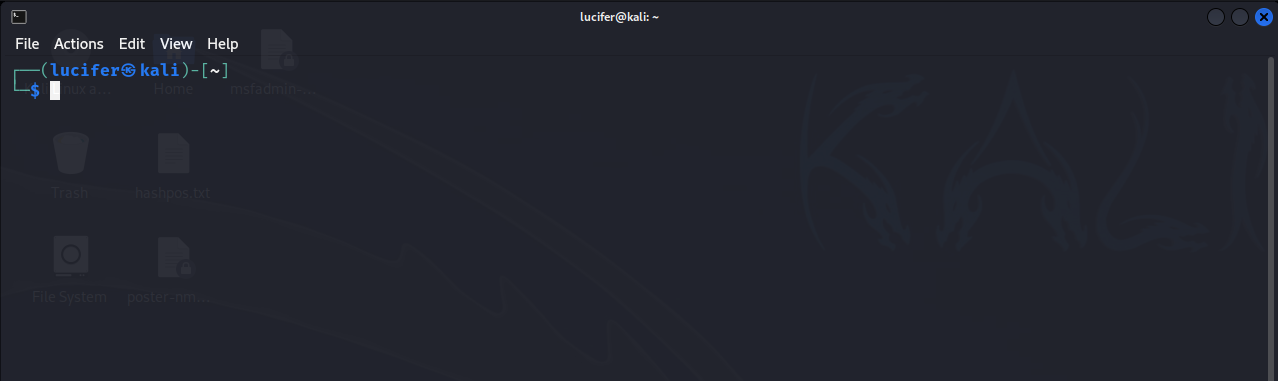
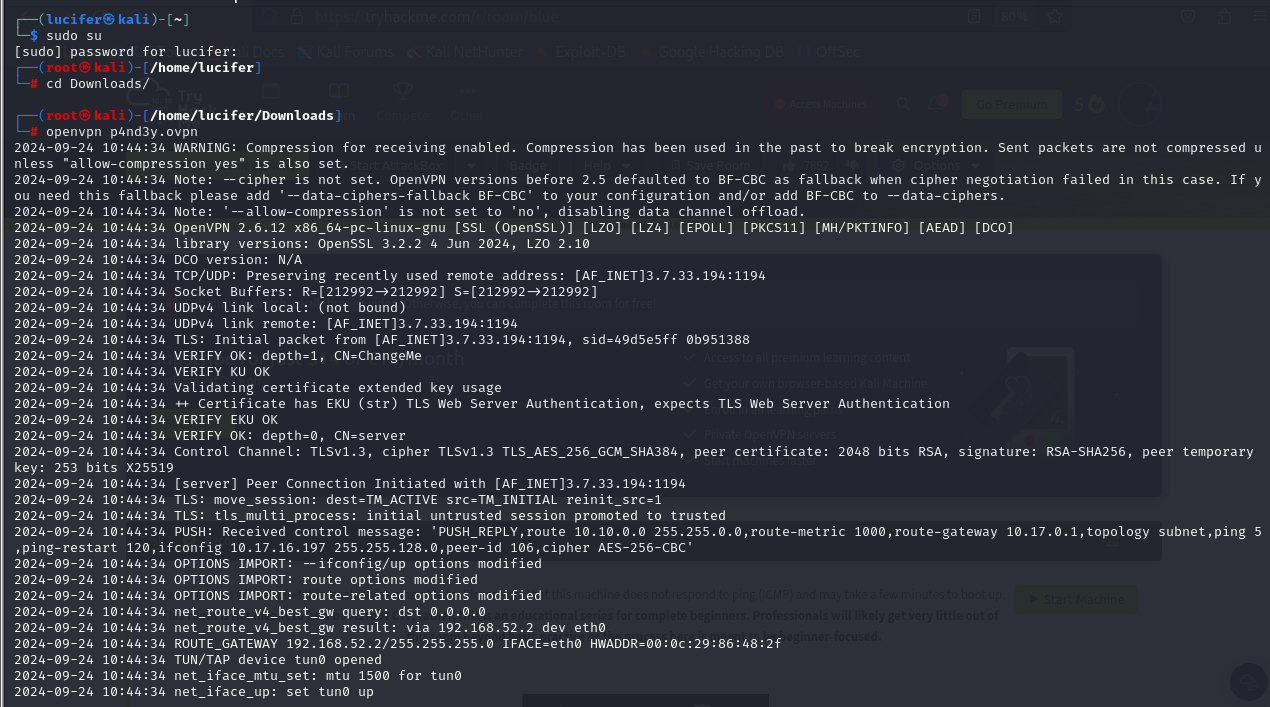
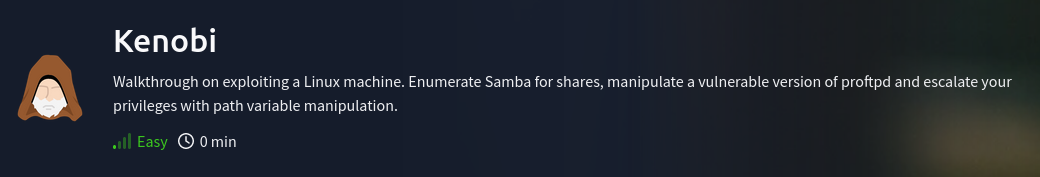
Kenobi is a box on tryhackme (<https://tryhackme.com/r/room/kenobi> ) created by **tryhackme**.

