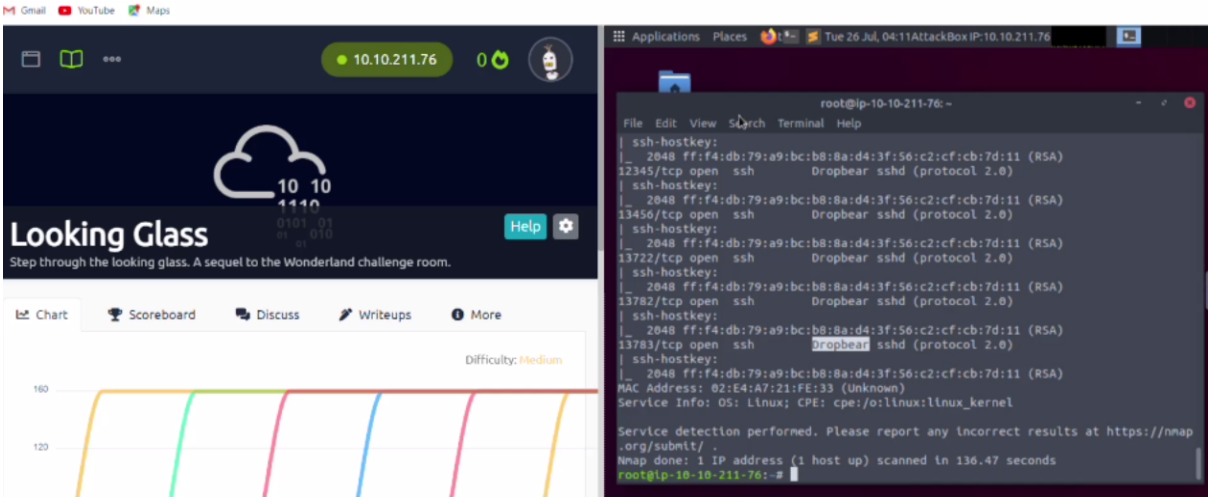
PenTest 1

ROOM A

SANG HAEKEO

ID	NAME	ROLE
1211101693	Savitha Murugumunisegaran	Member

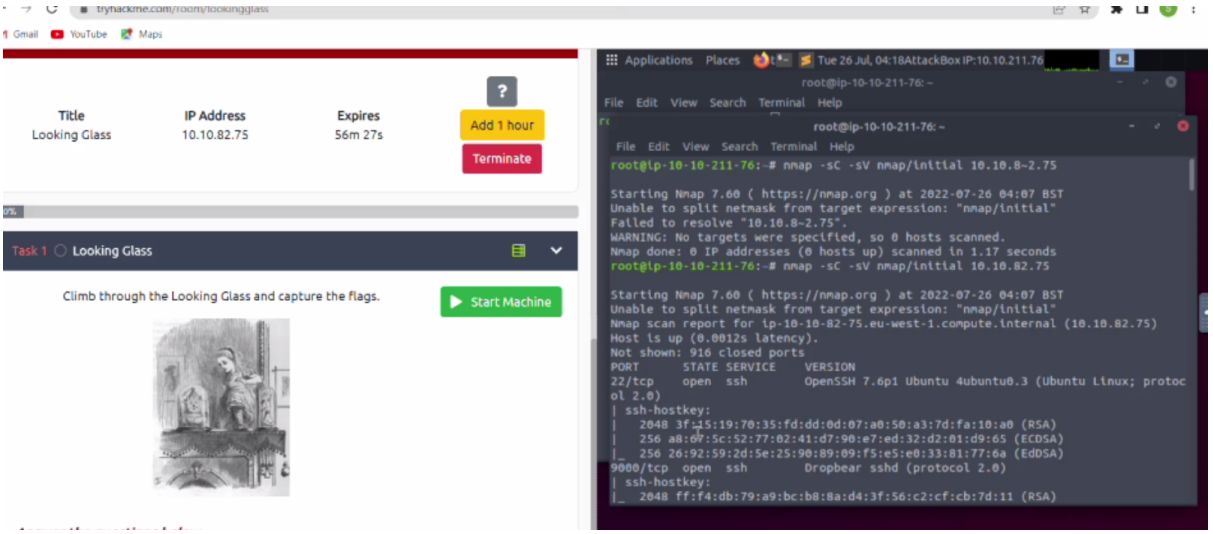
1. Enumerating



Tools Used: NMAP, Reverse shell (nc), PHP
Thought Process and Methodology and Attempts:

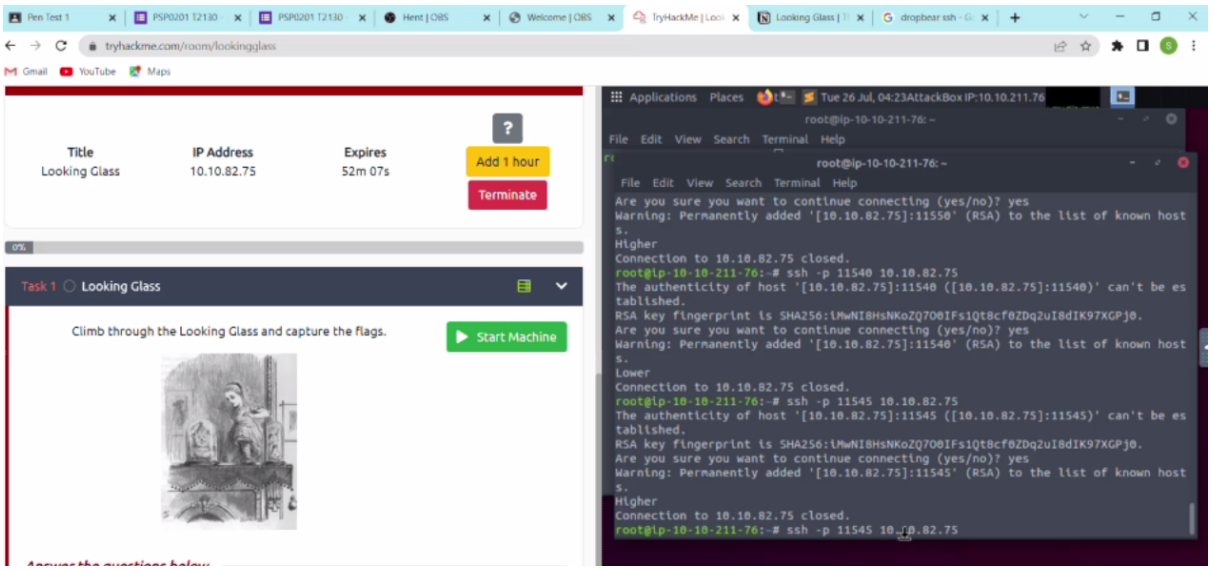
The first thing I do is launch a TCP Nmap scan with the following options against the 1,000 most popular ports

