PenTest 1

ROOM A

GeForce

Members

| **ID** | **Name** | **Role** |
| --- | --- | --- |
| 1211101248 | Ang Khai Pin | Leader |
| 1211101260 | Samson Yoong Wen Kuang | Member |
| 1211102775 | Rehnugha A/P Marali | Member |
| 1211102087 | Sharleen Ravi Mahendra | Member |

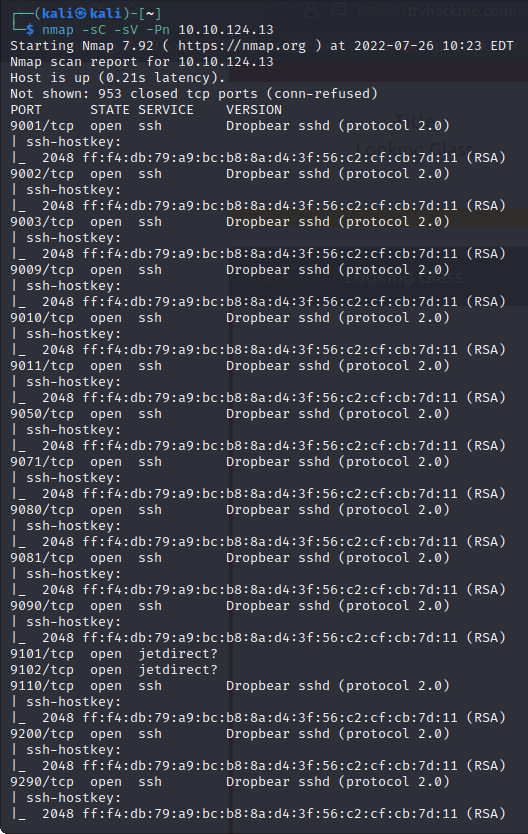
**Steps 1: Recon and Enumeration**

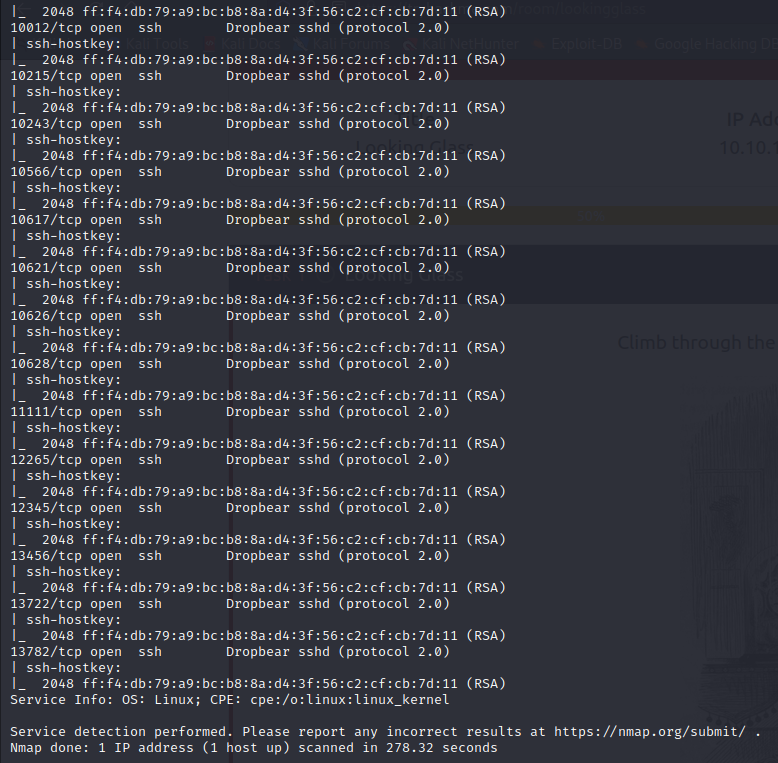
**Members Involved**: Sharleen

**Tools used**: **Nmap, Kali Linux, SSH**

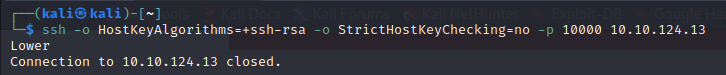
**Thought Process and Methodology and Attempts:**

Firstly, Sharleen started by using the Nmap command to check for open ports. She found that ports between 9001 and 13782 were open.

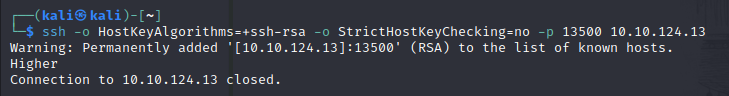




Sharleen then tried to connect to port 10000, one of the lower ports between the range. However, the message **Lower** was returned to her and she was disconnected from it.

