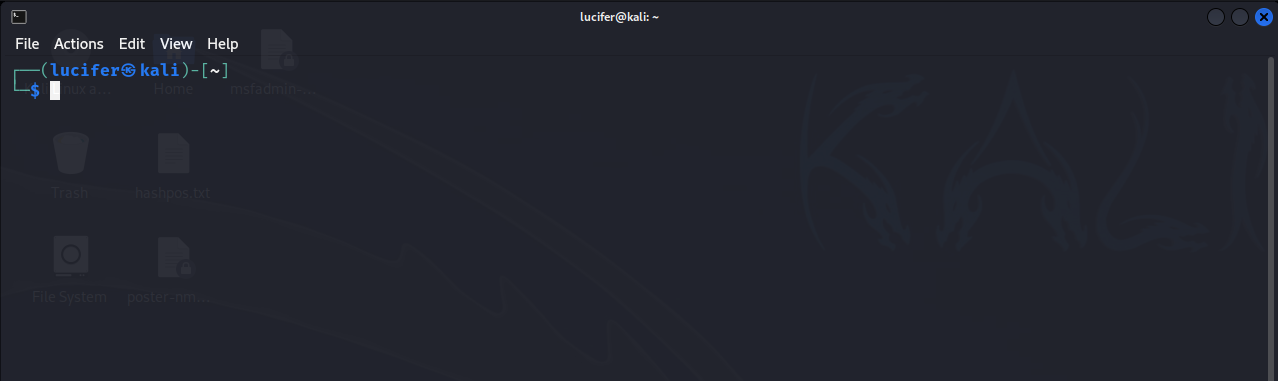
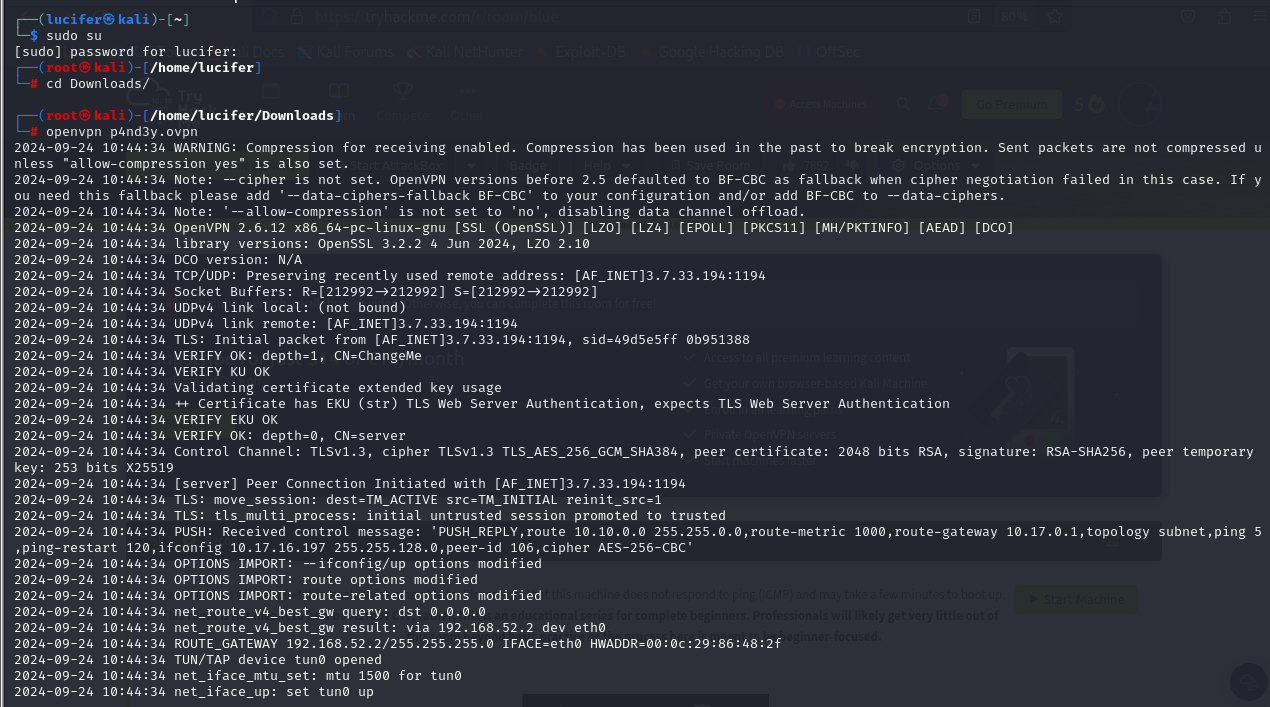
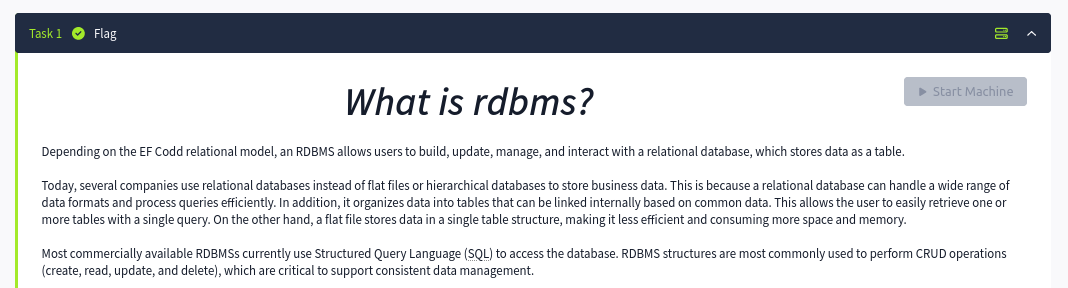
Poster is a box on tryhackme (<https://tryhackme.com/r/room/poster>) created by **stuxnet**.

