Task 1: Lab Setup & Wireshark Packet Capture Report

Cybersecurity & Ethical Hacking Internship

Company: ApexPlanet Software Pvt. Ltd.
Task Duration: Days 1–12
Task Name: Lab Environment Setup & Packet Analysis

---

1. Objective

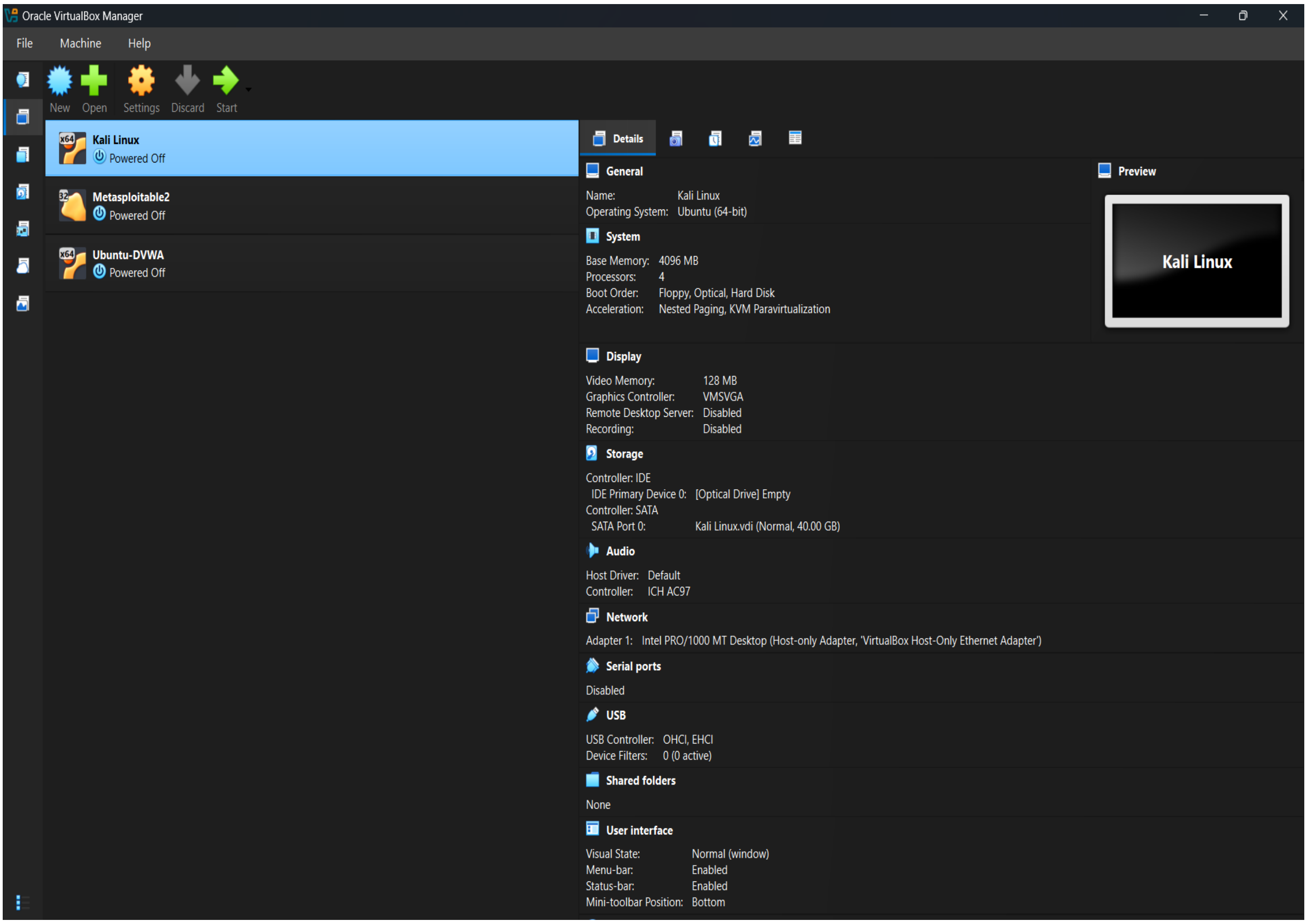
The objective of Task 1 is to set up a basic ethical hacking laboratory environment and demonstrate successful packet capture using Wireshark. This task focuses only on lab configuration, connectivity verification, and basic network traffic analysis.

