PenTest 1

ROOM: LOOKING GLASSES

STUDY GROUP

Members

ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211102835	Chew Ming Yao	Member
1211101534	Tan Chi Lim	Member

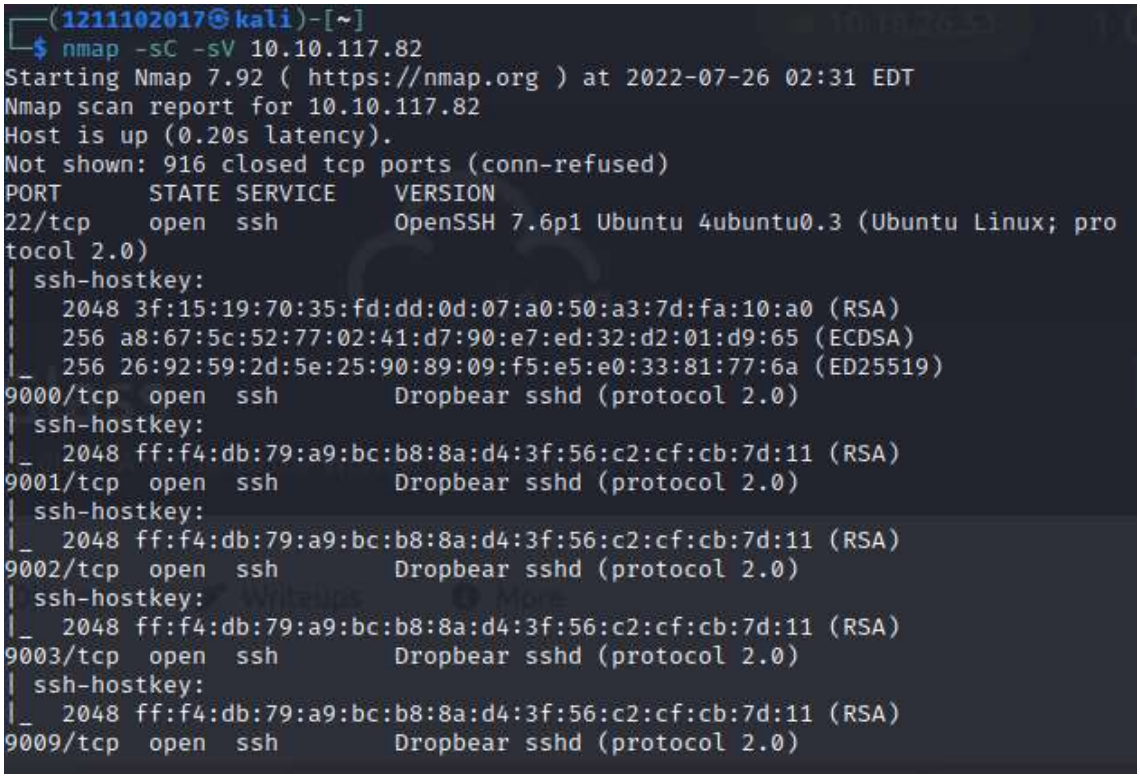
Steps: Recon and Enumeration

Members Involved: Chew Ming Yao

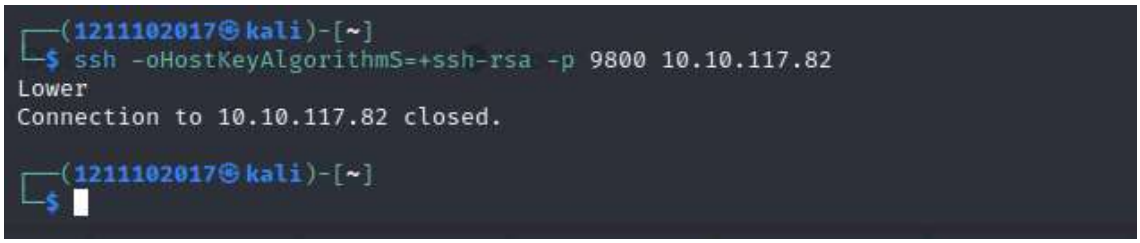
Tools used: Nmap/Vigenere/SSH/Online text reverter

