PenTest 1

ROOM A

MODUS POTENT

Members:

ID	NAME	ROLE
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah Bin Kamaruddin	Member
1211103649	Nur Qistina Binti Roslan	Member

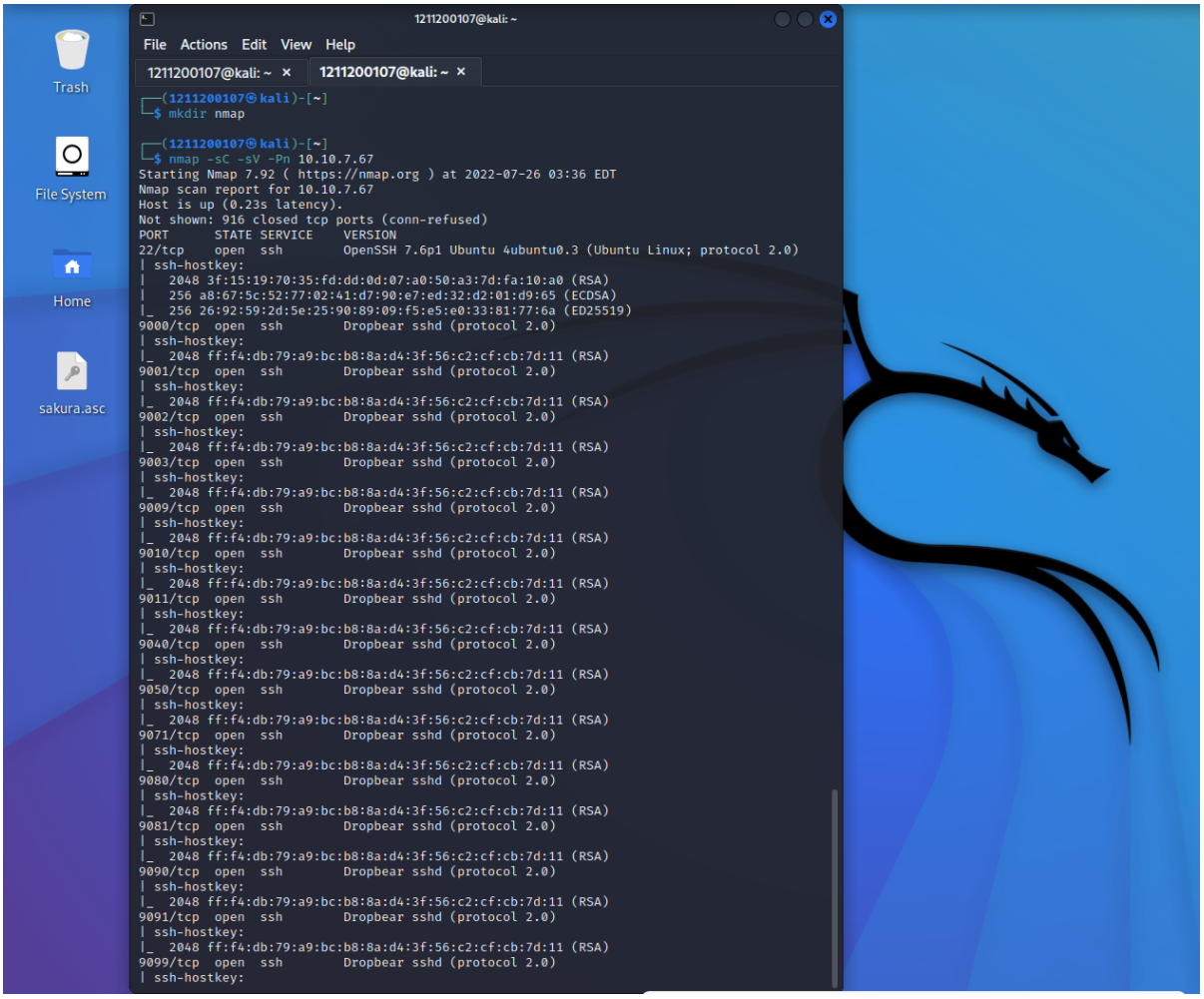
Recon and Enumeration

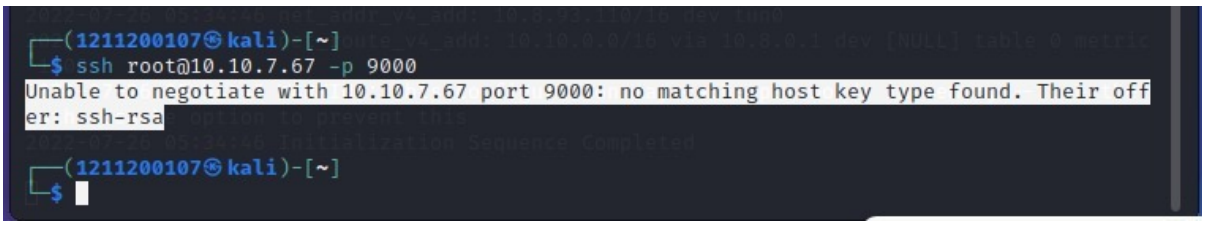
Members Involved: Afiezar

Tools Used: Kali Linux, Terminal, Attakbox, Firefox,

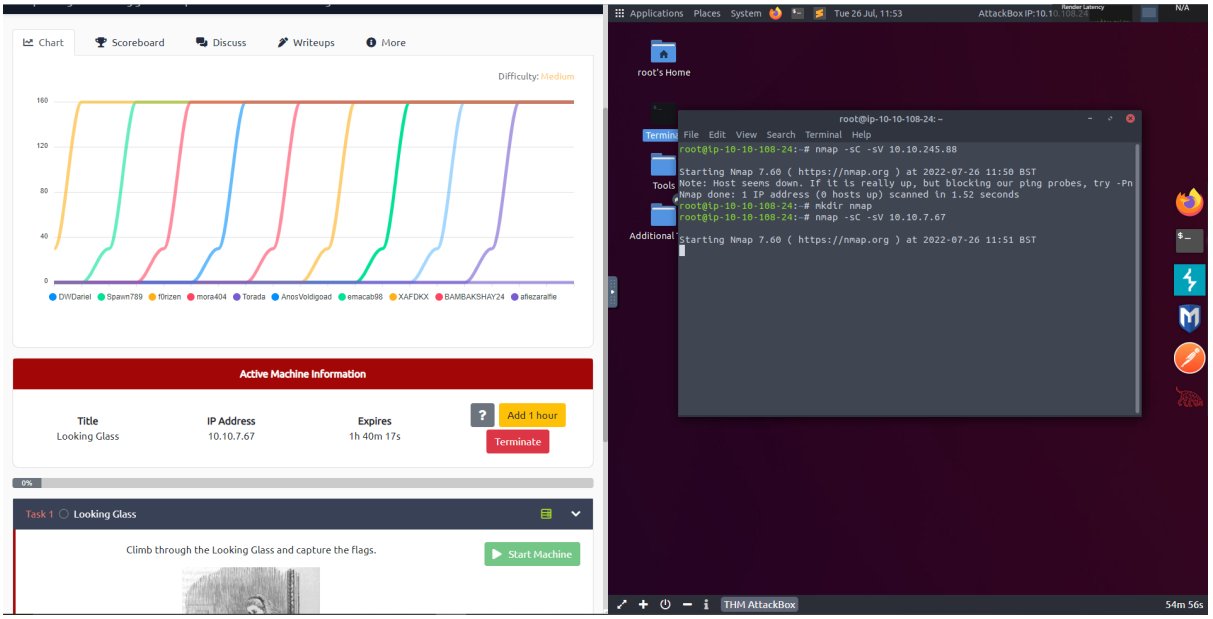
Afiezar's Attempt

First off, Afiezar tried to use his own Virtual Attackbox. After successfully running an nmap scan, Afiezar tries to open one of the ports. However for some reason, there was an error message saying that there is no matching host key. Afiezar is unable to solve the issue and changes to the TryHackMe Attackbox.



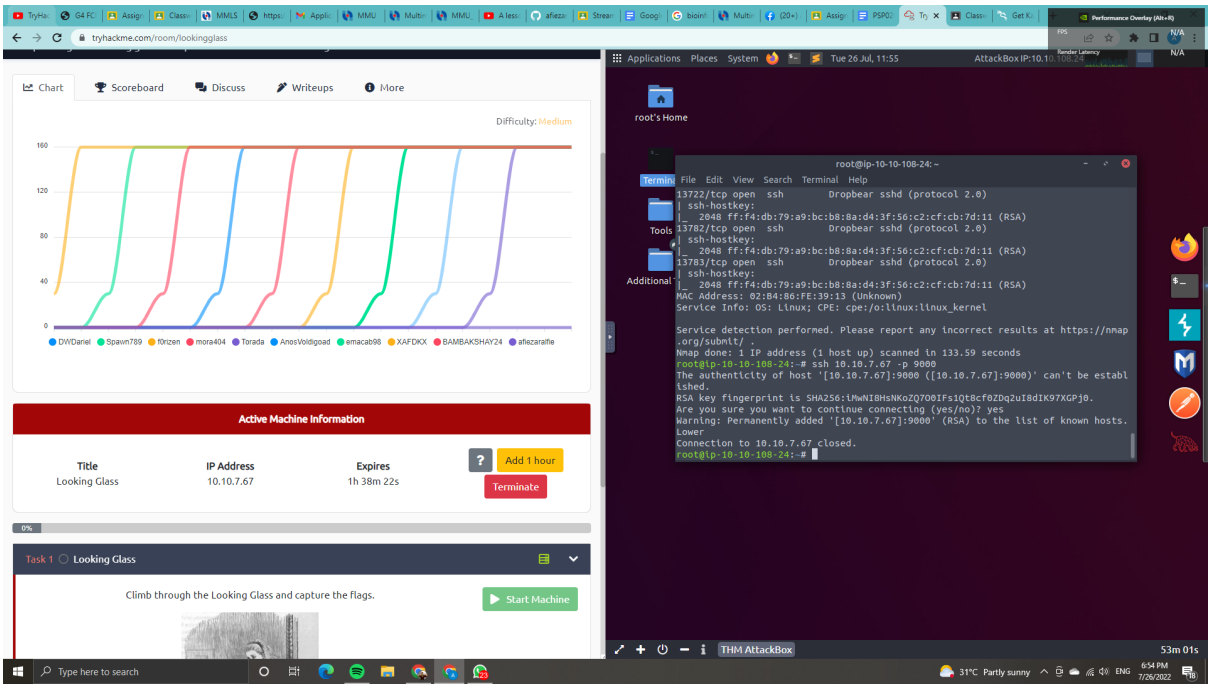


Then, Afiezar repeats the same process as he did previously. Afiezar starts an nmap and lets it run