---

2. Lab Environment Setup

2.1 Virtualization Platform

Oracle VirtualBox was installed and configured to create an isolated virtual laboratory environment.



Kali Linux — Powered Off
Metasploitable2 — Powered Off
Ubuntu-DVWA — Powered Off

General
Name: Kali Linux
Operating System: Ubuntu (64-bit)

System
Base Memory: 4096 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 40.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

Serial ports
Disabled

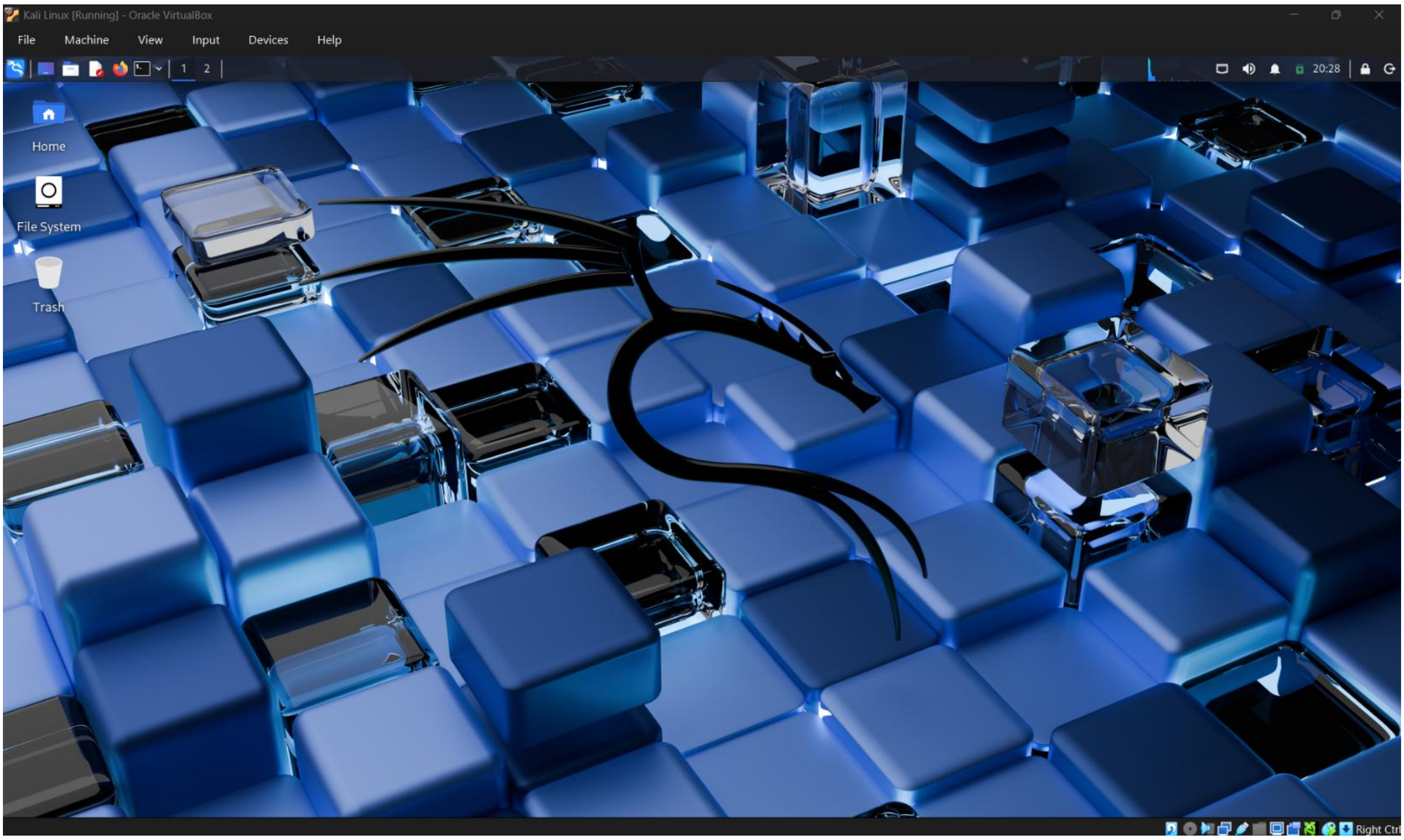
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

