PENTEST
ROOM A
F4urDeveloper

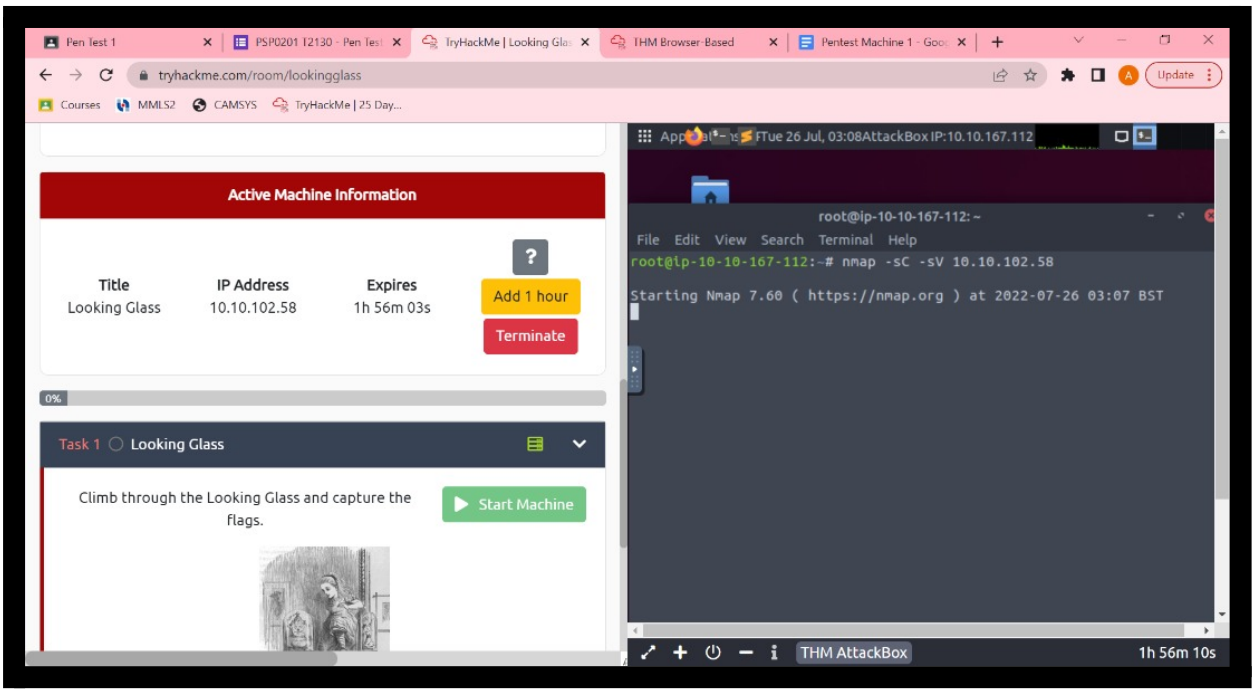
ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

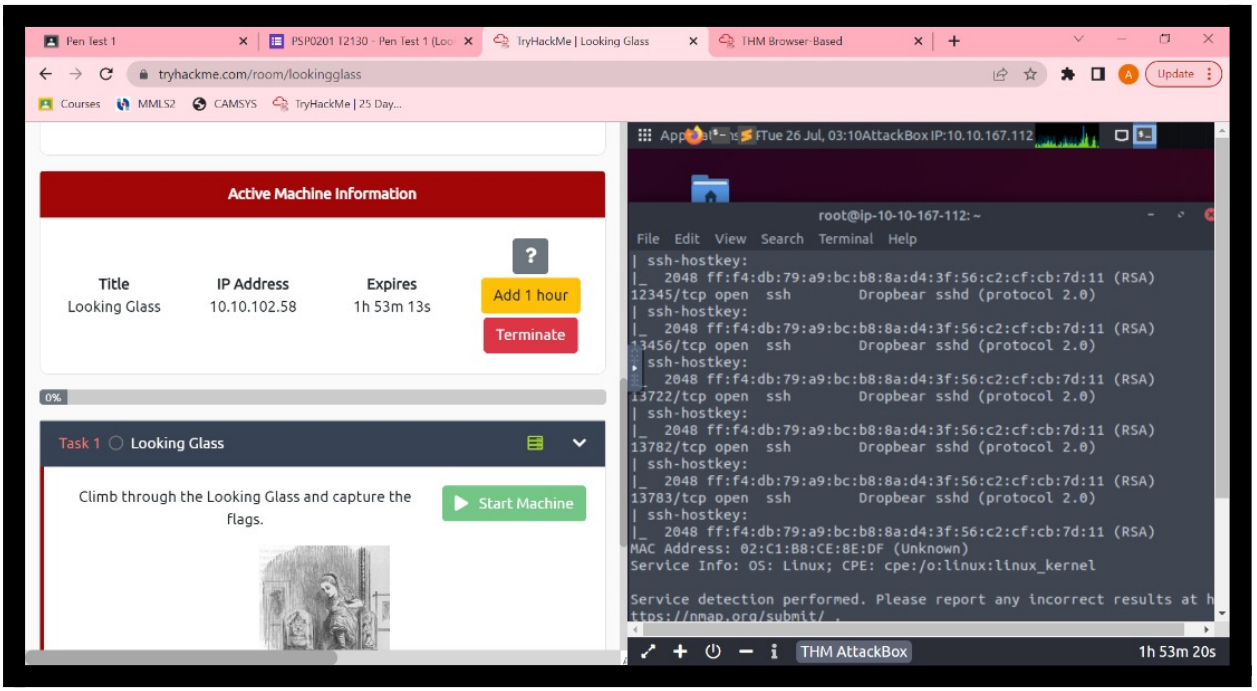
Recon and Enumeration

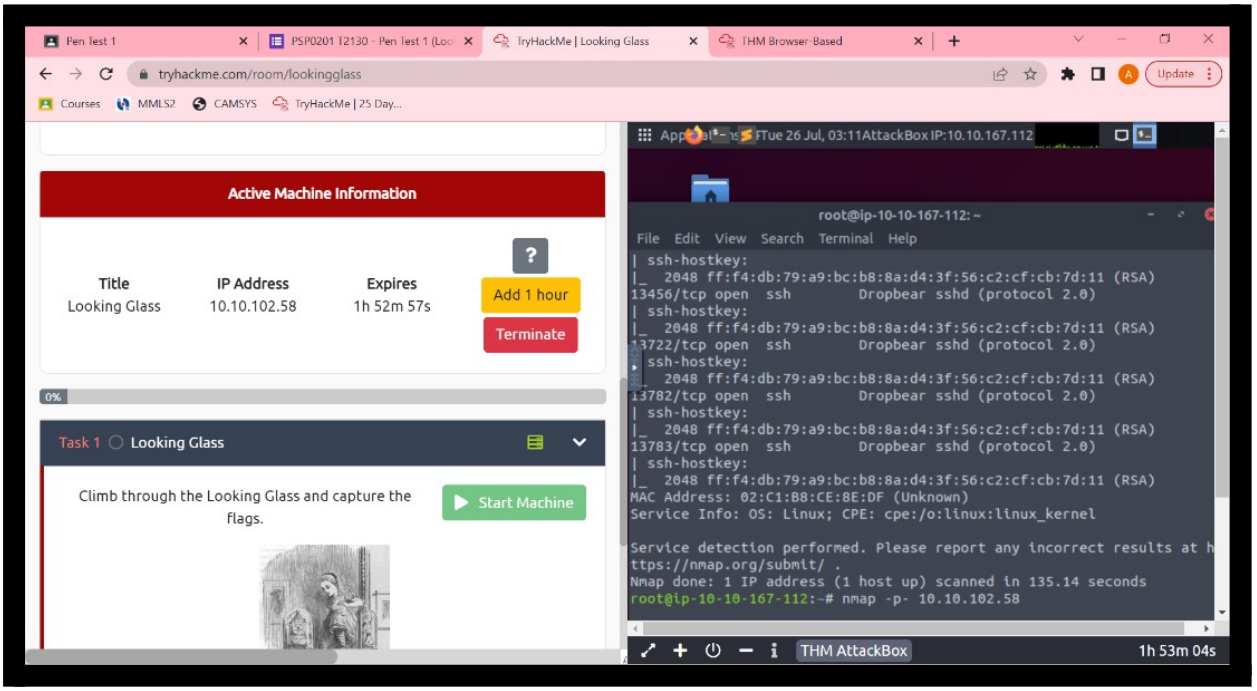
Member(s) involved: Alia Maisara Binti Shahrin

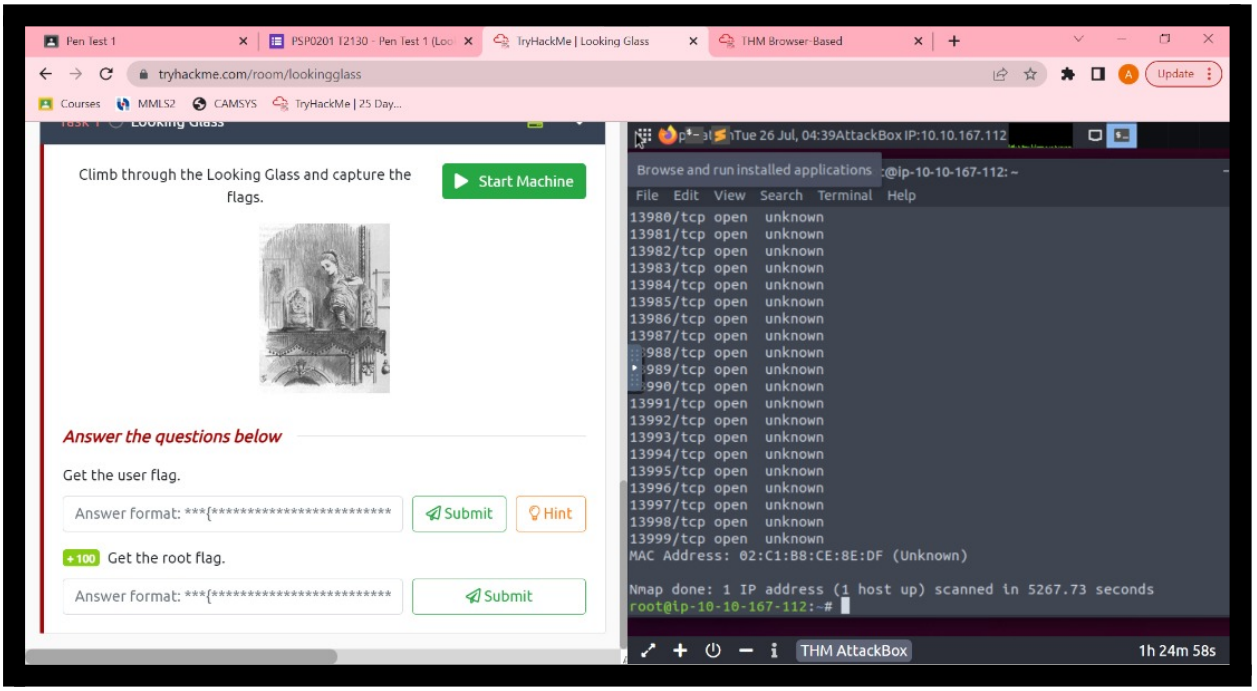
Tool(s) used: THM Attackbox, Google Chrome

Thoughts Process/Methodology:

