ApexPlanet Cybersecurity Internship: Task 1 Notes

Task Objective:

- Build a strong foundation in cybersecurity fundamentals.
- Set up a professional, private hacking lab environment.

1. Theory & Foundational Concepts

- **The CIA Triad**: The three core principles of information security.
    - **Confidentiality**: Keeping data secret (e.g., passwords).
    - **Integrity**: Ensuring data is accurate and trustworthy (e.g., bank records).
    - **Availability**: Making sure data is accessible when needed (e.g., a website staying online).
- **Threats & Attack Vectors**: A threat is a potential danger, while an attack vector is the method used to exploit a vulnerability.
    - **Common Threats**: Phishing, Malware, DDoS, SQL Injection, Brute Force, and Ransomware.
    - **Attack Vectors**: Social Engineering, Wireless Attacks, and Insider Threats.
- **Networking Basics**:
    - **OSI Model**: A 7-layer framework for network communication.
    - **TCP/IP**: The primary protocol suite for the internet.
    - **DNS/HTTP**: DNS translates domain names to IP addresses, while HTTP is the protocol for web traffic.
- **Cryptography Basics**:
    - **Symmetric vs. Asymmetric Encryption**: Symmetric uses one key, while asymmetric uses a public/private key pair.
    - **Hashing**: A one-way function to create a unique fingerprint of data (e.g., MD5, SHA256).

2. Lab Environment Setup

- **Virtualization**: Used **VirtualBox** to host virtual machines.
- **Attacker Machine**: Installed **Kali Linux**, an OS pre-loaded with security tools.
- **Target Machine**: Installed **Metasploitable2**, a vulnerable OS for ethical hacking practice.
- **Network Configuration**: Set up a **Host-Only Adapter** to create a private network, isolating the lab from the internet. This ensures that all activities remain contained.

3. Linux & Tool Cheat Sheet

This section includes key commands used during the task.

Category	Command	Description	Example
File System	ls	Lists files and directories.	ls -l
	cd	Changes the current	cd /home/kali/

Category	Command	Description	Example
		directory.	
	pwd	Prints the current working directory.	pwd
Networking	ifconfig	Displays network configurations.	ifconfig
	ping	Tests connectivity to a host.	ping 192.168.56.101
	netstat	Displays network connections.	netstat -ano
Permissions	chmod	Changes a file's permissions.	chmod +x script.sh
	chown	Changes a file's ownership.	chown kali:kali file.txt
Cryptography	openssl	Command-line cryptography tool.	openssl enc -aes-256-cbc ...
Scanning	nmap	Network scanning tool.	nmap 192.168.56.101
Packet Capture	wireshark	Packet analyzer.	sudo wireshark

4. Hands-on Demonstrations

- **Linux Fundamentals**: Practiced file and directory management using ls, cd, pwd, chmod, and chown.
- **Cryptography**: Successfully encrypted and decrypted a file using the openssl command to demonstrate an understanding of symmetric encryption.
- **Tool Familiarization**:
  - Used **ifconfig** to find the IP addresses of both the attacker and target machines.
  - Ran a **ping** command from Kali to Metasploitable2 to verify network connectivity.
  - Used **nmap** to perform a basic scan on the target, listing all open ports.
  - Launched **Wireshark** and performed a packet capture to monitor network traffic.