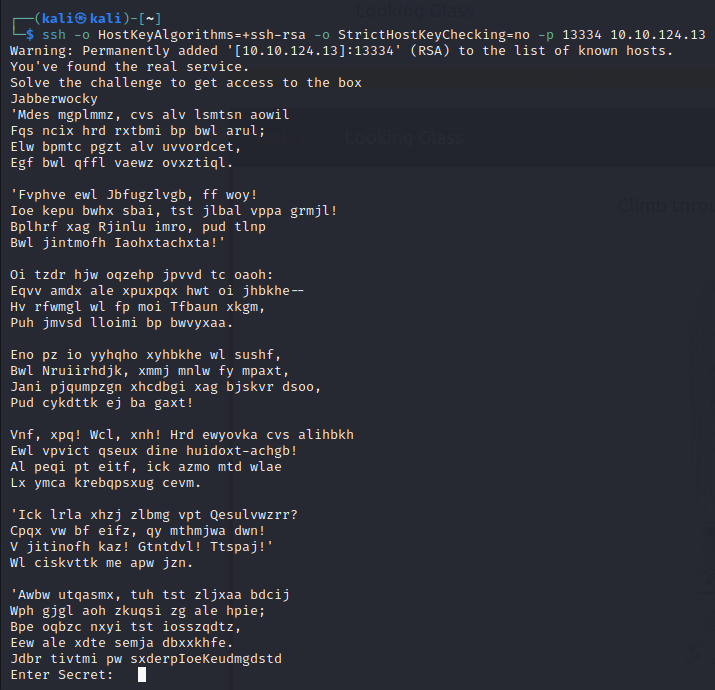


Then, Sharleen tried to connect to port 13500, one of the higher ports between the range.



This time, the message **Higher** was returned to her and she was disconnected from it. Hence, with the help of these clues, it is known to Sharleen that the correct port is between these two ports.

Sharleen kept trying until she was able to find the correct port. After Sharleen found the port and successfully connected to it, the following message was displayed:

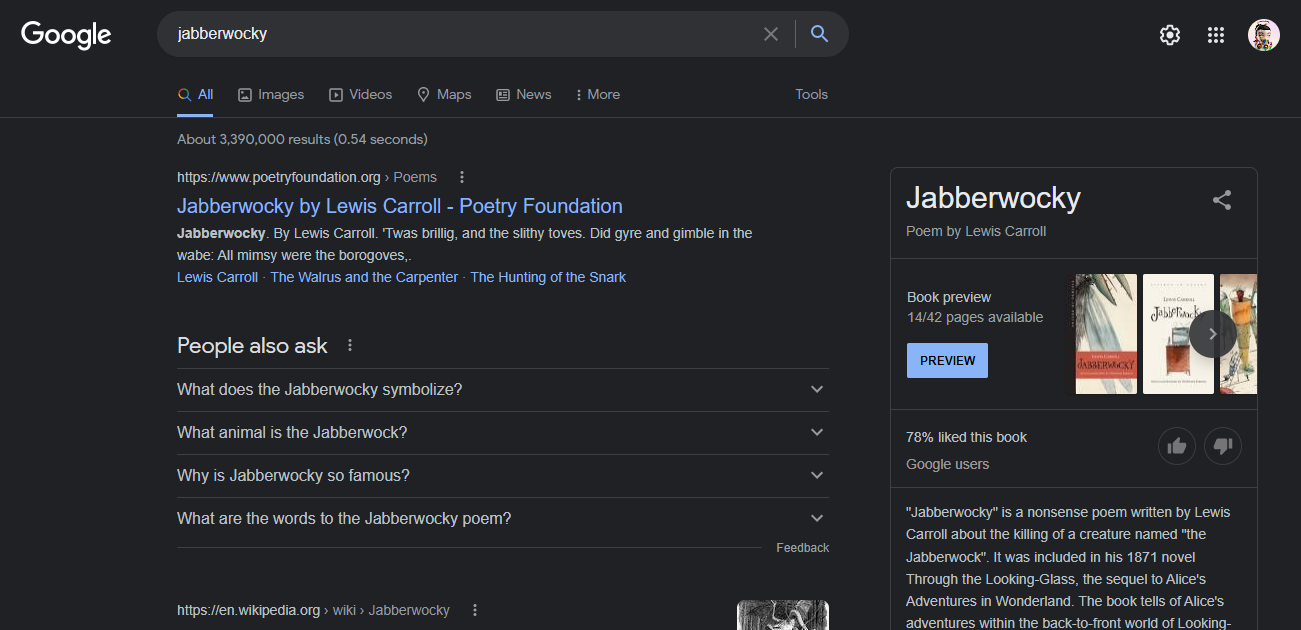


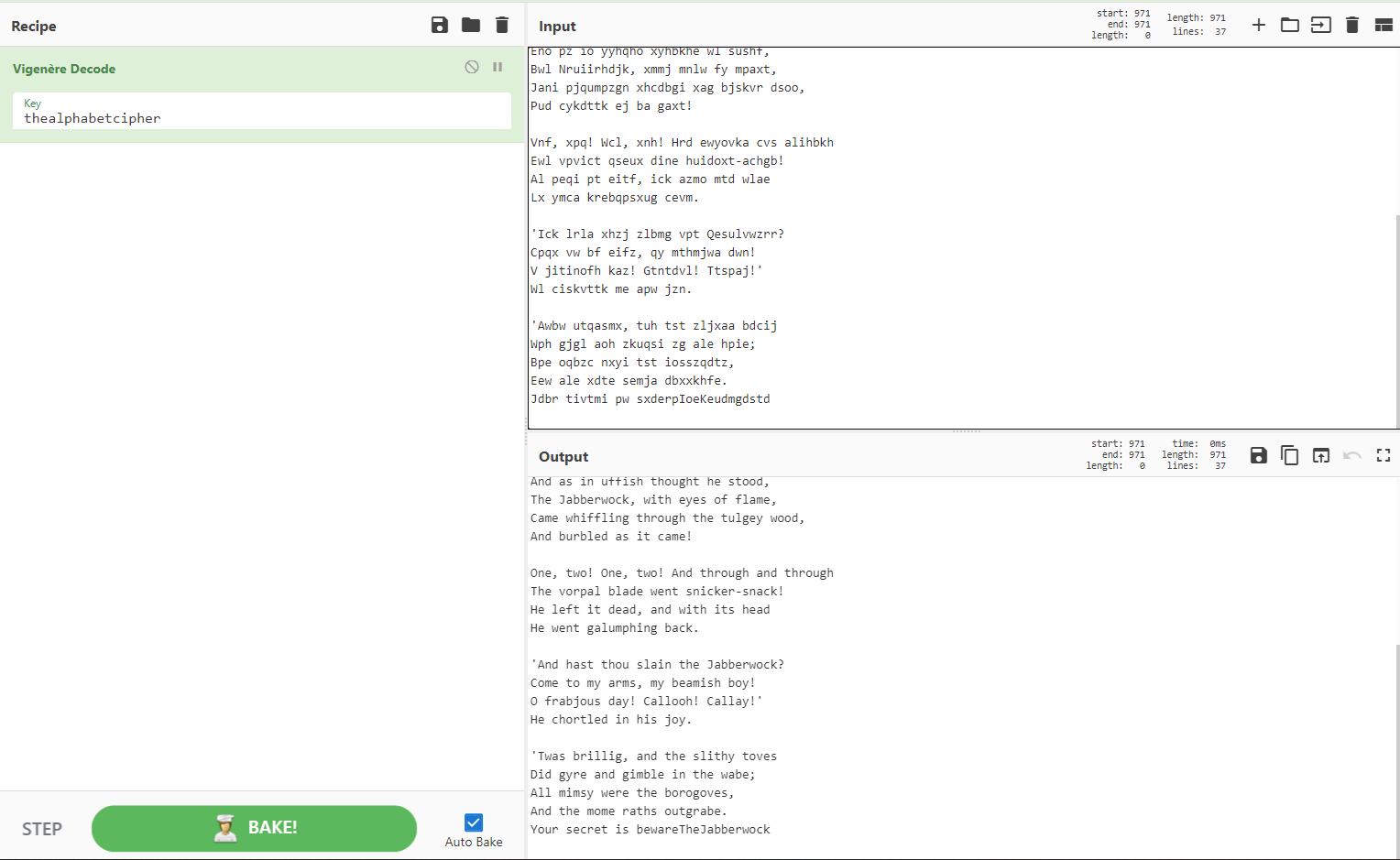
**Steps 2: Initial Foothold**

**Members Involved:** Samson Yoong

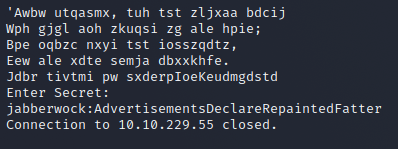
**Tool Used:** Kali Linux, CyberChef

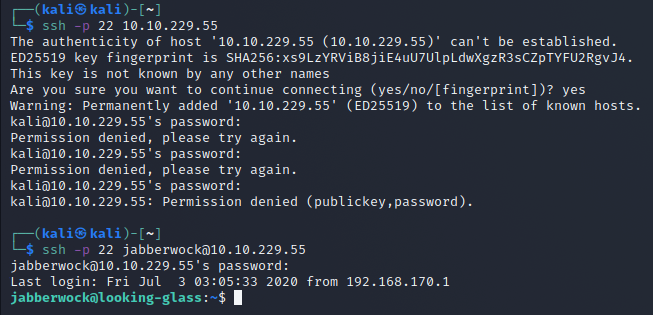
**Thought Process and Methodology and Attempts:**

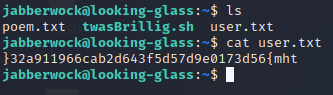
After Sharleen found the port, the port appears to have text contained in it. Samson proceeded with searching for information about the text. At the top there is a word “jabberwocky”, so Samson went ahead to search it on google. He found that the line of text is actually a poem.

But the poem in the terminal seems to be not readable. Samson went on to search about the text. He found out that the text seems to be a Vigenere encrypted text, so He went on to decode it. He went to Cyberchef and decoded the encrypted text and got the secret which is “bewareTheJabberwock”

Now Samson continued on to entering the secret, He got the password for the jabberwock account.

