**Lab Practical #02:**

TryHackMe Room: - **Brooklyn99**

1. Initially, we will try with the reconnaissance, so let’s start with the nmap scan.

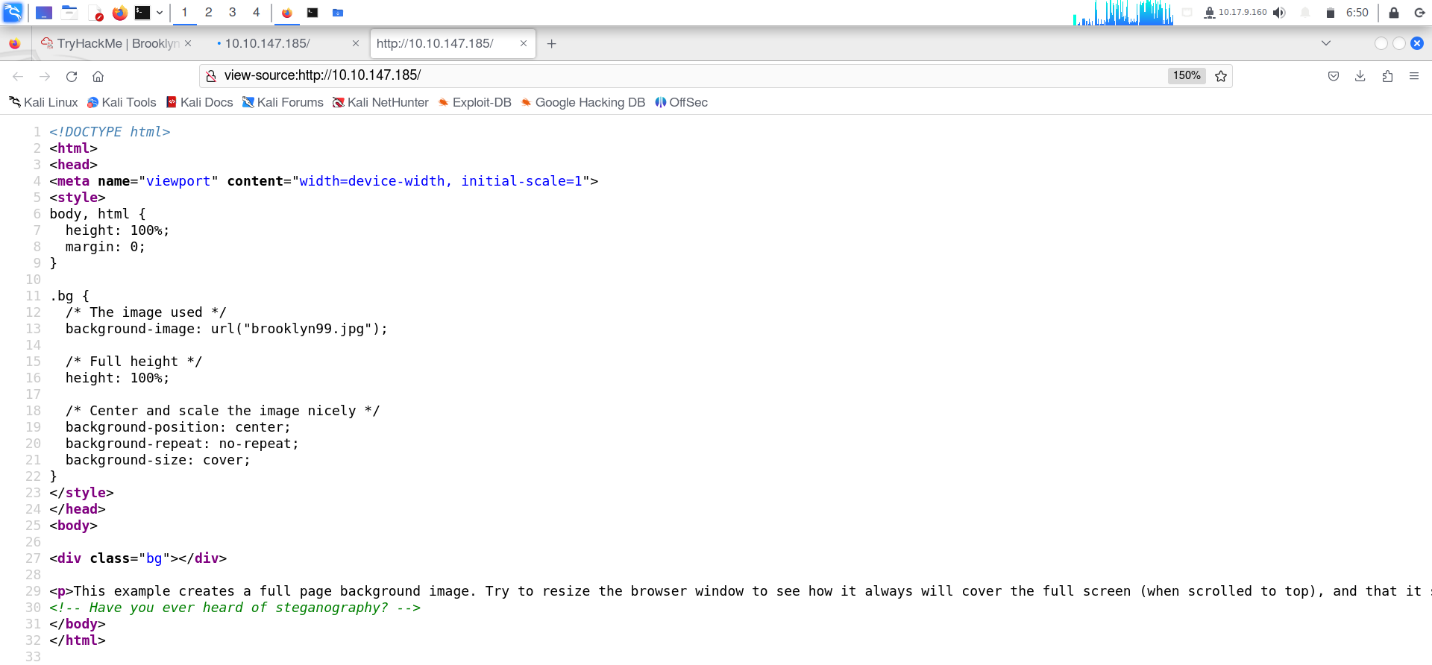
***nmap -sC -sV <10.10.147.185>***



**nmap results**

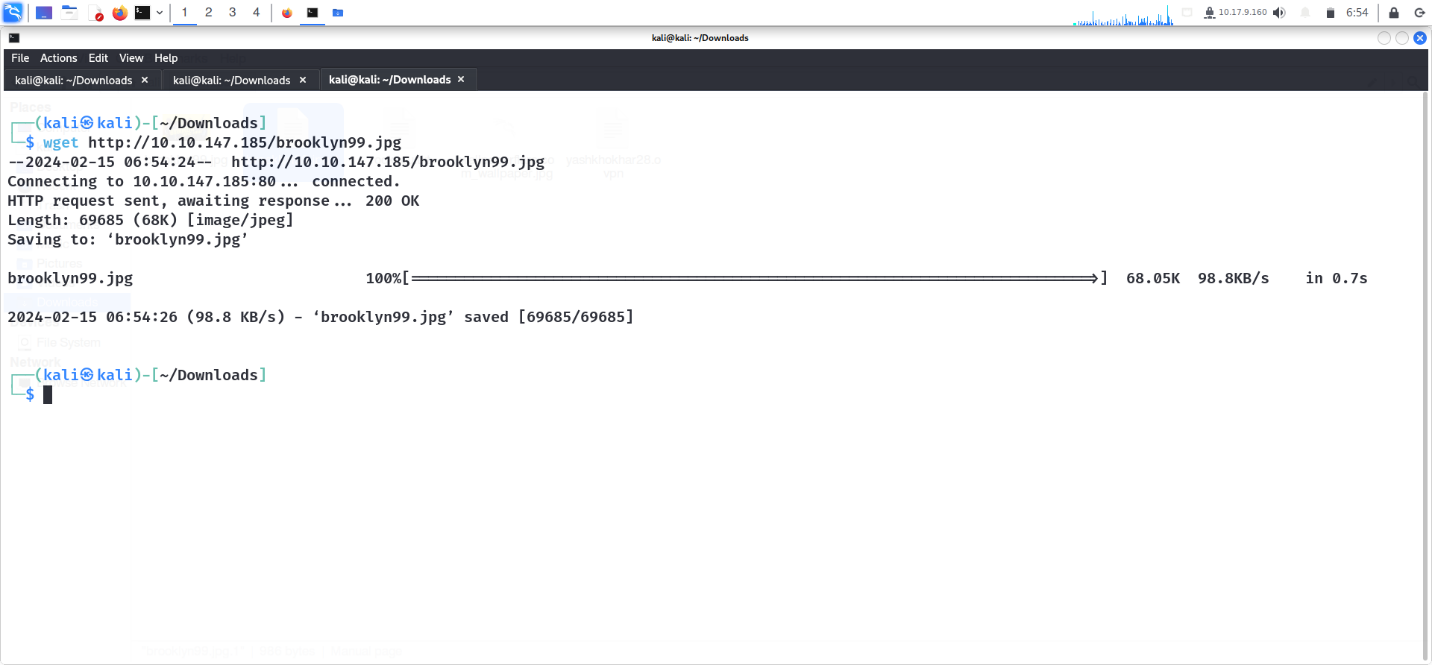
By looking at the above screenshot, we can see that we have found 3 ports open i.e. 21(FTP), 22(SSH) and 80(HTTP).

