Cybersecurity Internship – Task 1 Report

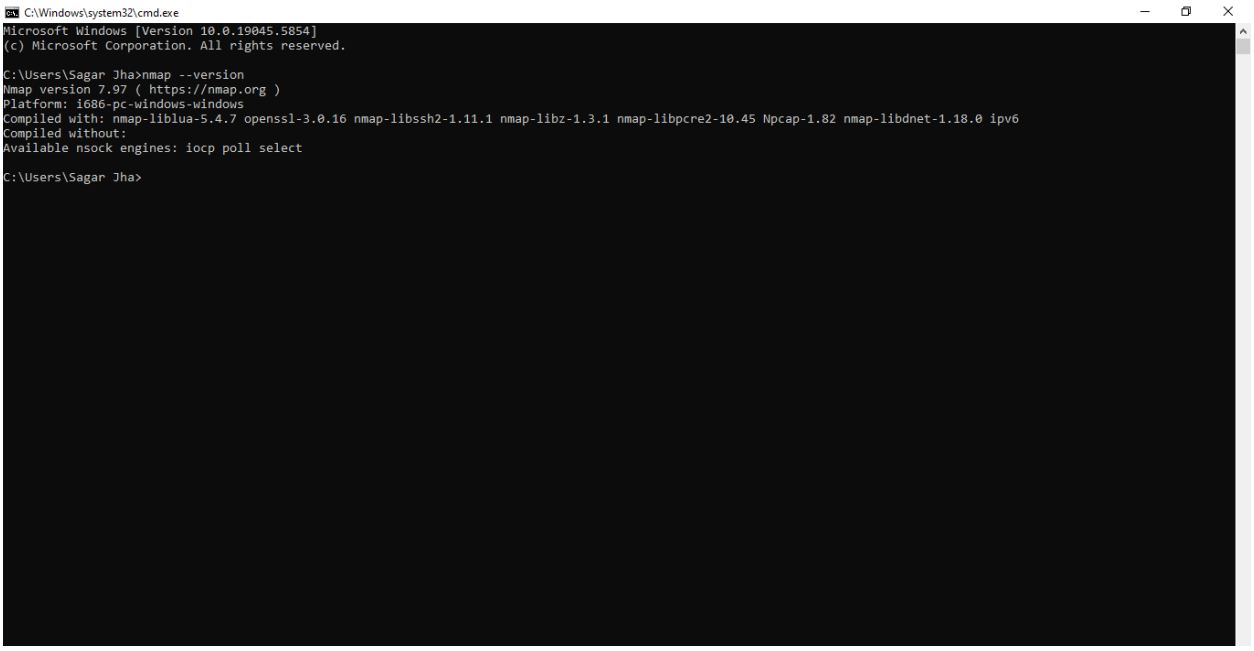
Task: Scan Your Local Network for Open Ports

🛠️ **Tools Used**

Tool	Description
Nmap	Network scanner used to discover devices and detect open ports and services.
Wireshark *(optional)*	Network protocol analyzer used to inspect and verify traffic at the packet level.
Command Prompt / Terminal	Used to run Nmap and system network commands like `ipconfig`.
Browser	For researching services and security risks associated with open ports.
Text Editor (e.g., Notepad/VSCode)	Used to save scan results, notes, and documentation.

Step 1: Install Nmap

- Download from: https://nmap.org/download.html
- Install the version for your operating system.
- Verify installation with the command: nmap --version



This Picture Shows the version of nmap.

Step 2: Find Your Local IP Range

Open Command Prompt or Terminal:

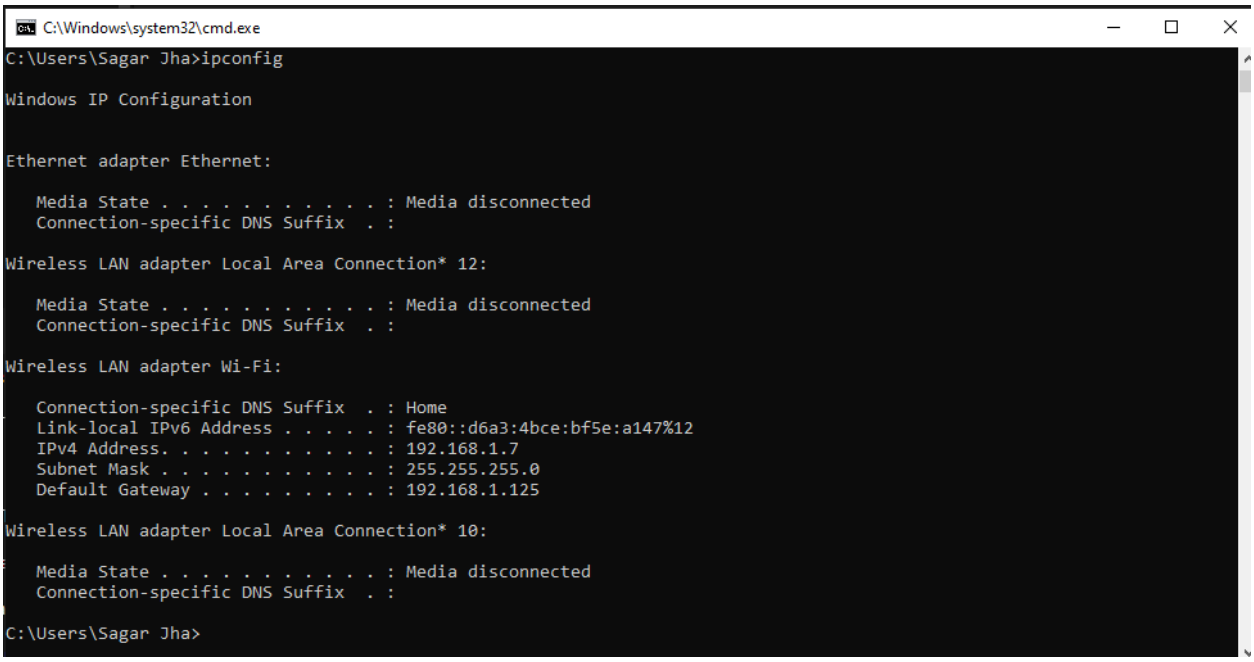
ipconfig (Windows)

ifconfig (Linux/Mac)

- Look for your IPv4 address. In my case it is:

  ```
  IPv4 Address: 192.168.1.7
  Subnet Mask: 255.255.255.0
  ```

- The IP range is usually: `192.168.1.0/24`



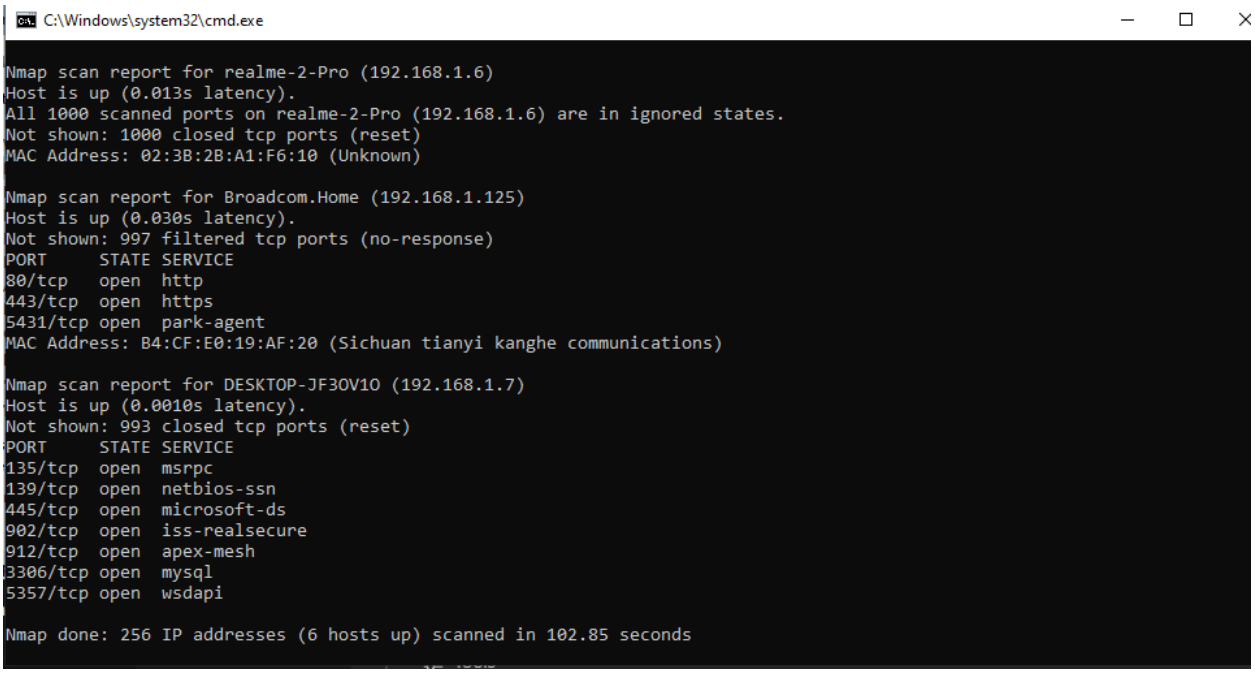
This Shows Local IP Range of my Network.

