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

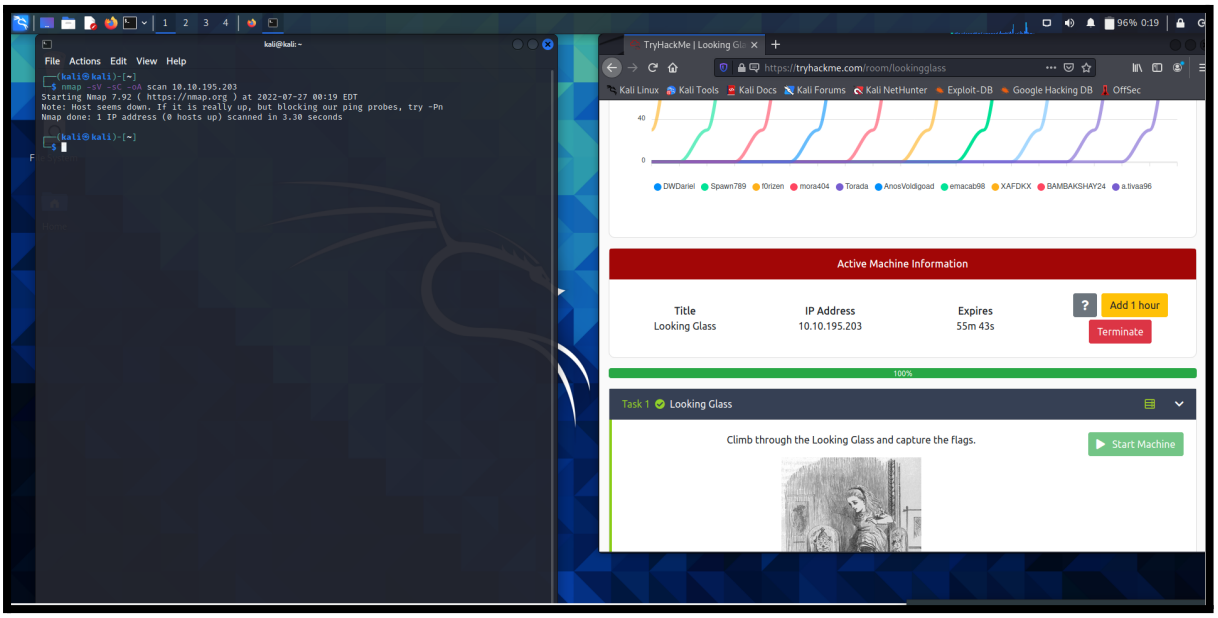
Steps: Recon and Enumeration

1) Recon and Enumeration

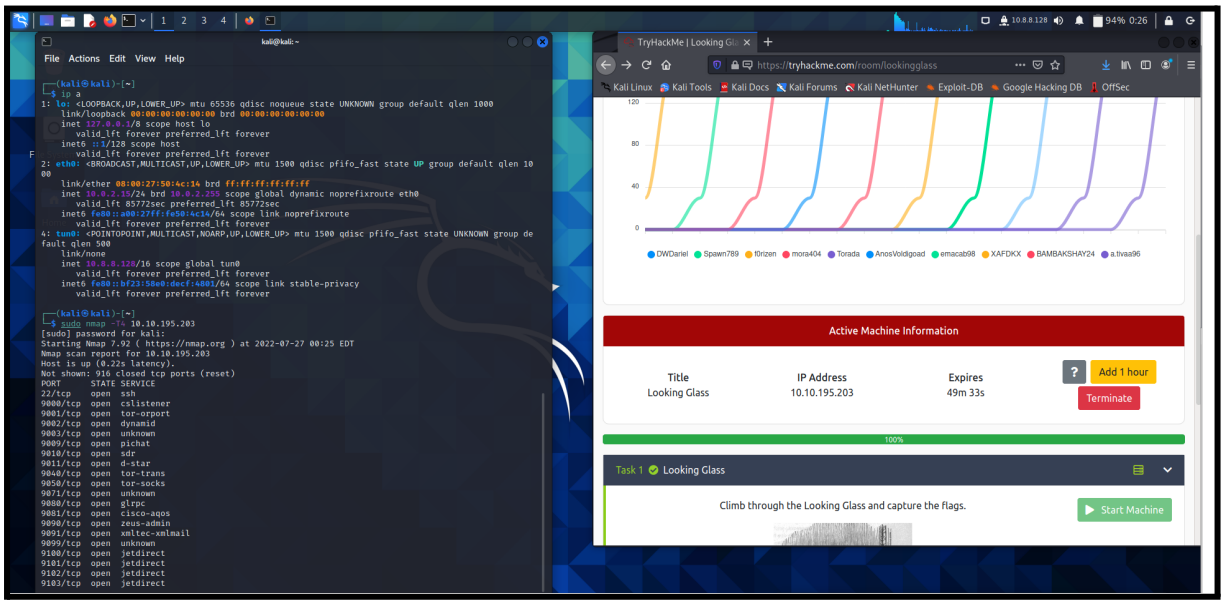
Members Involved: Tivaasheny Ananthan

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.

