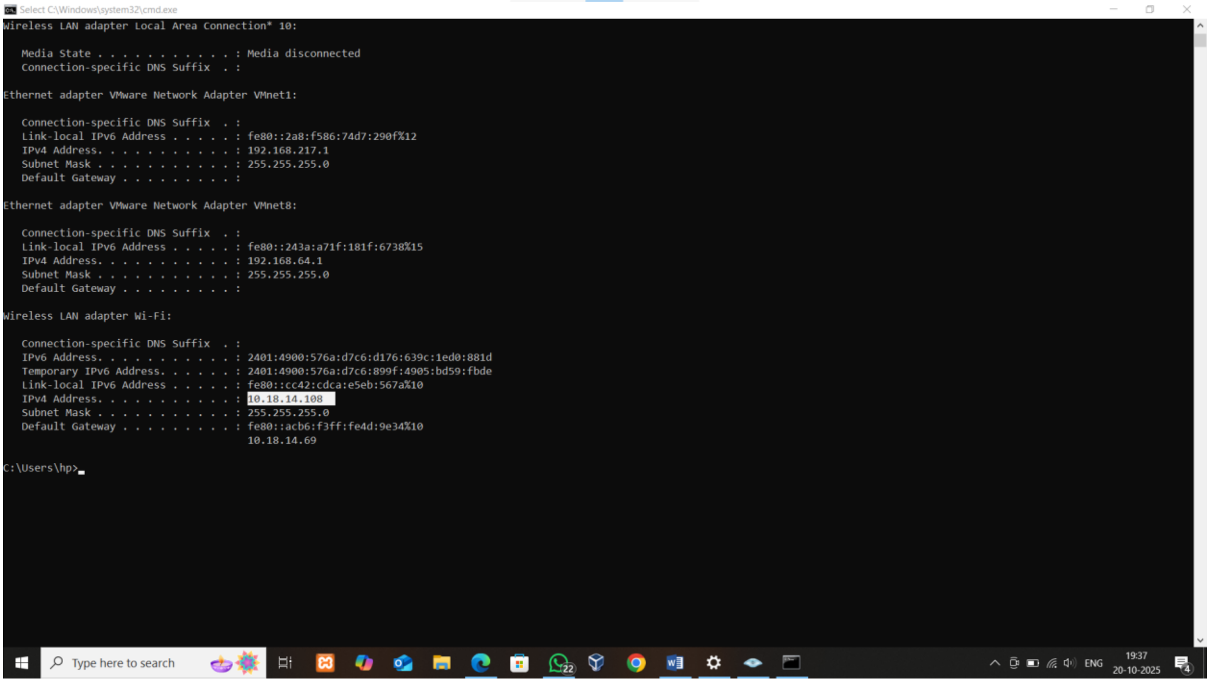
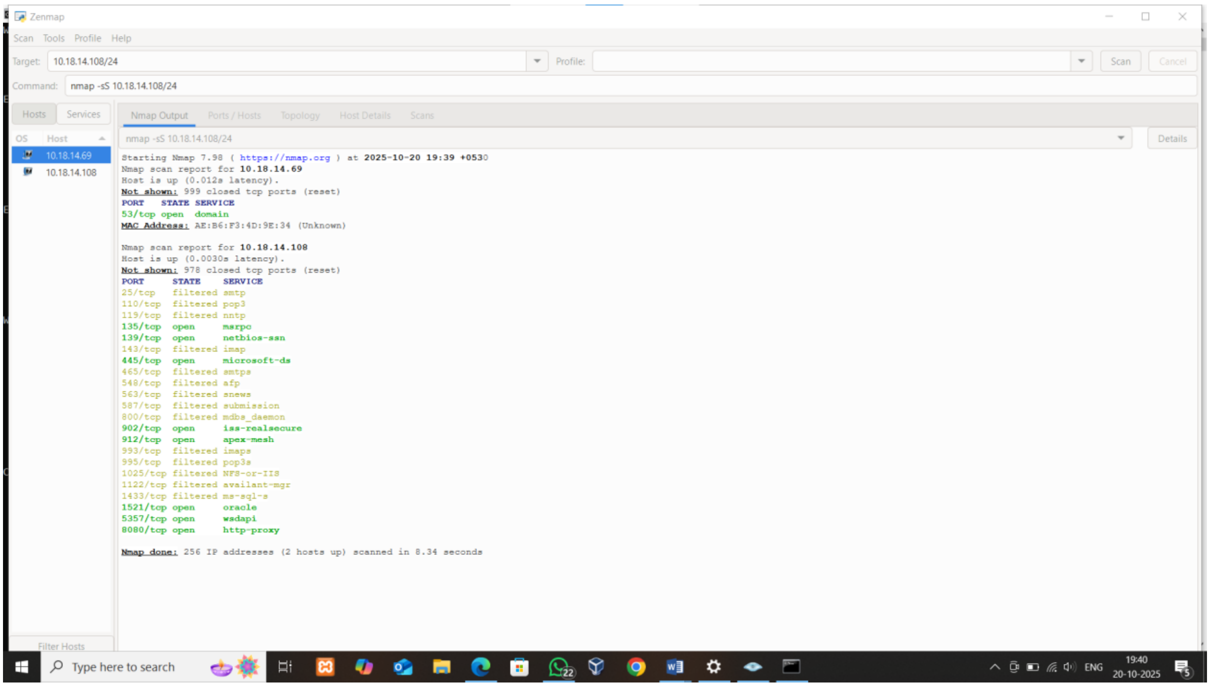
- **Ip address of our system that we are using right now:**



```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2a8:f586:74d7:290f%12
   IPv4 Address. . . . . . . . . . . : 192.168.217.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::243a:a71f:181f:6738%15
   IPv4 Address. . . . . . . . . . . : 192.168.64.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:576a:d7c6:d176:639c:1ed0:881d
   Temporary IPv6 Address. . . . . . : 2401:4900:576a:d7c6:899f:4905:bd59:fbde
   Link-local IPv6 Address . . . . . : fe80::cc42:cdca:e5eb:567a%10
   IPv4 Address. . . . . . . . . . . : 10.18.14.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::acb6:f3ff:fe4d:9e34%10
                                       10.18.14.69

C:\Users\hp>
```

