CYBERSECURITY INTERNSHIP

Organization name: Elevate labs

Student Name: Radhika Lakshmi. Teeramdasu

University: Aditya University

Domain: Cybersecurity

Duration: 1st January 2026 to 30th April 2026

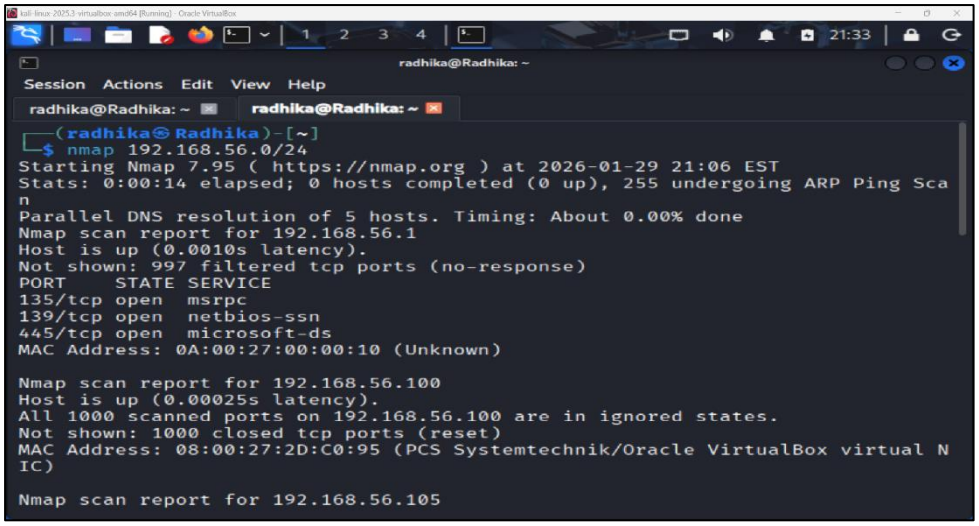
TASK-9: Network Vulnerability Scanning

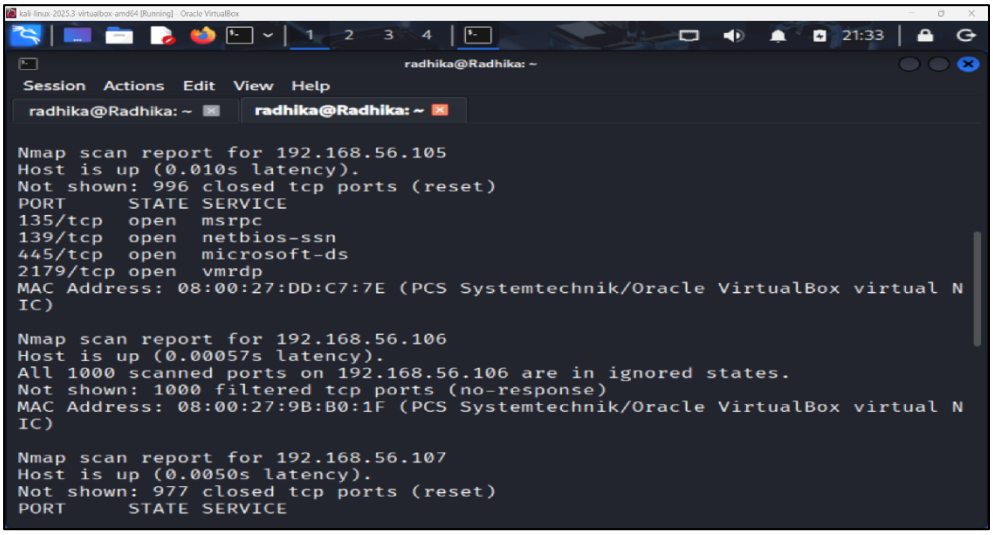
Network vulnerability scanning is the process of identifying security weaknesses in networked systems by scanning hosts, open ports, running services, operating systems, and known vulnerabilities using automated tools. It helps organizations discover potential entry points before attackers can exploit them.

