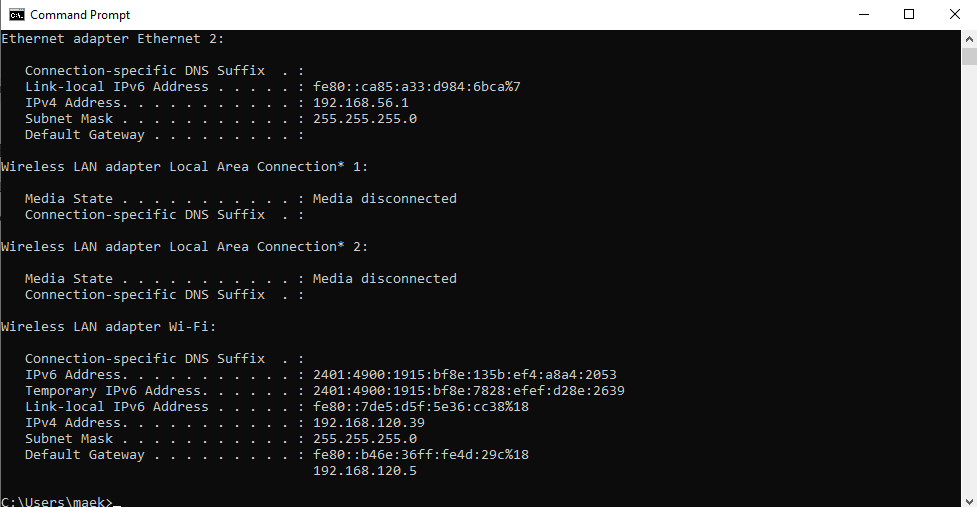
**CYBER SECURITY INTERNSHIP**

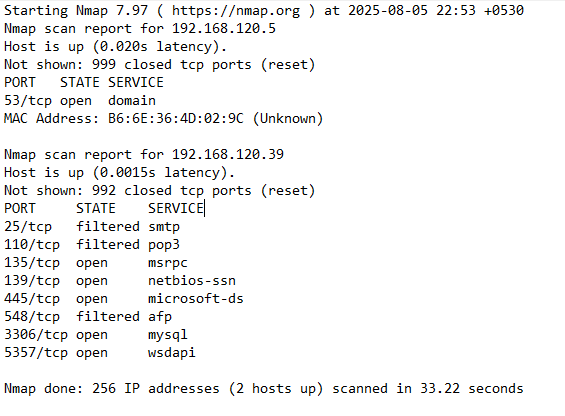
**Task 1: Scan Your Local Network for Open Ports:**

1. Find your local IP range:
   * Win + R -> cmd
   * Cmd -> ipconfig



Here my local Ip range is : 192.168.120.0/24

1. Run: nmap -sS 192.168.120.0/24 to perform TCP SYN scan.
2. Note down IP addresses and open ports found.



1. Research common services running on those ports:

|  |  |  |
| --- | --- | --- |
| **Port** | **Service** | **Description** |
| 22 | SSH | Secure remote login (can be abused for brute-force) |
| 80 | HTTP | Web server, often target for attacks |
| 443 | HTTPS | Secure web, usually okay |
| 21 | FTP | File transfer, vulnerable if misconfigured |
| 23 | Telnet | Obsolete, insecure |
| 3389 | RDP | Remote desktop, can be risky |

5. Identify Potential Security Risks:

- Devices with port 22 open are vulnerable to SSH brute-force if passwords are weak.

- Port 80 (HTTP) transmits data in plain text — vulnerable to sniffing and MITM.

- If any unusual or unknown ports are open, they could expose vulnerable services