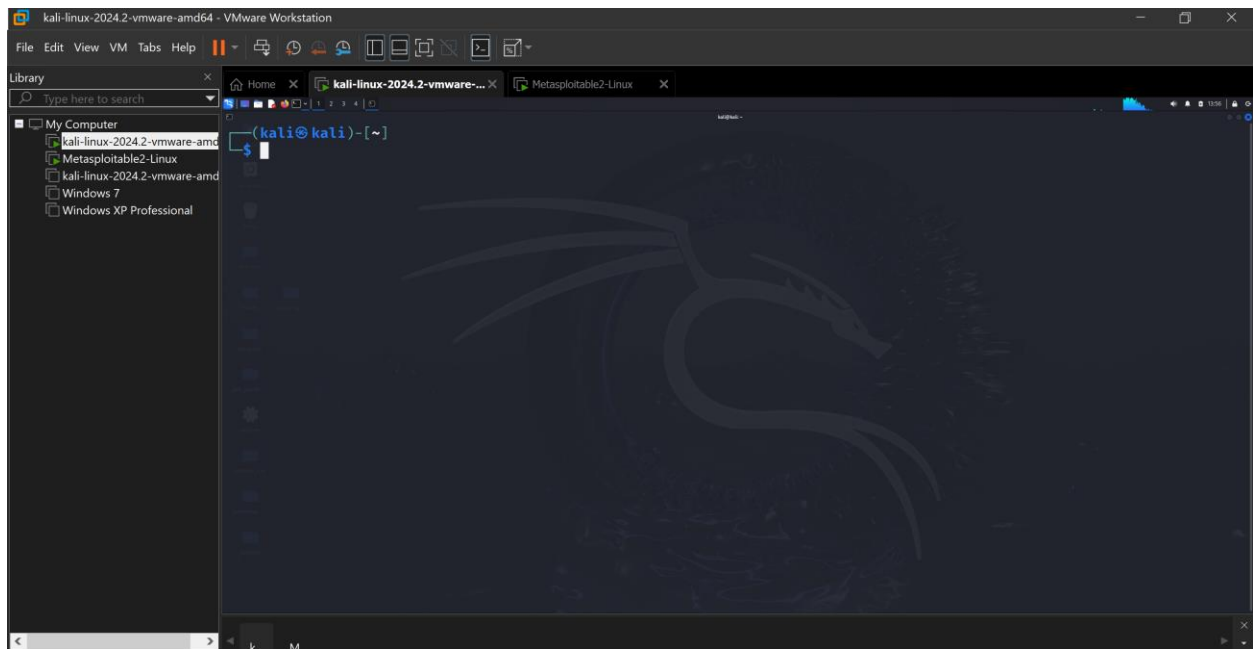
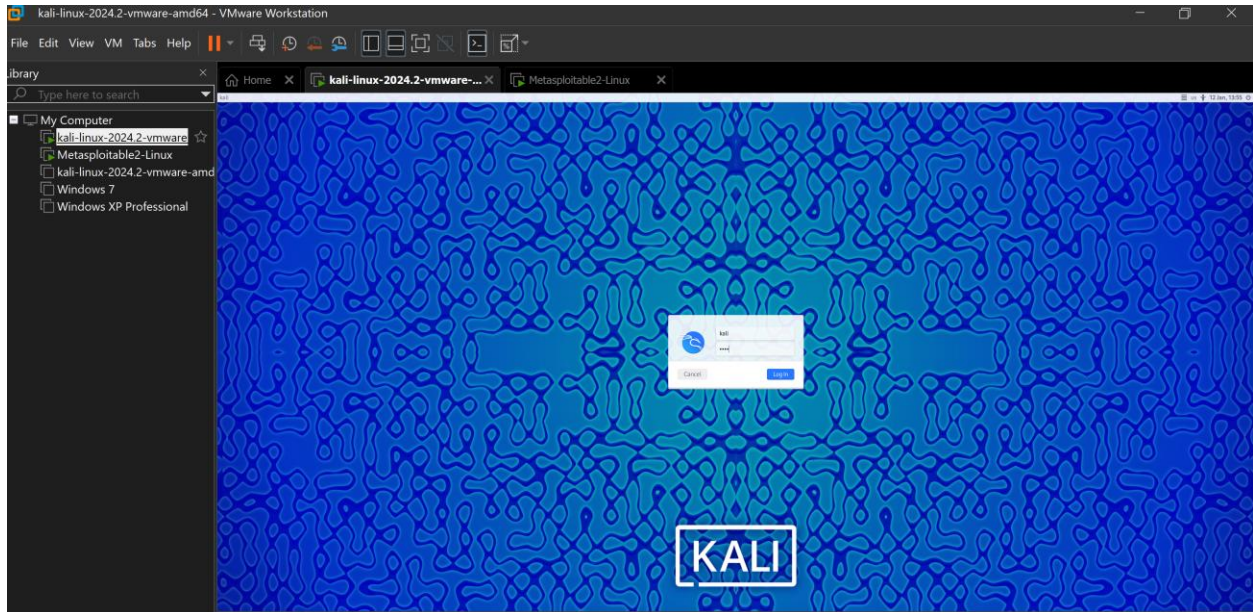