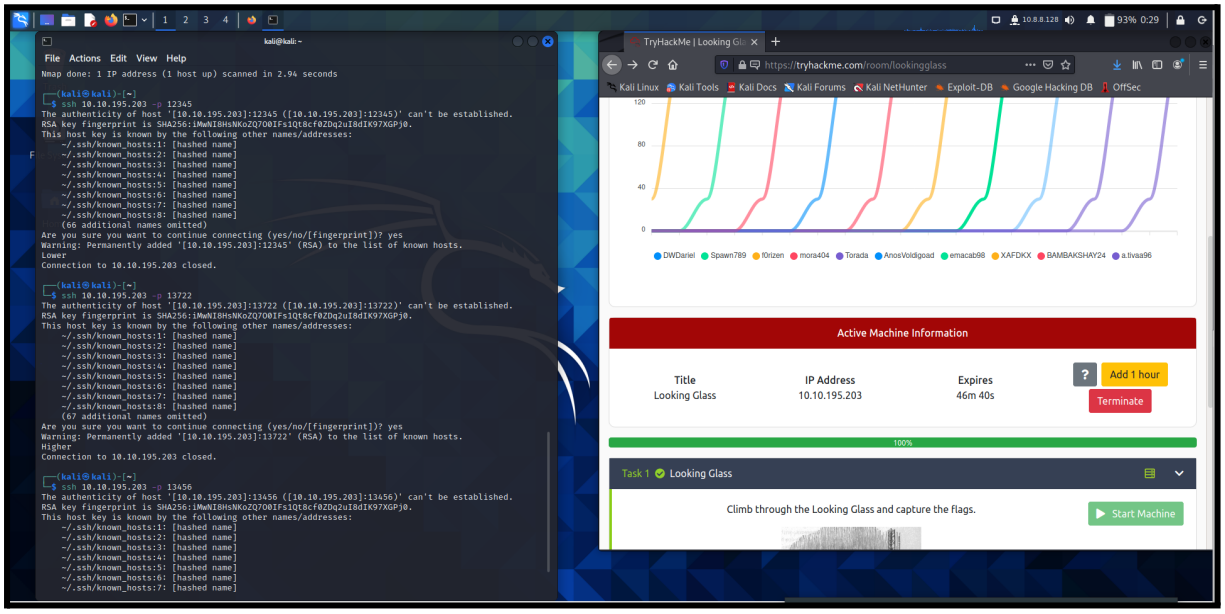


2. Gaining Access

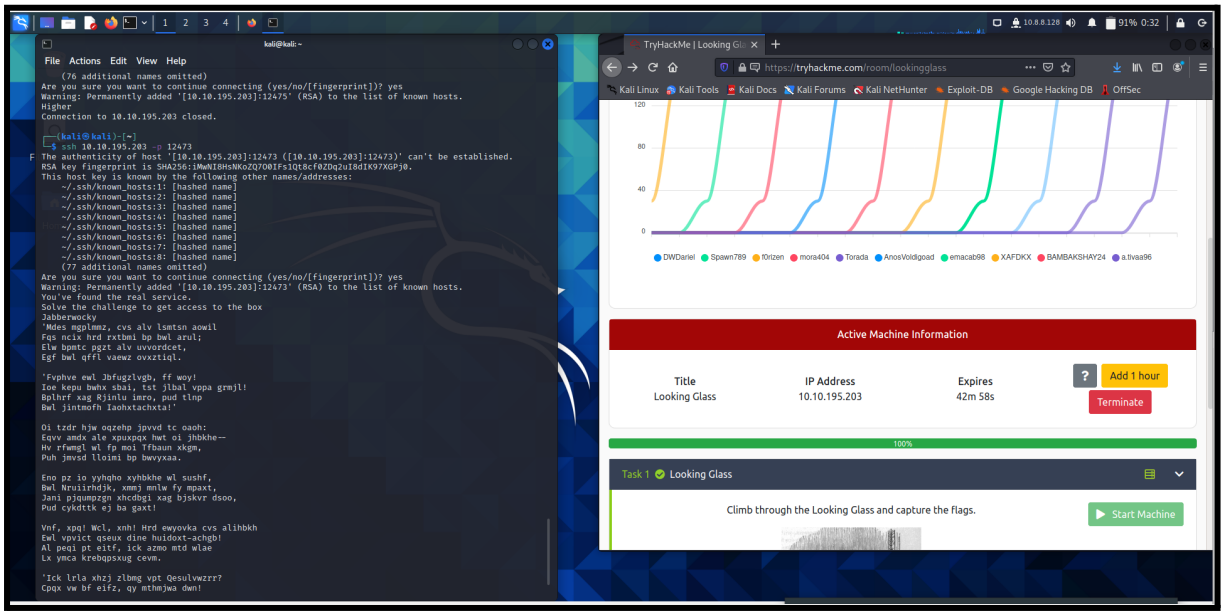
Members Involved: Tivaasheny Ananthan

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

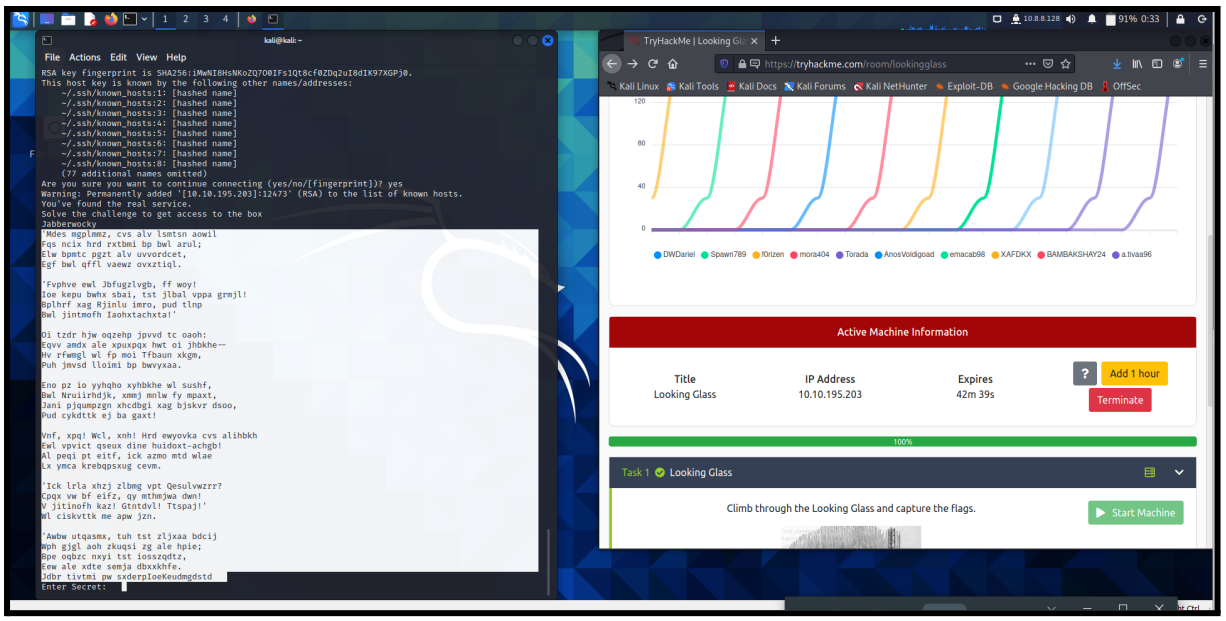
When we ssh to a port there are two outputs that we will get which are Higher and Lower. After some time we will know that this is mirrored. Which if the output is Lower that means you need to get a higher port. If the output is Higher that means you need to get a lower port. We have to find the correct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



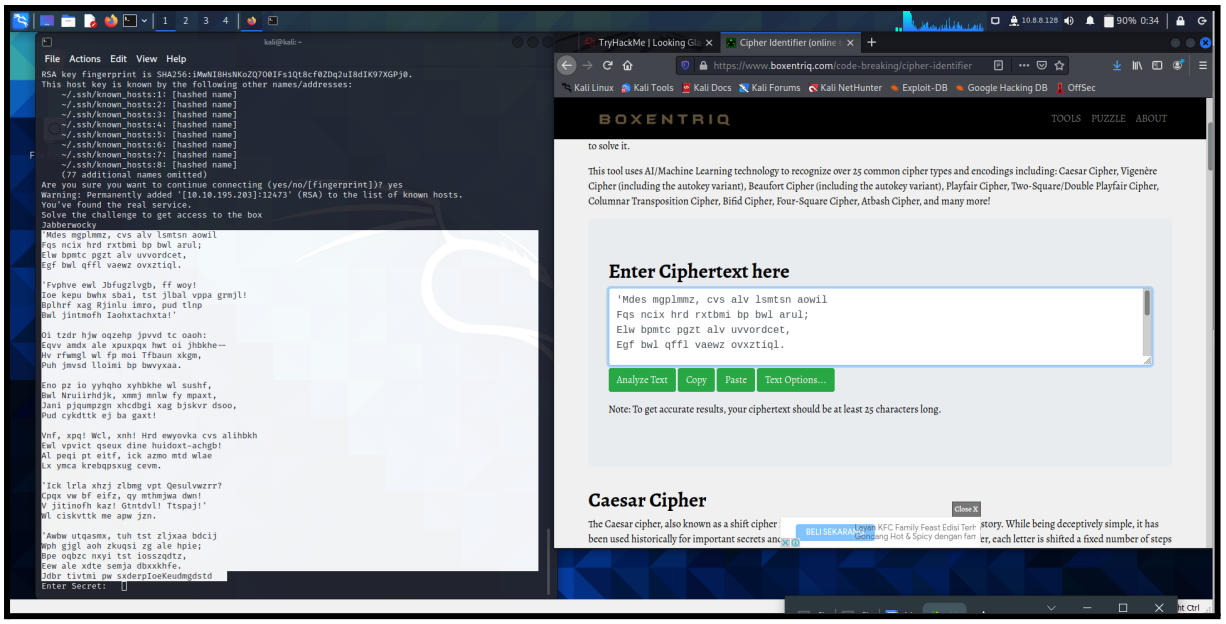
After some trials we managed to get the correct port.



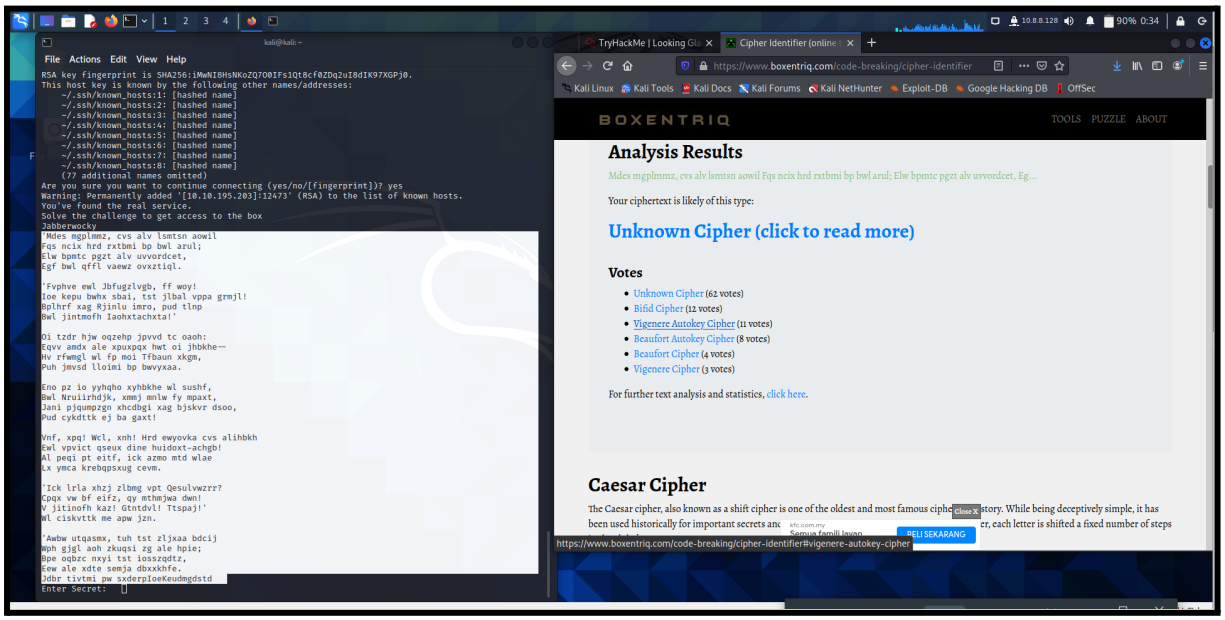
Then we need to copy the encoded text to decode.