Here our **terminal**  is opened.

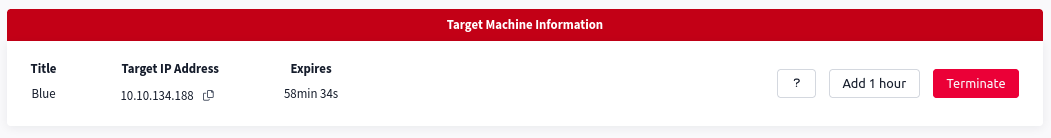


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.



Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. 

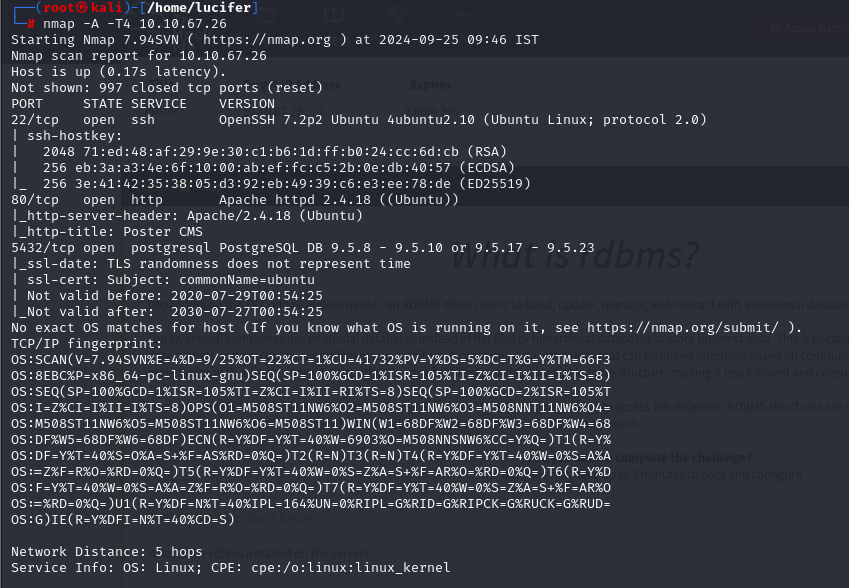
After starting the machine it’ll get one minute to show the ip.



After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.

