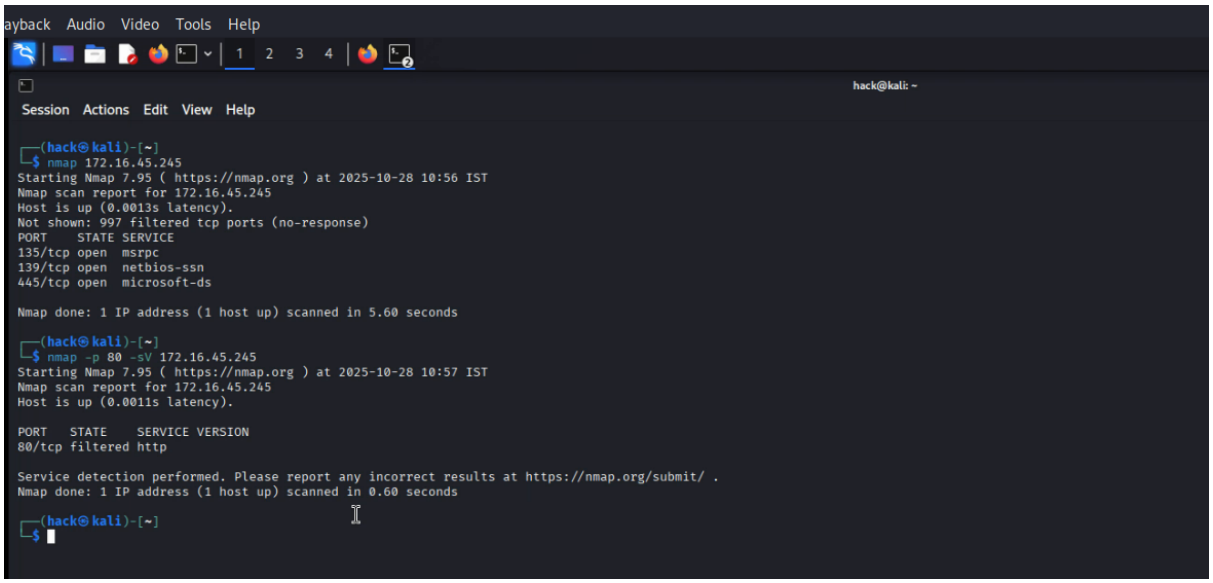
Task 1: Basic Network Scanning with Nmap

Nmap Scan:

Nmap scan is the process that is done with the help of the Nmap tool. The Nmap scan is used to scan the open ports in the connected network of the system, for the security purpose.



Open Ports & Its definitions:

1) Port 135/tcp (msrpc)

- **Service:** Microsoft RPC (Remote Procedure Call)
- **Purpose:** Used for Microsoft RPC services, which allow programs to execute processes on remote systems.
- **Commonly Found On:** Windows systems
- **Security Note:** Often targeted in attacks due to vulnerabilities in RPC services.

2) Port 139/tcp (netbios-ssn)

- **Service:** NetBIOS Session Service
- **Purpose:** Used for file and printer sharing across a network (NetBIOS over TCP/IP). It enables networked computers to communicate.
- **Commonly Used By:** Windows file and printer sharing
- **Security Note:** Should be blocked from the internet as it may expose sensitive shares.

3) **Port 445/tcp (Microsoft-ds)**

- **Service:** Microsoft Directory Services (SMB over TCP)
- **Purpose:** Supports file and printer sharing and network browsing. It runs the SMB (Server Message Block) protocol directly over TCP (without NetBIOS).
- **Used By:** Modern Windows networking, Active Directory, file sharing.
- **Security Note:** Frequently targeted by malware (e.g., WannaCry ransomware) and should not be exposed to untrusted networks.

Summary:

All these ports are associated with Microsoft network services and are typically found open on Windows servers. For security, these should not be exposed to the public internet unless strictly necessary, and should be protected by firewalls and proper security configurations.