- -sC to run default scripts
- -sV to enumerate applications versions

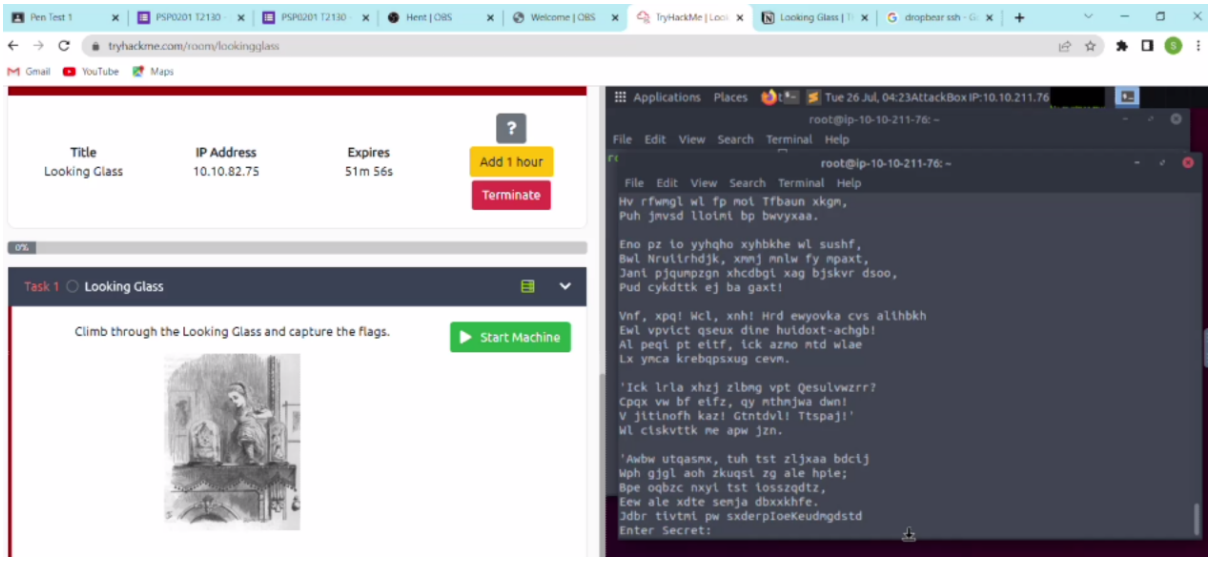


The scan has located SSH port 22 and a significant number of other SSH-using ports starting at port 9000. Using the -p- flag to do a scan and list all open ports: I google and understand the remaining port belongs to dropbear which is an ssh client as well.

2. Initial Foothold

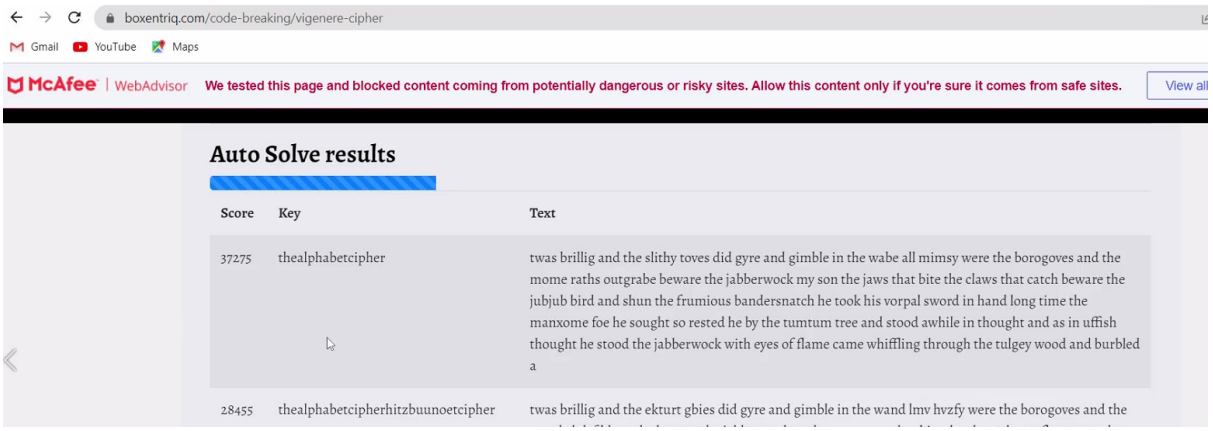


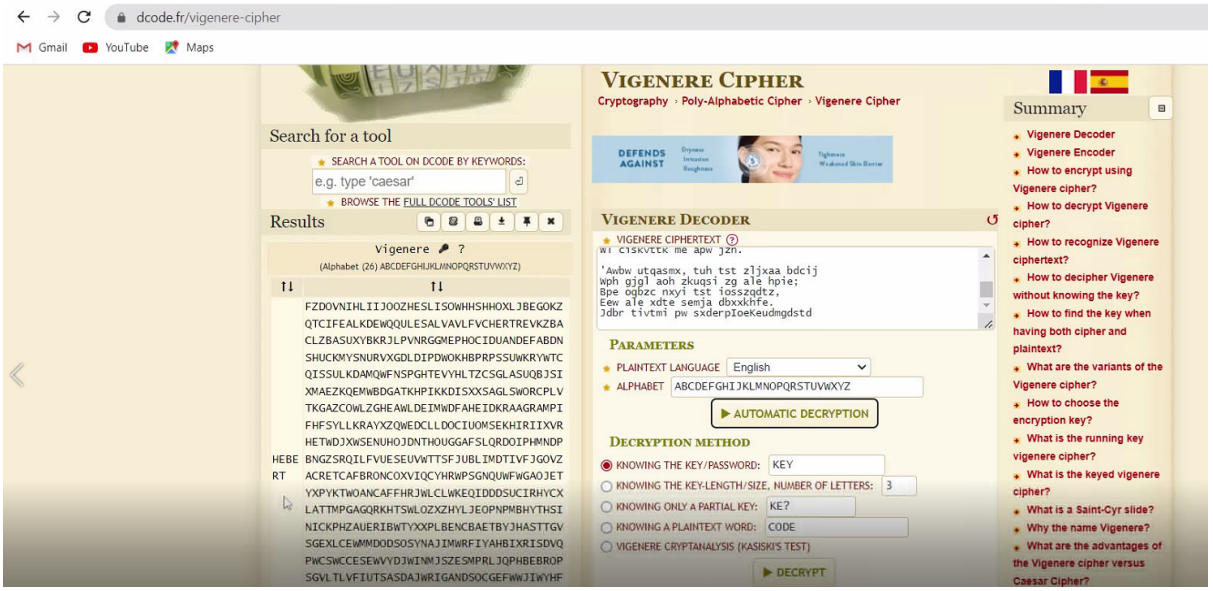
So, I quickly try to check access the dropbear port and its give weird respond as higher and lower while im putting the ports.



