Penetration Testing Report: h4cked

Objective: Investigate the pcap file from a recent attack.

Initial Discovery

- **Port Under Attack**: Identified Port 21 (FTP) as the target of the attack.
- **Brute Force Attack**: Hydra tool used to brute-force into the user account 'jenny'.
- **Password Compromised**: The password 'password123' was successfully obtained by the attacker.

Attack Progression

- **Directory Accessed**: The attacker navigated to the **/var/www/html** directory.
- **Malicious Upload**: A reverse shell script, **shell.php**, was uploaded. This script was sourced from Pentest Monkey's PHP Reverse Shell.

Post-Compromise Activities

- **TCP Stream Analysis**: Utilized 'Follow TCP Stream' in HTTP to analyze post-compromise activities through the web reverse shell.
- **Initial Commands Executed**: The attacker ran **whoami** after gaining a foothold with the user 'jenny@wir3'.
- **Shell Enhancement**: The attacker spawned a TTY stable shell using the command **python3 -c 'import pty; pty.spawn("/bin/bash")'**.
- **Privilege Escalation**:
    - Checked **sudo -l**, revealing that 'jenny' can run sudo on all commands.
    - Attacker used **sudo su** along with Jenny's password to gain root access.

Further Malicious Activities

- **Rootkit Installation**: Downloaded and installed a rootkit from Reptile GitHub Repository using **git clone**.

Counter-Investigation Efforts

- **FTP Access Attempt**: Initial attempt to access the FTP system failed as the attacker had changed the password.
- **Brute Force Counter**: Employed Hydra with the command **hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.50.60** to regain access.
    - **Credentials Recovered**: Successfully obtained the credentials: Host: 10.10.50.60, Login: jenny, Password: 987654321.
- **Reverse Shell Re-Establishment**:

- Located and modified **shell.php**, updating it with our settings.
- Uploaded the modified script to the FTP server.
- Initiated a Netcat listener on our machine using **nc -lvnp 1234**.
- Accessed **http://10.10.50.60/shell.php** to establish a reverse shell.
- Verified control by running **whoami**, confirming we were logged in as 'www-data'.

Gaining Root Access

- **Stable Shell Spawned**: Used **python3 -c 'import pty; pty.spawn("/bin/bash")'** to spawn a stable shell.
- **Privilege Escalation as Jenny**: Used Jenny's credentials (password: 987654321) to switch to the 'jenny' user and then to 'root'.
- **Final Objective**: Navigated to and accessed **flag.txt** as root.

Conclusion

The penetration test successfully retraced the attacker's steps, regained control of the compromised system, and accessed critical data, demonstrating vulnerabilities in the system's security. Further measures should be taken to enhance security, including strengthening password policies and monitoring for unusual access patterns.