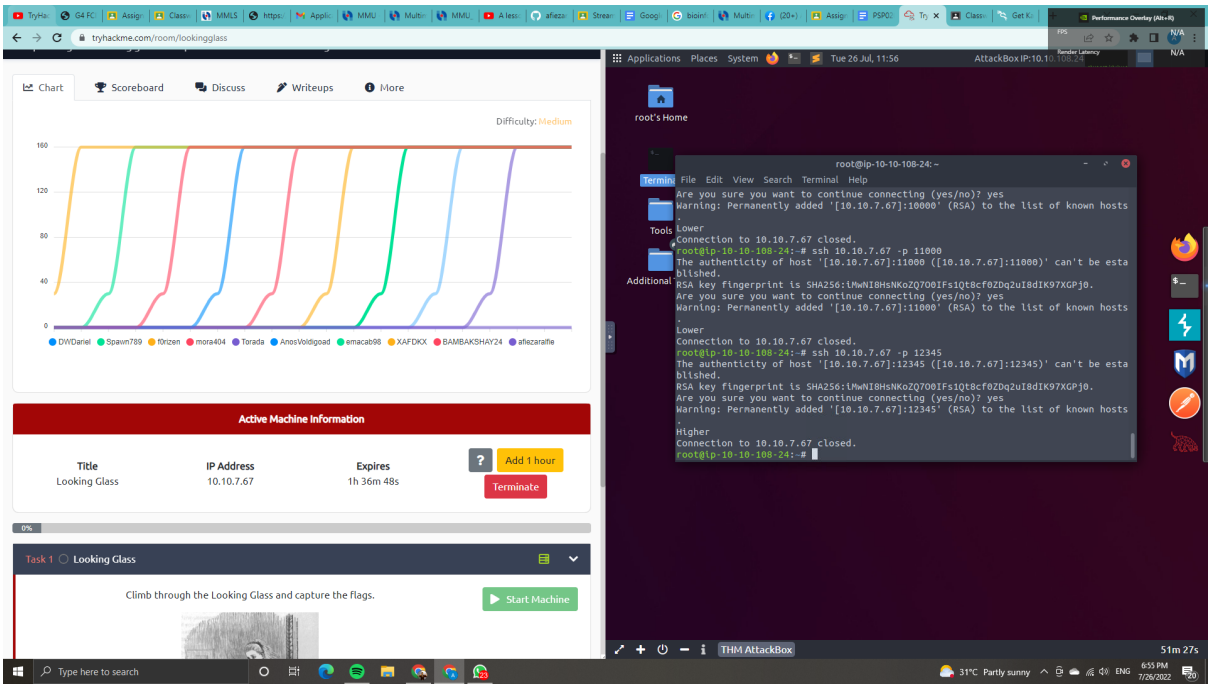


After the nmap scan has successfully run, there will be multiple ports. We also see OpenSSH running on port 22. Other than that, there will also be thousands of other ports ranging from 9000 to 14000 that most likely is seen running on Dropbear sshd. To get a clearer understanding on what dropbear ssh is, it is basically similar to SSH only it is mainly used for environments with low memory and processor resources, such as embedded systems.

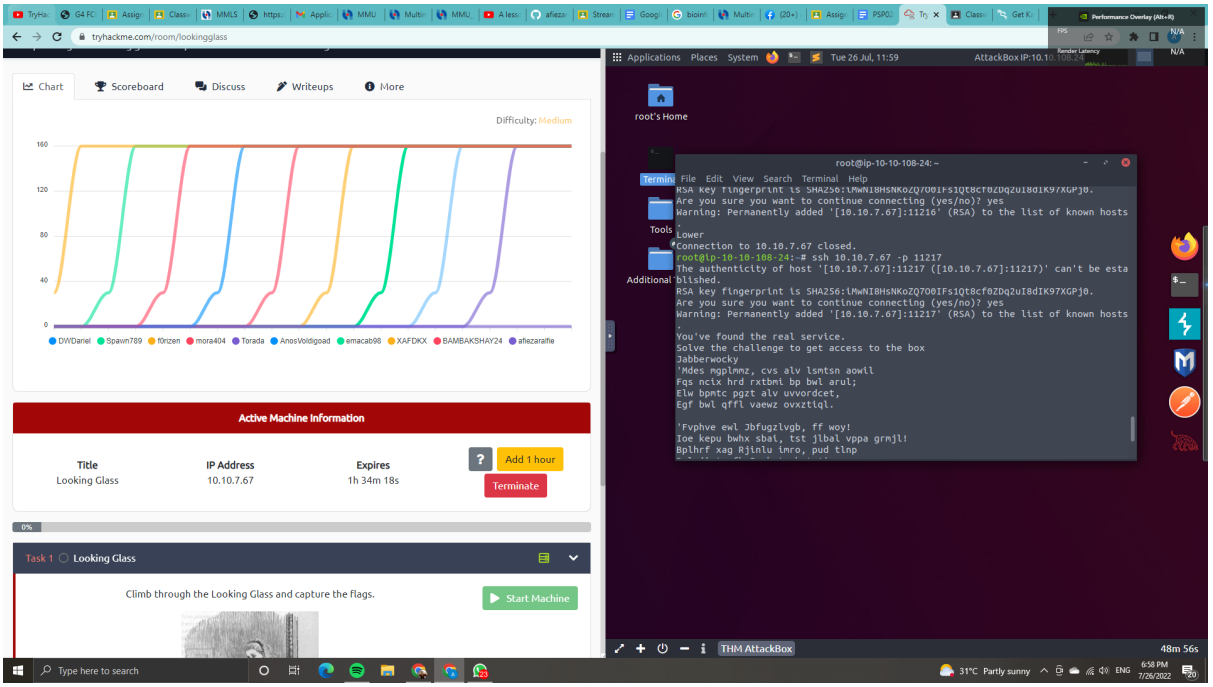
Following that, if we try to connect to any of the open ssh ports it would result in an output of ‘Higher’ or ‘Lower’, this gives us a hint to get to the correct port we need to use.



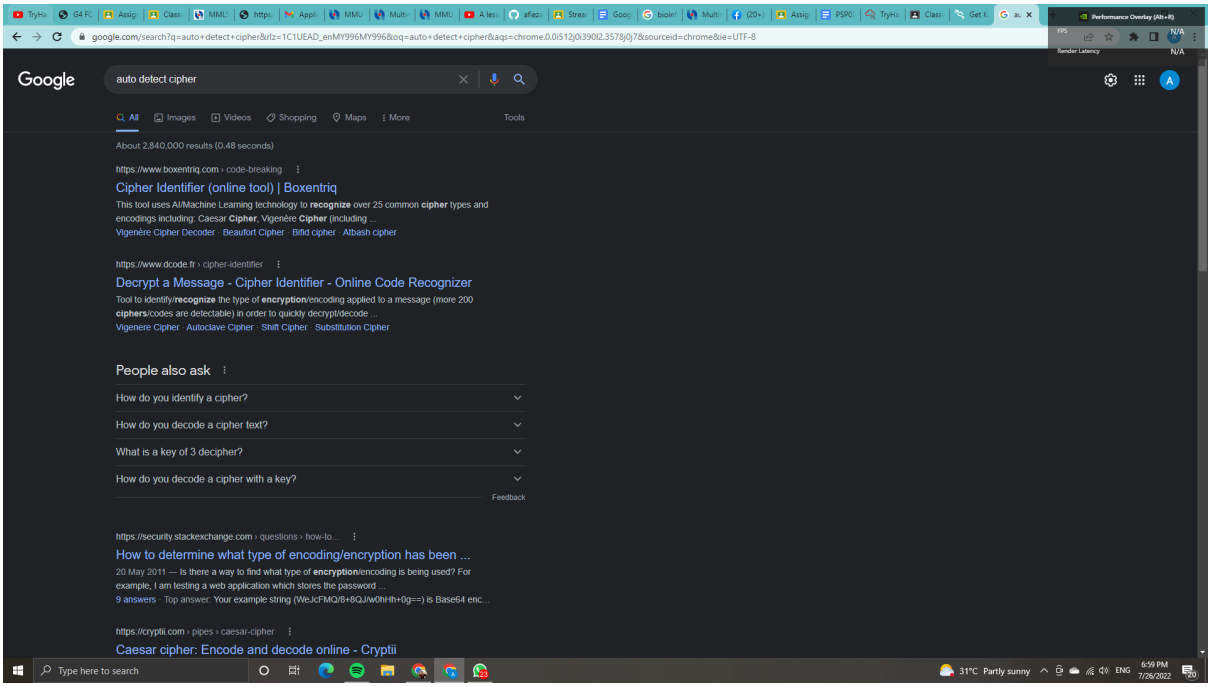
By logging in the lowest port it will give an output saying ‘Lower’ which may not make sense at first but if we think back on the concept of Looking Glass is a mirror it gives us another aspect of reversing the output taking the meaning of Lower means we have to go higher and go back and forth between high and low values to find the accurate port.

