PENTEST 1
ROOM A

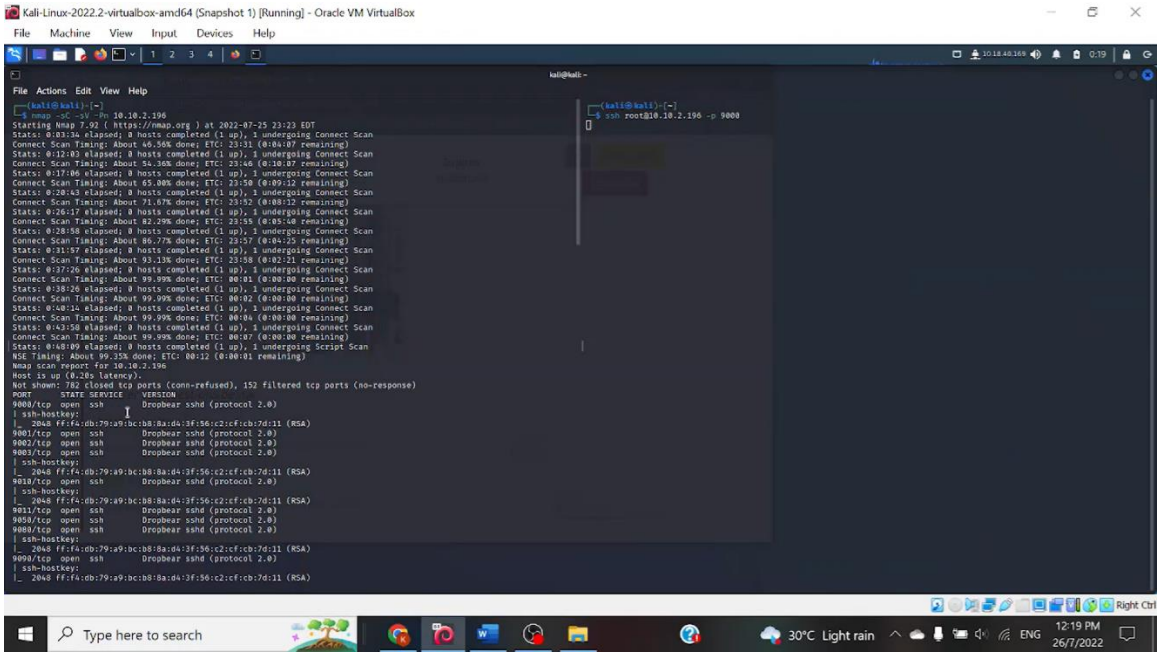
ID	NAME	ROLE
1211100930	Ku Najwa Syauqina Ku Azrin	-

RECON & ENUMERATION

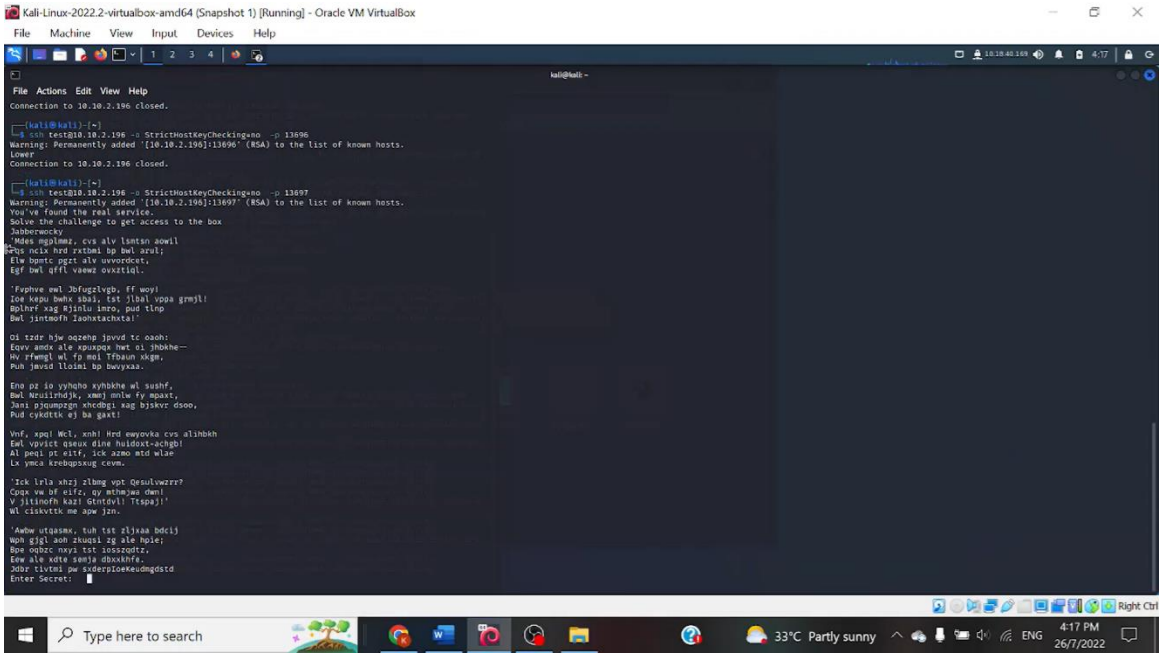
Tool used : Nmap

Thought Process and Methodology and Attempts:

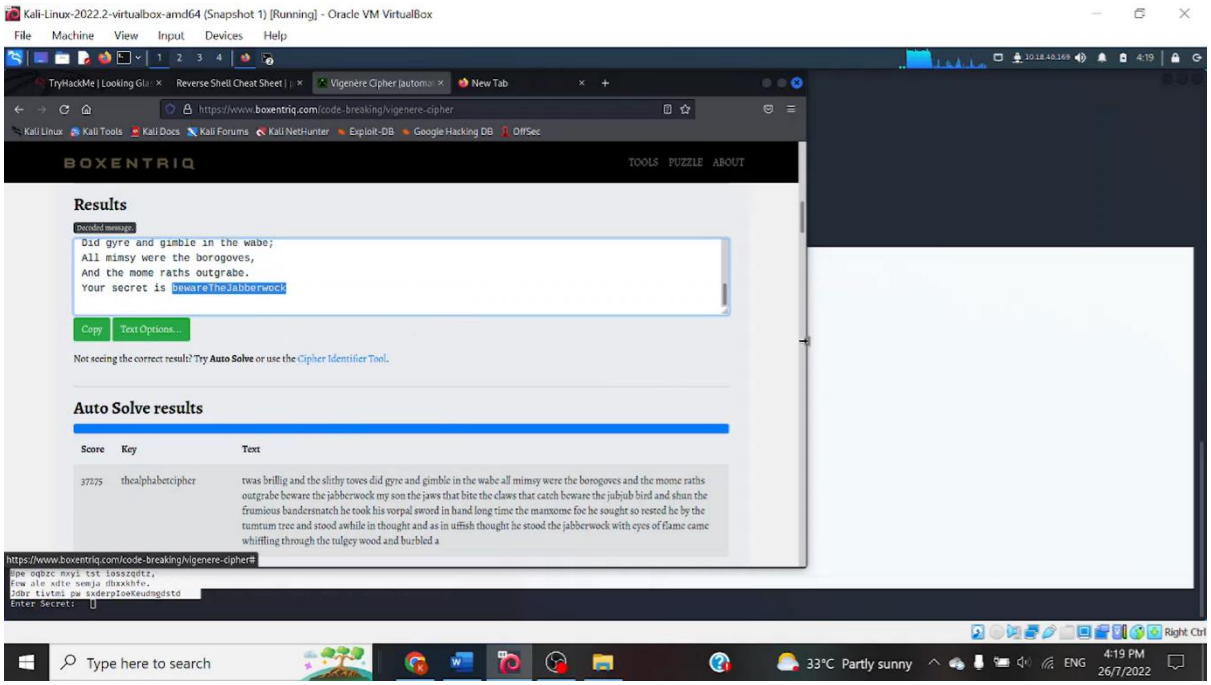
Check open ports with Nmap.