User interface
Visual State: Normal (window)
Menu-bar: Enabled
Status-bar: Enabled
Mini-toolbar Position: Bottom

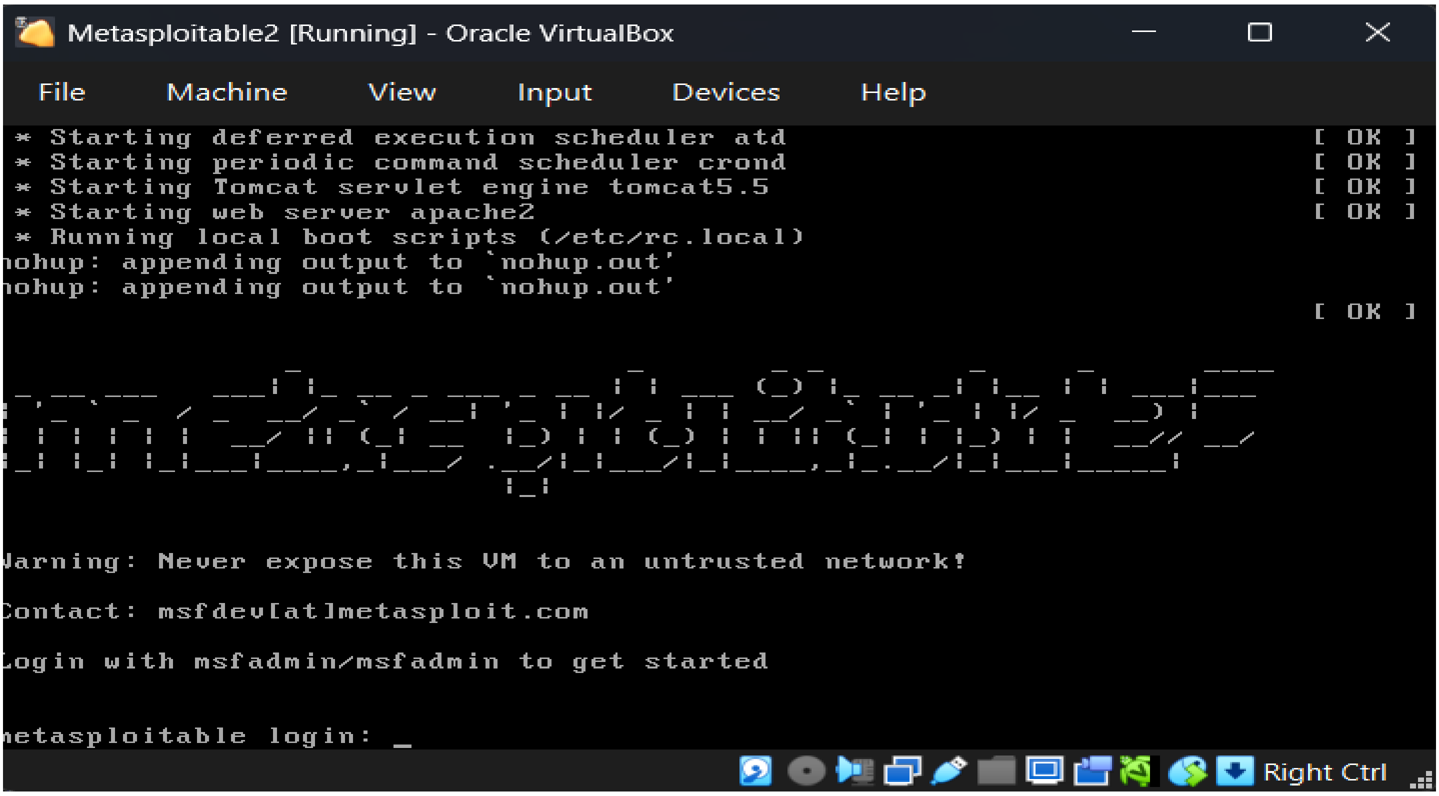
2.2 Attacker Machine Configuration

- **Operating System:** Kali Linux
  Kali Linux was used as the attacker machine for monitoring and capturing network traffic.