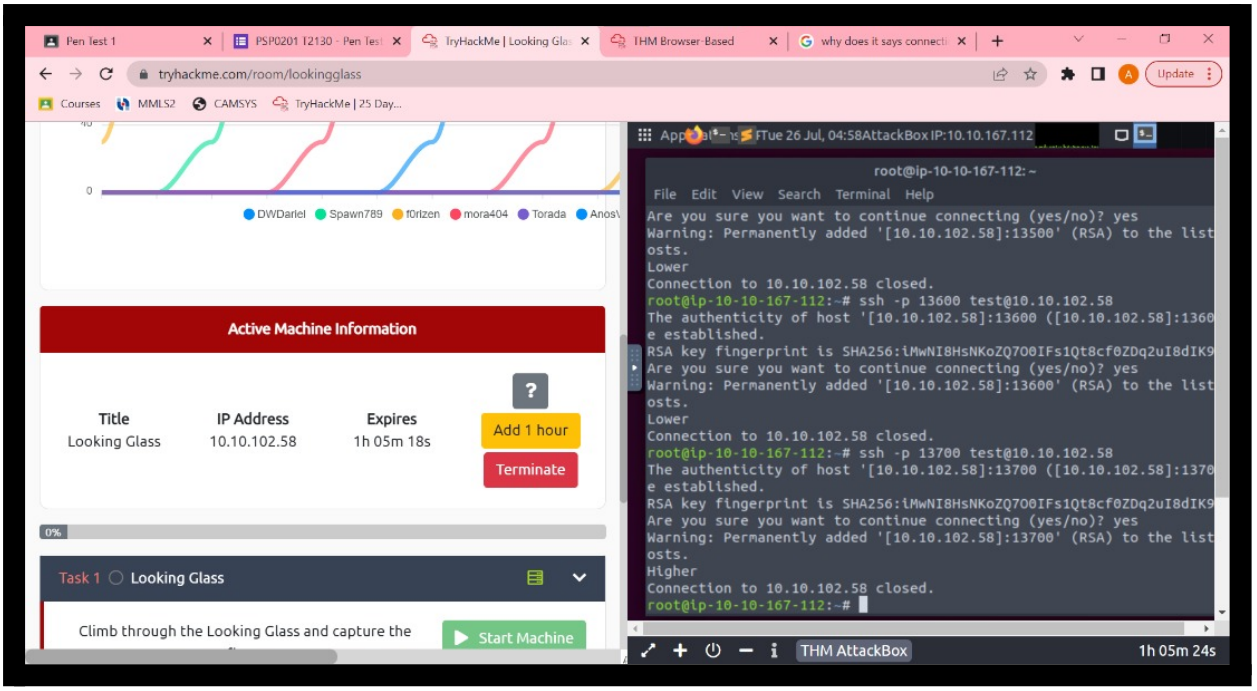




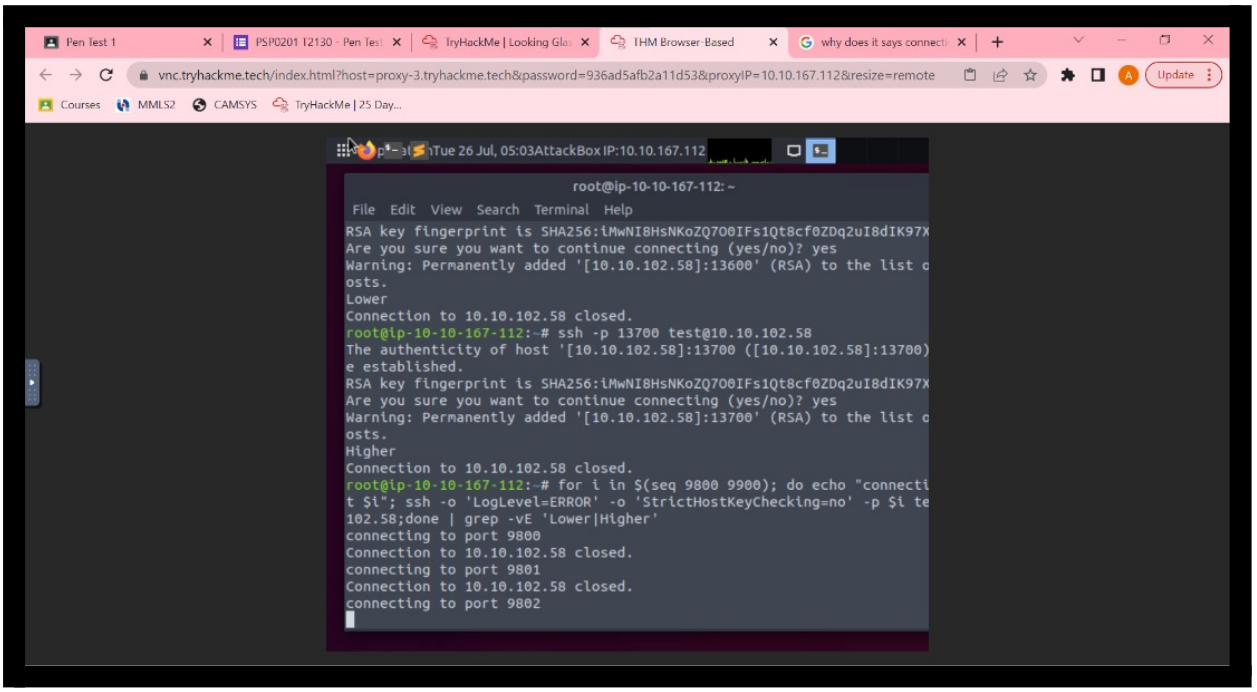




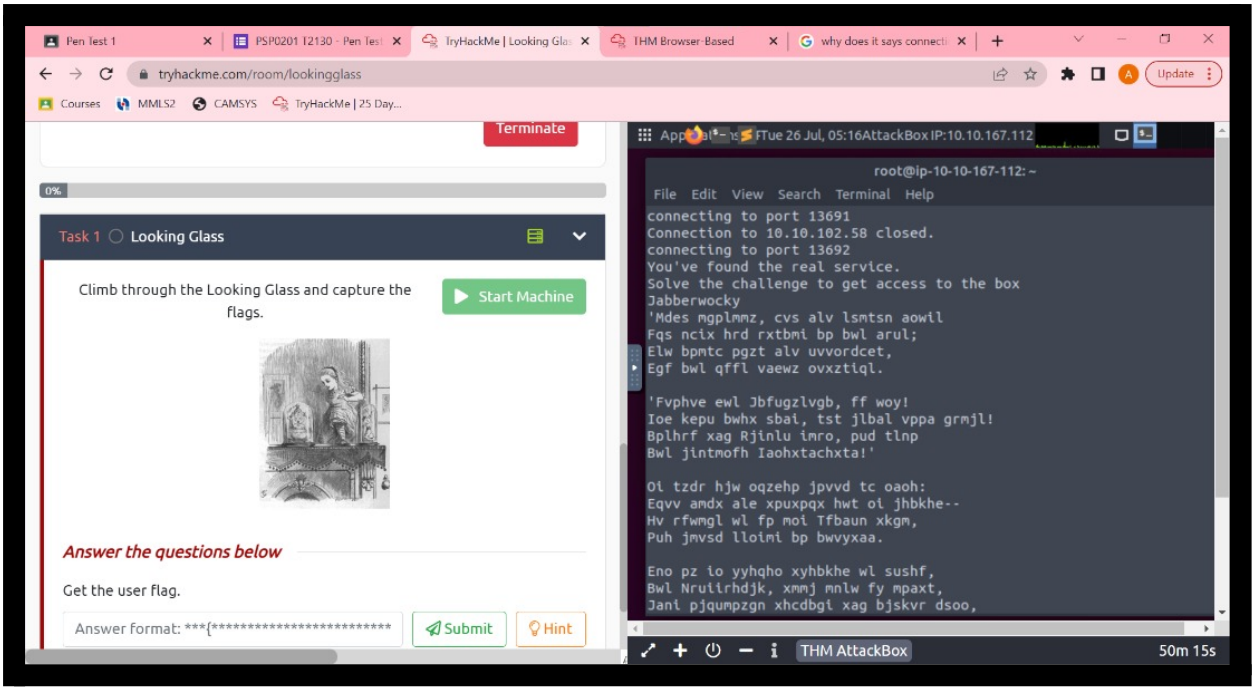
In order to gain access to the ports contained inside the server, Alia Maisara used Nmap to enumerate the server. Doing so will reveal all of the open ports available inside the particular server.



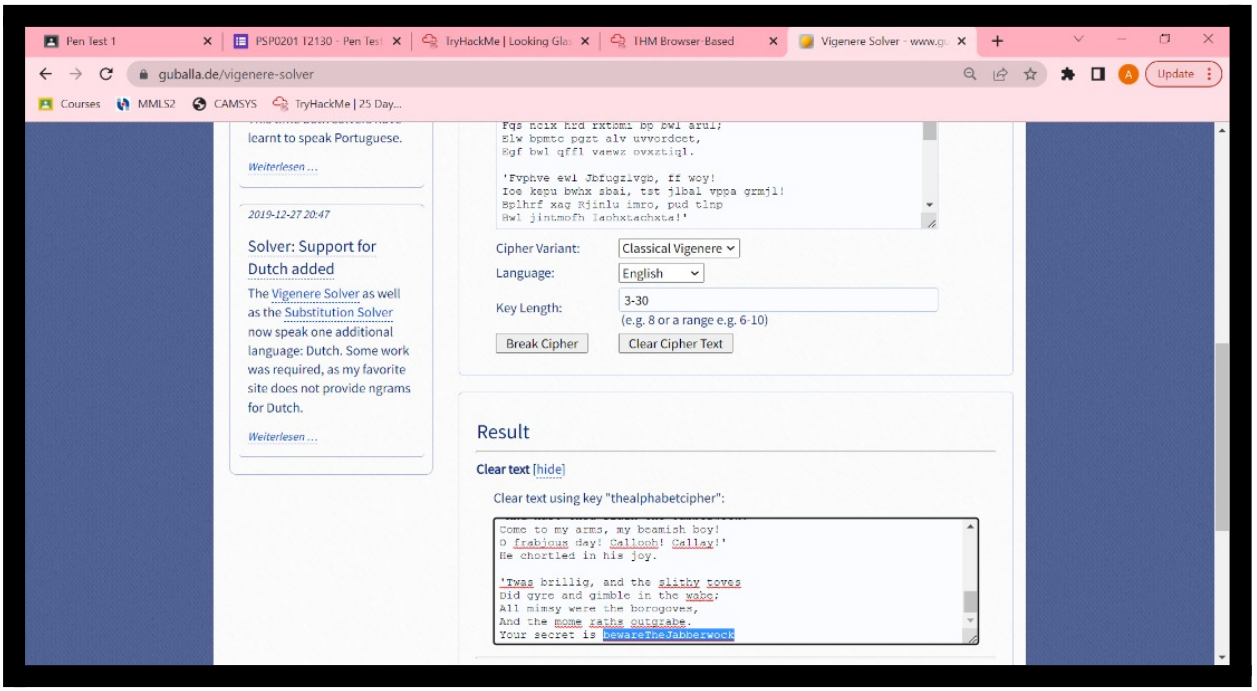
At this point, Alia Maisara had to find the specific port that contained the riddle in order to obtain the first flag. Therefore, she narrowed down the specific port as little as possible by using SSH.



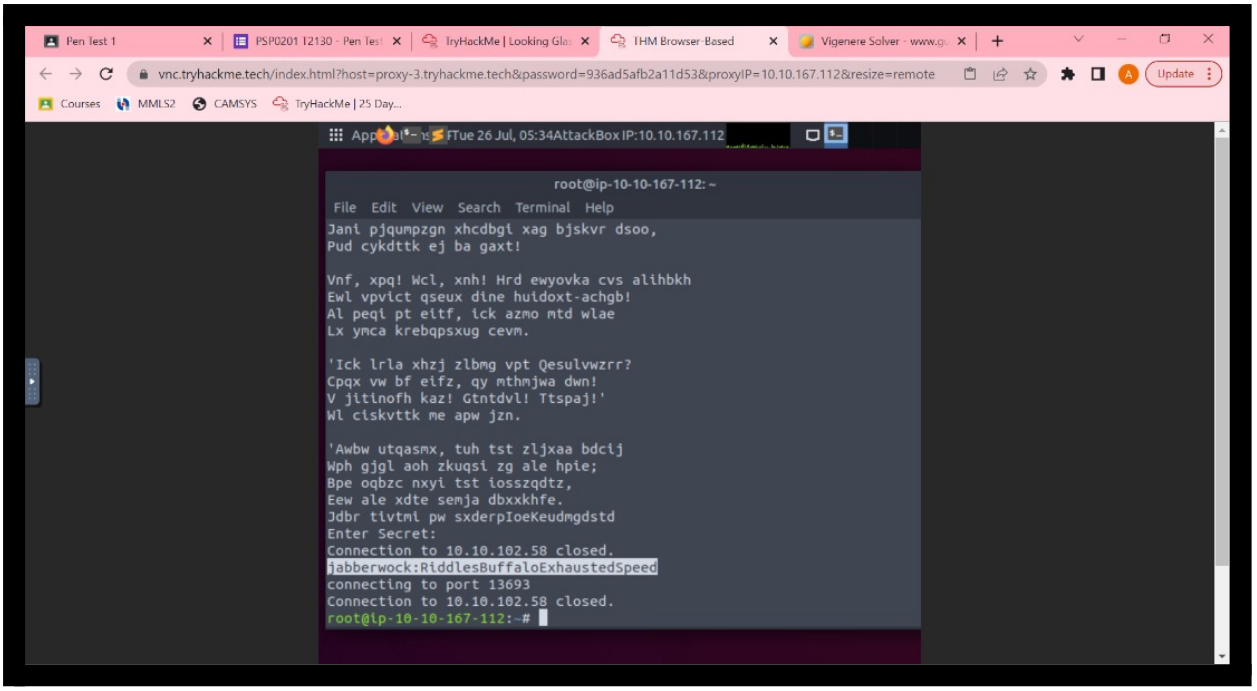
After finding the smallest range Alia Maisara could find, she used the following command in order to automatically reveal the specific port needed for this challenge.