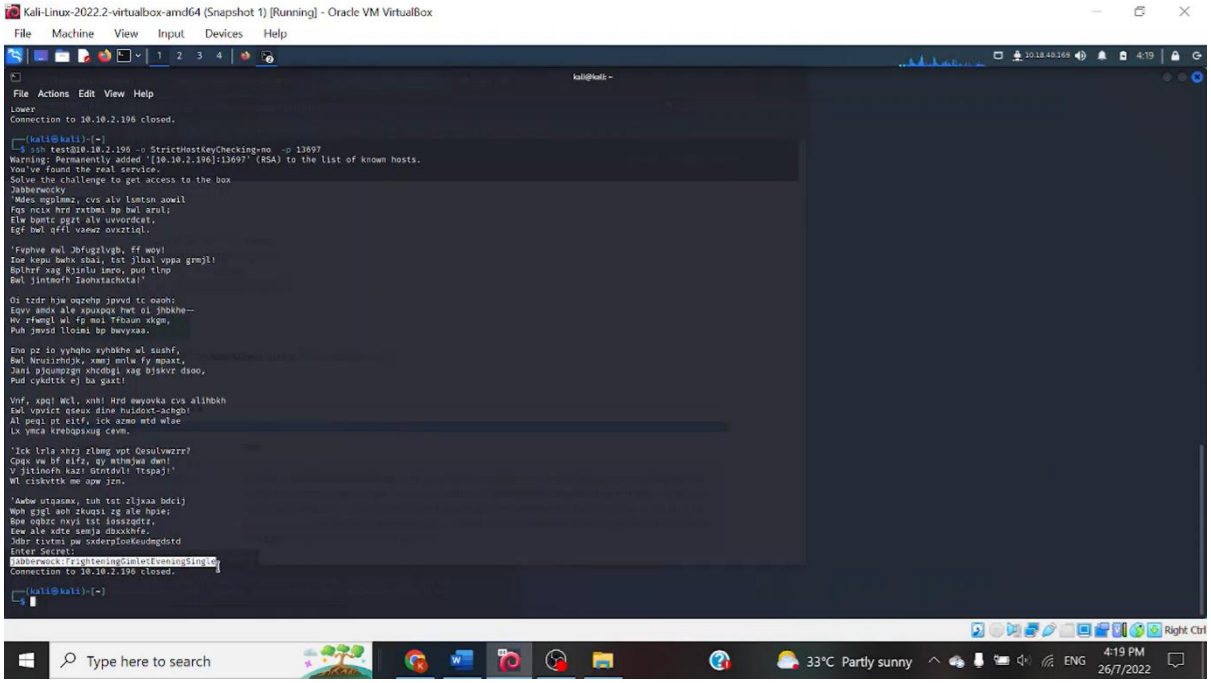
OpenSSH running on port 22, with thousands of other open ports. Now I will try connecting to one of them. Once connected, message Lower was returned. I tried connecting to other ports, same message. But I tried going for the highest port, message higher was returned. After a while, I guess that these are the clue for me to get the correct port. So, I keep on trying until I manage to find the right port.



After connecting to the right port. apparently, the output looks like an encrypted message that we have to decode. Using any cipher identifier site copy and paste the output. Click decode.



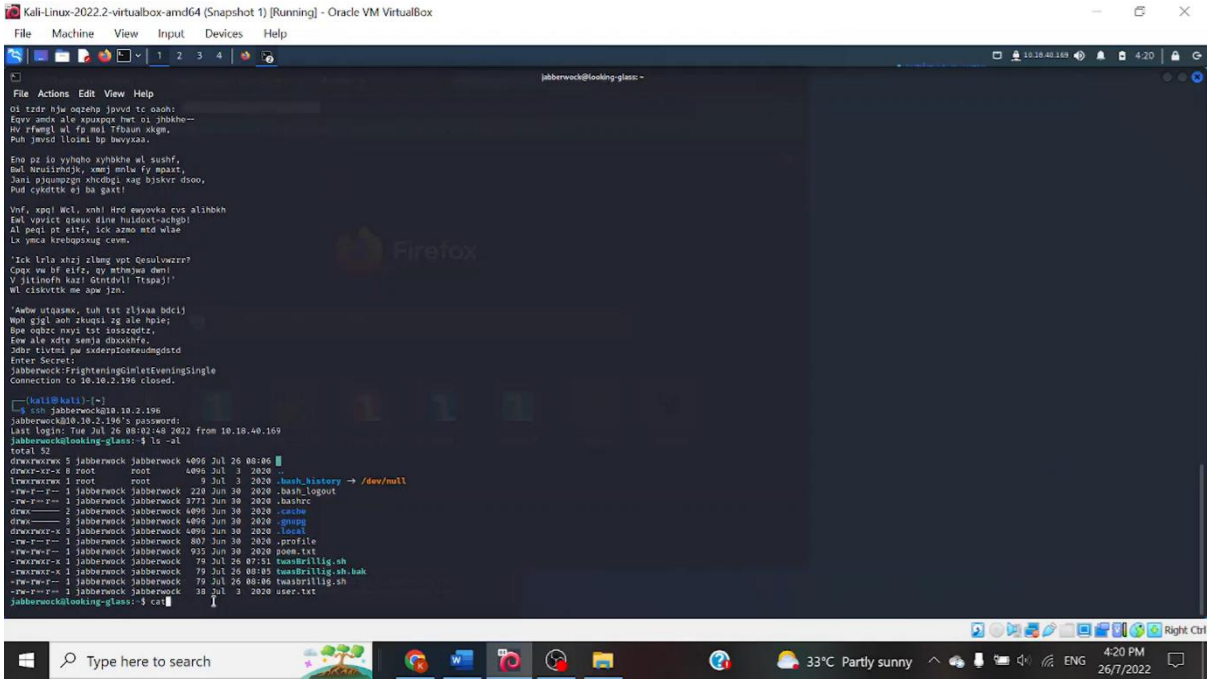
At the end of the output, it shows us the secret. Enter the secret message. We will get the username and the password.



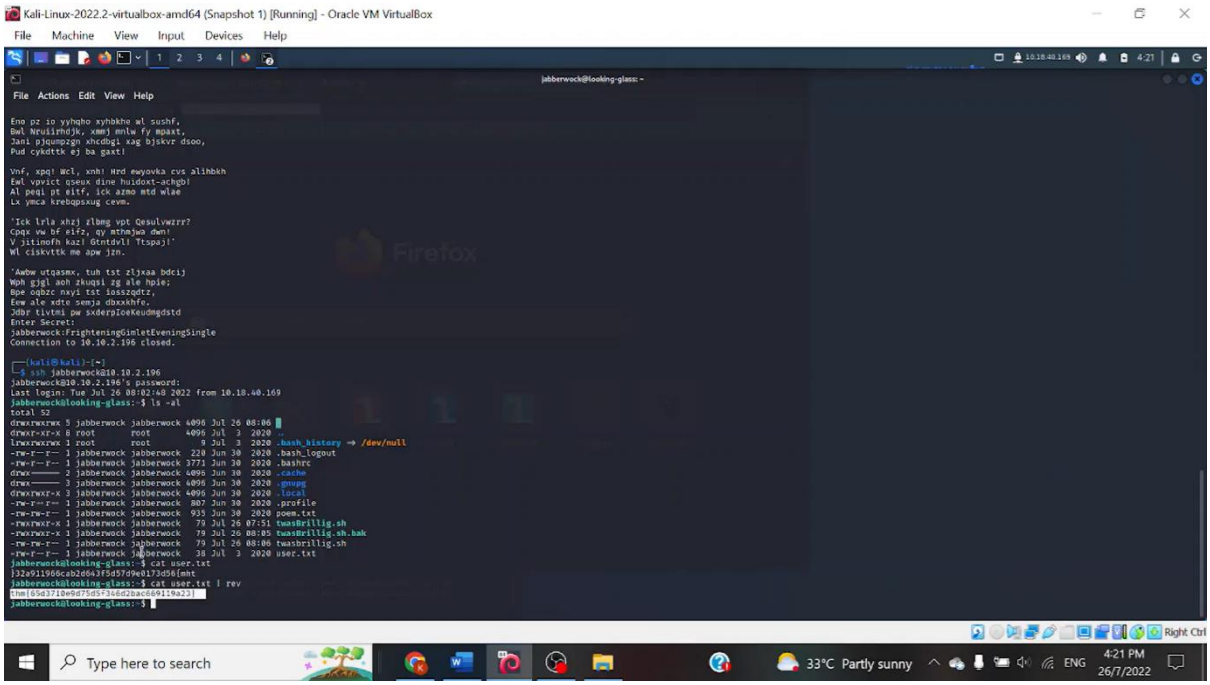
Initial Foothold

Thought Process and Methodology and Attempts:

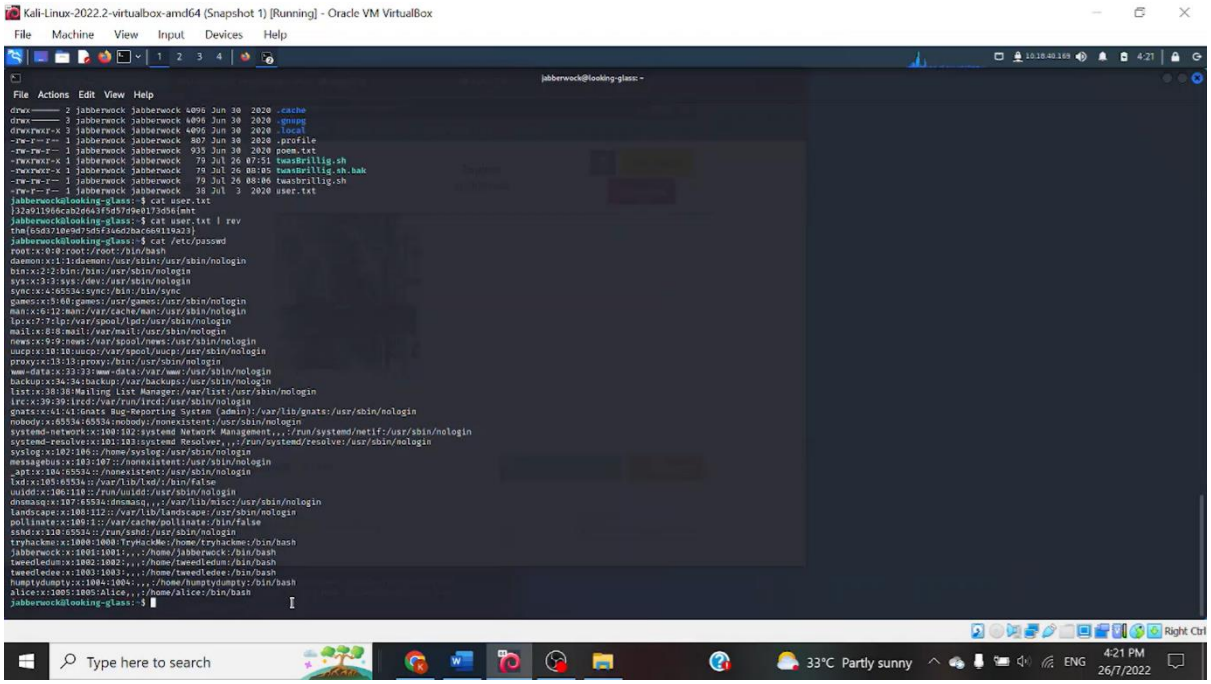
using ssh on the default port, which is port 22, enter the password and explore what file we have here.



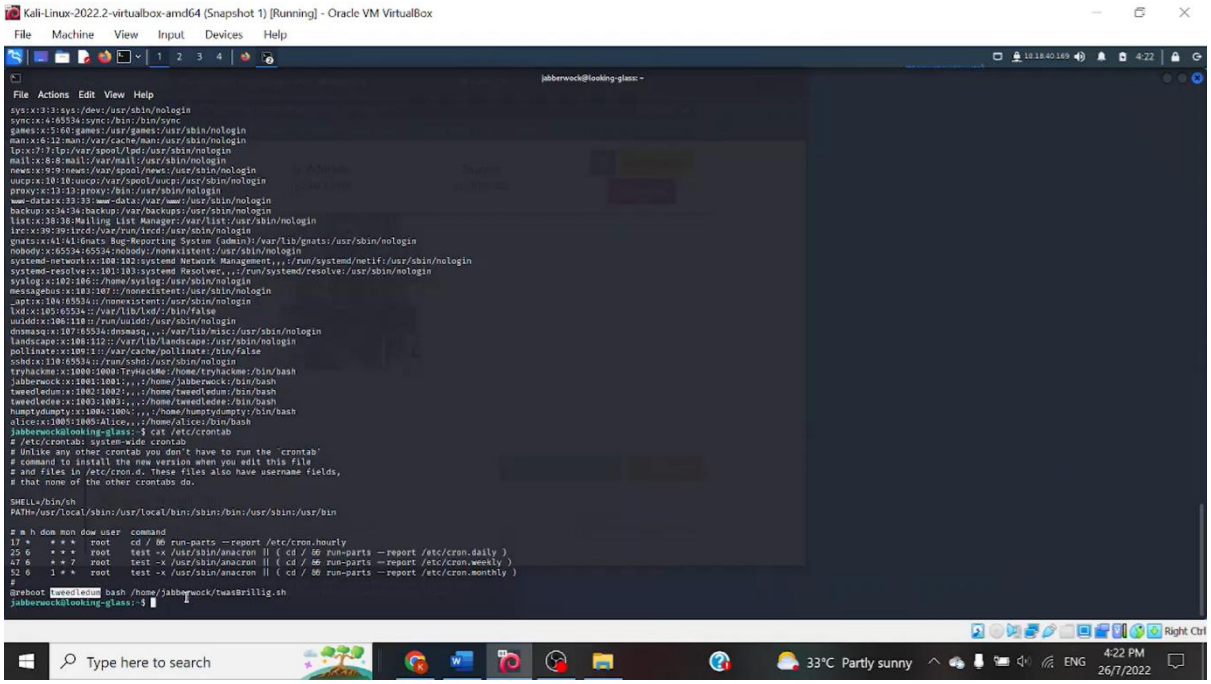
We can see user.txt is listed and we are asked to fine user flag. using cat command to get the user flag. but the flag is in reverse, so we'll need to reverse it.



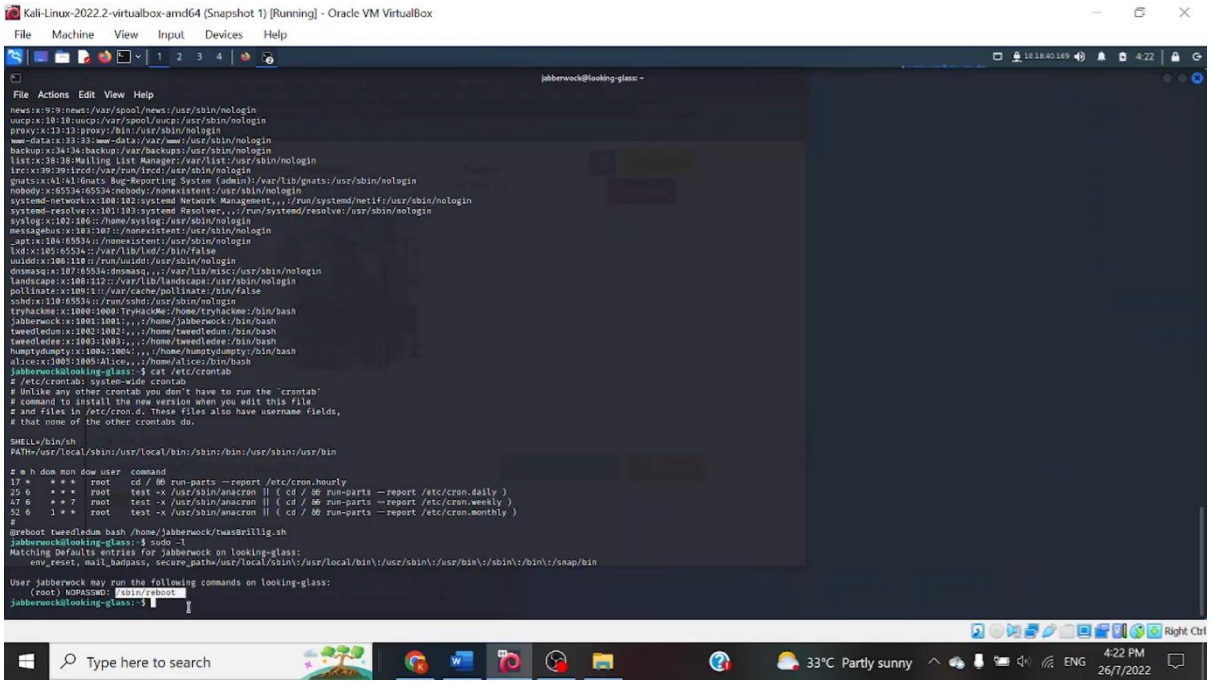
Go to passwd file to see available users.



