SUBMITION OF INTERNSHIP TASK-1

FOUNDATION AND ENVIRONMENT SETUP

INTERNSHIP TASK - 1

Name: Manoj N Naik

Gmail:1105manoj.n@gmail.com

Internship: ApexPlanet Cybersecurity & Ethical Hacking Internship Program Internship

Date: 12-02-2026

INTRODUCTION

In this first task, I focused on building a foundation in cybersecurity and setting up my own practice lab. Before diving into advanced security testing, I needed to understand the basics properly.

The task had two parts - studying core cybersecurity concepts like the CIA triad, network fundamentals, and cryptography, and then creating a safe virtual lab environment where I can practice penetration testing without affecting real systems.

For the lab, I used Kali Linux as my attacker machine and Metasploitable as the vulnerable target system. Both run on VirtualBox and are completely isolated from my main network.

CYBERSECURITY BASICS

CIA Triad

The CIA triad represents the three main principles of cybersecurity:

Confidentiality – Keeping information private and accessible only to authorized people. For example, your bank account details should only be visible to you, not to others. Companies protect confidential data like customer information and trade secrets from unauthorized access.

Integrity – Ensuring data remains accurate and unmodified. If someone changes "Transfer $100" to "Transfer $10,000" in a message, that's a breach of integrity. We use checksums and digital signatures to verify data hasn't been tampered with.

Availability – Making sure systems and data are accessible when needed. If a website crashes or server goes down, that's an availability problem. Companies use backup systems and redundant servers to maintain availability.

These three principles work together to protect information and systems.

Common Cyber Threats

Phishing – Attackers send fake emails pretending to be from banks or legitimate companies. These messages create urgency like "Your account will be locked!" to trick you into clicking malicious links or entering passwords on fake websites.

Malware – Short for malicious software. This includes viruses that spread between files, trojans that disguise themselves as legitimate programs, and spyware that secretly monitors your activities. Malware can steal passwords, delete files, or give attackers remote access.

DDoS (Distributed Denial of Service) – Attackers use many infected computers to flood a website with traffic, overwhelming the server until it crashes or becomes unusable. This doesn't steal data but makes services unavailable.

SQL Injection – Attackers insert malicious database commands through website input fields like login forms. If the website doesn't validate inputs properly, these commands can reveal sensitive data or delete information.

Brute Force – Using automated tools to try thousands of password combinations until finding the correct one. Attackers start with common passwords like "password123" then try dictionary words and random combinations.

Ransomware – Malware that encrypts all your files and demands payment to unlock them. Even after paying, there's no guarantee you'll get your files back. This has affected many companies and hospitals.

Attack Vectors

Attack vectors are the methods attackers use to break into systems:

Social Engineering – Manipulating people instead of hacking technology. Someone might call pretending to be IT support asking for your password, or leave an infected USB drive hoping someone plugs it in. It exploits human trust rather than technical vulnerabilities.

Wireless Attacks – Exploiting vulnerable Wi-Fi networks. Attackers can set up fake hotspots like "Free Airport WiFi" to intercept data, or crack weak Wi-Fi passwords. This is why using VPN on public Wi-Fi is important.

Insider Threats – Security risks from people inside the organization. This could be employees who steal data, accidentally click phishing links, or whose credentials get stolen. They're dangerous because they already have legitimate system access.

NETWORKING BASICS

OSI Model

The OSI model explains how data travels between computers in seven layers. Each layer has a specific function:

Layer 7 - Application: What users interact with (web browsers, email)

Layer 6 - Presentation: Formats and encrypts data

Layer 5 - Session: Manages connections between applications

Layer 4 - Transport: Ensures reliable data delivery (TCP works here)

Layer 3 - Network: Handles routing and IP addressing

Layer 2 - Data Link: Direct connections between devices (MAC addresses)

Layer 1 - Physical: Actual hardware like cables and network cards

Understanding these layers helps identify where network problems or attacks occur.

TCP/IP Protocol

TCP/IP is what actually runs the internet.

