Cybersecurity Lab Report
Foundation & Environment Setup

Objective

The objective of this lab was to build strong fundamentals in cybersecurity including networking, cryptography, and Linux system operations. This task focused on setting up a professional virtual lab environment using VirtualBox, configuring Kali Linux as the attacker machine and Metasploitable as the target machine, and establishing secure network communication between them.

The lab aimed to provide hands-on experience with essential cybersecurity tools such as Nmap, Wireshark, Burp Suite, OpenSSL, and Netcat. Through this setup, practical understanding of concepts like IP addressing, packet capture, port scanning, hashing algorithms, and HTTP interception was developed.

Lab Environment Setup

For this task, a virtual cybersecurity lab environment was created using Oracle VirtualBox. Two virtual machines were configured to simulate a real-world penetration testing scenario.

The following machines were used:

• Kali Linux – Attacker Machine
• Metasploitable 2 – Target Machine

Both virtual machines were configured using the Host-Only Network Adapter in VirtualBox. This allowed secure communication between the two systems within an isolated virtual network environment.

Kali Linux was used to perform security testing and run tools such as Nmap, Wireshark, Burp Suite, OpenSSL, and Netcat. Metasploitable was used as a vulnerable target system to test connectivity and security tools.

The virtual machines were successfully powered on and verified before proceeding with network configuration and testing.

