

LAB SETUP & NETWORK CONFIGURATION REPORT

Prepared by: Chennari Mohammed Idris

Date: February 21, 2026

Project: Task 1 - Foundation & Environment Setup

1. Introduction

The objective of this task was to establish a secure, isolated virtualization environment for penetration testing and network analysis. The lab consists of an **Attacker machine (Kali Linux)** and a **Vulnerable Target (Metasploitable2)**, connected via a private virtual network.

2. Environment Specifications

- **Virtualization Software:** Oracle VM VirtualBox
- **Attacker VM:** Kali Linux 2024.x (Debian-based)
- **Target VM:** Metasploitable2 (Linux-based)
- **Network Strategy:** Host-Only Adapter (to ensure isolation from the public internet).

3. Implementation Steps

3.1 Virtual Machine Deployment

I successfully imported the Metasploitable2 virtual disk (.vmdk) and configured the system settings.

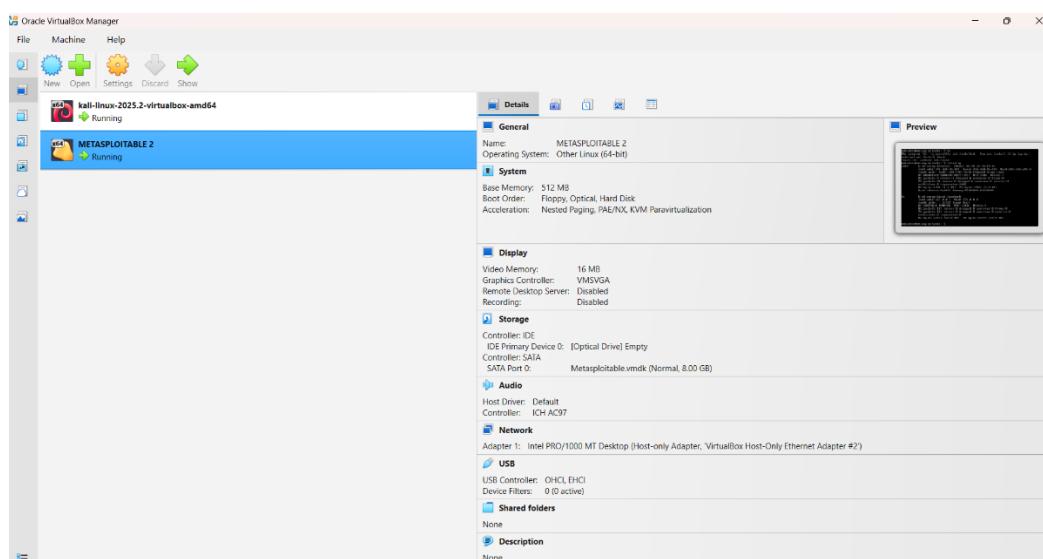


Image 1: Virtual Box with Both VMs running Screenshot

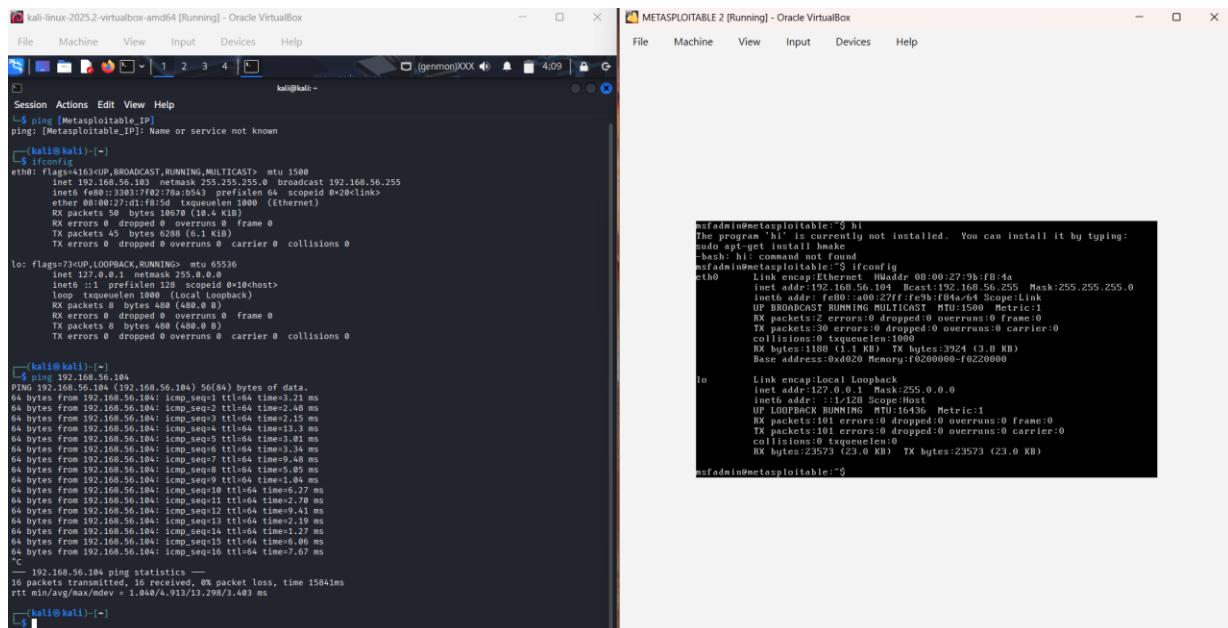
3.2 Network Configuration

To allow the machines to communicate while remaining isolated, I configured both VMs to use a **Host-Only Adapter**.

- **Kali Linux IP:** 192.168.56.103
- **Metasploitable IP:** 192.168.56.104

3.3 Connectivity Testing

I performed a connectivity test using the ping command from the Kali terminal to verify that the target machine was reachable.



The screenshot shows two terminal windows side-by-side. The left window is titled 'kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox' and the right window is titled 'METASPOITABLE 2 [Running] - Oracle VirtualBox'. Both windows have a standard Linux terminal interface with a black background and white text. The left terminal shows the output of a ping command from Kali Linux to Metasploitable's IP address (192.168.56.104). The right terminal shows the output of a ping command from Metasploitable to Kali Linux's IP address (192.168.56.103). Both pings were successful, with no errors reported.

```
