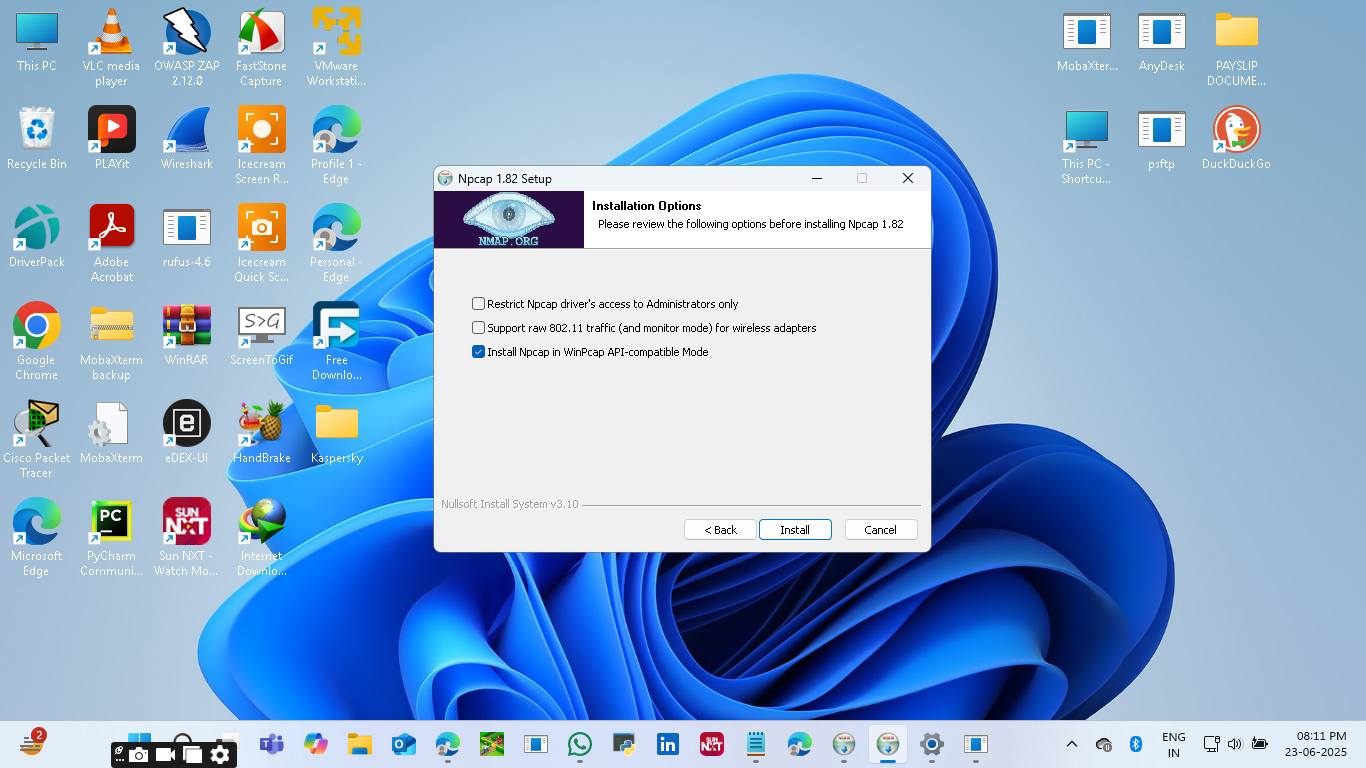
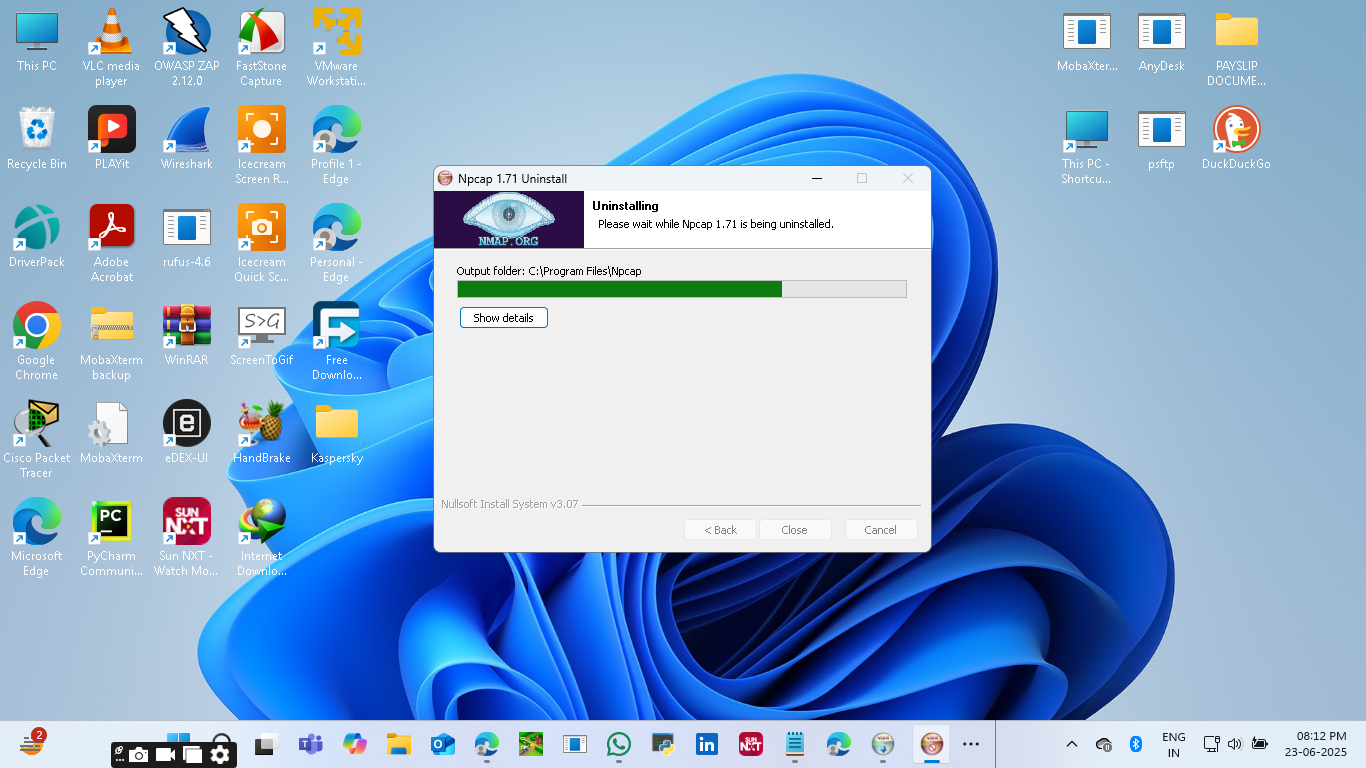
