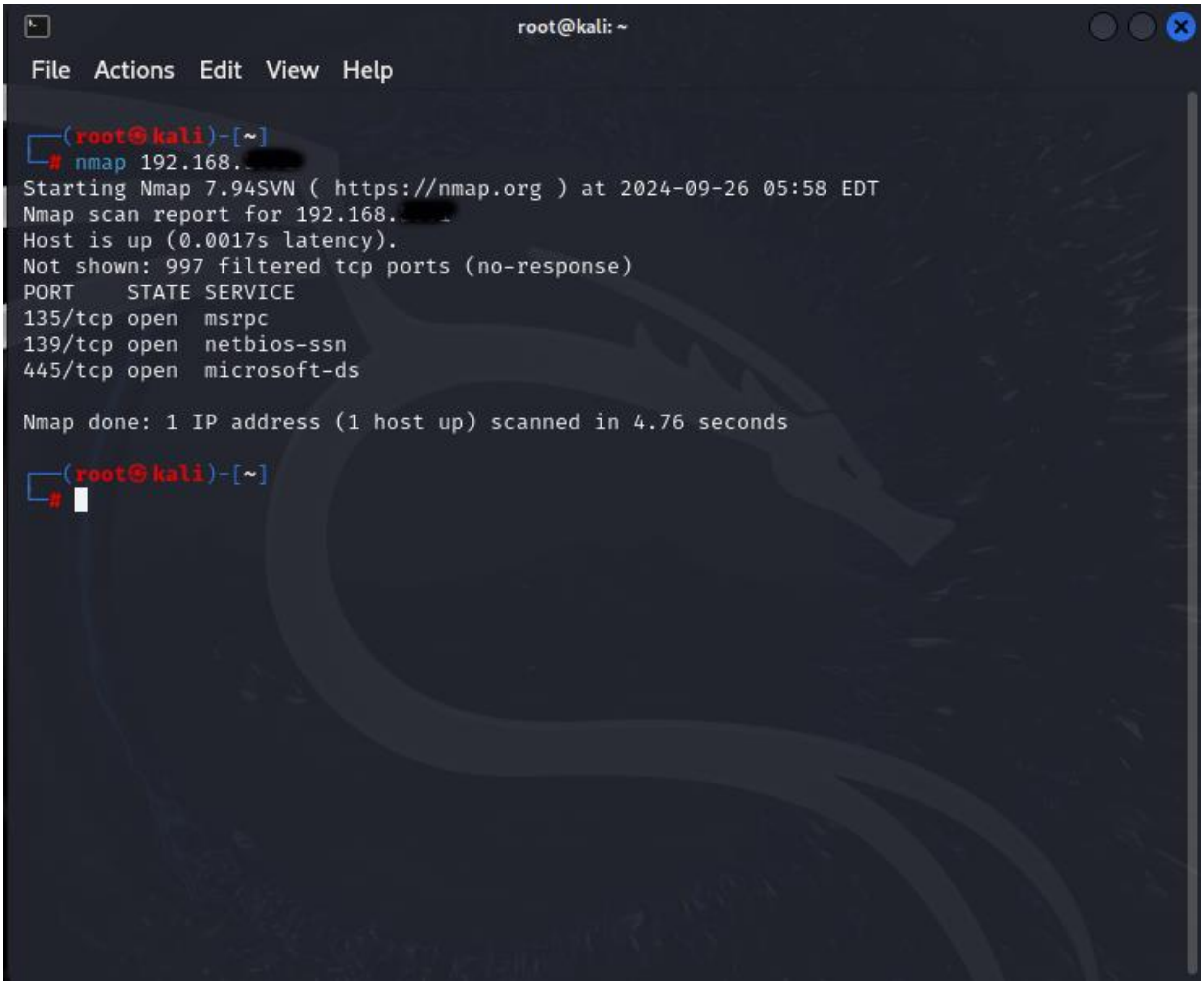
Intermediate Task

Task1: Basic Vulnerability Scan Using Nmap

In this task, I performed a basic vulnerability scan on the target IP 192.168.x.x using **Nmap**, an open-source network scanning tool. The goal was to identify vulnerabilities.

Normal Scanning:

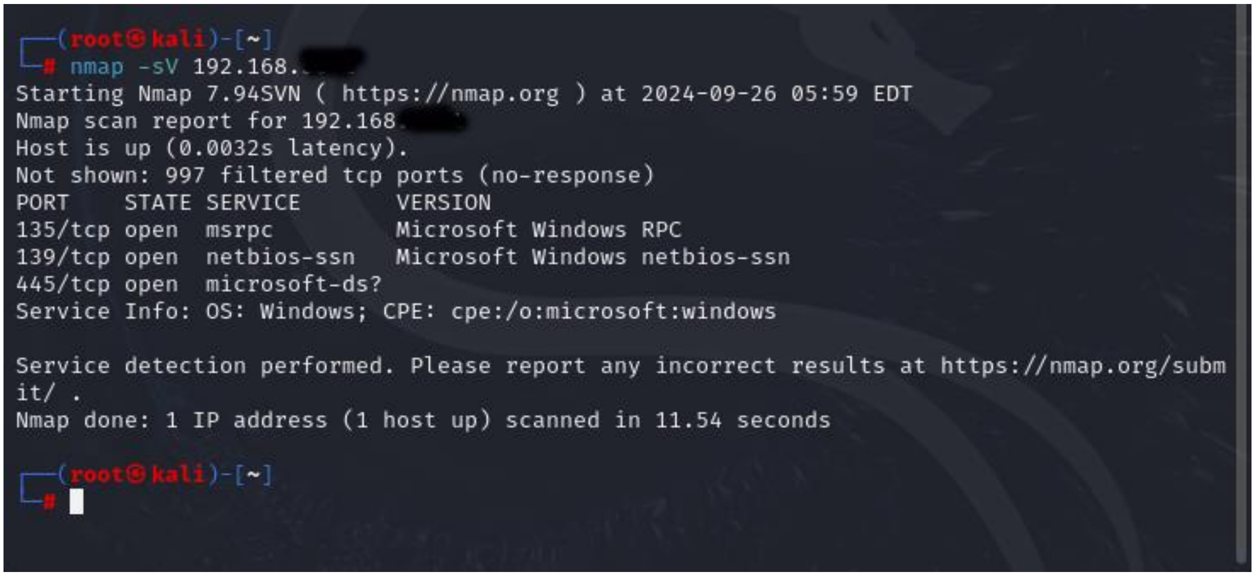


```
┌──(root㉿kali)-[~]
└─# nmap 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 05:58 EDT
Nmap scan report for 192.168.[redacted]
Host is up (0.0017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds

┌──(root㉿kali)-[~]
└─# 
```

Sofware Version Scanning:

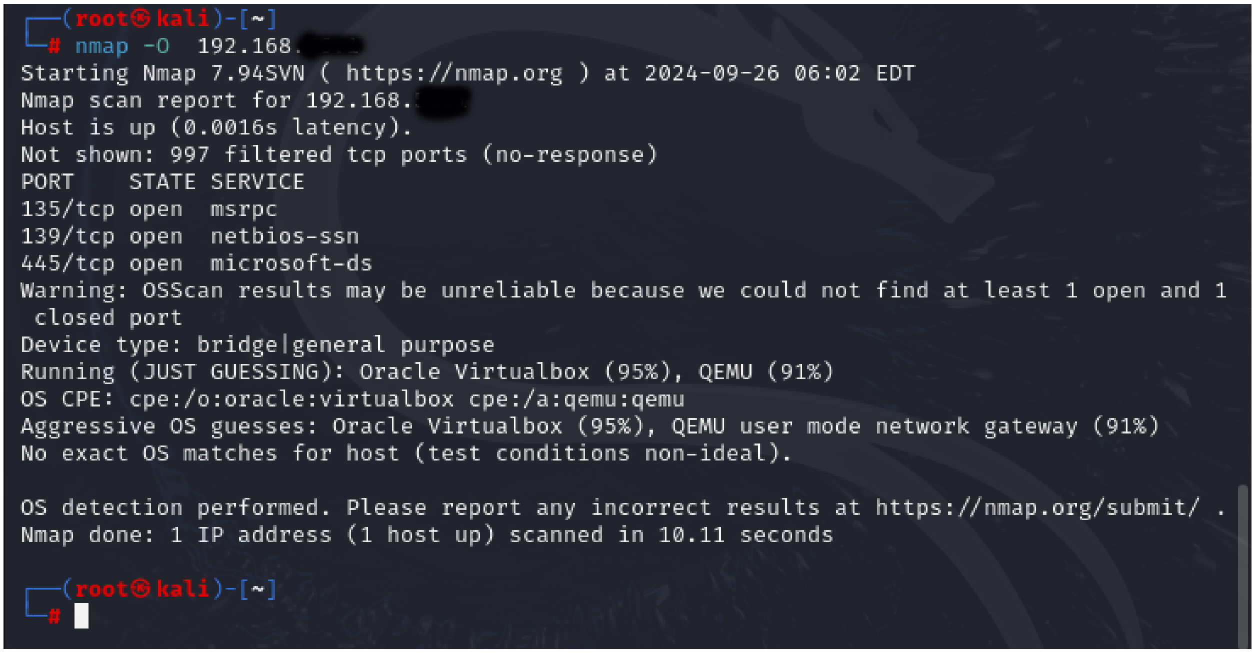


```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 05:59 EDT
Nmap scan report for 192.168[redacted]
Host is up (0.0032s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds

┌──(root㉿kali)-[~]
└─# █
```

OS Scanning:



```
┌──(root㉿kali)-[~]
└─# nmap -O  192.168.[redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 06:02 EDT
Nmap scan report for 192.168.[redacted]
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.11 seconds

┌──(root㉿kali)-[~]
└─# █
```