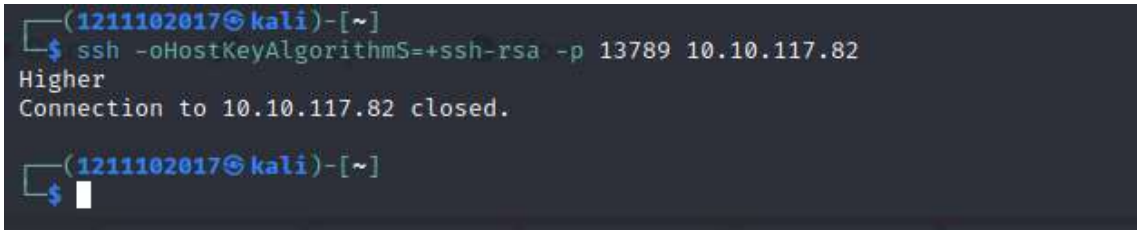
Thought Process and Methodology and Attempts:

Chew Ming Yao use the Nmap to scan all the open port that is available using the Ip address

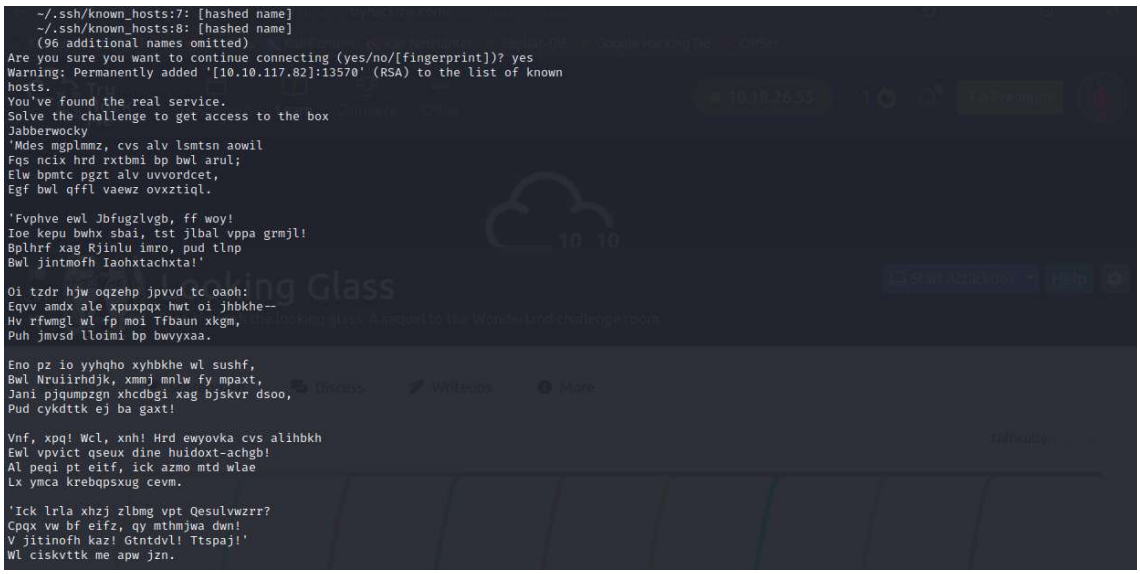


Later, Ming Yao used the ssh to test all the ports found by using the ssh command. And then he found that if the port is not correct it will be shown higher and lower, which can be used to guess the correct port number [higher means that the port number is higher than the correct port number, lower means that the port number is lower than the correct port number]



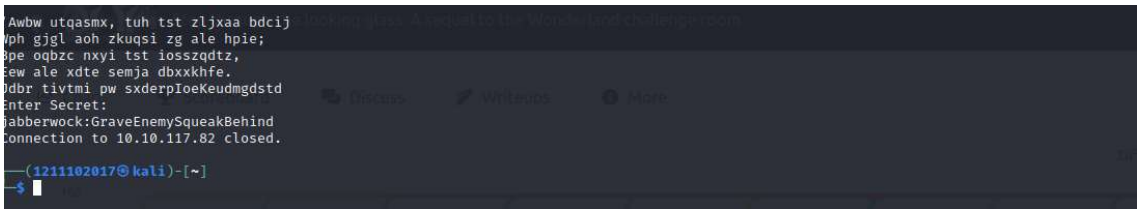


After a few trials, Ming Yao found that a text was shown up with the correct port number.