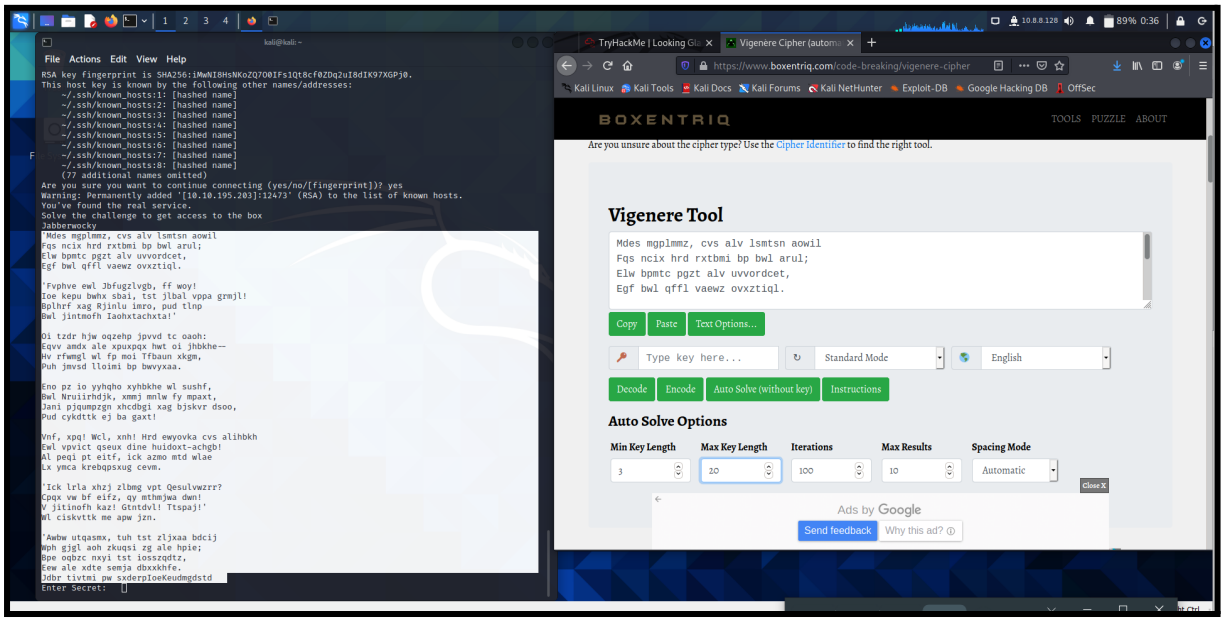
Now we have to copy paste that in the cipher identifier and analyzer. Then we have to remove(‘) this in starting of the paragraph and press analyze text.



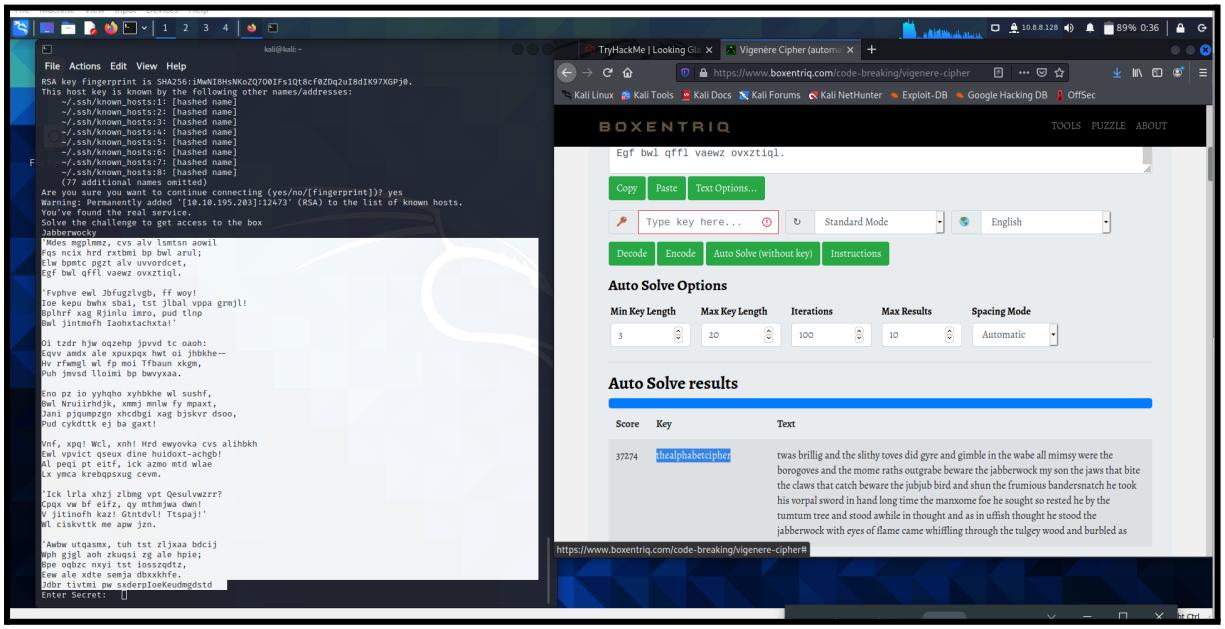
Now we have to press vigenere Autokey Cipher to open vigenere tool and paste it.



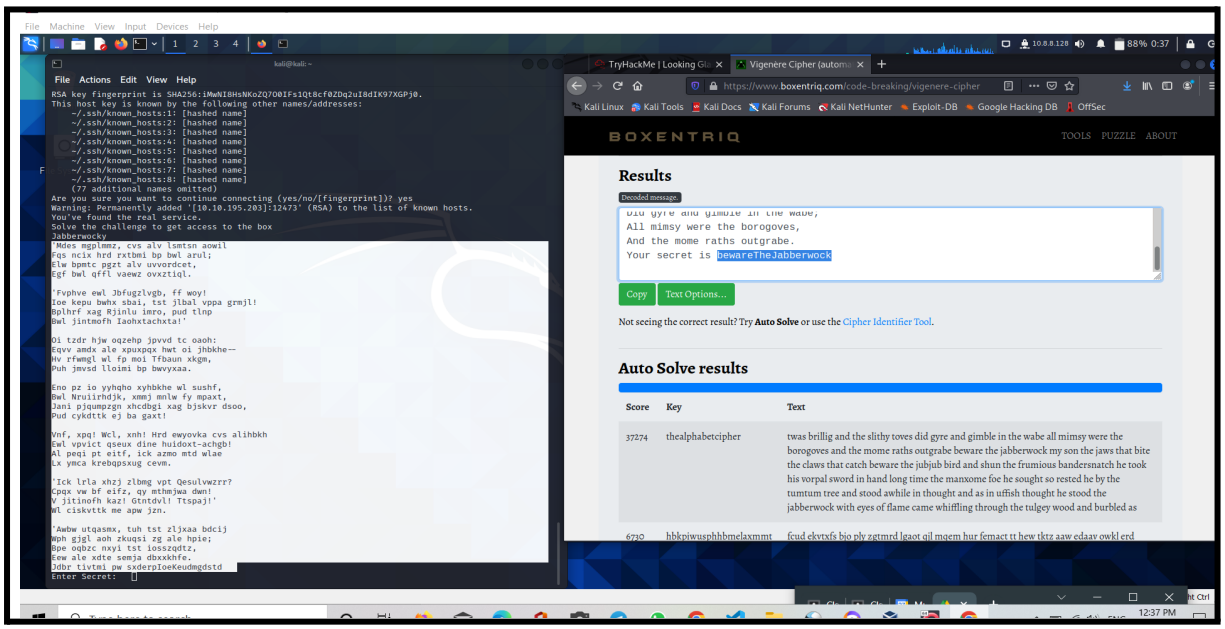
We have to change the max key length to 20 and press auto solve withoutkey.