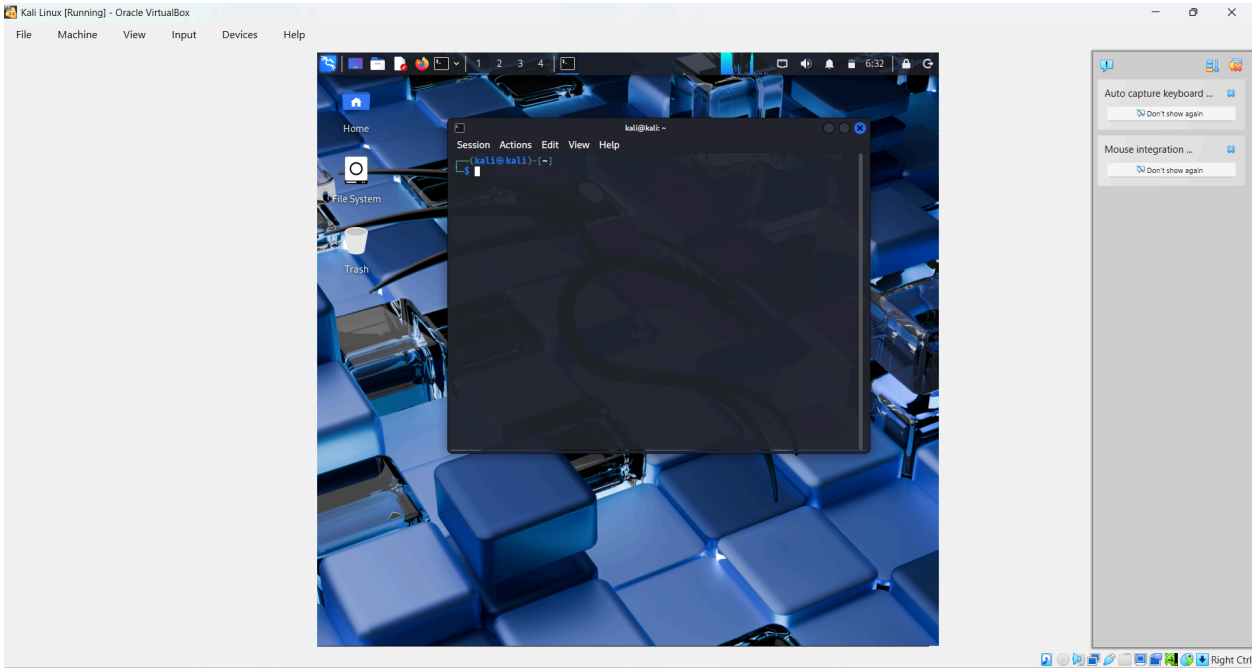

Fig 1 : Kali Linux Running

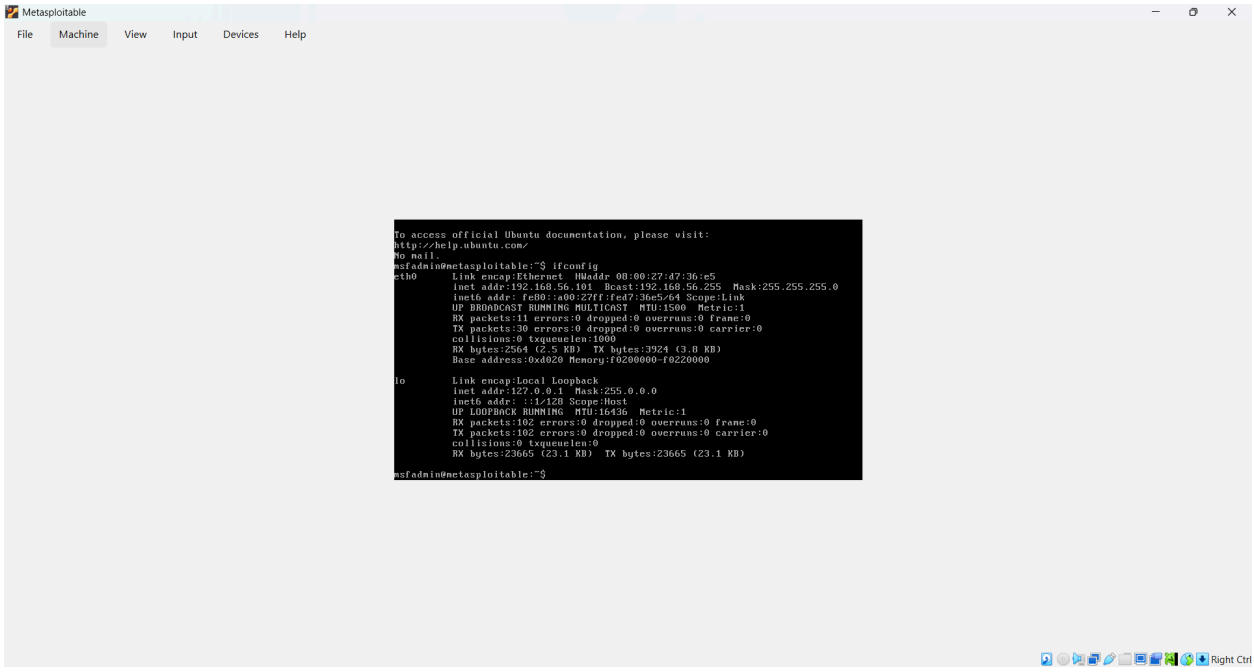

Fig 2 : Metasploitable Running

Network Configuration

After setting up the virtual machines, network configuration was verified to ensure proper communication between Kali Linux and Metasploitable.

The `ifconfig` command was used on both systems to check their IP addresses.

The assigned IP addresses were:

• Kali Linux IP Address: 192.168.56.102
• Metasploitable IP Address: 192.168.56.101

Both machines were connected using the Host-Only Network Adapter, which allowed them to communicate within the same virtual network.

To verify connectivity, a ping test was performed from Kali Linux to Metasploitable using the following command:

```
ping 192.168.56.101
```

The successful ping response confirmed that network communication between the two virtual machines was properly established.

