🏴‍☠️ Write-Up: Máquina "Pressenter"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

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

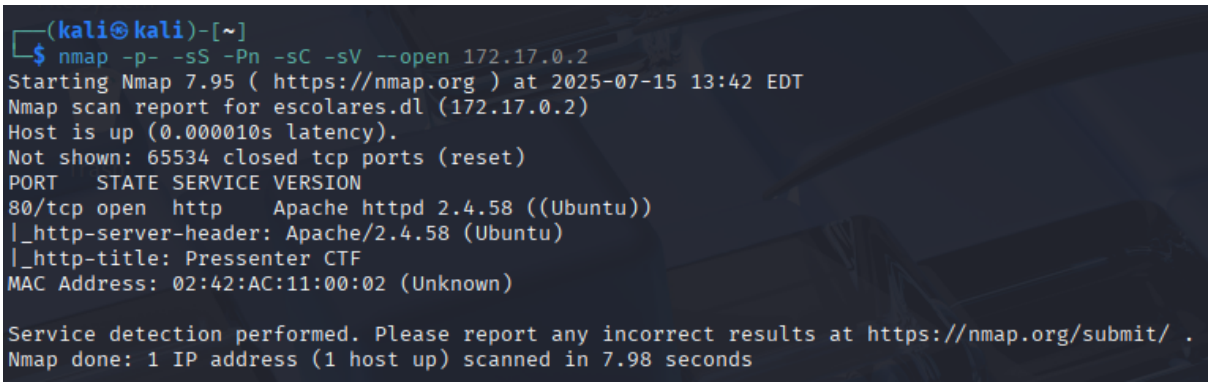
📡 1. Reconocimiento y Recolección de Información

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
```

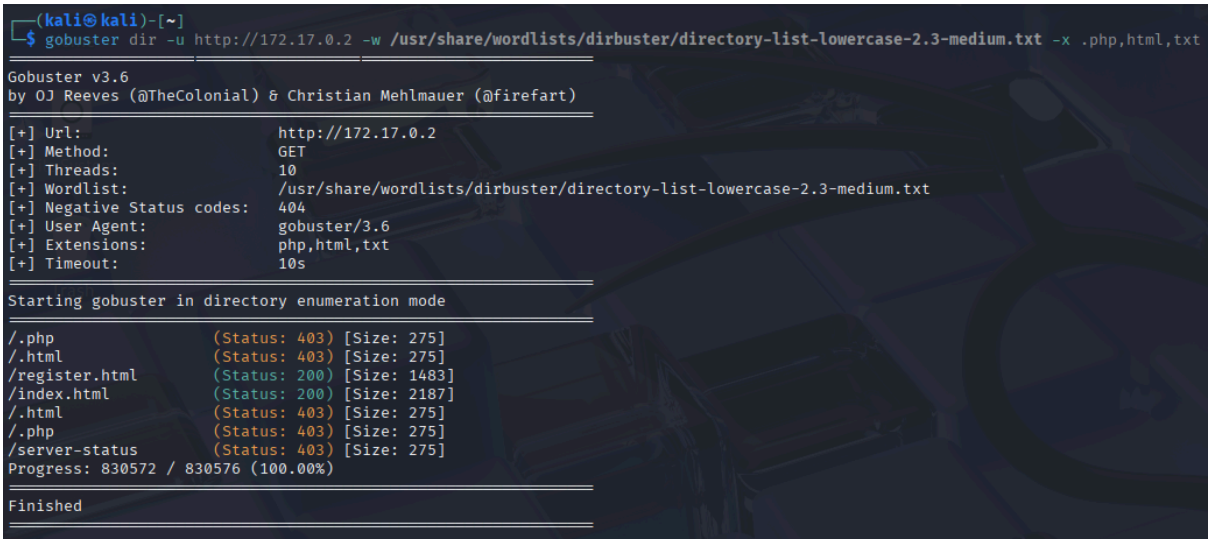
🎯 2. Escaneo y Enumeración

Busco y enumero los puertos junto a sus versiones.