****

After retrieving the password, Samson moved on to logging in to the account. In the terminal he used the ssh command to gain access to the account. In the first attempt, Samson wrote the command wrongly so he couldn’t log in but after that he managed to get it right. After that, it will ask for password so he keyed in the password that he got and successfully logged into the account.

After logging into the account, Samson looked into the account to find information. He found out that there are 2 text files and a .sh file inside. He looked into the user.txt file and found the flag was in there! But the order for the flag seems to be messed up. So, Samson went ahead and corrected it and was able to retrieve the flag.



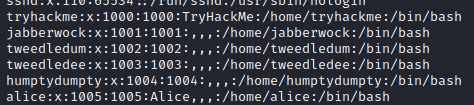
**Steps 3: Horizontal Privilege Escalation**

**Members Involved**: Rehnugha

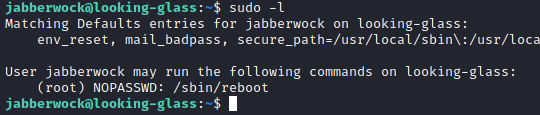
**Tools used**: **Nmap, Kali Linux, hashes.com**

**Thought Process and Methodology and Attempts:**

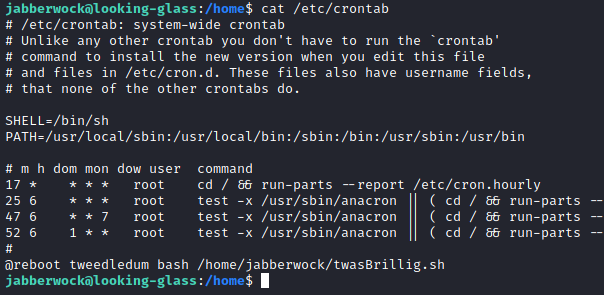
After Samson finds the flag, it's time for Rehnugha to find the privilege escalation. Rehnugha looked at the “/etc/passwd” file and there were a lot of users to escalate the privileges to.



Jabberwock is allowed to run /sbin/reboot as root. Rehnugha found this with the sudo -l command on the terminal.

****

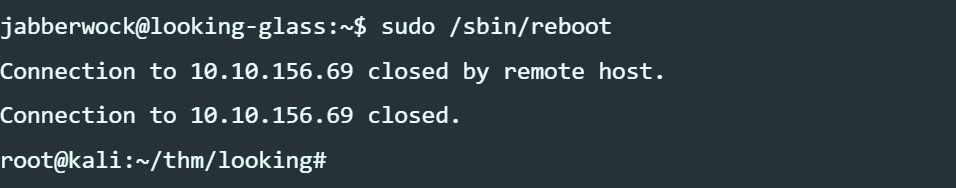
There was nothing on GTFOBins and simply executing it with sudo rights won’t do anything. So something has to be done with it. When Rehnugha looked at “/etc/crontab” Rehnugha found the “twasBrillig.sh” file in there.

****

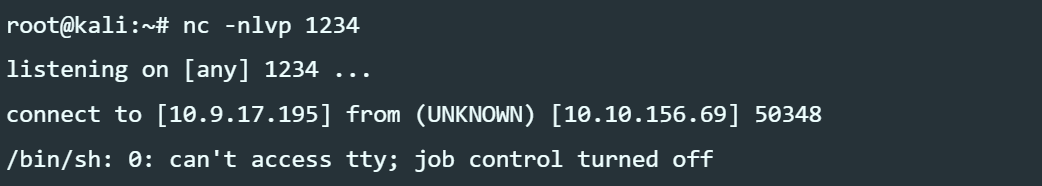
We can create a simple listener with netcat and get our connection to it.

The twasBrillig.sh can be exploited by using ‘echo’ to get the connection to the next user, which is ‘tweedledum’.

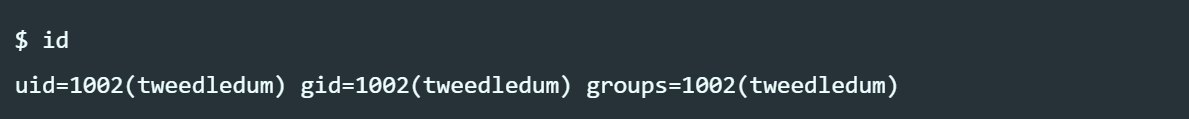
 Rehnugha just executes the command for it and reboot the looking glass machine with the command: sudo reboot.

****

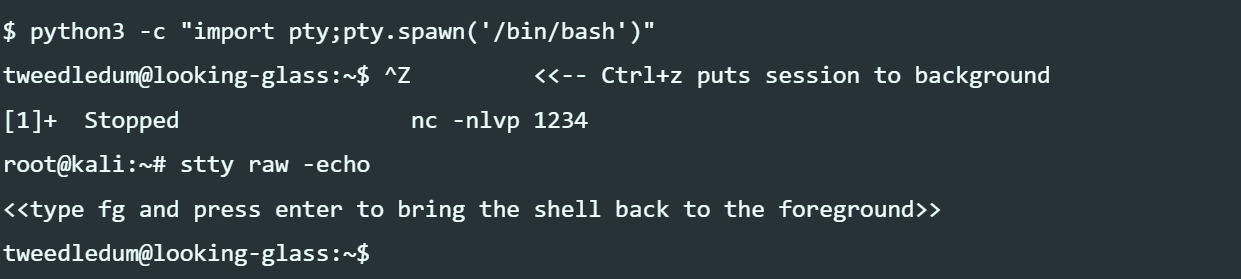
After a short while Rehnugha sees the box connecting.