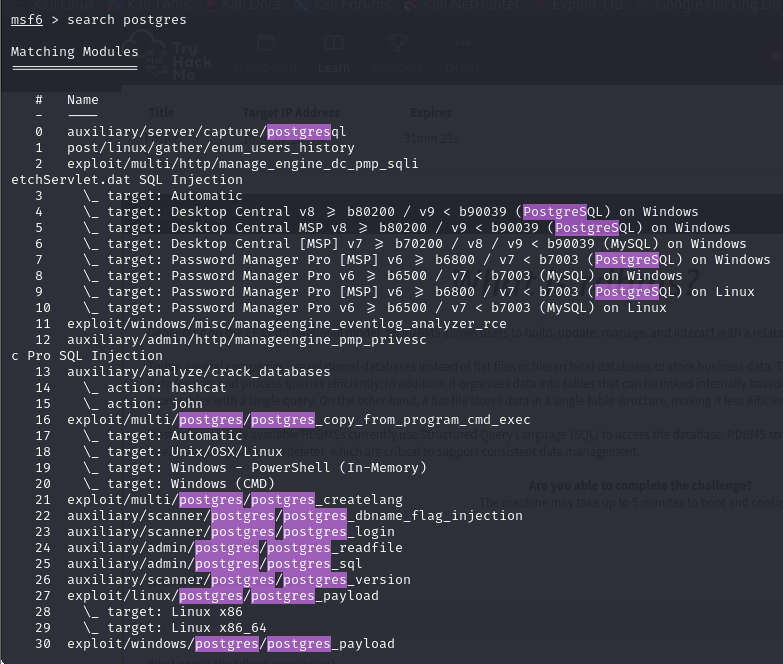
Here I am using **nmap -A**  **-T4 <IP>**  to see all the ports. You can use many more scripts like **nmap -sCv -T4 <IP>**

Seems like our scan is completed. Looks like there are total 12 ports open and 3 under 1000.



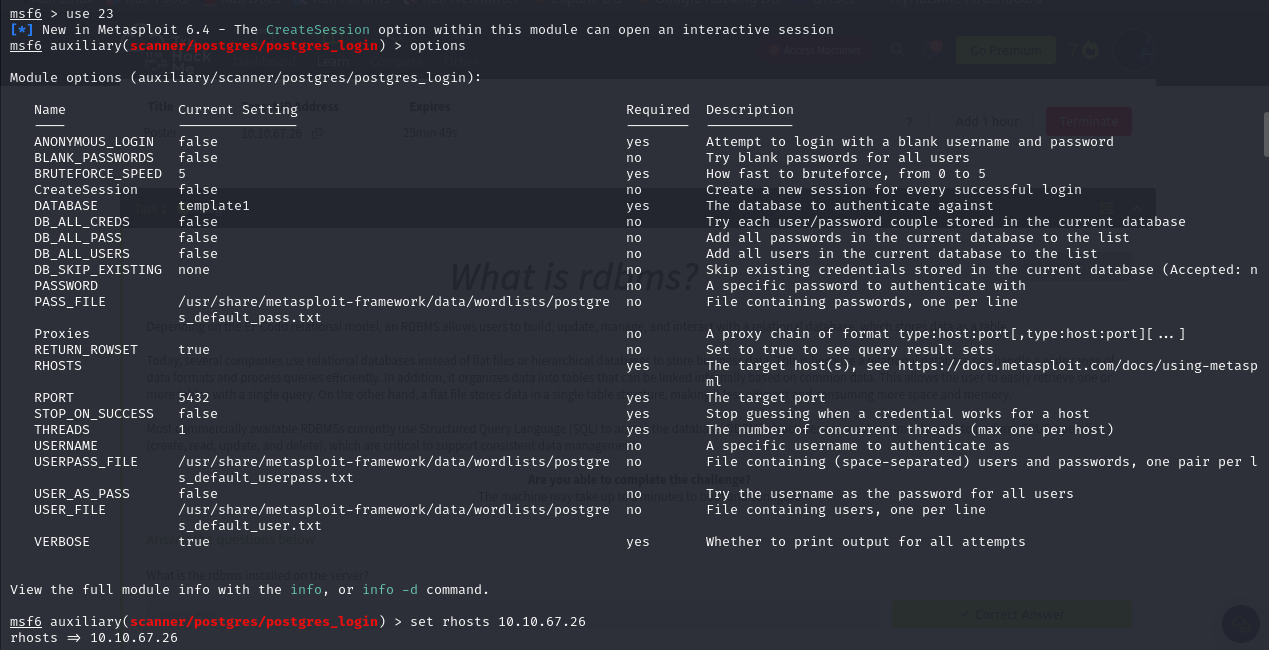
Now that we have know the information from port 5432 using nmap and there lies a severe vulnerability in Postgres database. We can use **searchsploit** or google it about the previous exploits in it. Guess what we found it using searchsploit. Seems that it has severe vulnerability in login bypass and many more.

Now we’ll use **msfconsole(metasploit)**  to exploit this machine as we know the vulnerability after further research. We’ll search the exploit on metasploit.