So I assume it's responding based on the correct port with the port I have entered. So I try to match the high and lower as minimum as possible. When a connection is made to port 9850, it responds with the following riddle.Its look like some poem with the wording being mixed. And I understand, if I am able

to solve the riddle, it's asked to enter a secret. So my next hunt to solve the riddle and Mr google help me out.

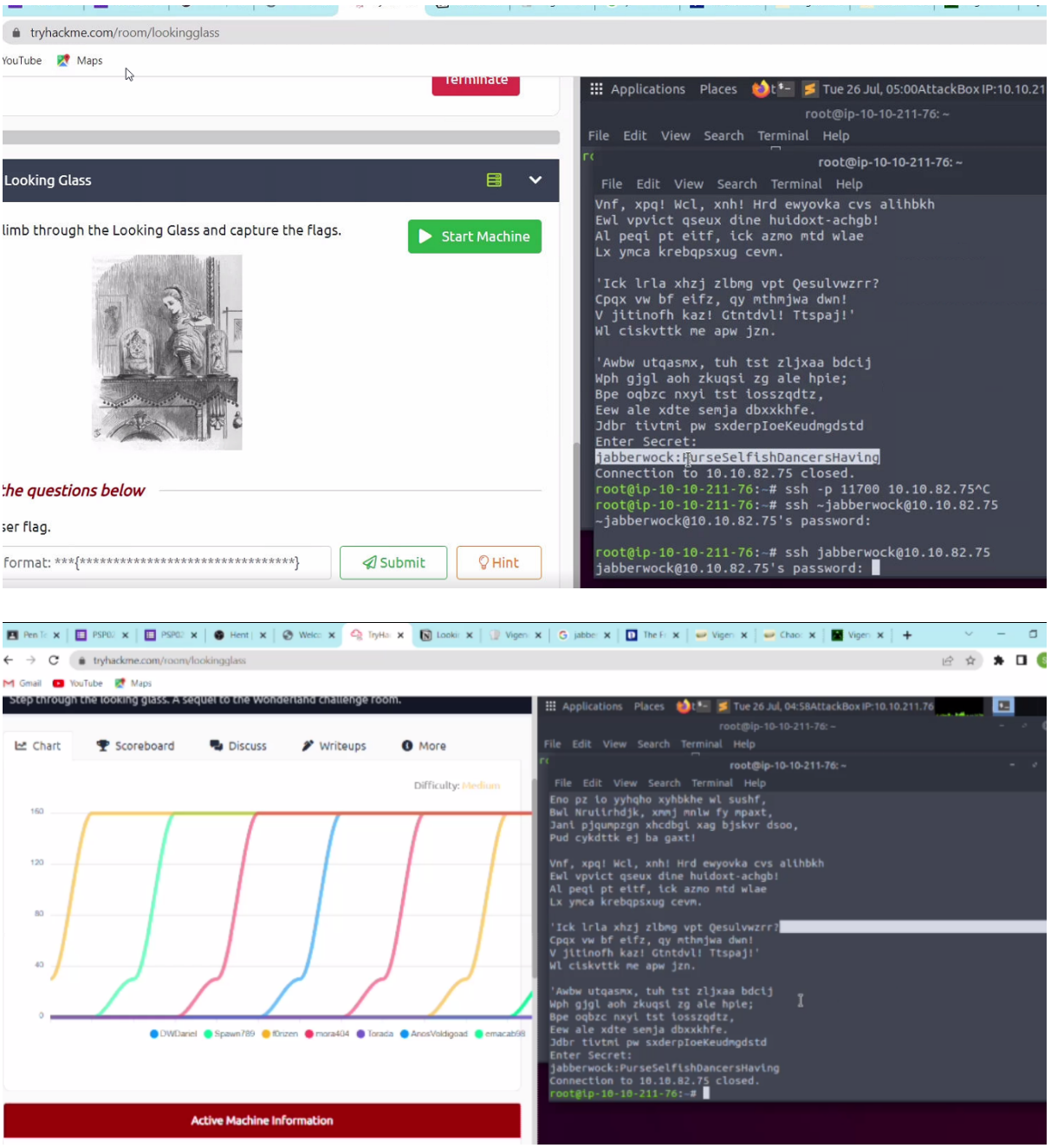




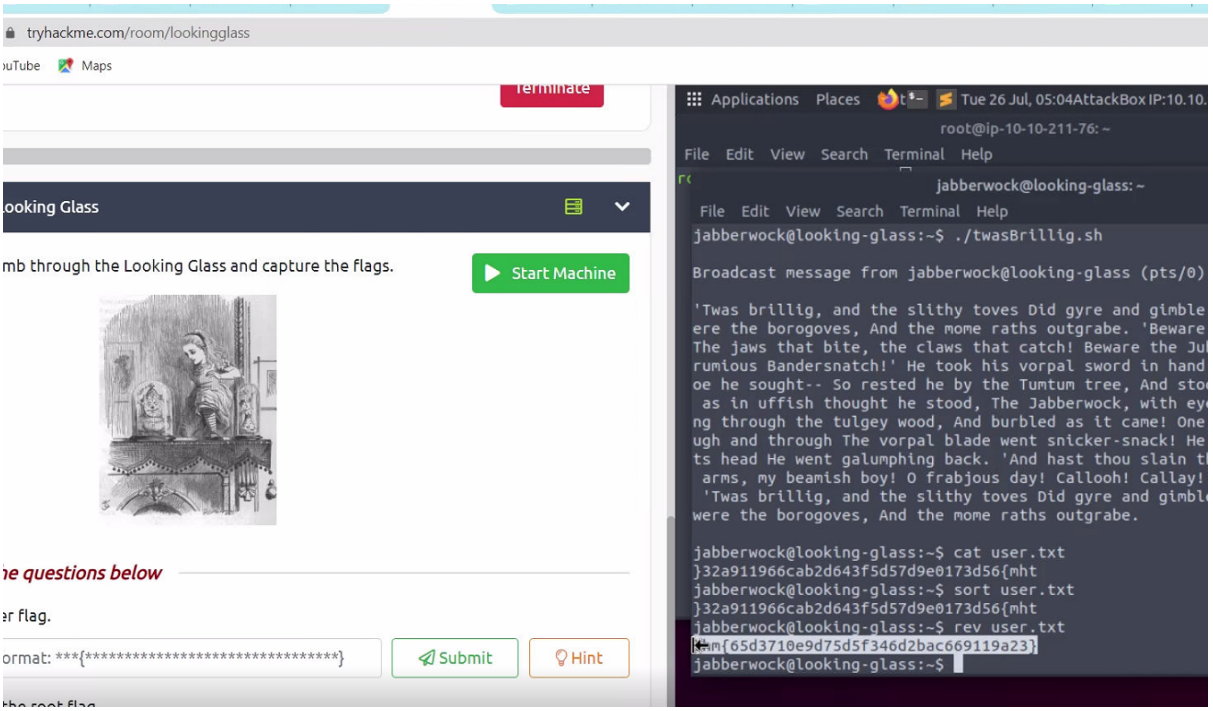
After a struggle of a few hours. I managed to sort out the riddle from the websites called boxentriq and dcode.fr.

Jabberwocky looks to be a key wording to sort out this riddle.: Then it gives another key called the alphabet cipher.

