PenTest 1
Looking Glass
GROUPNAME : GGez

Members

Student ID	Name	Role
1211101951	Muhd Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhd Arief Fahmi BIn Syahril Anuar	Members
1211101643	Sivaharriharann A/L Ramanathan	Members
1211101120	Adam Uzair Bin Mohd Sori	Members

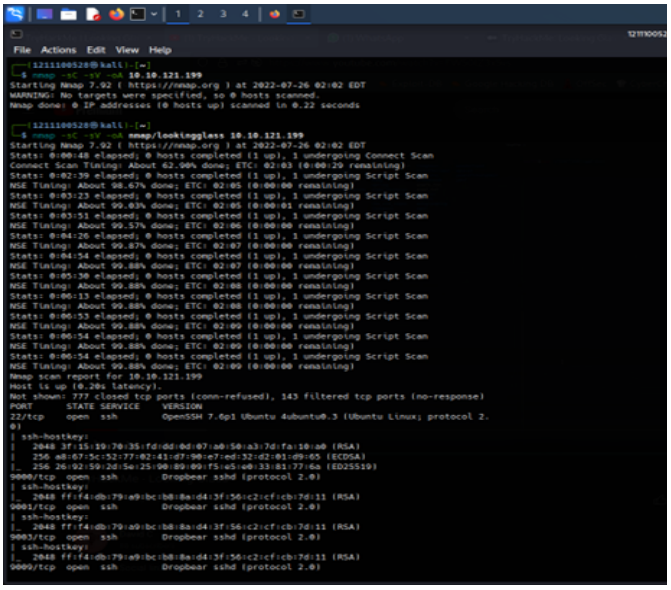
1) **Recon and Enumeration (Where you gather data) Flag 1**
2) **Initial Foothold (where you gain the first reverse shell) Flag 2 up to before starting root user**
3) **Horizontal Privilege Escalation (If any, if you pivot to other users) Flag 2 root user stuff**
4) **Root Privilege Escalation (final step, rooting) Flag 2 root user stuff part 2**

Recon and Enumeration

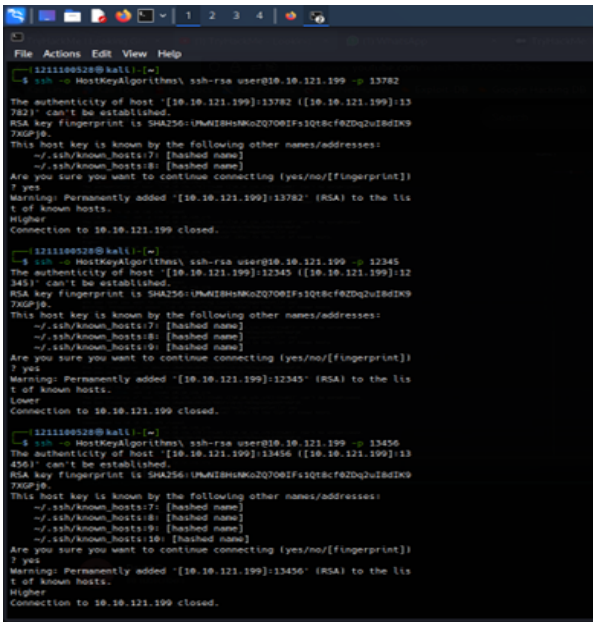
Members Involved: Arief
Tools used: kali linux , terminal , nmap , ssh

Thought Process & Methodology::

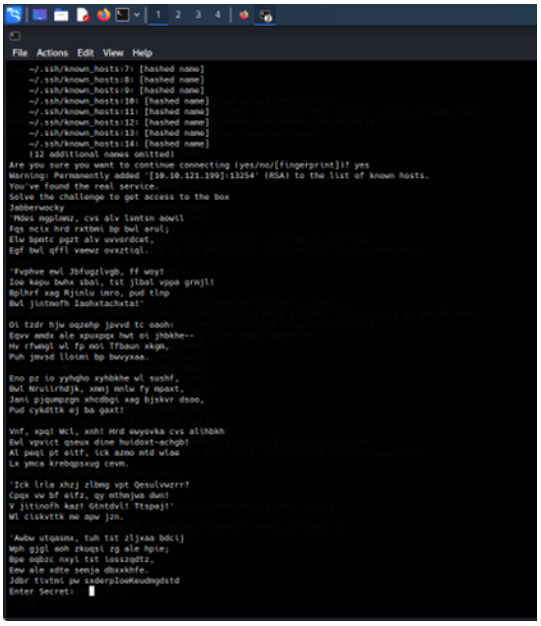
So first of all Arief has to get the IP address from the tryhackme looking glass task.