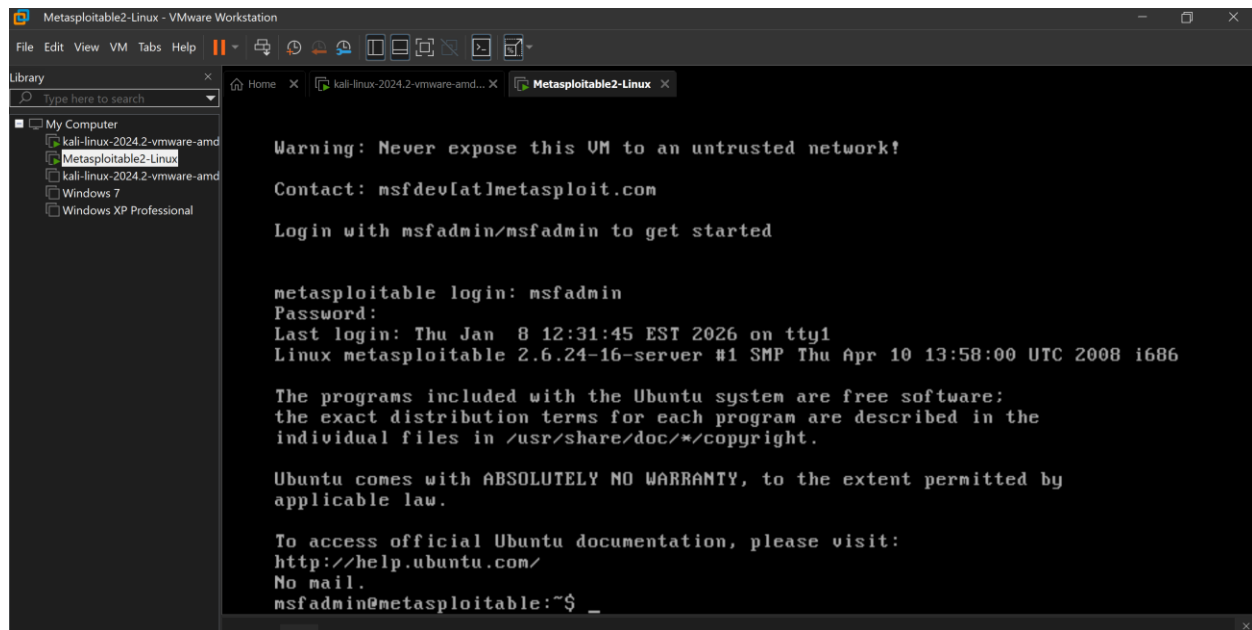