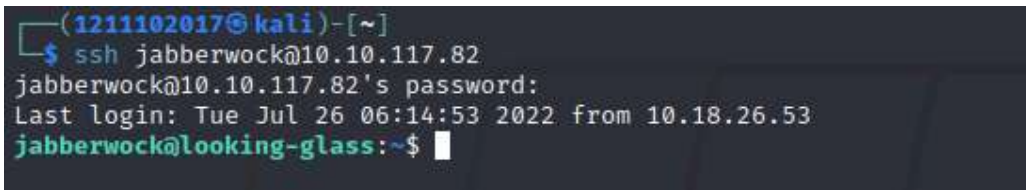


After that, Ming Yao decodes by using the link at reference which to decode the Vigenere. And then he found that there is a secret password after the decoded the text given.

Ming Yao login by using the secret password that was found just now

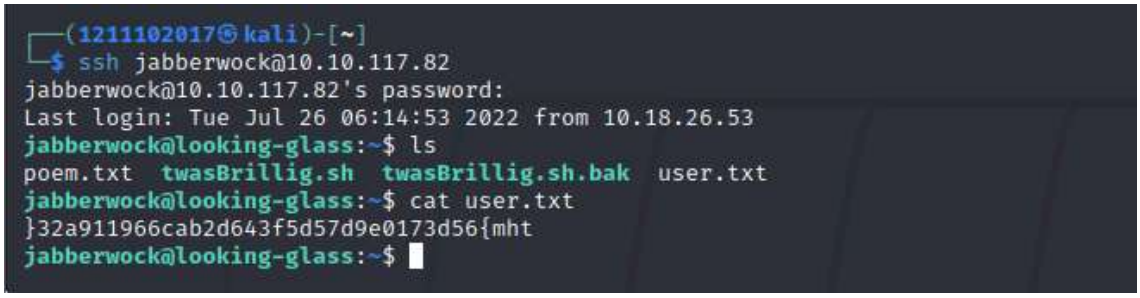


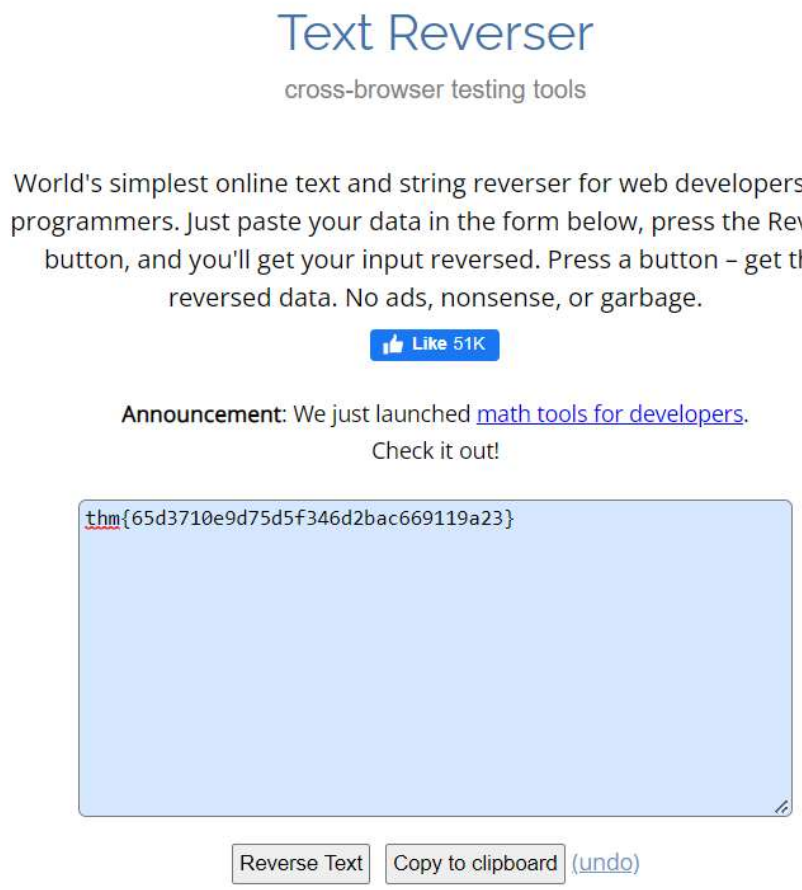
After that, Ming Yao switch the user to Jabberwock by using ssh and used the password given just now, lastly, he successfully login into the Jabberwock account.