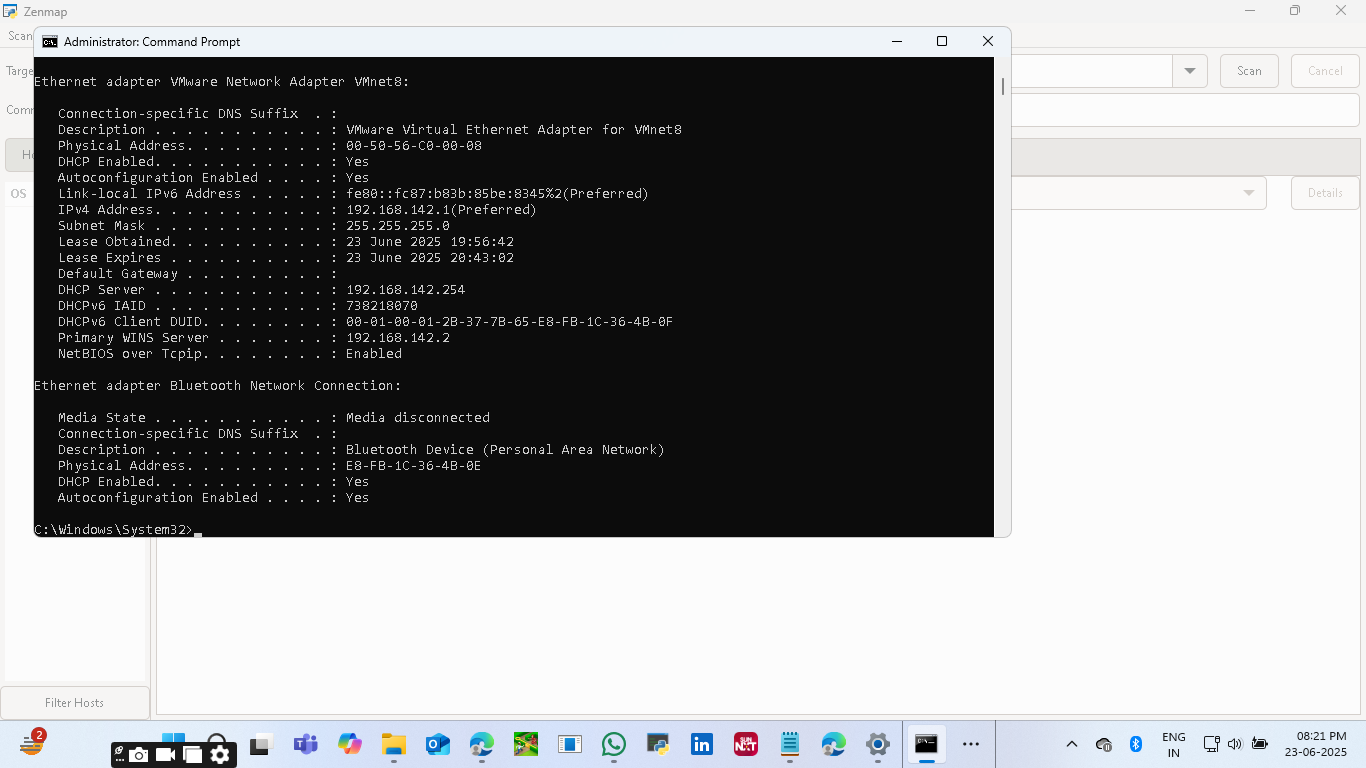
**Install - Nmap**