Once I enter, it sorts out the full details and I manage to get the secret key!

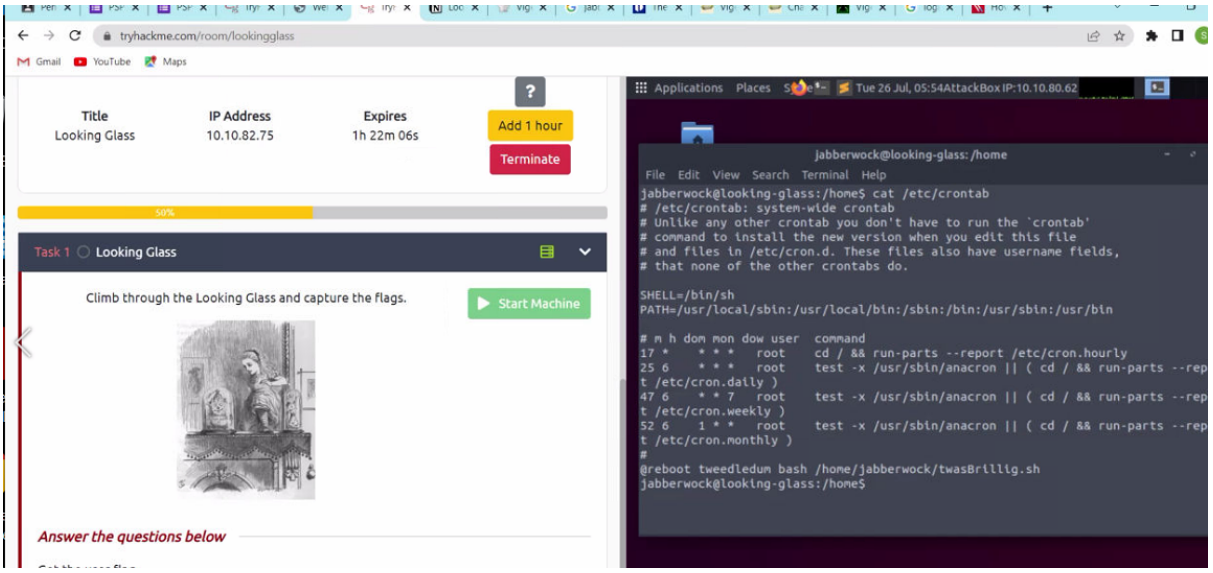


I received a password for the user jabberwock by entering the secret. With this, I access SSH as usual . I manage to sort the first flag from the user but its reverse format.



So I have to use the rev command to get it right and paste it on the flag. I managed to sort out the first flag and now the next step for the root flag!

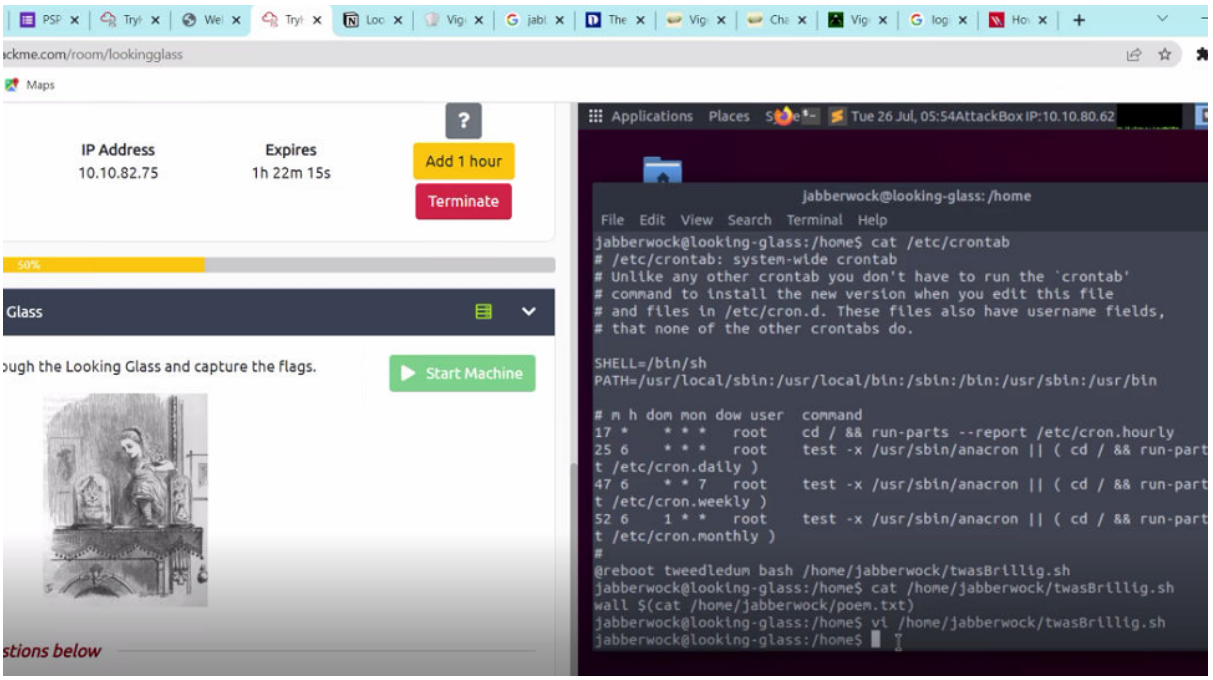
3. Root Privilege Escalation



I was checking the users rights and any loopholes to become root users. Unfortunately, my user right only allows me to reboot the server. But I saw, there is script will be run when the server is rebooted. So I was thinking of putting the