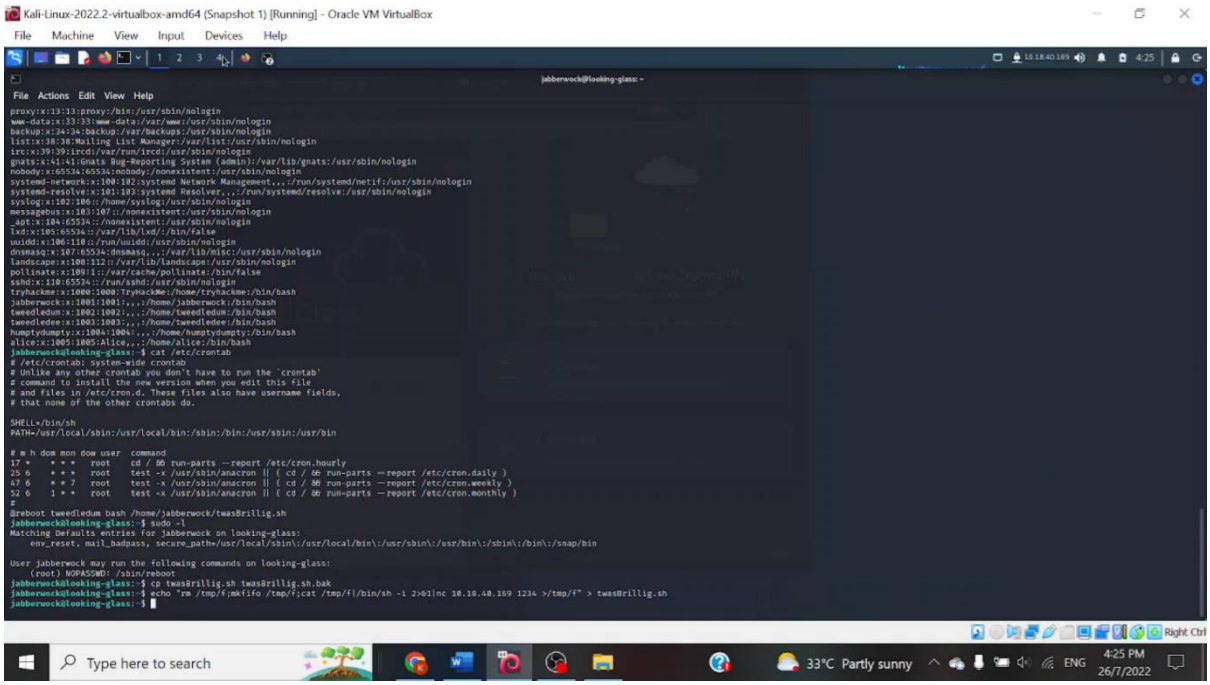
Using command cat /etc/crontab to see any cron job running. twasBrillig.sh is running as user Tweedledum as server reboot.



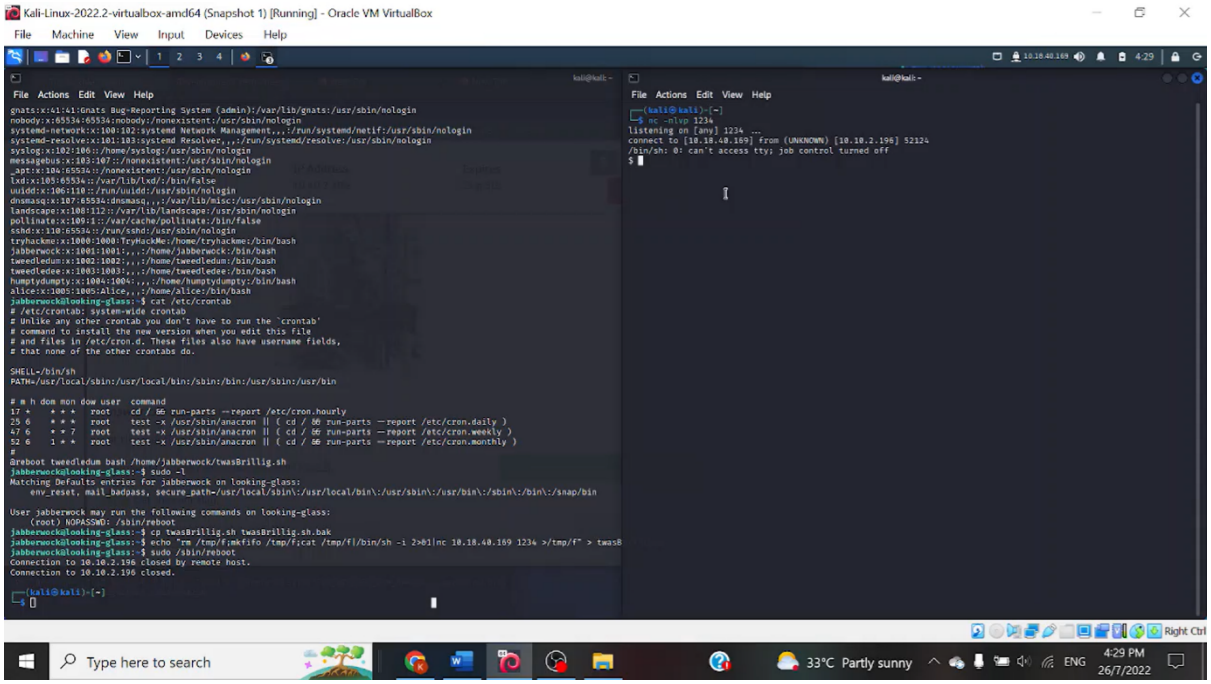
Using sudo command to check what sudo permission we have. And it looks like we don't need password to reboot the box.



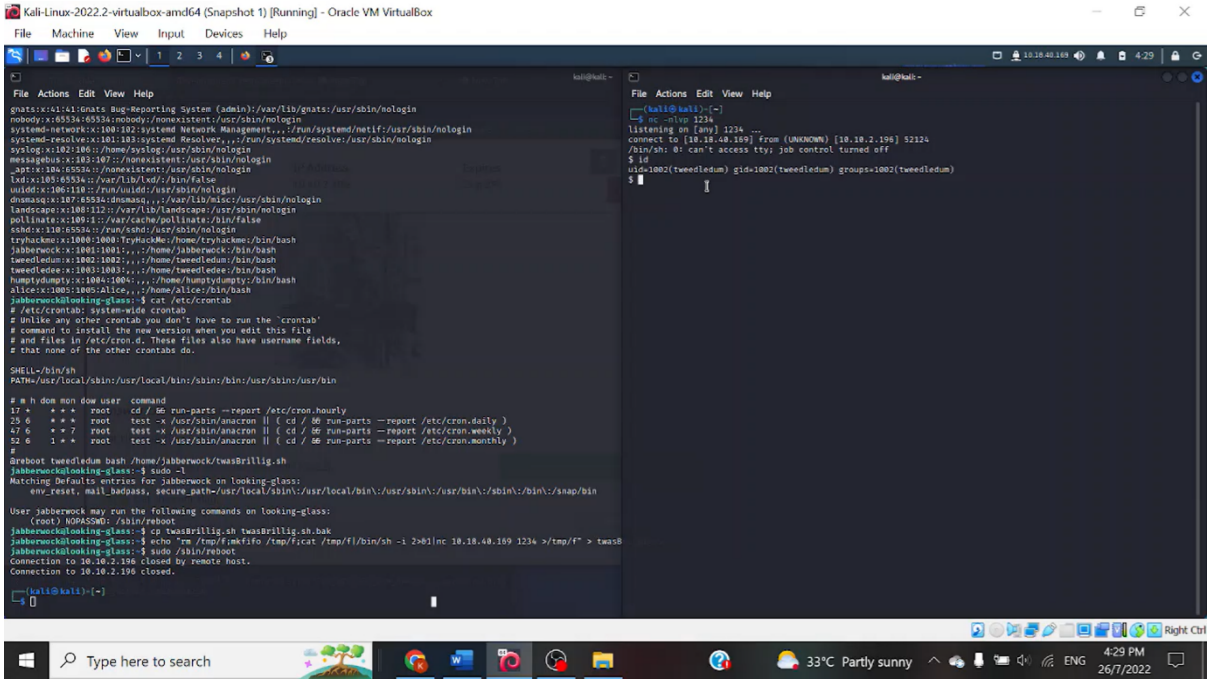
I replace the content of twasBrillig.sh with one from the PentestMonkeys site.



