Introduction

Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access, cyber attacks, and potential threats. It ensures the core principles of the CIA Triad: **Confidentiality, Integrity, and Availability**, which are essential for maintaining secure and reliable information systems.

Lab Setup

In this task, a controlled cybersecurity lab environment was established using Oracle VirtualBox. **Kali Linux** was configured as the attacker machine, and **Metasploitable2** was deployed as the vulnerable target machine. Both systems were connected using a **Host-Only network**, allowing safe and isolated testing of security tools and techniques without affecting external networks.

Networking Basics

The **OSI (Open Systems Interconnection) Model** consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application, each responsible for specific communication functions. The **TCP/IP model** includes four layers: Network Access, Internet, Transport, and Application, and is widely used in real-world networking. The **Domain Name System (DNS)** translates domain names into IP addresses, enabling communication between devices. **HTTP** is used for web communication, while **HTTPS** provides secure communication using **SSL/TLS encryption**. **Network Address Translation (NAT)** converts private IP addresses into public IP addresses for internet access.

Cryptography

Cryptography is used to secure information by converting it into an unreadable format. **Symmetric encryption** uses a single key for both encryption and decryption, whereas **asymmetric encryption** uses a pair of keys: a public key and a private key. **Hashing algorithms** such as MD5 and SHA-256 ensure data integrity by generating unique hash values. **SSL/TLS protocols** provide secure communication over networks by encrypting transmitted data and verifying digital certificates.

Tools Used

The following cybersecurity tools were utilized during this task:

- **Nmap** – for network scanning and service detection
- **Wireshark** – for packet capture and network traffic analysis
- **Netcat** – for network communication and debugging
- **OpenSSL** – for encryption and decryption of data

Practical Implementation

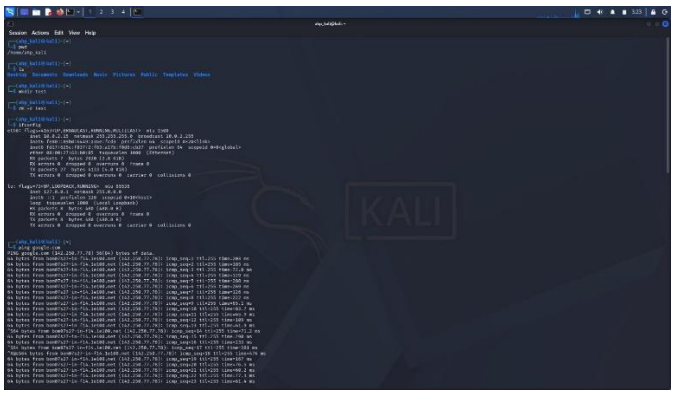
Practical experiments were conducted to verify network communication and demonstrate cybersecurity tools. Connectivity between Kali Linux and Metasploitable2 was confirmed using the **ping command**. The **Nmap tool** was used to scan open ports and identify running services on the target machine. **Wireshark** was utilized to capture and analyze ICMP packets generated during network communication. Additionally, **OpenSSL** was used to successfully encrypt and decrypt a sample message, demonstrating basic cryptographic operations.

Conclusion

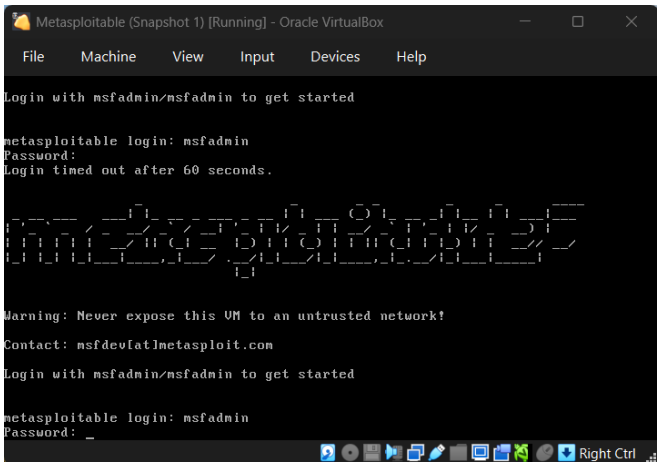
This task provided a strong foundation in cybersecurity concepts, networking, and cryptography. It also offered hands-on experience in setting up a secure lab environment and using essential security tools for network analysis and encryption. The knowledge and skills gained from this task are fundamental for understanding real-world cybersecurity practices.

1.Kali Desktop

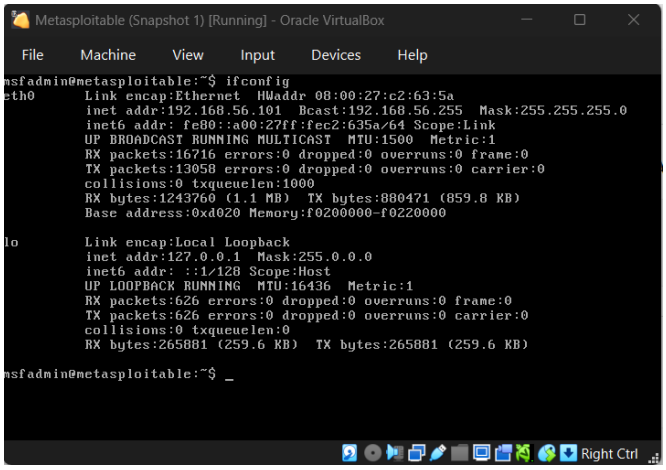
2. Basic commands



3. Metasploitable login



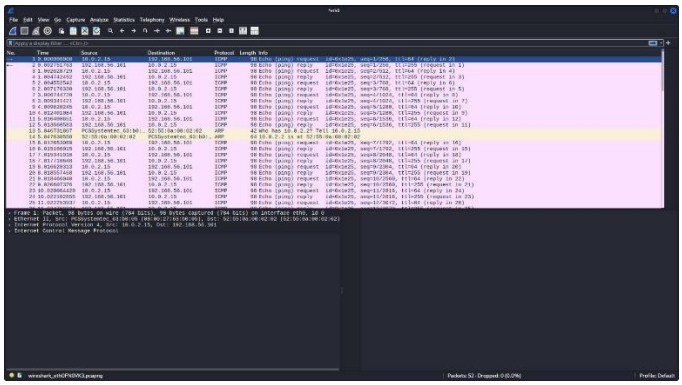
4. Metasploitable IP



5. Ping

6. Nmap

7. Wireshark



8.OpenSSL