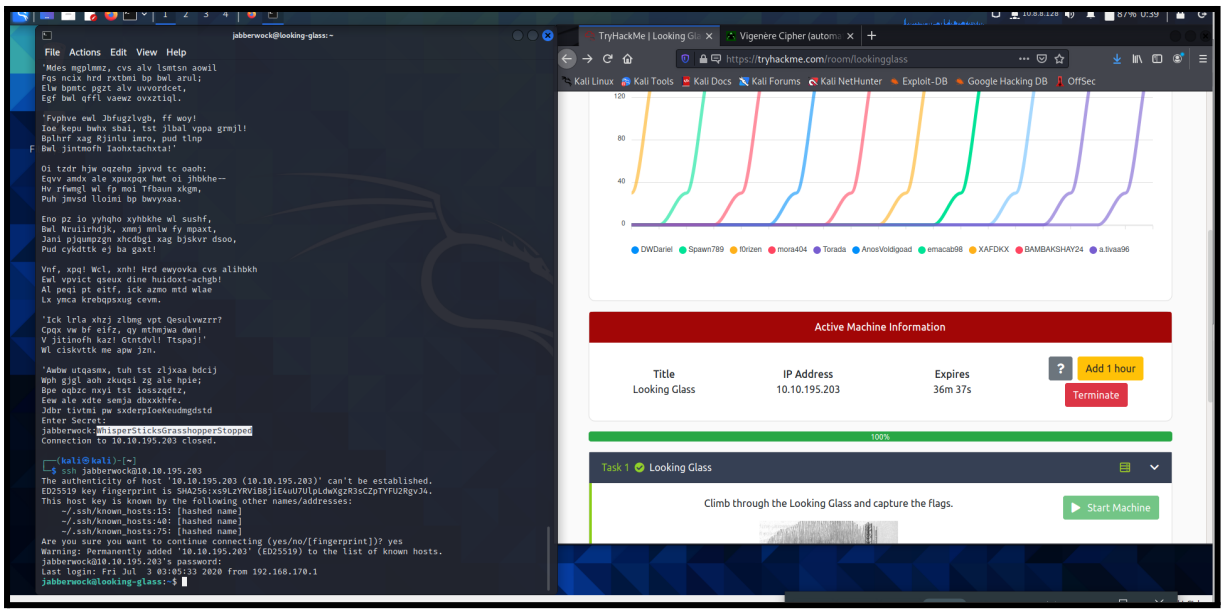
Then we have to copy the first key and paste it there to decode.



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



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:

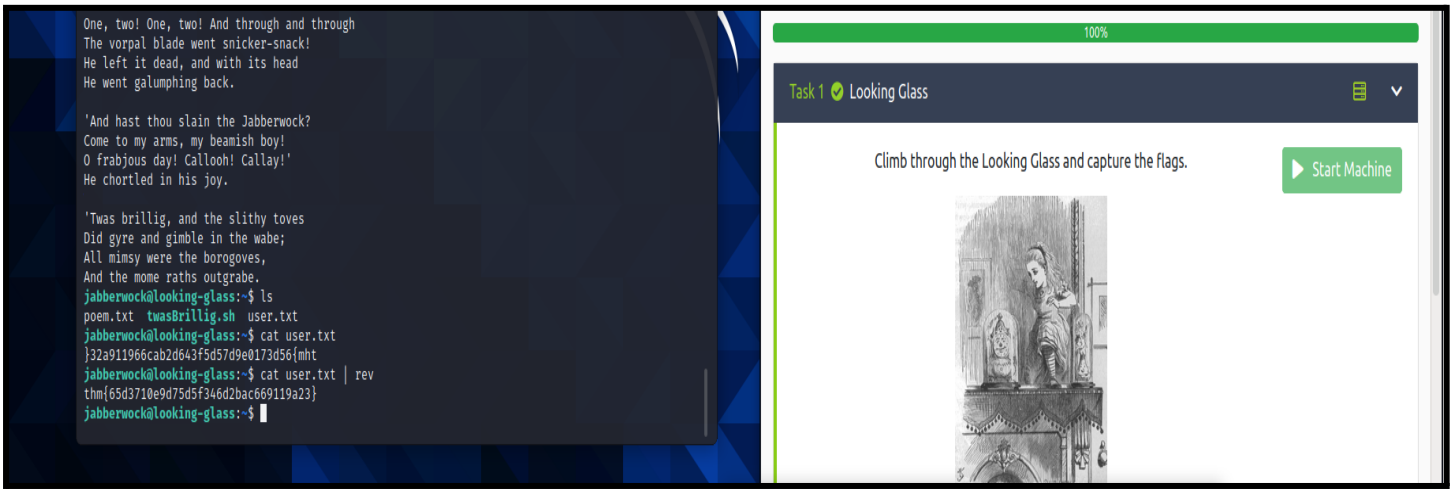
We have to scan nmap and find cirrect portal. Then decode the encoded text to get secret. Then paste the secret to get jabberwock password. Next we have to ssh jabberwock n paste the password that we get when put the secret.

Steps : User Flag

3. User Flag

Members Involved: Hemma Ravindran

Tools used: Kali linux , Terminal



Thought Process and Methodology and Attempts:

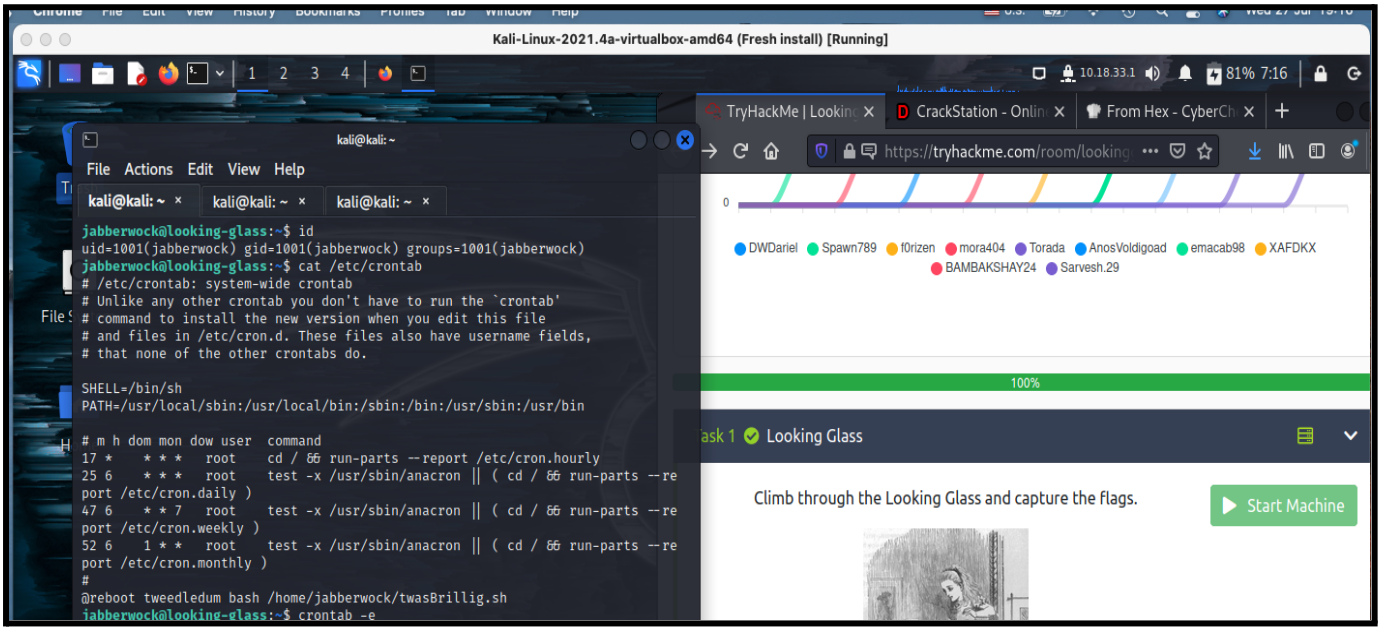
Looking at the files, the result when you connect to the port is poem.txt and twasBrillig.sh. It's intriguing that the script has read, write, and execute rights. The user.txt file is our first flag, but you'll need to flip it around because it's backwards.

Steps : Privilege Escalation

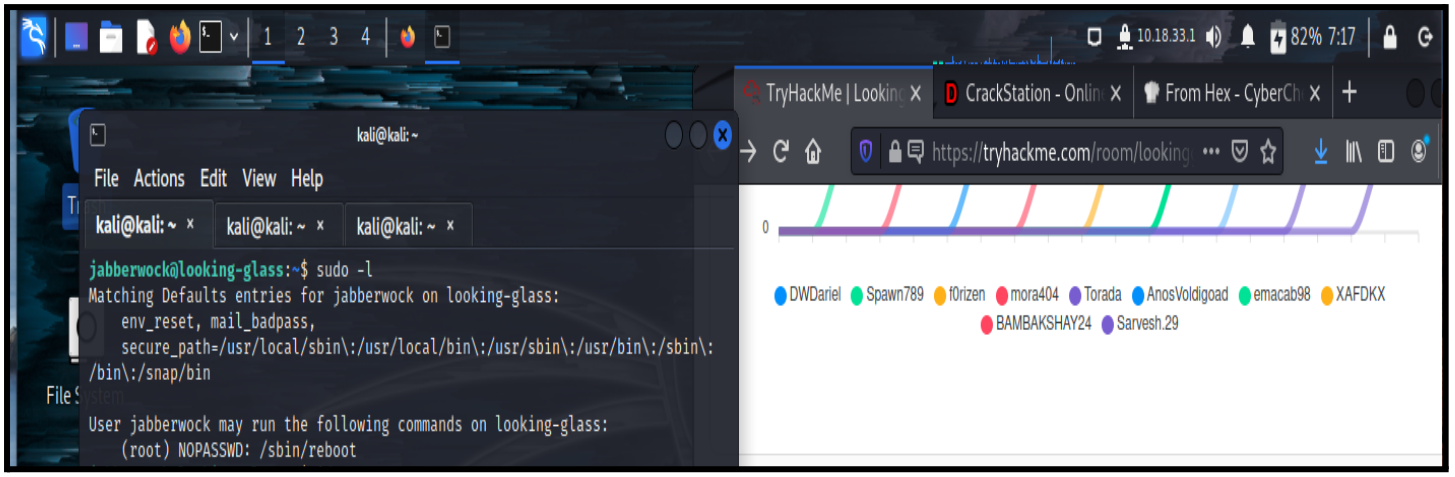
4. Privilege Escalation

Members Involved: Hemma Ravindran
Tools used: Kali linux , Terminal , PentestMonkey