Final Result

Use command ls, and then Ming Yao found that there is a user.txt file and used the cat command to view it. Lastly, the flag was shown in reverse, we copy it and use text reverter to correct it.





Step: Initial foothold

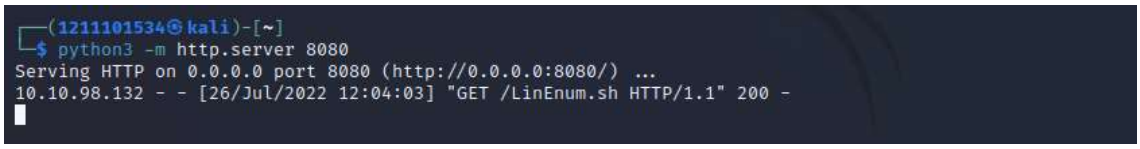
Member involves: Tan Chi Lim

Tools used: LinEnum/netcat/reverse shell/sudo

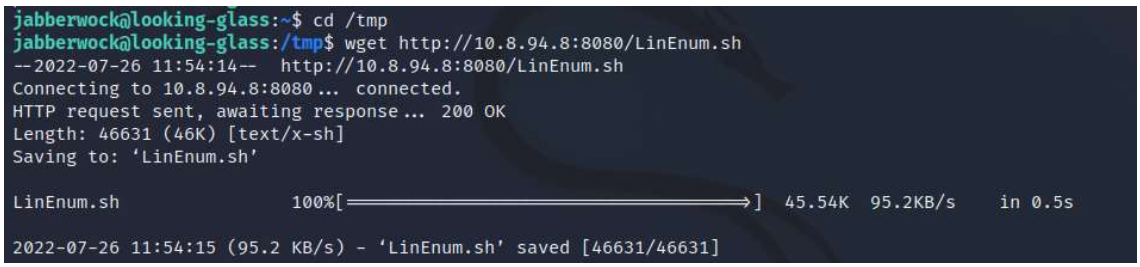
Thought Process and Methodology and Attempts:

Tan Chi Lim used LinEnum to enumerate the target machine. First, download the LinEnum on your machine.

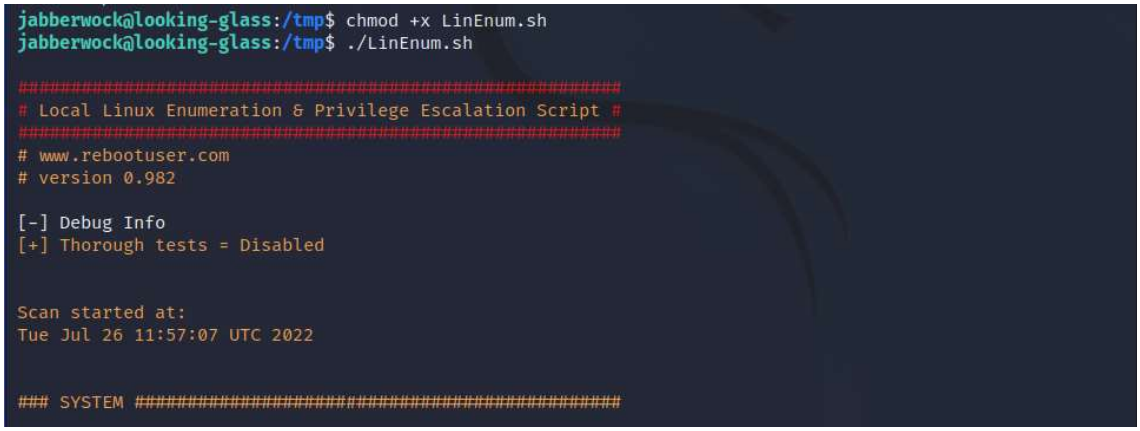
Then, Chi Lim use python3 to turn your machine into a web server.