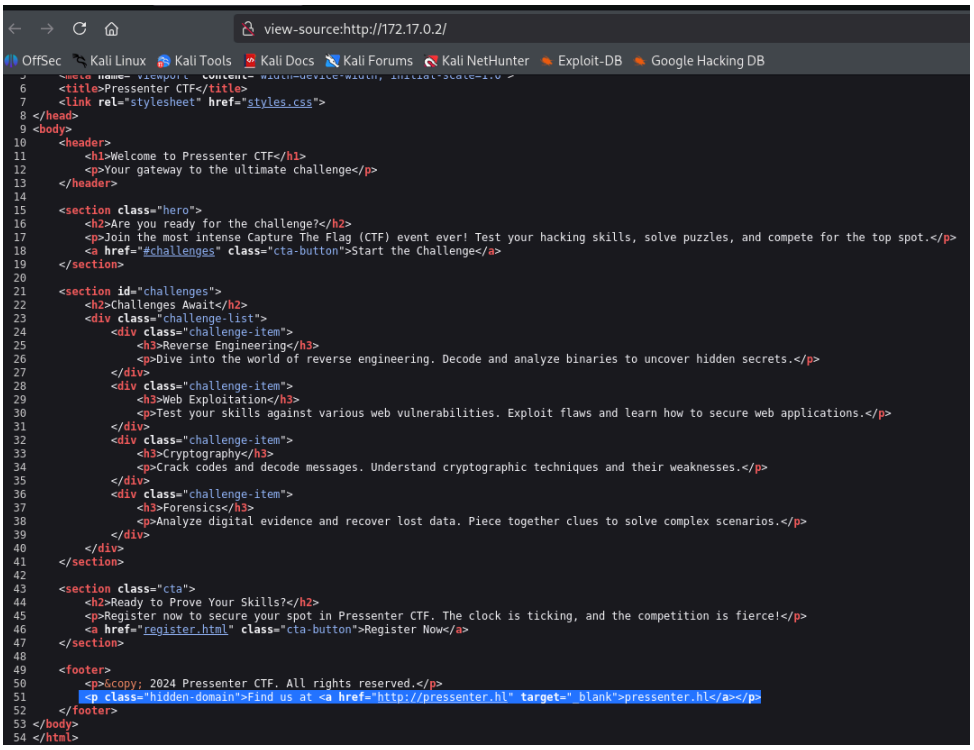
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 13:42 EDT
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000010s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    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.

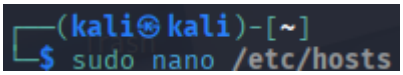


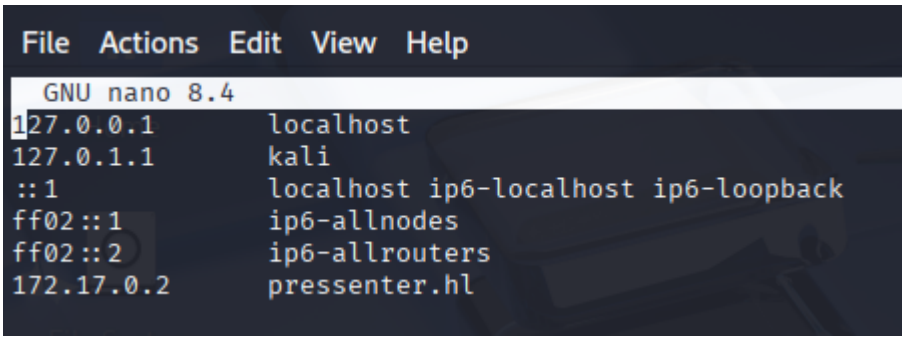