2.3 Target Machine Configuration

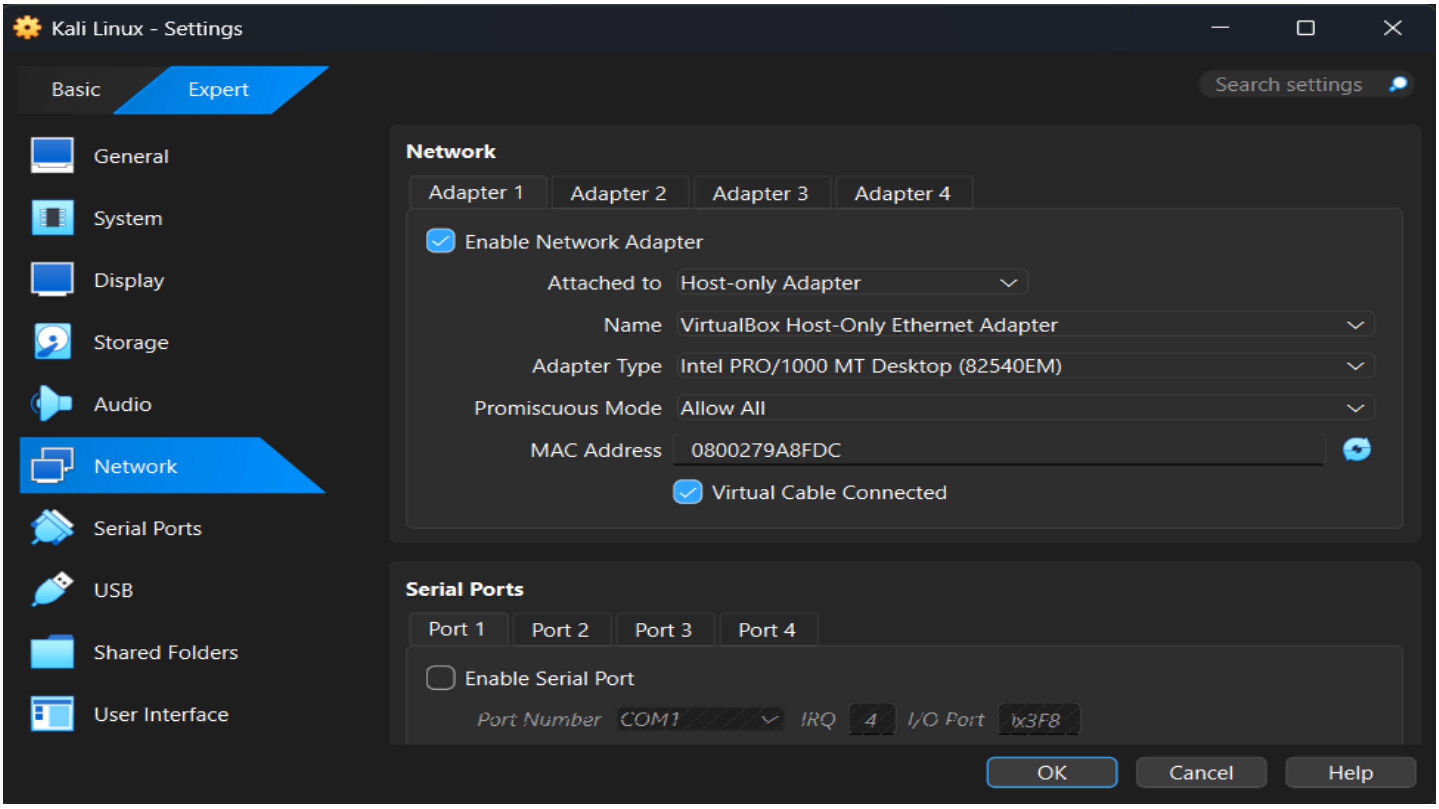
- **Operating System:** Metasploitable2
  The target machine was configured with intentionally vulnerable services for testing purposes.



```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