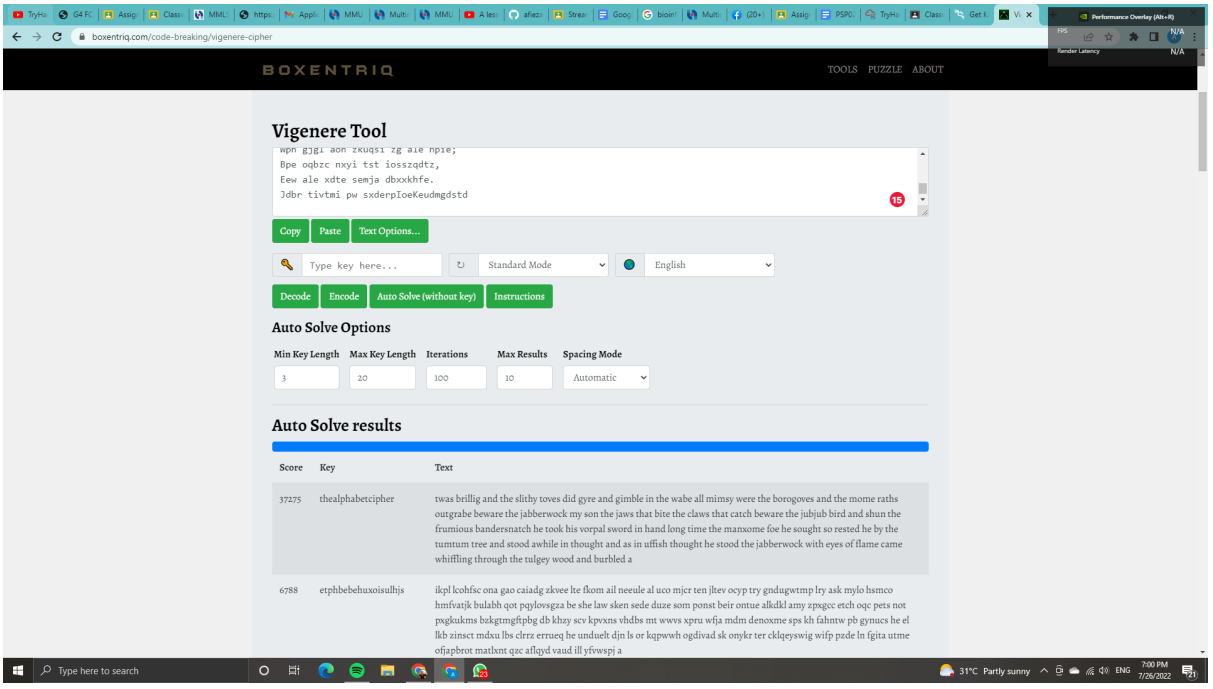


After numerous iterations, we are then presented with an encrypted version of the Jabberwocky poem and at the far bottom we are requested to put in the secret password, in order for people to not assume we are trying to crack the cypher. At first, the text seems to follow the structure of the poem, likely using a rotation cipher for instance a ROT13 or a Vigenere cipher. However, ROT13 did not work in the end. As for Vigenere, we will need a decode key where we can obtain through multiple sites that can brute force the key



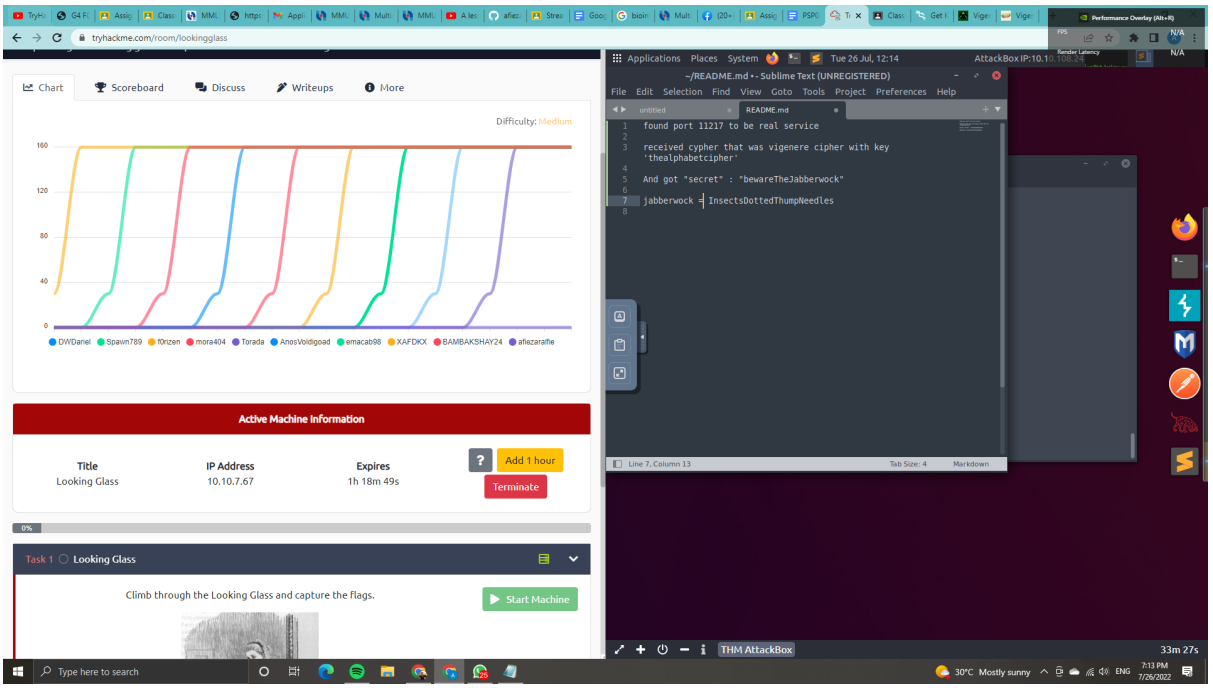
The first site we used being ‘Vigenere Tool’ did not manage to decode it at the beginning, it was mainly because the encrypted text had some words that were longer than the other 10 characters. In order to get the results we changed the default settings’ Max Key Length to 20 and tried again and managed to get the key is “thealphabetcipher”. The Boxentriq website didn’t get us the full text, so we tried changing to another vingere tool website.



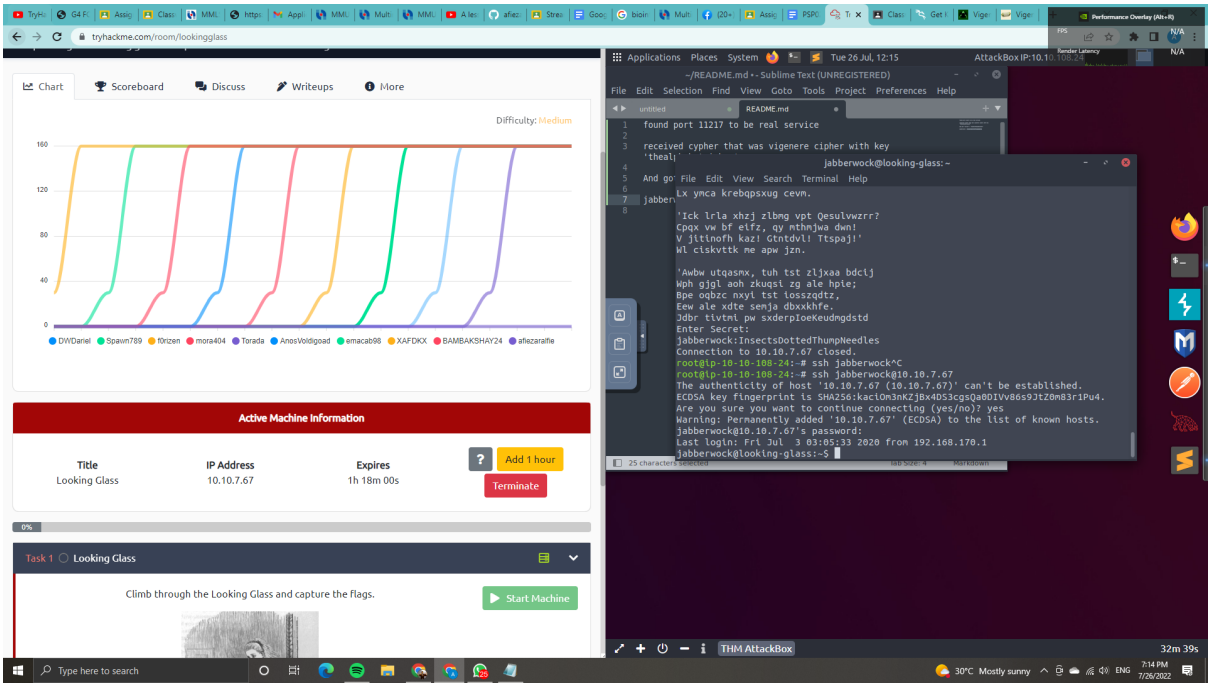


On this website, we are able to put in the key “thealphabetcipher” and we pasted in the whole encrypted text into the decoder. The results we get is the answer to the secret, “bewareTheJabberwock”. We will copy and paste the answer to the terminal.

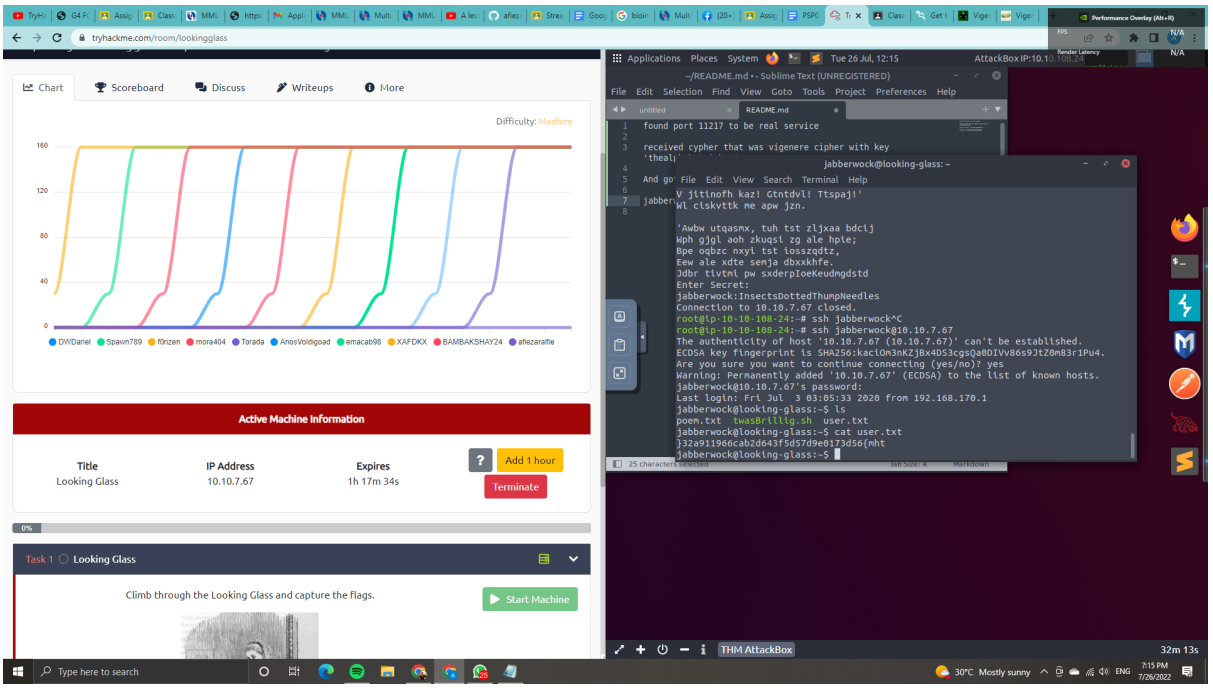
It gives out the answer “jabberwock”:”InsectsDottedThumpNeedles”. We will put the answers in a notepad for future reference.