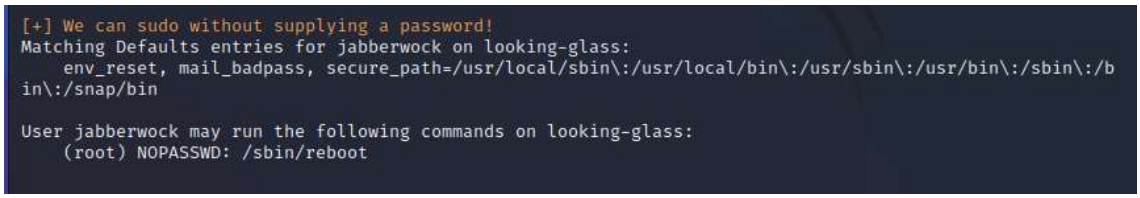
Then, Chi Lim gets the LinEnum from the web server.



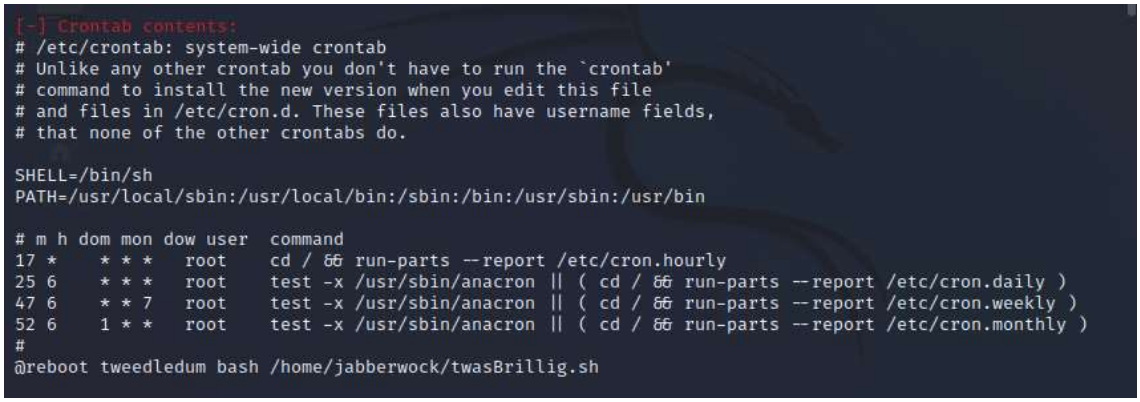
Chi Lim add the execution permission to LinEnum.sh and execute LinEnum.sh on the vulnerable Instance



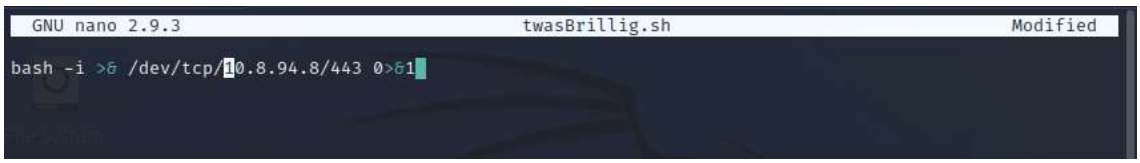
Chi Lim use the command sudo -l to find out what command we can use. We found that command /sbin/reboot is the sudo command that we can use to reboot the server without a password



Chi Lim also found that tweedledum will execute the twasBillig.sh when we reboot. So we can make a reverse shell and execute the reboot.

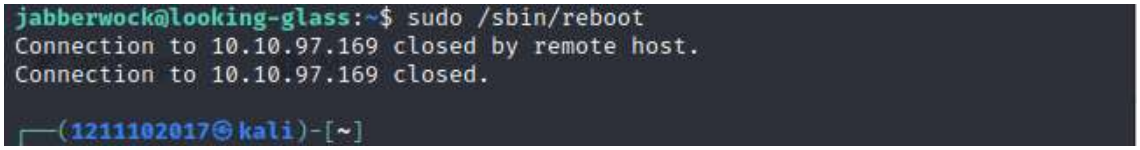


After that, Chi Lim uses the Netcat command to make a reverse shell in the twasBrillig.sh file, so that we can access other user accounts by rebooting the server.



