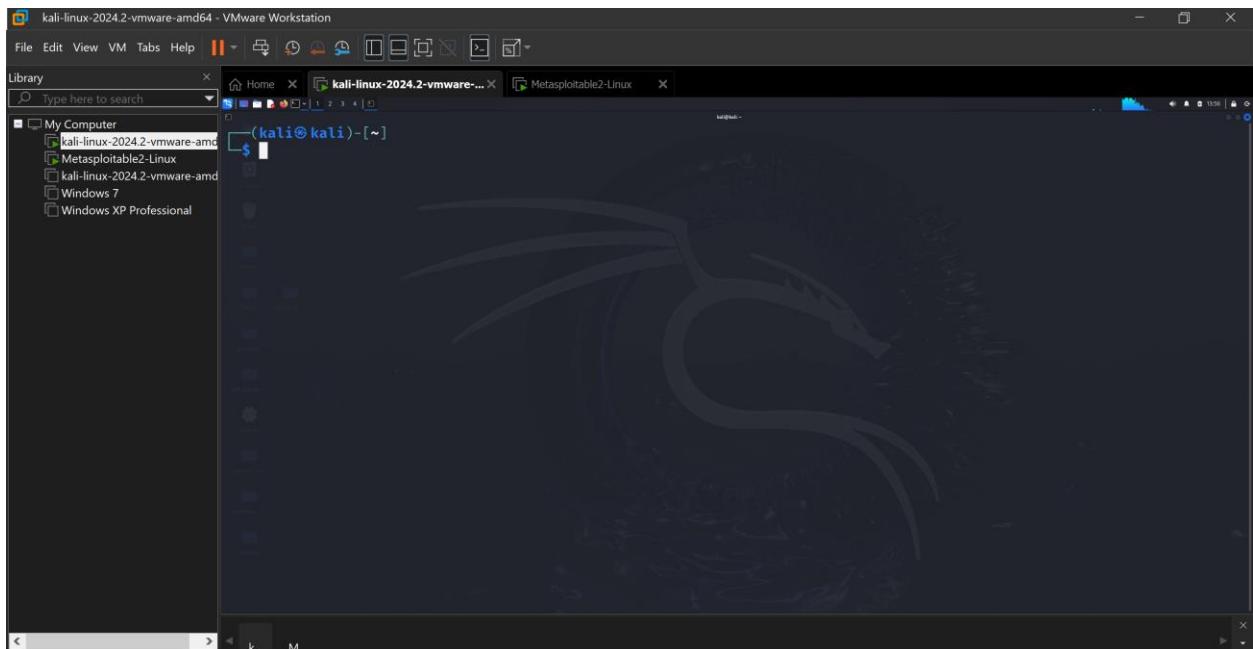
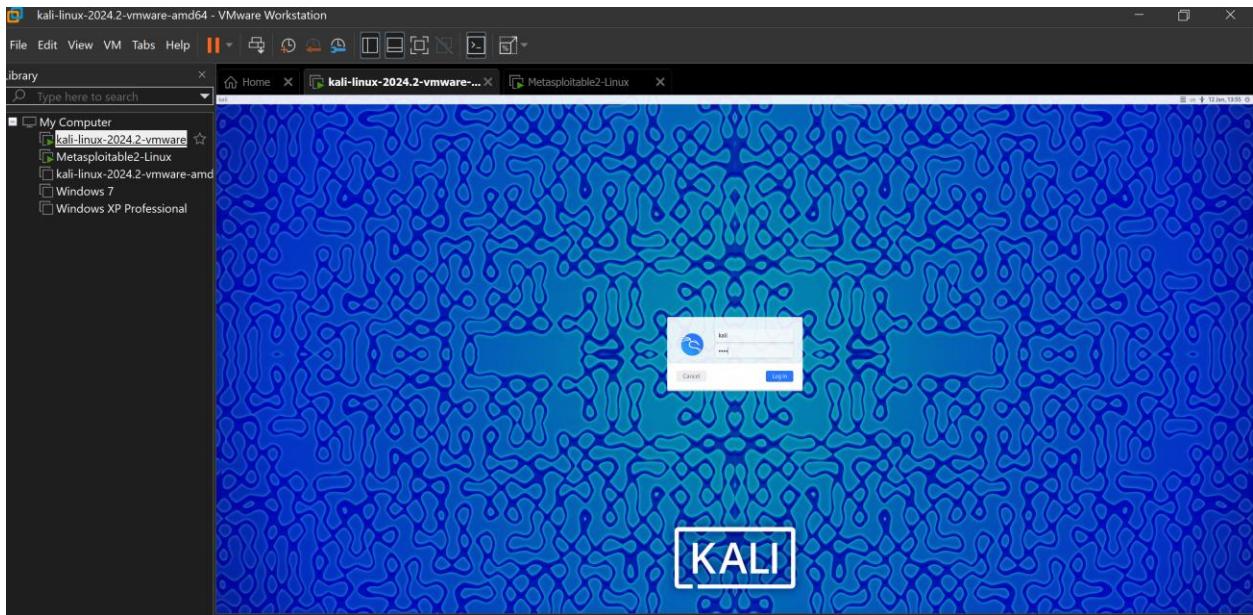
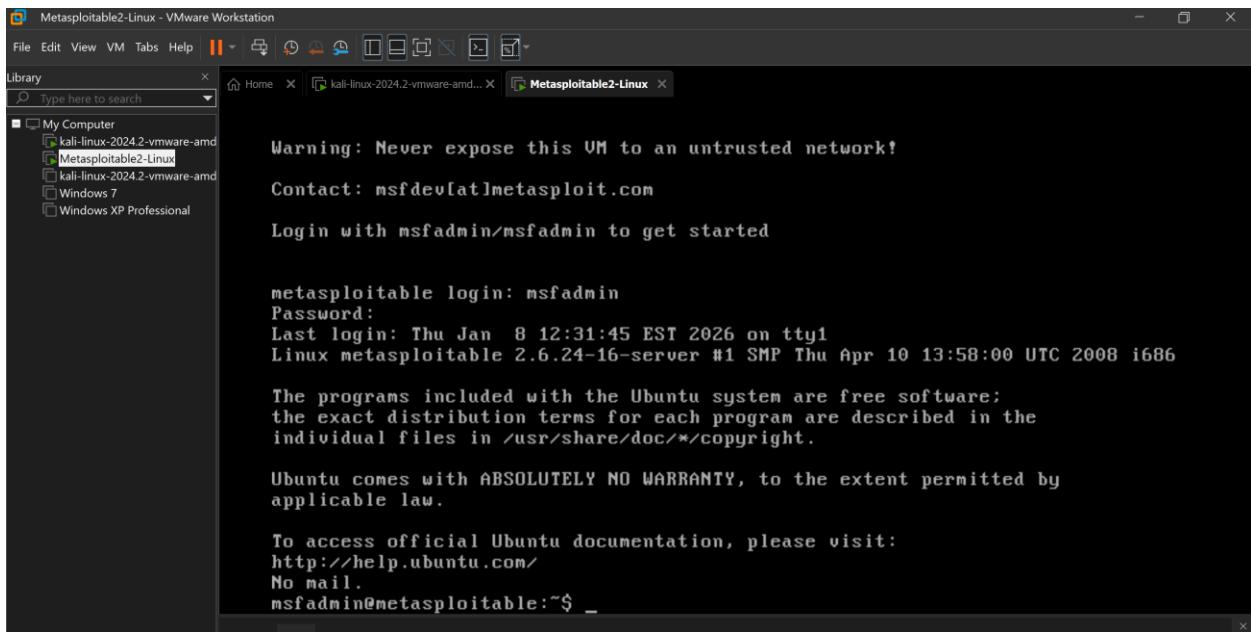