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================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

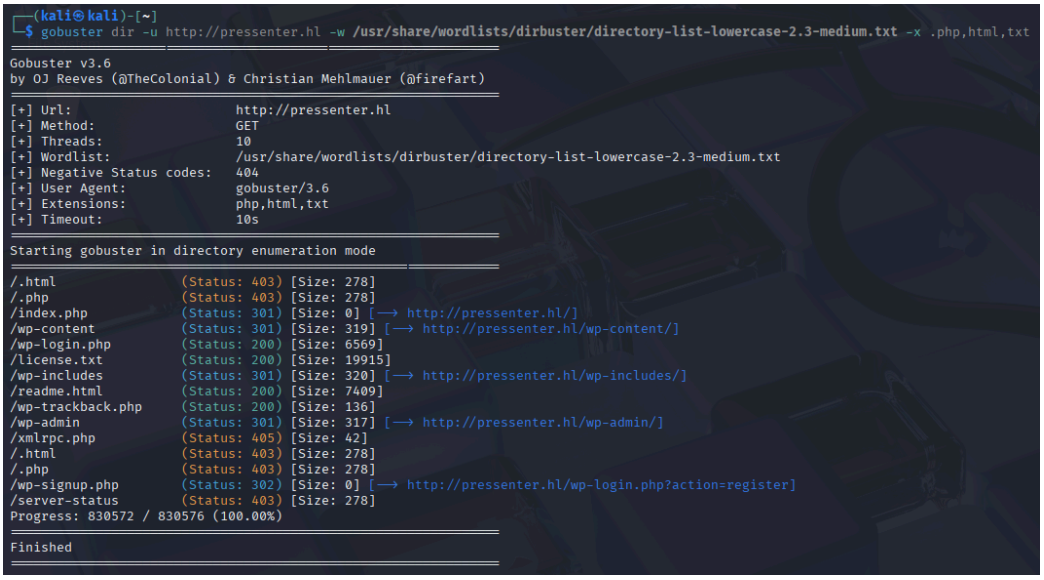


Relaciono el dominio encontrado a la ip de la máquina para poder acceder mediante el dominio.

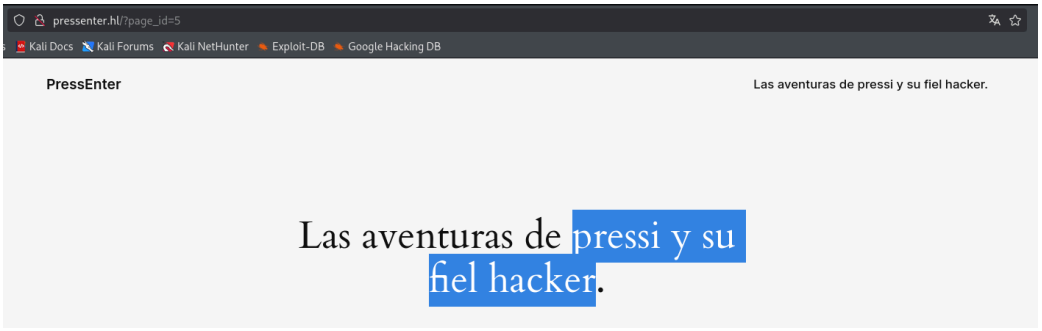




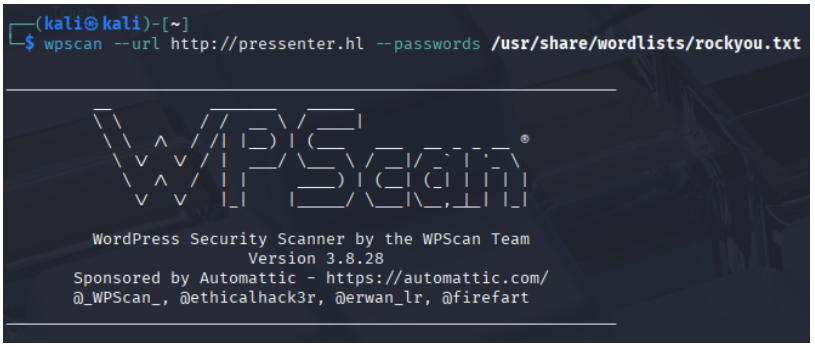
Busco directorios en la web pero usando el nuevo dominio. Me doy cuenta que es una web WordPress.