After that, Chi Lim open another terminal and set a netcat listener to port 4444 that we had set just now.

Then he use the command just now to reboot the server, and we wait for the netcat to show up,



Step: Horizontal Privilege Escalation

Member involves: Siow Yeeceng

Tools used: Netcat/Cyberchef/ SSH

Thought Process and Methodology and Attempts:

after finding some resources from google, Siow Yee Ceng know that the command python -c 'import pty; pty.spawn("/bin/bash")' is used to spawn another shell and begin to make it interactive

Modern Ubuntu installs come with python3 installed, we can spawn another shell and begin to make it interactive:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@08d09e204883:/var/www/html/vulnerabilities/exec$

www-data@08d09e204883:/var/www/html/vulnerabilities/exec$ echo $0
echo $0
/bin/bash
www-data@08d09e204883:/var/www/html/vulnerabilities/exec$
```

There are many ways you can make your shell interactive if Python is not installed.

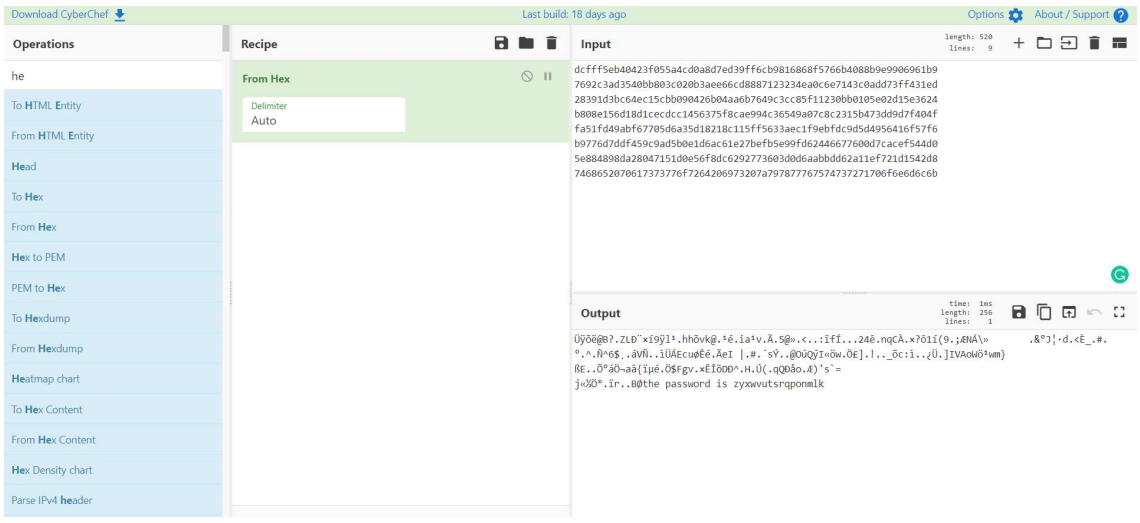
He use command id to check who's account are we in and also get into the tweedledum's account.

After Yee Ceng get into tweedledum account, we used command ls to see how many files were inside this account. After that, we used the command cat to check all the files one by one. And then we find a mysterious text inside the humptydumpty file.

```
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ cat poem.txt
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
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
```

Since the largest alphabet in this txt file is F Yee Ceng get to know that this is based on hexadecimal. And he copy all of it and then puts it into cyberchef and a secret password shows up



From the password file just Yee Ceng knows that there is a username called humtydumpty, and he believes that the password just now is the password of humptydumpty. Then he use command su to switch between users and we type in the password found just now.

```
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

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

Once He get into the humptydumpty's account, He used the command ls to look for all the directories, and it has shown nothing. So when Yee Ceng get into the home directory and use the command ls again, we found some files inside.