****

After a while, Rehnugha got a reverse shell as the user “tweedledum”!

****

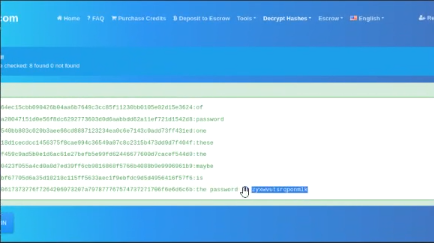
So now we are connected as user "tweedledum". Rehnugha upgraded to a proper shell before we do anything else.

****

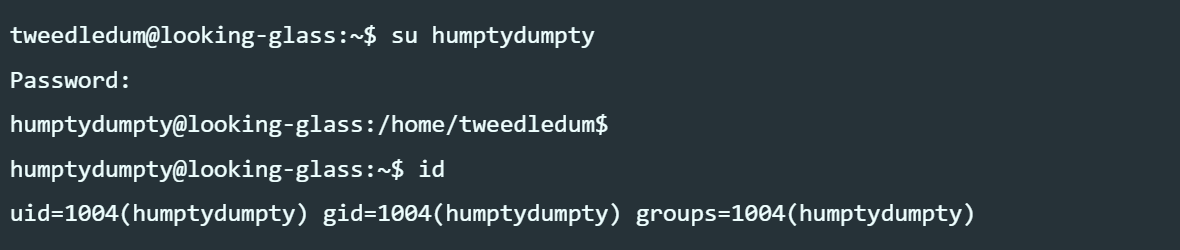
In the home directory of "tweedledum", I read the “humptydumpty.txt” file and saw some strings.

****

Rehnugha has two files, a poem and what looks to be something else that’s encrypted. These looked more like hashes than ciphers, so Rehnugha tried an online hash cracker. Rehnugha detects same as SHA256PLAIN hashes, and they decode to reveal a sentence. The last one is not a SHA256 hash, but instead it is hex encoded. Luckily, the website auto detected it and decoded that one along with the others.

****

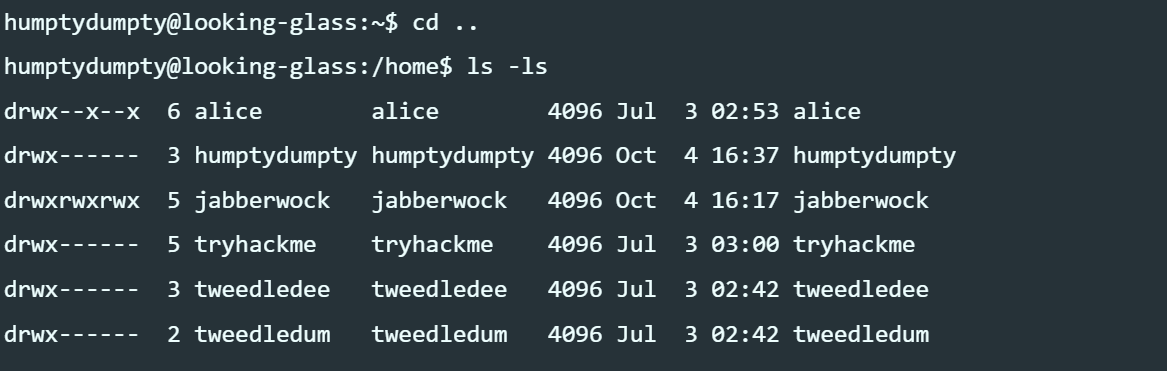
So we now have another password, from a file called humptydumpty.txt. And we know from earlier when we looked at the passwd file that there is a user called humptydumpty, so Rehnugha tried switching to them.



Now Rehnugha looked for the context in the folder.

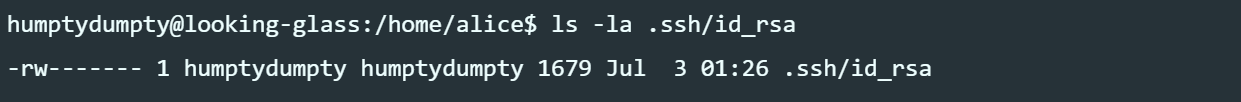


We came across this home page where we got some information.