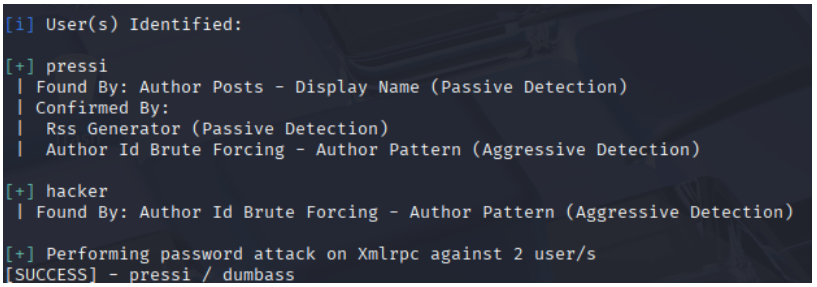


Viendo la web, puede ser que pressi sea un usuario.



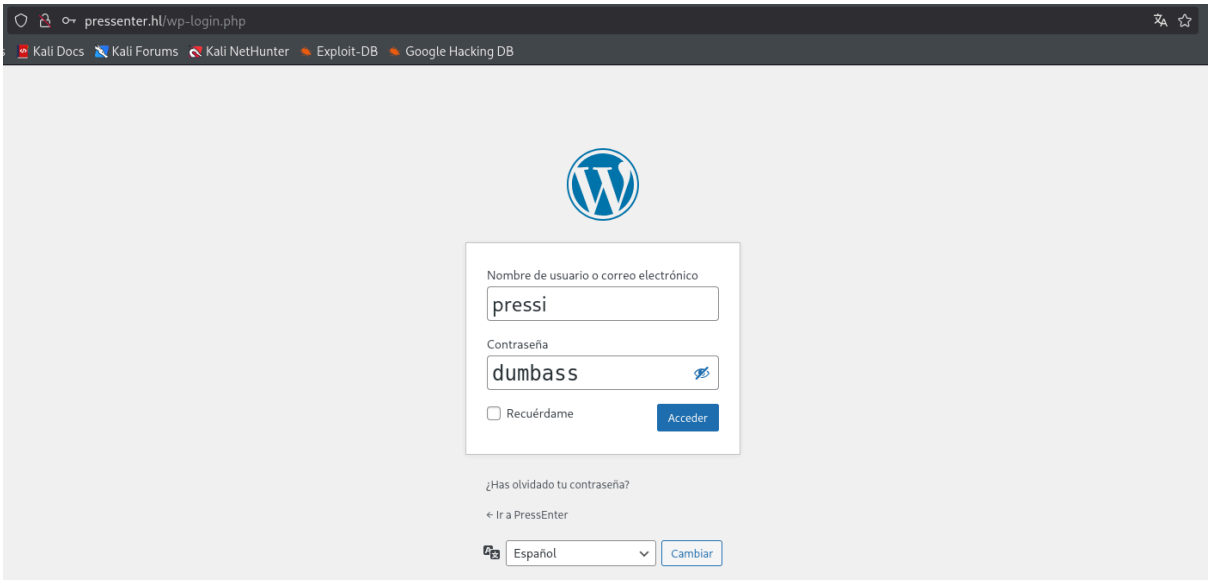
Uso wpscan para buscar usuarios en la cuenta de WordPress e intentar encontrar su contraseña mediante fuerza bruta.