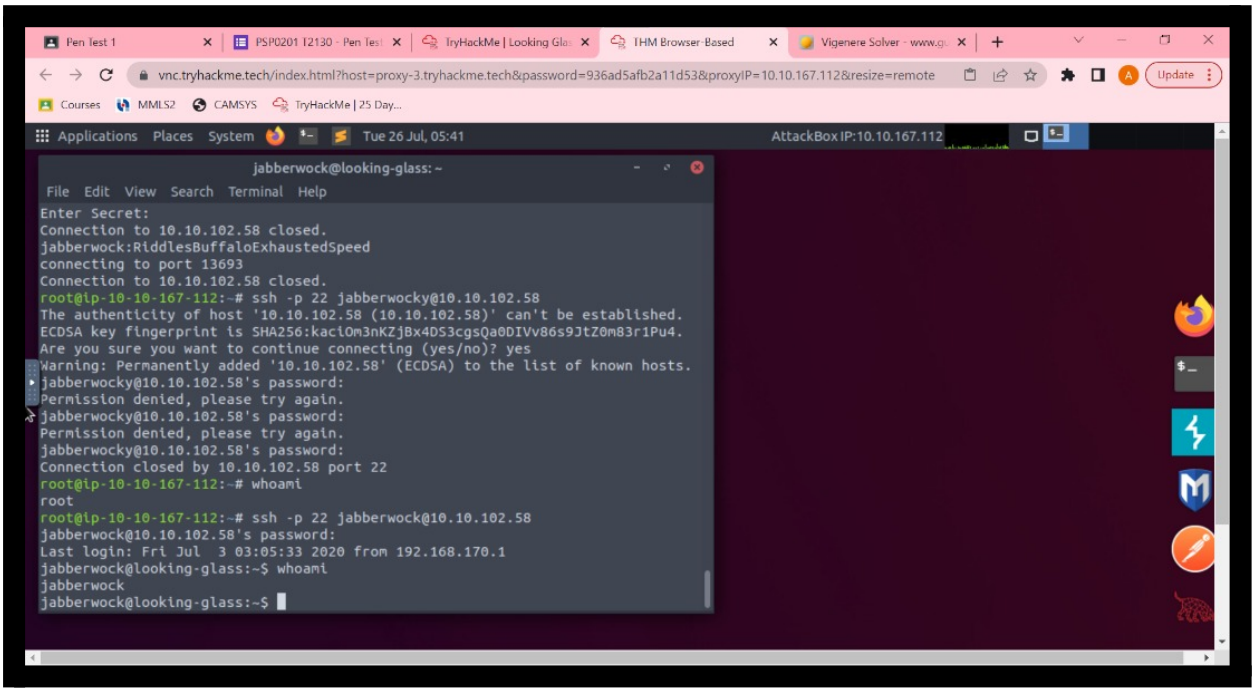
After waiting for quite a while, the correct port will reveal a riddle that would require translation in order to move on to the next step.



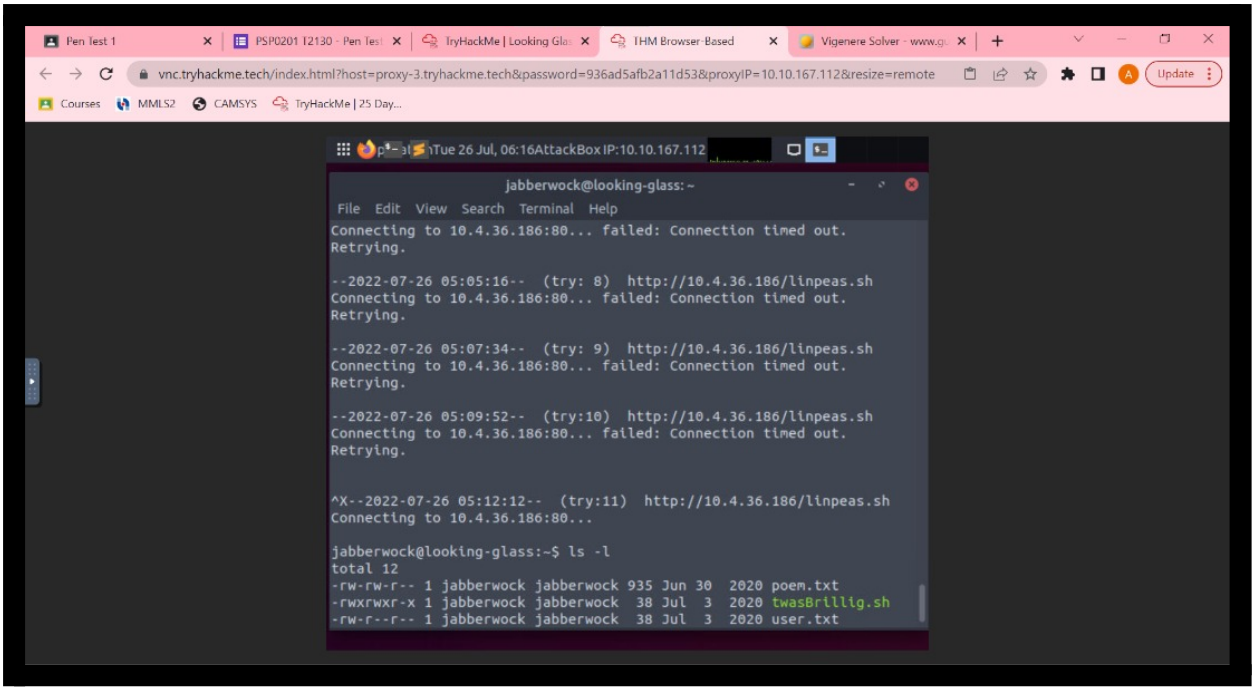
Alia Maisara translated the poem that was found on the port that was opened by using an online Vigenere decryption tool. The secret that was found in this poem is noted for our next step.



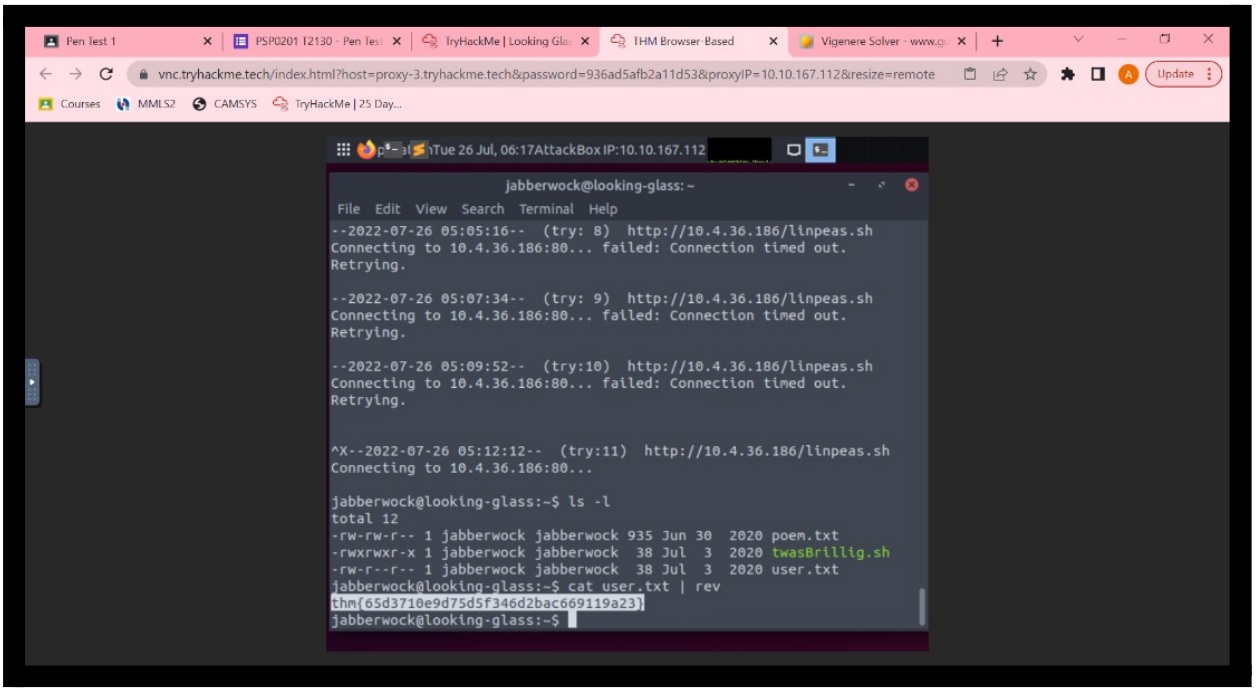
The machine asked for the user to enter the secret before allowing the user to gain access to the credentials. After Alia Maisara enters the secret, the credentials are given. It is noted that every machine has a different password after multiple attempts.



Alia Maisara logged in into user jabberwock via SSH by using the credentials that she found earlier.



In order to look at the list of contents that exists in this user, Alia Maisara used the following command and found the file named user.txt.



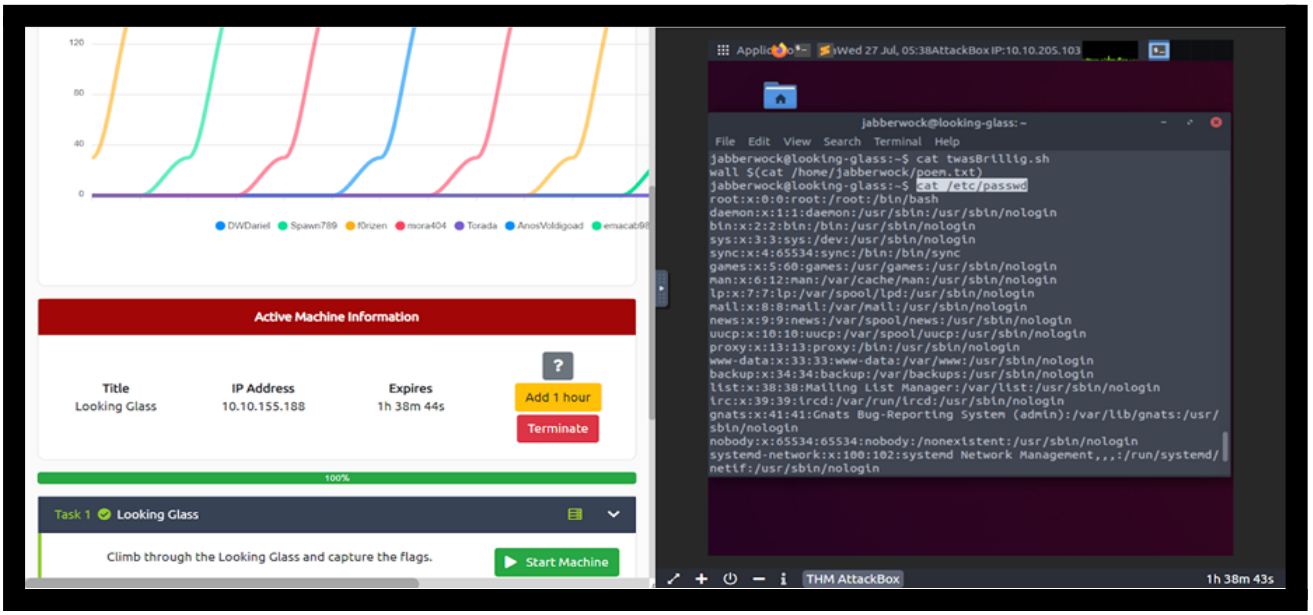
In order to look at the file content, Alia Maisara concatenated user.txt file and found the user flag.

