**Documentation Day - 1**

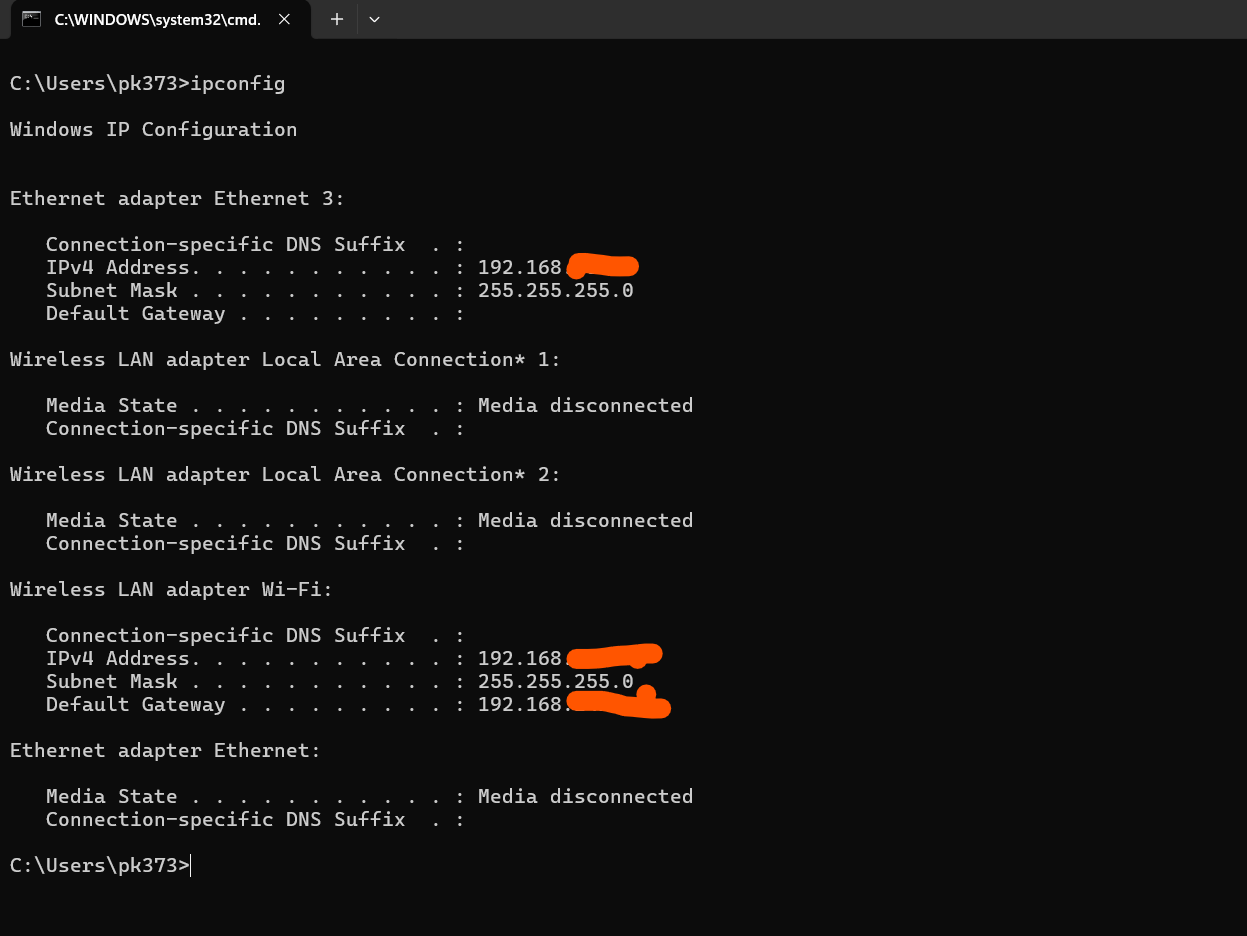
**Task 1: Scan Your Local Network for Open Ports**