kali@kali:~$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=3.21 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=2.48 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=64 time=2.48 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=64 time=3.33 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=64 time=3.01 ms
64 bytes from 192.168.56.104: icmp_seq=6 ttl=64 time=2.48 ms
64 bytes from 192.168.56.104: icmp_seq=7 ttl=64 time=9.48 ms
64 bytes from 192.168.56.104: icmp_seq=8 ttl=64 time=5.05 ms
64 bytes from 192.168.56.104: icmp_seq=9 ttl=64 time=1.04 ms
64 bytes from 192.168.56.104: icmp_seq=10 ttl=64 time=1.07 ms
64 bytes from 192.168.56.104: icmp_seq=11 ttl=64 time=2.70 ms
64 bytes from 192.168.56.104: icmp_seq=12 ttl=64 time=9.41 ms
64 bytes from 192.168.56.104: icmp_seq=13 ttl=64 time=2.19 ms
64 bytes from 192.168.56.104: icmp_seq=14 ttl=64 time=2.15 ms
64 bytes from 192.168.56.104: icmp_seq=15 ttl=64 time=0.06 ms
64 bytes from 192.168.56.104: icmp_seq=16 ttl=64 time=7.07 ms
```
C```
- 192.168.56.104 ping statistics --
16 packets transmitted, 16 received, 0% packet loss, time 15841ms
rtt min/avg/max/mdev = 1.040/4.913/13.298/3.483 ms
```
kali@kali:~$ ```

metadmin@metasploitable:~$ hi
hi: command not found
metadmin@metasploitable:~$ h
You have to install the 'hi' package. You can install it by typing:
sudo apt-get install hi
metadmin@metasploitable:~$ ifconfig
Link encap:Ethernet HWaddr 08:00:00:9b:f0:4a
inet addr:192.168.56.104 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::a00:9bff:fe9b:f04a/64 Scope:Link
UP BROADCAST NOARP MTU:1500 Metric:1
RX packets:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:12 errors:0 dropped:0 overruns:0 frame:0
TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
collisions:10 txqueuelen:1000
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)
Base address:0x6c20 Memory:f0200000-f0220000
```
metadmin@metasploitable:~$ ```

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: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)
```
metadmin@metasploitable:~$ ```


```

Image 2: Successful Ping results Screenshot

4. Traffic Analysis (Wireshark)

To verify the flow of data at the Network Layer, I used **Wireshark** to capture packets on the eth0 interface. I filtered for **ICMP** protocol to isolate the ping traffic.