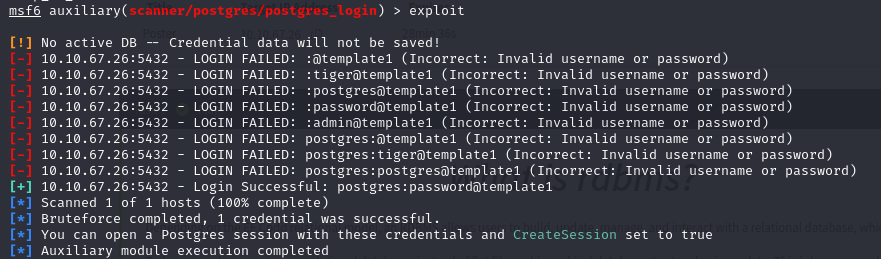
We found many exploits. Now we’ll use it one by one for different purposes.

Our first exploit that we’ll use is login bypass which is in option 23.



We’ll set **RHOSTS** as the target ip and rest will be default.

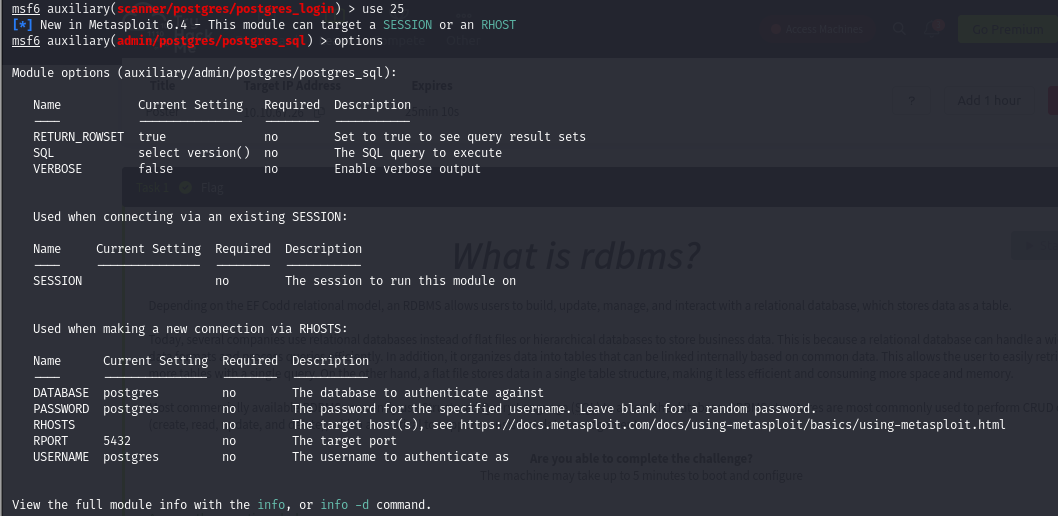
We’ll now start the exploit.



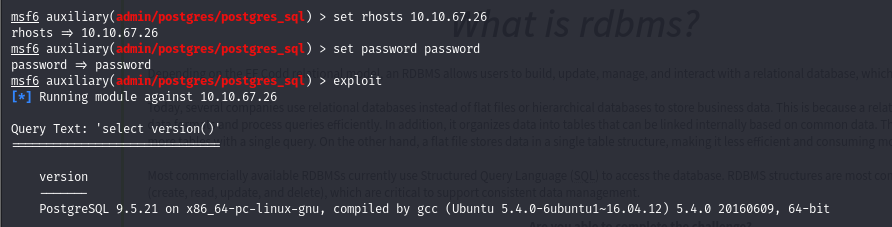
Here we found our username and pass – **postgres:password**

Now we will set our new exploit that will help us to know what exact version **PostgreSQL**  is using.

The exploit is in option 25 from 2nd page.