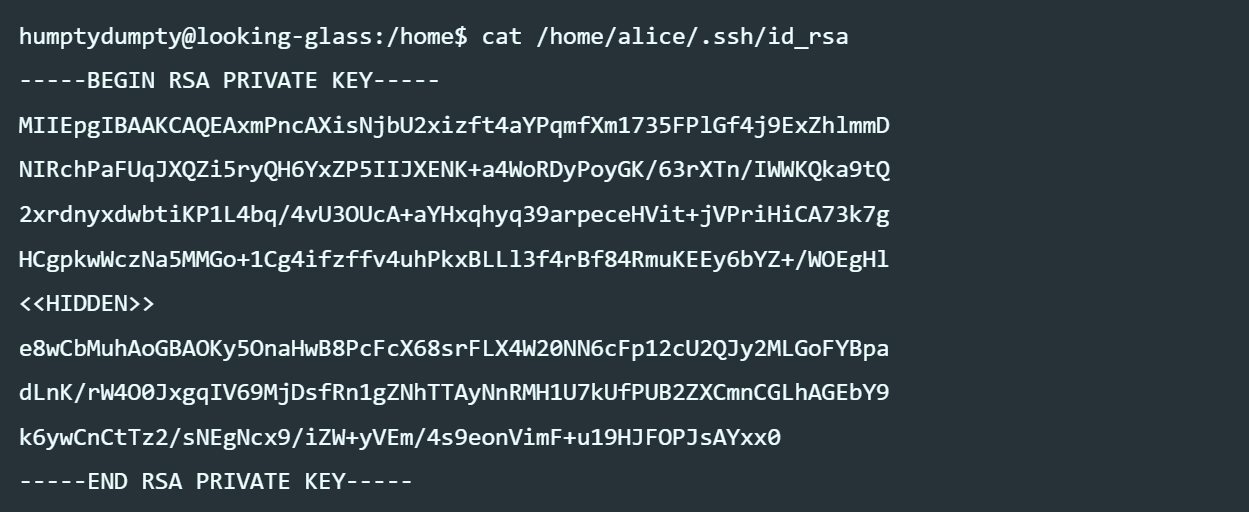
****

So we have permissions to read the .bashrc file in the alice home folder, even though we haven’t got permissions to view the contents of that folder.

Now Rehnugha checked to see if we can find something else obvious like an rsa key.



Rehnugha gets to see there is an id\_rsa file in the expected .ssh folder, but also notices it is owned by the currently logged on user humptydumpty. So Rehnugha can read the contents in the folder.



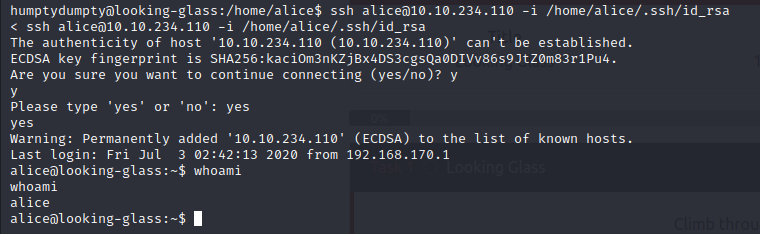
**Steps 4: Root Privilege Escalation**

**Members Involved**: Ang

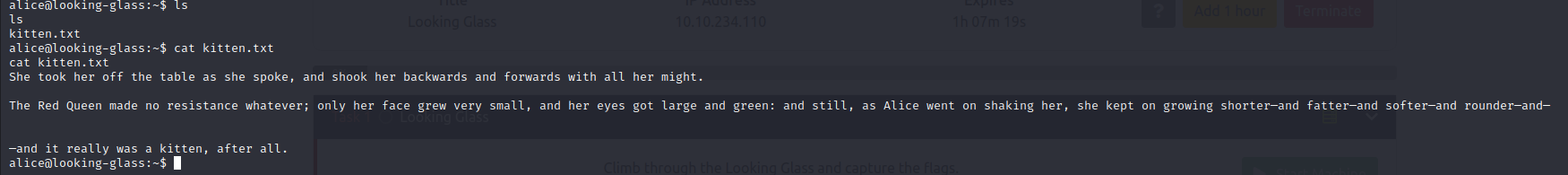
**Tools used**: **Nmap, SSH, nano, Kali Linux**