TCP (Transmission Control Protocol) – Works like registered mail, ensuring data arrives completely and in order. It breaks data into packets, numbers them, and waits for confirmation. If packets get lost, TCP resends them.

IP (Internet Protocol) – Handles addressing and routing using IP addresses like 192.168.1.1. It routes packets from source to destination but doesn't guarantee delivery. That's why TCP is needed on top of IP.

DNS and HTTP/HTTPS

DNS (Domain Name System) – Like a phonebook for the internet. It translates website names like "google.com" into IP addresses that computers can understand. When you type a website name, your computer asks a DNS server for the IP address first.

HTTP (Hypertext Transfer Protocol) – The language browsers and servers use to communicate. Your browser sends HTTP requests asking for webpages, and servers respond with HTML and other files.

HTTPS (HTTP Secure) – HTTP with encryption. All data between browser and server is encrypted, so interceptors can't read it. Always look for the padlock icon before entering passwords or credit card details.

IP Addressing and NAT

IP Addresses – Unique identifiers for devices on networks, like street addresses. IPv4 looks like 192.168.1.1 while IPv6 is much longer. Private IP addresses (192.168.x.x, 10.x.x.x) are used within local networks and can't be accessed directly from the internet.

NAT (Network Address Translation) – Allows multiple devices to share one public IP address. Your router has one public IP, but all your home devices (phones, laptops, TVs) can access the internet through NAT. The router tracks which device made each request and forwards responses accordingly.

CRYPTOGRAPHY BASICS

Symmetric Encryption

The same key encrypts and decrypts data, like a physical lock and key. If I encrypt a message with "SecretKey123", you need that exact key to decrypt it. The challenge is safely sharing the key without it being intercepted.

AES (Advanced Encryption Standard) is commonly used because it's fast and secure. Symmetric encryption is used for encrypting files and VPN connections.

Asymmetric Encryption

Uses two mathematically related keys:

- Public Key: Freely shared, used to encrypt data

- Private Key: Kept secret, used to decrypt data

To send me a secure message, you encrypt it with my public key. Only my private key can decrypt it. This solves the key distribution problem of symmetric encryption.

RSA is a common algorithm. It's slower than symmetric encryption, so it's often used to exchange a symmetric key securely, then the symmetric key handles actual data encryption.

Hashing

Hashing is a one-way process that converts any input into a fixed-length output. You can't reverse it to get the original back.

Example:

Input: "password123"

SHA-256 Hash:
"ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f"

Even tiny input changes produce completely different hashes. Hashing is used for:

- Storing passwords (websites store password hashes, not actual passwords)

- Verifying file integrity (compare hash before and after download)

- Digital signatures

Common algorithms: MD5 (outdated), SHA-1 (also outdated), SHA-256 (currently secure).

SSL/TLS

SSL/TLS creates encrypted connections over the internet. When you visit HTTPS sites:

1. Browser asks for the website's certificate

2. Website sends certificate with its public key

3. Browser verifies the certificate is valid

4. They use asymmetric encryption to agree on a symmetric key

5. All further communication uses that symmetric key (faster)

This ensures encryption, authentication, and data integrity.

LAB SETUP

Setting up my penetration testing lab was the most practical part. I needed a safe environment to practice without affecting real systems.

Why Virtual Machines?

I used VirtualBox to create virtual machines (VMs). VMs are like computers running inside your computer - they have their own OS and network but are isolated from your main system.

The Setup:

- Host Machine: My actual computer

- Kali Linux VM: My attacking machine with pre-installed security tools like Nmap and Metasploit

- Metasploitable 2 VM: Intentionally vulnerable system designed for practice

- Network: Both VMs use "Host-Only Adapter" which creates a private network between them, completely isolated from the internet and my home network

Verification Steps:

1. **IP Address Check:**

   - Kali Linux: Typed "ip a" in terminal - showed IP like 192.168.56.101

   - Metasploitable: Typed "ifconfig" - showed IP like 192.168.56.102

   - Both being in 192.168.56.x range confirmed they're on the same network

2. **Connectivity Test:**

   - From Kali, pinged Metasploitable: ping 192.168.56.102

   - Received responses, confirming the machines can communicate

3. **Packet Capture with Wireshark:**

   - Opened Wireshark on Kali and started capturing

   - Pinged Metasploitable again

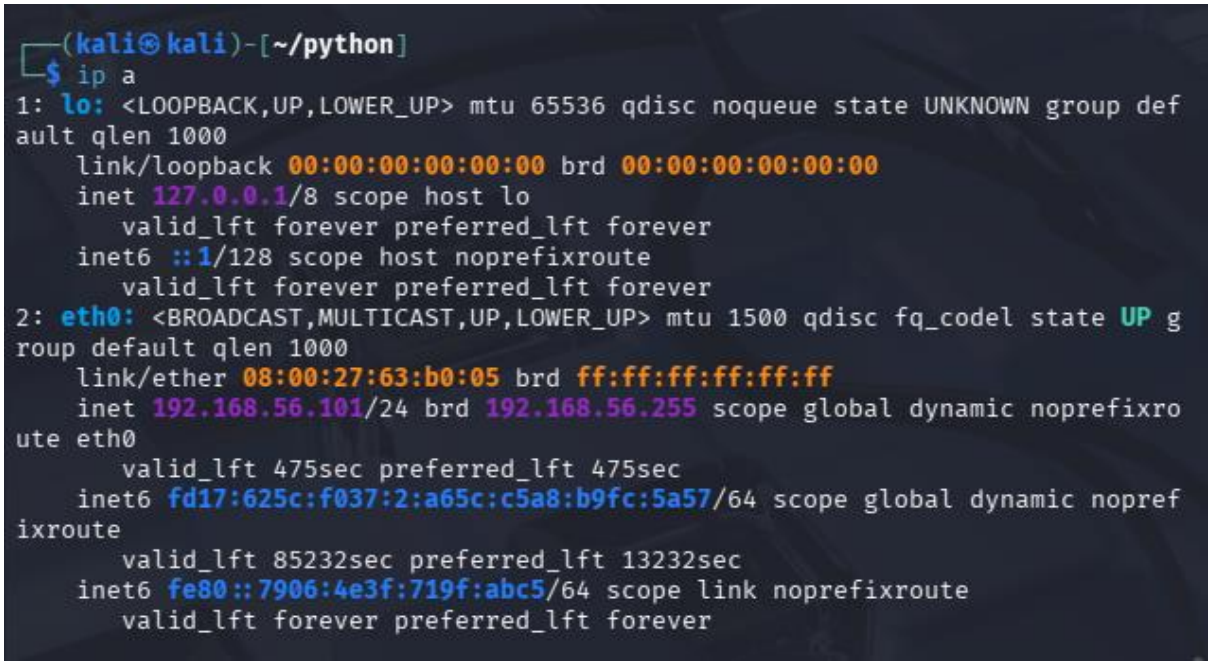
   - Saw ICMP packets (ping requests/replies) in Wireshark

   - Confirmed network traffic flows properly

SCREENSHOTS:

1.kali IP Adress

Kali Linux IP address using ip a



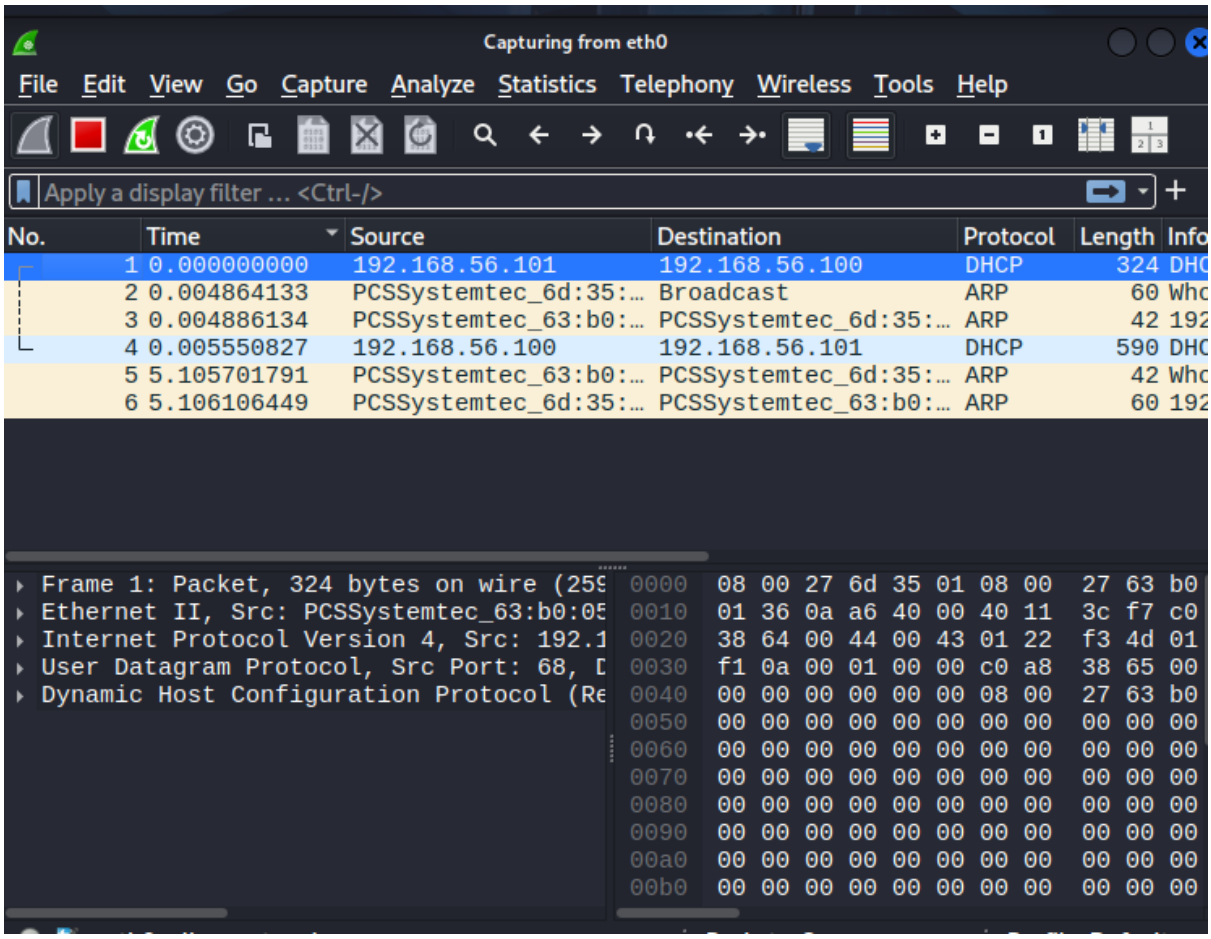
2.Metasploitable Ip Address

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:16:fc:4e
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe16:fc4e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1974 (1.9 KB)  TX bytes:4686 (4.5 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:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40385 (39.4 KB)  TX bytes:40385 (39.4 KB)

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ _
```

3.Ping Test

```
┌──(kali㉿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=0.223 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.026 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.053 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.039 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.085 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.045 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.028 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.035 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.038 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.038 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.031 ms
^C
── 192.168.56.101 ping statistics ──
13 packets transmitted, 13 received, 0% packet loss, time 12473ms
rtt min/avg/max/mdev = 0.026/0.063/0.223/0.056 ms
```

4.Wireshark Capture:



CONCLUSION

This task gave me a solid foundation in cybersecurity. I now understand the CIA triad principles, can identify various cyber threats, and grasp how networks function through the OSI model, TCP/IP, and related protocols.

Learning about cryptography - symmetric and asymmetric encryption, hashing, and SSL/TLS - showed me how data is protected. Most importantly, I successfully built my own isolated penetration testing lab with Kali Linux and Metasploitable.

Having this safe practice environment means I can now apply what I learn without risking real systems. I'm ready to move forward with advanced security testing techniques in upcoming tasks.