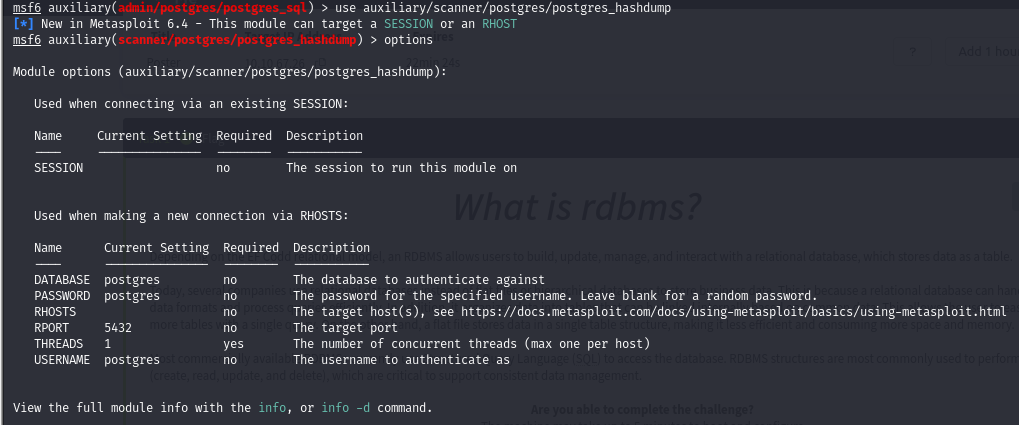


We will now modify the **password** and **rhosts**  in the options and run the exploit.

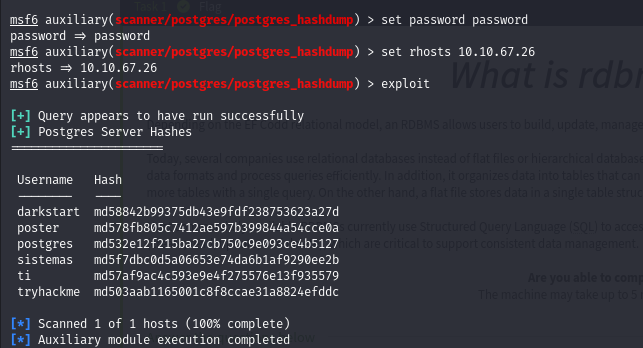


We found the version of the database which is **9.5.21.**

Now we will use our next exploit from 2nd page to dump all the hashes in the target system.



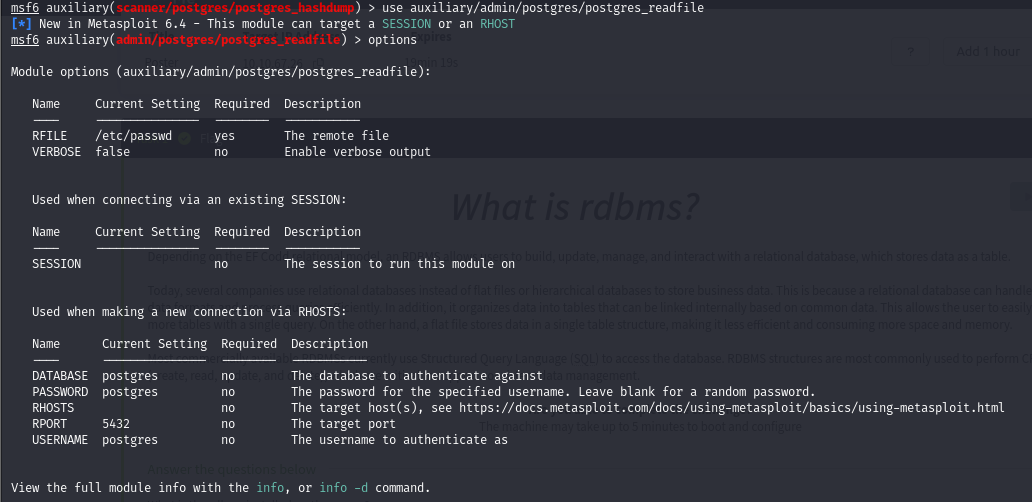
Again We will now modify the **password** and **rhosts**  in the options and run the exploit.