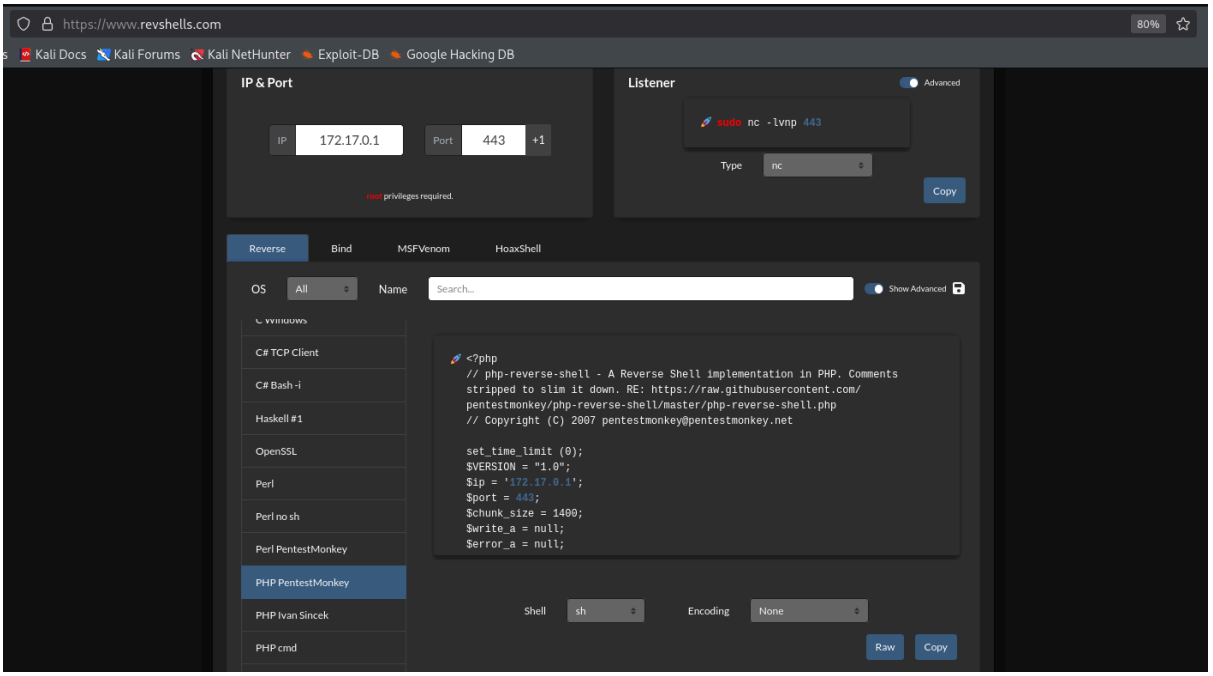


💥 3. Explotación de Vulnerabilidades

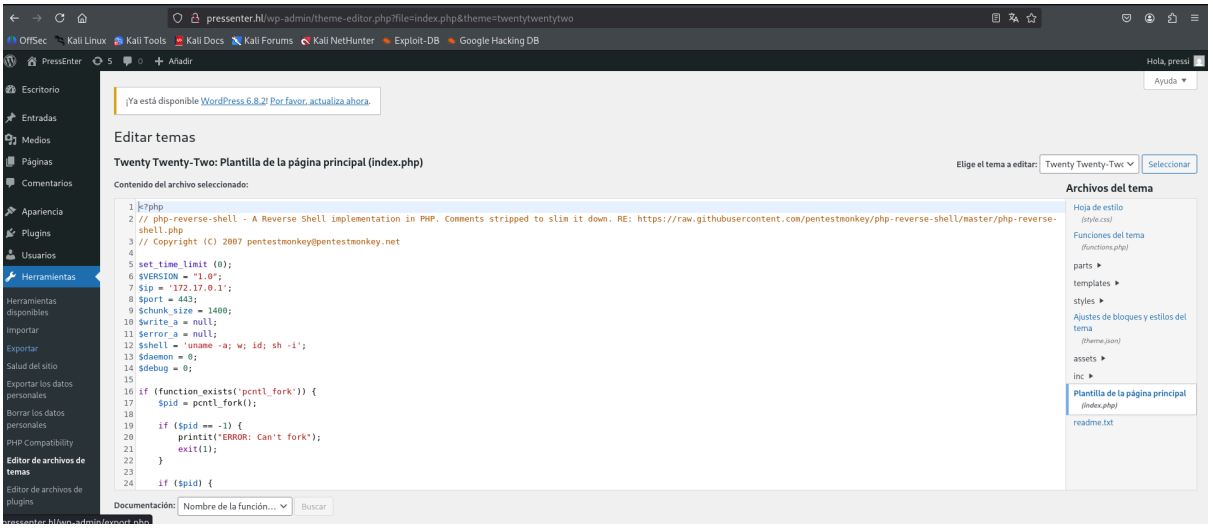
Ingreso usando las credenciales encontradas anteriormente.



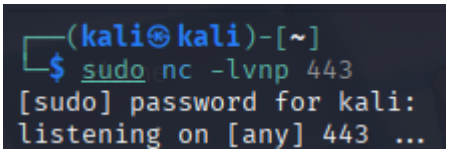
Dando vueltas por el panel, encontré un archivo en php que puedo modificar para ejecutar una reverse shell. Por ende, busco la famosa reverse shell de PentestMonkey.