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

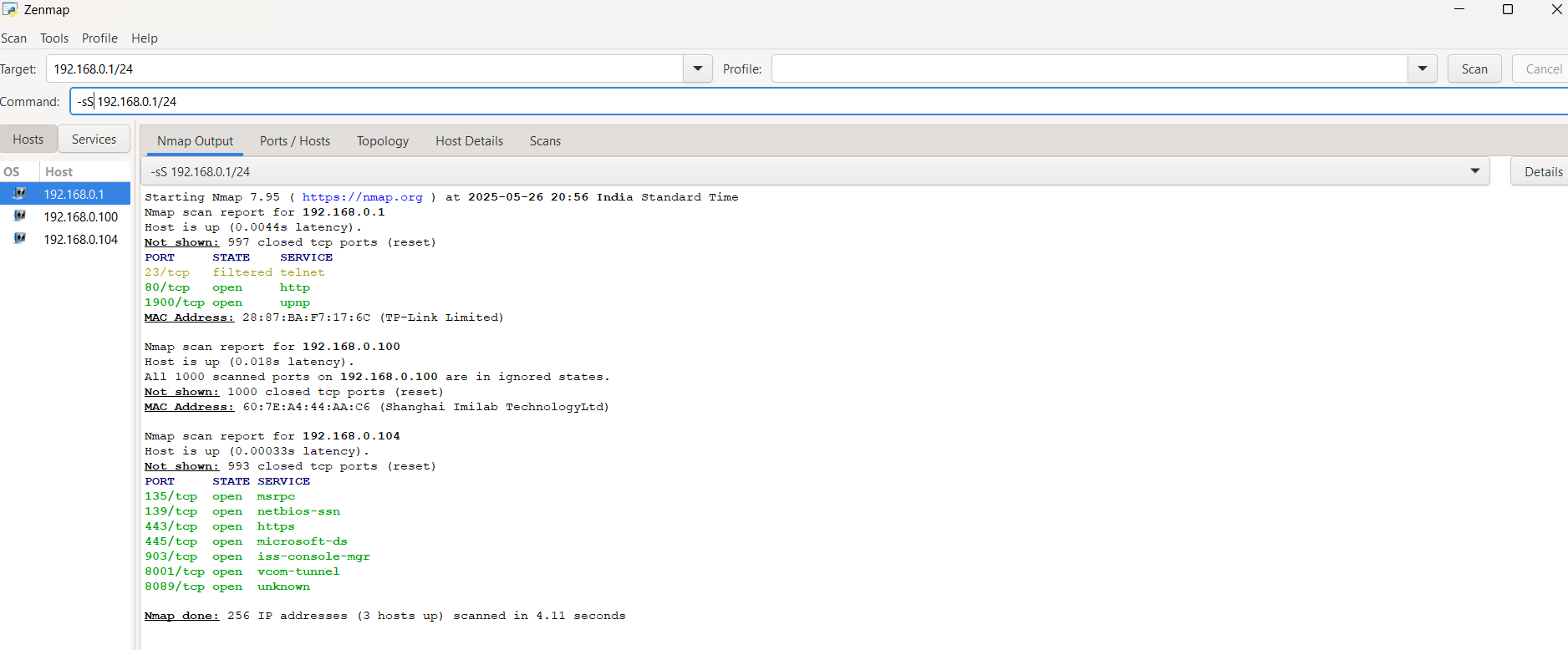
**Procedure:**

First, install Nmap and Wireshark from their official websites.

To know our IP address, type the command prompt and type **ipconfig.** It displays all current TCP/IP network configurations and refreshes DHCP and DNS settings for all adapters on your computer. There you can find your **private IP address** of your computer.



Now, to find the open ports on my mission, I need to use the Nmap tool to perform a TCP SYN scan. Go to the application, note down the desired IP address from the command prompt, and type a command: -sS 192.168.00.00



Here I got 7 open ports. Of those, 3 are risky, 3 are medium, and 1 is safe. They are:

Risky

Port 135/tcp (msrpc) abused for lateral movement.

Port 139/tcp (netbios-ssn) Legacy service, vulnerable to exploitation.

Port 445/tcp (microsoft-ds) Common ransomware entry point.

Modrate

port 903/tcp (iss-console-mgr) Admin interface, should be restricted and secured.

Port 8001/tcp (vcom-tunnel) Application-specific, needs access control.

Port 8089/tcp (unknown) Need to identify; unknown ports should be reviewed.

Safe

Port 443/tcp (HTTPS) Secure web traffic, SSL/TLS.