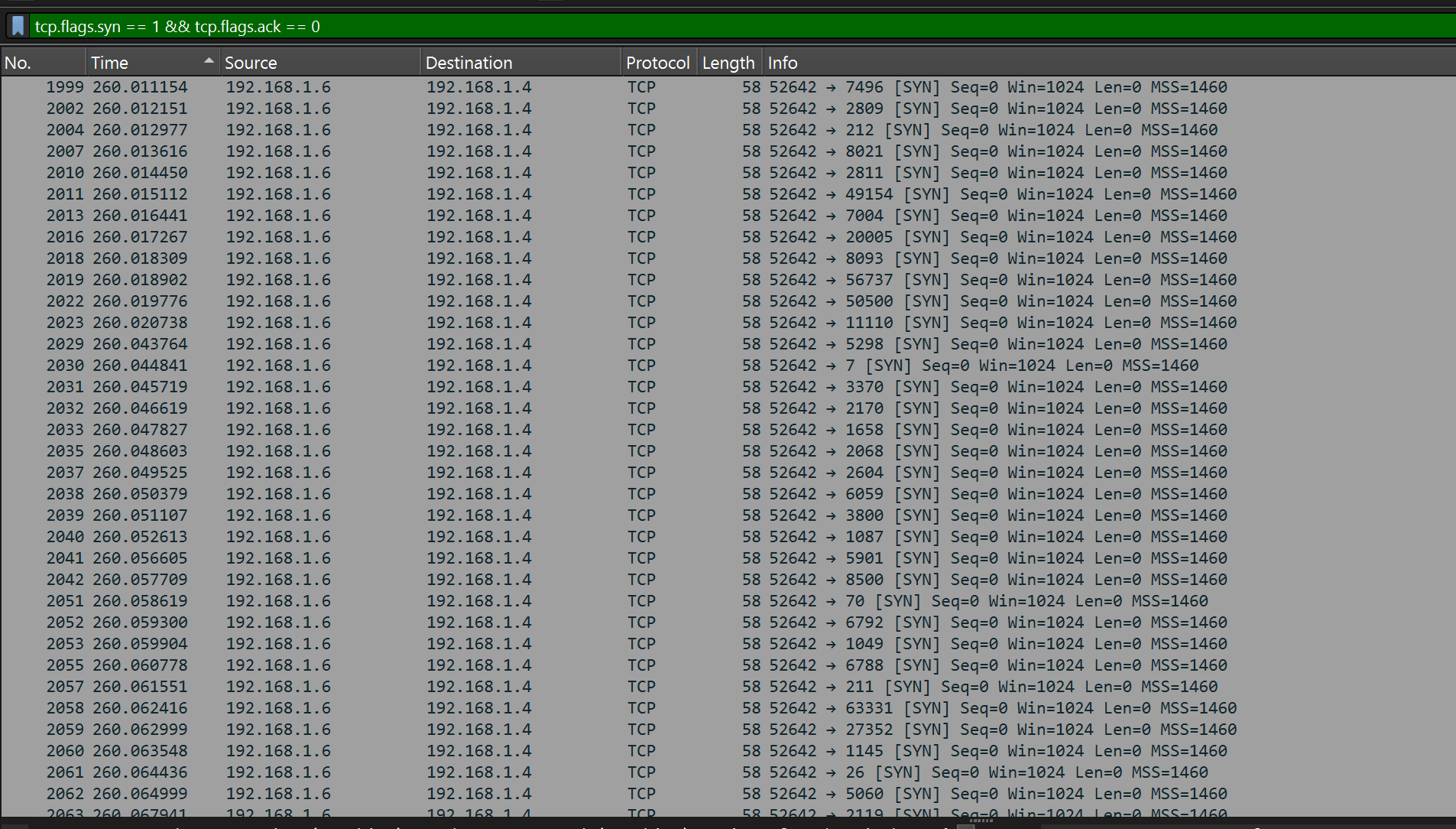
* These ports are **normal on Windows machines** but **should not be exposed to the internet**.
* SMB (445) is often targeted by malware (e.g., WannaCry).
* If file sharing isn’t needed, these can be closed or firewalled.
* **WSDAPI** is used for discovering devices like printers, but could expose metadata.

**Recommendations**

* Ensure Windows firewall is enabled and configured to allow these only on Private networks.
* Disable SMBv1 (it’s outdated and insecure).
* If this device doesn’t need to share files, disable File and Printer Sharing

Analyzing packet with wireshark with applying filter like  
tcp.flags.syn == 1 && tcp.flags.ack == 0 – it will give all the SYN scan packets





Opening one by one packet and we can get all info about the packet