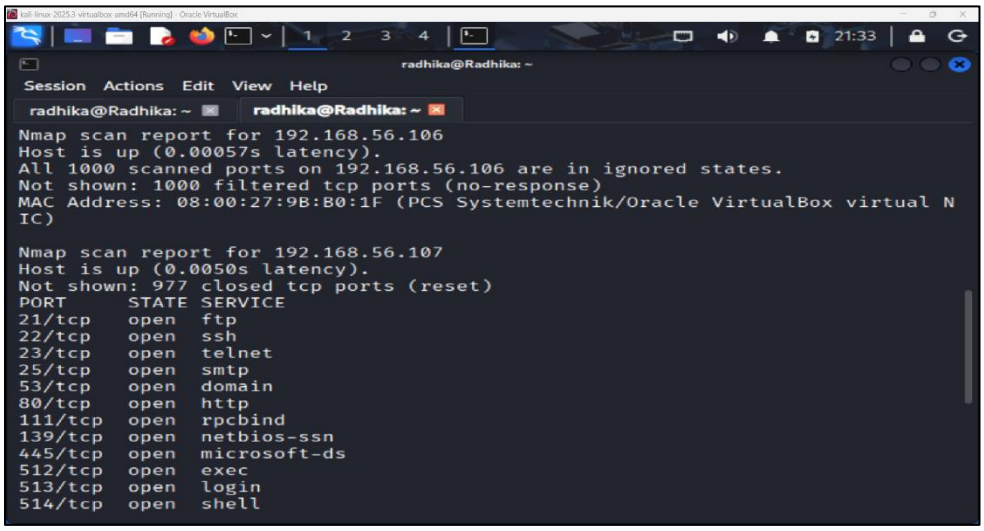
- **Scan Local Network:**

Local network scanning means identifying all active devices (hosts) connected to the same network. This helps understand what systems are reachable and could be potential attack targets.

1. To find IP address – **ipconfig** (windows), **ifcongif** (linux)
2. To scan the local network – **nmap -sn (ip address).0/24**


radhika@Radhika: ~
Session Actions Edit View Help
radhika@Radhika: ~
radhika@Radhika: ~
(radhika㉿Radhika)-[~]
$ nmap 192.168.56.0/24
Starting Nmap 7.95 (https://nmap.org) at 2026-01-29 21:06 EST
Stats: 0:00:14 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 5 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.56.1
Host is up (0.0010s 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
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2D:C0:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105


radhika@Radhika: ~
Session Actions Edit View Help
radhika@Radhika: ~
radhika@Radhika: ~
Nmap scan report for 192.168.56.105
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2179/tcp open vmrdp
MAC Address: 08:00:27:DD:C7:7E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:9B:B0:1F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.107
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE


radhika@Radhika: ~
Session Actions Edit View Help
radhika@Radhika: ~
radhika@Radhika: ~
Nmap scan report for 192.168.56.106
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:9B:B0:1F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.107
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell

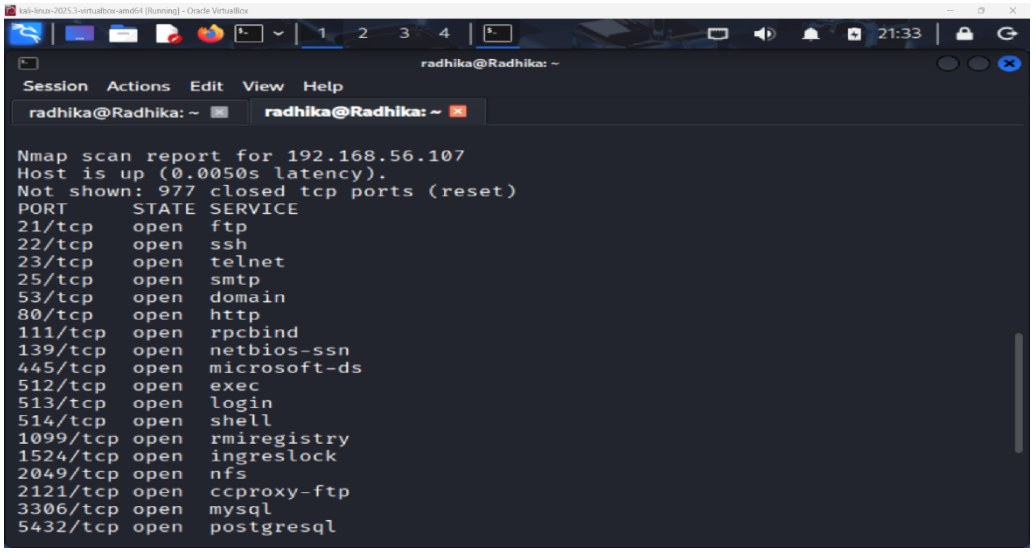
- **Identify open ports:**

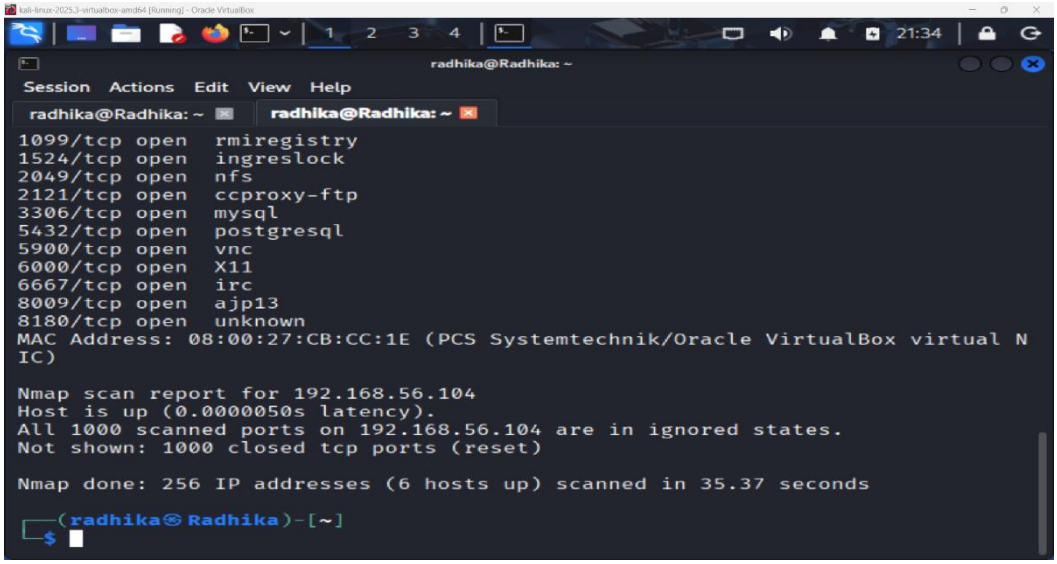
Open ports are communication endpoints that accept incoming connections. Identifying them shows which services are accessible from the network.

Common ports:

1. 80 – HTTP
2. 443 – HTTPS
3. 22 – SSH
4. 21 – FTP

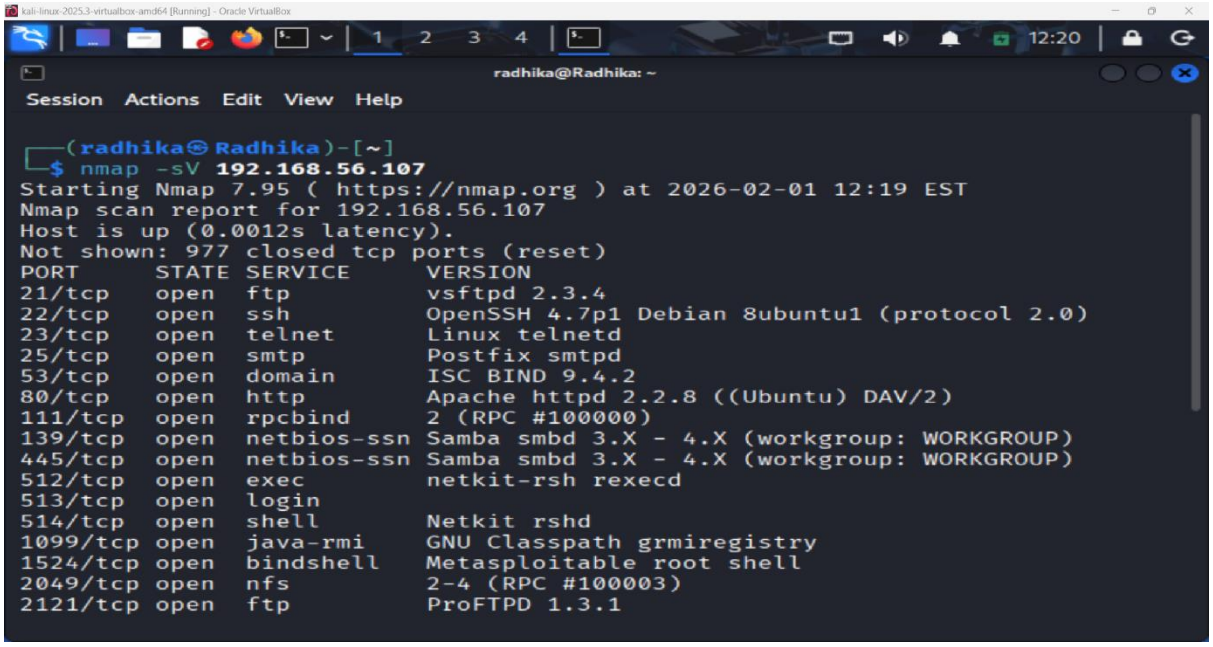
Open ports can become attack points if poorly secured.

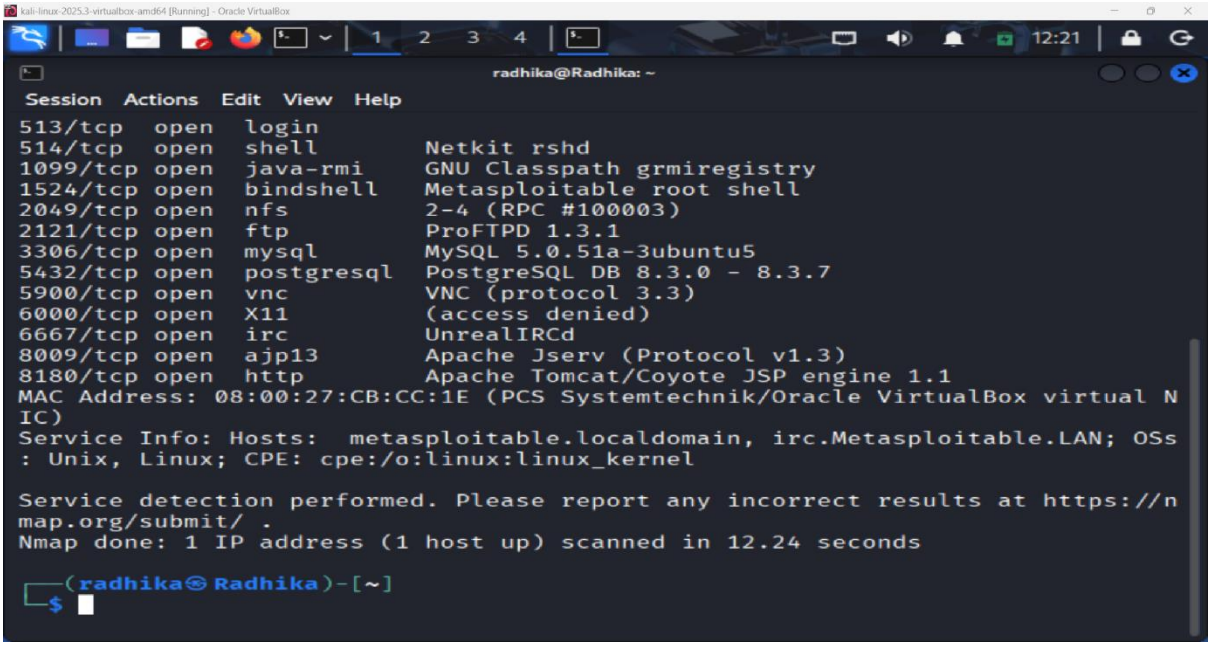




- **Detect Services:**

Service detection identifies what application is running on each open port, such as: Apache or Nginx web server, SSH daemon, FTP service. This step helps attackers and defenders understand what software is exposed.

