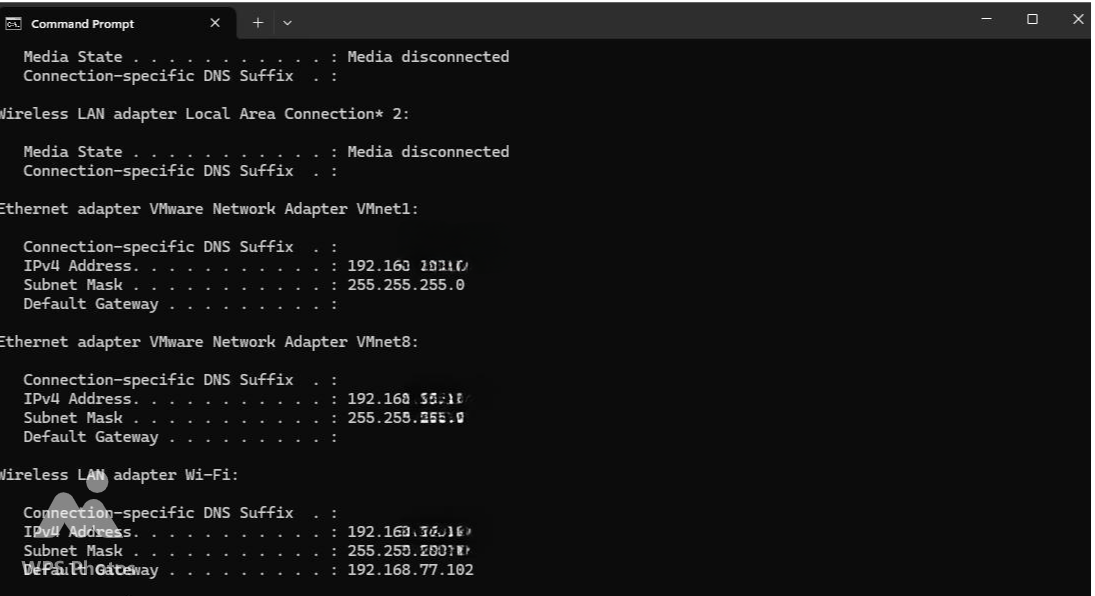
**DOCUMENT**

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

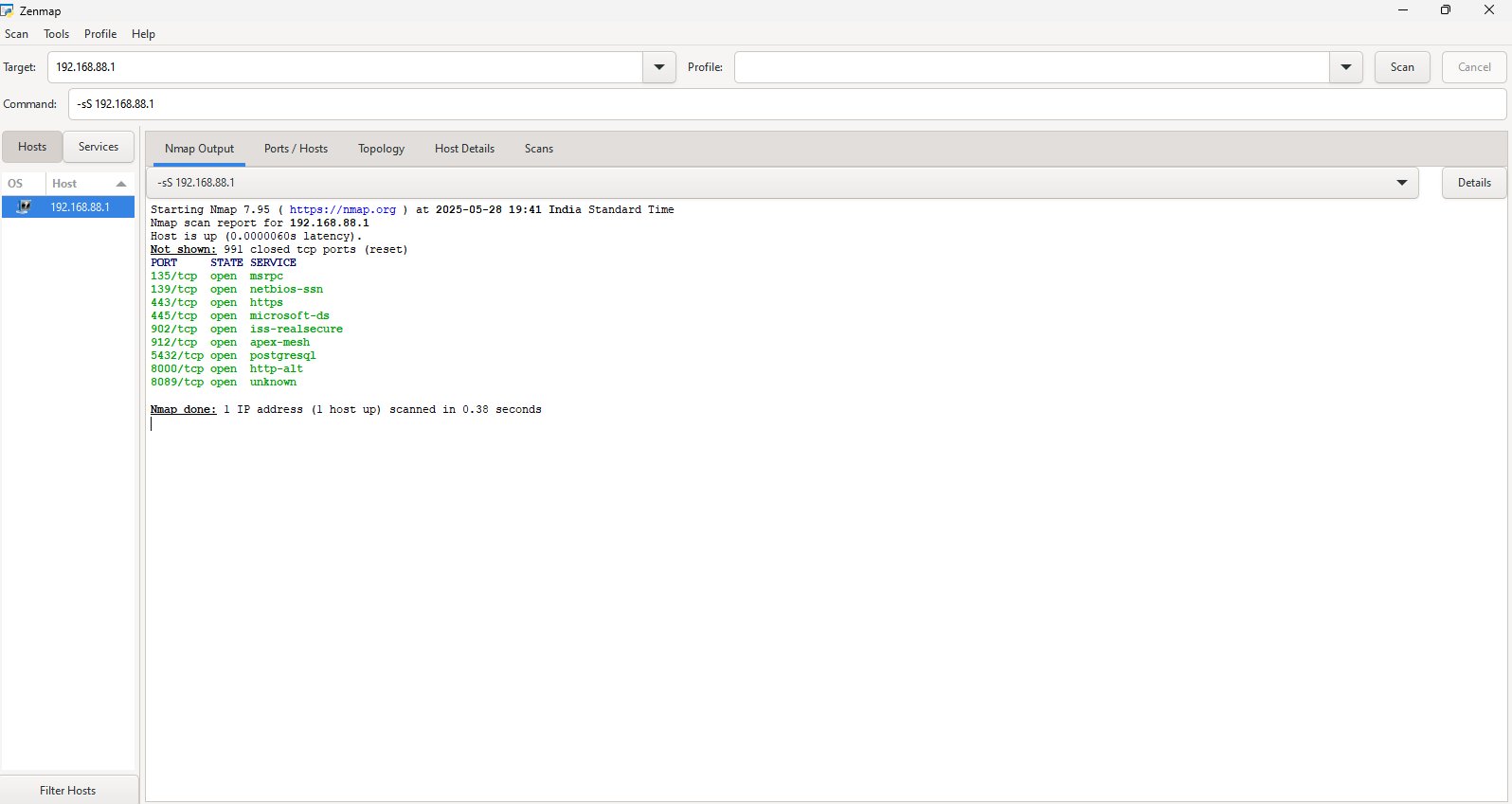
* **Objective:** Learn to discover open ports on devices in your local network to understand network exposure.
* **Tools:** Nmap, Wireshark

**Process :**

* First install Nmap and wireshark form official websites.
* Find our ip address using commant Prompt, Go to the command prompt and type **ipconfig**
* Displays the your **Private ip address** of your computer.



* The second step is find the open port on our device using **Nmap** tool to perform TCP SYN scan.
* Open the Nmap, mention our ip addess in Target .
* ip address form the command prompt and type a command :-sS 192.168.\*\*.\*\*



Here I got 9 open ports

Risky level

port 445/tcp (microsoft-ds) Commonly exploited

port 139/tcp (netbios-ssn) File sharing, risky

port 135/tcp (msrpc) Remote control risk

Modrate

port 902/tcp (iss-realsecure) VMware-related

Port 5432/tcp (postgresql) Database brute-force risk

Port 8089/tcp (unkonwn) Often Splunk/logging

Low Risk

912/tcp(apex-mesh) Uncommon, unknown use

8000/tcp(http-alt) Dev server?

Safe

Port 443/tcp (HTTPS) Okay if secured