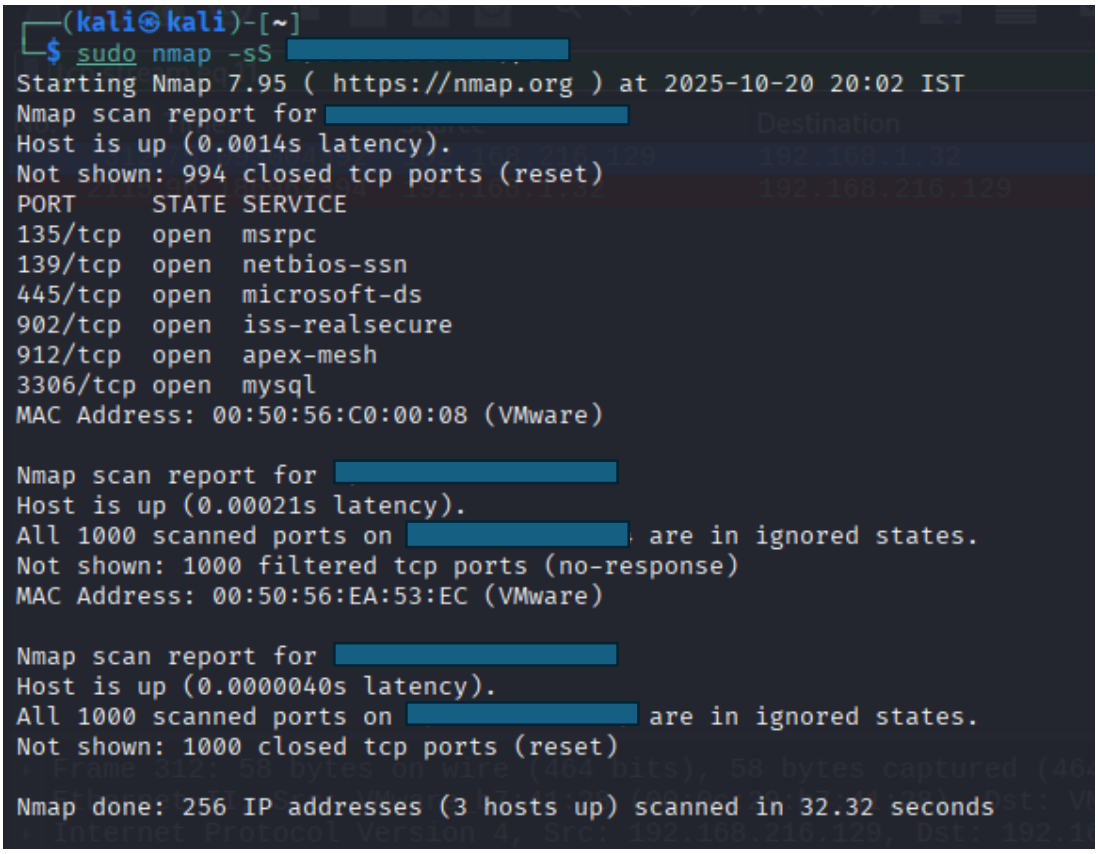
Task 1:

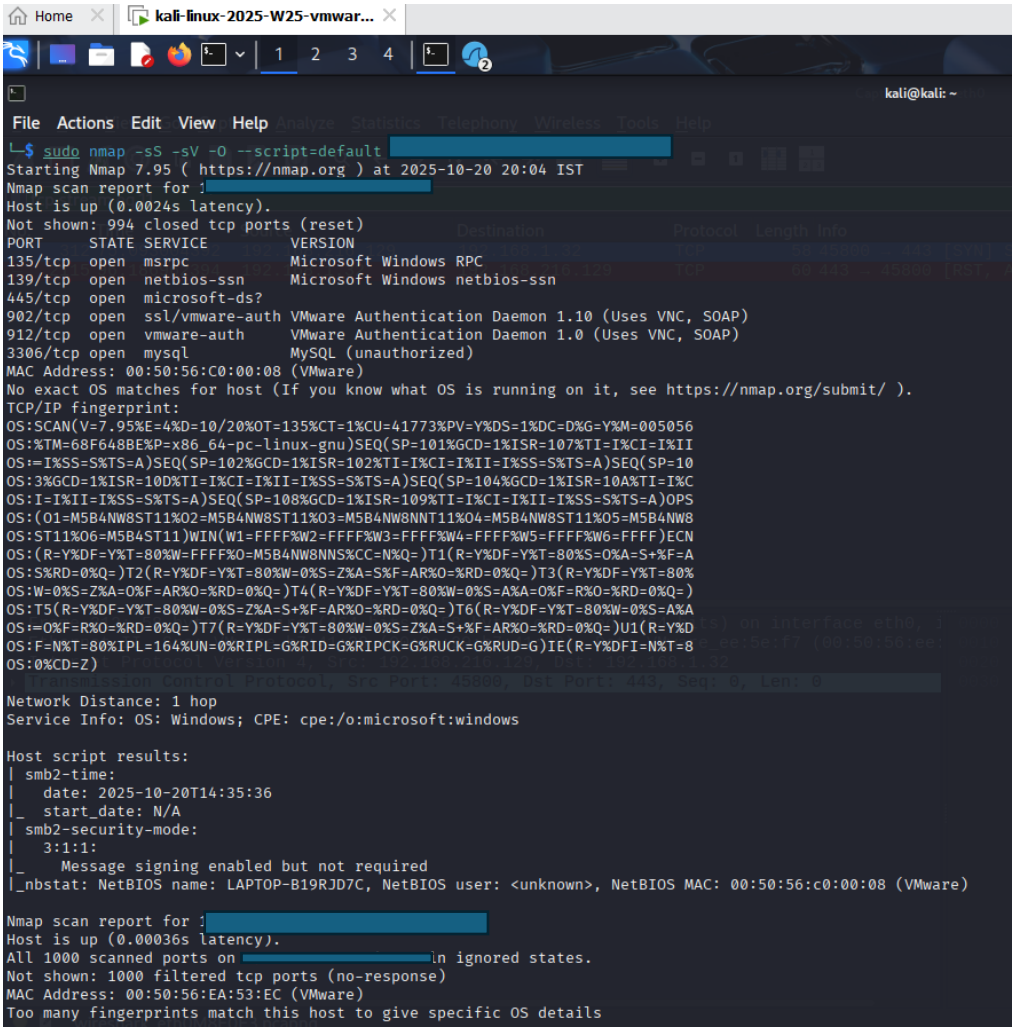
Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap

Scanning IP:

Nmap result:





Open ports:-

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

3306/tcp open mysql

Potential security risks from open ports:-

135/tcp (msrpc)

Exposes Windows RPC endpoint used for service discovery—can be leveraged for enumeration and to pivot using RPC-based exploits.
If unpatched or reachable from untrusted networks, attackers may enumerate services and use RPC to launch further attacks or remote code execution.

139/tcp (netbios-ssn)

Allows NetBIOS name resolution and SMB-over-NetBIOS share enumeration; it can reveal share names, users, and machine info.
If exposed, it enables information disclosure, null-session abuse, and easier lateral movement or credential attacks.

445/tcp (microsoft-ds / SMB)

SMB exposure is a high-value target for ransomware, worms, and remote code exploits—vulnerable/old SMB implementations are actively exploited.
Open SMB can permit file/share abuse, credential theft or relay attacks, and full network compromise if not patched or properly restricted.

902/tcp (VMware management)

Often used by VMware management/console services—if reachable, it can leak VM/host management interfaces and metadata.
Misconfiguration or vulnerable VMware versions can allow remote management abuse or information disclosure about VMs and hypervisor.

912/tcp (apex-mesh / vendor service)

Uncommon/vendor-specific service — unknown daemons increase risk due to lack of visibility and potentially weak/default configs.
If unnecessary or unpatched, it may contain exploitable bugs or allow unauthorized control/information leakage.

3306/tcp (MySQL)

Publicly reachable database port risks data exfiltration, brute-force access, and exploitation of database-specific vulnerabilities.
If bound to 0.0.0.0 or using weak credentials, attackers can access or dump sensitive data and pivot into internal systems.

Saved scan results in text:-