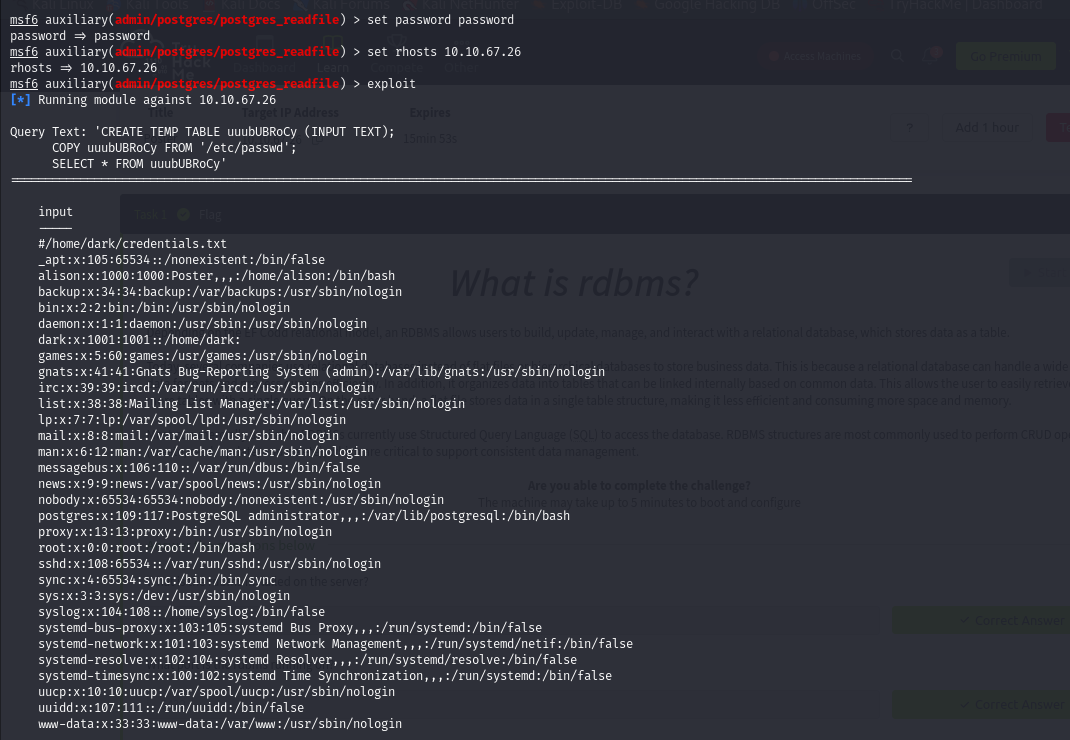
We see that there are total six hashes of six users.

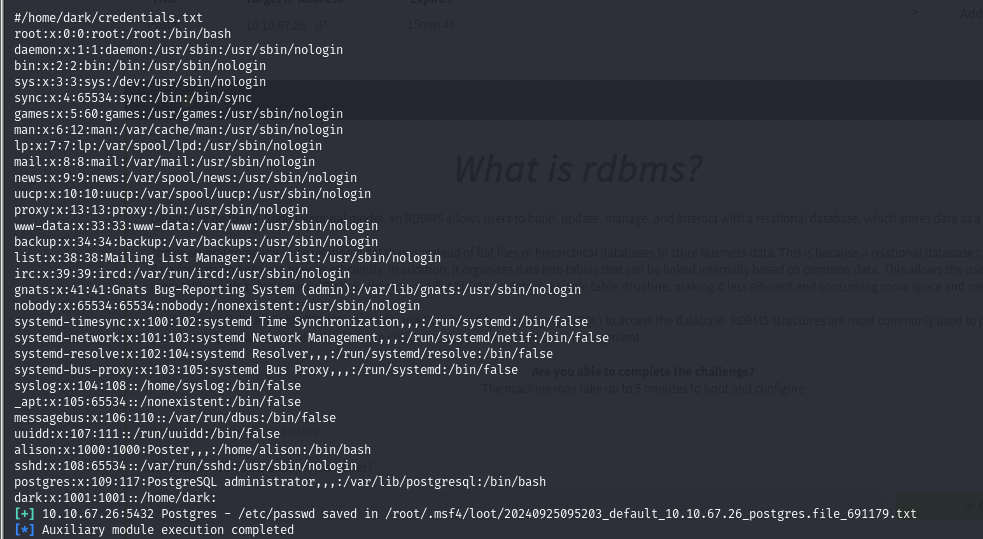
Now will check the /etc/passwd file to confirm the users and their password locations.

We’ll take new exploit from page 2nd which is **postgres\_readfile.** It will show us the table containing users and their addresses present in target system including root.



We will modify the **password** and **rhosts**  and run the exploit.





From these tables we know that there are two main users on the system including root which are **alison** and **dark.**