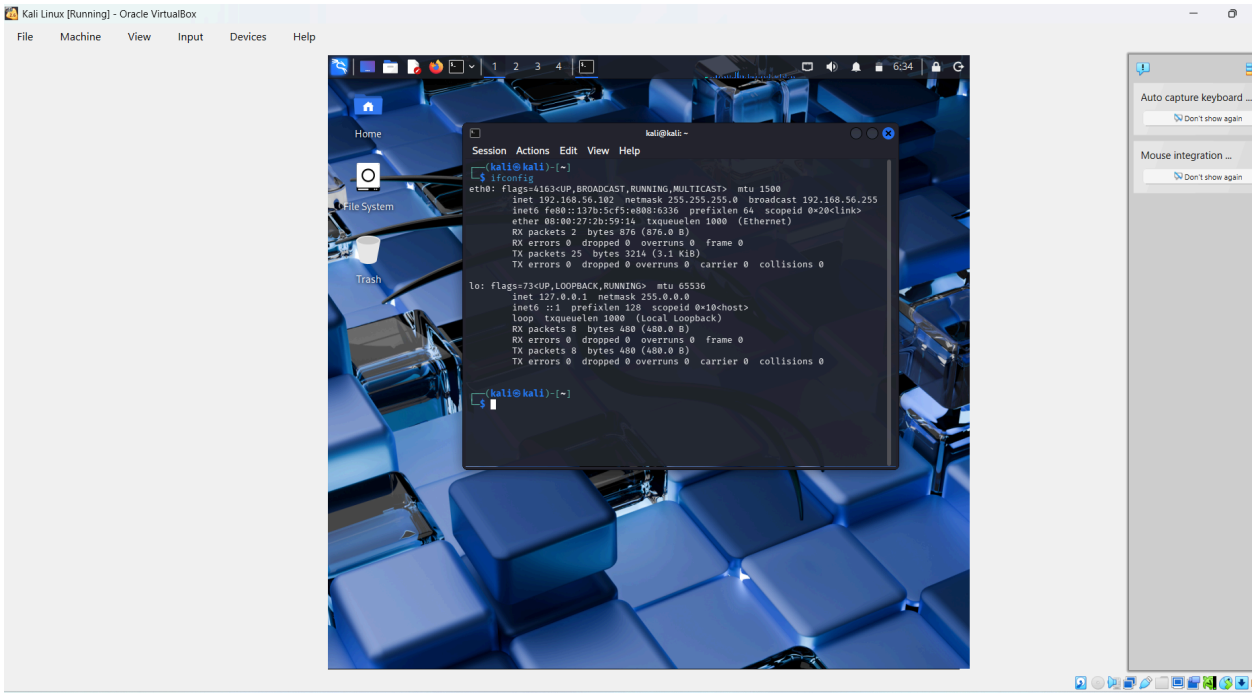

Fig 3 : ifconfig output (showing IP addresses)

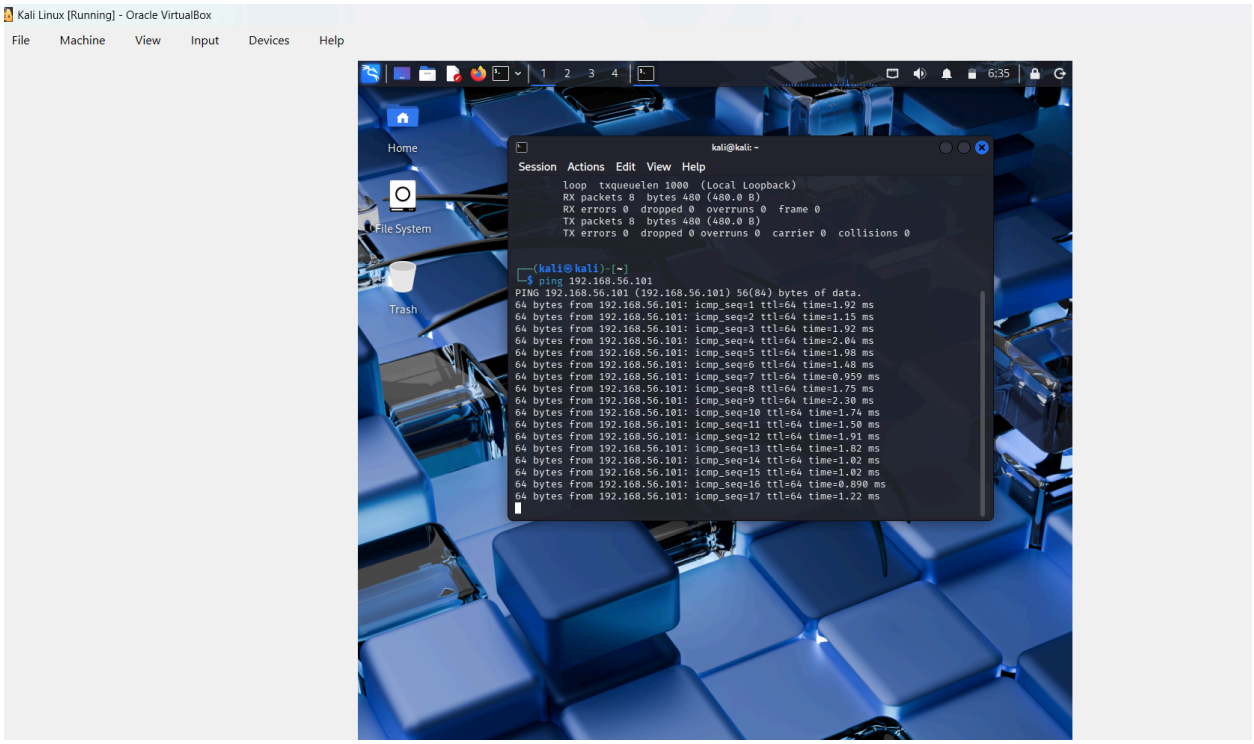

Fig 4 : Successful Ping Test

Linux Fundamentals Practice

Basic Linux commands were practiced in Kali Linux to understand file system navigation and system operations.

