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.

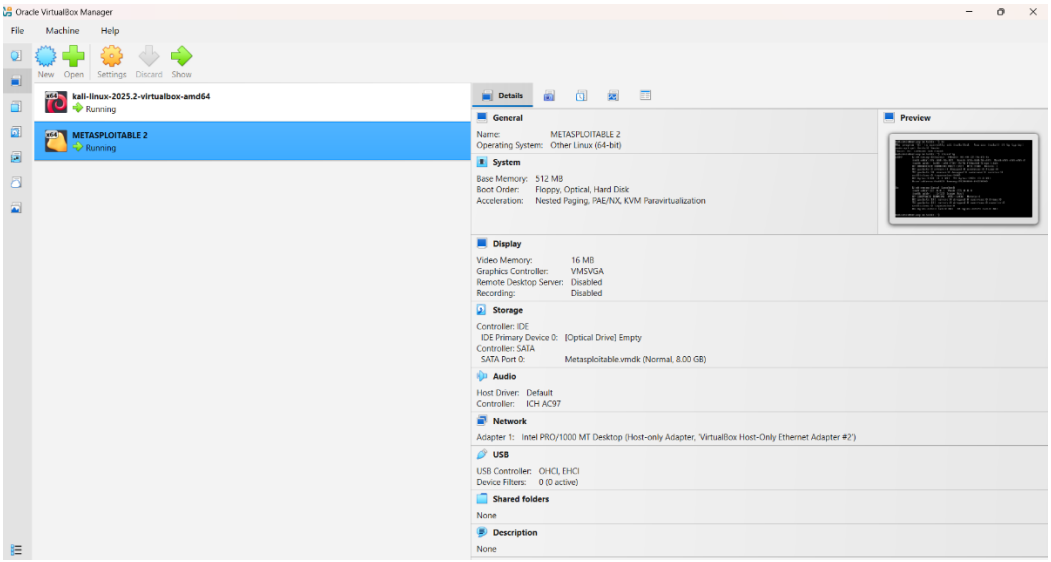

Image 1: Virtual Box with Both VMs running Screenshot

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.