2.4 Network Configuration

- **Network Mode:** Host-Only Adapter
  This configuration ensures secure internal communication between virtual machines while preventing access to external networks.



Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 0800279A8FDC

☑ Virtual Cable Connected

Serial Ports

☐ Enable Serial Port

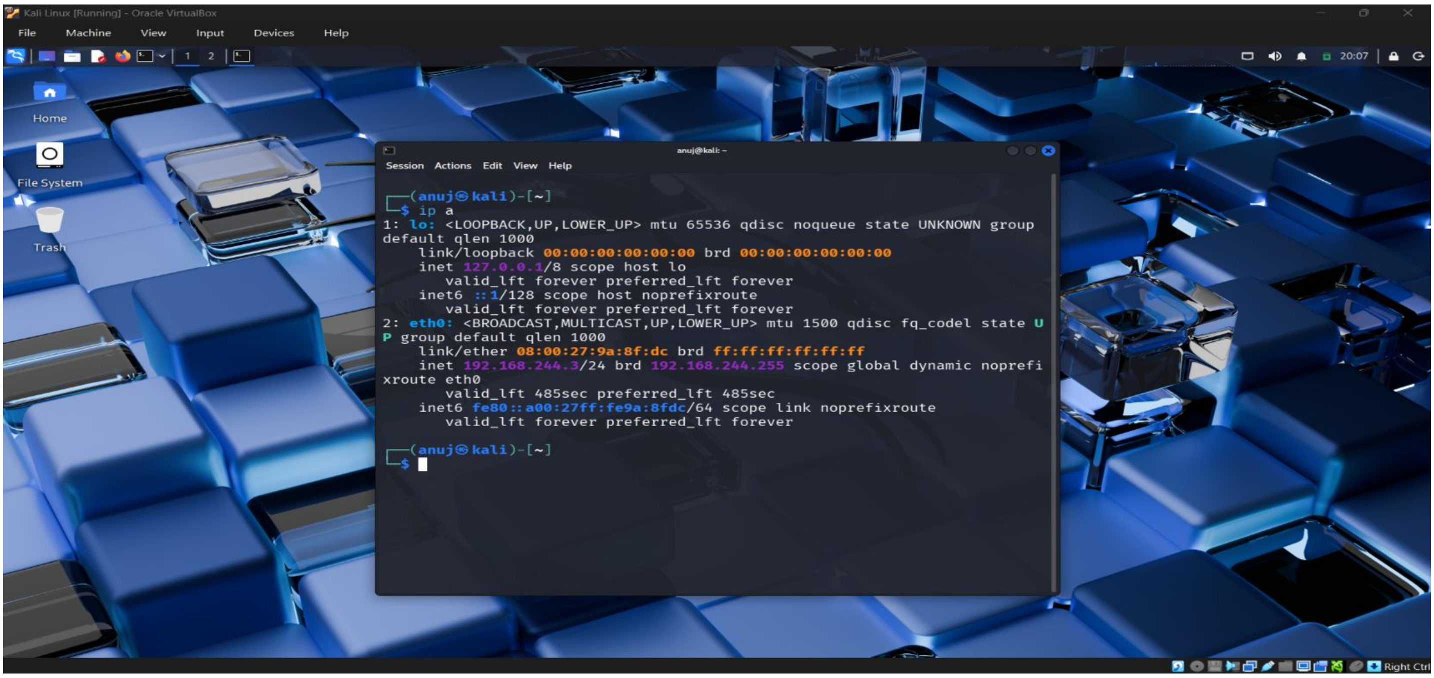
Port Number: COM1 IRQ: 4 I/O Port: 0x3F8

---

3. Lab Verification

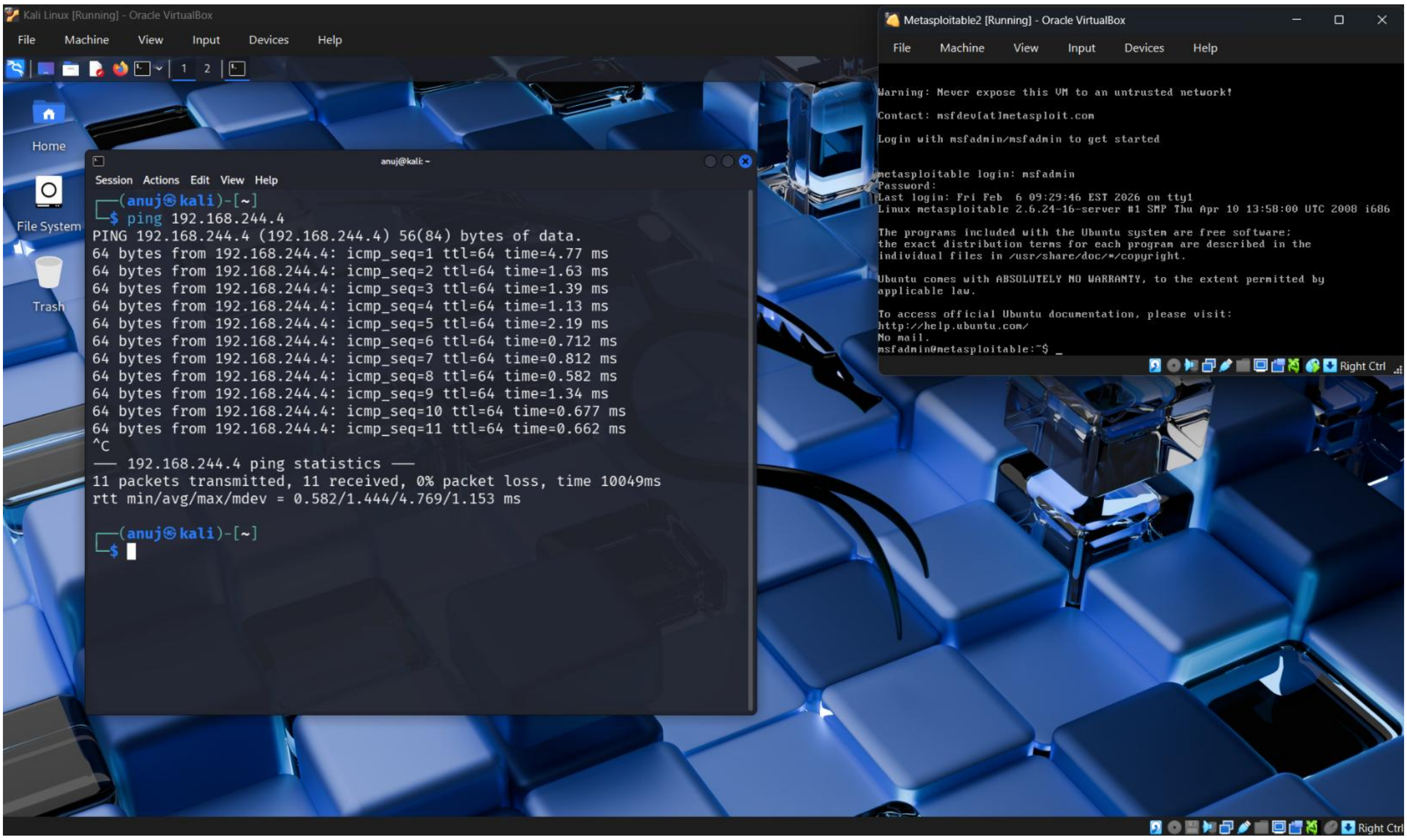
The lab setup was verified using the following steps:

- Checked IP addresses using ifconfig / ip a.