**Thought Process and Methodology and Attempts:**

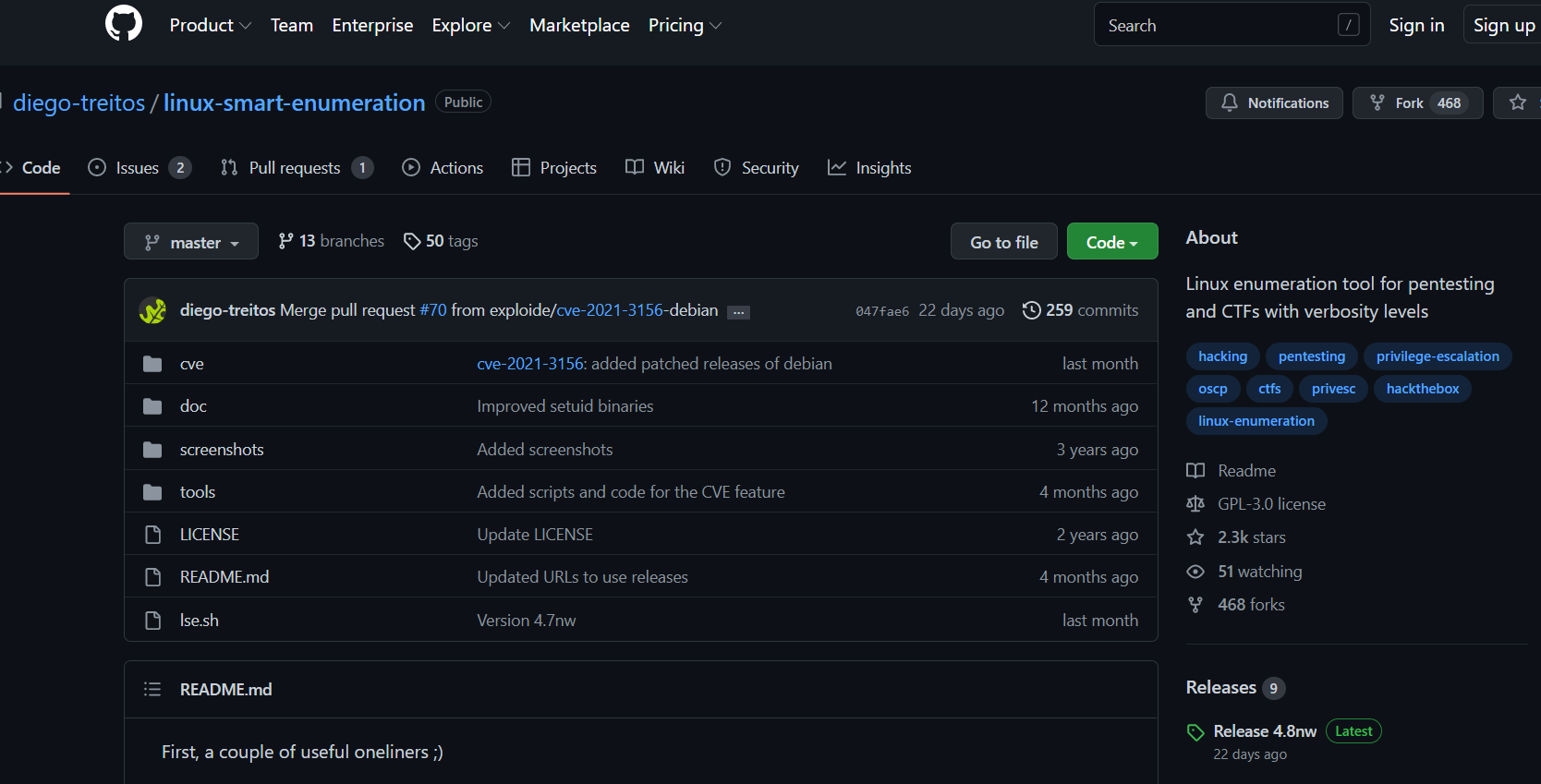
From previous steps, Rehnugha found the rsa private key for the user ‘alice’. Ang then SSH to ‘alice’ using the key:



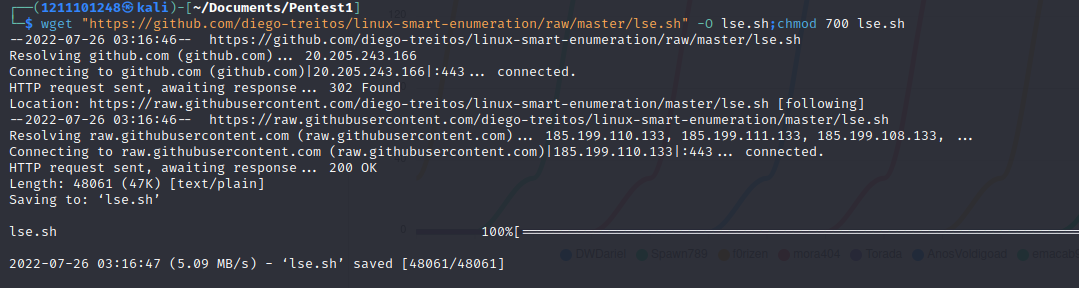
Ang look around file, with the command ‘ls’, he found kitten.txt, however, the file doesn’t seems to contains any useful information.



In order to look more into the files, Ang went to github to search for an enumeration script. After some digging, he fnd linux-smart-enumeration.



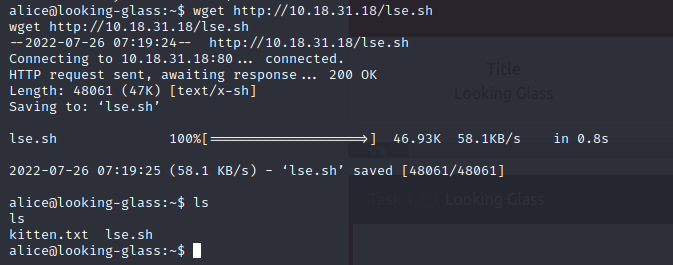
Switching back to Kali box, Ang use ‘wget’ to download the files from github.