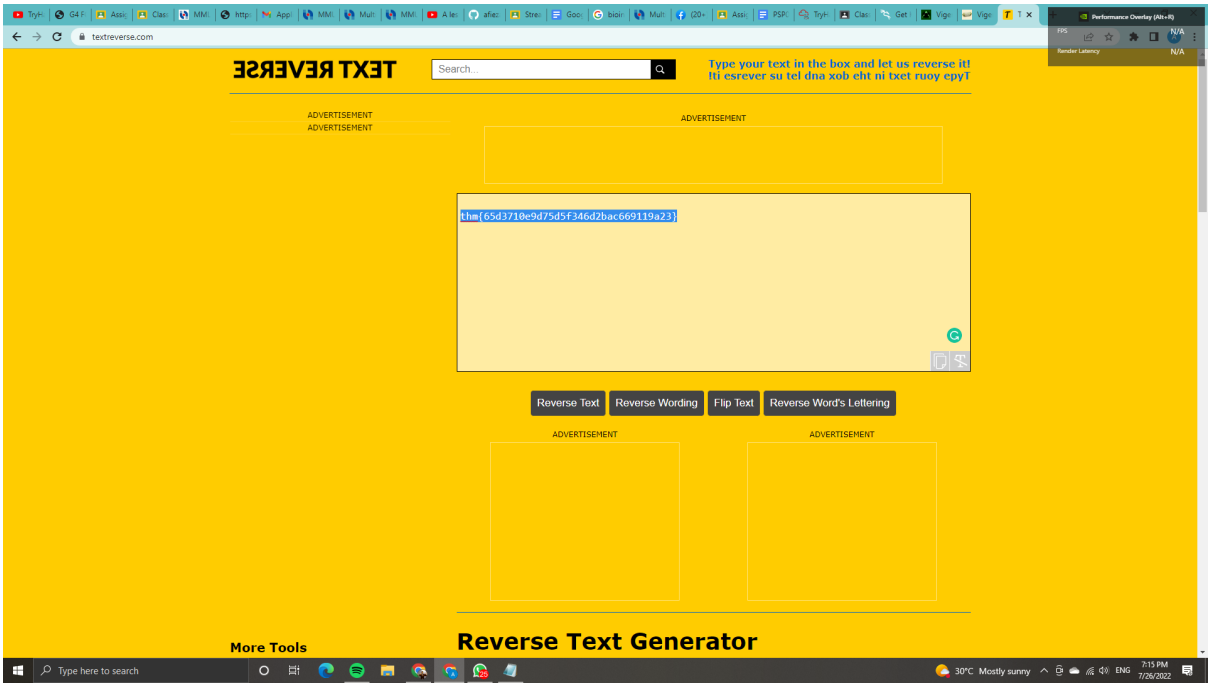
With the given credentials we are able to connect to the regular ssh ports using “jabberwock” and the password we obtained earlier which is “InsectsDottedThumpNeedles”. From there on we have gained access to the box temporarily



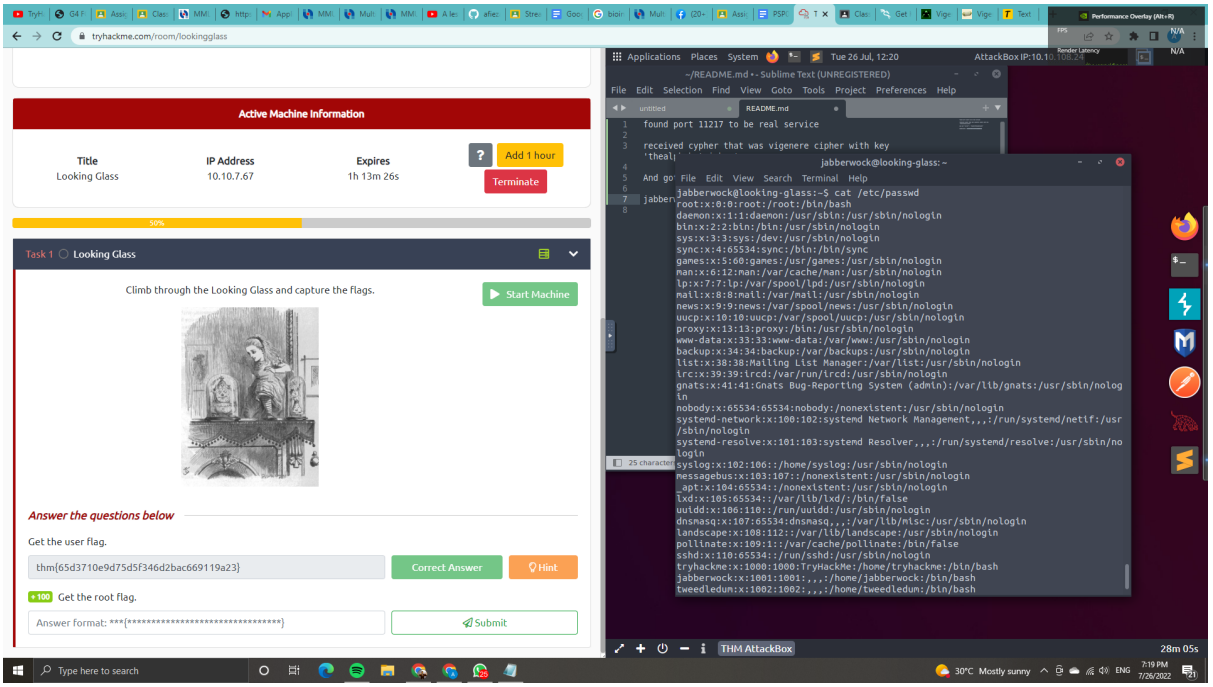
We will use the ls command to see what we have. We find that there is a user.txt file. We will need to grab the user.txt file in order to get the user flag but we will be presented with a thm flag backwards so we could easily use a reverse text site and get the thm flag easily.



Using an online text reverser, we pasted the answer and get the flag for the first question



With that, we got the first question down which is thm{65d3710e9d75d5f346d2bac669119a23}. We will now paste the answer into TryHackMe to ensure that that is the correct answer.



We then try to move onto the next question but was unfortunate because Afiezar ran out of time and wasn't able to continue.

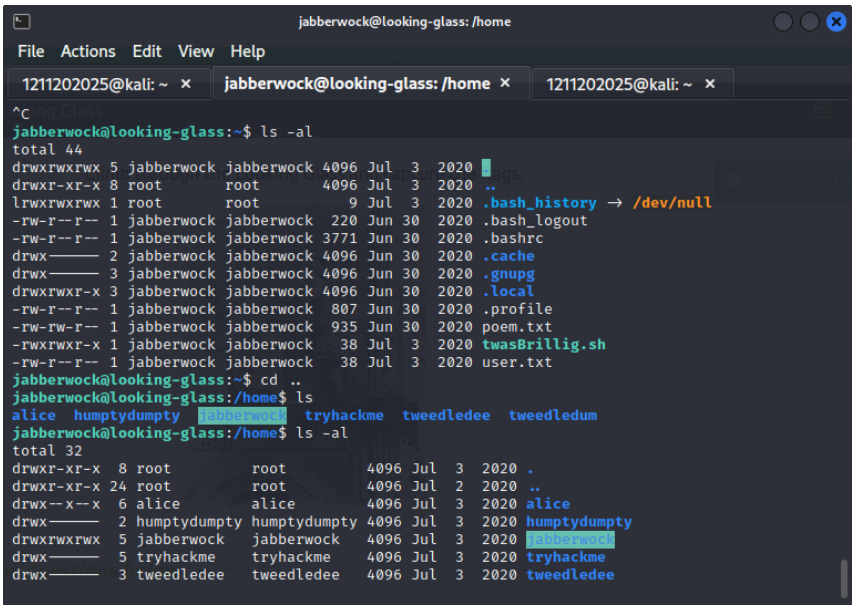
Initial Foothold

Members Involved: Abdullah

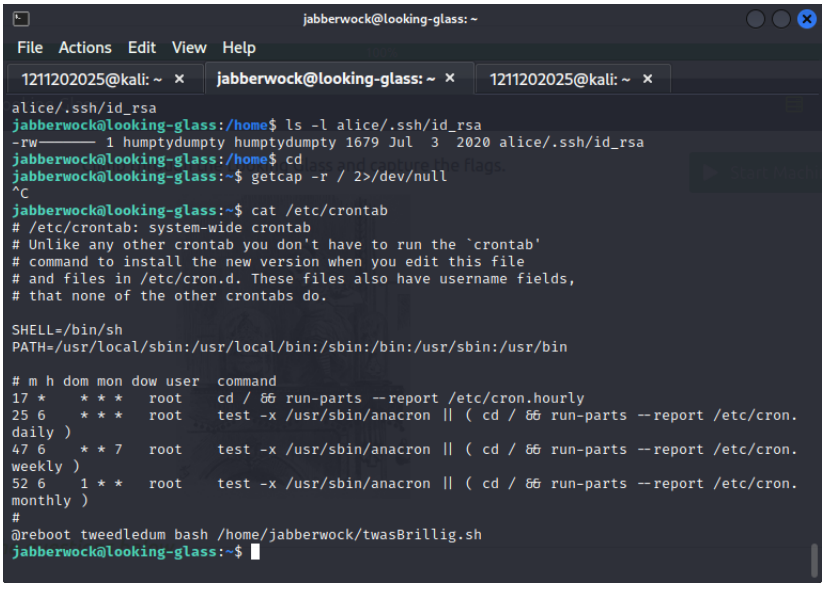
Tools Used: Kali Linux, Attackbox, Terminal, Firefox