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



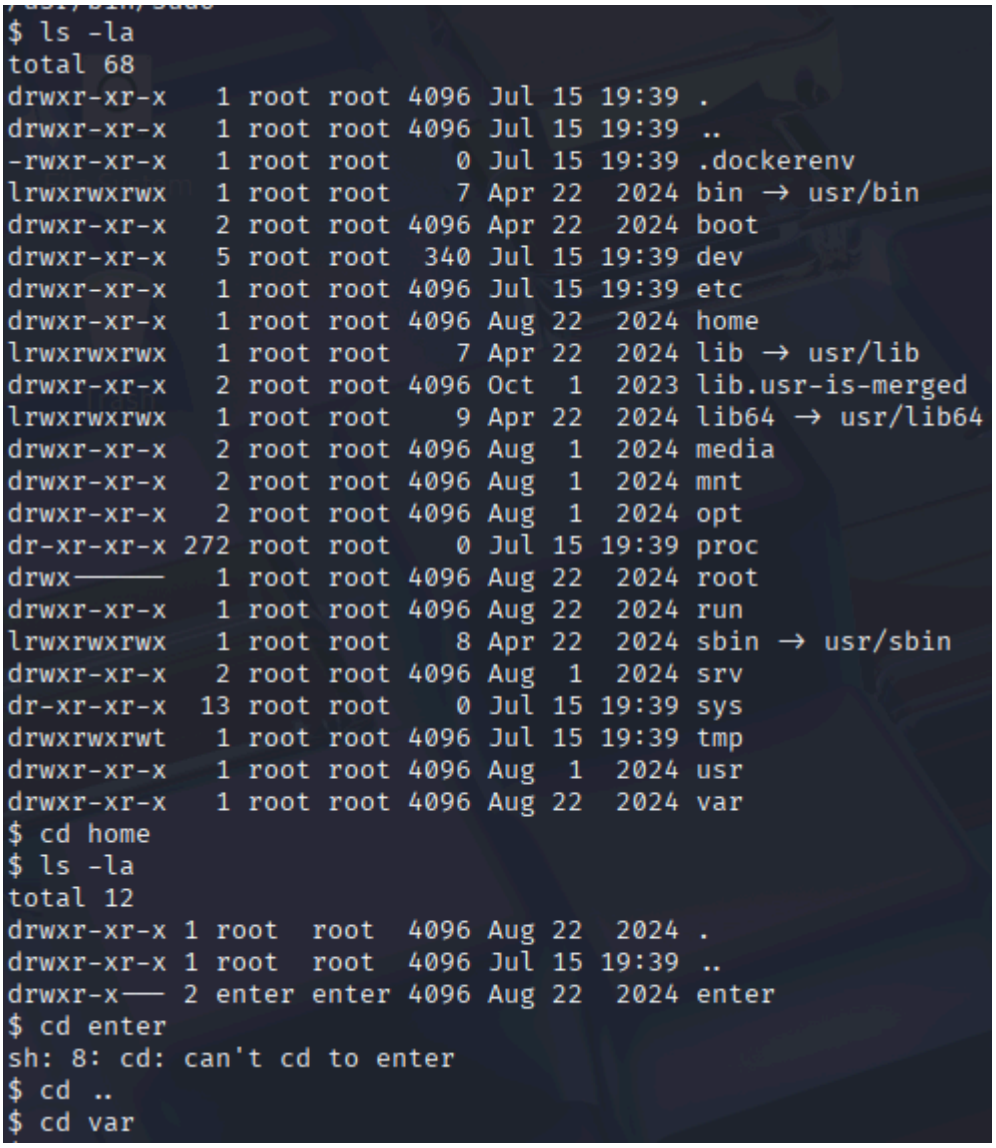
Me pongo a la escucha con netcat



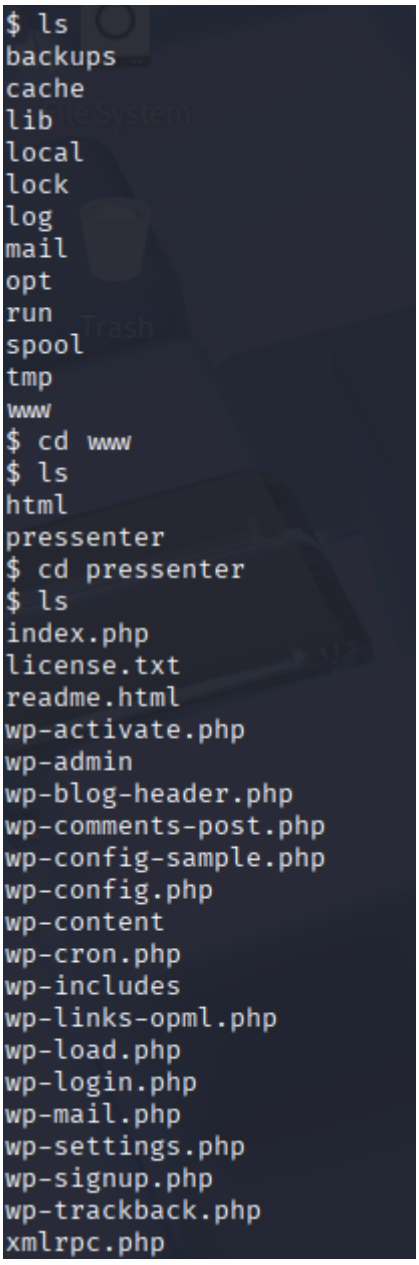
Ingreso a la ruta donde está el archivo php modificado con mi reverse shell, en mi caso: http://pressenter.hl/wp-content/themes/twentytwentytwo/index.php. Esto