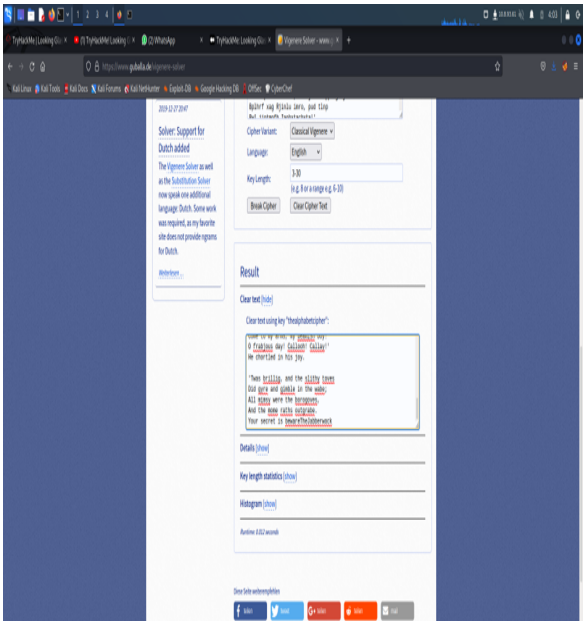
After Arief has got the IP address he starts the scanning of the IP address by using NMAP to see what ports are open . Then Arief found out that the ports that are open are from port 9000 to 13456 .



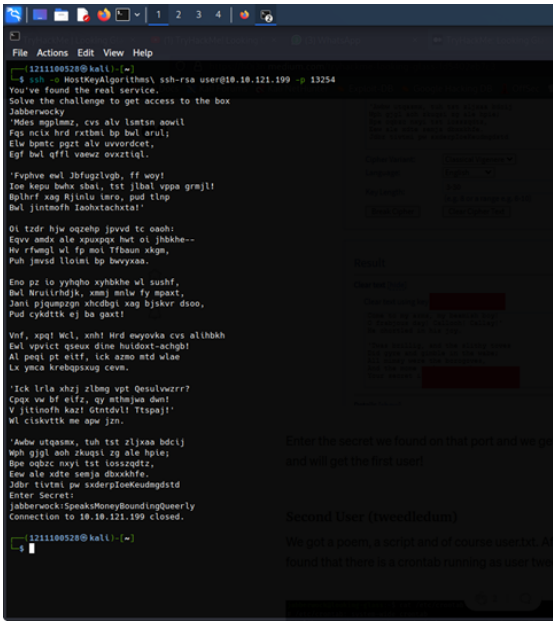
After that Arief started to use the ssh method to find the right port to proceed to the next step . Arief does it by scanning each port and getting the input whether the ports are lower than the scanned port or higher .



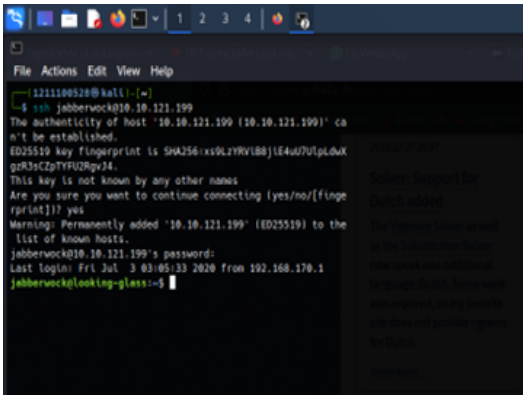
After a while , Arief found the right port and it showed a message that we need to encrypt/decode and there is a secret message that we need to find.



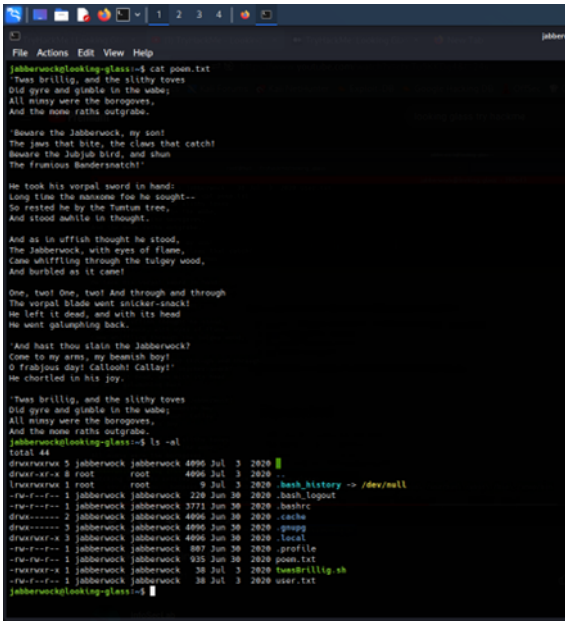
Later Arief used a website for the vigenere from a website called guballa.de and found out the user name .



Then Arief put the secret ID that he found to get the password to the new user .



Then Arief used the user Jabberwock and input the password that he got from the previous image.