Abdullah's Attempt

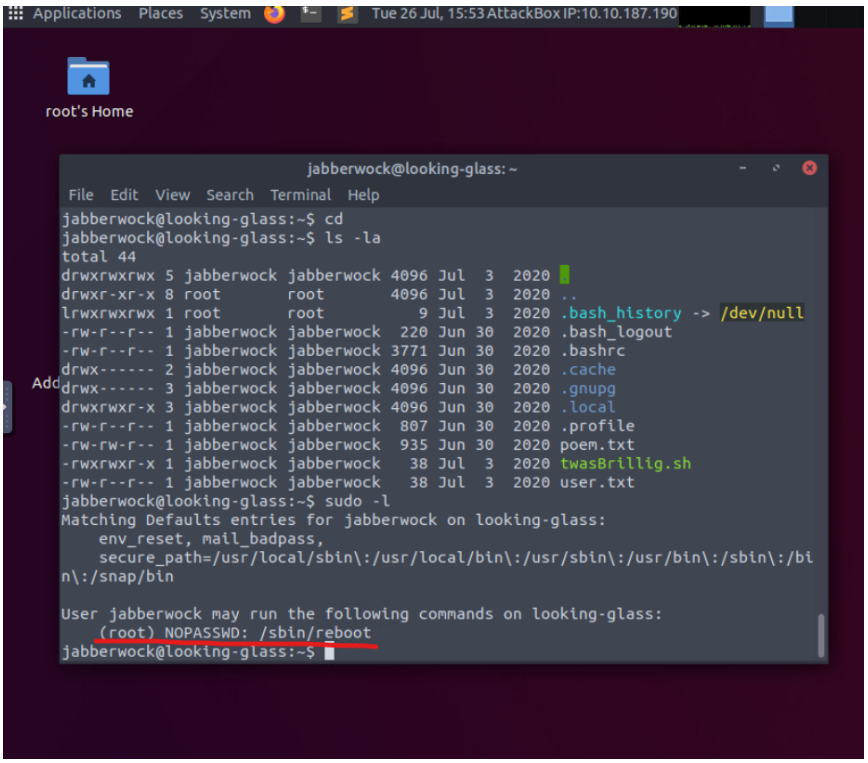
Continuing on from what Afiezar was left on, we used the exact same step to log into jabberwock@looking-glass. After successfully logged in, we used the ls command to check for files and directories. Sure enough, there are some suspicious ones like twasBrillig.sh. We also got to know that there are other users, alice, humptydumpty, tryhackme, tweedledum and tweedledee.



We also check crontab to see if there are any cron jobs running. So as seen from the line at the bottom, there is a cron job being run by user tweedledum which runs the /home/jabberwock/twasBrillig.sh we saw earlier. There is also a key clue here, in that the cron job only runs on reboot.

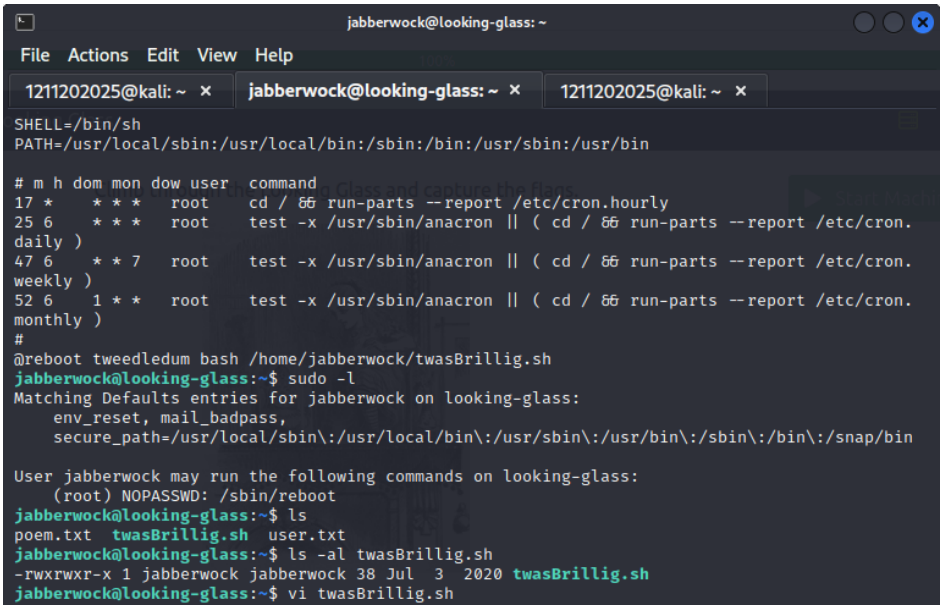


We tried this countless times so it is all over the place with different IP addresses and stuff. But before all this we tried in the THM AttackBox and using the sudo command, we were able to know that we can reboot the box without a password as our initial user jabberwock.

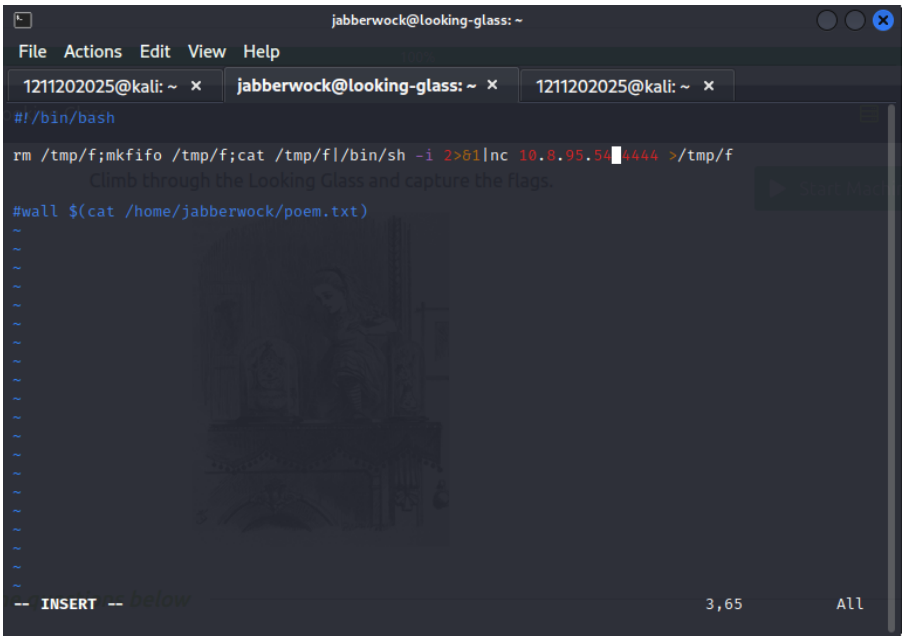


By doing so we now also know how to reboot the box.

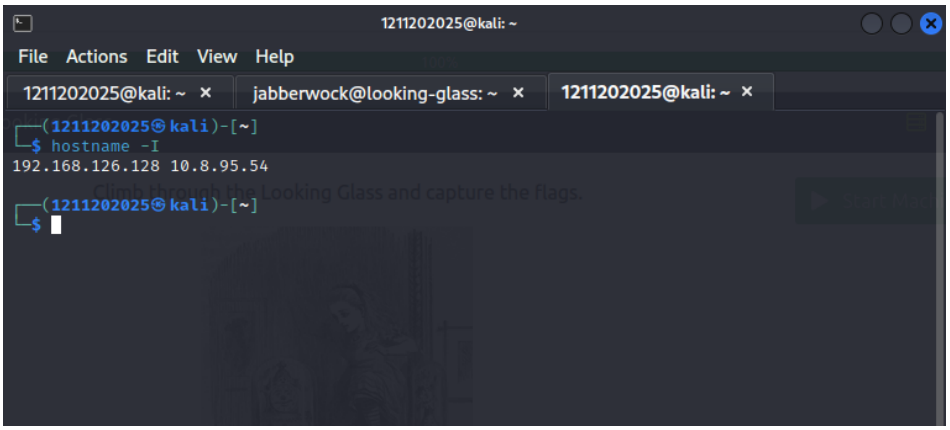
Moving on, we then modify the twasBrillig.sh by using the command vi,

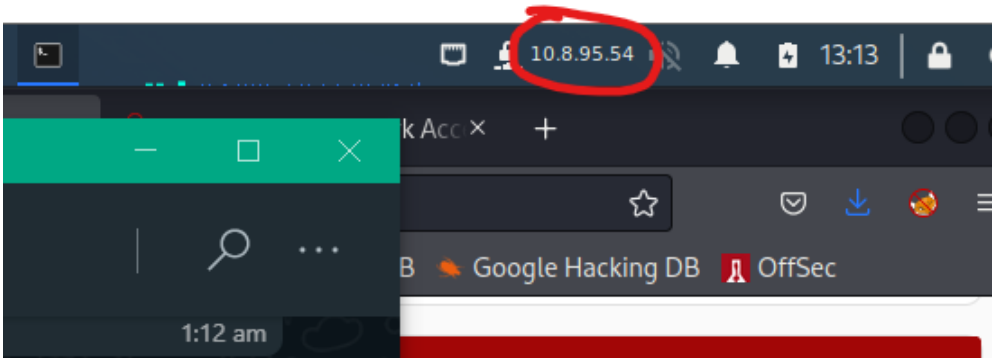


and putting in the reverse shell command in it.