Here our **terminal**  is opened.

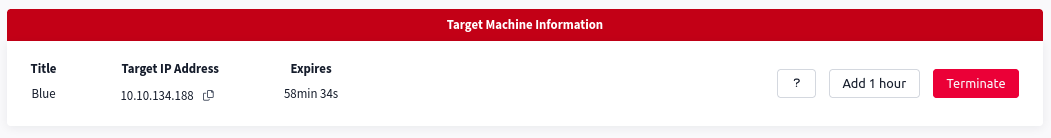


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

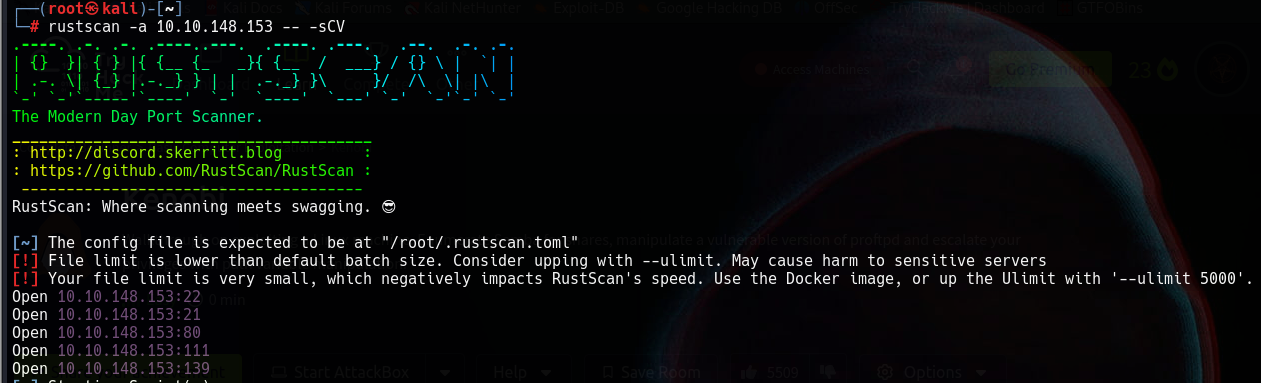


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. 

After starting the machine it’ll get one minute to show the ip.