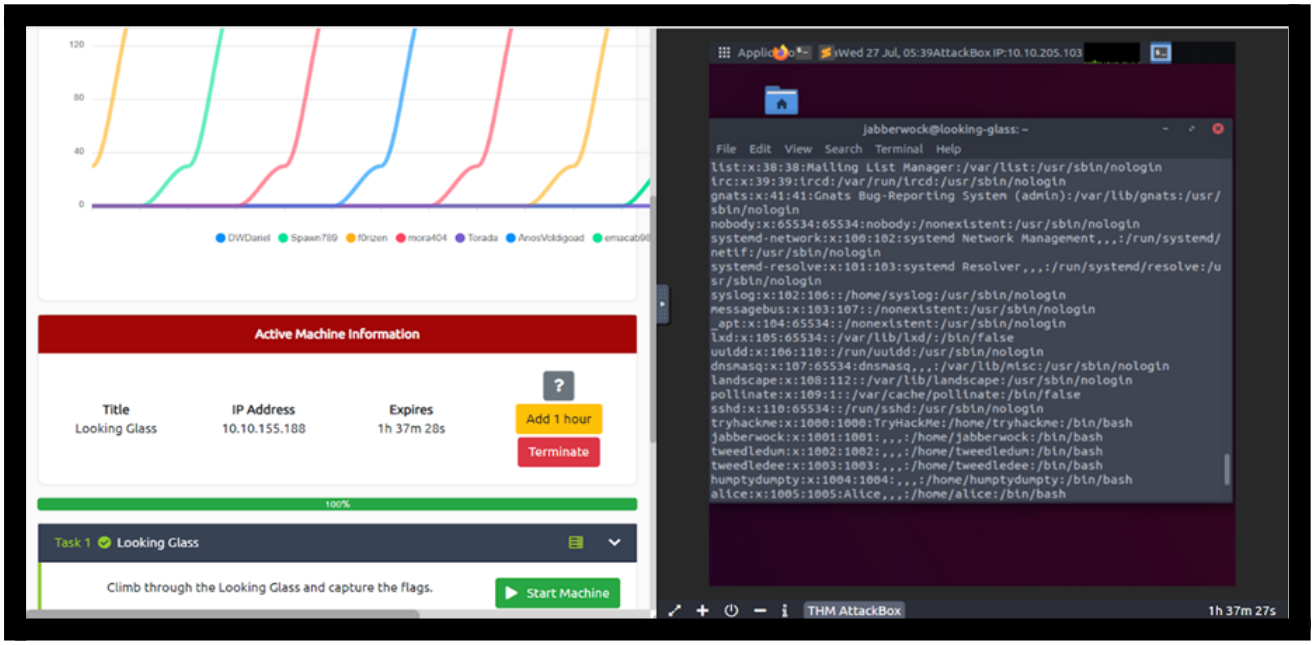
Initial Foothold

Member(s) involved: Mischelle Thanusha Julius

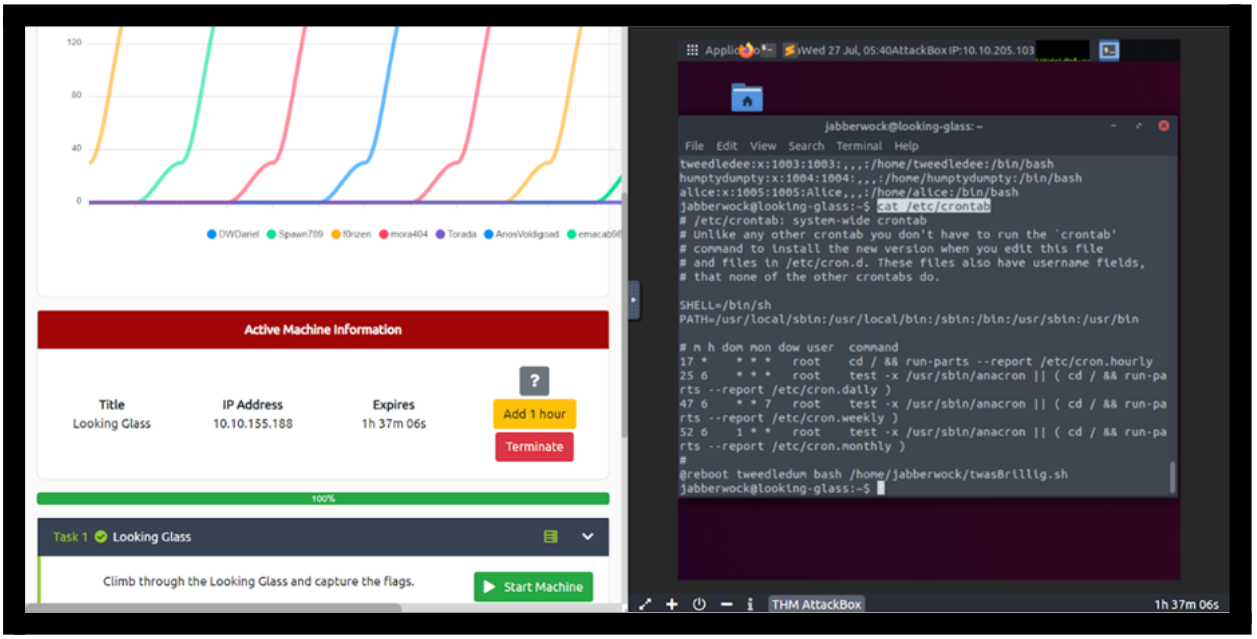
Tool(s) used: THM Attackbox, Reverse Shell Generator, Google Chrome, Netcat

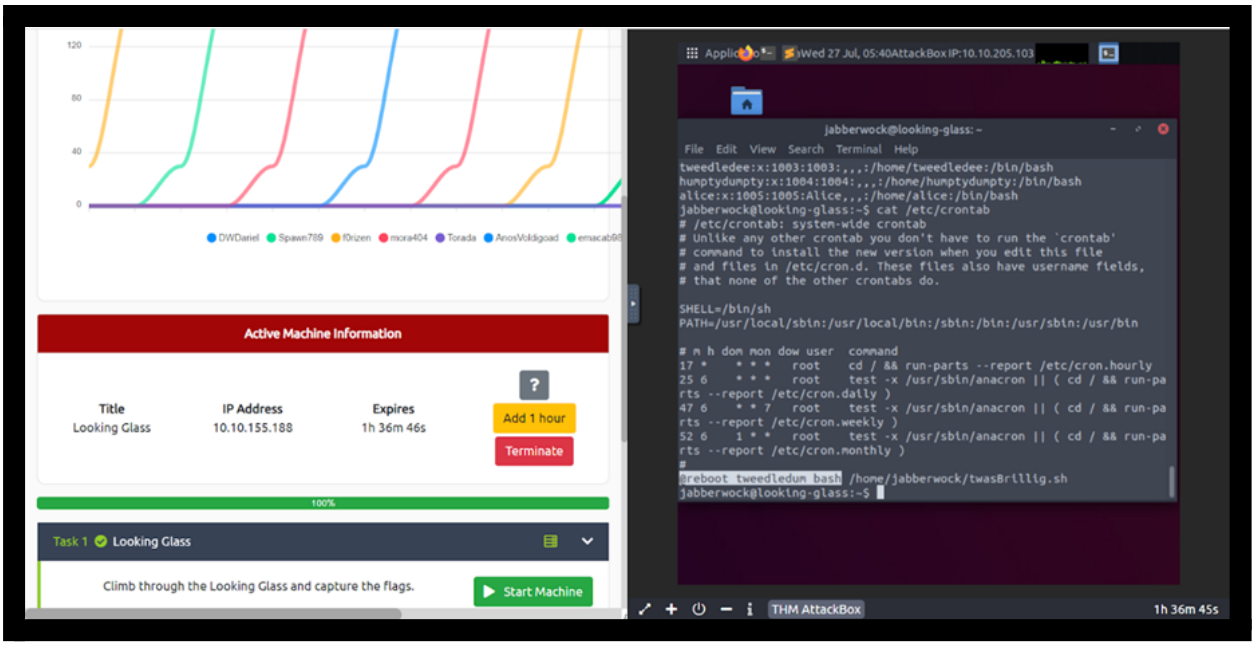
Thoughts Process/Methodology:



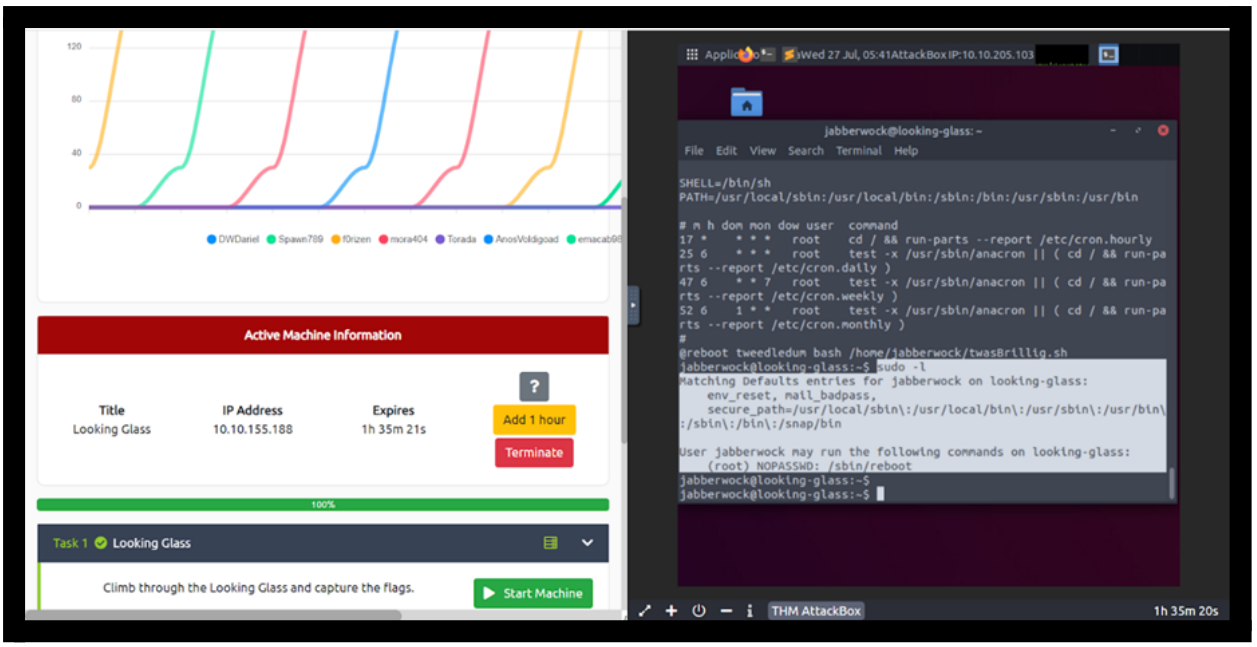


After Alia Maisara has found the **User Flag,** Mischelle can look for whether there is another file in the directory. Mischelle notices that there is a file called twasBrillig.sh. To discover who has access to the current system, the following command is used.

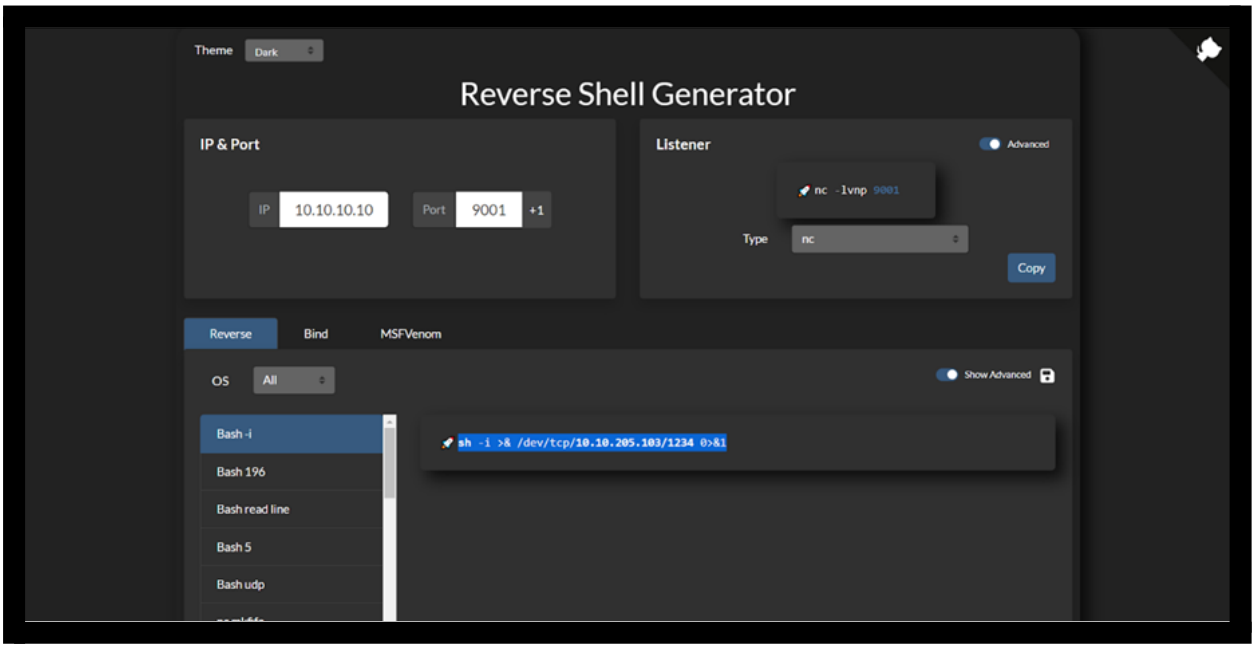




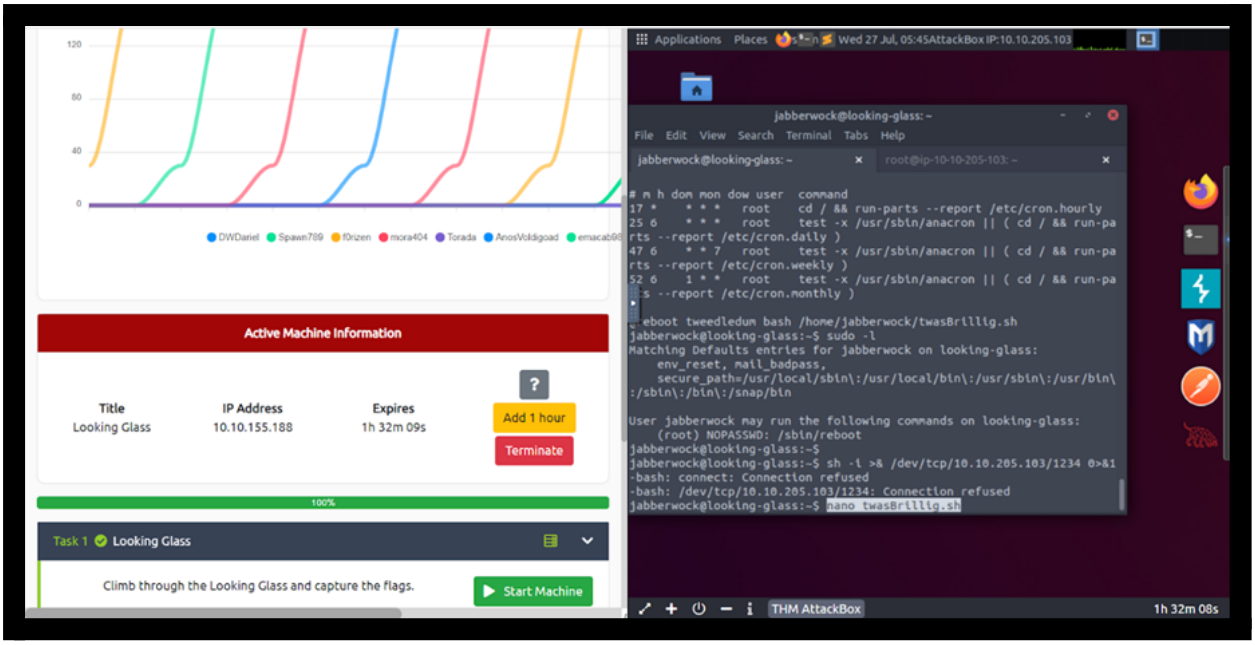
Mischelle used the Crontab command to check out the random port that is going to give feedback. There seems to be a “twasBrillig.sh” shell giving a response.