The following commands were executed:

- `pwd` – Displays the current working directory
- `ls` – Lists files and directories
- `mkdir` – Creates a new directory
- `cd` – Changes the current directory
- `touch` – Creates a new file
- `chmod` – Changes file permissions

These commands helped in understanding how Linux manages files, directories, and permissions. Practicing these commands is essential for performing cybersecurity tasks efficiently, as most security tools operate in a Linux environment.

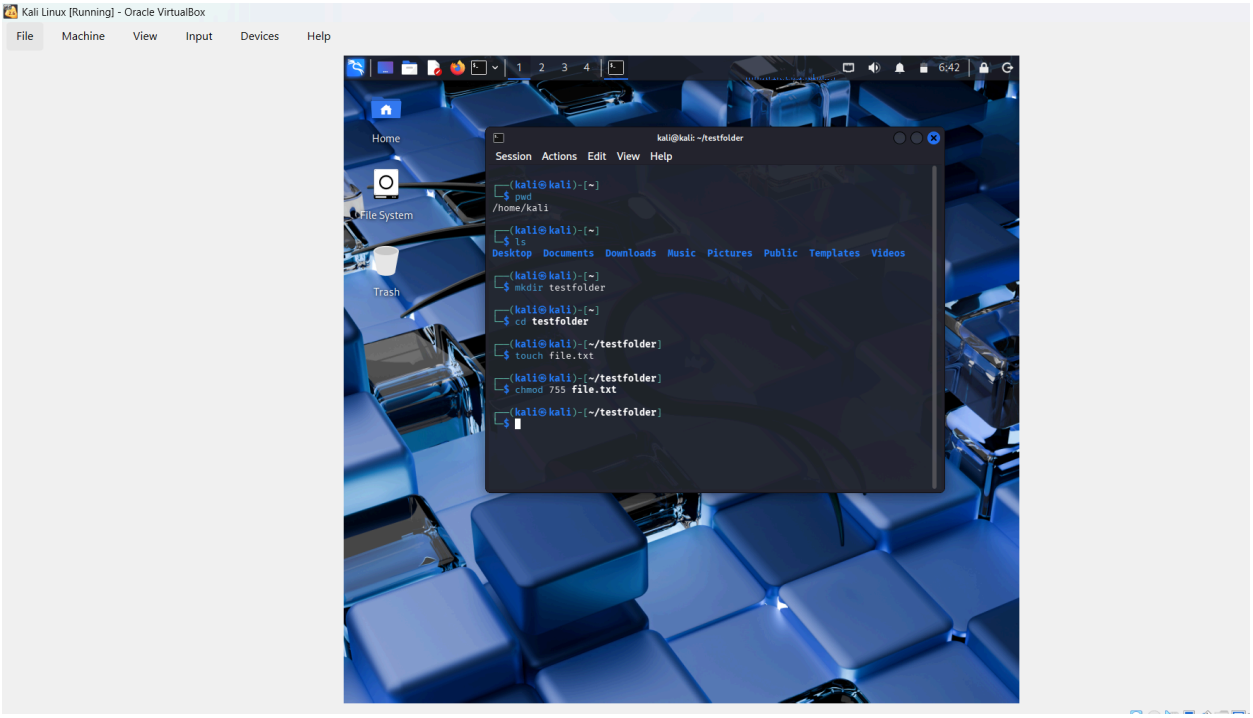

Fig 5 : Linux Commands Execution

Nmap Port Scanning

Nmap (Network Mapper) is a powerful network scanning tool used to discover open ports and services running on a target machine.

In this lab, Nmap was used from Kali Linux to scan the Metasploitable machine using the following command:

```
nmap 192.168.56.101
```

The scan successfully identified multiple open ports and running services on the target system. This demonstrates how Nmap can be used to gather information about a system before performing further security testing.

Port scanning is an important step in cybersecurity because it helps identify potential entry points and vulnerabilities within a networked system.