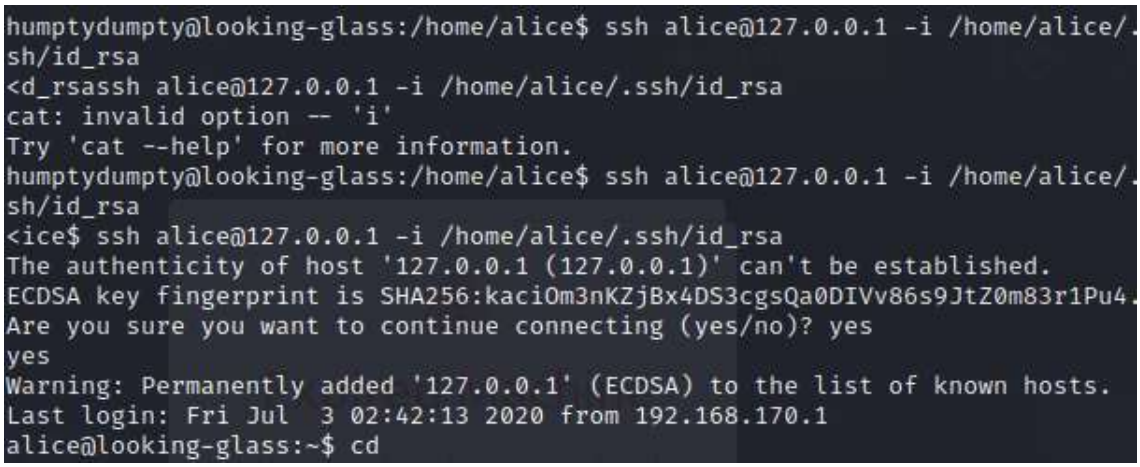
```
humptydumpty@looking-glass:~$ cd /home
cd /home
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ ls -ls
ls -ls
total 24
4 drwx--x--x 6 alice        alice        4096 Jul  3  2020 alice
4 drwx------ 3 humptydumpty humptydumpty 4096 Jul 26 10:11 humptydumpty
4 drwxrwxrwx 5 jabberwock   jabberwock   4096 Jul 26 09:54 jabberwock
4 drwx------ 5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
4 drwx------ 3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
4 drwx------ 2 tweedledum   tweedledum   4096 Jul  3  2020 tweedledum
```

Yee Ceng had tried a few ways to gain access to Alice's account but finally, we got the rsa key by using ssh

```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
ls -la .ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
cat .ssh/id_rsacat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
```

Final Result

After that He use ssh to get into Alice's account, by using all the information we gain just now.