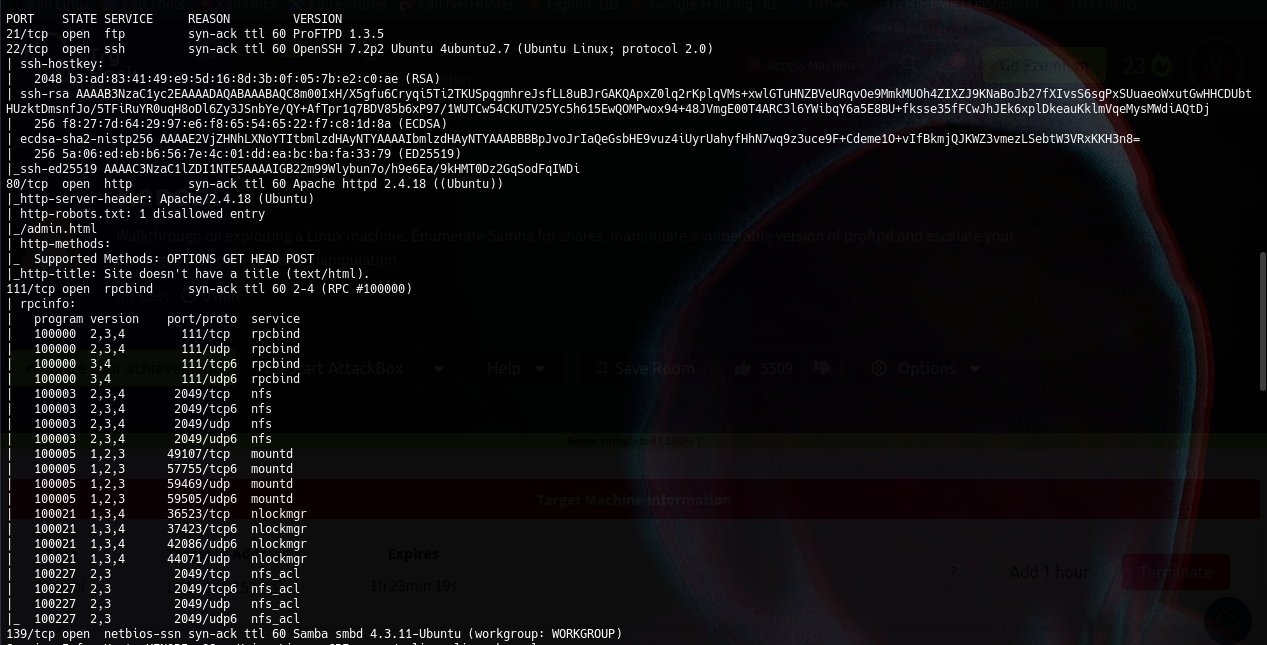


After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.



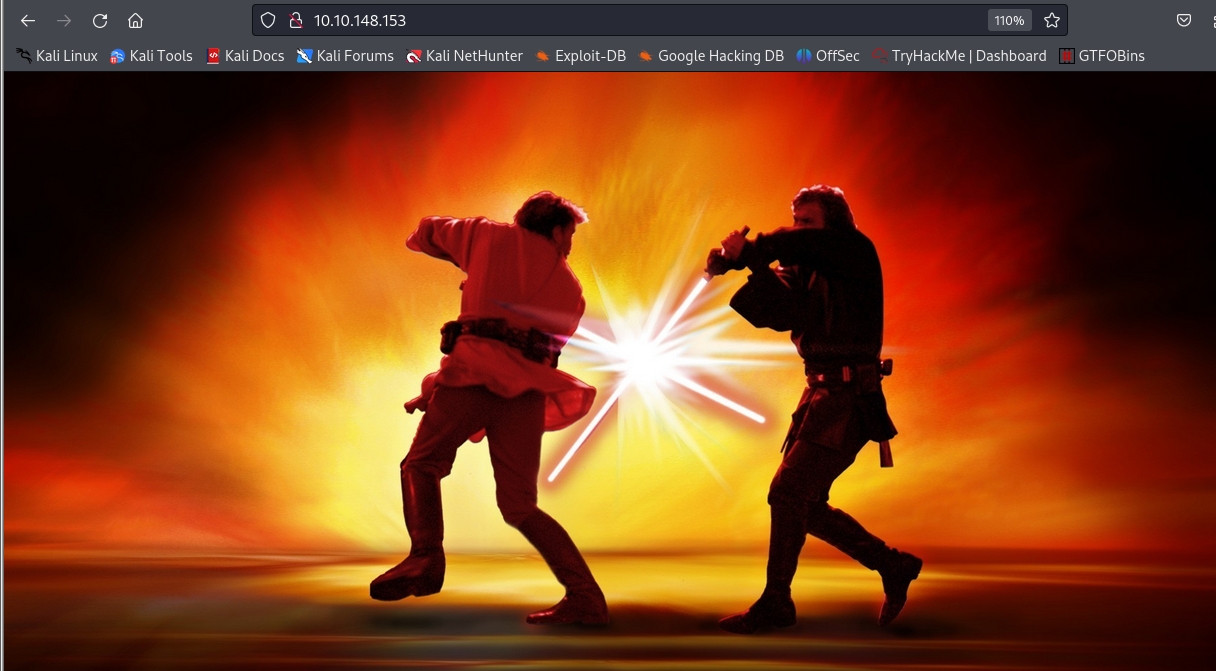
Here I am using **rustscan -a <ip> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