Vulnerability Assessment Lab

Open Kali Linux



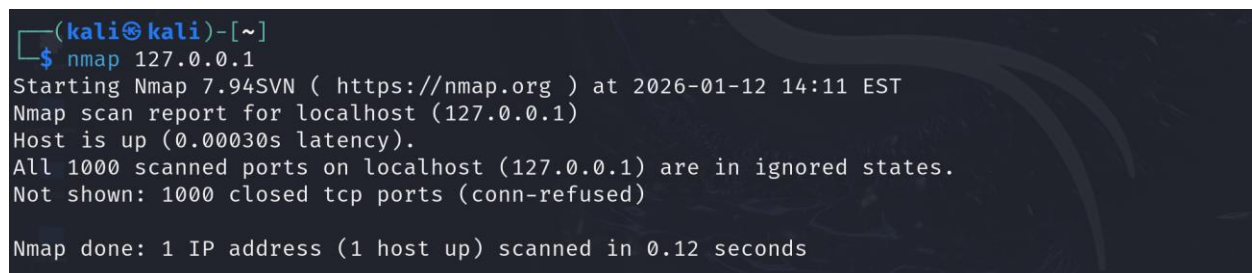
Open Metasploitable2



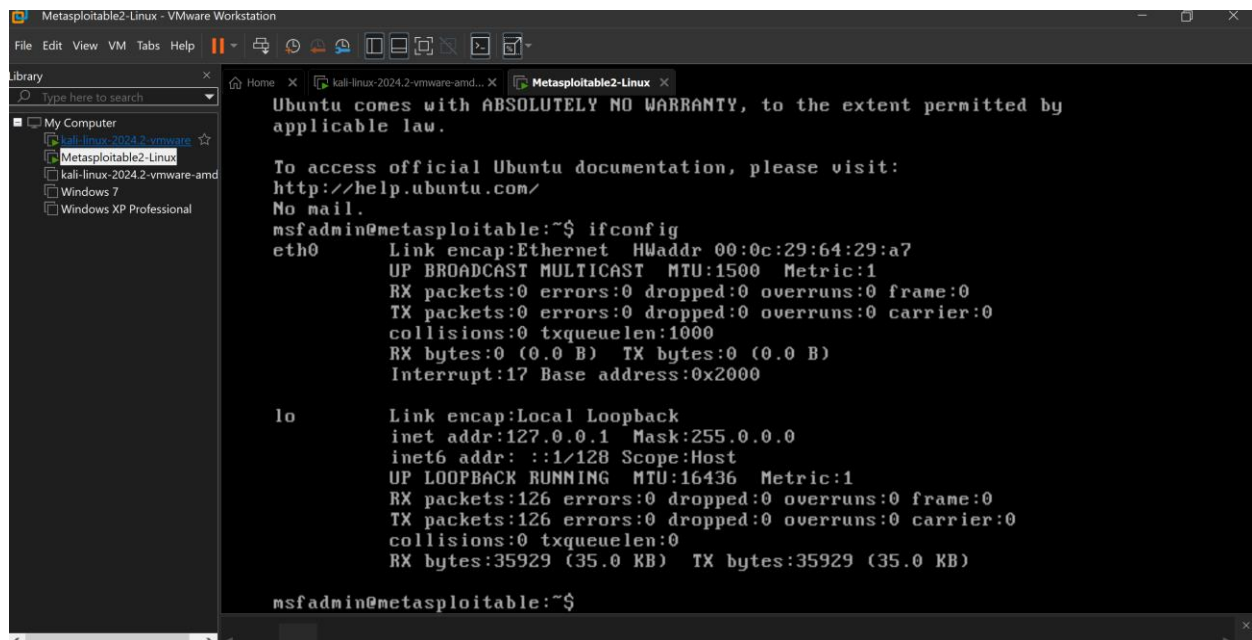
For Checking IP Address

Ifconfig

Kali Linux Result



Metasploitable2 Result



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help

Library
Type here to search
My Computer
  kali-linux-2024.2-vmware-amd64
  Metasploitable2-Linux
  kali-linux-2024.2-vmware-amd64
  Windows 7
  Windows XP Professional

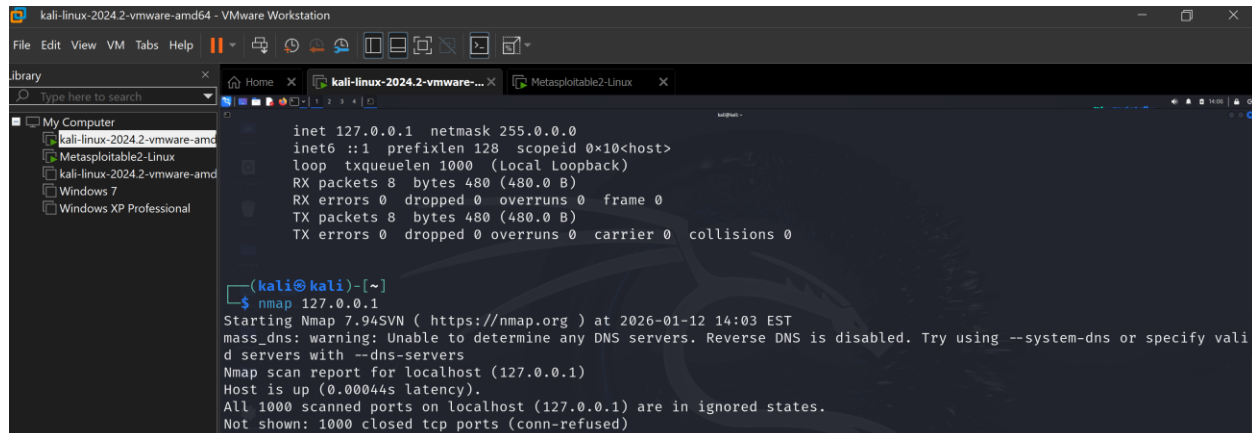
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