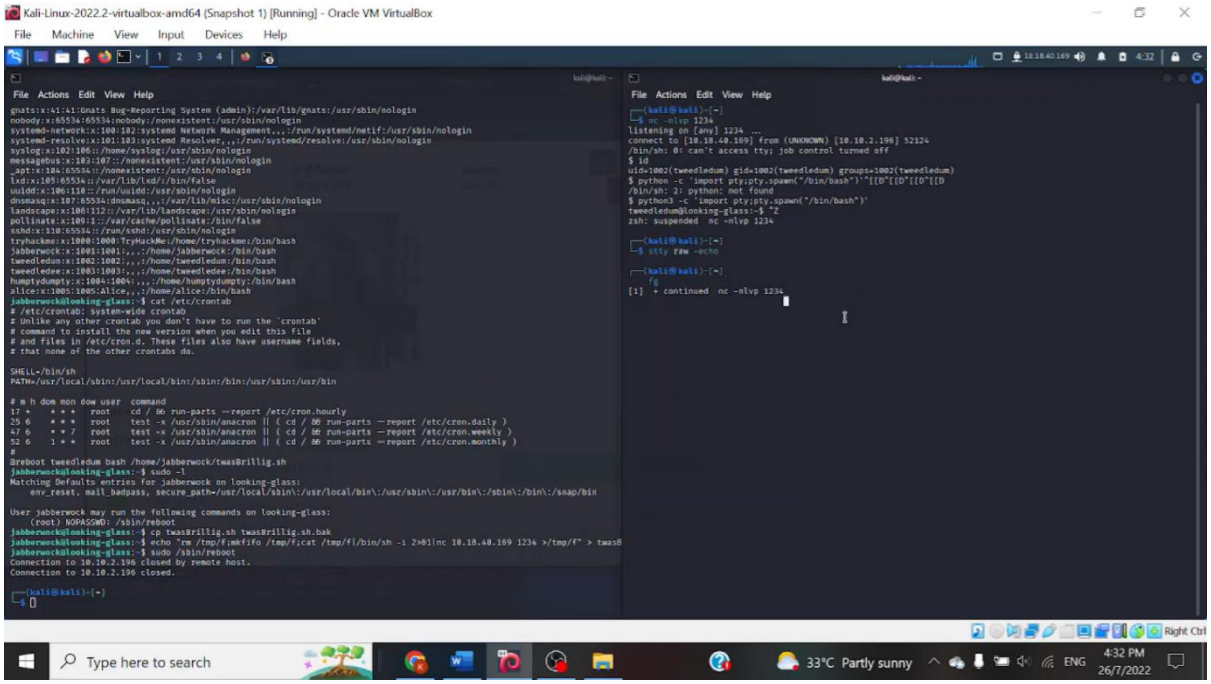
Start a netcat listener. And reboot the box. After few seconds, the box is connected



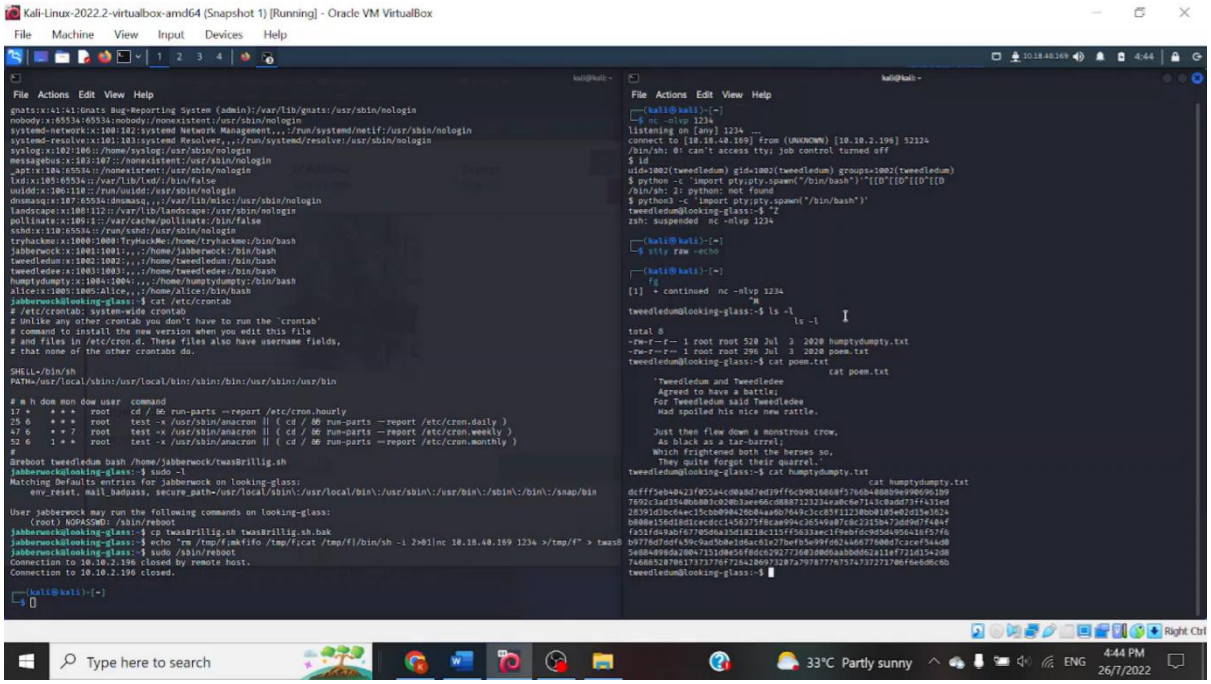
We are connected as user Tweedledum.



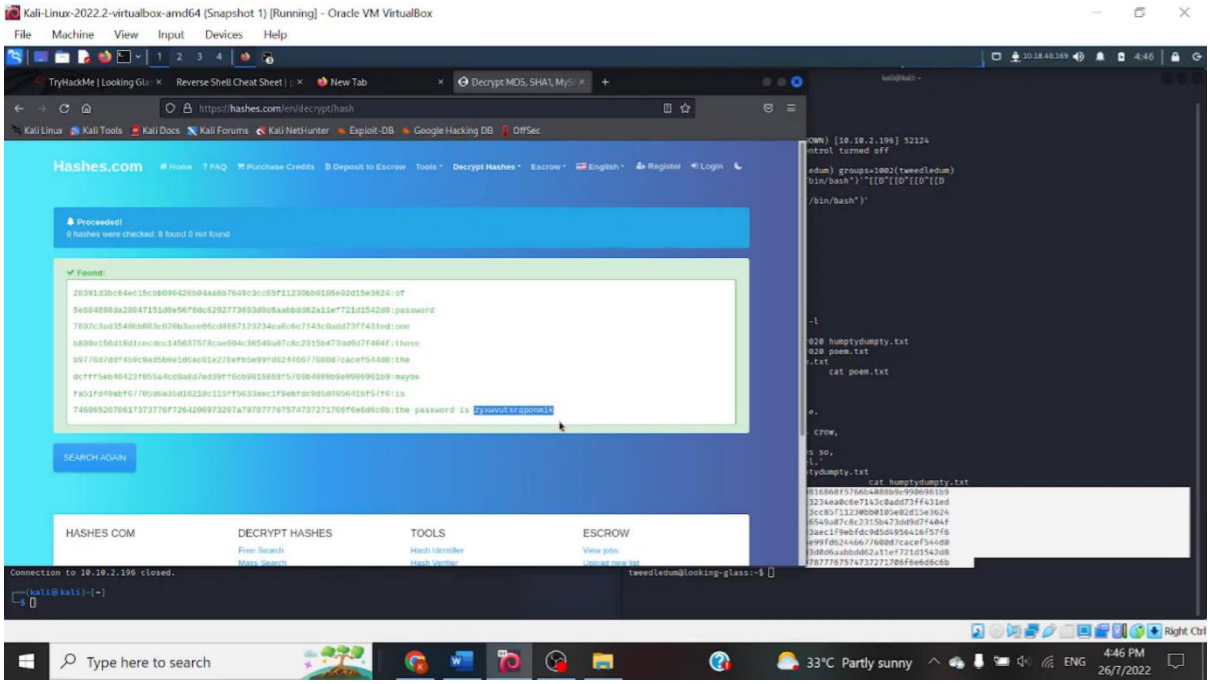
Upgrade the shell to the proper shell.



let see what we have in the home folder. We have two files here. One is a poem and another one is encrypted.