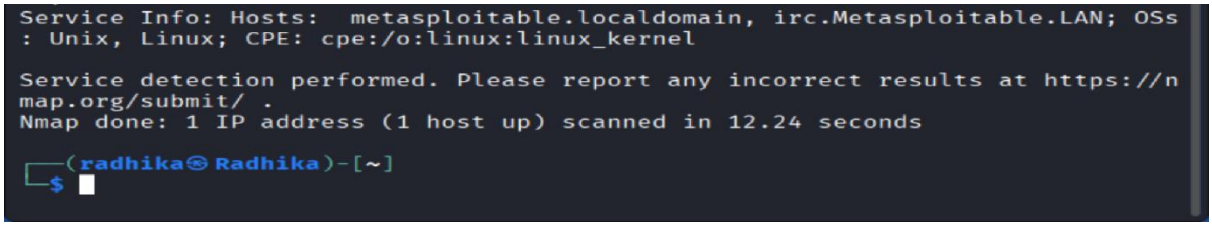




- **Identify OS:**

OS detection attempts to determine whether the target system is running - Windows, Linux, macOS, Network devices (routers, firewalls). Knowing the OS helps in mapping OS-specific vulnerabilities.

nmap -o (ip address)



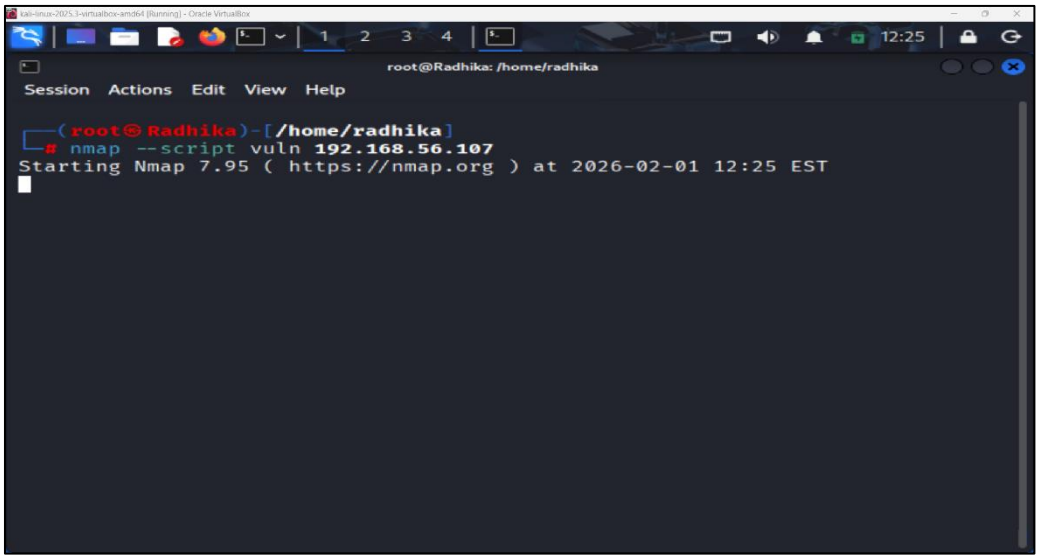
- **Analyze vulnerabilities:**

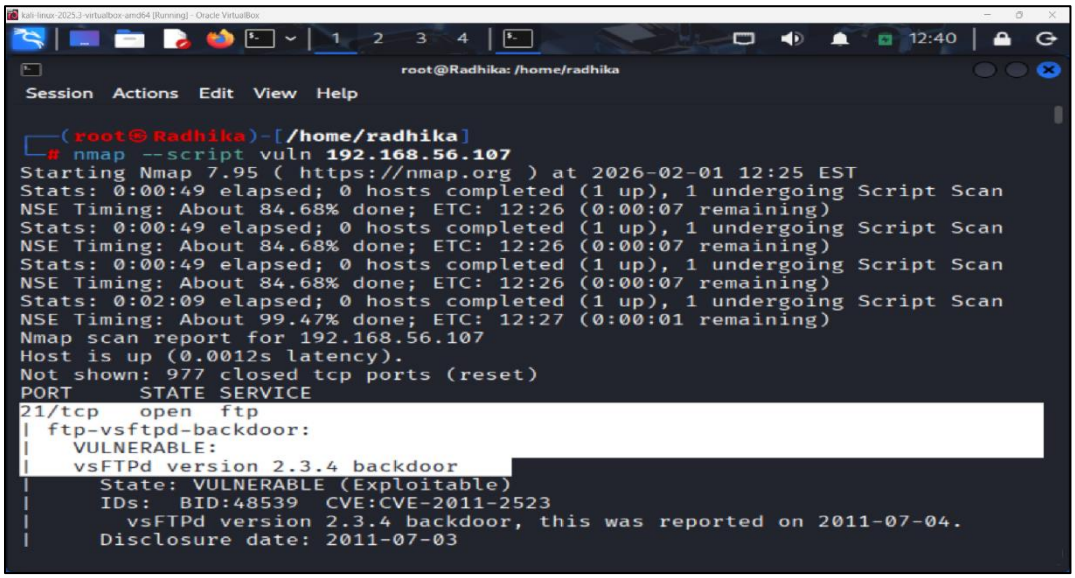