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



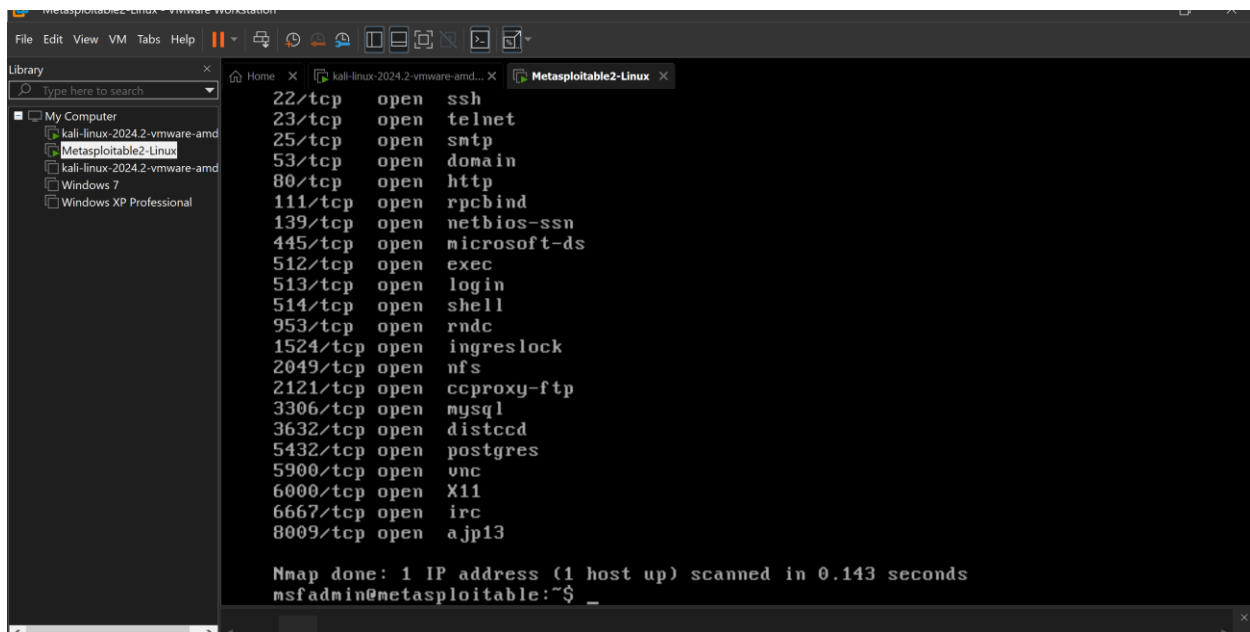
```
kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help

Library
Type here to search
My Computer
  kali-linux-2024.2-vmware-amd64
  Metasploitable2-Linux
  kali-linux-2024.2-vmware-amd64
  Windows 7
  Windows XP Professional

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

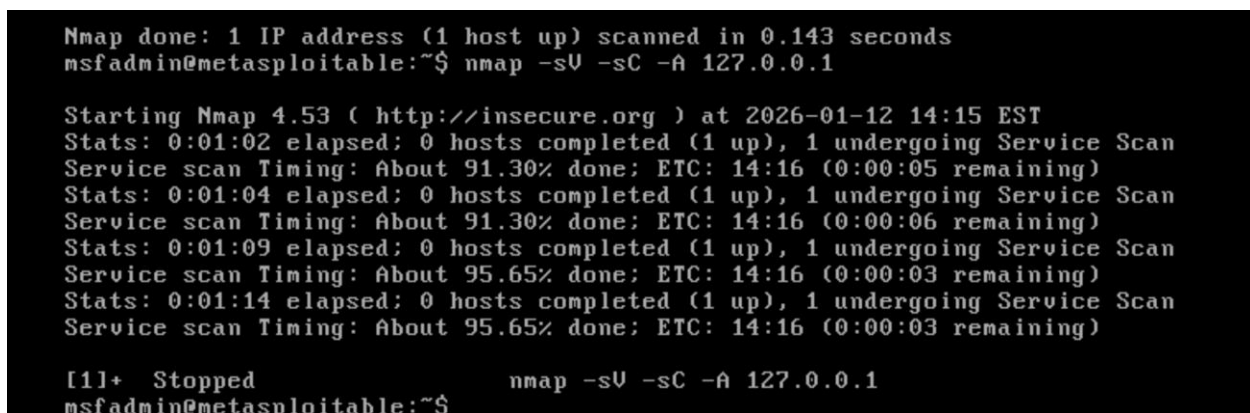
(kali@kali)-[~]
$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 14:03 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00044s 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



Detailed Nmap Scan

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



Save Nmap Results