1. As port 80 is open, copy-paste the IP in the browser and check the source page of this.



**source page**

1. I will download the jpg file now –



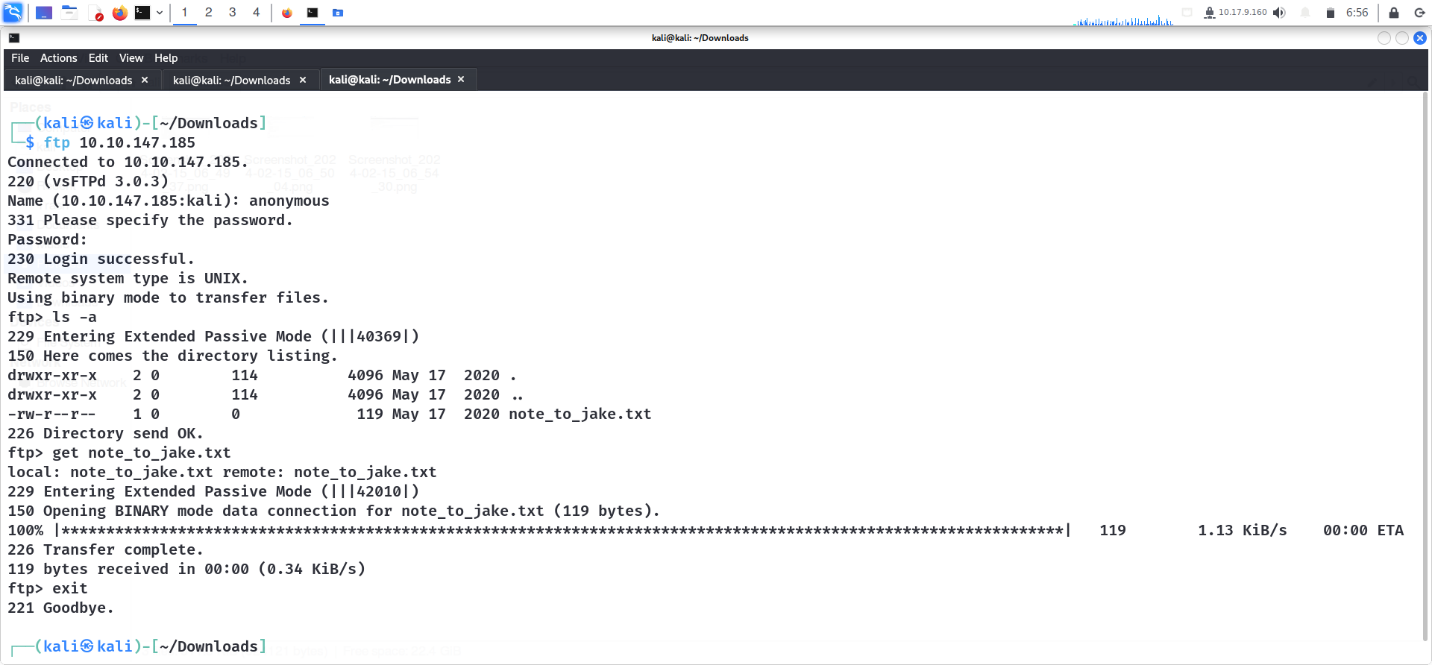
1. Didn’t get anything interesting here..

We have also seen that Anonymous FTP login is allowed which means it