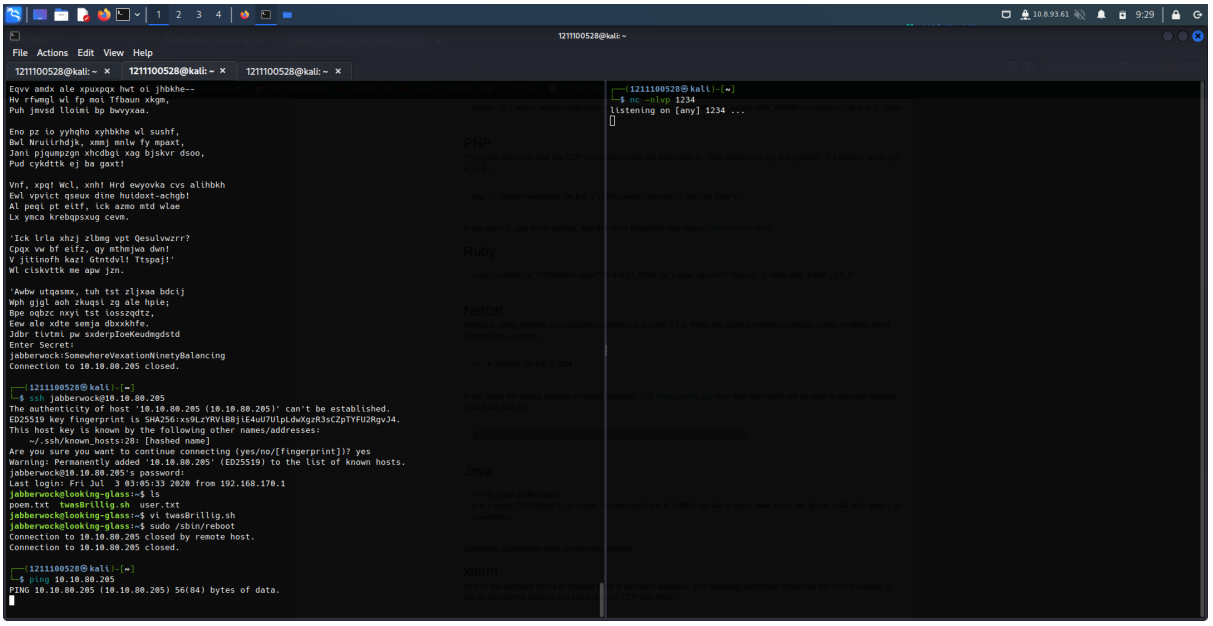


Then after Arief got access to the user Jabberwock he got information which is user.txt and poem.txt . Arief got the first flag on the user.txt .

Initial Foothold

Members Involved: Zaieff Danial
Tools used: kali linux , terminal

Thought Process & Methodology::

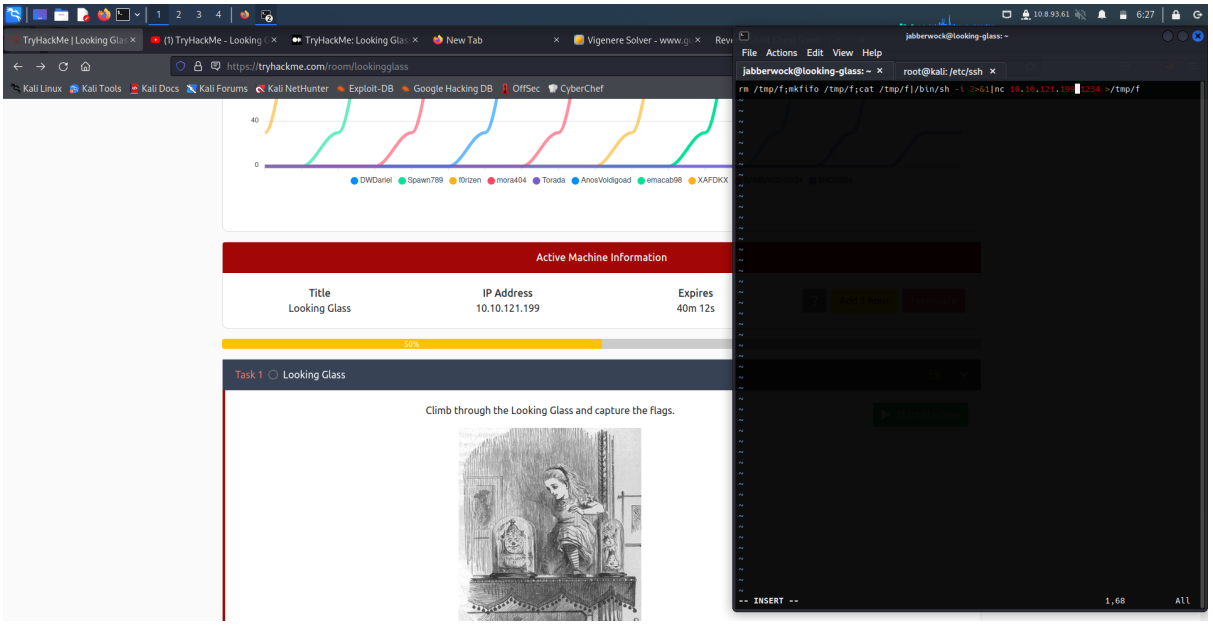


Closed the connection in the riddle after we get the first flag. Then set up ssh jabberwock@IP_MACHINE. Insert directory list until bin reboot command to remote host. Therefore ping our IP_MACHINE and command netcat listener to gain our reverse shell for our root command.