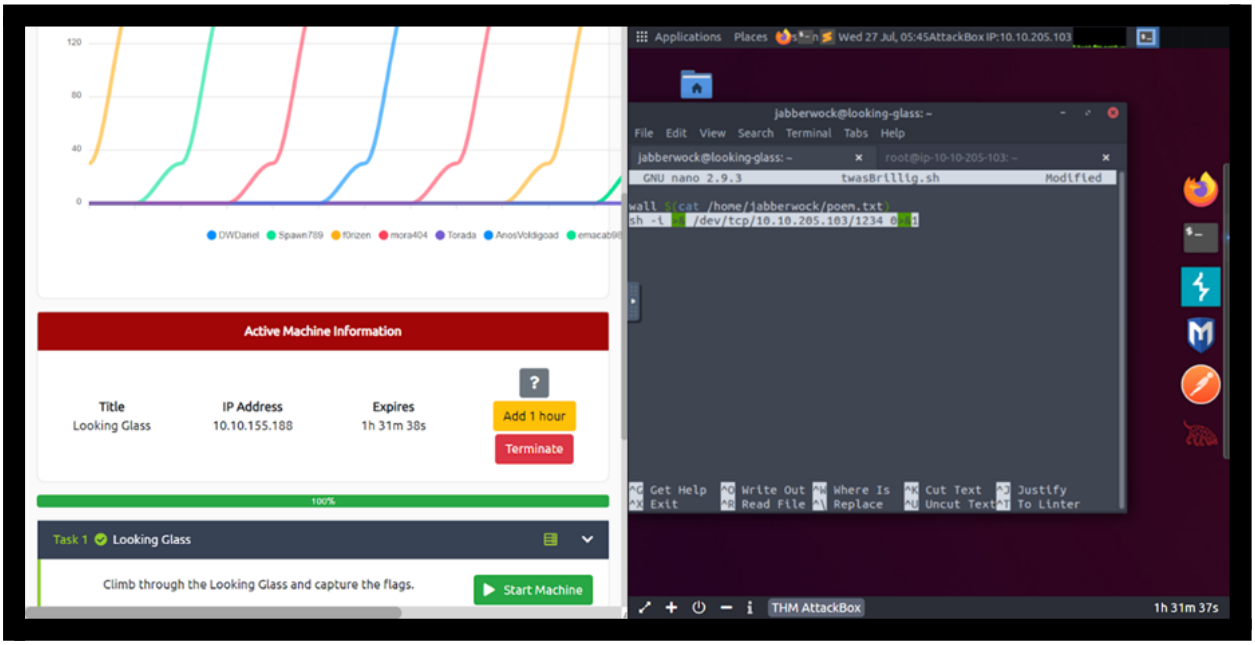


Next, Mischelle checks the lists of the user's privileges by using the sudo -l command. Mischelle can see that it does not need any credentials or password to reboot the box.

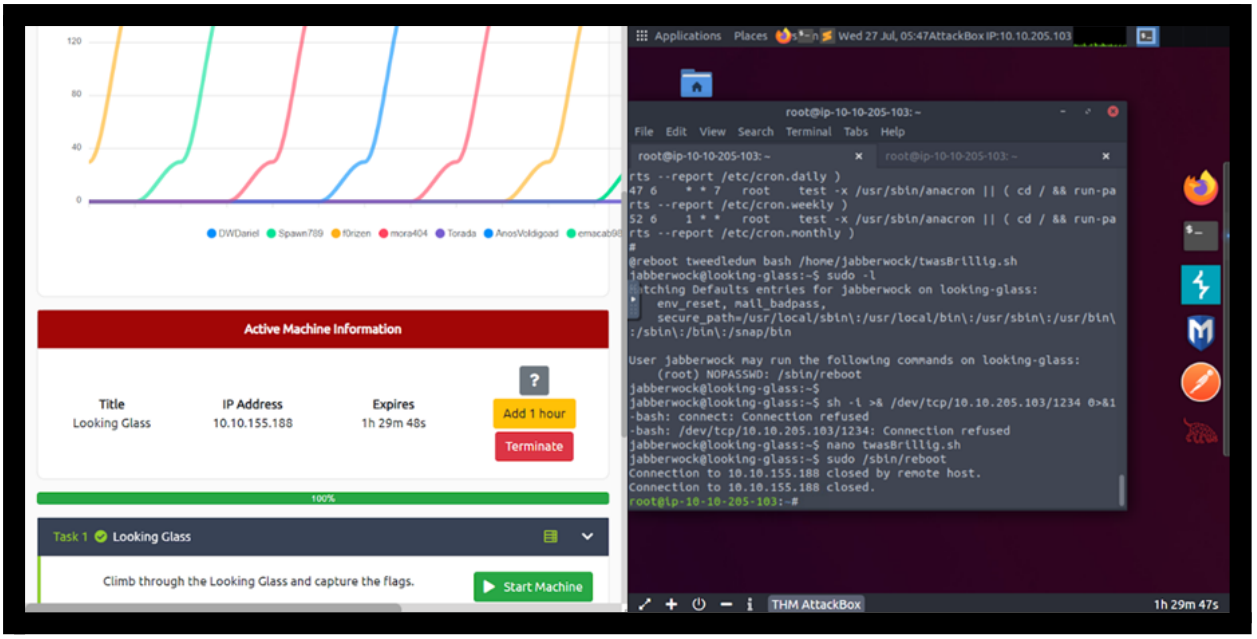


To make a connection to the attackbox machine from the server, Mischelle uploads a reverse shell. By referring to the Reverse Shell Generator, the Bash-i command is used

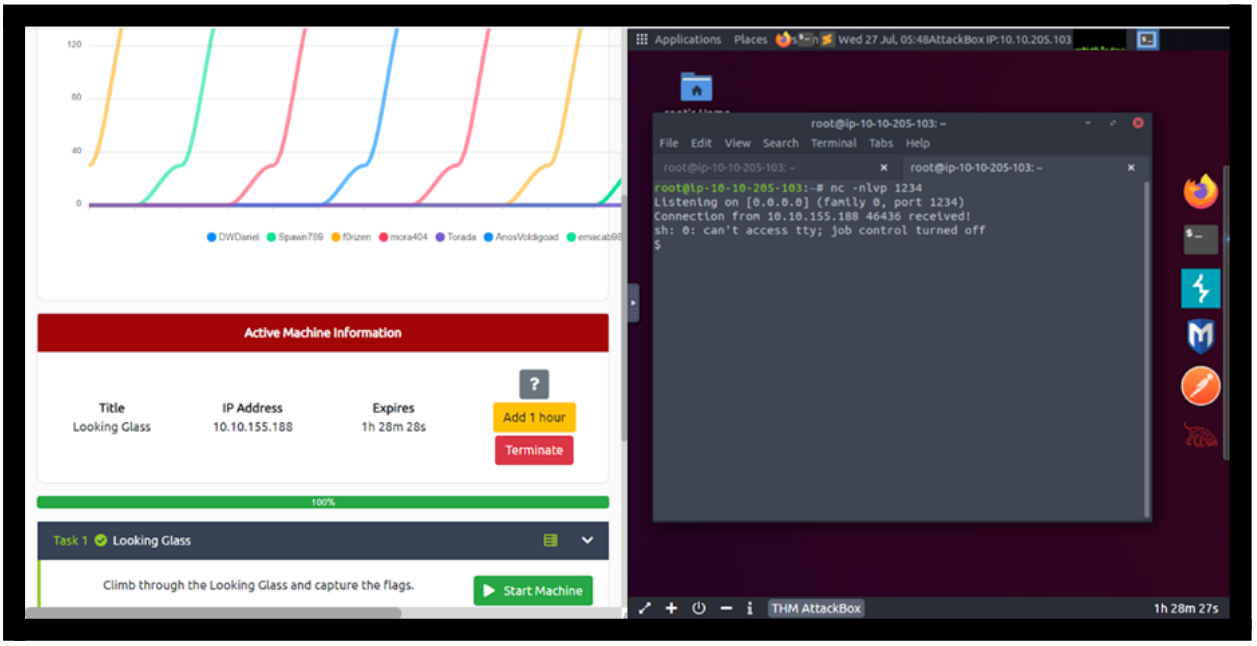




Mischelle edits the twasBrillig.sh file and pastes in the Reverse Shell in it by using the nano command. The IP address in the command is set into Mischelle's attack box's IP address and the port is set into 1234. Then, the file could be saved.



Mischelle performs a privilege escalation and reboots the Linux system. The root user could be seen in the terminal.



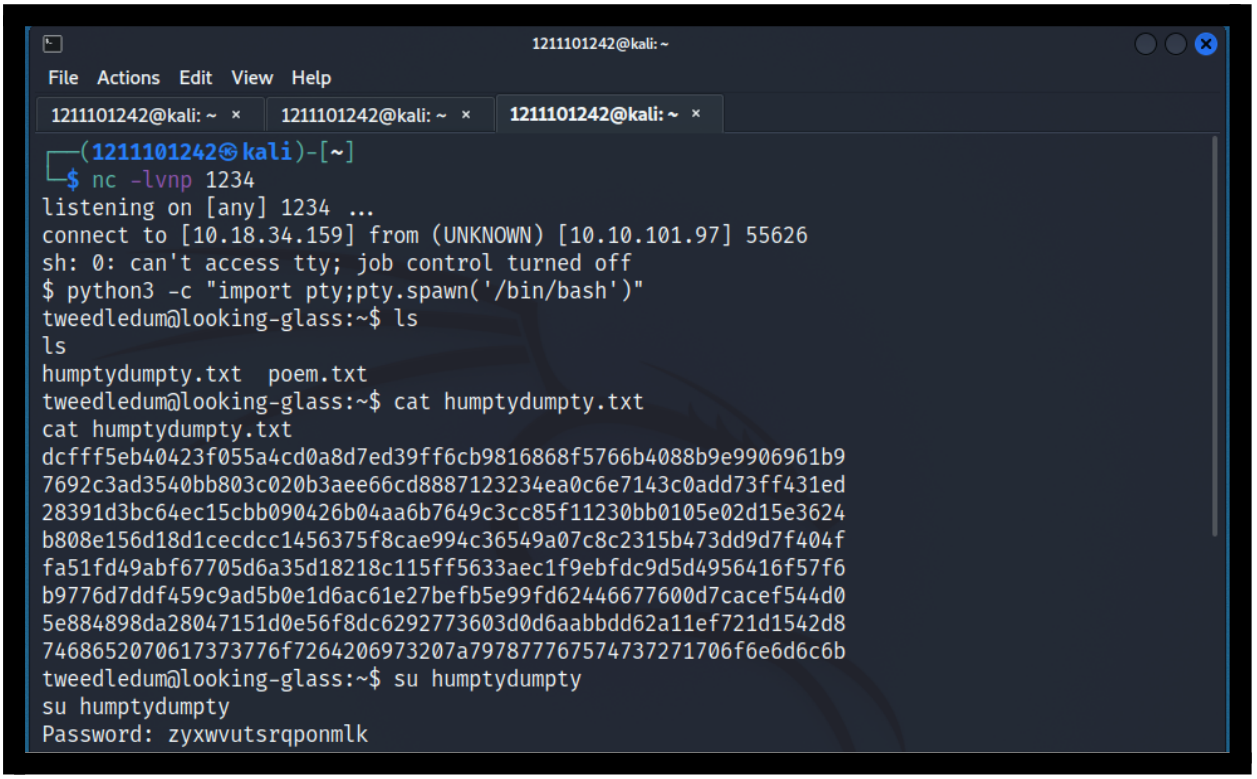
Mischelle then opens another terminal and uses the netcat listener to receive the executed connection which is produced by the reverse shell itself.