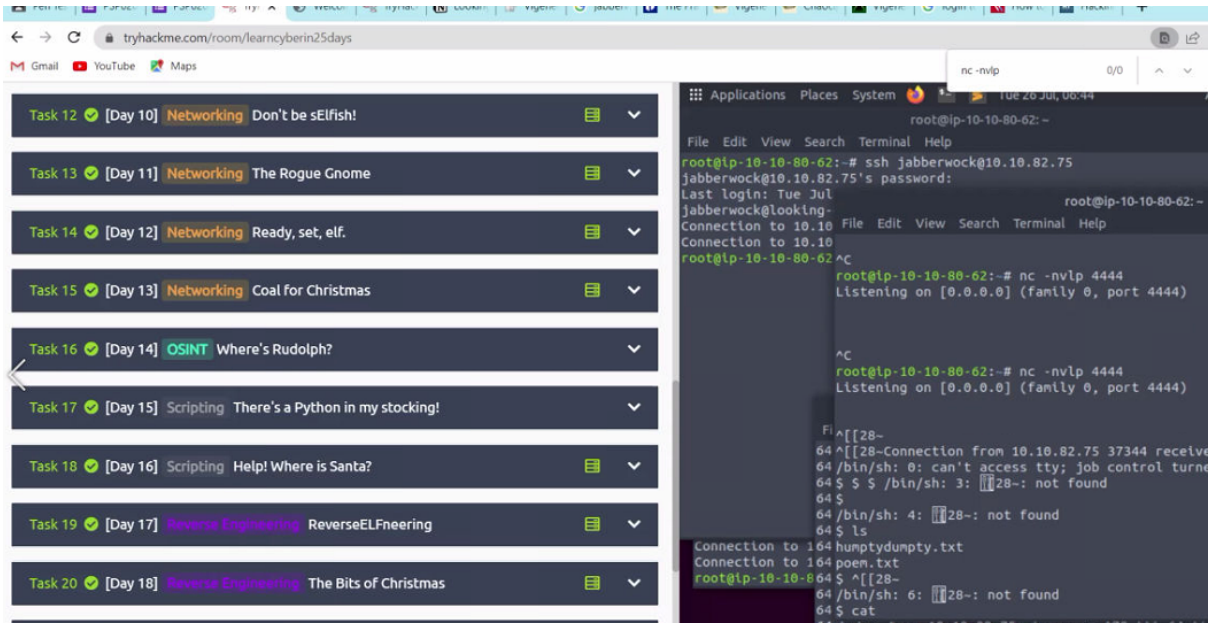
reverse engineering python script to login as root using the nc command.

So I found a command to enter on the script to listen in port 4444 from my attack box and I rebooted the system to get auto login.

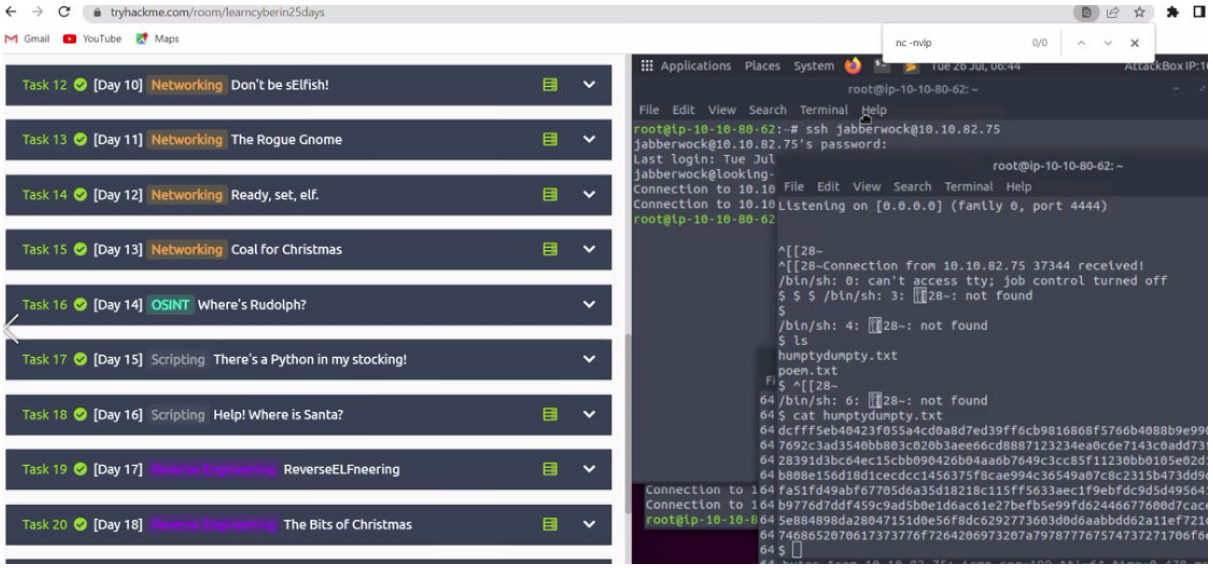


Unfortunately the password for the jabberwock users has been changed. It can't login with the same password. So I have gone through the same method to get the password and login to the system again.