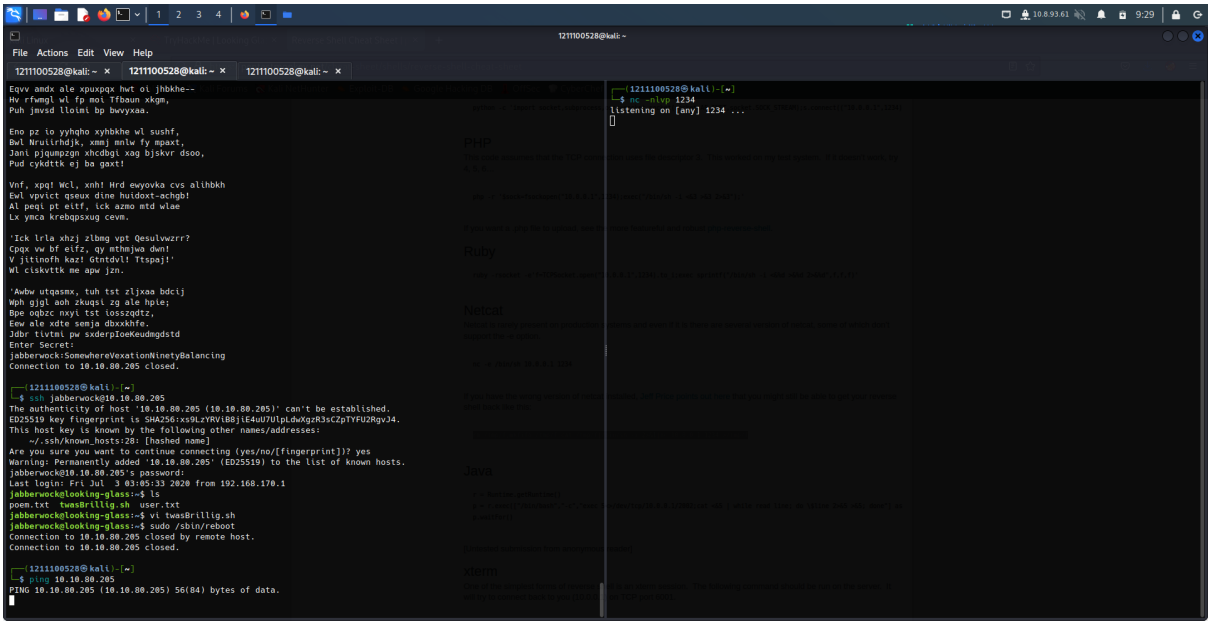
Horizontal Privilege Escalation

Members Involved: Siva
Tools used: kali linux , terminal , root , cyberchef

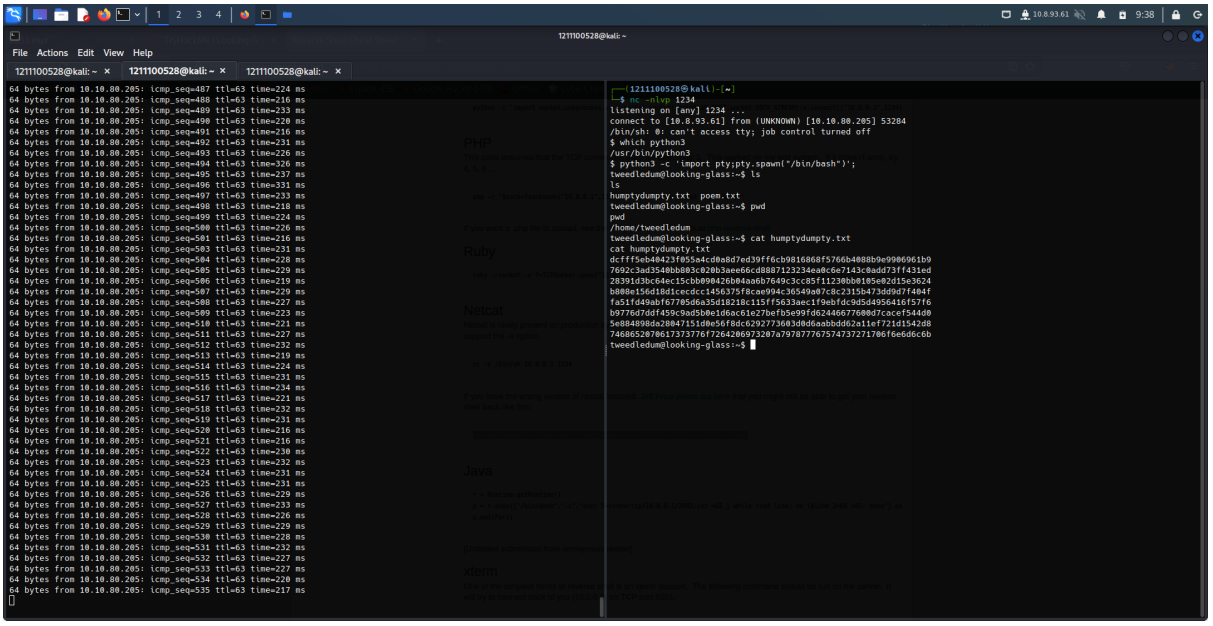
Thought Process & Methodology::