Seems like our scan is completed. Looks like there are total 5 ports open.



Now we know that what ports are running currently on the target machine.

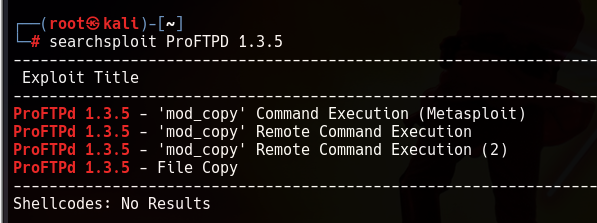
We will look for anything suspicious on the web server.

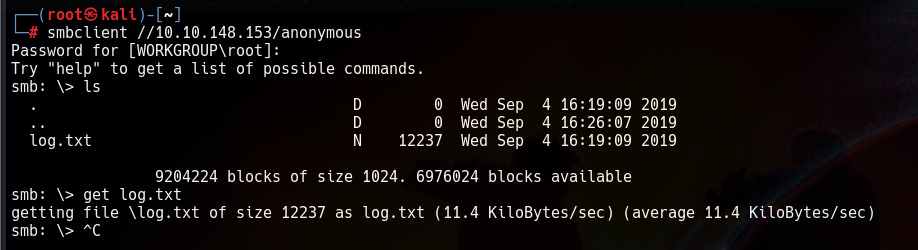


There is nothing valuable found on web server.

Now we look for our next port i.e. **ftp**  . It has **ProFTPD version 1.3.5** running. We will use searchsploit to look for any exploits or vulnerabilities present there.

We found four exploits that is based on **mod\_copy** module.



Before moving on further we know that anonymous login is present on smb server. 

After looking into the **log.txt** file we get information about how to exploit using the ProFTPD version.

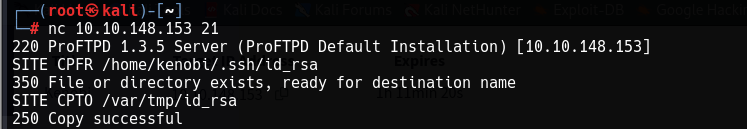
Let’s move forward to it.

We will use netcat to connect to the machine on the FTP port.

**nc <ip> 21**

****When the connection is established we will use commands from the **mod\_copy module.** 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. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination.

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



We knew that the /var directory was a mount we could see. So we've now moved Kenobi's private key to the /var/tmp directory.

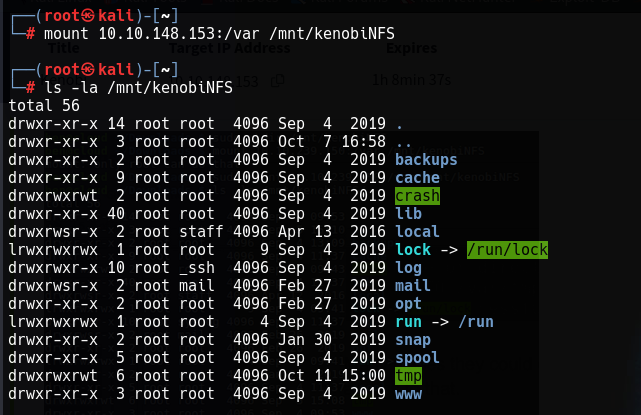
Lets mount the /var/tmp directory to our machine.