Step 3: Run Nmap TCP SYN Scan

- Run this command in your terminal:

  ```
  nmap -sS 192.168.1.0/24
  ```

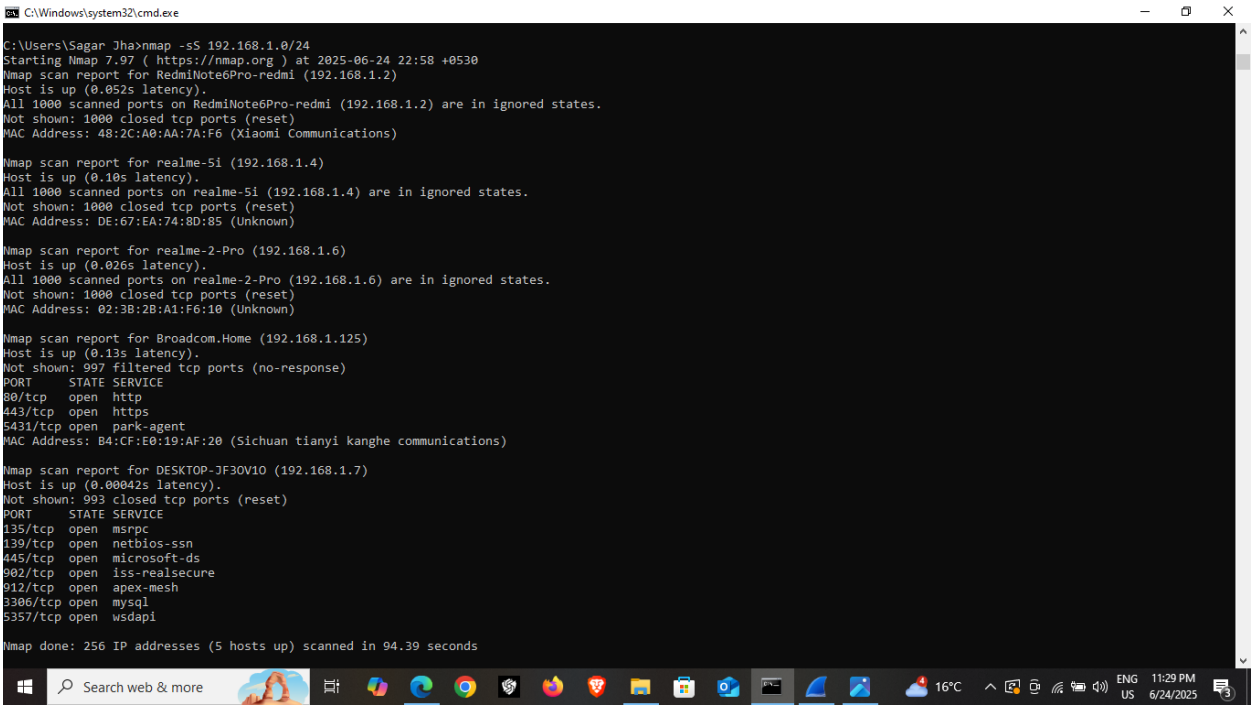
- This performs a TCP SYN scan on all devices within your subnet.
- You will see which IPs are live and what ports are open.



This Shows the TCP SYN Scan of all devices with in my network.

Step 4: Note IPs and Open Ports

Output:



This Shows the IPs and Open Ports of all the devices in the network.