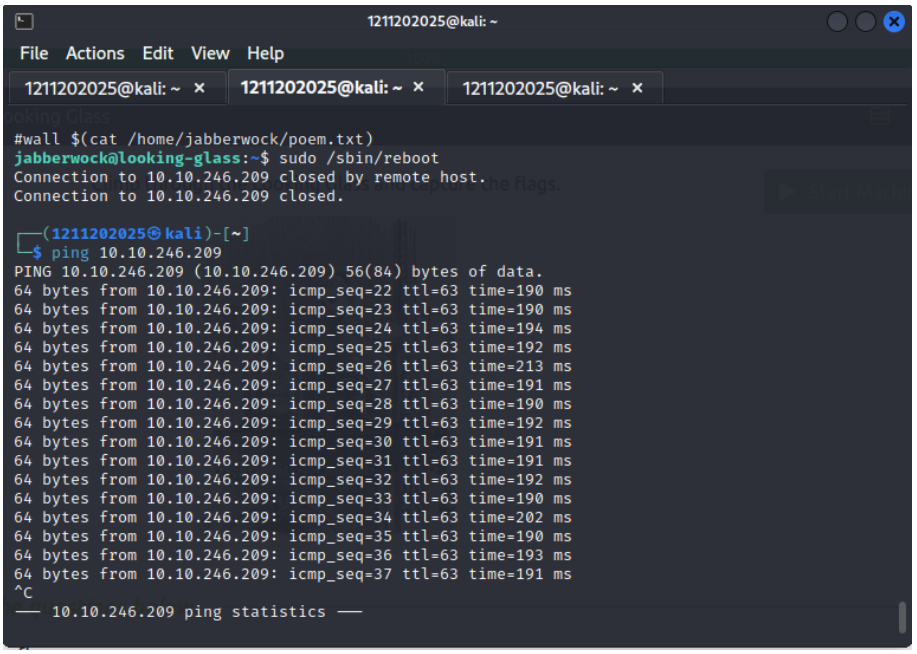


Just to make sure that we are putting in the correct ID, we used the command hostname -I on our Kali machine and got 10.8.95.54.

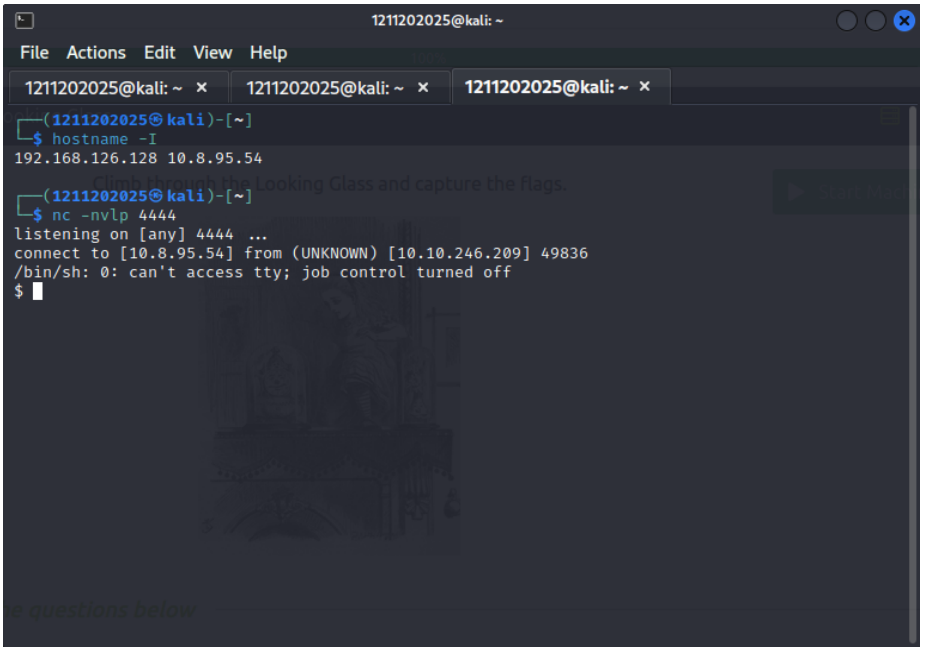




Now we can start a netcat listener on our Kali machine. After starting, we then reboot the box and ping the machine's IP on our Kali machine.



That allows us to get a connection when it comes back up.



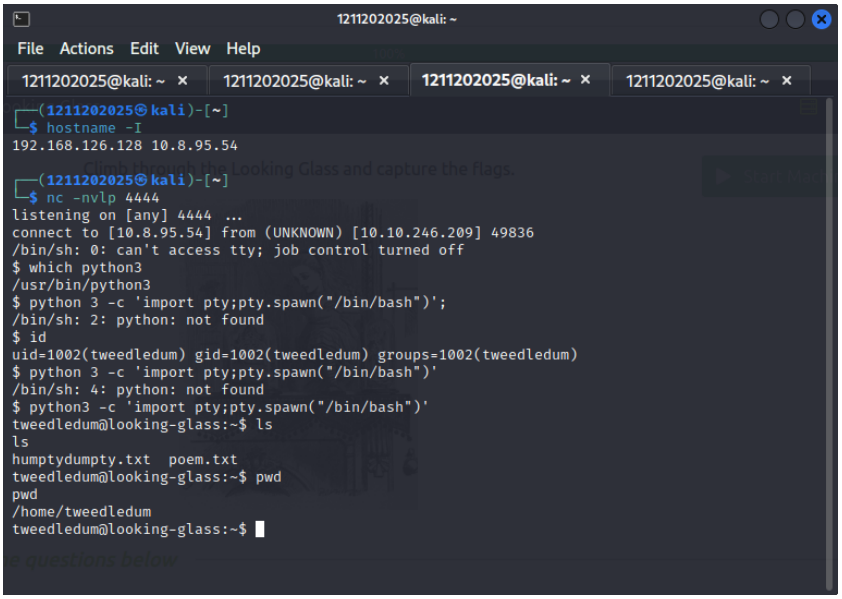
Horizontal Privilege Escalation

Members Involved: Abdullah

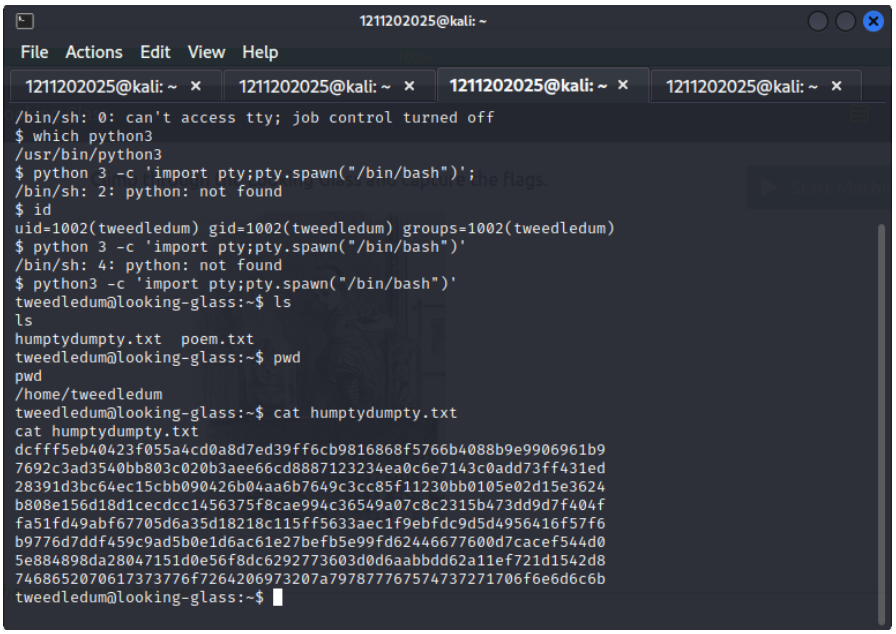
Tools Used: Kali Linux, Attackbox, Terminal, Firefox

tweedledum -> humptydumpty

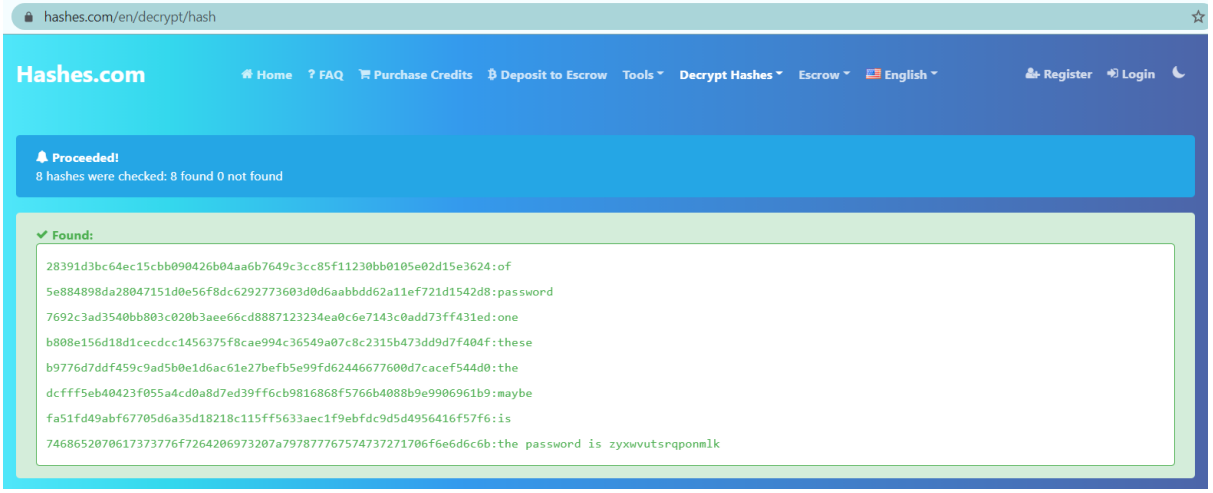
By entering id, we know that we are tweedledum. But we still need to upgrade to a proper shell, and we did so by using the python3 command.