```
┌──(anuj㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state U
P group default qlen 1000
    link/ether 08:00:27:9a:8f:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.244.3/24 brd 192.168.244.255 scope global dynamic noprefi
xroute eth0
       valid_lft 485sec preferred_lft 485sec
    inet6 fe80::a00:27ff:fe9a:8fdc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(anuj㉿kali)-[~]
└─$ 
```

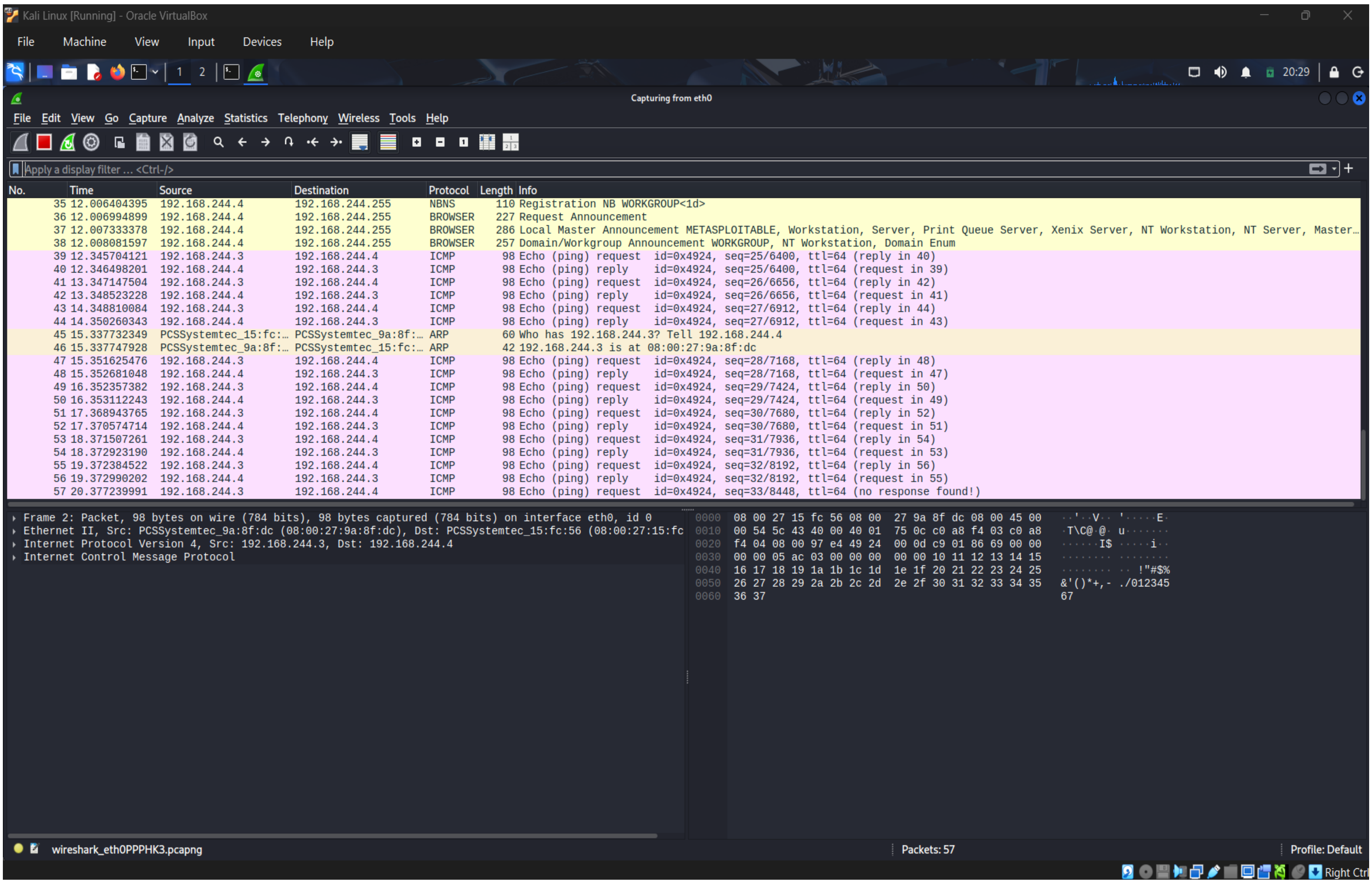
- Verified connectivity between machines using ping.


Kali Linux [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Home
File System
Trash
anuj@kali: ~
Session Actions Edit View Help
Metasploitable2 [Running] - Oracle VirtualBox
Right Ctrl