permite que al acceder a esa ruta, el navegador ejecuta el archivo php.

🔐 4. Escalada de Privilegios y Post-explotación

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



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



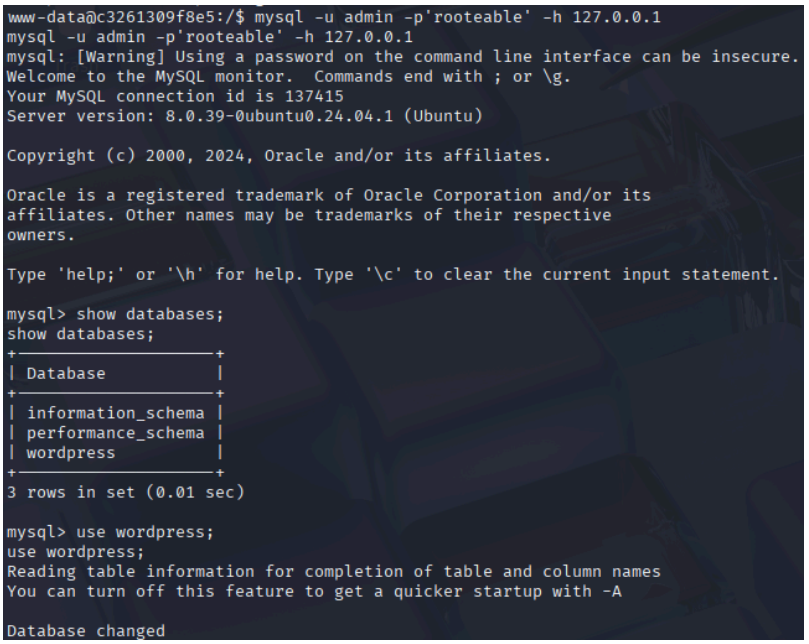
Leo el archivo y encuentro las credenciales de la base de datos.