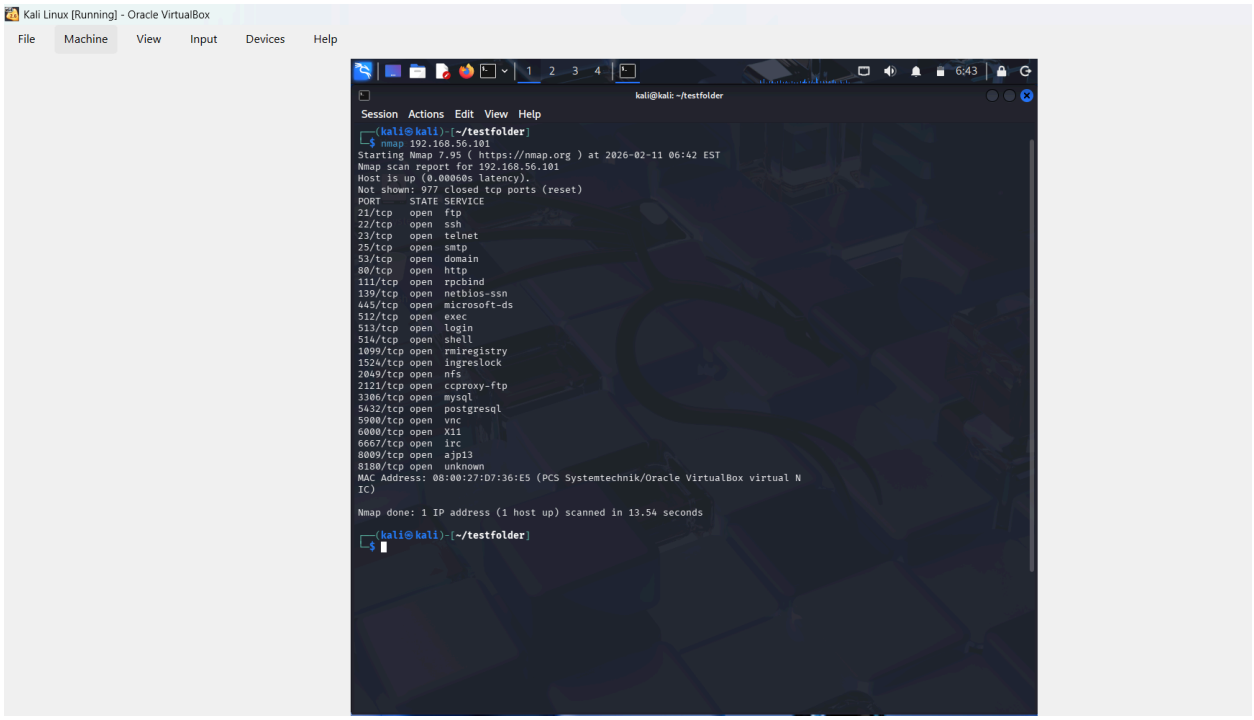

Fig 6 : Nmap Scan Result Showing Open Ports

Wireshark Packet Capture

Wireshark is a network protocol analyzer used to monitor and capture network traffic in real time.

In this lab, Wireshark was used on Kali Linux to capture packets exchanged between Kali Linux and Metasploitable during the ping test. The capture showed ICMP (Internet Control Message Protocol) packets, which are generated when using the ping command.

By analyzing the captured packets, it was possible to observe source IP address, destination IP address, protocol type, and packet details. This demonstrates how Wireshark can be used to monitor and analyze network communication for troubleshooting and security analysis.

Packet capturing is an essential skill in cybersecurity as it helps in detecting suspicious traffic and understanding how data travels across a network.