allows anyone who can use FTP to log on to the server, using a general username and without a password check.. So, let’s go for it –

***ftp <10.10.147.185>***

***ls -a****— to list the files in the directory.*

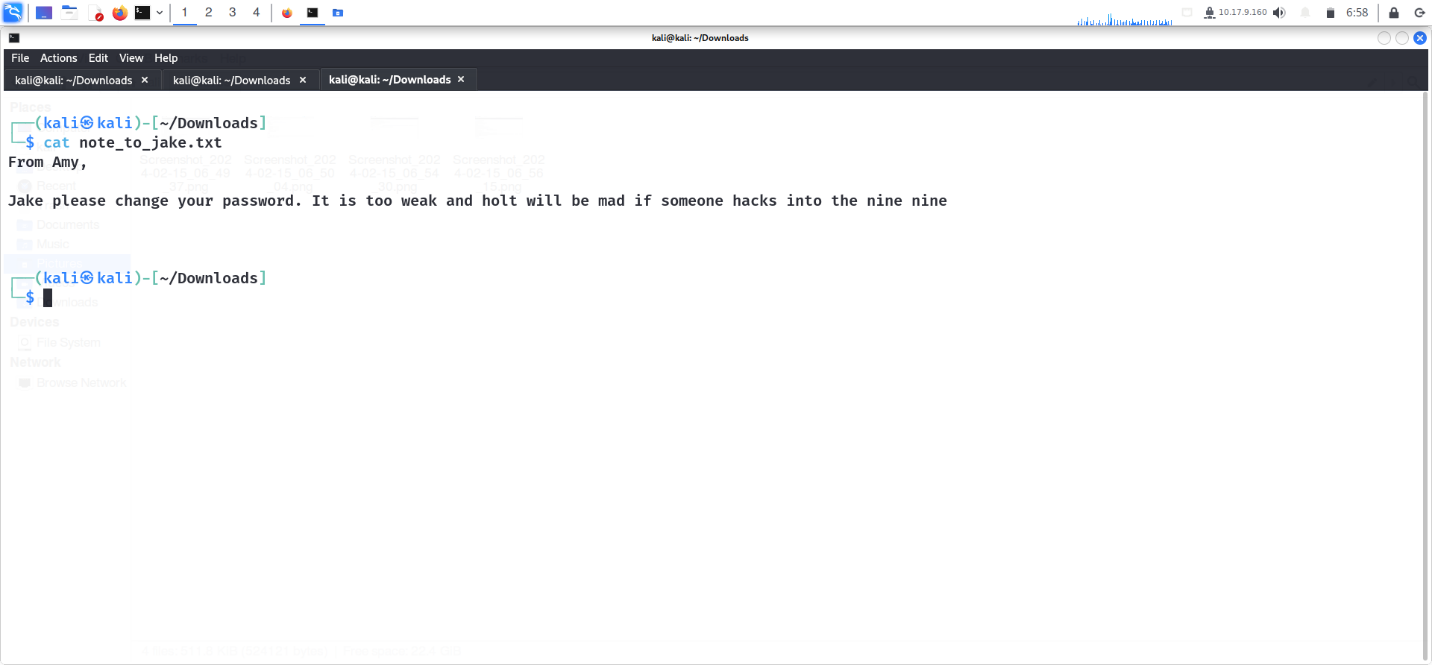
***get note\_to\_jake.txt****— to download the file*