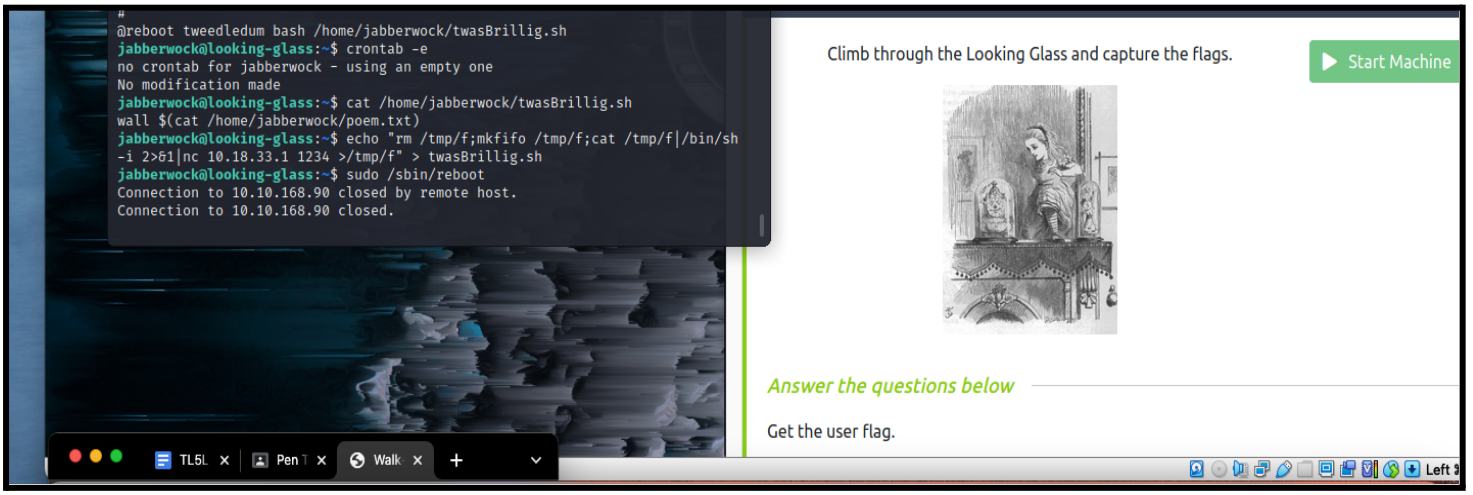
Now we need to figure out how to get to root. A quick look at the passwd file reveals that there are several users. We can also look into crontab. This could assist us in determining what is running when the box boots that causes the random port to respond.The bottom line indicates that when the server 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.



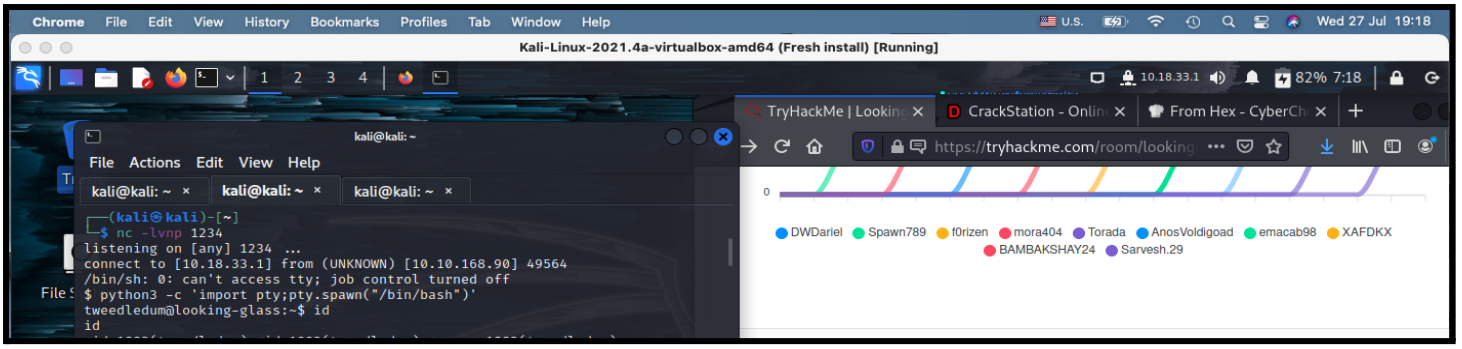
Next, we have to know which sudo permission we have.With the permission we can now reboot the box without a password.

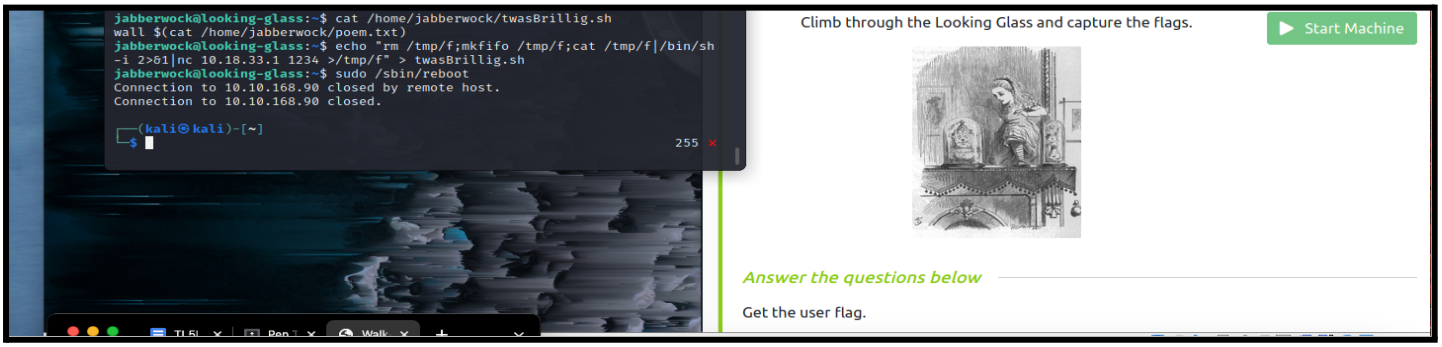


I used the PentestMonkeys cheatsheets and replaced the contents of twasBrilling.sh .



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





Thought Process and Methodology and Attempts:

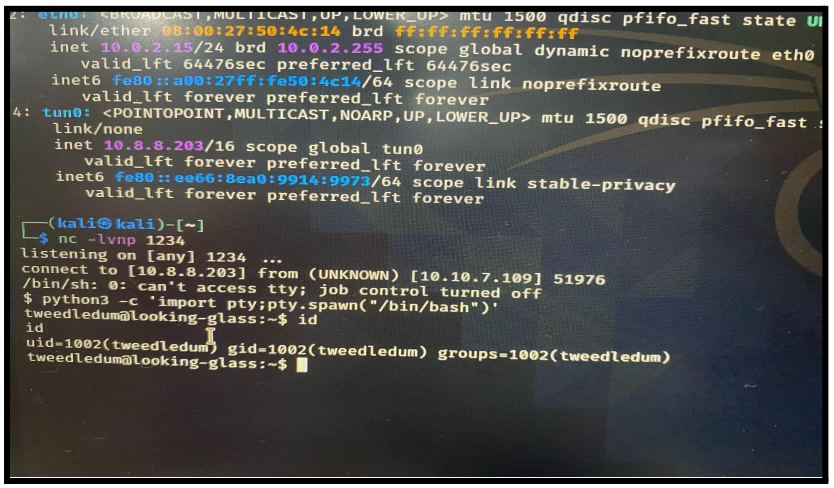
Now we need to figure out how to get to root. A quick look at the passwd file reveals that there are several users. We can also look into crontab. This could assist us in determining what is running when the box boots that causes the random port to respond.The bottom line indicates that when the server 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