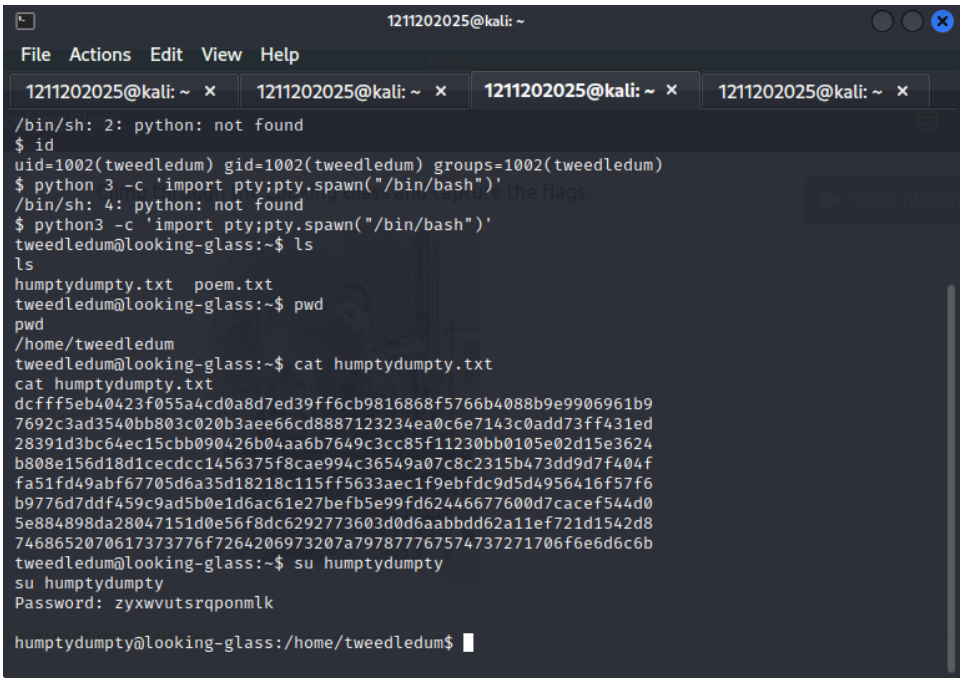
Looking into the user tweedledum, we were able to find text files named humptydumpty.txt and poem.txt. Using command cat to check further into humptydumpty.txt first, we found a series of something that looks encrypted.



Using hashes.com, we can see that the last line is the most suspicious one, telling us the password, but who is the question here.

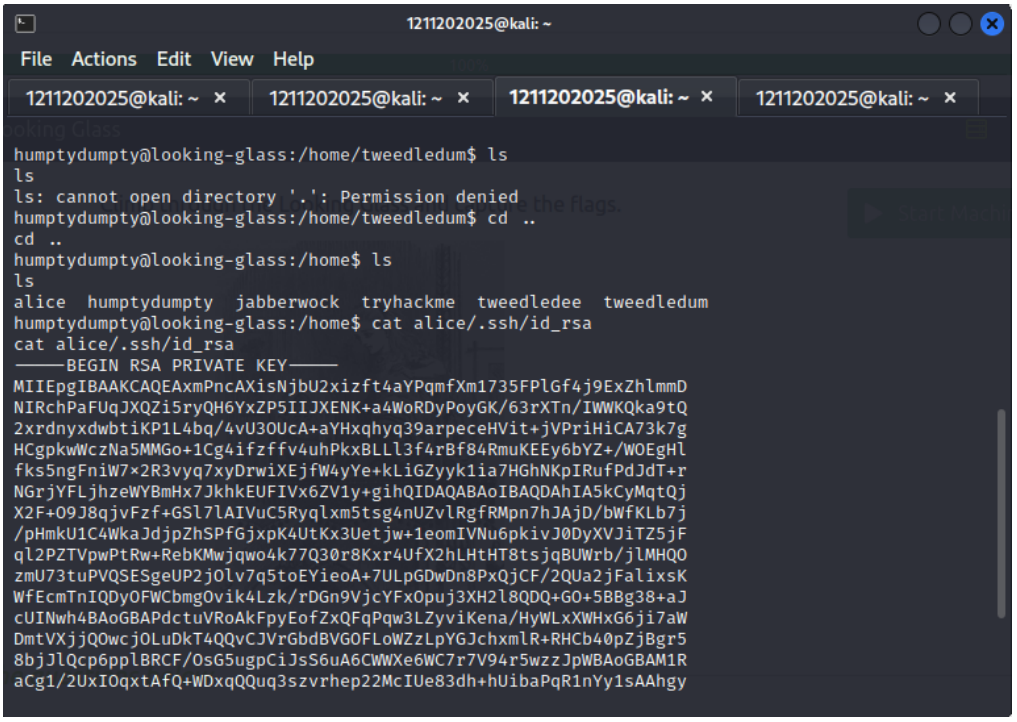


Using our luck and knowledge from before, we know that there is a user named humptydumpty and since this file that tells us the password is named after him, we use the command su humptydumpty to switch user to him and using the acquired password, we were able to logged in as him.

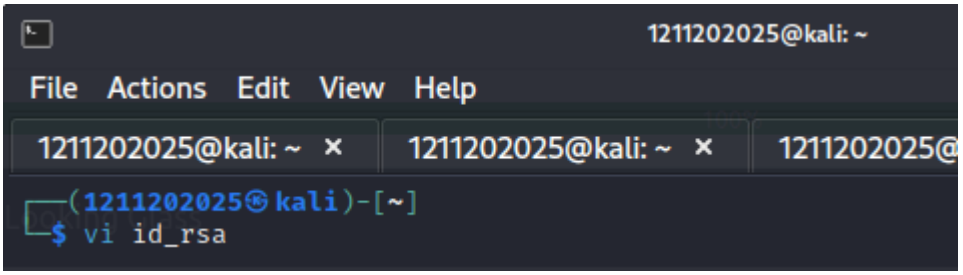


humptydumpty -> alice

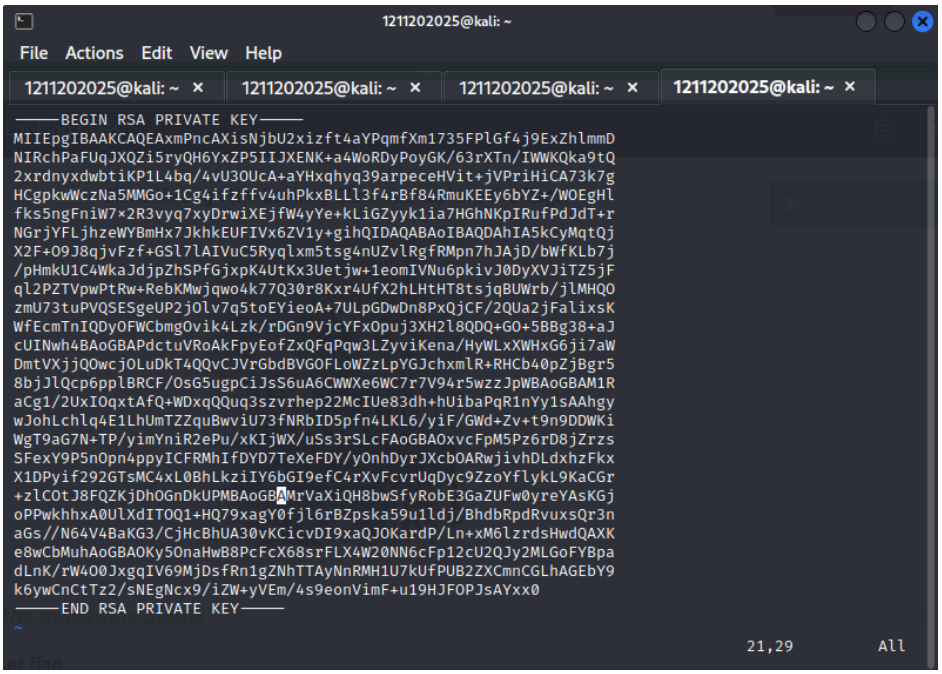
After logging in as always, we used ls to check what was inside. And we see alice here which is good, since she seems like our main objective here. We also did the command cd to change directory into some places, particularly here home directory. Then, we used the command cat alice/.ssh/id_rsa to check and see her private key, and indeed we got it.



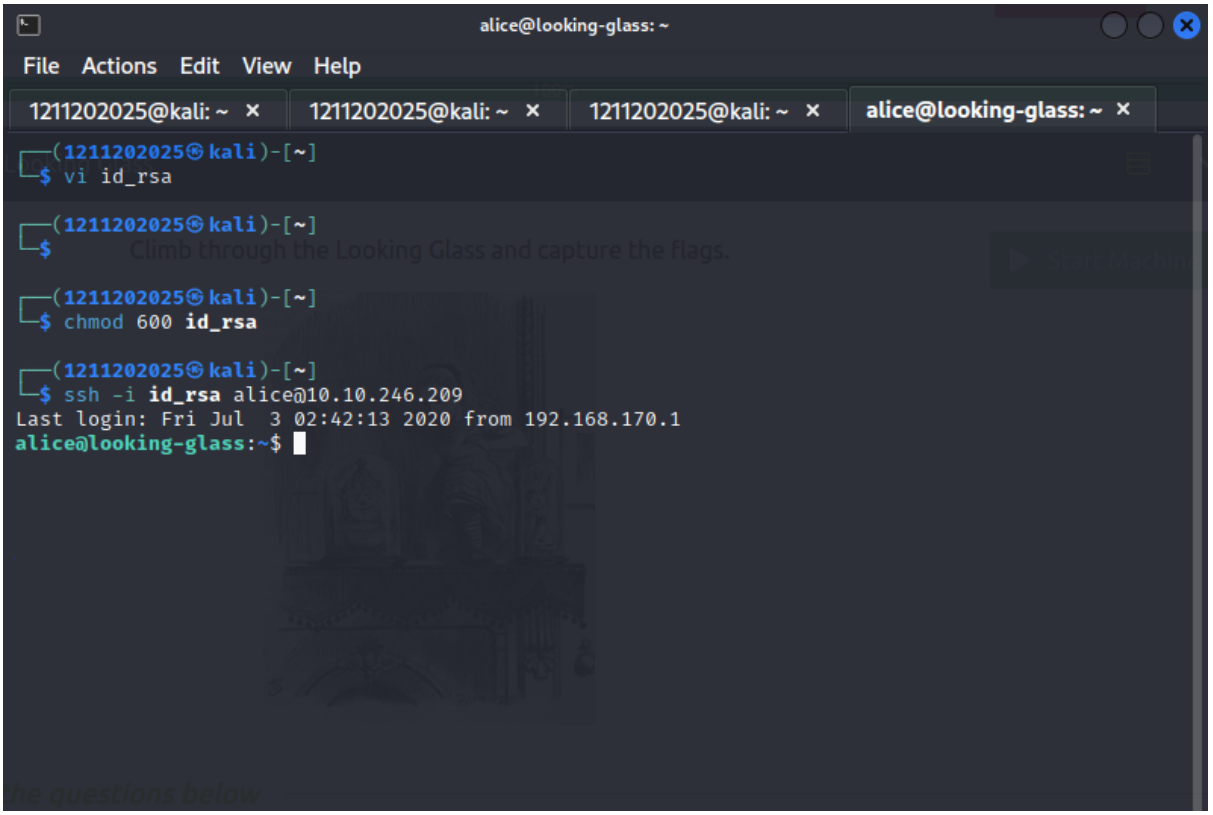
Using the command vi, we created a file named id_rsa,



and we copied and pasted the whole RSA private key in that particular file.