- **Nmap results:**



Target: 10.18.14.108/24

Command: nmap -sS 10.18.14.108/24

```
nmap -sS 10.18.14.108/24

Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 19:39 +0530
Nmap scan report for 10.18.14.69
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: AE:B6:F3:4D:9E:34 (Unknown)

Nmap scan report for 10.18.14.108
Host is up (0.0030s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
119/tcp  filtered nntp
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds
465/tcp  filtered smtps
548/tcp  filtered afp
563/tcp  filtered snews
587/tcp  filtered submission
800/tcp  filtered mdbs_daemon
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
993/tcp  filtered imaps
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s
1521/tcp open     oracle
5357/tcp open     wsdapi
8080/tcp open     http-proxy

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.34 seconds
```

- **common services running on those ports. Identify potential security risks from open ports.**

  - **53 - domain name system server**
  - **135 - Microsoft remote procedure call endpoint mapper**
  - **139 - NetBIOS session service**
  - **445 - Microsoft directory services**
  - **902 - VMware authentication daemon (vmware-authd)**
  - **912 - Vmware authentication daemon (vmware-authd)**
  - **1521 - Oracle Database Listener**
  - **5357 - Web Services for Devices (WSDAPI)**
  - **8080 - HTTP Alternate (Web Servers, Proxies, Applications)**

- **Potential security risks: -**

  - **53 -** TCP port 53 is typically used for DNS Zone Transfers. If the server is misconfigured to allow zone transfers to any client, an attacker can map the entire internal network structure (hostnames, IP addresses) in seconds for reconnaissance.

  - **135 -** Microsoft Remote Procedure Call (RPC) Endpoint Mapper. The RPC service has been exploited by worms like Blaster to launch Denial-of-Service (DoS) attacks or achieve RCE. It acts as a gateway for other Windows services, and an attack here can affect many core system functions.

  - **139 -** Used for older NetBIOS-based file sharing. It's often associated with null sessions and enumeration attacks that allow an attacker to gather sensitive system and user information before attempting a full compromise.

  - **445 -** High-profile ransomware and worms like WannaCry, NotPetya, and Conficker have historically exploited vulnerabilities in the SMB protocol (particularly older SMBv1) running on this port. An attacker can gain remote code execution (RCE) or use it for lateral movement (spreading throughout the network) and credential theft.

  - **902/912 -** Exposing the VMware Authentication Daemon to an untrusted network is a major security risk. Vulnerabilities in this service (historically present in older versions) can be exploited to gain full control over the ESXi host and, consequently, all the virtual machines running on it. Attackers can use brute-force attacks against the authentication daemon to gain login credentials.

- **1521 -** Oracle Database Listener If not secured, attackers can attempt to connect directly to the Oracle database listener. Older Oracle listeners may reveal version info or configuration data. Misconfigured or unpatched Oracle services have had known RCE vulnerabilities. Weak or default credentials can be exploited.

- **5357 -** Web Services for Devices (WSDAPI) may leak network device details to unauthenticated users. Attackers inside the network can use WSDAPI to discover devices for further attacks. Can be exploited in reflection/amplification attacks if exposed to the internet.

- **8080 -** HTTP Alternate (Web Servers, Proxies, Applications) Exposed admin panels like, Web consoles often run on 8080 (e.g., Tomcat Manager). Cross-site scripting (XSS), SQL injection, RCE are Common web app vulnerabilities. HTTP (not HTTPS) can expose sensitive data. Default or weak credentials often left unchanged.