Horizontal Privilege Escalation

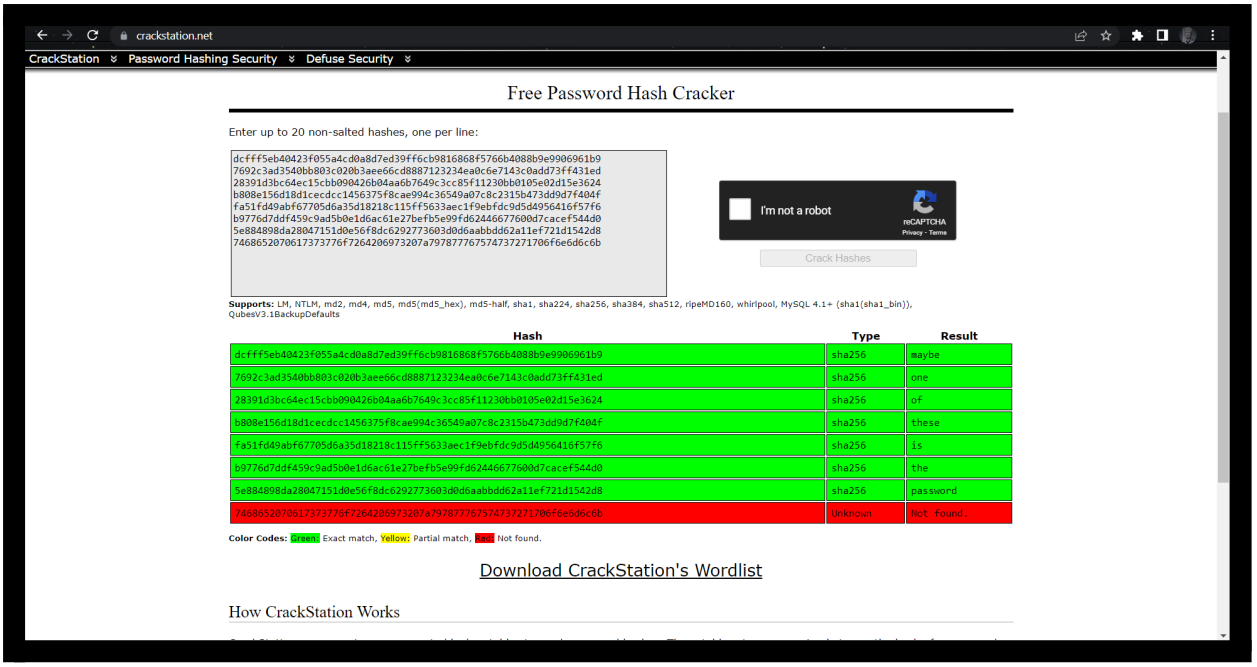
Member(s) involved: Raja Fitri Haziq Bin Raja Mohd Fuad

Tool(s) used: Kali Linux Attackbox, Reverse Shell, Crackstation, Cyberchef

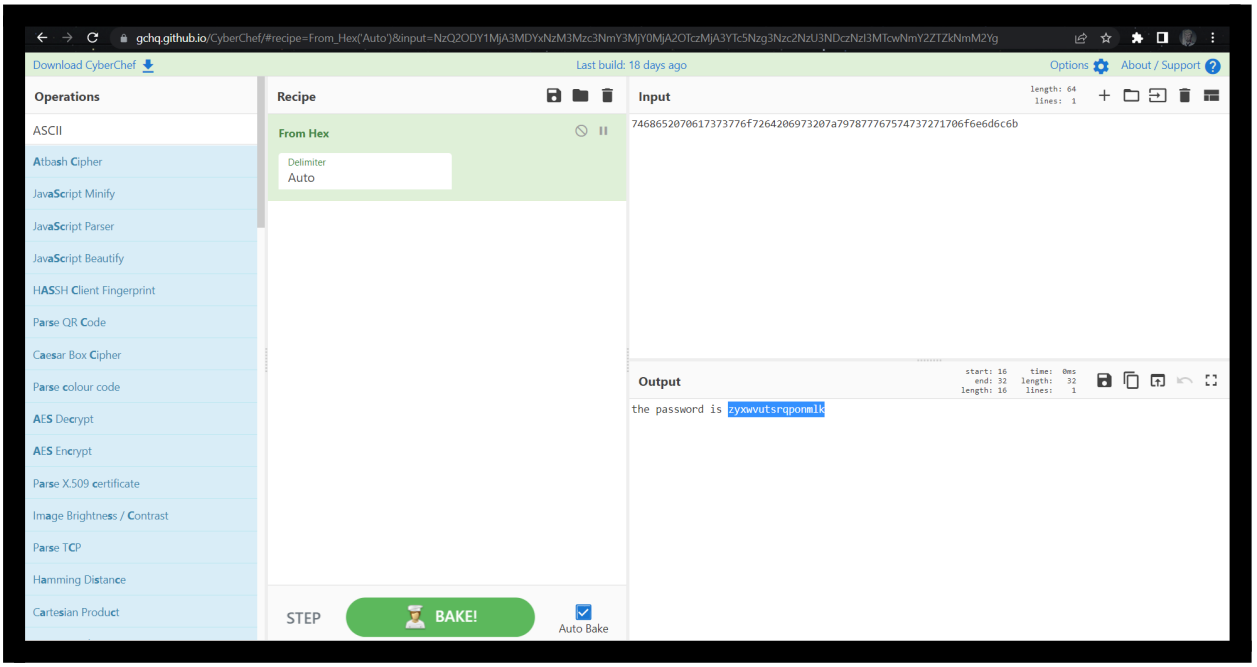
Thoughts Process/Methodology:



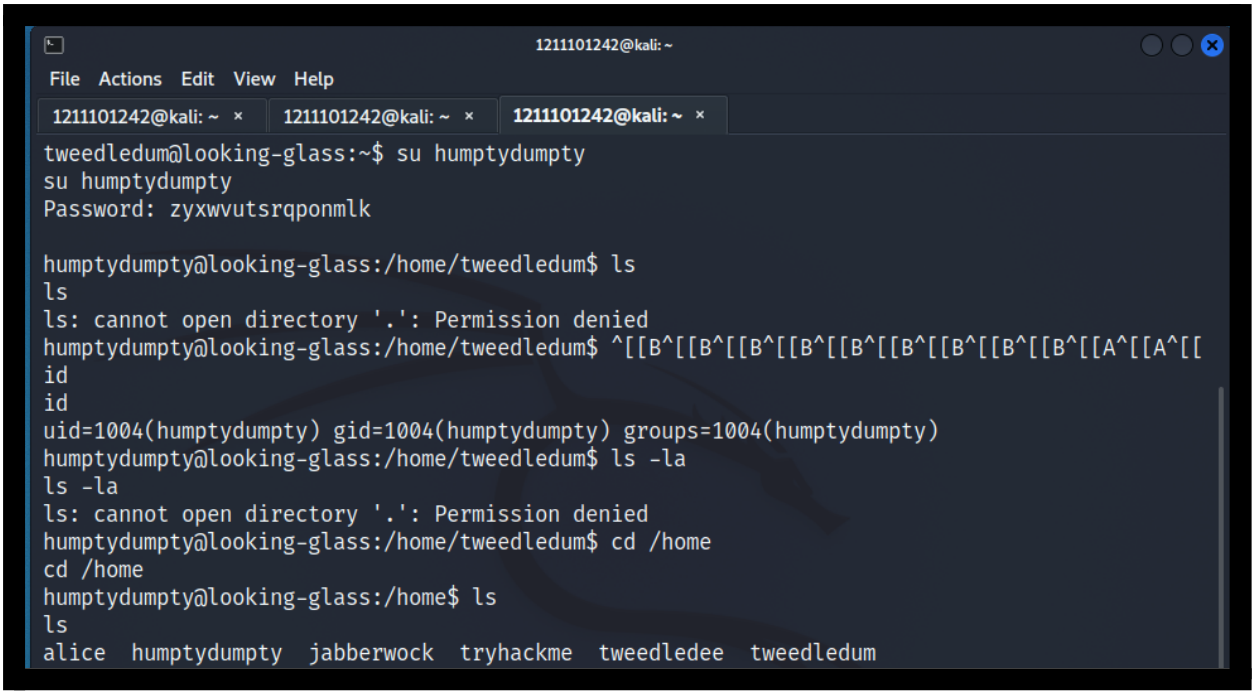
After Mischelle Thanusha Julius managed to put in the reverse shell on twasBrillig.sh and reboot the machine, the netcat listener should be able to connect to a new profile under the name “tweedledum”. Before continuing further into the task, Raja Fitri Haziq had to upgrade the reverse shell by using the following python3 command to gain access to tweedledum’s profile. By typing in “ls”, Raja Fitri Haziq was able to find two txt files located inside tweedledum’s profile which are “humptydumpty.txt” and “poem.txt”. In order to see the content of each file, Raja Fitri Haziq had to use cat filename. Typing in cat humptydumpty.txt would reveal a bunch of strings which include both alphabets and numbers.



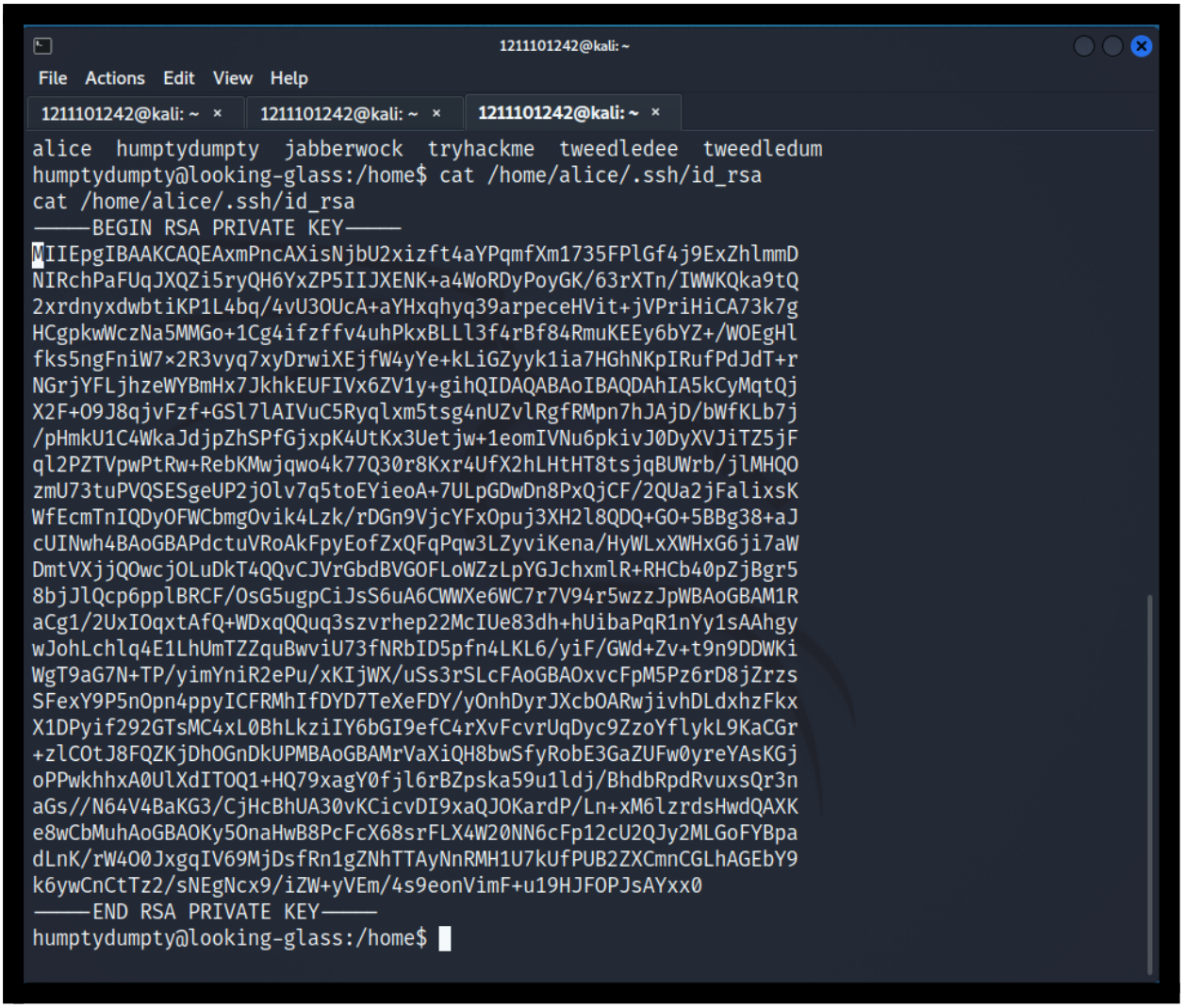
Raja Fitri Haziq used Crackstation in order to crack the content in humptydumpty.txt. As shown in the image above, only one set of particular strings were unable to be cracked by Crackstation.