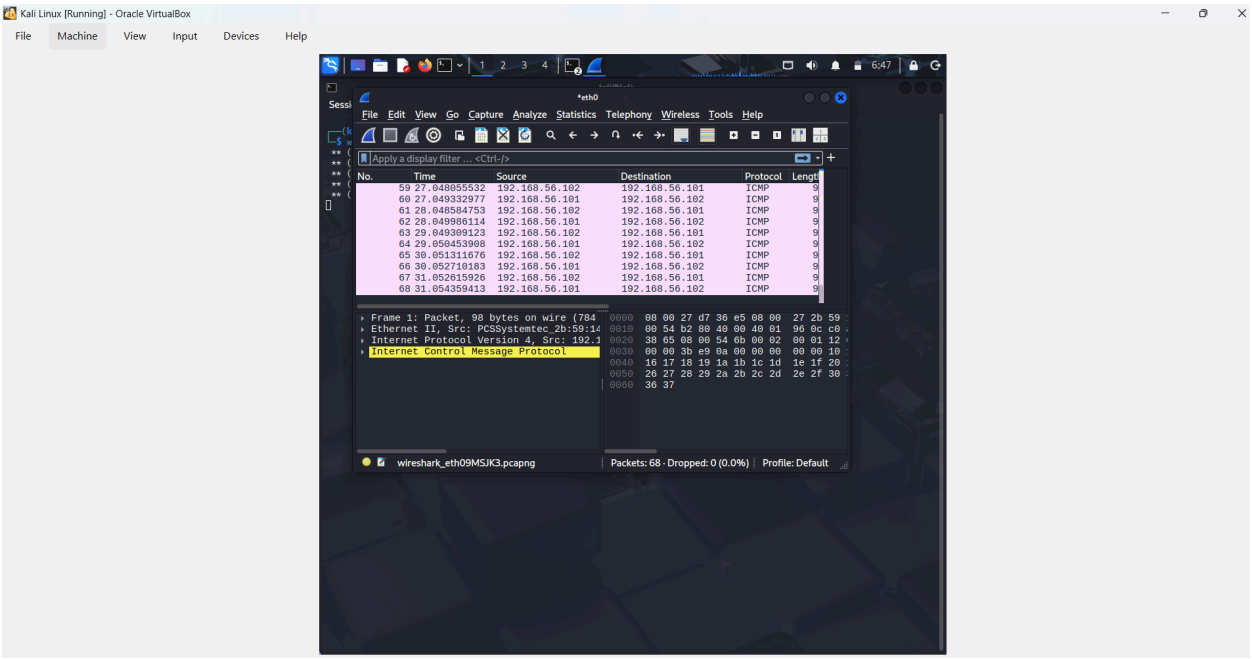

Fig 7 : Wireshark Showing ICMP Packet Capture

Cryptography Practice (Hash Generation)

Cryptography is a fundamental concept in cybersecurity used to protect data confidentiality and integrity. In this lab, hashing techniques were practiced using OpenSSL in Kali Linux.

The following commands were executed:

```
echo "cyberlab" | openssl dgst -md5
 echo "cyberlab" | openssl dgst -sha256
```

The MD5 and SHA256 algorithms were used to generate hash values of a sample text. A hash function converts input data into a fixed-length string and is a one-way function, meaning the original data cannot be easily retrieved from the hash.

Hashing is commonly used for password storage, file integrity verification, and digital signatures.

This activity helped in understanding the practical implementation of cryptographic hashing techniques.