We will use:

**mkdir /mnt/kenobiNFS**

**mount 10.10.148.153:/var /mnt/kenobiNFS**

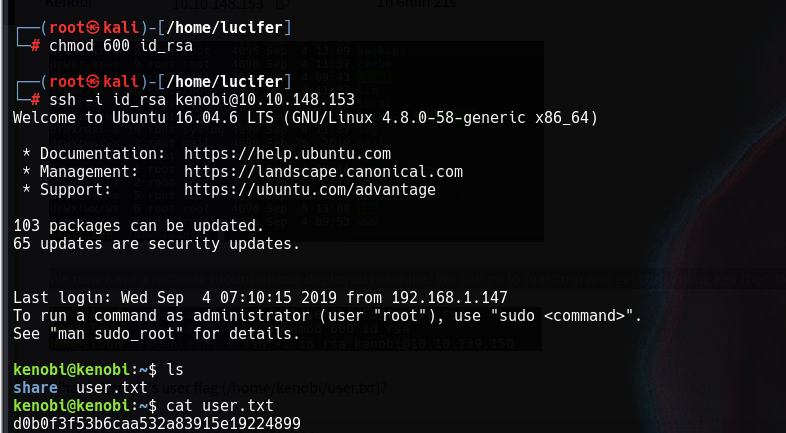
**ls -la /mnt/kenobiNFS**

****

We now have a network mount on our deployed machine! We can go to /var/tmp and get the private key then login to Kenobi's account.

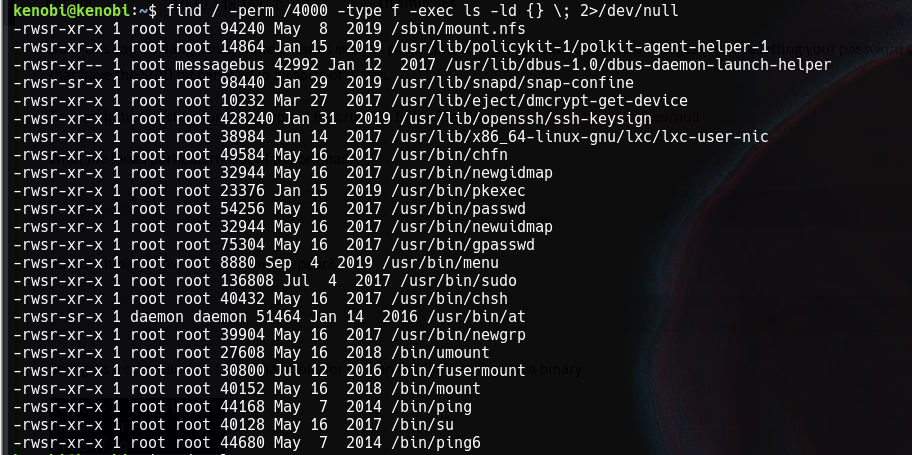
Now we will copy the **id\_rsa file** to our system, change it permission and force ssh to the target system using **ssh -i id\_rsa kenobi@<ip>**

****

****

We will get our **user.txt** file. Now we need to escalate privileges to gain root as we know our root flag will be in root folder.

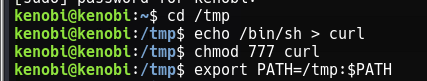
We will now look for permissions to the root files and look for any odd one which we can exploit.



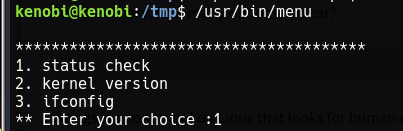
We can see the **/usr/bin/menu**  directory as odd. May be it could give us root.

We will create a file called curl in the /tmp directory and writes /bin/sh into it. This file effectively becomes a script that launches a shell.

We will then change it’s permissions and then update the $PATH environment variable to include the /tmp directory at the beginning of the search path for executables. This ensures that when the system or user tries to execute curl, it will first check in /tmp, where the malicious or custom curl script resides.



Now we will execute the /usr/bin/menu file and set our choice to 1.



And we are **root!** Now we can get the root file which is our final flag.