Step 5: Analyze With Wireshark

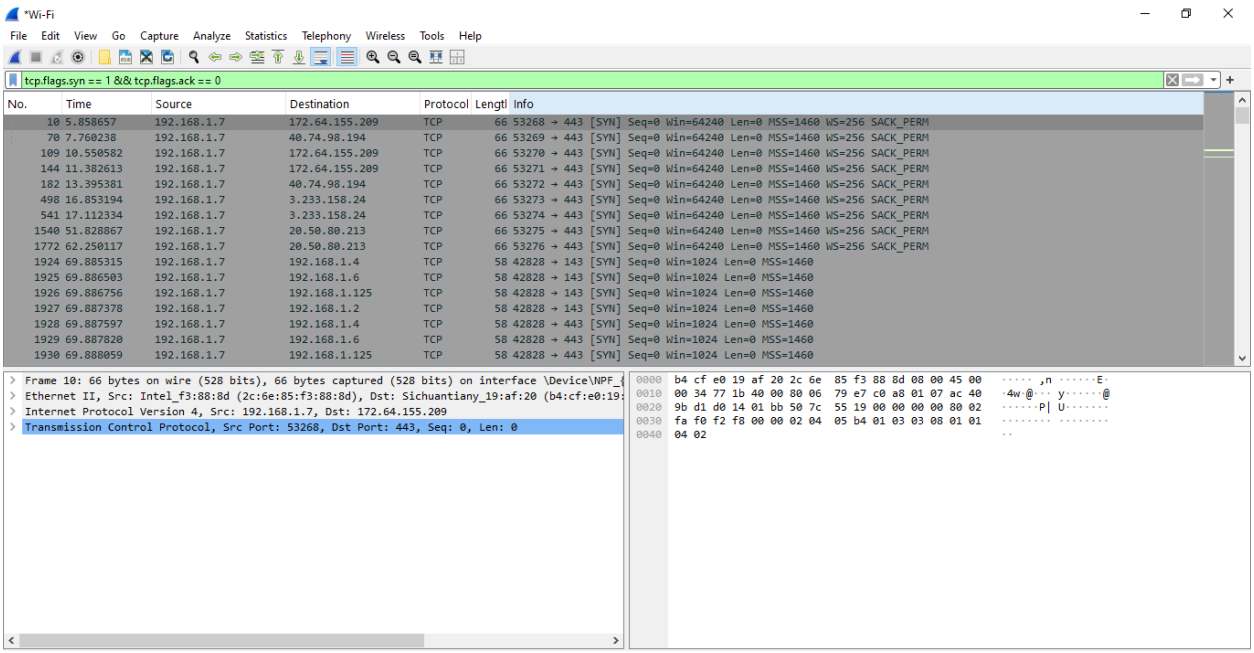
Steps:

1. Open Wireshark.
2. Select the active interface (e.g., Ethernet or Wi-Fi).
3. Start packet capture.
4. While capturing, run:

```
nmap -sS 192.168.1.0/24
```