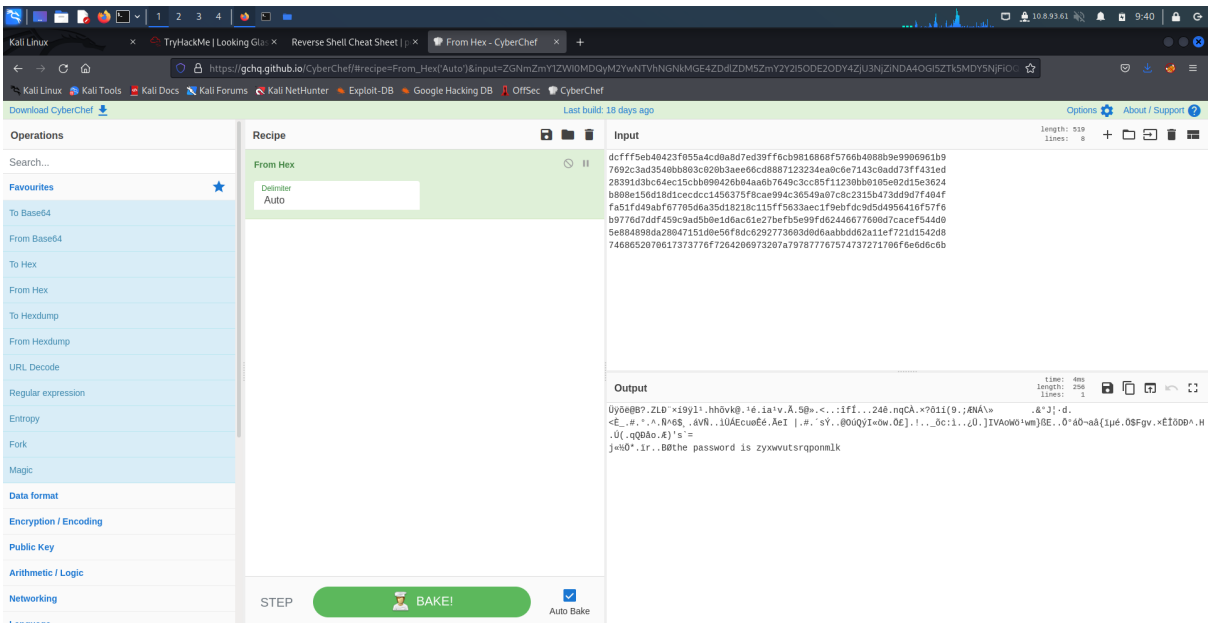
So the attack vector is to overwrite the twasBrillig.sh file with a reverse shell, set up a listener on our attack machine and then reboot the remote machine. I elevated user Tweedledum.



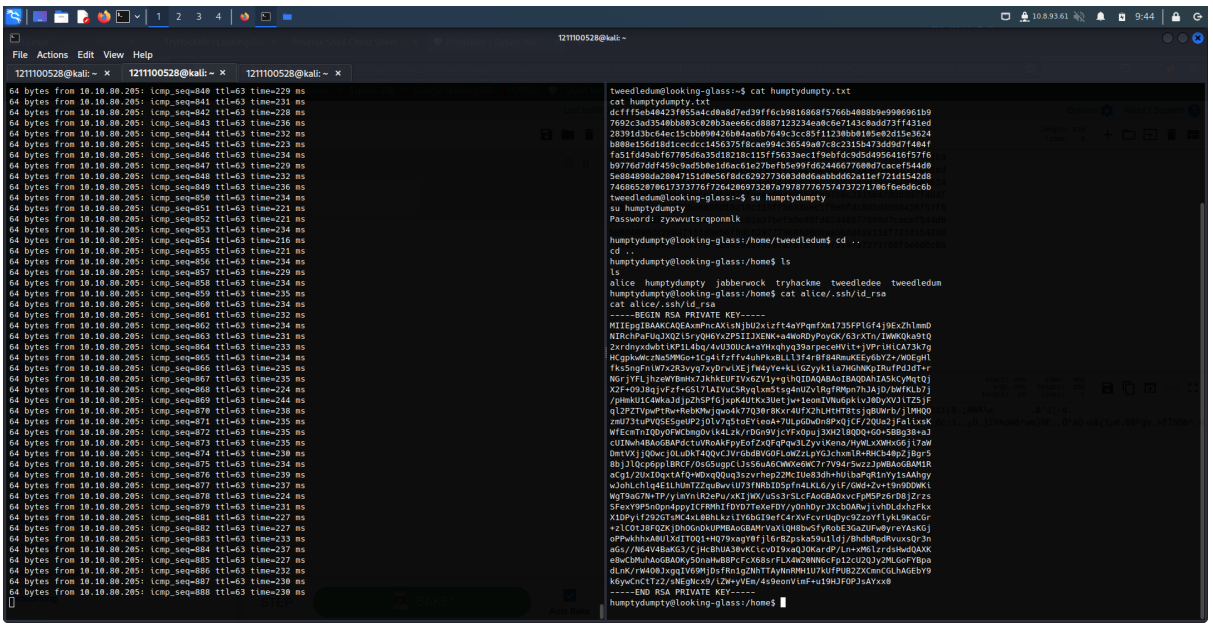
The next step is to set up a Netcat listener, which will catch the reverse shell when it is executed by the victim host, using the following flags: lvnp.



