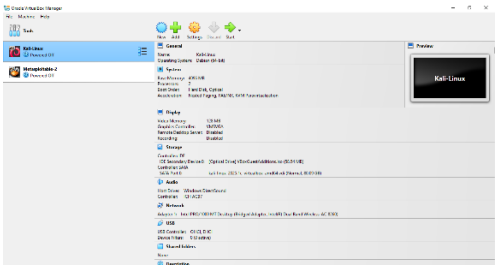
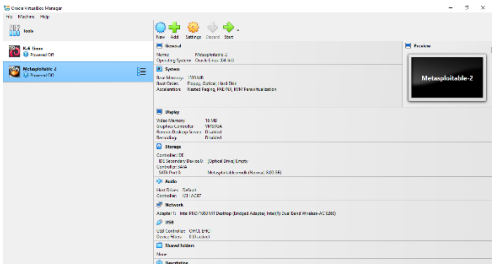
Vulnerability Scanning Using Nmap

Task-1 :- Network Configuration & Connectivity

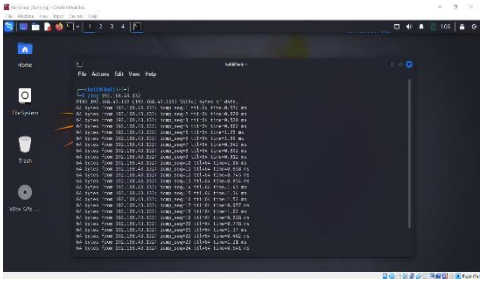
a.) Kali Linux & Metasploitable VMs





b.) Verify IP address using “ifconfig”

c.) Use “ping” to confirm connectivity between the machines



Task-2 :- Basic Port Scan

Run a simple Nmap scan on the Metasploitable target using “nmap <target-ip>”

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.43.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 01:49 EDT
Nmap scan report for 192.168.43.132
Host is up (0.00026s 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CA:93:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Task-3 :- Service Version Detection

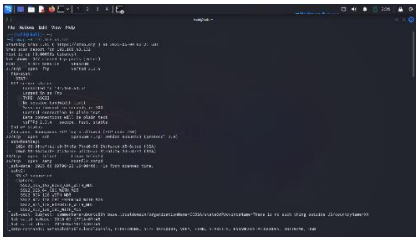
Run a version detection scan using “nmap -sV <target-ip>”

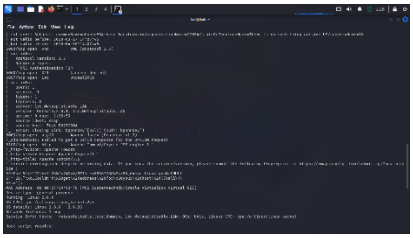
Task-4 :- Operating System Fingerprinting

Run an OS detection scan using “nmap -O <target-ip>”

