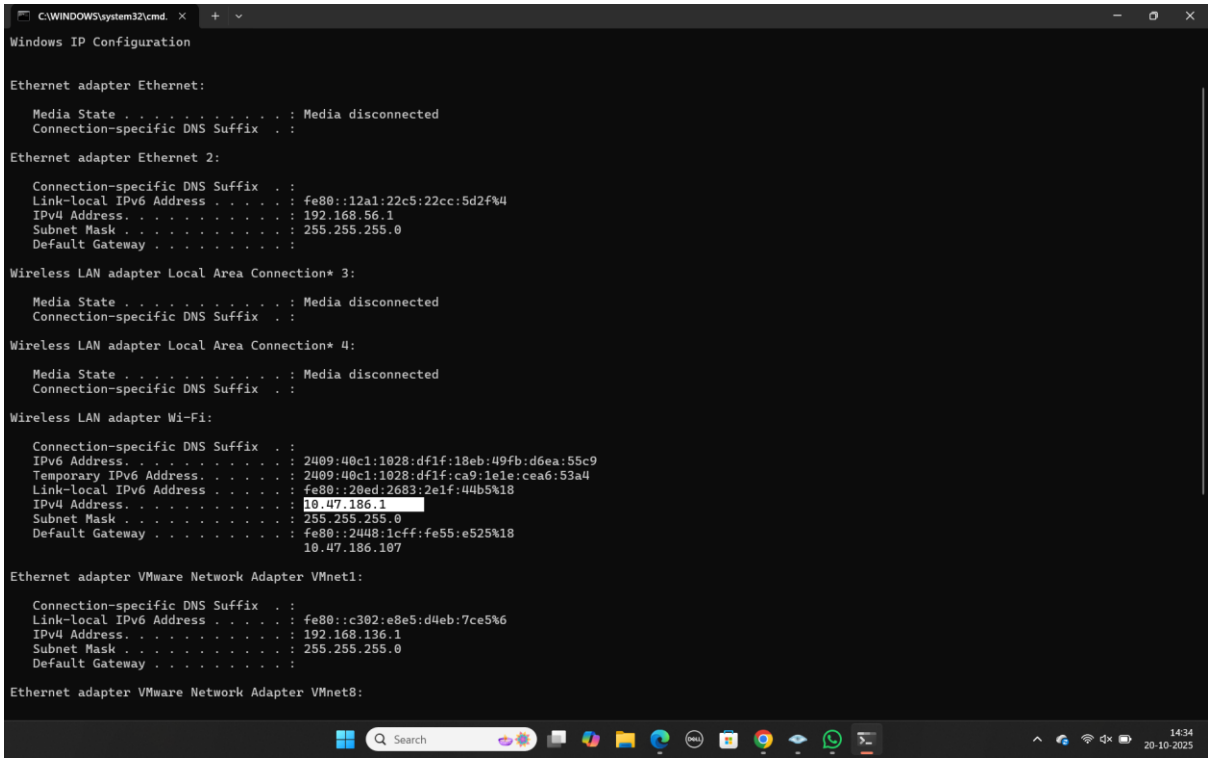
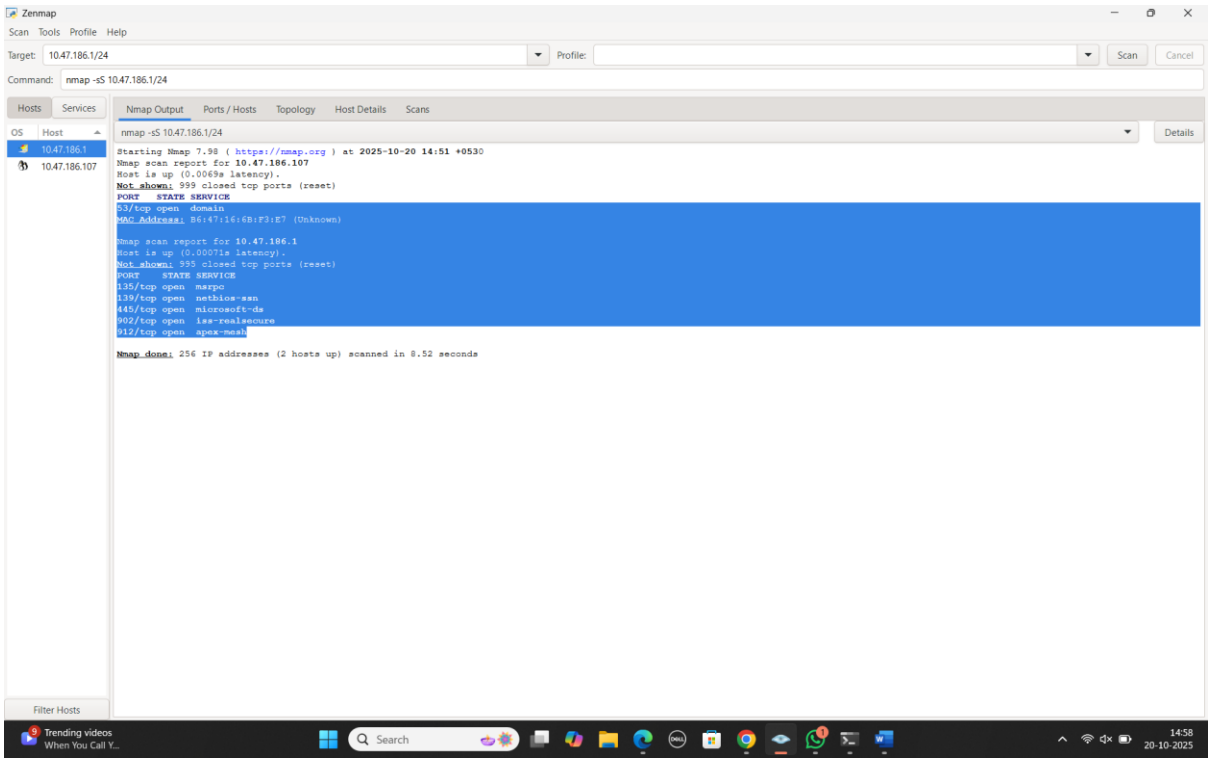
- IP address of system we are using.





- open ports.

- 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)

- 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.