we execute /sbin/reboot to restart the system, a callback on the Netcat listener is received, granting a shell as the tweedledum user.We enuemrates common files and directories, found a file containing what looks like a number of hashes.



Using the Cyberchef online cracking tool, it was able to crack all of these apart from one, which according to the others seems to be the password and the last one does not seem to be a hash, when decoding it from HEX it reveals a password.

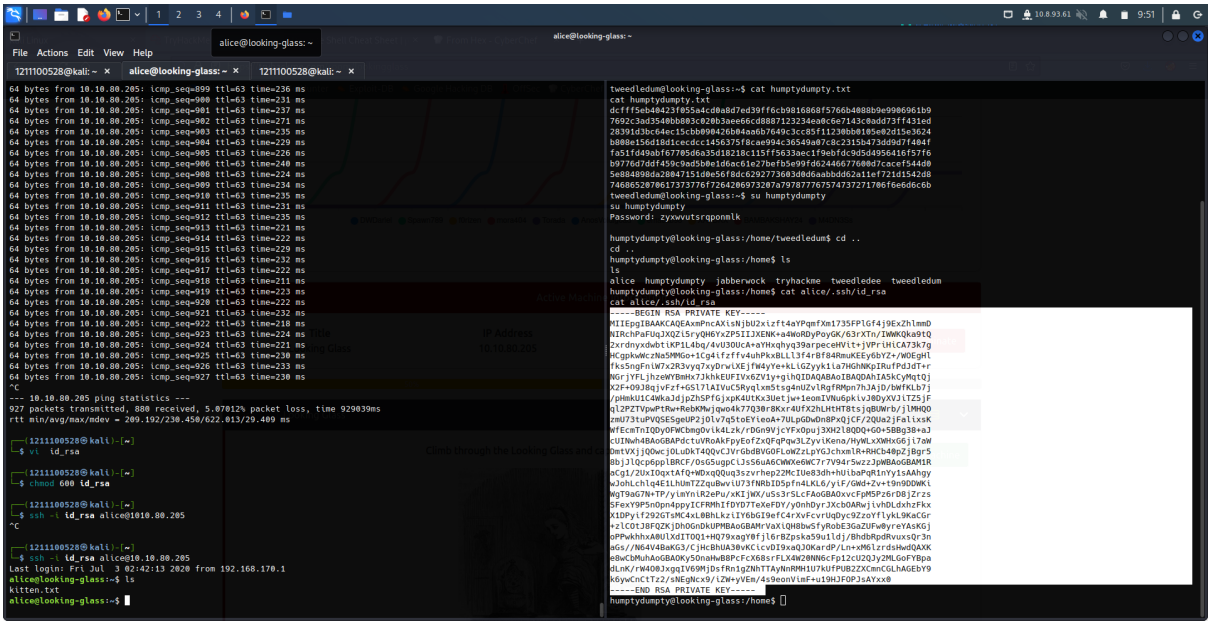


We will get the password for the humtydumpty user.

