

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.

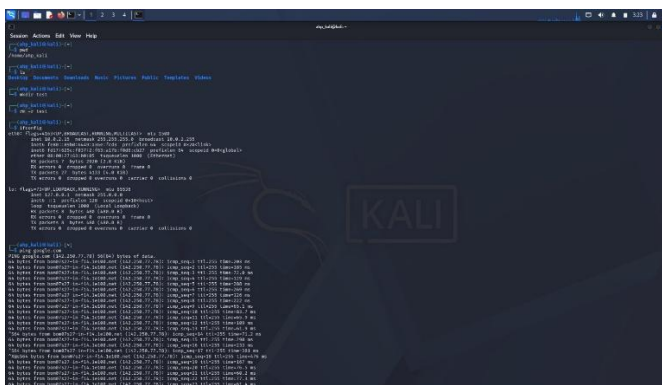
Conclusion

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.

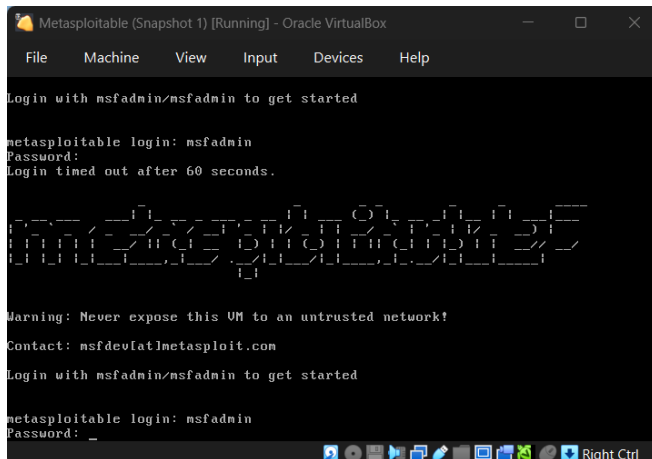
1.Kali Desktop



2. Basic commands



3. Metasploitable login



The screenshot shows a terminal window titled "Metasploitable (Snapshot 1) [Running] - Oracle VirtualBox". The terminal displays the following text:

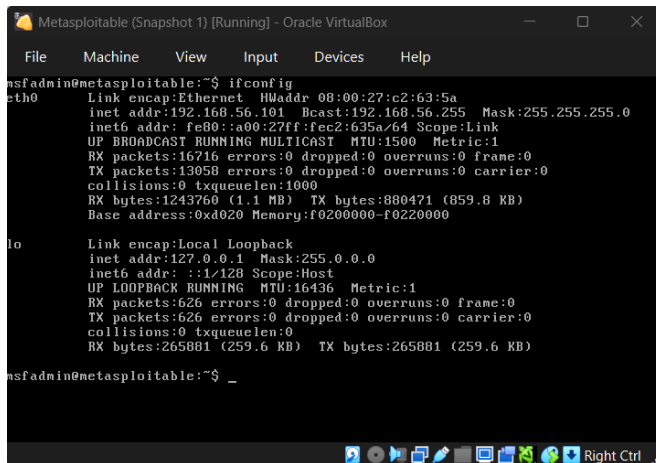
```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Login timed out after 60 seconds.

Warning: Never expose this VM to an untrusted network!
Contact: msfdevfat@metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: _
```

4. Metasploitable IP



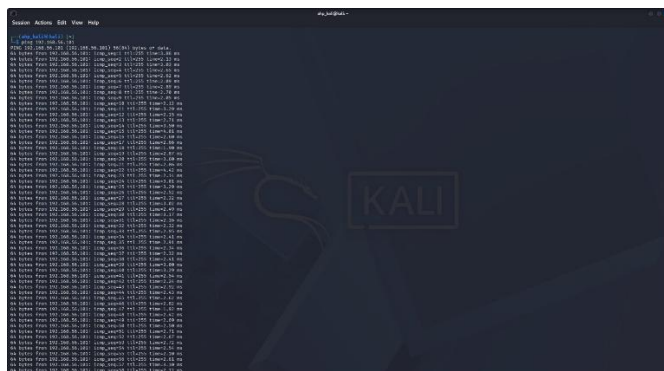
The screenshot shows a terminal window titled "Metasploitable (Snapshot 1) [Running] - Oracle VirtualBox". The terminal displays the output of the command `ifconfig`:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c2:63:5a
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec2:635a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16716 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13058 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1243760 (1.1 MB)  TX bytes:880471 (859.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:626 errors:0 dropped:0 overruns:0 frame:0
          TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:265881 (259.6 KB)  TX bytes:265881 (259.6 KB)

msfadmin@metasploitable:~$ _
```

5. Ping

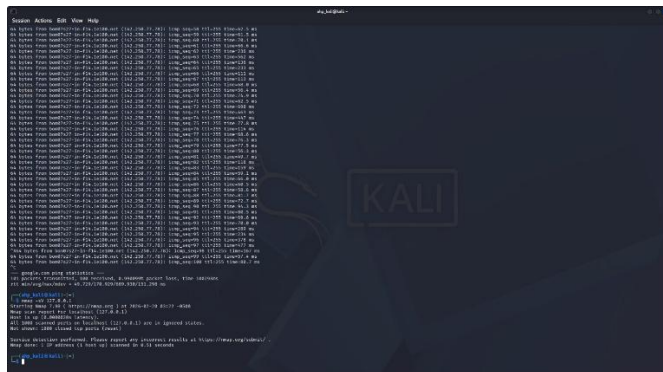


The screenshot shows a Kali Linux terminal window with a dark background and a "KALI" logo. The terminal displays the output of a `ping` command:

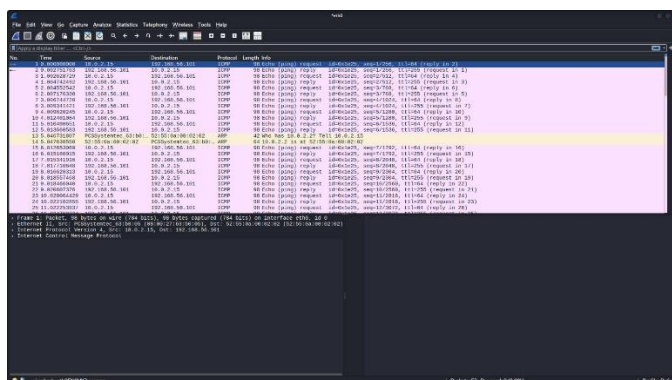
```
msfadmin@kali:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.042 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.042 ms
^C

```

6. Nmap



7. Wireshark



8.OpenSSL