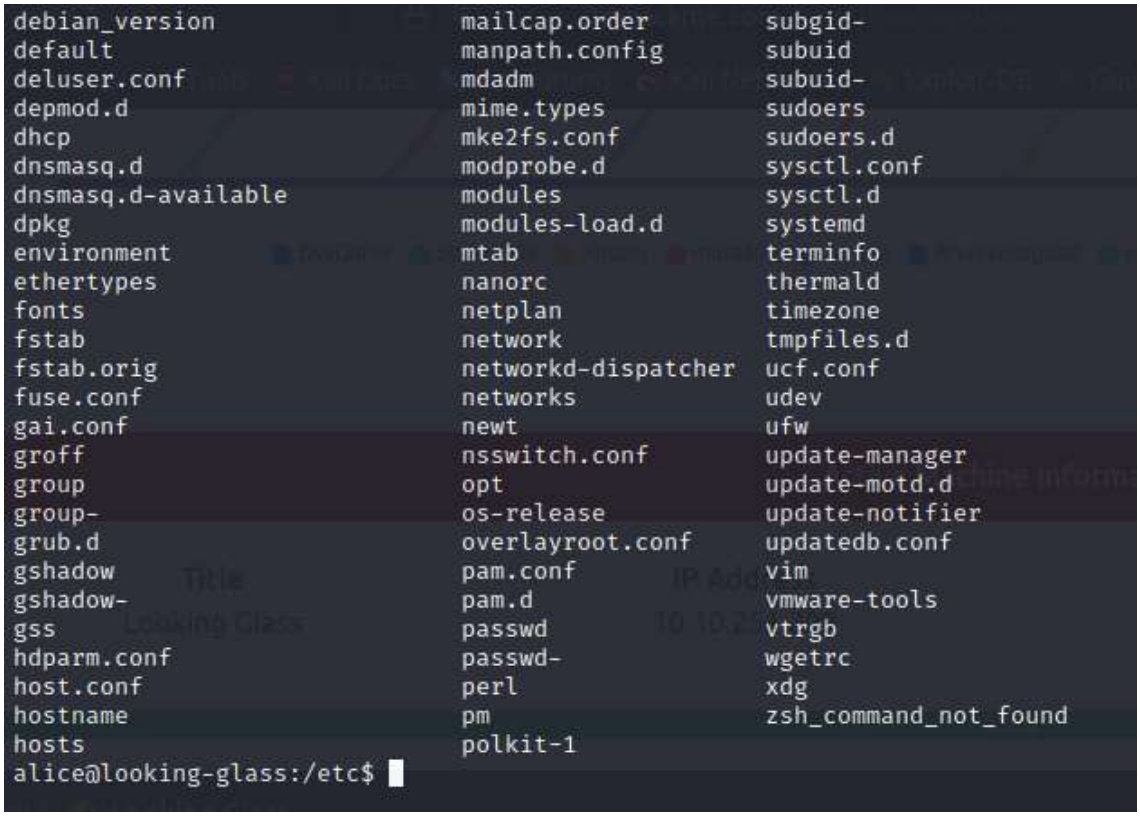
Step: Root Privilege

Member involves Lo Pei Qin

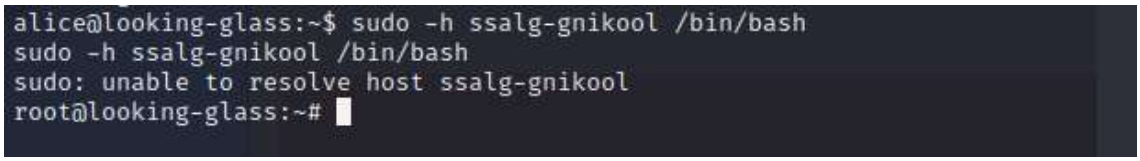
Tools used: **SSH/Netcat/Sudo**

Thought Process and Methodology and Attempts:

Lo Pei Qin get into the etc directory and then we look through one by one and lastly we found that file sudoers.d is the root

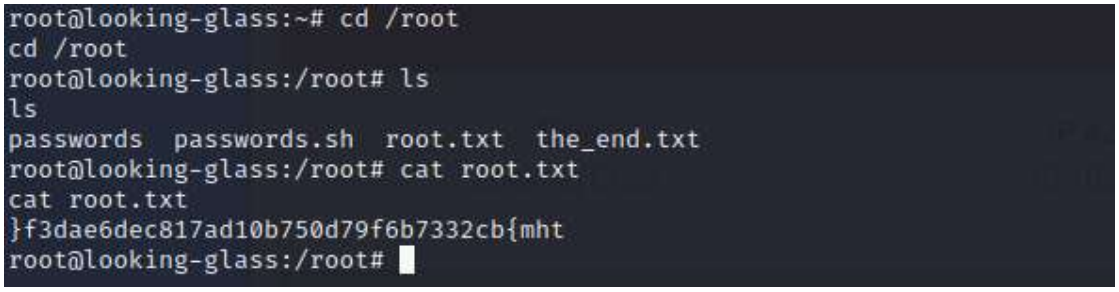


He use sudo -h to and the command given just now to gain access to the root.



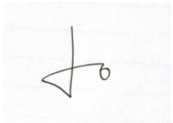
Final Result

Lastly, He go to the root directory and use ls to list all the files contain, he saw that there is a root.txt file and lastly he finally captured the flag of the root.



Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211101157	Lo Pei Qin	Root privilege / Writeup	
1211101534	Tan Chi Lim	Initial foothold / Video editing	
1211102835	Chew Ming Yao	Recon and Enumeration / Video editing	
1211102017	Siow Yee Ceng	Horizontal Privilege Escalation / Writeup	

VIDEO LINK: https://youtu.be/d-Dr0ZL1uz4