Task-5 :- Aggressive Scan

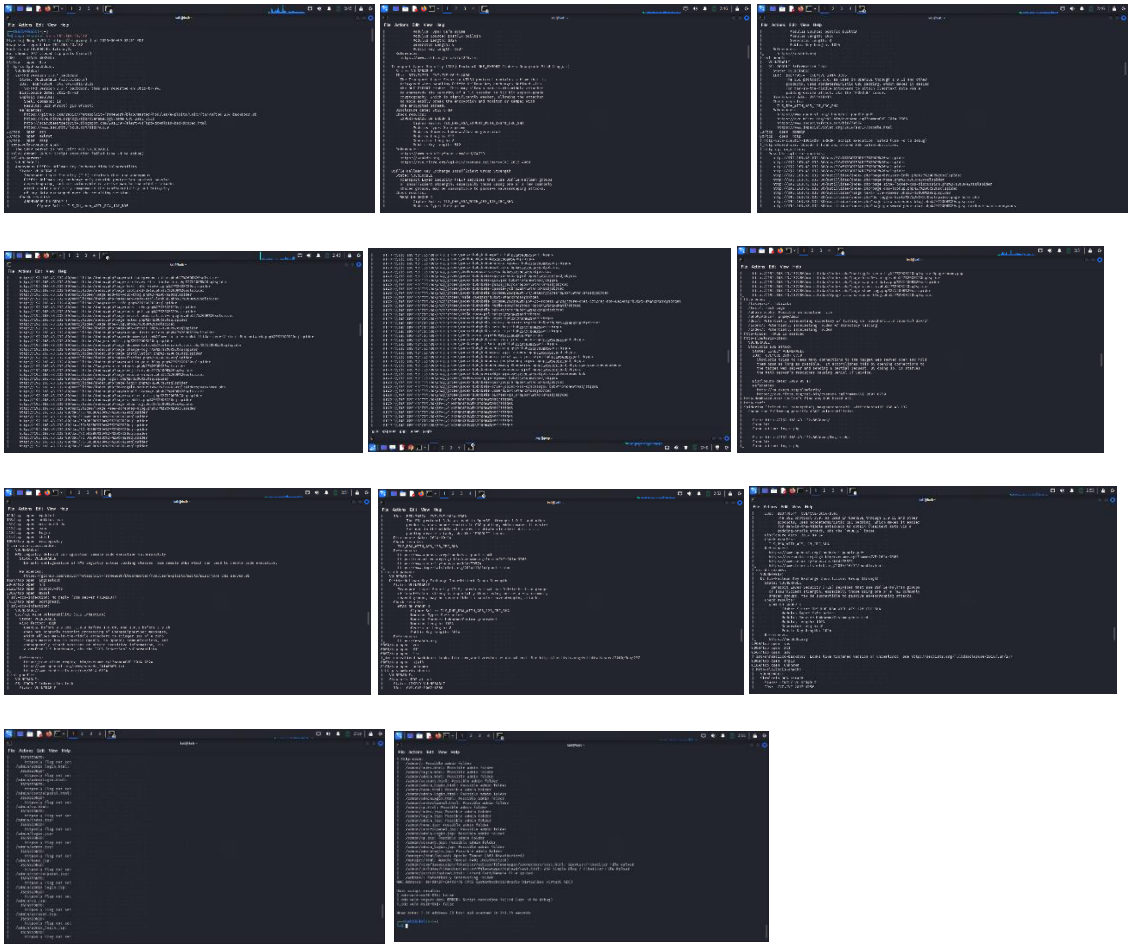
Perform a full aggressive scan using “nmap -A <target-ip>”





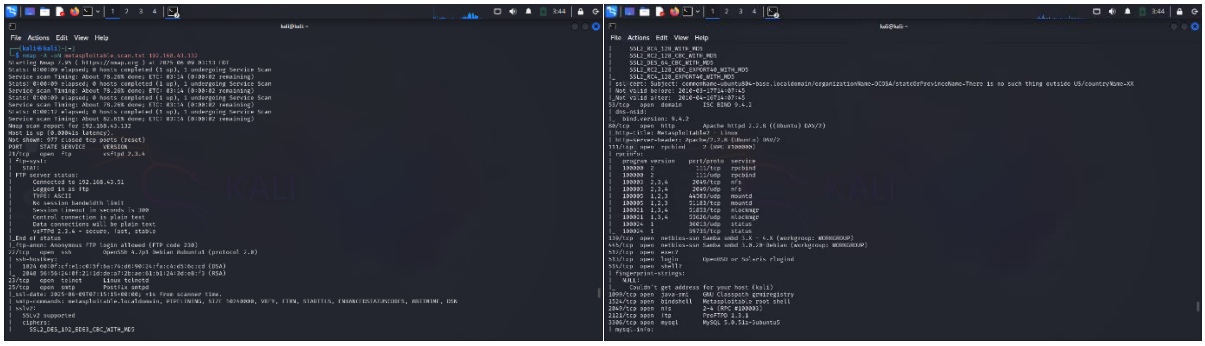
Task-6 :- Vulnerability Detection Using NSE Scripts