5. Apply this filter in Wireshark:

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

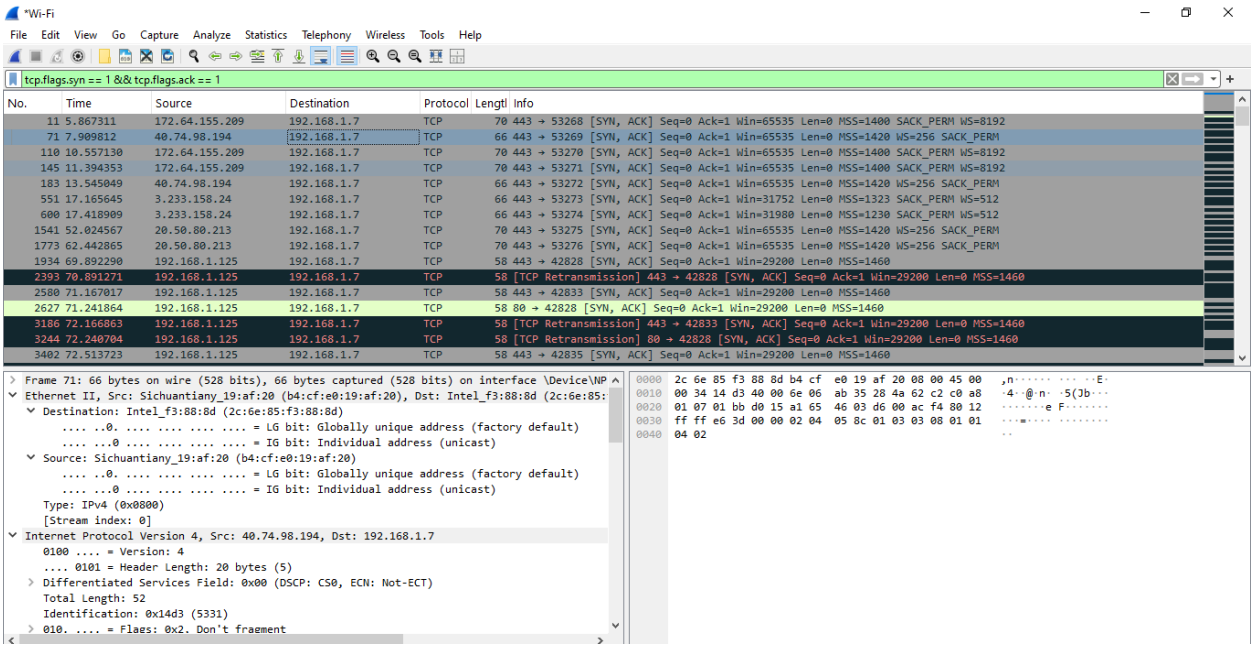


This shows only **SYN packets**, i.e., connection requests made by Nmap.

→ Shows SYN packets sent by Nmap.

6. To see SYN-ACK responses (indicating open ports), use:

`tcp.flags.syn == 1 && tcp.flags.ack == 1`



This shows full 3-way handshakes.

7. Stop capture and save file as `nmap_scan.pcapng`.

Step 6: Research Common Services

These are the ports discovered during the scan along with their typical associated services and a brief description of each:

Port	State	Service	Description
80	open	HTTP	Web traffic over unencrypted Hypertext Transfer Protocol.
443	open	HTTPS	Secure web traffic using TLS/SSL encryption.
5431	open	park-agent	Typically used by **UPnP** media servers or printer discovery agents.
			(MAC address shows device from Sichuan tianyi kanghe communications.)
135	open	MSRPC	Microsoft RPC, used for DCOM and network communication with Windows services.
139	open	NetBIOS-SSN	NetBIOS Session Service; legacy file/printer sharing on Windows networks.
445	open	Microsoft-DS	SMB (Server Message Block); used for file and printer sharing in Windows.
902	open	iss-realsecure	Associated with VMware (Remote Console); sometimes used in intrusion systems.
912	open	apex-mesh	Possibly used by APEX mesh networking or IoT device protocols.
3306	open	MySQL	Default port for MySQL database service.
5357	open	WSDAPI	Web Services for Devices API — used for device discovery in Windows.

🔍 Security Risk Highlights

- **Port 445/139/135**: Frequently targeted in Windows SMB exploits (e.g., EternalBlue).
- **Port 3306**: Must be secured with strong DB credentials and firewall rules.
- **Port 902/912**: Uncommon ports may signal proprietary or IoT services — review for exposure.
- **Port 5431**: UPnP ports can be misused to expose devices to the internet if not firewalled.

Step 7: Identify Security Risks

Port	Service	Risk	Mitigation
80	HTTP	Unencrypted traffic can be intercepted or modified (MITM attacks).	Redirect to HTTPS, use TLS certificates.
443	HTTPS	Secure by default, but misconfigured certificates or outdated SSL versions pose risks.	Use strong TLS configs and updated certificates.
5431	park-agent / UPnP	Often associated with UPnP, which can expose internal services externally without authentication.	Disable UPnP on routers/devices unless absolutely needed.
135	MSRPC	Used by Windows DCOM; commonly targeted by worms (e.g., Blaster).	Restrict to local/internal access. Patch Windows systems regularly.
139	NetBIOS-SSN	Legacy Windows file/printer sharing. Vulnerable to sniffing and NetBIOS name spoofing.	Disable NetBIOS if not required. Use SMBv3 or above.
445	Microsoft-DS (SMB)	Highly vulnerable to exploits like EternalBlue (WannaCry). Open SMB can leak data.	Block on WAN interface, use firewalls, and patch OS.
902	iss-realsecure	Linked to VMware remote services; can expose control channels to attackers if not restricted.	Limit access to trusted IPs. Disable if not using VMware services.
912	apex-mesh	Rare service; may be used by mesh or IoT devices. Unverified ports may introduce unknown vulnerabilities.	Research the device; restrict unknown ports via firewall.

3306	MySQL	If exposed to the internet, vulnerable to brute-force or SQL injection if app is insecure.	Bind MySQL to `localhost`, use strong passwords, and restrict remote access.
5357	WSDAPI	May allow device enumeration and control via HTTP; could leak system info to local attackers.	Restrict to local devices or disable Web Services for Devices (WSD) if unused.

General Security Practices

- Close all unnecessary ports and disable unused services.
- Apply the principle of least privilege — only allow access where needed.
- Use network segmentation and internal firewalls.
- Monitor unusual traffic from open or high-numbered ports.

Step 8: Save Scan Results

nmap -sS 192.168.1.0/24 -oN scan_results.txt