**brooklyn99.jpg**

1. Let’s check what’s in that txt file.

***cat note\_to\_jake.txt***

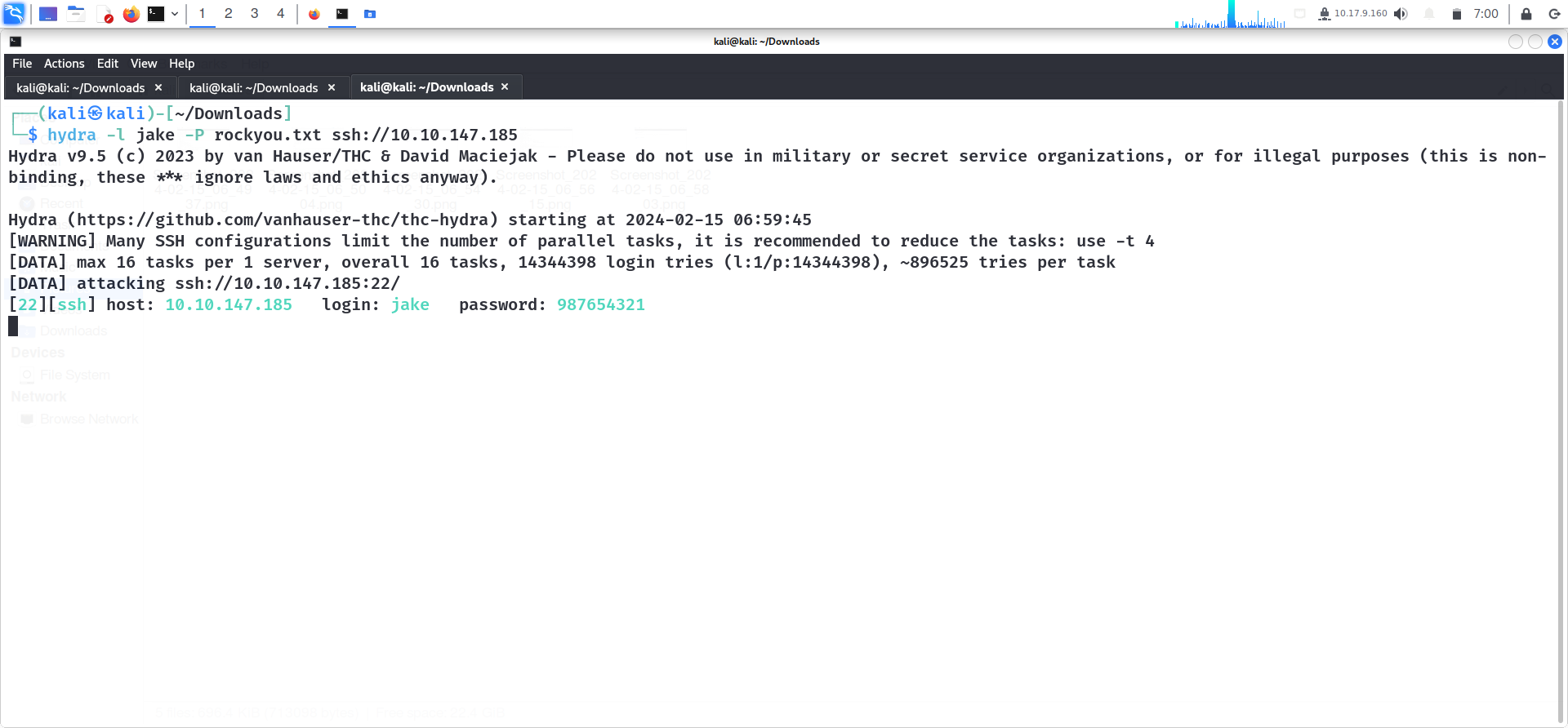


**cat**

1. From the above file we can conclude that Jake’s password is weak and so we can use bruteforce to know his password. Also, we have got 3 usernames from it i.e. Amy, Jake and Holt.

We will now use hydra for bruteforce Jake’s password for ssh.