By combining open ports, services, and OS details, potential vulnerabilities can be inferred, such as:

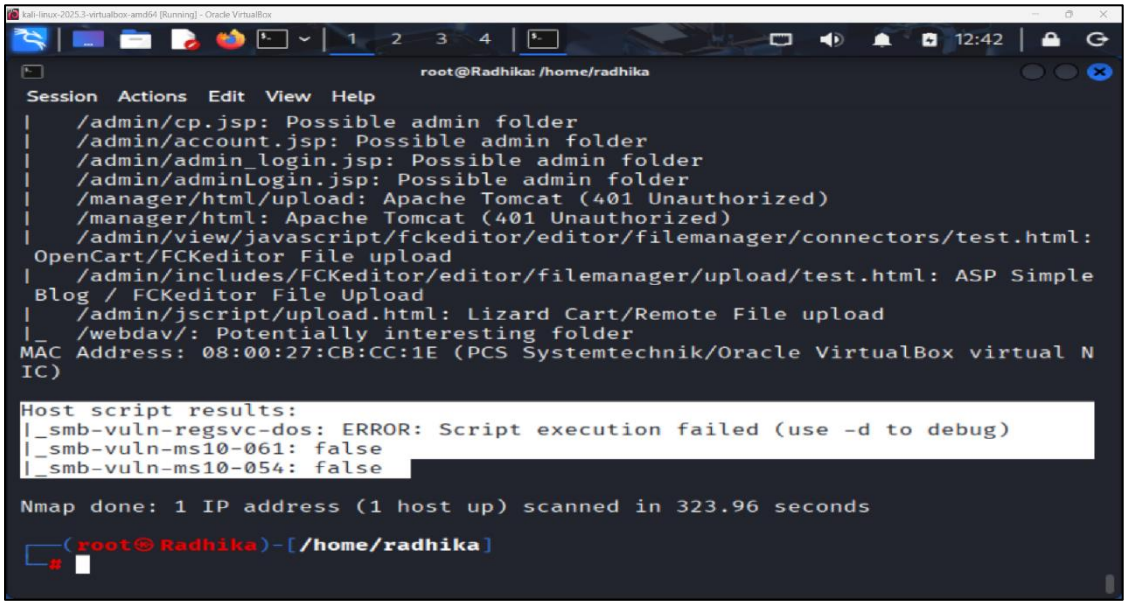
- Outdated software versions
- Unencrypted services
- Misconfigured services

This step does not exploit, only identifies weaknesses.

nmap –script vuln (target ip address)







- **Document Findings:**

All results are recorded in a structured report including:

- Target IP
- Open ports
- Services detected