- **Observation:** The capture confirmed four (4) Echo Requests and four (4) Echo Replies.
- **Result:** This proves that the virtual switch is correctly routing traffic between the two nodes.

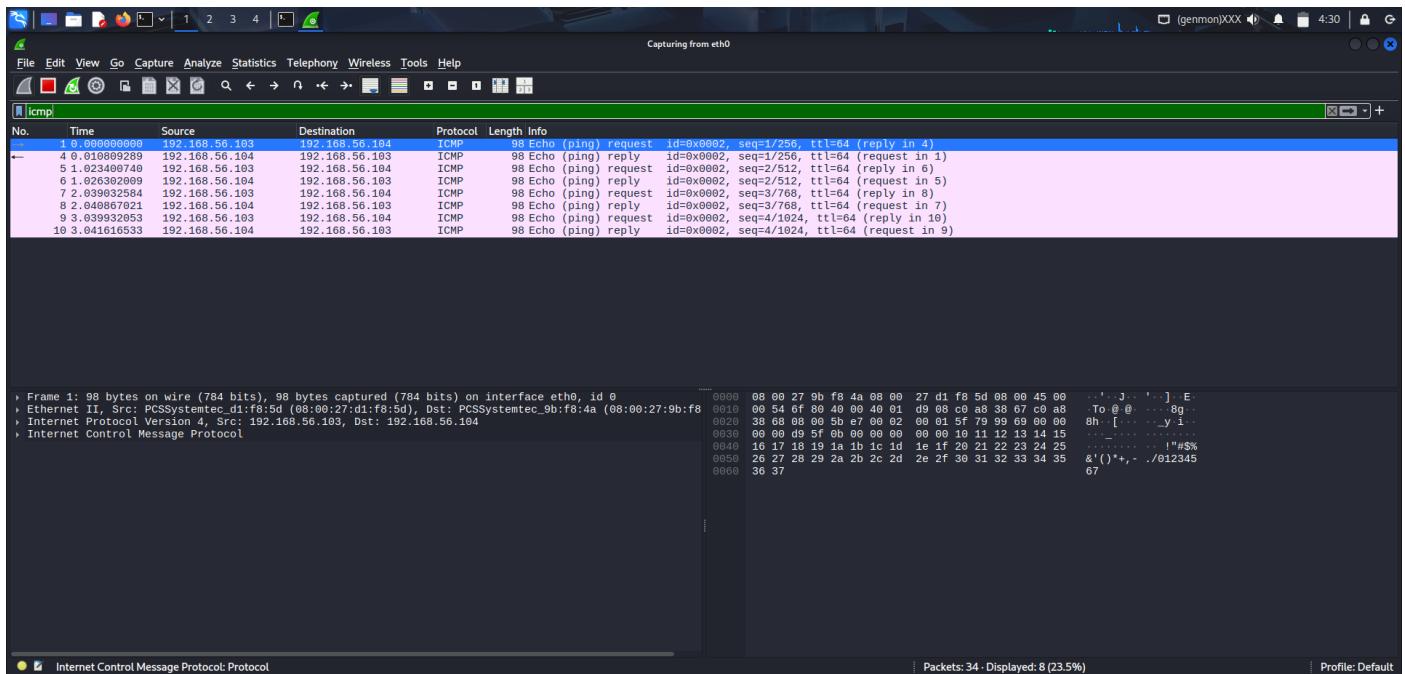


Image 3: Wireshark test capture Screenshot

5. Documentation & Resources

As part of this task, I developed a centralized documentation system on GitHub. This repository includes:

- **Linux Cheat Sheet:** A searchable guide for common commands.
- **Lab Notes:** Technical details for future reference.

6. Conclusion

Task 1 was completed successfully. The lab is fully functional, isolated, and ready for the next phase of the internship: **Network Security & Scanning**.