Vulnerability Assessment Lab

Open Kali Linux



Open Metasploitable2



For Checking IP Address

Ifconfig

Kali Linux Result

```
(kali㉿kali)-[~]
└─$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 14:11 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00030s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Metasploitable2 Result

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:64:29:a7
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35929 (35.0 KB) TX bytes:35929 (35.0 KB)

msfadmin@metasploitable:~$
```

Nmap Scan Result

```
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 14:03 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0004s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
```

Metasploitable2 Result

```

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
953/tcp open  rndc
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.143 seconds
msfadmin@metasploitable:~$ 

```

Detailed Nmap Scan

- `-sV` → Service version detection
- `-sC` → Default scripts
- `-A` → Aggressive scan (OS + traceroute)

```

(kali㉿kali)-[~]
$ nmap -sV -sC -A 192.168.56.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 14:14 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.59 seconds

```

```

Nmap done: 1 IP address (1 host up) scanned in 0.143 seconds
msfadmin@metasploitable:~$ nmap -sV -sC -A 127.0.0.1

Starting Nmap 4.53 ( http://insecure.org ) at 2026-01-12 14:15 EST
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 14:16 (0:00:05 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 14:16 (0:00:06 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:16 (0:00:03 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:16 (0:00:03 remaining)

[1]+  Stopped                  nmap -sV -sC -A 127.0.0.1
msfadmin@metasploitable:~$ 

```

Save Nmap Results