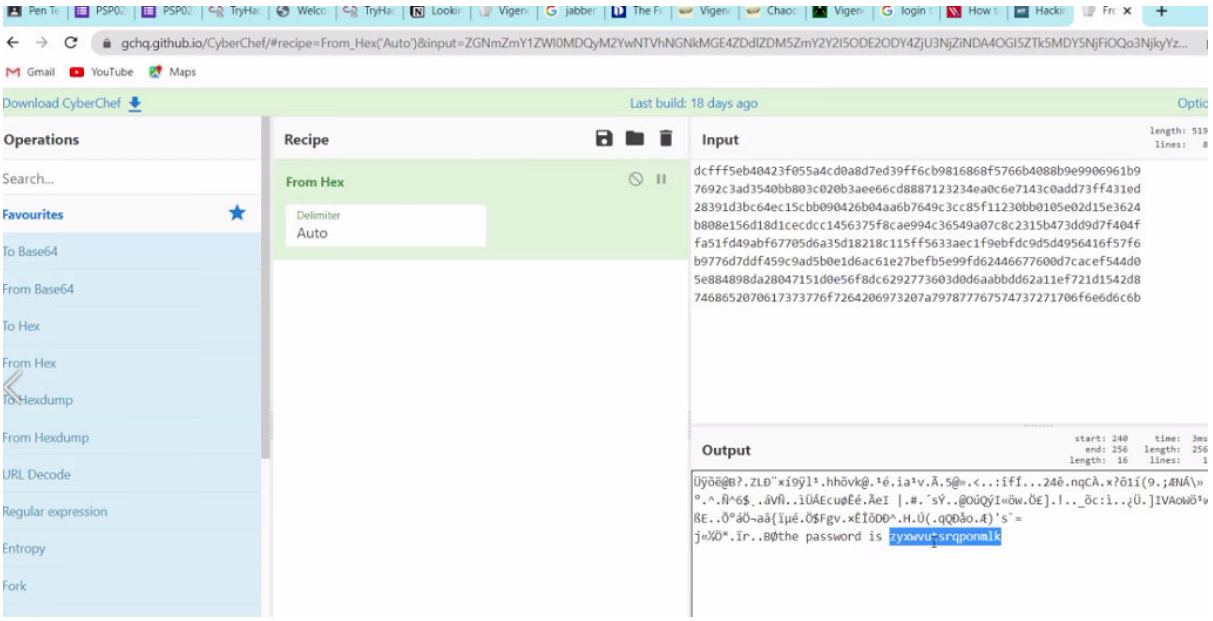
At last i managed to login to the system using reverse bash shell script.



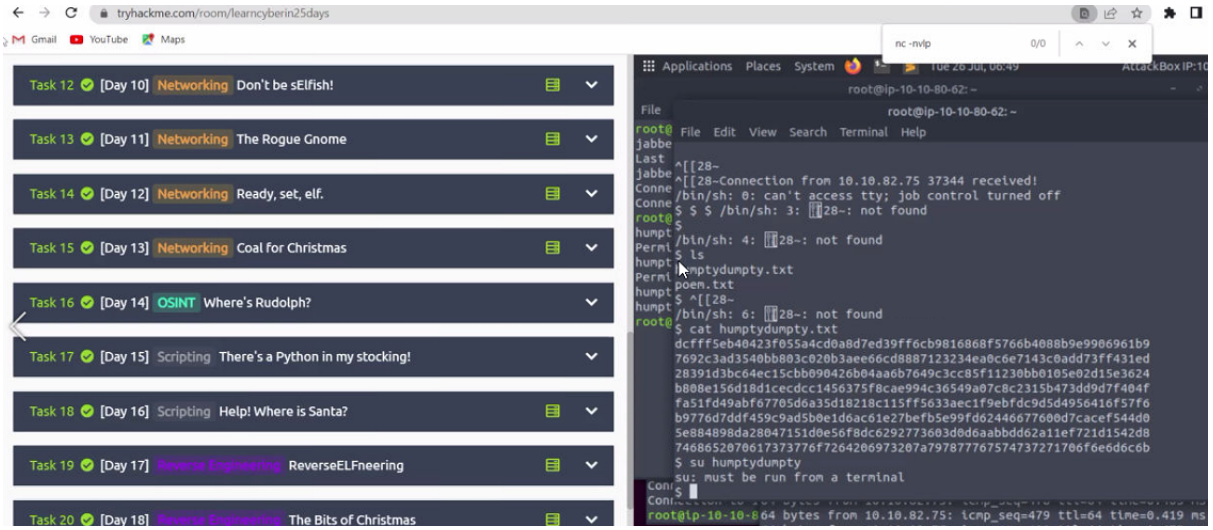
Get some guidance from the THM 25 days course and apply the same for reverse bash script.



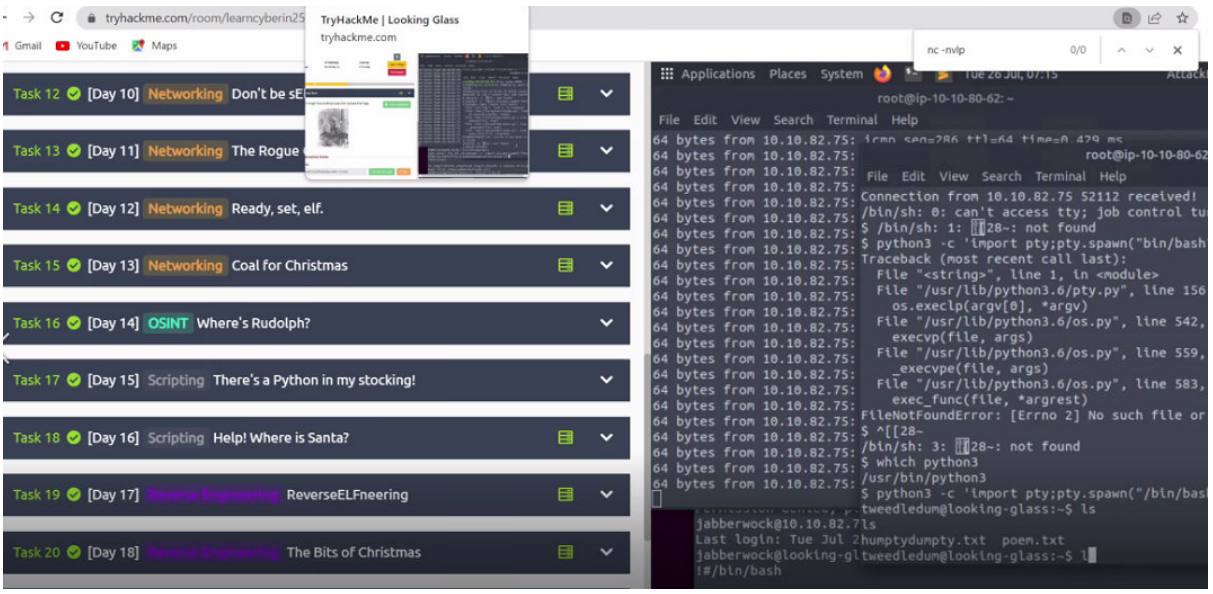
Once I logged in I saw there is a file called humpty dumpty. I used the file to crack using cyberchef and manage to get the password for a humpty dumpty user.