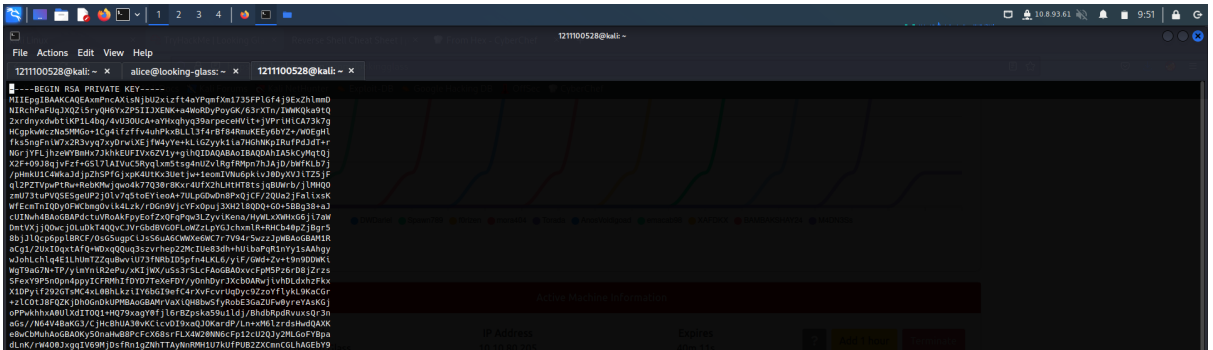
Root Privilege Escalation

Members Involved: Adam Uzair
Tools used: kali linux , terminal , root

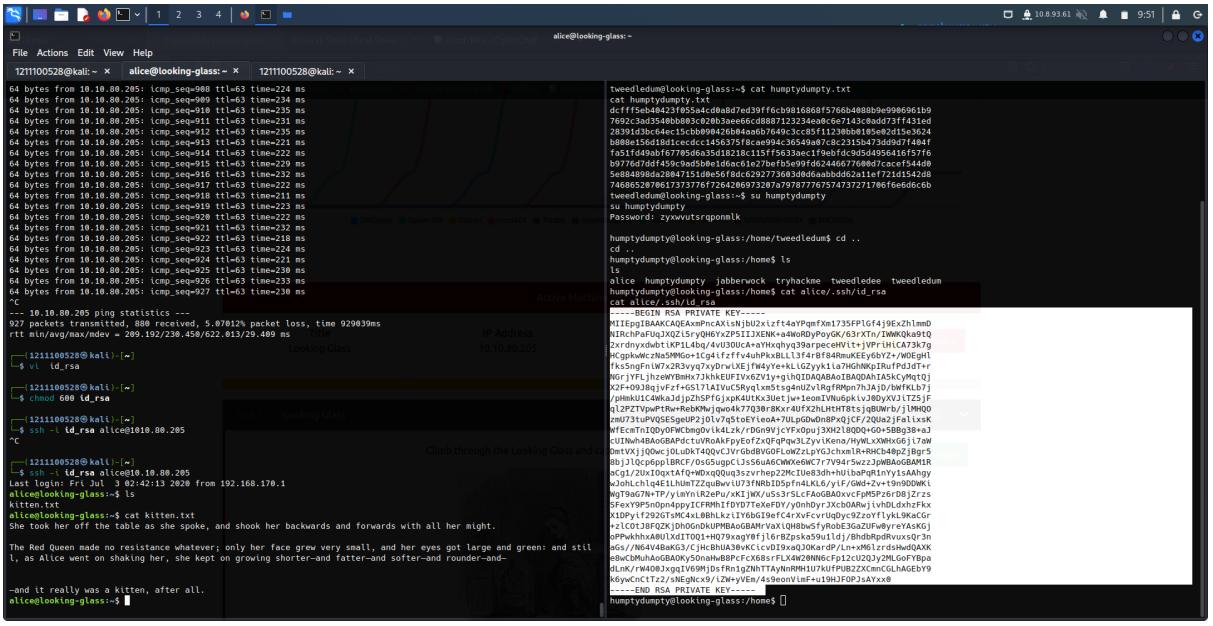
Thought Process & Methodology::



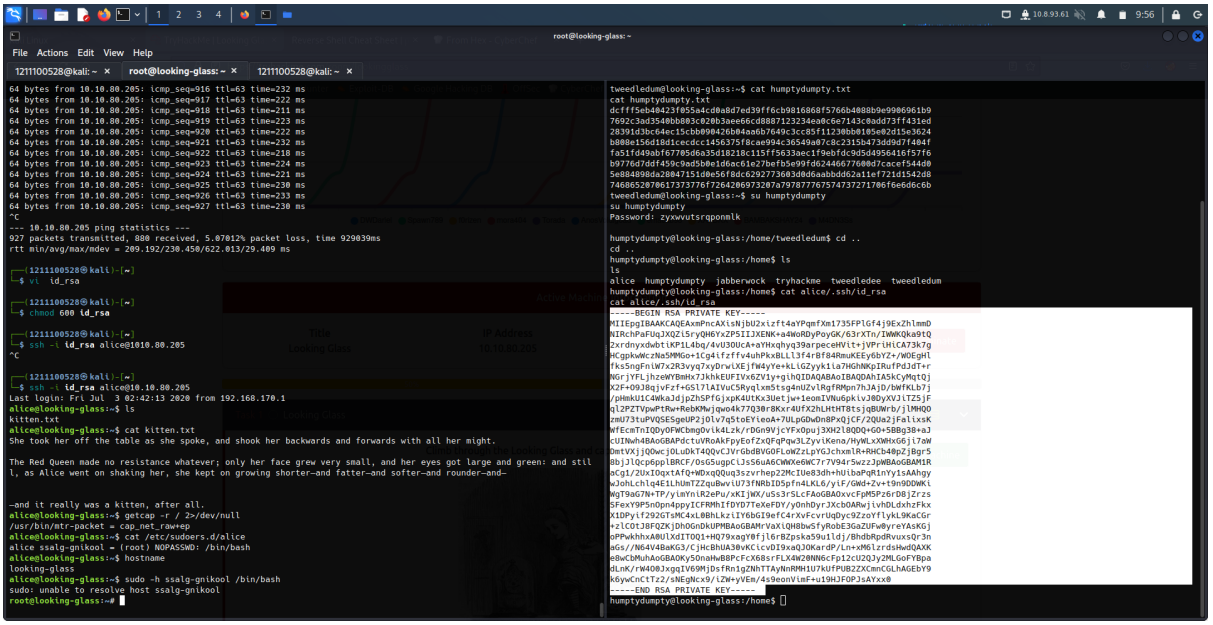
After we get the password ,we change the user to humptydumpy by using the command “su humptydumpy”. Then ,we enter the password. It will be the RSA PRIVATE KEY.