```
┌──(anuj㉿kali)-[~]
└─$ ping 192.168.244.4
PING 192.168.244.4 (192.168.244.4) 56(84) bytes of data.
64 bytes from 192.168.244.4: icmp_seq=1 ttl=64 time=4.77 ms
64 bytes from 192.168.244.4: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 192.168.244.4: icmp_seq=3 ttl=64 time=1.39 ms
64 bytes from 192.168.244.4: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 192.168.244.4: icmp_seq=5 ttl=64 time=2.19 ms
64 bytes from 192.168.244.4: icmp_seq=6 ttl=64 time=0.712 ms
64 bytes from 192.168.244.4: icmp_seq=7 ttl=64 time=0.812 ms
64 bytes from 192.168.244.4: icmp_seq=8 ttl=64 time=0.582 ms
64 bytes from 192.168.244.4: icmp_seq=9 ttl=64 time=1.34 ms
64 bytes from 192.168.244.4: icmp_seq=10 ttl=64 time=0.677 ms
64 bytes from 192.168.244.4: icmp_seq=11 ttl=64 time=0.662 ms
^C
--- 192.168.244.4 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10049ms
rtt min/avg/max/mdev = 0.582/1.444/4.769/1.153 ms

┌──(anuj㉿kali)-[~]
└─$ 
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Feb  6 09:29:46 EST 2026 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$ _
```

4. Wireshark Packet Capture


Kali Linux [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
20:29
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_eth0PPPHK3.pcapng
Packets: 57
Profile: Default
Right Ctrl

```
No.   Time         Source                Destination           Protocol  Length Info
   35 12.006404395 192.168.244.4         192.168.244.255       NBNS      110 Registration NB WORKGROUP<1d>
   36 12.006994899 192.168.244.4         192.168.244.255       BROWSER   227 Request Announcement
   37 12.007333378 192.168.244.4         192.168.244.255       BROWSER   286 Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master…
   38 12.008081597 192.168.244.4         192.168.244.255       BROWSER   257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
   39 12.345704121 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=25/6400, ttl=64 (reply in 40)
   40 12.346498201 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=25/6400, ttl=64 (request in 39)
   41 13.347147504 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=26/6656, ttl=64 (reply in 42)
   42 13.348523228 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=26/6656, ttl=64 (request in 41)
   43 14.348810084 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=27/6912, ttl=64 (reply in 44)
   44 14.350260343 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=27/6912, ttl=64 (request in 43)
   45 15.337732349 PCSSystemtec_15:fc:… PCSSystemtec_9a:8f:… ARP        60 Who has 192.168.244.3? Tell 192.168.244.4
   46 15.337747928 PCSSystemtec_9a:8f:… PCSSystemtec_15:fc:… ARP        42 192.168.244.3 is at 08:00:27:9a:8f:dc
   47 15.351625476 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=28/7168, ttl=64 (reply in 48)
   48 15.352681048 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=28/7168, ttl=64 (request in 47)
   49 16.352357382 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=29/7424, ttl=64 (reply in 50)
   50 16.353112243 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=29/7424, ttl=64 (request in 49)
   51 17.368943765 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=30/7680, ttl=64 (reply in 52)
   52 17.370574714 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=30/7680, ttl=64 (request in 51)
   53 18.371507261 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=31/7936, ttl=64 (reply in 54)
   54 18.372923190 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=31/7936, ttl=64 (request in 53)
   55 19.372384522 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=32/8192, ttl=64 (reply in 56)
   56 19.372990202 192.168.244.4         192.168.244.3         ICMP       98 Echo (ping) reply    id=0x4924, seq=32/8192, ttl=64 (request in 55)
   57 20.377239991 192.168.244.3         192.168.244.4         ICMP       98 Echo (ping) request  id=0x4924, seq=33/8448, ttl=64 (no response found!)
```

```
› Frame 2: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_9a:8f:dc (08:00:27:9a:8f:dc), Dst: PCSSystemtec_15:fc:56 (08:00:27:15:fc
› Internet Protocol Version 4, Src: 192.168.244.3, Dst: 192.168.244.4
› Internet Control Message Protocol
```

```
0000  08 00 27 15 fc 56 08 00  27 9a 8f dc 08 00 45 00   ··'··V·· '·····E·
0010  00 54 5c 43 40 00 40 01  75 0c c0 a8 f4 03 c0 a8   ·T\C@·@· u·······
0020  f4 04 08 00 97 e4 49 24  00 0d c9 01 86 69 00 00   ······I$ ·····i··
0030  00 00 05 ac 03 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

4.1 Tool Description

Wireshark is a network protocol analyser used to capture and analyse packets transmitted over a network interface.

4.2 Packet Capture Procedure

- Wireshark was launched on Kali Linux.
- Active network interface was selected.
- ICMP traffic was generated using ping commands.
- Packets were captured and observed in real time.

4.3 Observations

- ICMP Echo Request and Echo Reply packets were identified.
- Source and destination IP addresses were analysed.
- Packet details such as protocol type and sequence were observed.

---

5. Tools Used

- Oracle VirtualBox
- Kali Linux
- Metasploitable2
- Wireshark

---

6. Conclusion

Task 1 was successfully completed by setting up a functional ethical hacking lab and capturing network traffic using Wireshark. The lab environment is ready for further security testing tasks in subsequent phases of the internship.