Ang then use python to set up a server to later on insert the ‘lse.sh’ into ‘alice’ box.



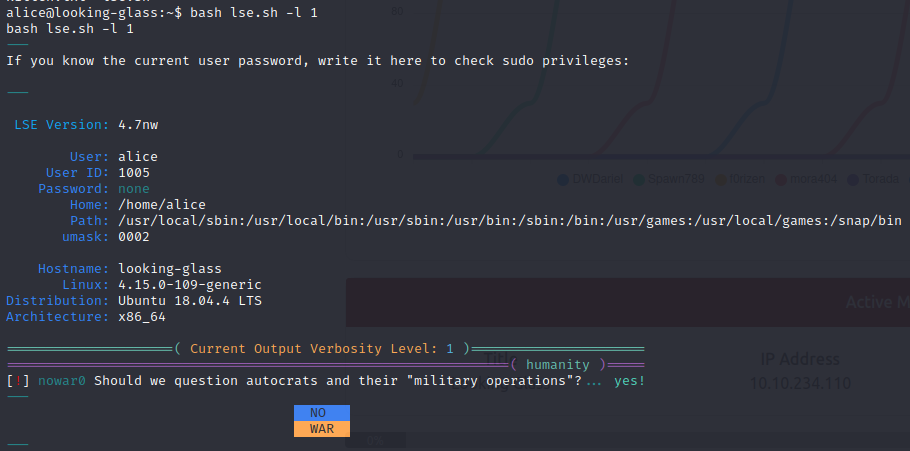
With the script downloaded and staged, Ang switch back to ‘alice’ box and grab the script.



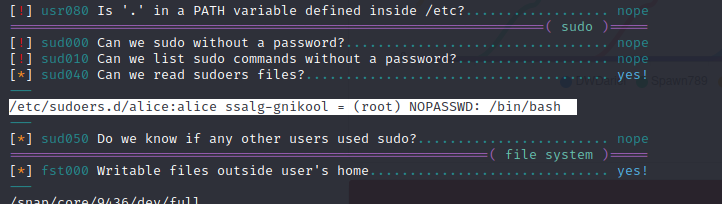
This is the proof that the script has been successfully grabbed:



After grabbing the script, Ang run it with the command ‘bash lse.sh -l 1’.



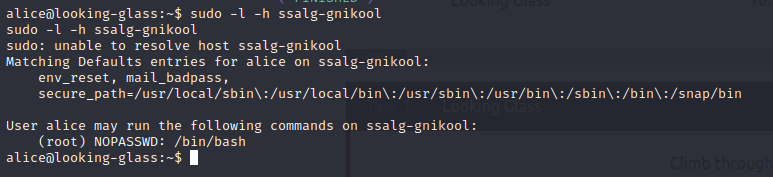
After some time, the scripts found many information. By scrolling over the information gathered, Ang spotted the obvious path to root.



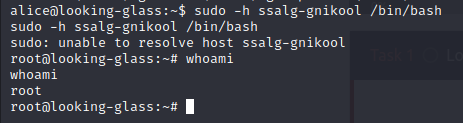
The path shows us several information:

1. User: alice
2. Hostname: ssalg-gnikool
3. Permissions: (root) NOPASSWD
4. Directory: /etc/sudoers.d
5. Command to be executed: /bin/bash

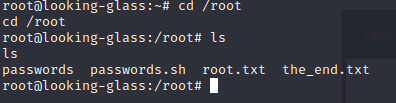
With the information broken down, Ang can start to exploit it using sudo. He can easily do so by adding ‘-h’ command to indicates the host.



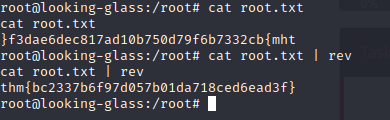
With this, Ang can confirm that he is on the right path. So, he can now escalate to root.



After gaining access to the ‘root’ user, Ang navigate to ‘/root’ and list all the files within.



Now Ang can see the ‘root.txt’, he read it and found out that it was reversed. A simple ‘cat root.txt| rev’ command solved the problem. And with that, the flag was retrieved and the challenge for this room is completed.



**Contributions:**

| **ID** | **Name** | Contribution | Signatures |
| --- | --- | --- | --- |
| 1211101248 | Ang Khai Pin | Did the Root Privilege Escalation report part. Took part in video presenting by explaining the Root Privilege part. Presented his screen during the video presentation, and did the THM room. |  |
| 1211101260 | Samson Yoong Wen Kuang | Did the Initial Foothold part report part. Took part in video presenting by explaining the Initial Foothold part. Recorded the video presentation and did the editing part. |  |
| 1211102775 | Rehnugha A/P Marali | Did the Horizontal Privilege Escalation report part. Took part in video presenting by explaining the Horizontal Privilege part. |  |
| 1211102087 | Sharleen Ravi Mahendra | Did the Recon and Enumeration report part. Took part in video presenting by explaining the Recon and Enumeration part. |  |

**VIDEO LINK:** https://youtu.be/sGCVYF6imag