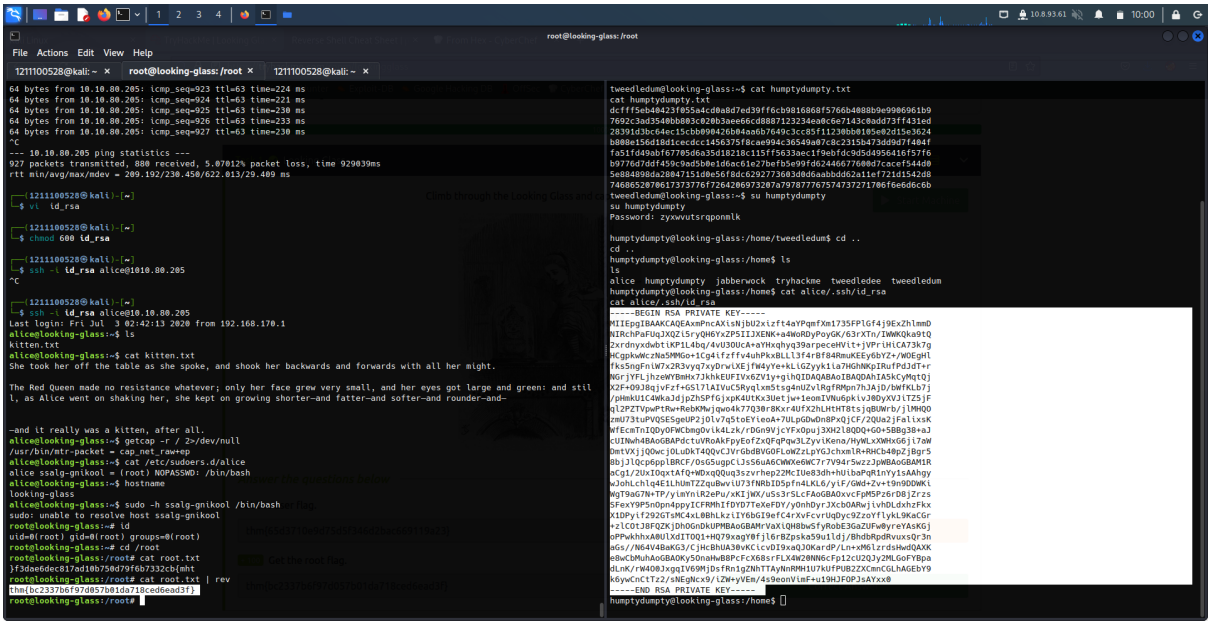
We copy the RSA PRIVATE KEY .We open a new terminal tab and type in a ‘vi’ command with id_rsa to open a new file and paste the RSA PRIVATE KEY. Then ,save it. The file is save as id_rsa



Enter a new command “chmod 600 id_rsa” to the terminal so that only the owner of the file has full read and write access to it. Then , we log in as Alice with the command “ssh -i id_rsa alice@ip address” .

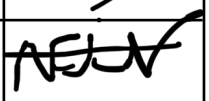


After that, we type in ‘cat’ command with “/etc/sudoers.d/alice” to get its root .We change the user to root by using the command “sudo -h ssalg-gnikool /bin /bash” .To make sure that it is the root ,we will use a command which is “id” .If its uid , gid and groups are all 0, then it is the root .



Then we enter the command cd /root to change the directory to root file. Finally, we use the ‘cat’ command with root.txt to view the contents of the file. The flag will be shown in reverse. To change to a flag that we want ,we use enter the command with an additional “| rev” added to the end of the command. The flag will be shown.

Contribution

ID	Name	Contribution	Signatures
1211101951	Zaieff	Did the Initial Foothold part , found the first flag , moral support giver	
1211100528	Arief	Did the recon and enumeration , food supplier	
1211101643	Siva	Did the horizontal privilege escalation part , drinks supplier	
1211101120	Adam	Did the root privilege escalation part , found the second flag