***hydra -l Jake -P rockyou.txt 10.10.147.185***



**bruteforce**

1. We have got Jake’s password — 987654321 (That’s really weak!!)

Now, we will use this password and login to Jake’s account using ssh.

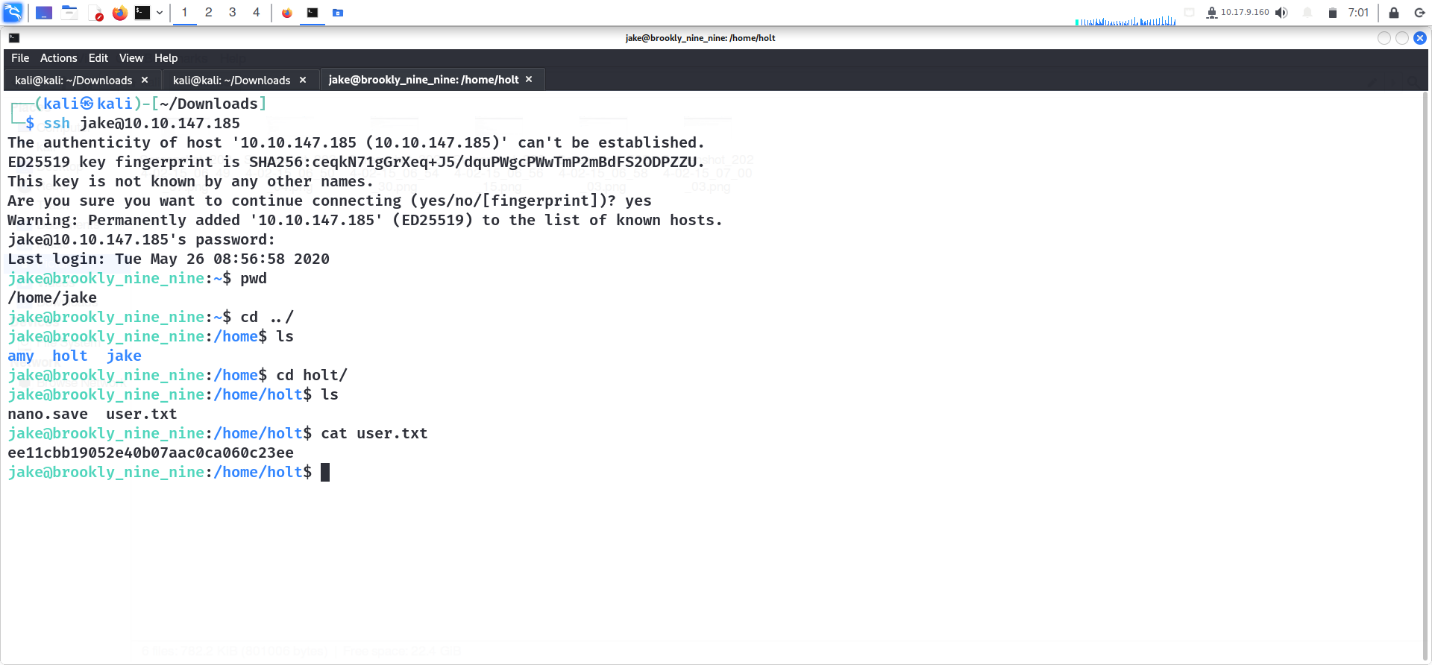
***ssh [jake@<10.10.147.185](mailto:jake@%3c10.10.147.185)>***

We have got a txt file in Holt’s dir. Let’s check what’s can we get from that file.