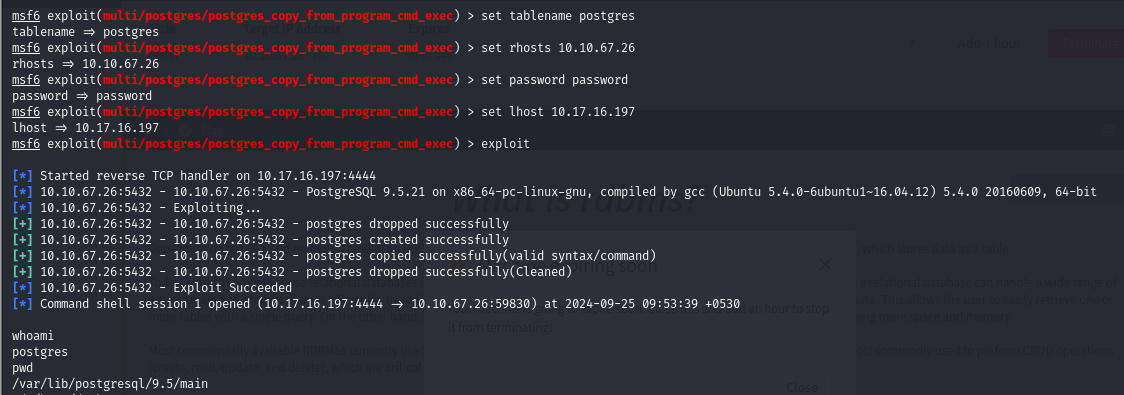
We now know the users so we will try to do command execution in the target system to get **command prompt.**

We can see in 2nd page that there is an exploit for remote command execution. We will use that exploit.

We will use the exploit shown below and modify the options which are needed.

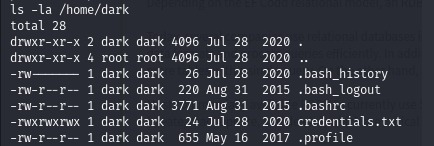


We need to modify **tablename, password, rhosts and lhost**  and then we can run the exploit.



As you can see we got command shell in the target machine and we are **postgres**  and our current directory is **/var/lib/postgresql/9.5/main.** We will now explore the machine.

As we know we have user **dark** we can use **ls -la /home/dark**  command to see what this user has got.

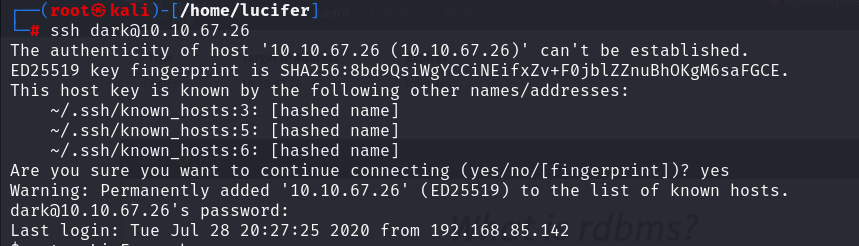


We can see there is a **credentials.txt** file and we can cat it out using cat command.



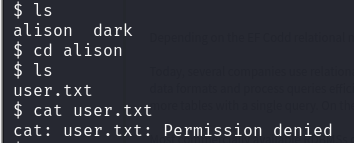
We got dark’s password.

Now we will ssh using dark’s username and password and see what’s there.



After doing this we get our **bash shell.**

Let’s explore the system. We can see that there are two users as we found on table in home directory - **alison** and **dark and alison** has our **user.txt** file. But dark has not the privileges to read the file in alison’s folder.