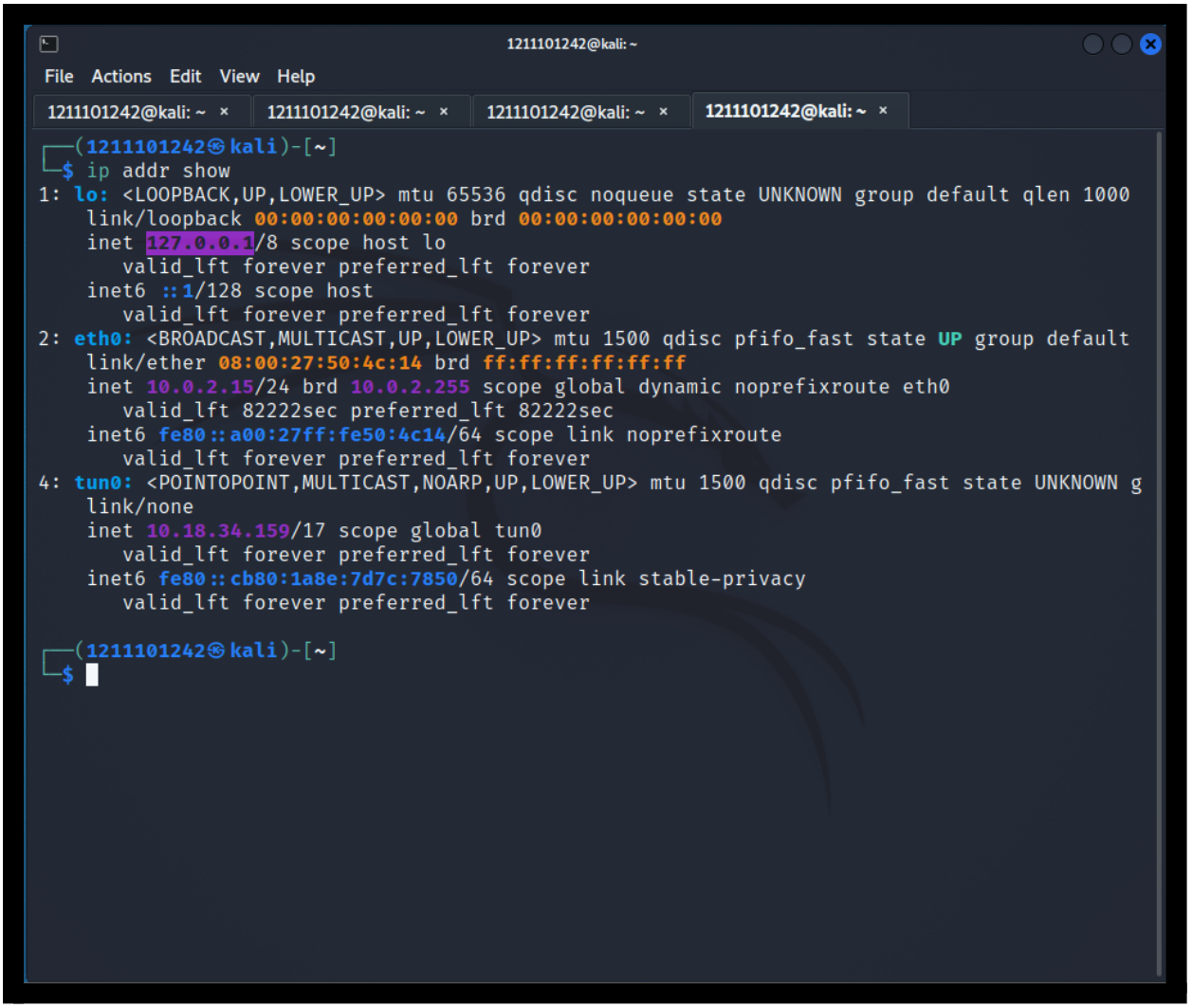
Therefore, Raja Fitri Haziq went to Cyberchef to decode the encoded set of strings and was able to due to using Hex as its recipe. The password for humptydumpty was revealed as shown in the image above.



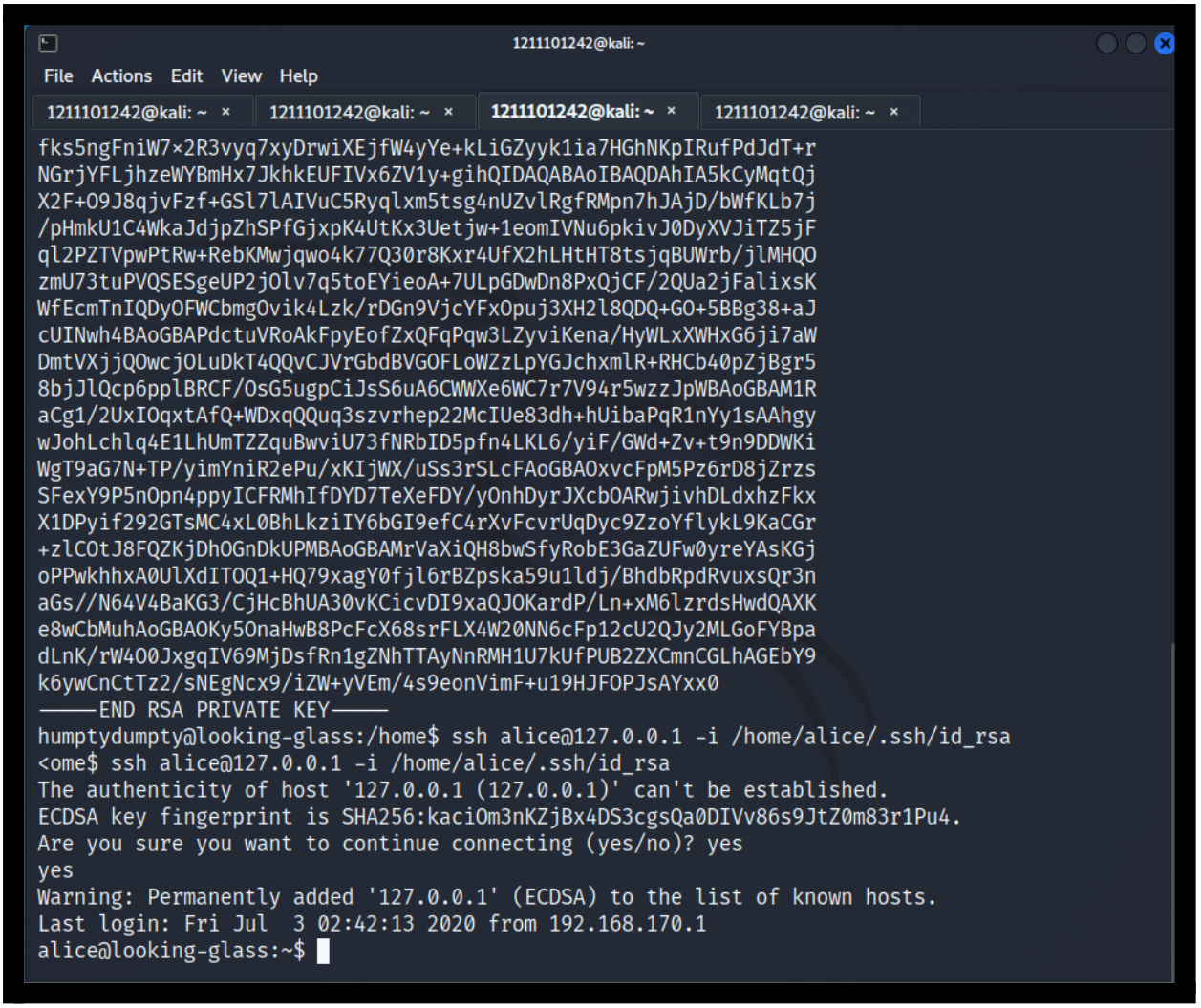
Raja Fitri Haziq then was able to change the user from tweedledum to humptydumpty by using “su humptydumpty”. After accessing humptydumpty’s profile, Raja Fitri Haziq used the command “cd /home” follow up by “ls” in order to see everyone who was available there.



As the only file Raja Fitri hadn't viewed as was Alice, we are able to do so by using a specific command which is "cat /home/alice/.ssh/id_rsa". This would reveal and told us that the file has a bunch of RSA keys inside alice which will help later on to change to root profile.



Before Raja Fitri Haziq was able to change the privilege to alice, we have to obtain a specific ip address by using the following command as shown in the image above.



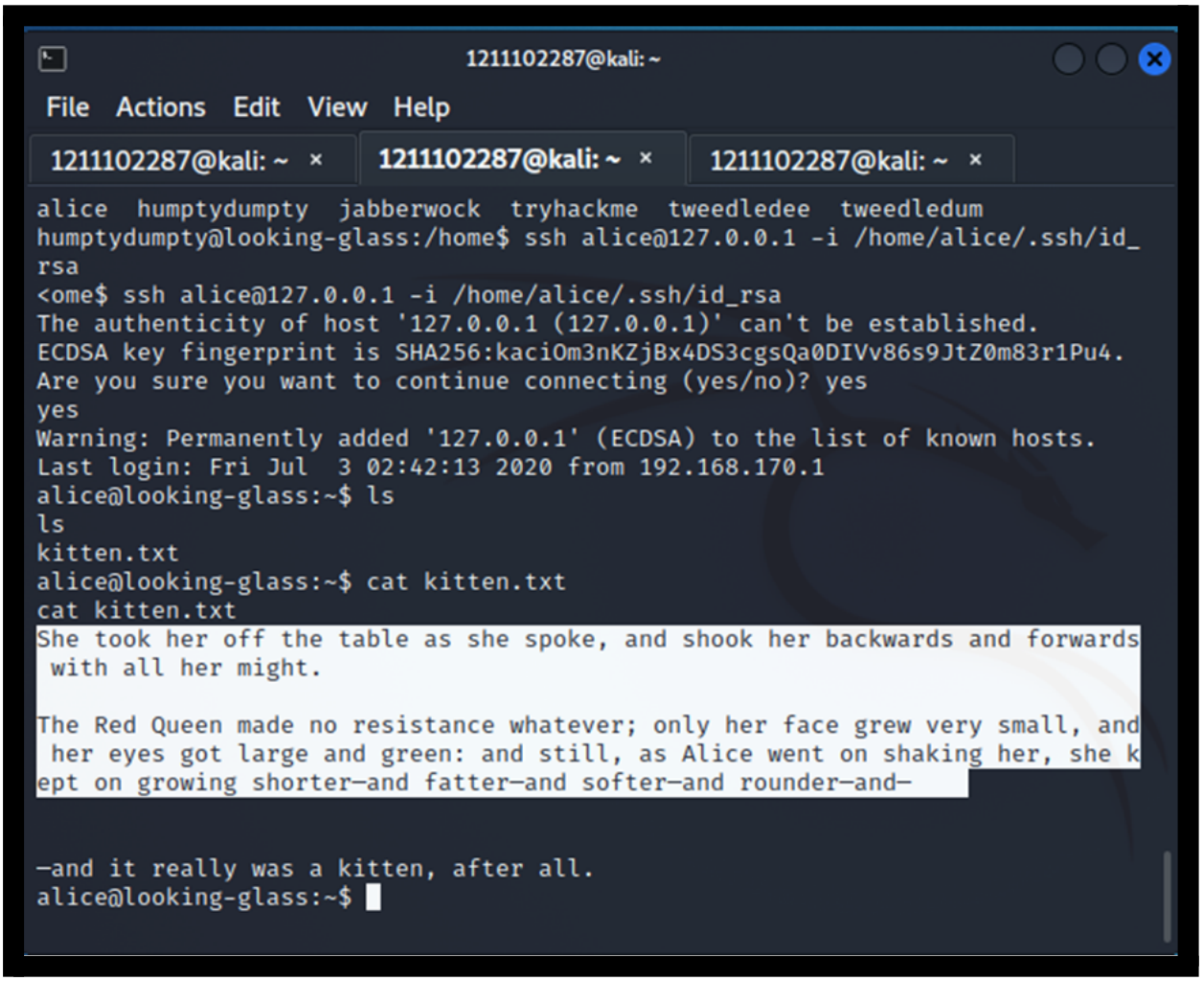
After obtaining the ip address, Raja Fitri Haziq managed to log into alice's profile by typing in ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa

Root Privilege Escalation

Member(s) involved: Terrence Cheng

Tool(s) used: Kali Linux Attackbox, Reverse Shell

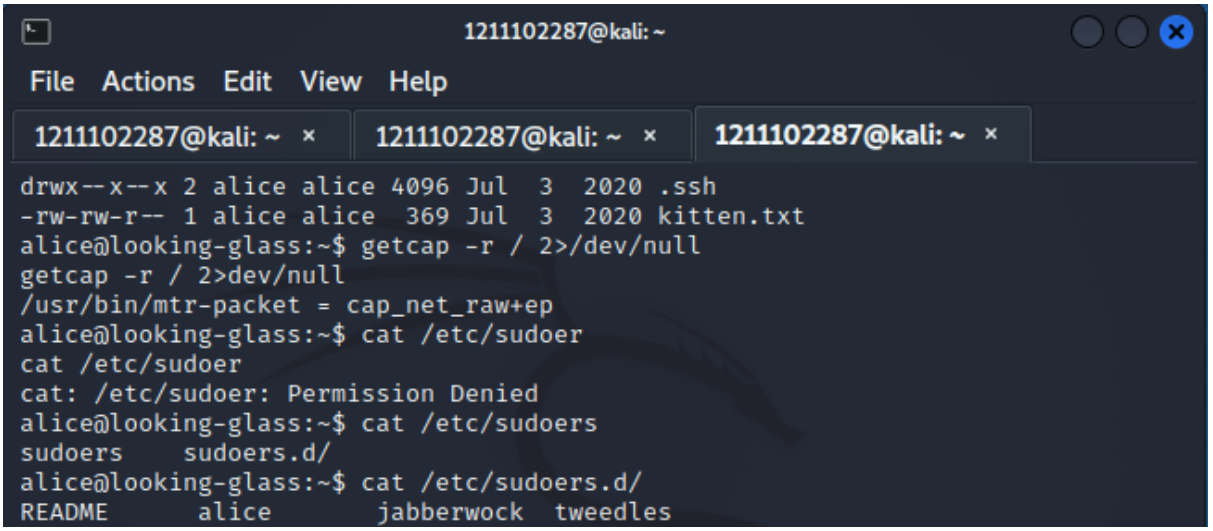
Thoughts Process/Methodology:



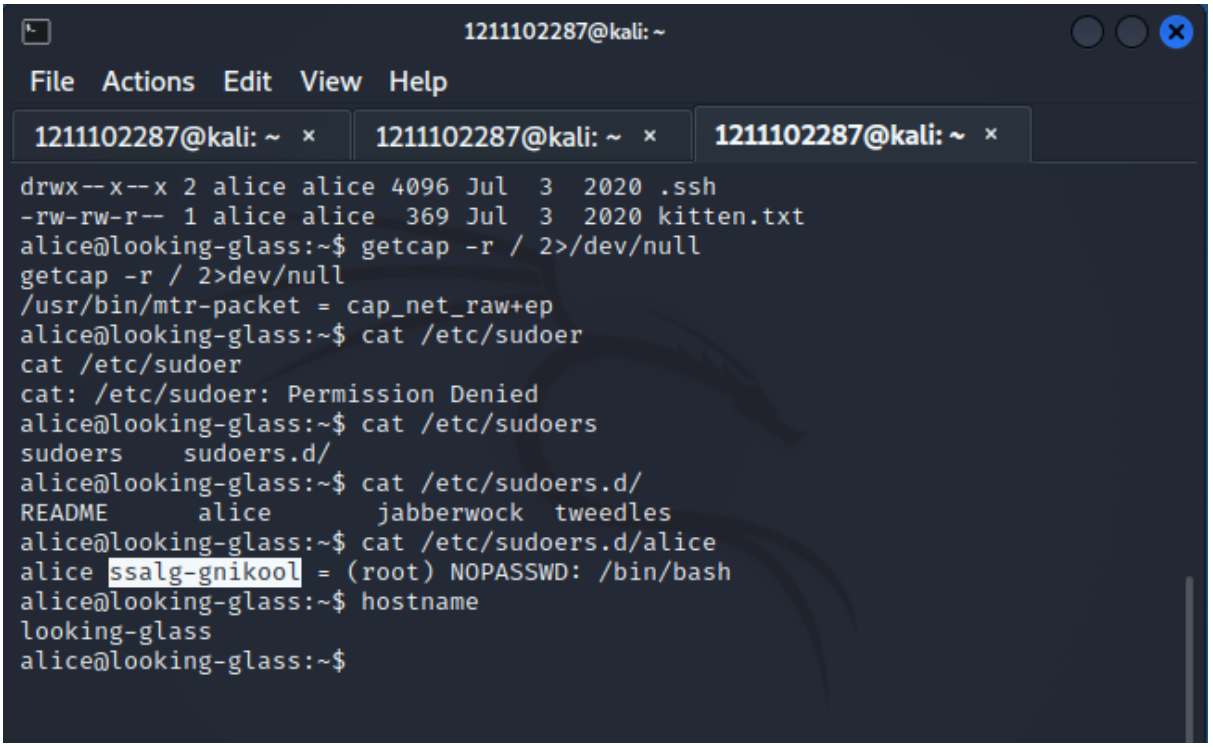
After Raja Fitri Haziq has managed to log into Alice's profile, Terrence looks for the files in the directory and finds out there is a “kitten.txt” inside. It looks like it is just a normal text with no use.

```
alice@looking-glass:~$ ls -al
ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$
```

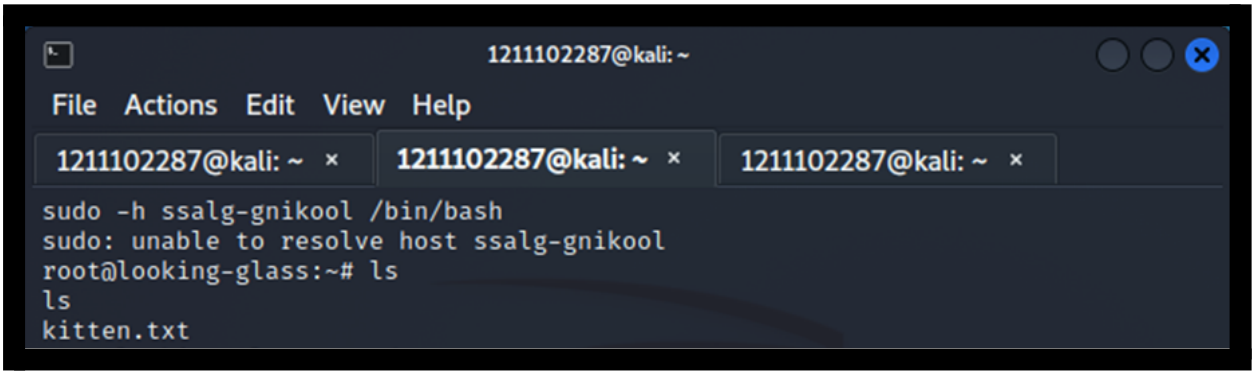
Terrence finds the hidden folder by using the bash command. Terrence sees the folder for (.bash_history) which is a special file in this user's system.



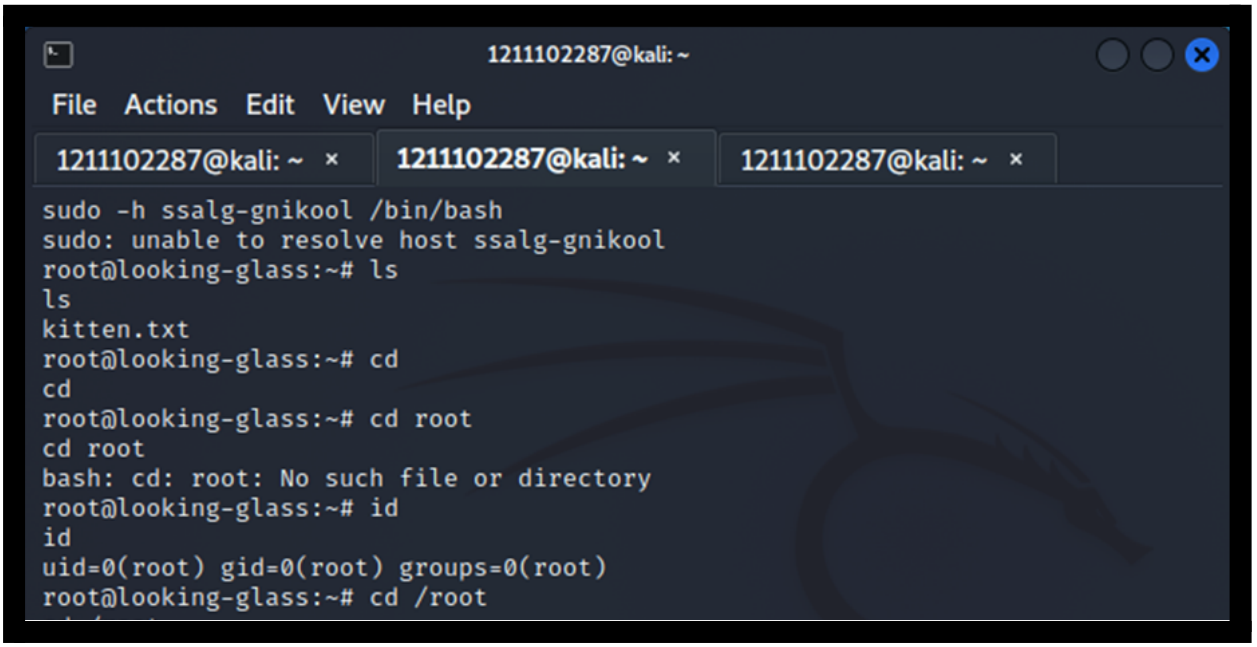
After discarding the errors on that special file , Terrence then finds the requirements and circumstances for the user to run commands that require elevated privileges. By typing the correct command, Terrence found out that there are two files in the directory. Terrence looked at the sudoer.d/ file and found out there are more files in it.



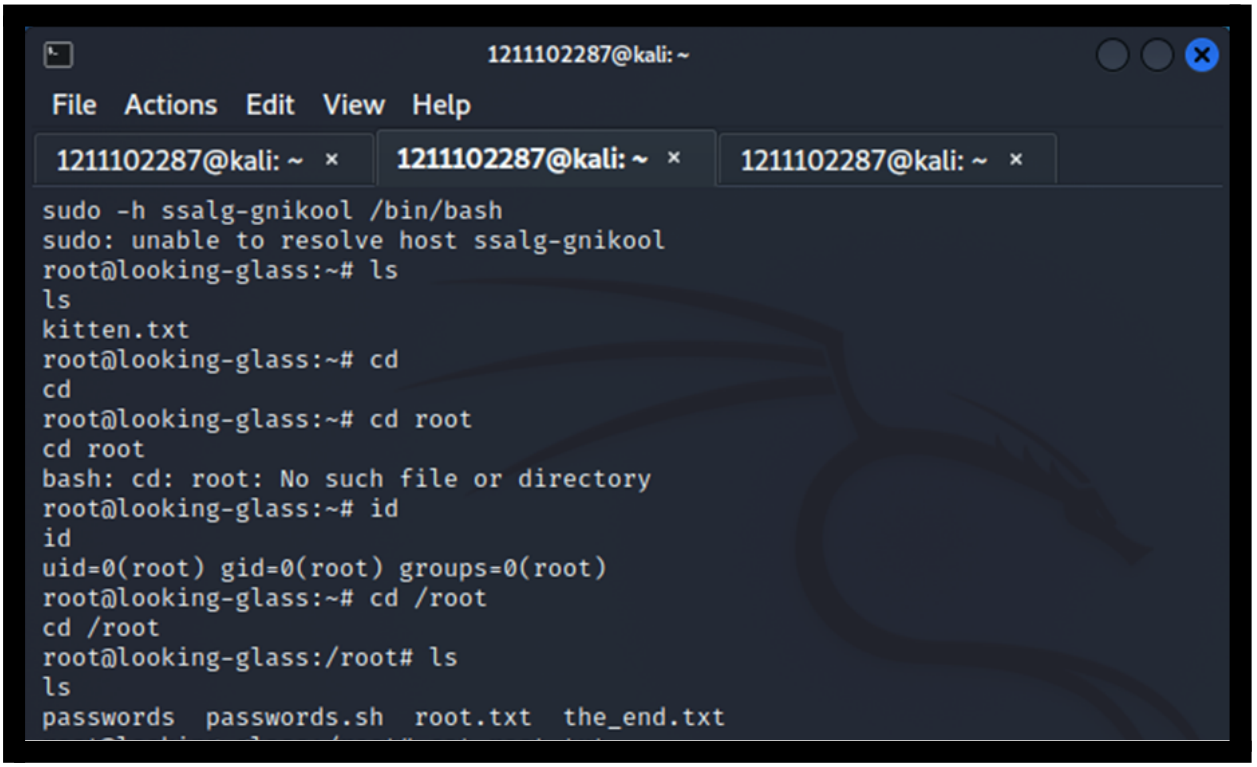
Terrence looked into the “alice” file and it shows that there are no passwords needed to access the root user of it. It is also under the same hostname which is looking-glass in the reverse version.



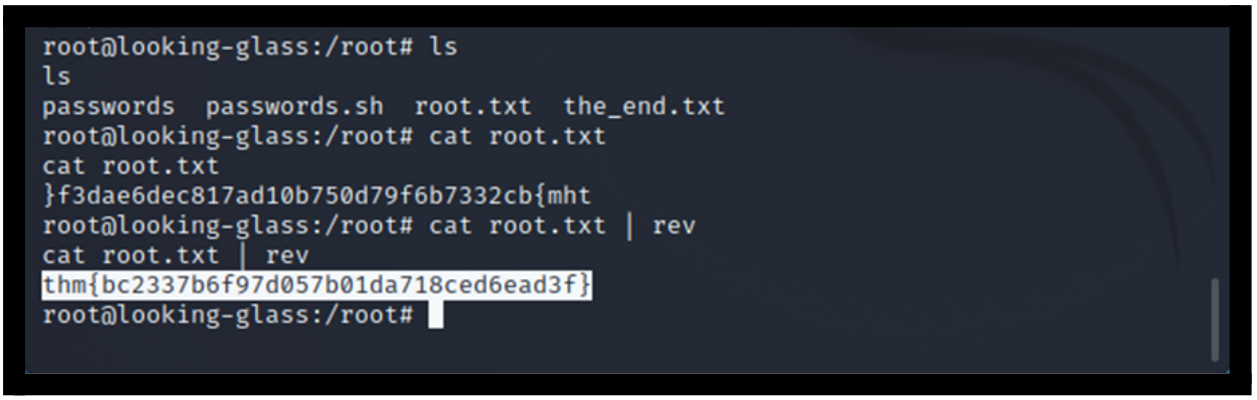
To escalate to root and gain access to it, Terrence used the sudo command and to run commands on the host.



Terrence checked and made sure that he is in the root user by finding the id. It is confirmed that Terrence is in the root of the user.

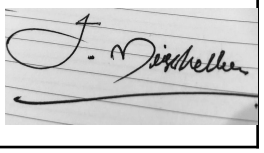


Terrence managed to get into the root user's directory by using the bash command and looked into the list of contents in the directory.



Terrence looked into the root.txt file. Finally, Terrence successfully found the root flag by reversing the current content in the root.txt file.

Contributions

ID	Name	Contribution	Signatures
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	Changing the privilege escalation from jabberwock to tweedledum to alice.	
1211104237	ALIA MAISARA BINTI SHAHRIN	Enumerate the ports that exist inside the servers, find the port that contains the riddle and credentials of the user, log in to the user jabberwock by using SSH and get the user flag.	
1211102287	TERRENCE CHENG	Perform Privilege Escalation from alice to the root user. Finding the root flag.	
1211101153	MISCHELLE THANUSHA JULIUS	Adding the Reverse shell to be executed	

Video link: https://youtu.be/9x5TFg5SJzI