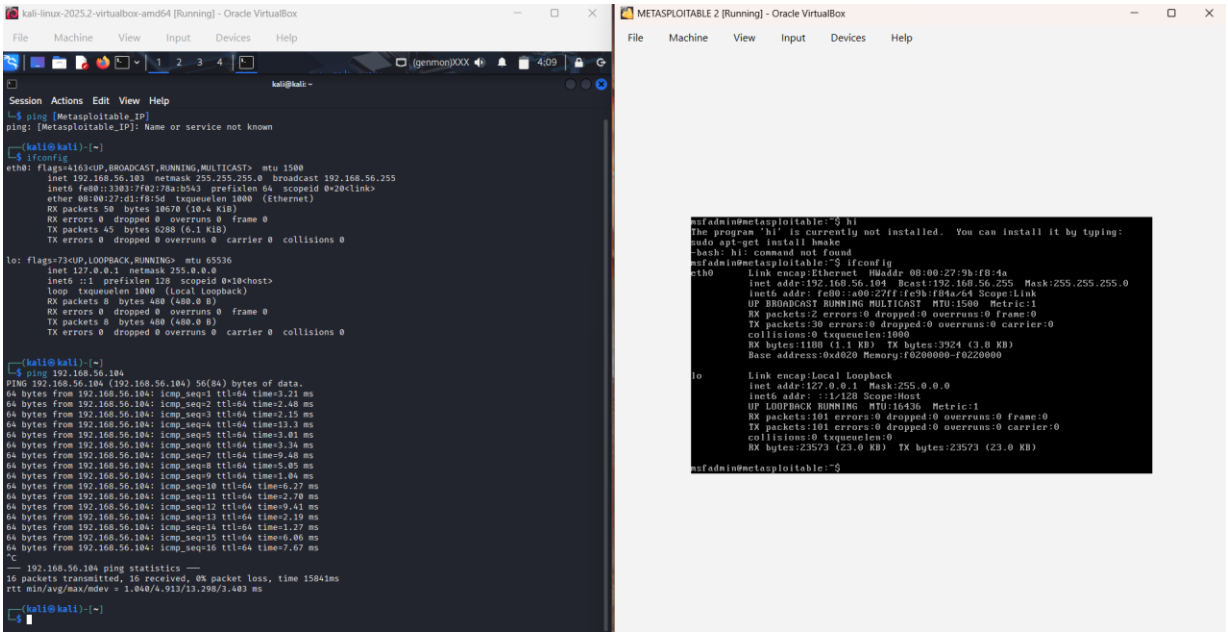

Image 2: Successful Ping results Screenshot

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.

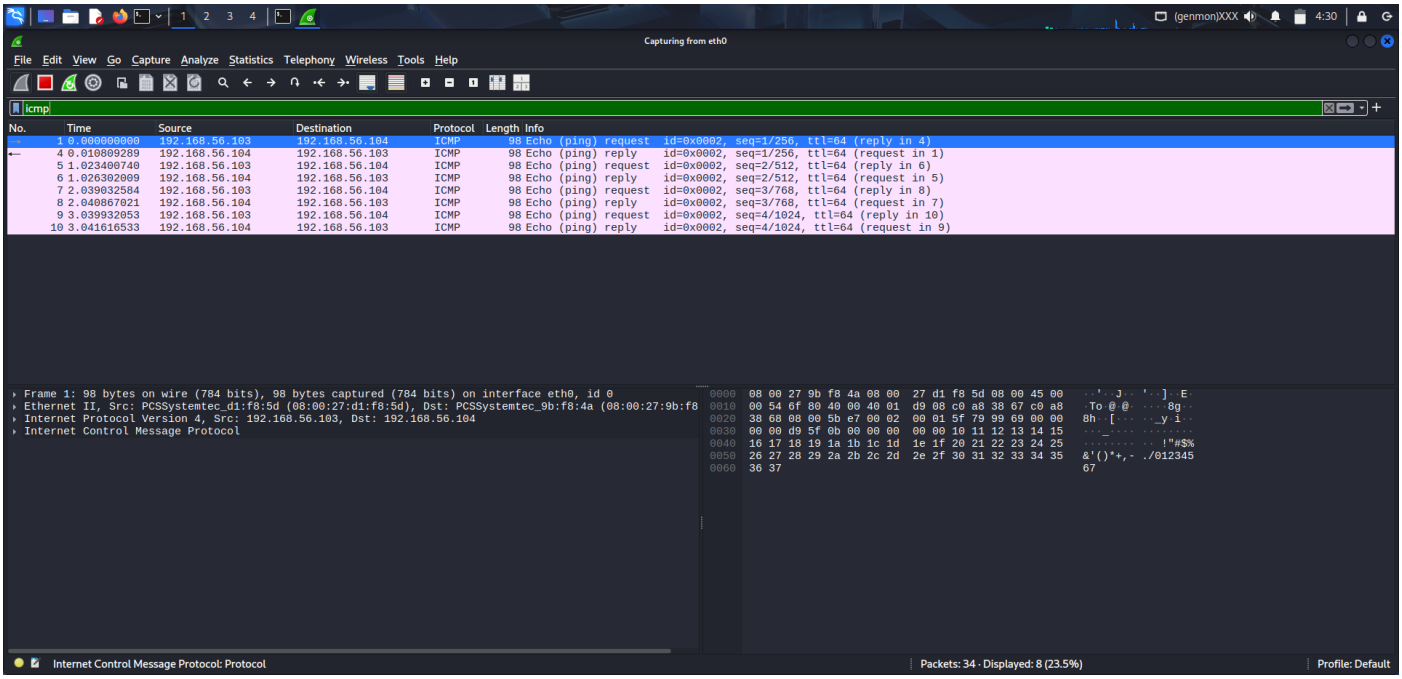

Image 3: Wireshark test capture Screenshot

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.**