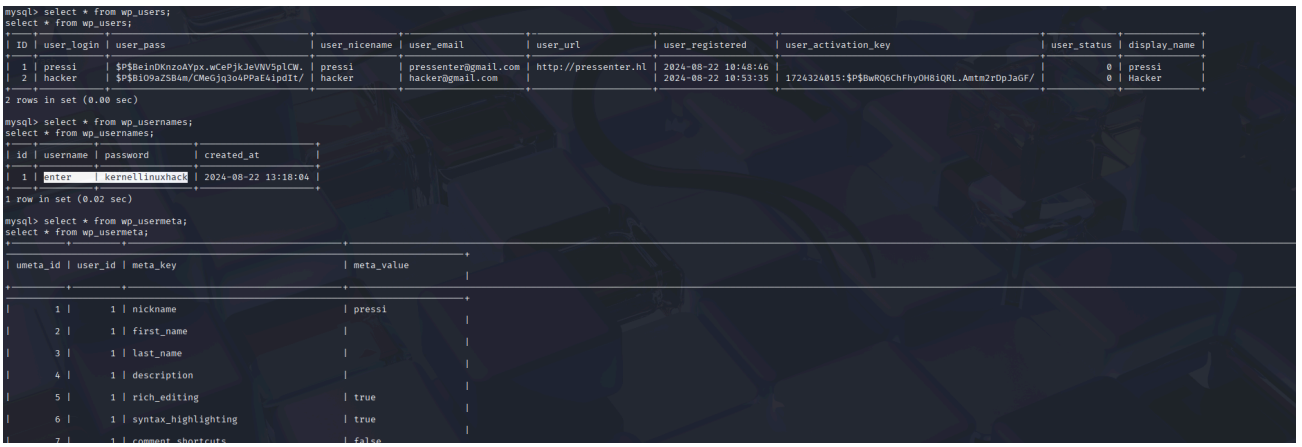
```
$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the website, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * 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.



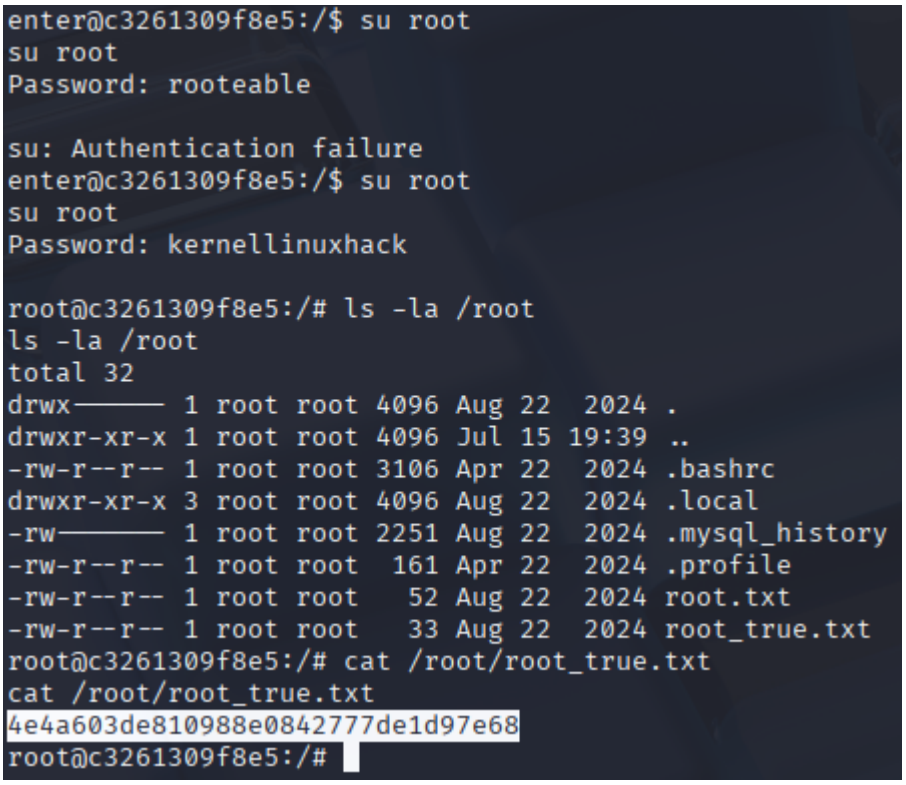


Busco la bandera de user. Luego, busco archivos con permisos SUDO para intentar escalar privilegios. Encontré un par, uso cat para leer la bandera de root ya que supuse que se llamaría root.txt porque en casi todos los CTF la bandera de root se llama así, además, la bandera de usuario es usuario.txt, 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.



🏆 Banderas y Resultados

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