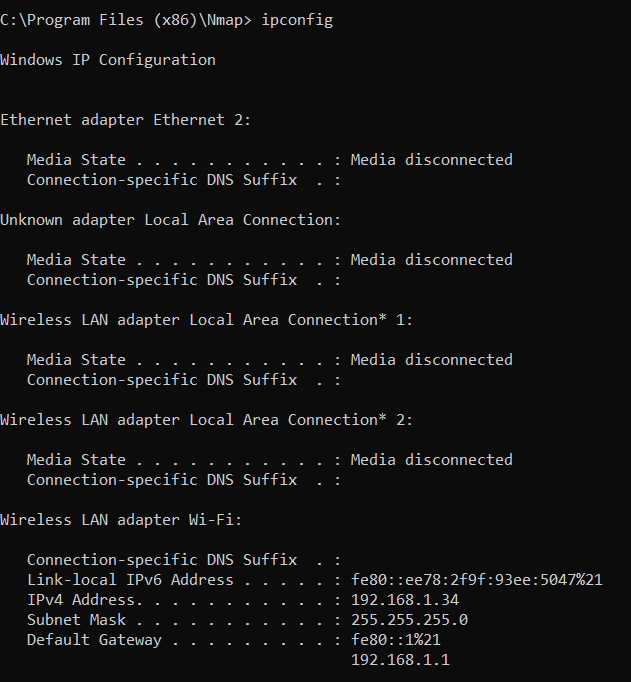
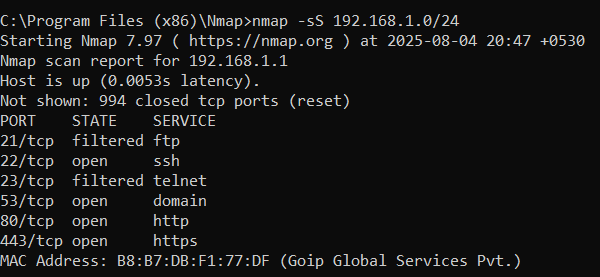
**TASK 1**

**Local IP range :**

****

**TCP SYN Scan , IP addresses and Open ports:**

****

**For Analyze packet capture I attached a video in git repo:**

**----------------------------------------------------------------------**

**Common Services Running and security risks from these open ports 22,53,80,443:**

**Port 22 – SSH (Secure Shell)**

* **Protocol:** TCP
* **Service:** SSH (Secure Shell)
* **Purpose:** Secure remote login and command execution on servers.
* **Common Use Cases:**
  + System administration
  + Secure file transfer using SCP or SFTP
* **Security Notes:**
  + Use strong passwords or SSH key-based authentication
  + Disable root login directly
  + Use non-default ports or fail2ban to prevent brute force attacks

**Port 53 – DNS (Domain Name System)**

* **Protocol:** TCP and UDP
* **Service:** DNS
* **Purpose:** Resolves domain names (e.g., google.com) into IP addresses
* **Common Use Cases:**
  + Every web or email request starts with a DNS query
  + UDP is used for queries, TCP is used for zone transfers or large responses
* **Security Notes:**
  + Susceptible to DNS amplification and spoofing attacks
  + Use DNSSEC for validation and integrity
  + Restrict zone transfers to authorized IPs only

**Port 80 – HTTP (Hypertext Transfer Protocol)**

* **Protocol:** TCP
* **Service:** HTTP
* **Purpose:** Unencrypted web traffic
* **Common Use Cases:**
  + Hosting websites without SSL/TLS (insecure)
  + Redirects to HTTPS sites
* **Security Notes:**
  + Vulnerable to MITM (man-in-the-middle) attacks
  + Use only for redirection to HTTPS or local/dev environments
  + Don't transmit sensitive data over HTTP

**Port 443 – HTTPS (HTTP Secure)**

* **Protocol:** TCP
* **Service:** HTTPS
* **Purpose:** Encrypted web traffic using SSL/TLS
* **Common Use Cases:**
  + Secure websites (e.g., online banking, e-commerce)
  + APIs requiring encrypted communication
* **Security Notes:**
  + Uses SSL/TLS for encryption and certificate-based identity
  + Ensure valid, up-to-date SSL certificates (e.g., via Let's Encrypt)
  + Use strong cipher suites and disable deprecated protocols (like SSLv3, TLS 1.0)