Going back to our Kali machine and using the command, we can now ssh to alice using the file that we recently created. And there, we were able to log in as alice now.

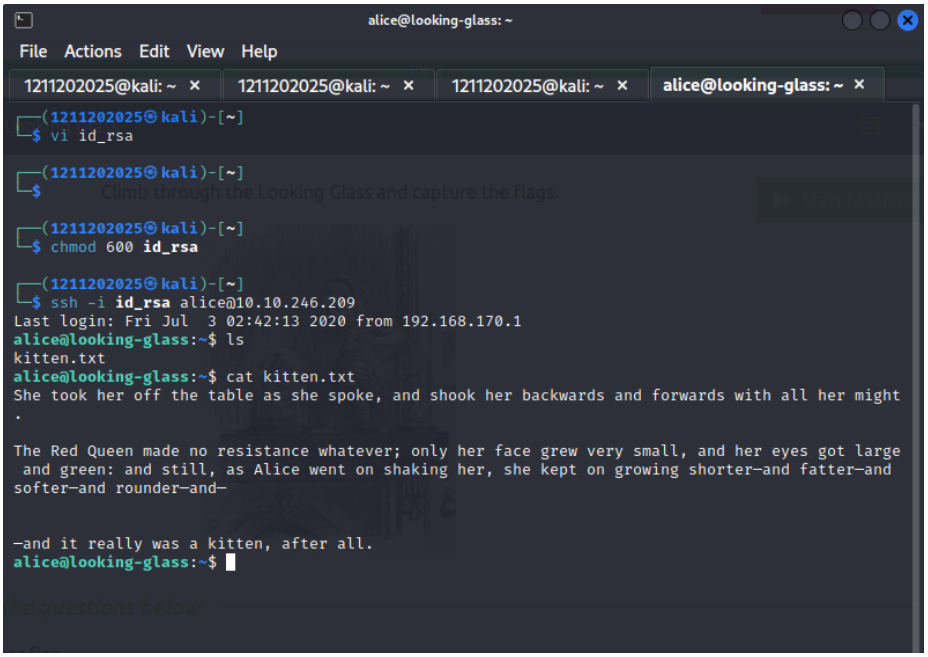


Root Privilege Escalation

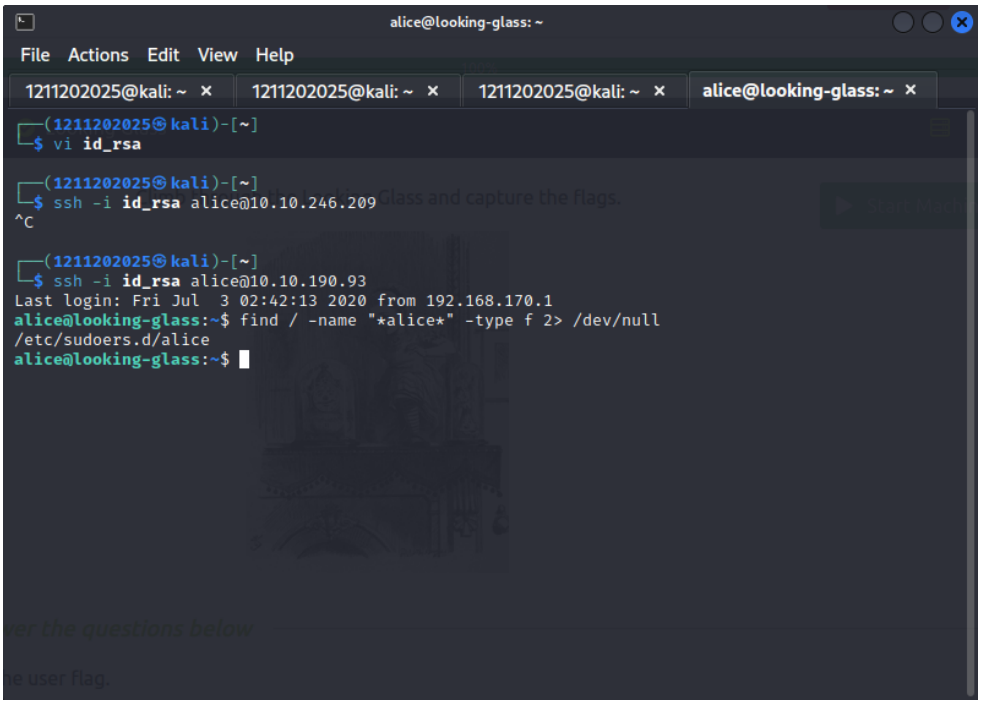
Members Involved: Abdullah

Tools Used: Kali Linux, Attackbox, Terminal, Firefox

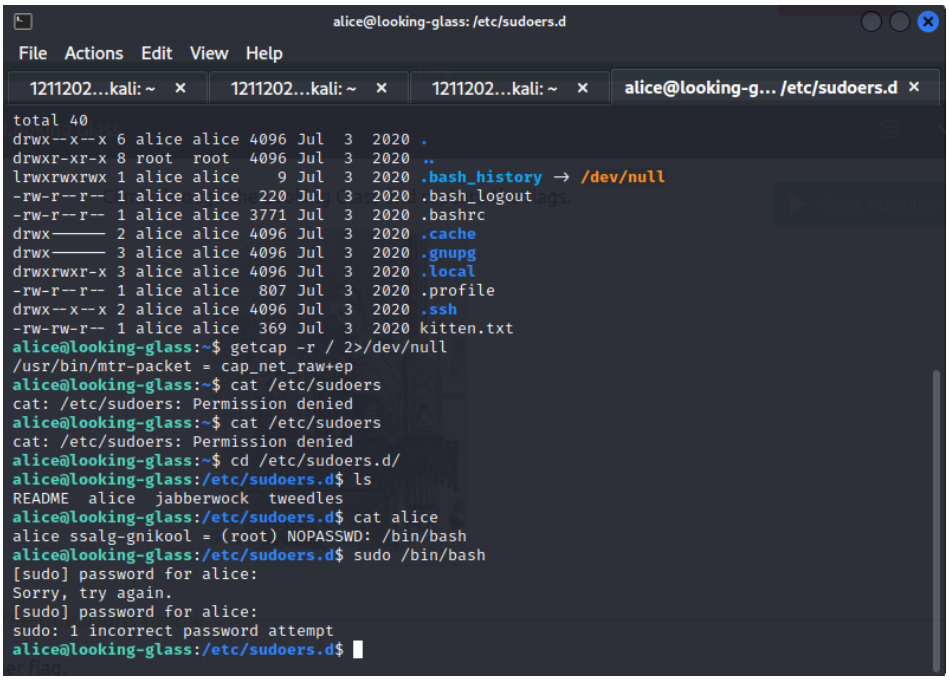
Using the ls command, we see that there is only a single text file inside, and using the command cat, we can see the content of the file.



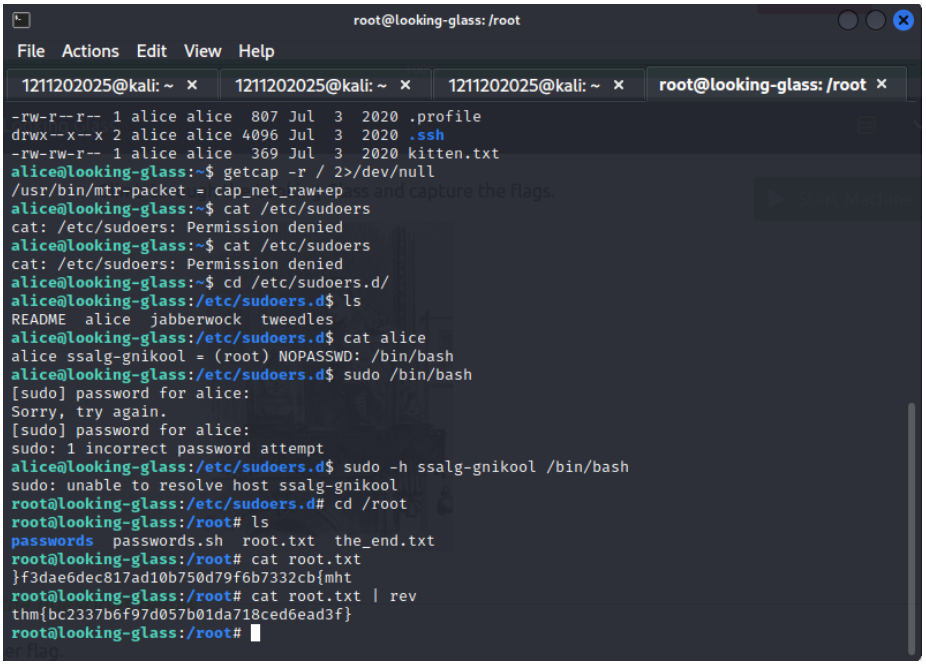
Using the command and specifying the name alice, we were able to find the sudoers directory.



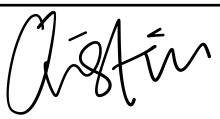
And from there we can go to that directory and using cat alice, we get to know that we cannot execute the /bin/bash command since we are not the right hostname.



So, by simply using the command -h and the right hostname that we want, we were able to escalate to root. Then using ls to check, we were able to find the root.txt file and using cat root.txt, we got the second flag.



Contributions

ID	**Name**	Contribution	Signatures
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Did the recon and enumeration stage	
1211202025	Abdullah Bin Kamaruddin	Did the initial foothold, horizontal and root privilege escalation	
1211103649	Nur Qistina Binti Roslan	Edited most of the google docs and youtube video	

VIDEO LINK: https://youtu.be/l2qXiMPnjxg