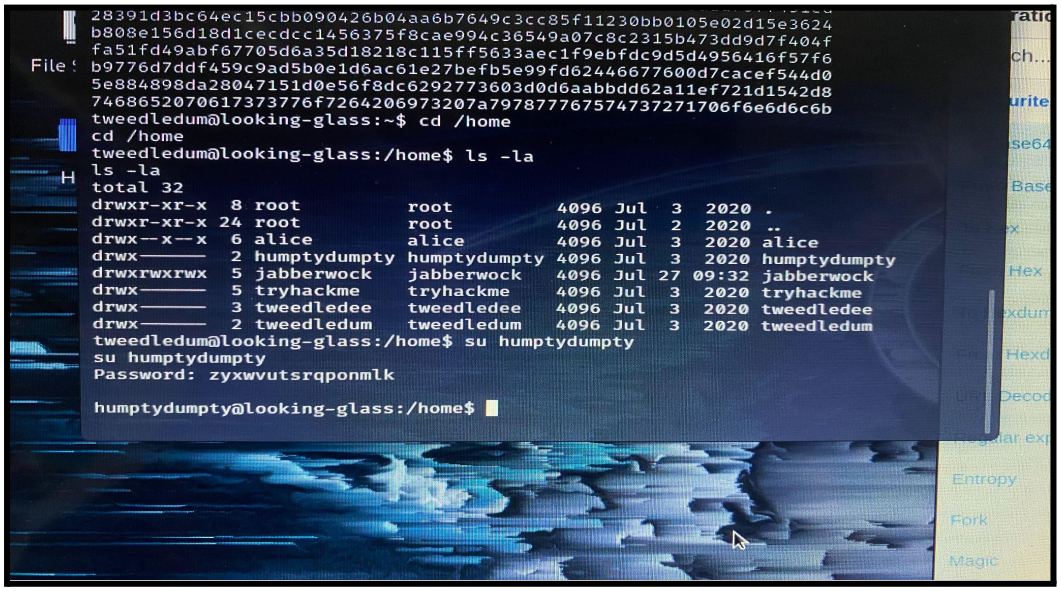
5. Second user

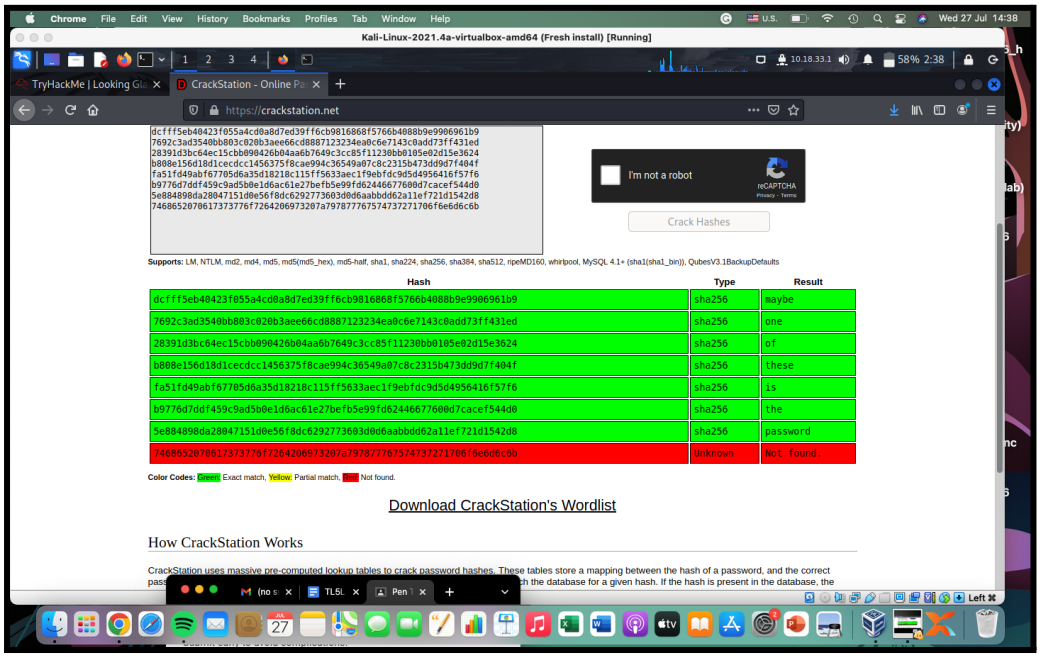
Members involved: Sarvesh A/L Munusamy
Tools used : Kali Linux, Terminal , Crackstation

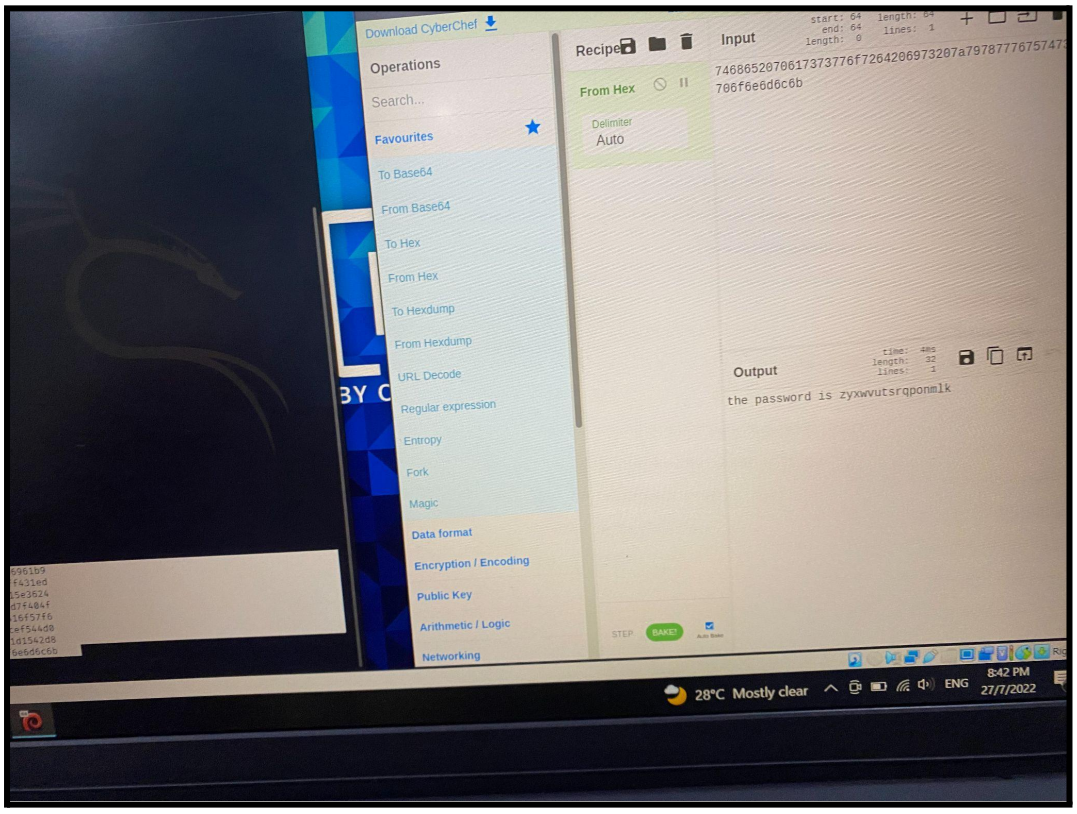
We are currently logged in as user tweedledum. Before we proceed, let's update to a decent shell.



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.




Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running]
https://crackstation.net
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb890426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d0a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f726420697320 7a79787776757473727 1706f6e6d6c6b
I'm not a robot
reCAPTCHA
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults
Hash
Type
Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
sha256
maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
sha256
one
28391d3bc64ec15cbb890426b04aa6b7649c3cc85f11230bb0105e02d15e3624
sha256
of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
sha256
these
fa51fd49abf67705d0a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
sha256
is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
sha256
the
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
sha256
password
7468652070617373776f726420697320 7a79787776757473727 1706f6e6d6c6b
Unknown
Not found.
Color Codes: Green Exact match, Yellow Partial match, Red Not found.
Download CrackStation's Wordlist
How CrackStation Works


Download CyberChef
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Recipe
From Hex
Delimiter
Auto
Input
7468652070617373776f726420697320 7a79787776757473
706f6e6d6c6b
Output
the password is zyxwvutsrqponmlk
28°C Mostly clear
ENG
8:42 PM
27/7/2022

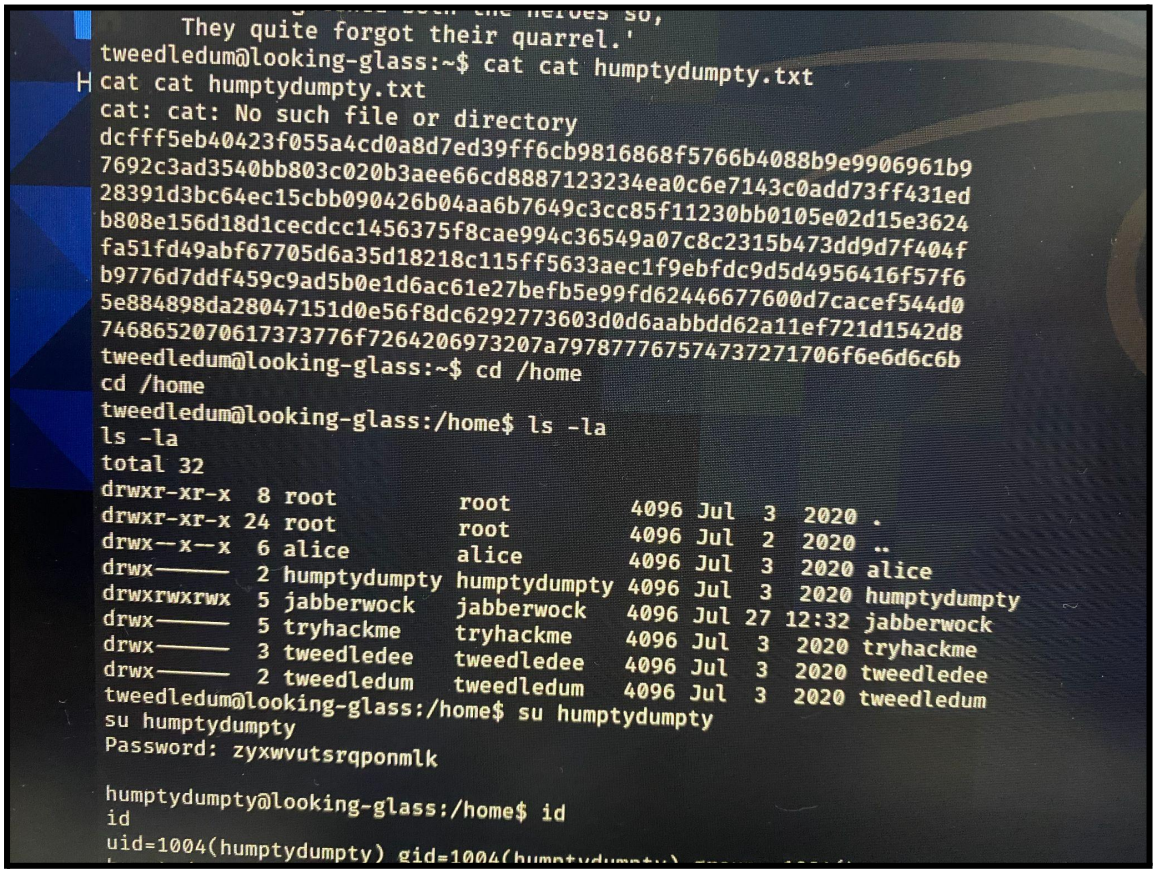
Steps: Third user

6. Third user

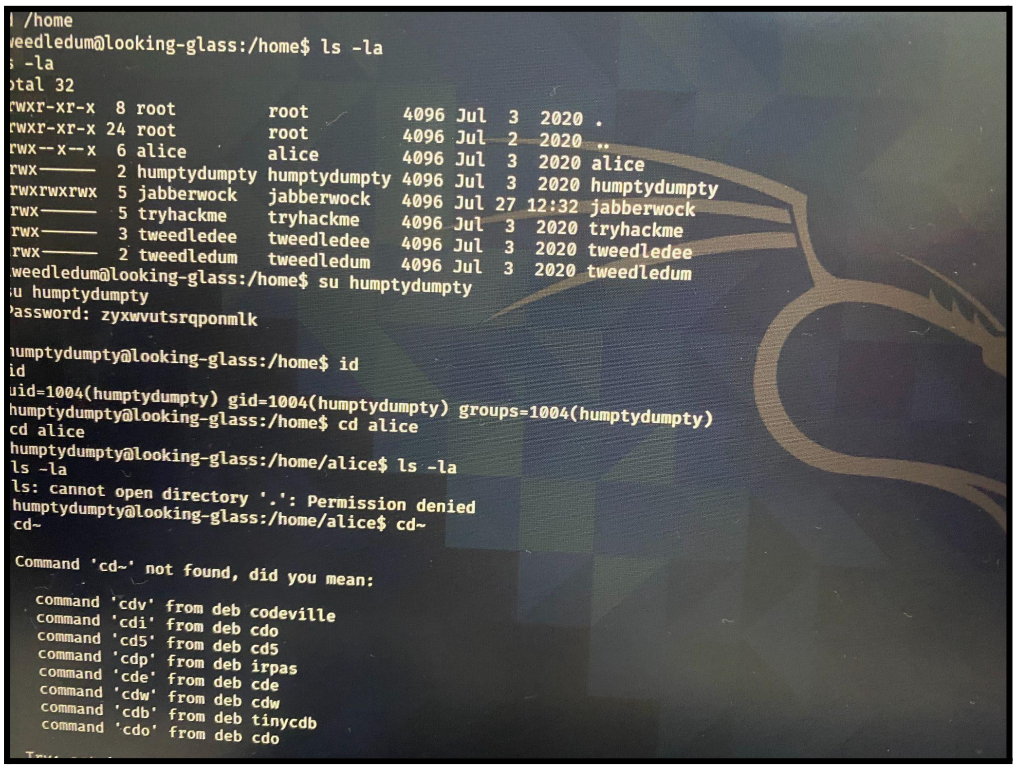
Members involved: Sarvesh A/L Munusamy

Tools used : Kali Linux, Terminal

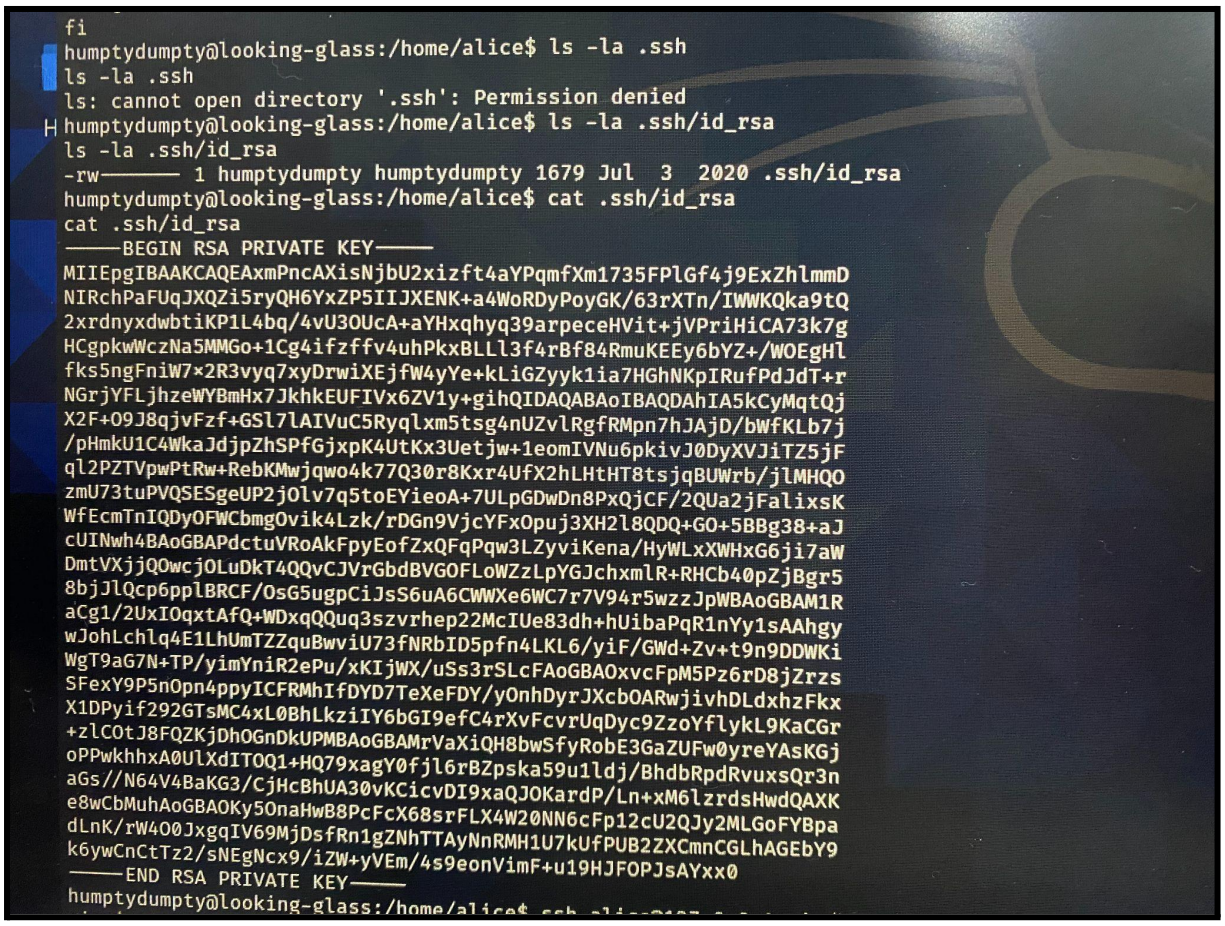
Therefore, we have another password that had been obtained from the humptydumpty.txt file. And since we already know that there is a user named humptydumpty because we already examined the passwd file, let's try switching to them.