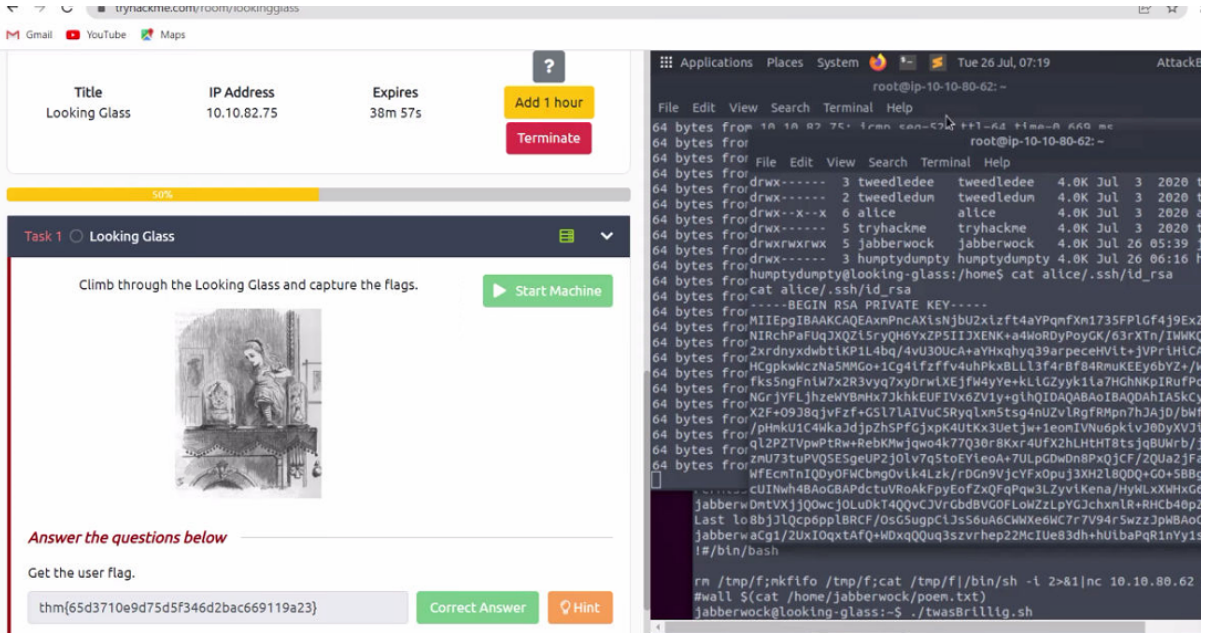
it does not allow me to login as users without bash. Either it does not allow me to login from my attackbox directly using username and password.



Then I used the python command to make this as bash script.

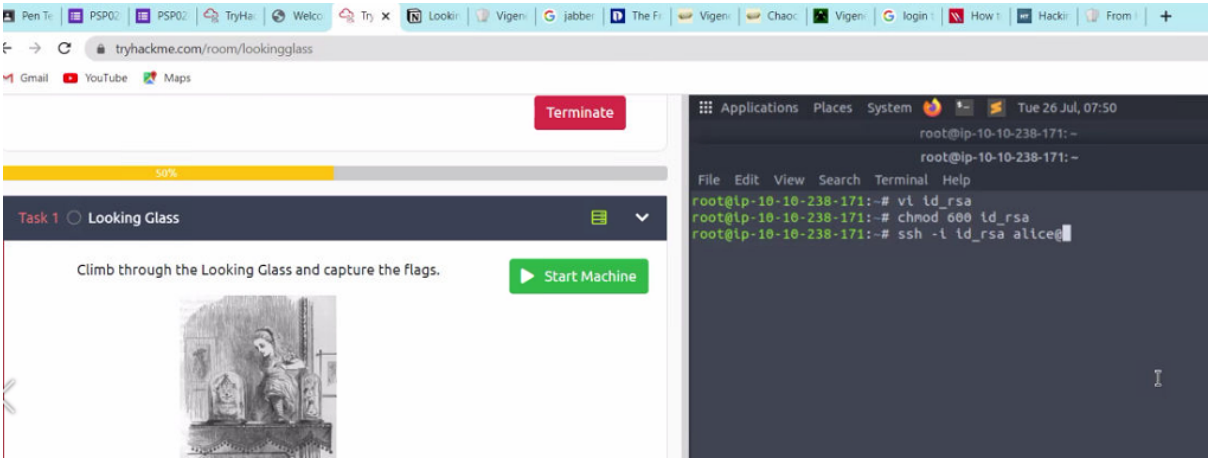


Once i login, i checked, i have the access for the users alice rsa ID. So I need to login as Alice to check the file inside her ID.

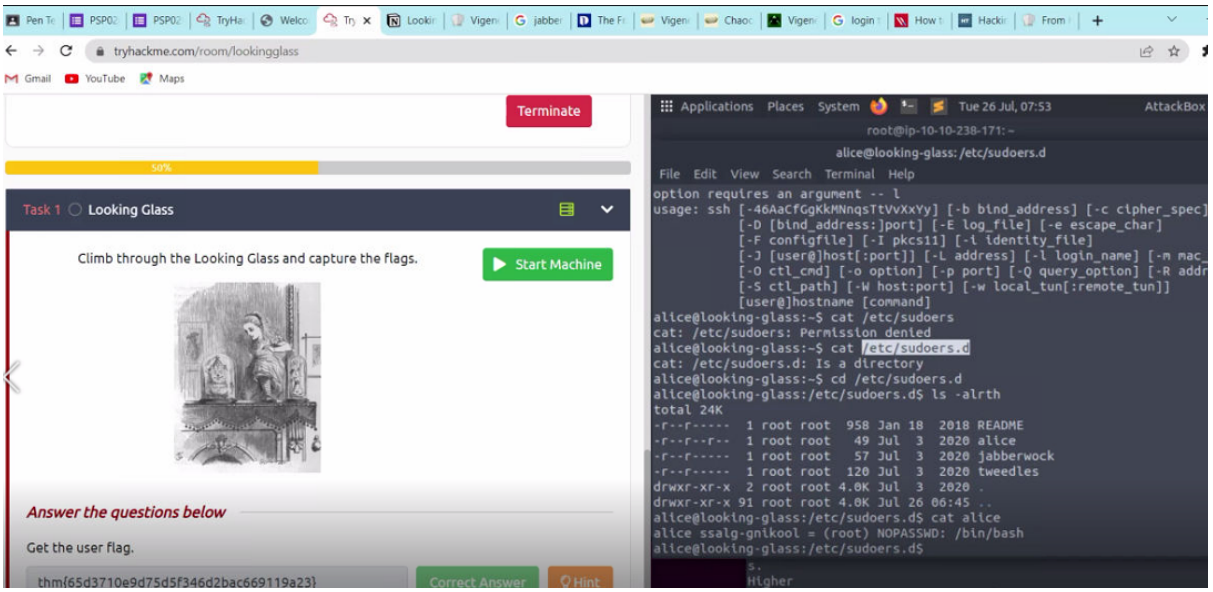


I notice that I have access to a private key to login to servers without a password.