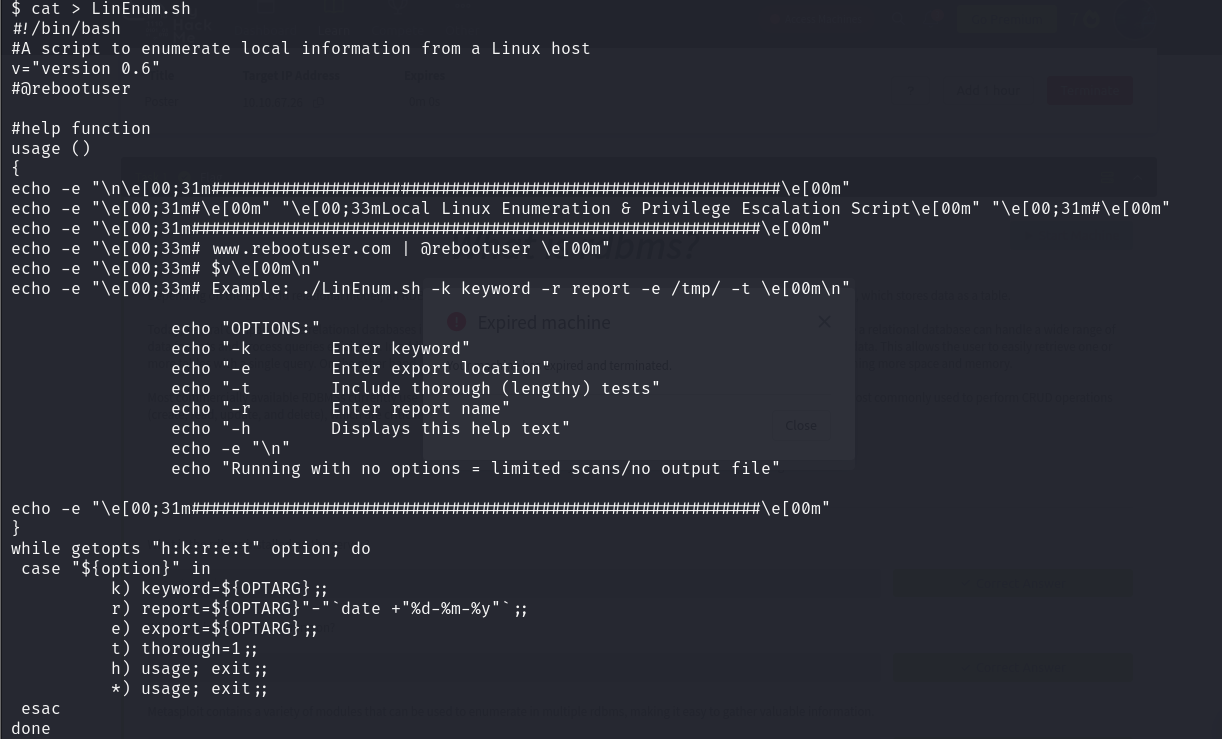


We will now return to dark’s folder and try to find alison’s password using a **bash script.**

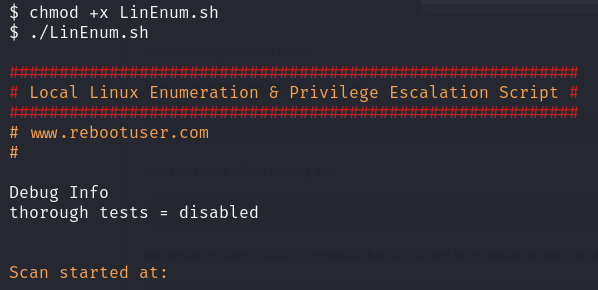
Let’s make a file called **LinEnum.sh** which will get us all the credentials permissions and many more things present on the target machine. It was made by **sneakymonkey** and it is present on github**.**

Our script’s raw file is present on (<https://raw.githubusercontent.com/sneakymonk3y/LinEnum/master/LinEnum.sh>)

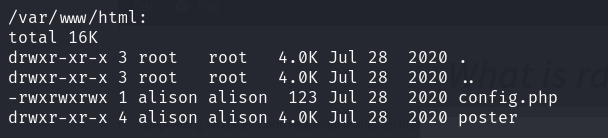
We will copy the raw file and paste it in LinEnum.sh file.



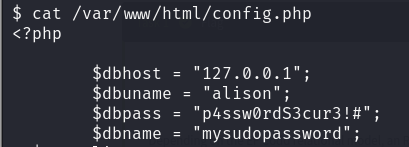
After changing the permissions we will run the bash script.



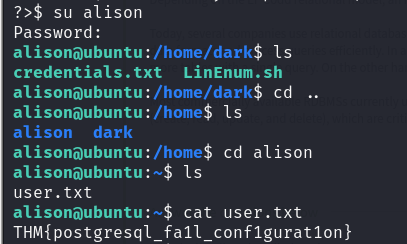
After running this script we get a config file which is **alison’s password.**



We will now cat out the **config.php** file shown above using **cat /var/www/html/config.php**  command.



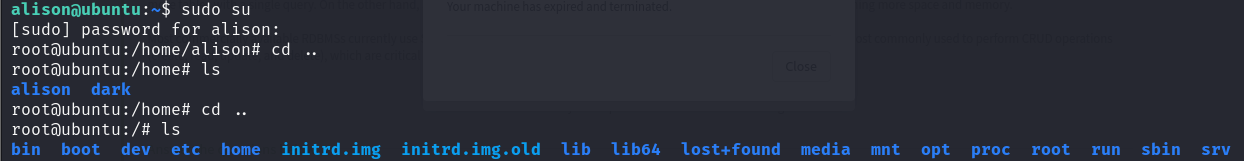
Here we found password of alison and now we will switch user to alison **(su).**



As we already knew where the user.txt file was we directly got our **first flag.**

Our **second flag** is in **root.txt** file which is surely on root’s folder.

We will now try to **sudo su**  alison.



We gained  **root** access and our **second flag** is in root folder .