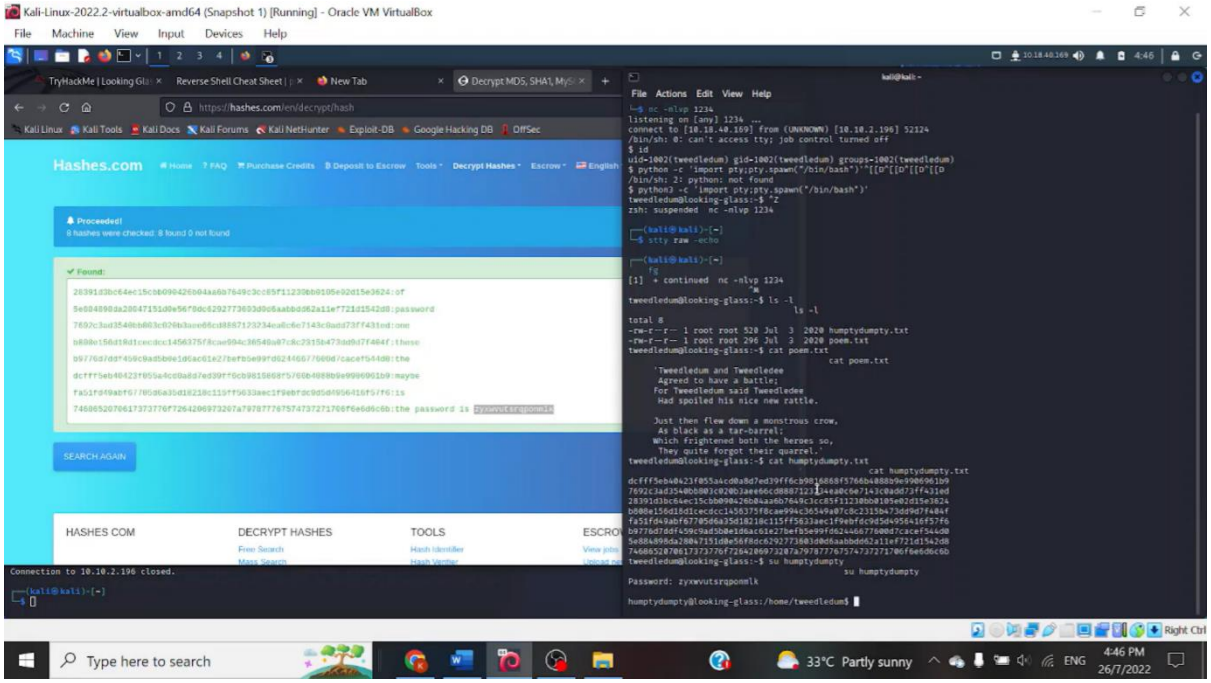
I use an online hash cracker; hashes.com to crack the encrypted message. We get a password.



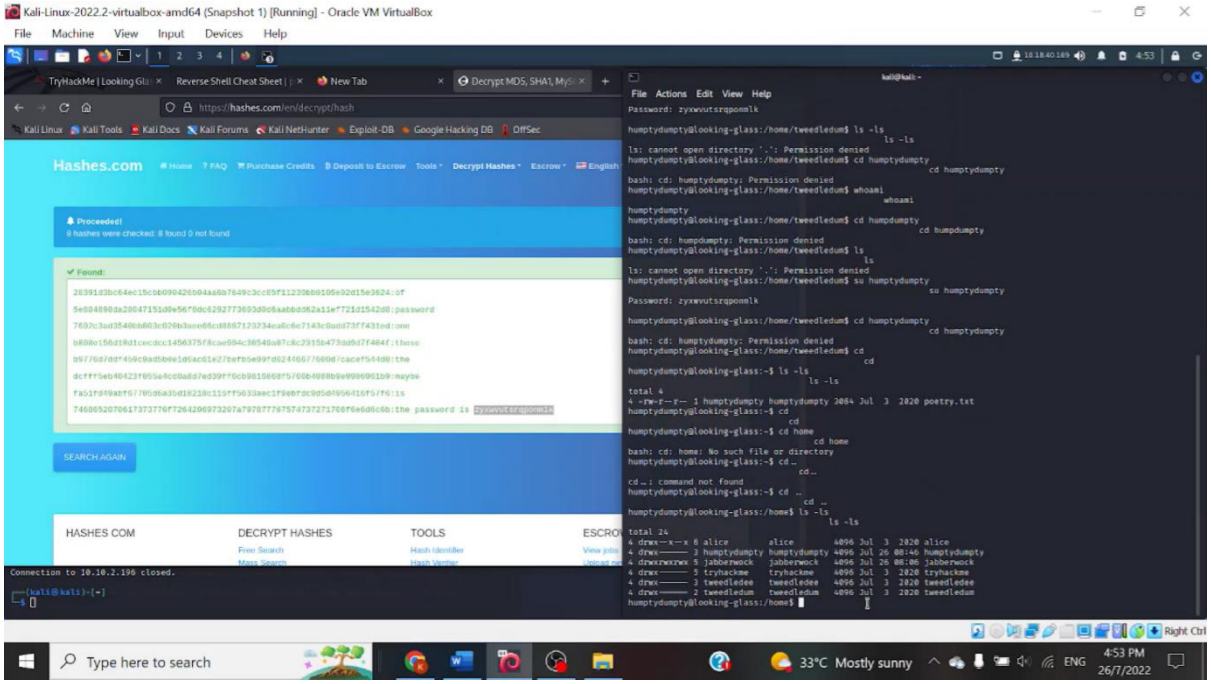
Horizontal Privilege Escalation

Thought Process and Methodology and Attempts:

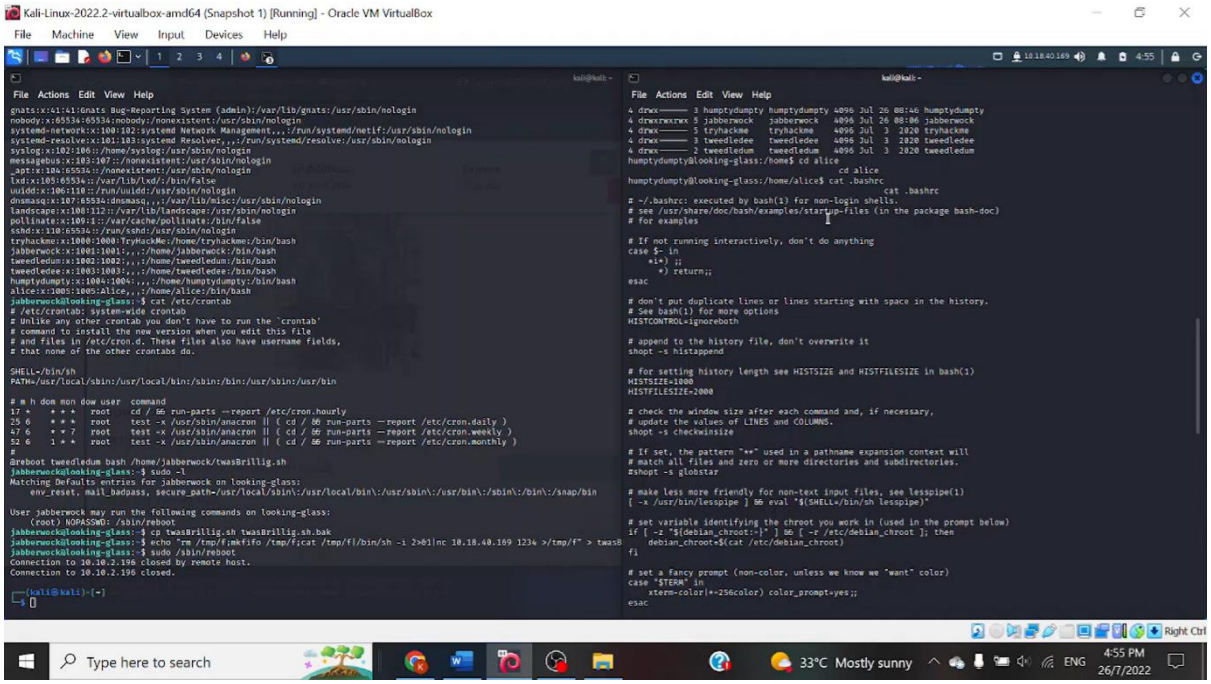
Since we know there is a user humptydumpty, and the password we gain is from humptydumpty.txt. so, I guess it's the password for that user. Using the su command to switch to user humptydumpty and enter the password.