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.



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.



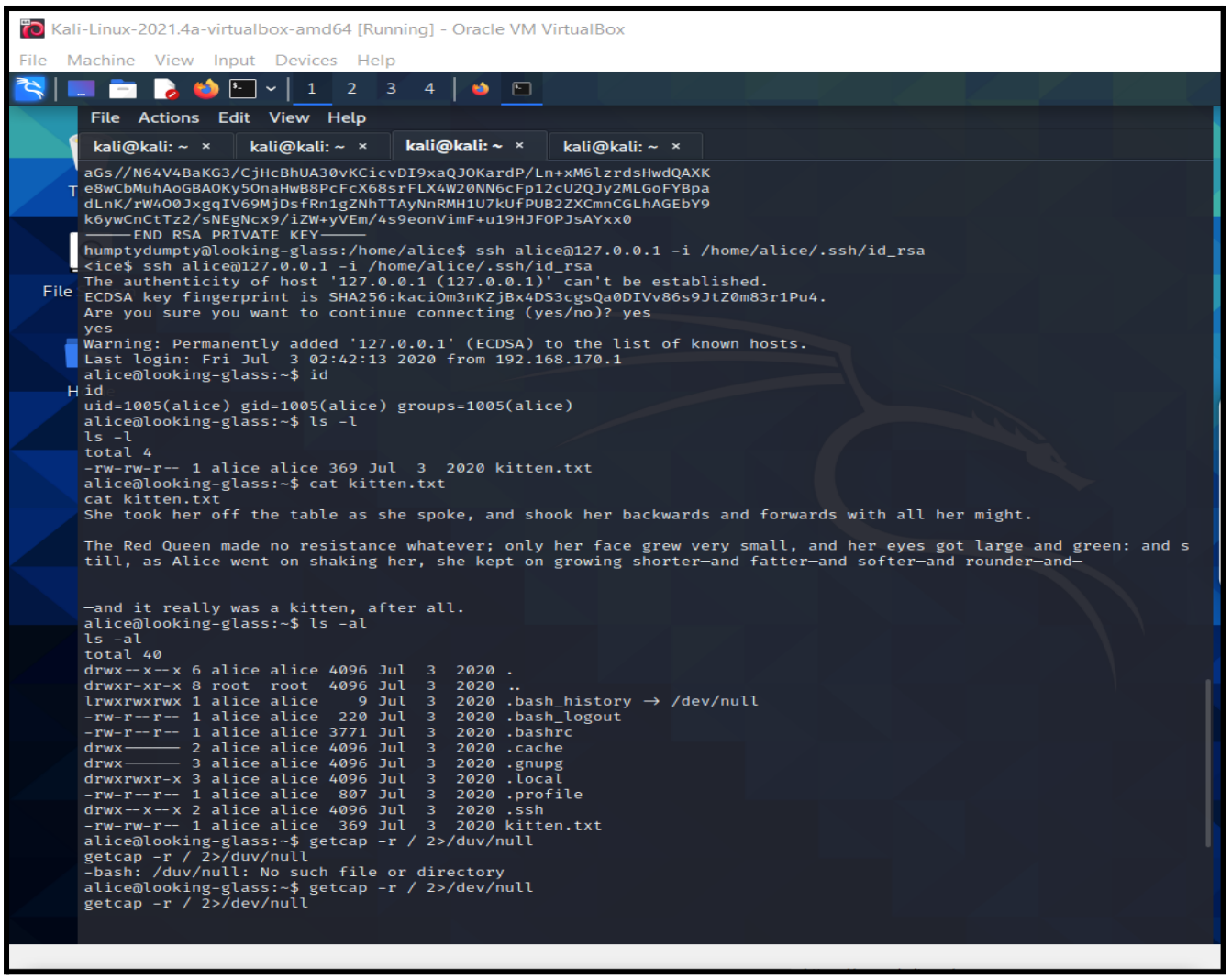
Steps:Fourth user

7. Fourth user and root flag

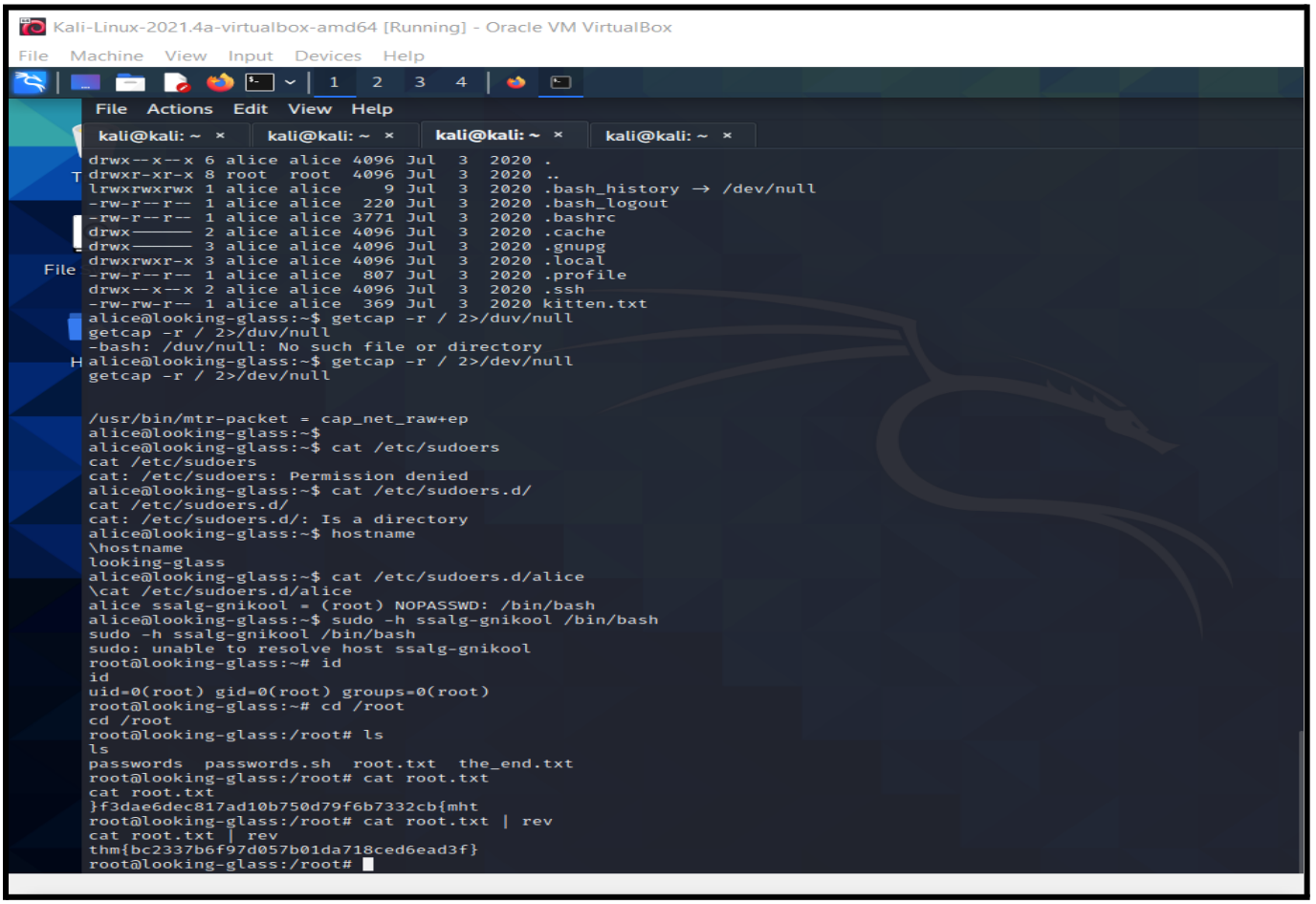
Member involved: Nicholas Cheok Jia Jie

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”.



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.



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.	R.hemma
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.	A.tivaa
1211102168	Nicholas Cheok Jia Jie	In charged of fourth user process and root flag. Involved in the write up.	Nich
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.	M.vesh

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