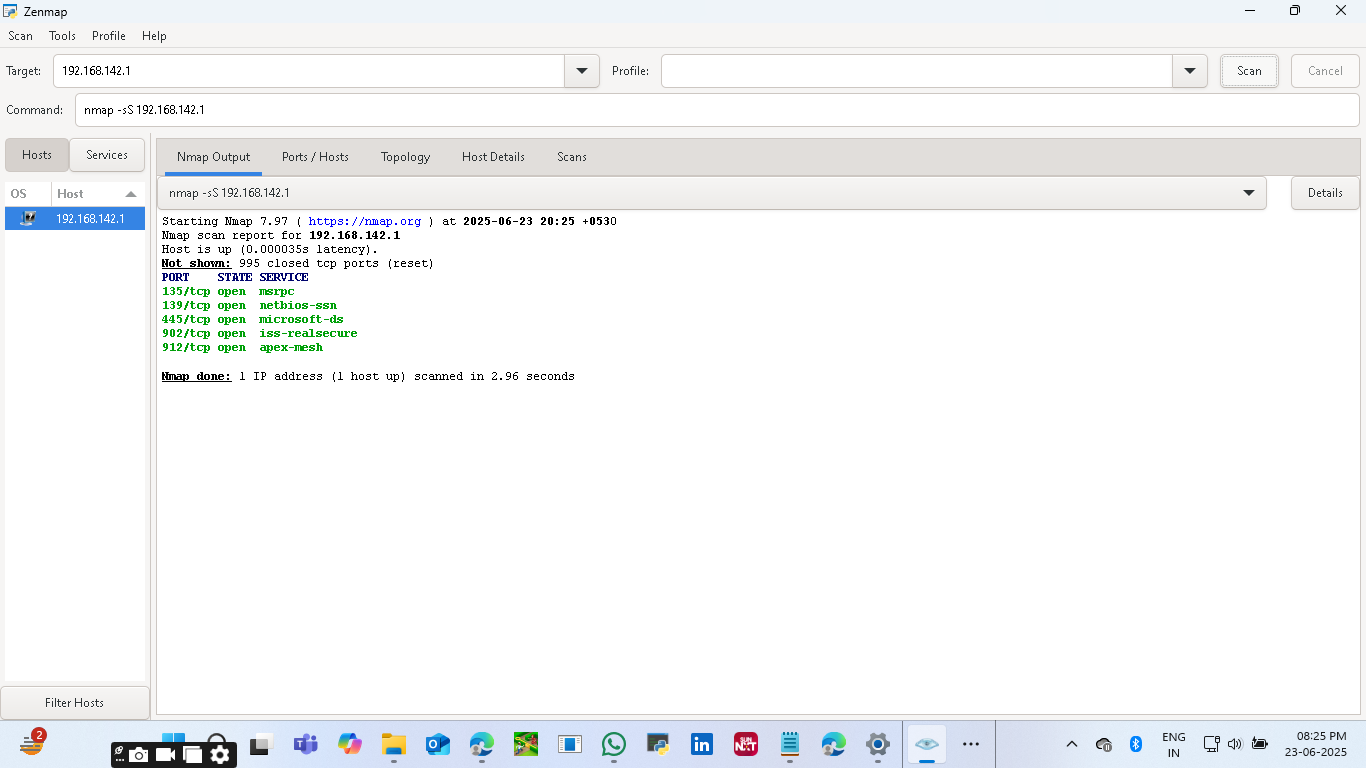


**Run CMD as Admin:**

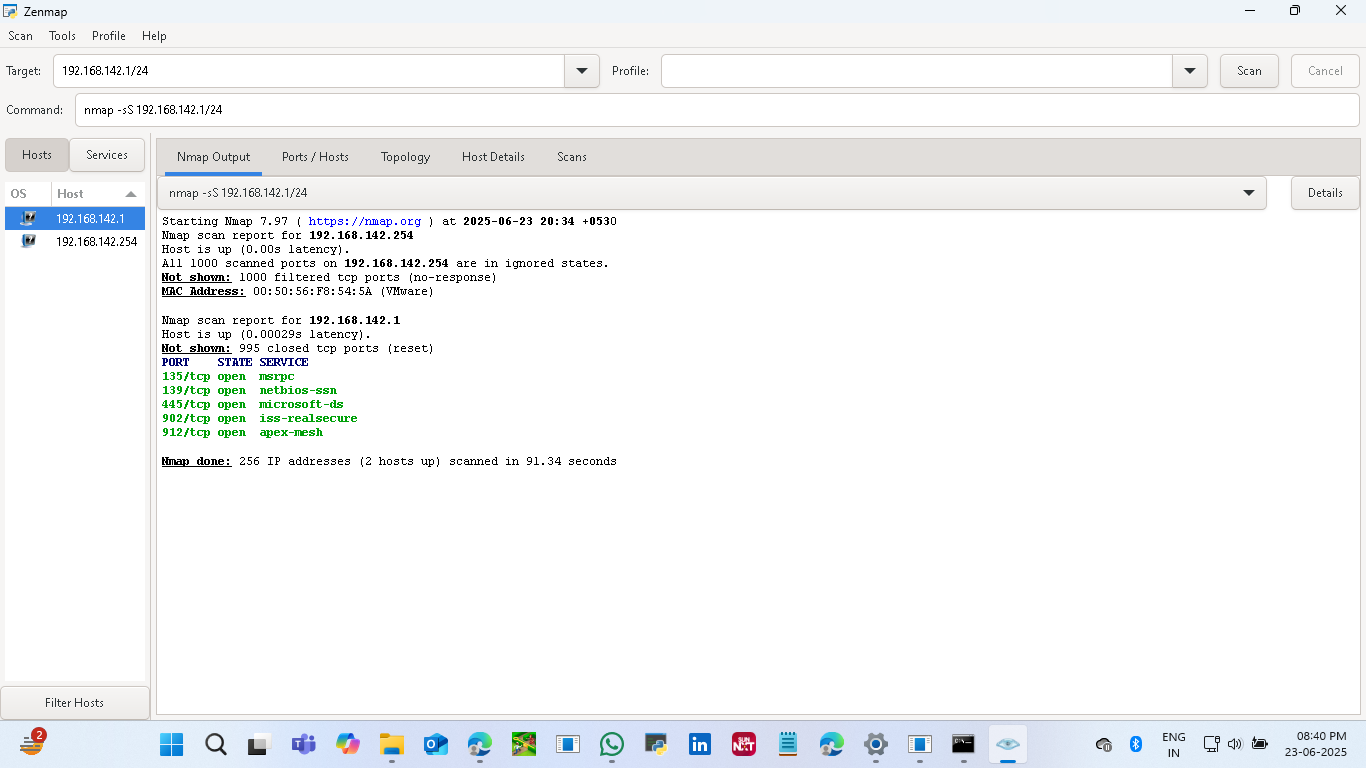
Gathering and IP information founded ,

****

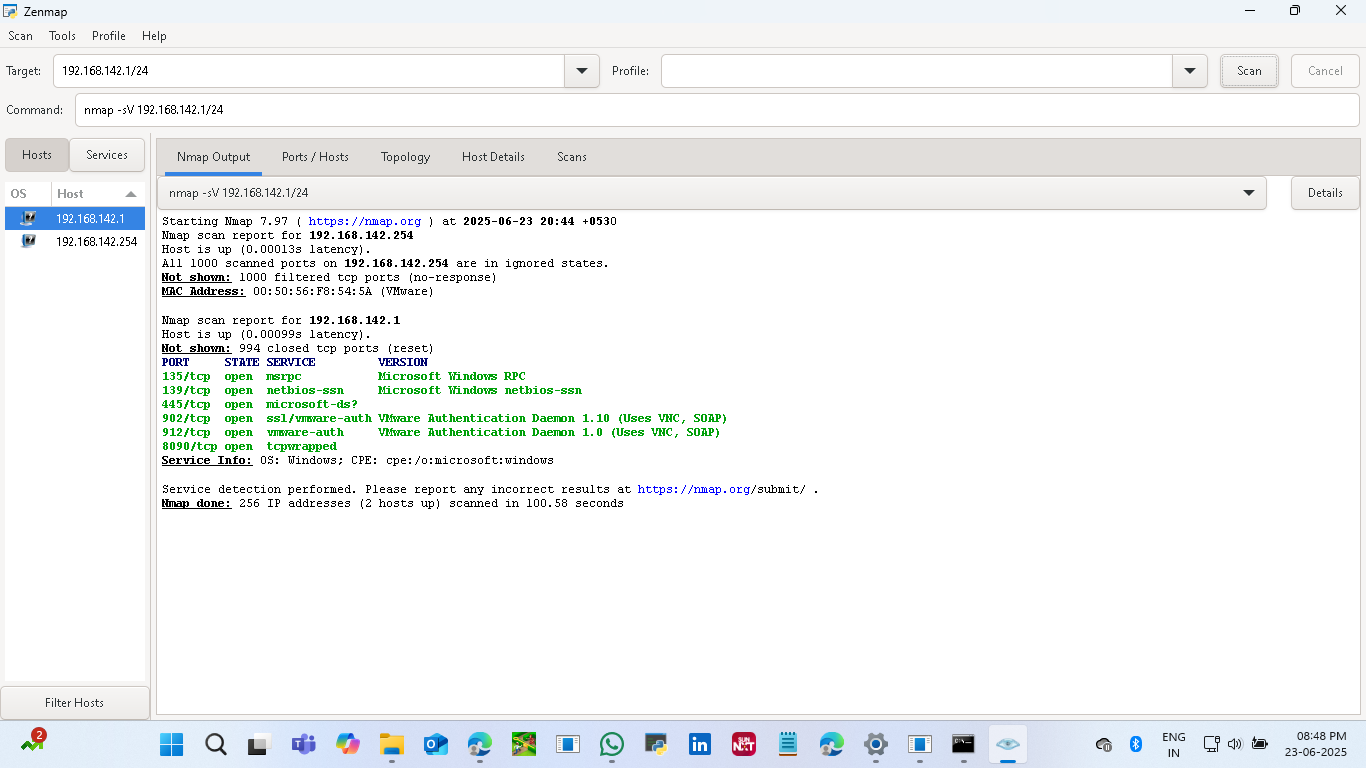
**Run CMD on Nmap-“Nmap –sS 192.168.142.1/24”**

****

**Noted Open Ports and IP Addresses:**

****

**Service Detection Performed:**

****

**Identified Potential Risks From the Open Ports:**

 **Port 135 (MSRPC)**: Often targeted due to its use in DCOM and RPC services. Vulnerabilities like **CVE-2020-7589** allow unauthenticated attackers to read/modify configurations remotely.

 **Port 139 (NetBIOS-SSN)** and **Port 445 (Microsoft-DS)**: These are commonly exploited in attacks like WannaCry and NotPetya. Port 445, in particular, is notorious for **SMB vulnerabilities** such as EternalBlue (CVE-2017-0144). These ports should never be exposed to the internet3.

 **Ports 902 & 912 (VMware Authentication Daemon)**: These are used for remote management of VMware products. If not properly secured, they can be exploited for unauthorized access or remote code execution. Always ensure VMware is updated and access is restricted.

 **Port 8090 (tcpwrapped)**: This is a generic wrapper and could be hiding any service. It’s often used by web applications or proxies. Vulnerabilities depend on the actual service running behind it, so further inspection is needed.