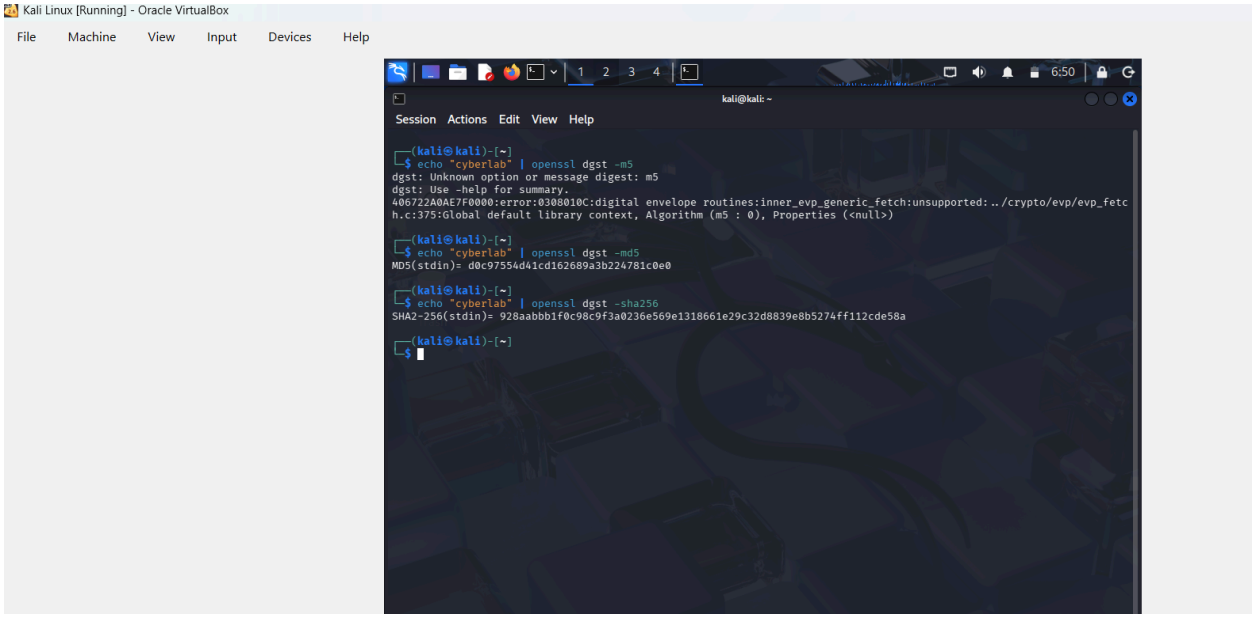

Fig 8 : MD5 and SHA256 Hash Output

Burp Suite – HTTP Interception

Burp Suite is a web application security testing tool used to intercept, inspect, and analyze HTTP/HTTPS traffic between a browser and a web server.

In this lab, Burp Suite was launched on Kali Linux and configured to intercept web traffic. While accessing the DVWA (Damn Vulnerable Web Application) page hosted on the Metasploitable machine, the HTTP request was successfully captured using the Proxy → Intercept feature.

The intercepted request displayed important details such as:

• HTTP method (GET request)
• Host IP address
• Requested resource path
• HTTP headers

This demonstrated how web requests can be monitored and analyzed during security testing. HTTP interception is an important step in web application security assessment.