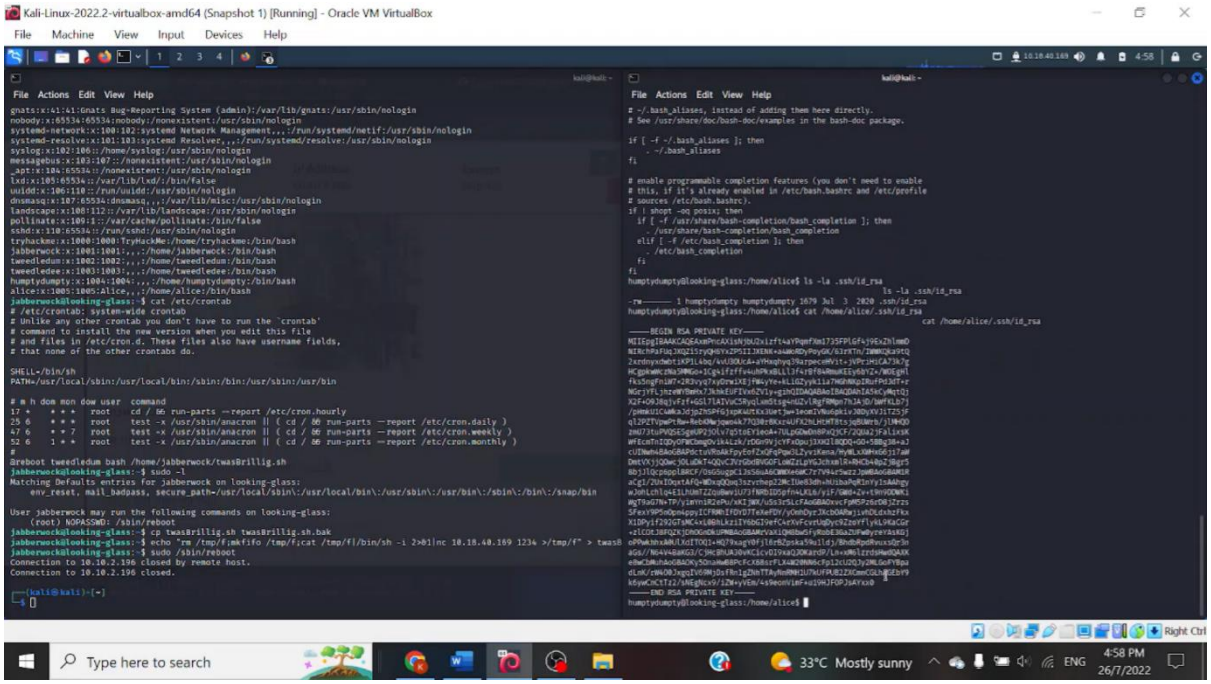
Let's look at what we have here, there's a folder named alice and we know it's one of the users.



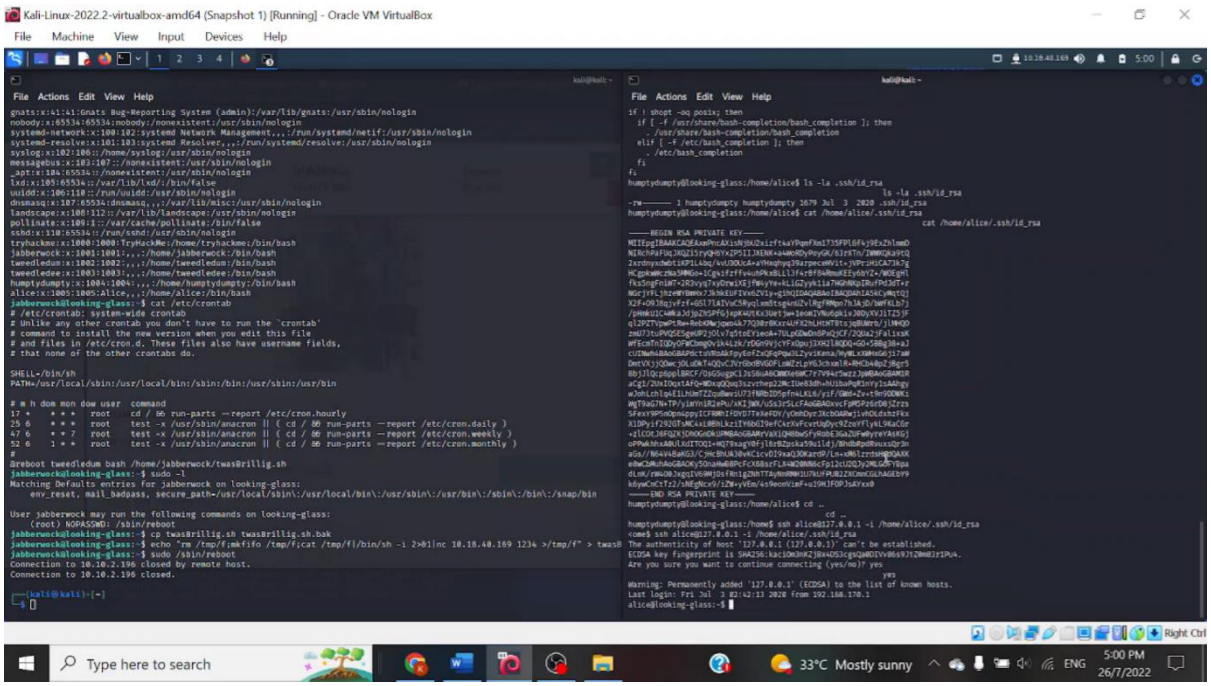
Go to alice home folder. We have permission to read the .bashrc file.



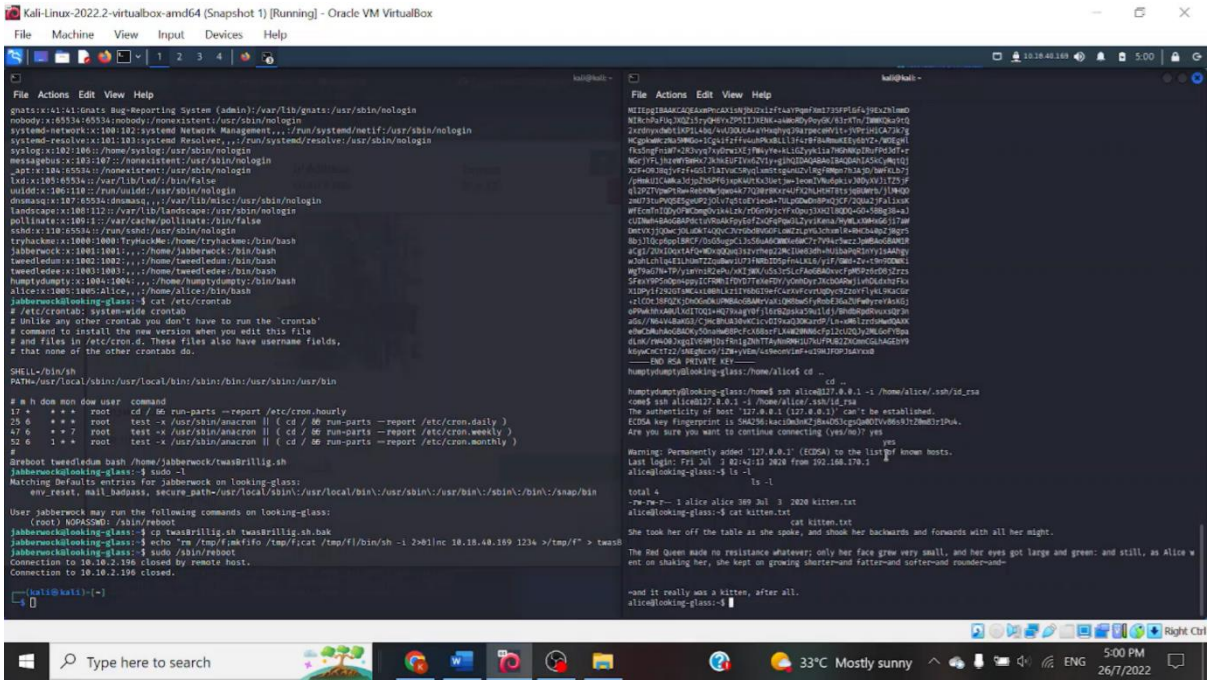
Find rsa_key. Just as I expected, the id_rsa file is in .ssh/folder. And fortunately owned by humptydumpty so we can read the content



ssh to alice using that file and we are logged in as alice.