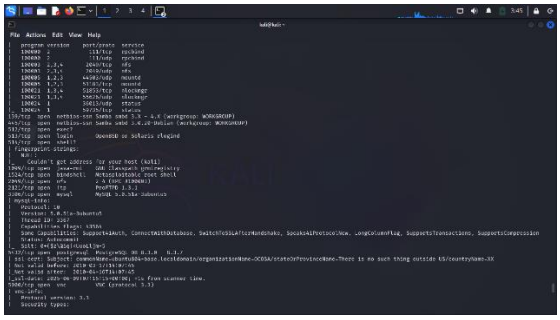
Run a vulnerability scan using “nmap --script vuln <target-ip>”

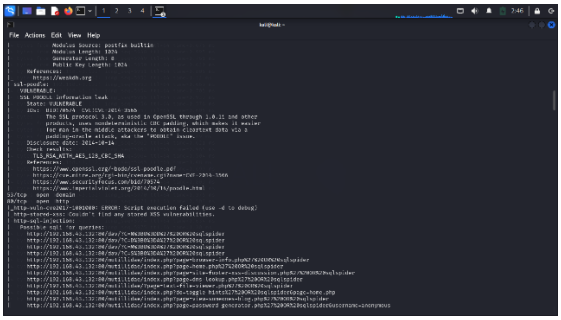


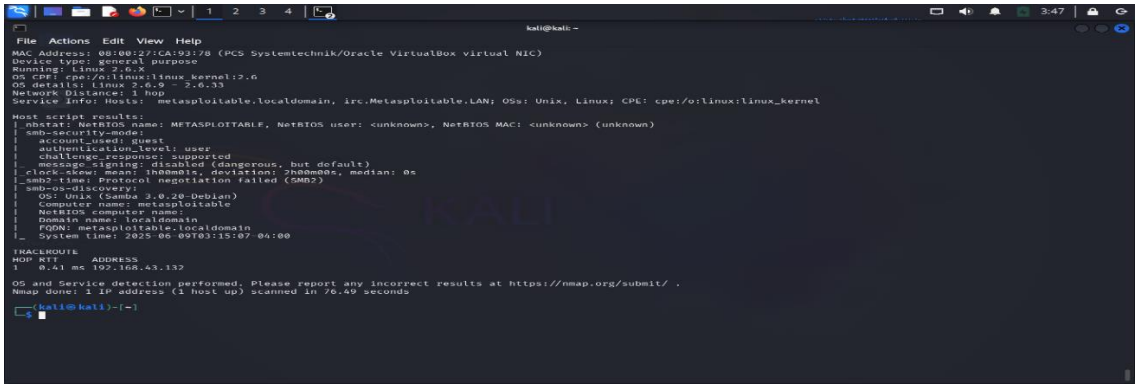
Task-7 :- Report Generation & Documentation

Save your scan results to a text file using “nmap -A -oN metasploitable_scan.txt <target-ip>”









Task-8 :- Analysis Of Findings

Port	Service	Version	Known Vulnerability
21	ftp	vsftpd 2.3.4	Brute-Forcing passwords, Man-in-the-middle
22	ssh	OpenSSH 4.71p1	Leaked SSH keys, Brute-forcing Credentials
23	telnet	Linux telnetd	Credential brute-forcing, spoofing and credential sniffing
25	smtp	Postfix smtp	Spoofing, spamming
53	domain	ISC Bind 9.4.2	DDoS attacks
80	http	Apache 2.2.8	SQL injections, Cross-site scripting
111	rpcbind	2	Difficult to Detect, Difficult to Resolve
139	netbios-ssn	Samb smbd 3.x – 4.x	EternalBlue exploit, Capturing NTLM Hashes

445	netbios-ssn	Samb smbd 3x – 4x	Inject Malware, Ransomware
513	login	-	Brute force, Multipe buffer overflows