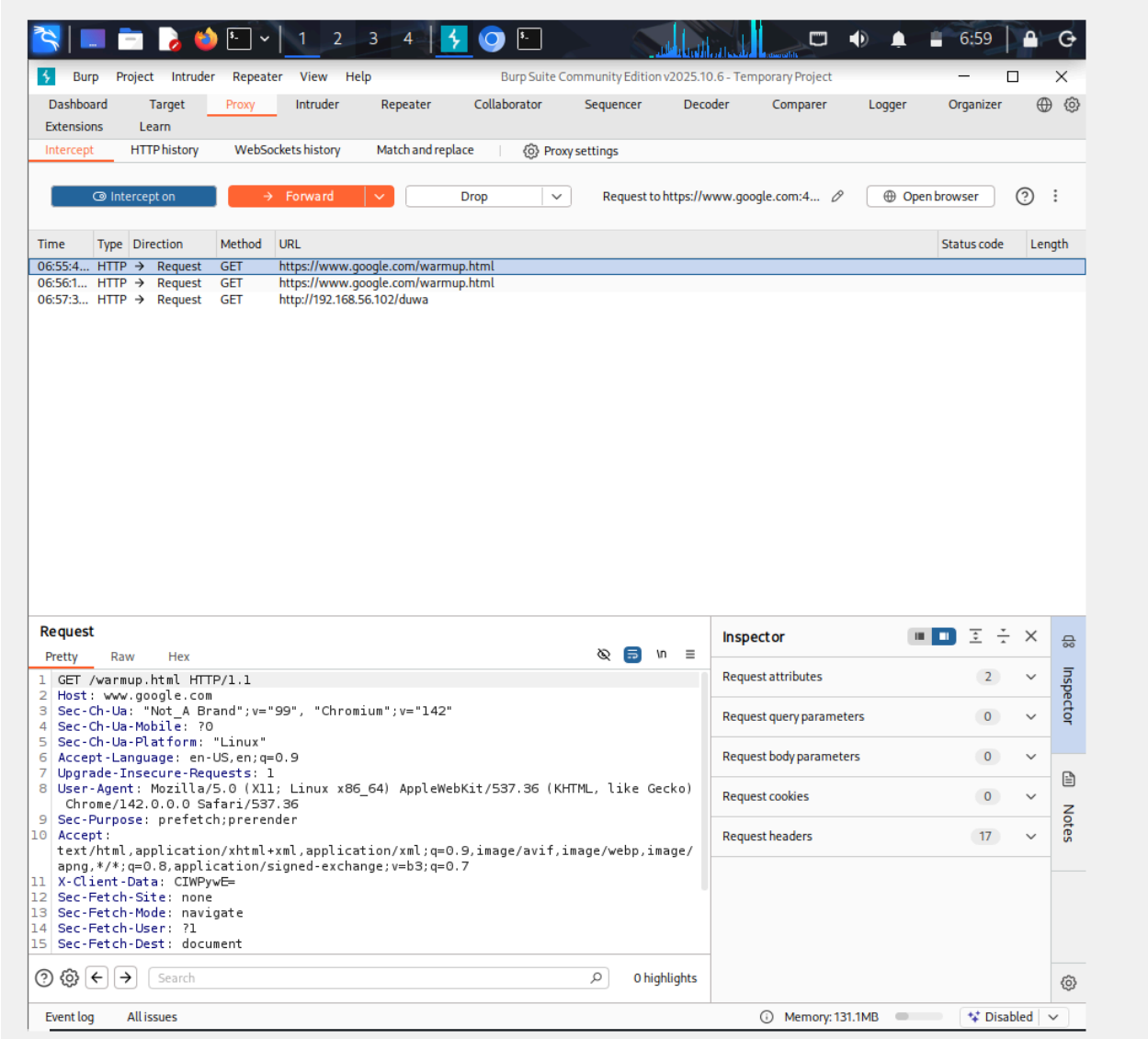

Fig 9 : Burp Suite Showing Intercepted HTTP Request

Netcat – TCP Communication Test

Netcat is a networking utility tool used for reading and writing data across network connections using TCP or UDP protocols. It is often referred to as a “Swiss Army knife” for networking.

In this lab, Netcat was used to establish a TCP connection between Kali Linux and the Metasploitable machine.

First, Metasploitable was set to listen on port 4444 using the command:

```
nc -lvp 4444
```

Then, from Kali Linux, a connection was initiated using:

```
nc 192.168.56.101 4444
```

After the connection was successfully established, a test message was sent from Kali Linux and received on Metasploitable. This confirmed that TCP communication between both virtual machines was working correctly.

This activity demonstrated how network communication can be manually established and tested using Netcat, which is useful in penetration testing and troubleshooting scenarios.

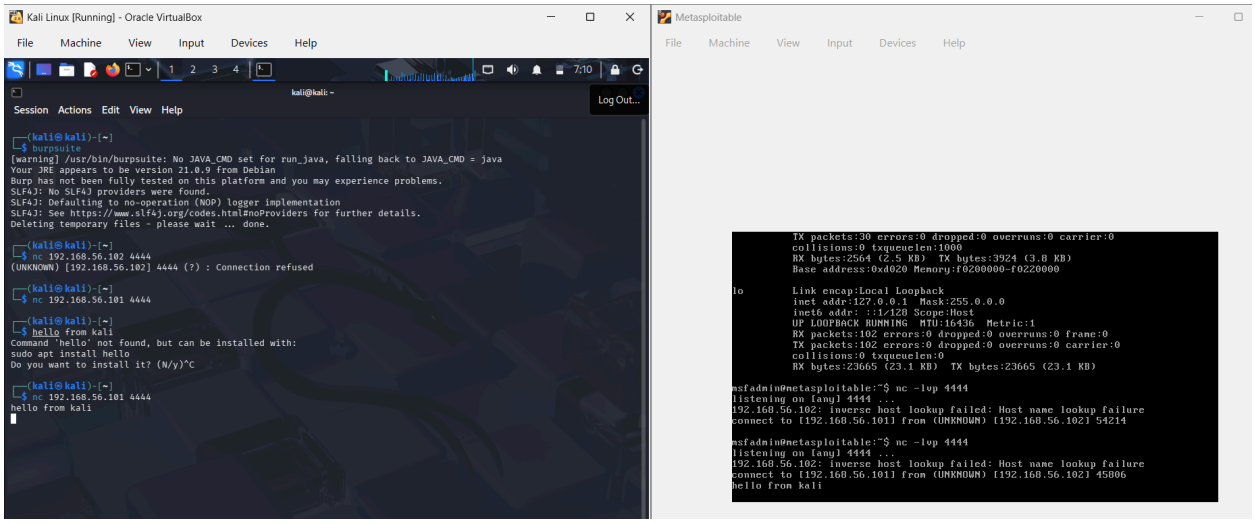

Fig 10 : Netcat Connection Established Between Kali and Metasploitable

Conclusion

This lab successfully demonstrated the setup of a cybersecurity testing environment using VirtualBox. Kali Linux was configured as the attacker machine and Metasploitable was configured as the target machine using a Host-Only network to ensure secure internal communication.

Network connectivity was verified using the ping command, and IP addresses were confirmed using ifconfig. Various cybersecurity tools were practiced, including Nmap for port scanning, Wireshark for packet capture, OpenSSL for hash generation, Burp Suite for HTTP interception, and Netcat for TCP communication testing.

Through this hands-on practice, a strong foundational understanding of networking, Linux commands, cryptography, and basic security tool usage was developed. The lab environment was successfully configured and tested, meeting all the objectives of the task.