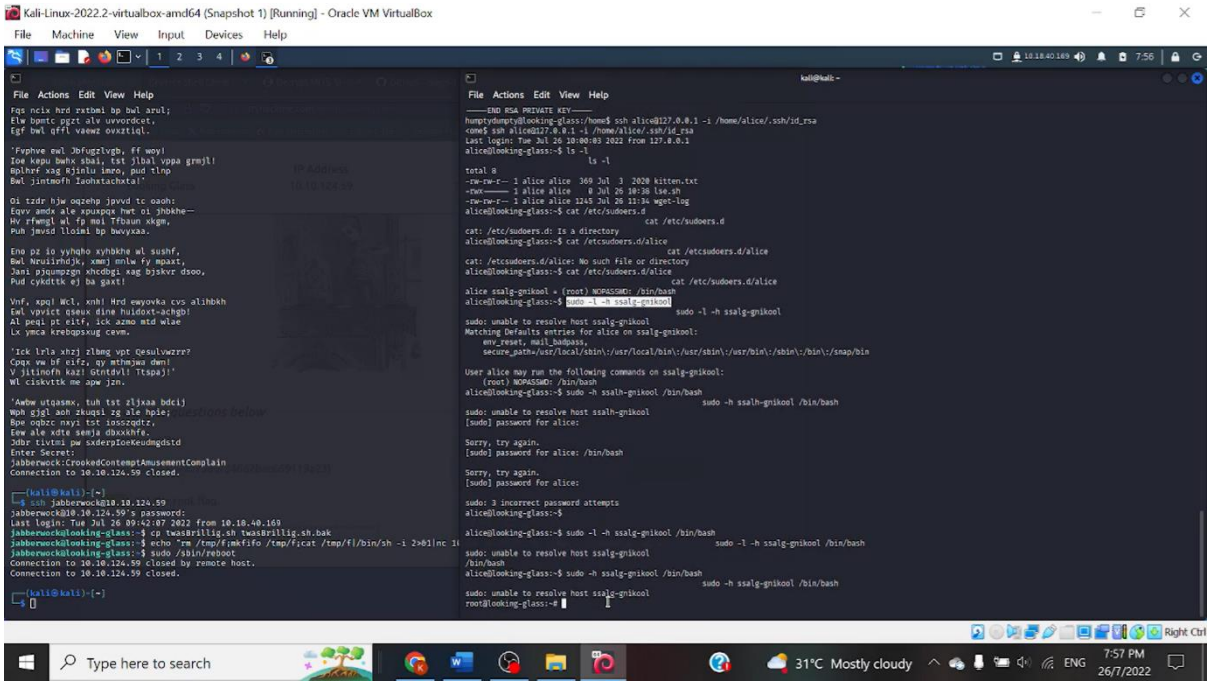
We have only one file kitten.txt, but it's useless to us so we have to use the enumeration script.



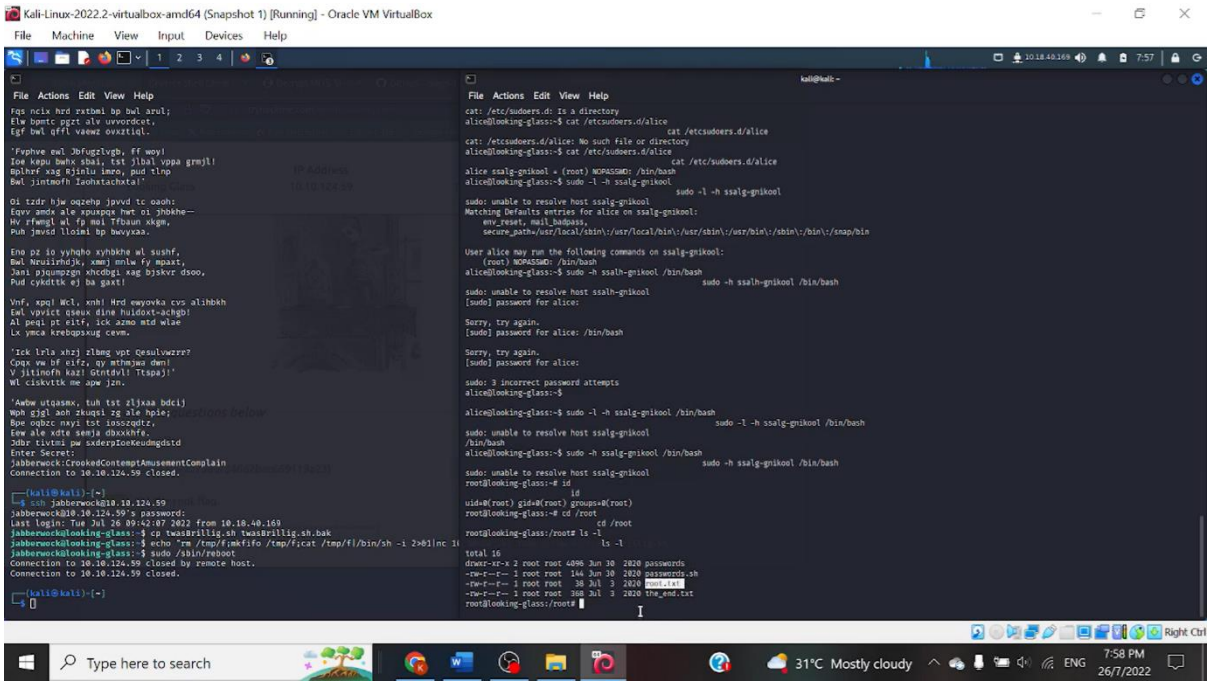
Root Privilege Escalation

Thought Process and Methodology and Attempts:

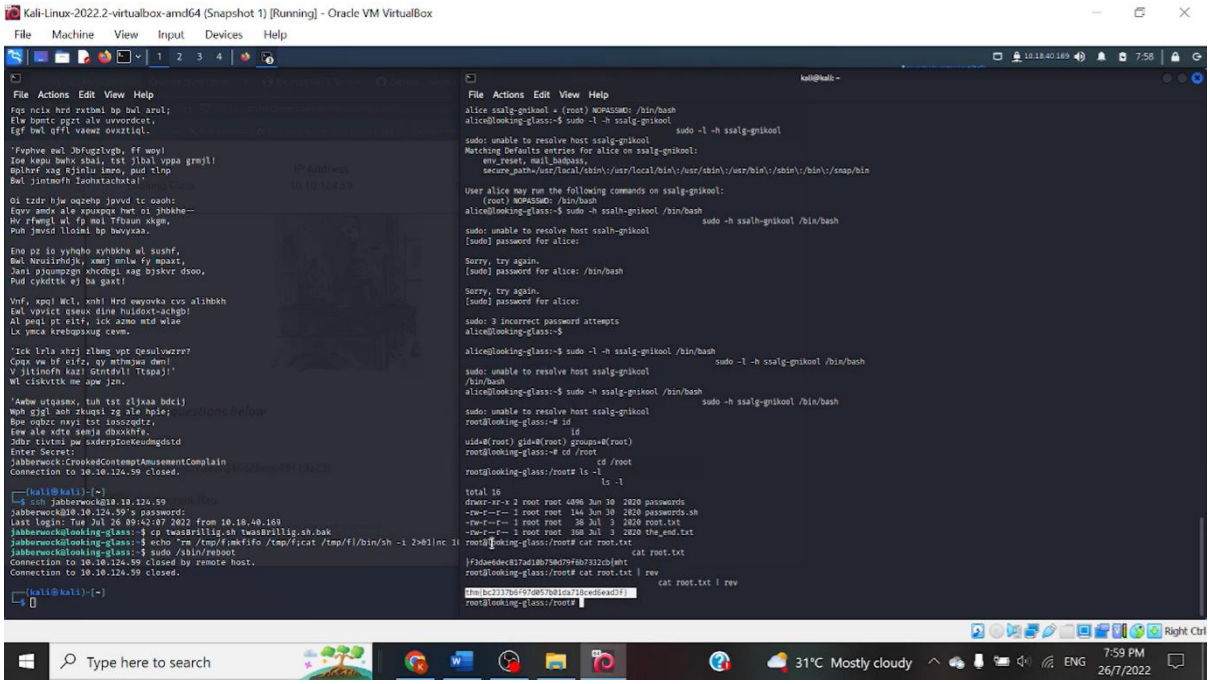
Using cat command to view the etc/sudoers.d/alice file. We can run /bin/bash as root but we can't run this directly using sudo /bin/bash like we used to. We can specify the hostname using -h with sudo though. We know that ssalg-gnikool is the hostname. So, to prove, we can use the -h flag. once confirmed we can escalate to root!



Using the command cd root to go to root and let see what file we have. since what we want is the root flag let's view root.txt



Using cat command to view root.txt, and finally, we get the flag!



Contribution:

id	Name	Contribution	Signature
1211100930	Ku Najwa Syauqina Ku Azrin	-	

Note: Screenshots are from obs' screen recording that's why all the screenshots look a bit blurry.

LINK VIDEO: https://www.youtube.com/watch?v=lBTfBki-3FA