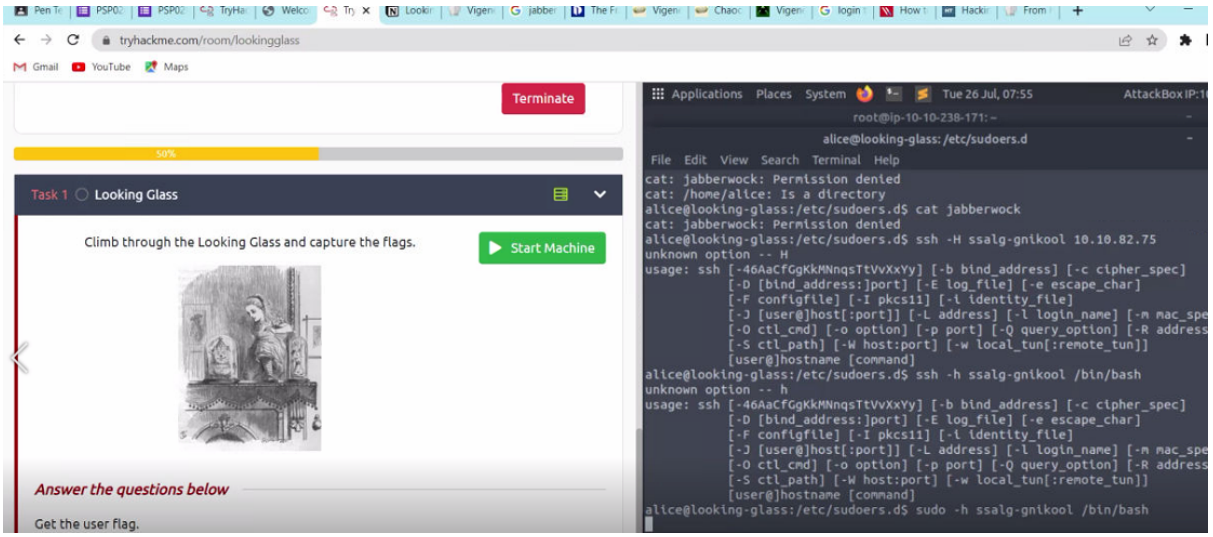
I download the file to attackbox and use that key to login to servers.



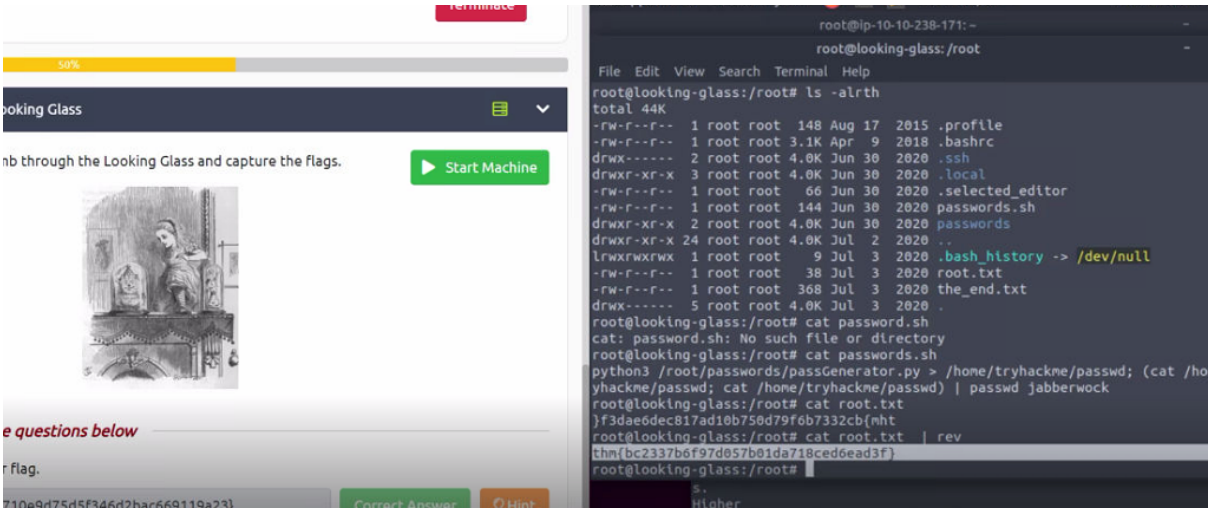
To gain root, just one more privilege escalation remains! However, there is only one sudo command I can execute as Alice. I checked the file "/etc/sudoers.d" to locate this command.



Then, I switch users to root, it does not allow me and asks for password. I checked the sudoers file and noticed there is a reverse format of the hostname. So I have to use the sudo -H command to login to bash. It's unable to resolve the host but I manage to login as root.



Whoah! I managed to enter the server as root!. As a final step,I login to servers and get the flag. It's on rev order as well, but i manage to use command and make it right!



CONTRIBUTION

ID	NAME	CONTRIBUTION	SIGNATURES
1211101693	Savitha Murugumunisegaran	Launch a TCP Nmap scan	Savitha
1211101693	Savitha Murugumunisegaran	Solve the riddle from the website called boxentriq and dcode.fr	Savitha
1211101693	Savitha Murugumunisegaran	Use the reverse engineering python script to login as root using the nc command	Savitha
1211101693	Savitha Murugumunisegaran	Enter the server as root and login to servers and get the flag. Using rev order and use command to make it right!	Savitha

VIDEO LINK:
https://www.youtube.com/watch?v=Kw8CWJNt0CY