***cat holt/user.txt***

We got the user flag..

**User Flag : ee11cbb19052e40b07aac0ca060c23ee**



1. Now, we will have to look for the root flag.

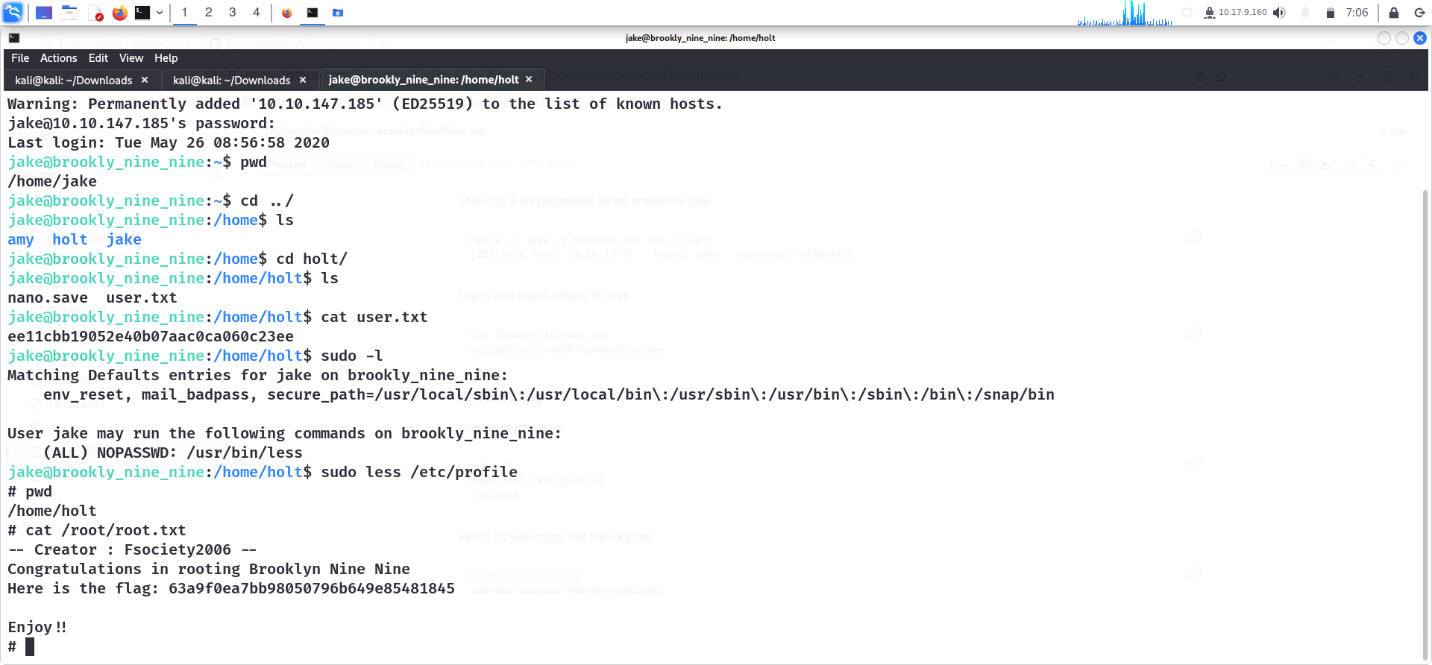
Using sudo -l command, to check which commands Jake can use as root priviledges.

Now, execute the below command

***less root/root.txt***

Finally, got the root flag too!!!

**Root Flag : 63a9f0ea7bb98050796b649e85481845**



1. TryHackMe Tutorial

