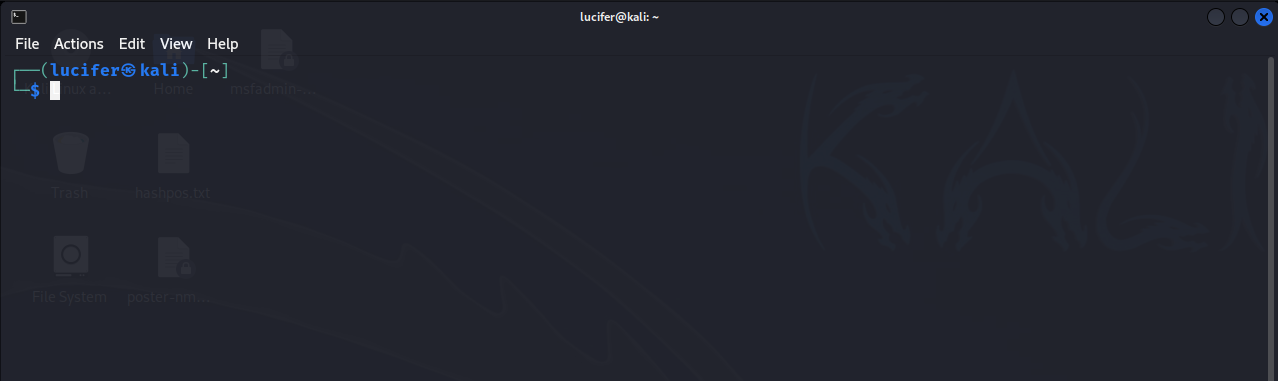
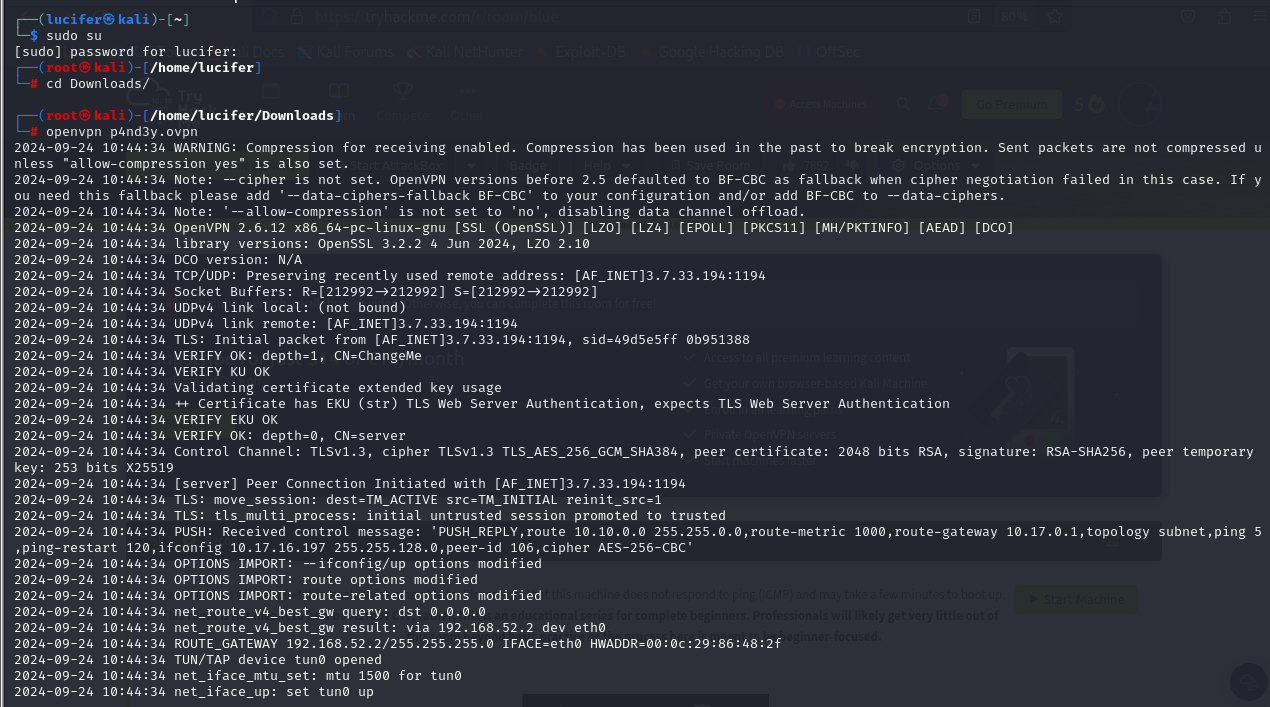
LazyAdmin is a box on tryhackme (<https://tryhackme.com/r/room/lazyadmin> ) created by **MrSeth6797**.

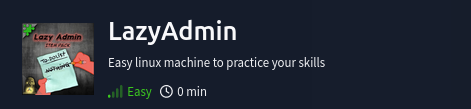
Here our **terminal**  is opened.



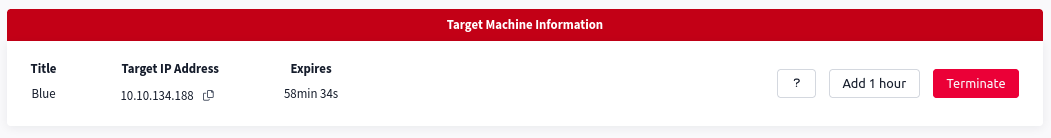
Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.



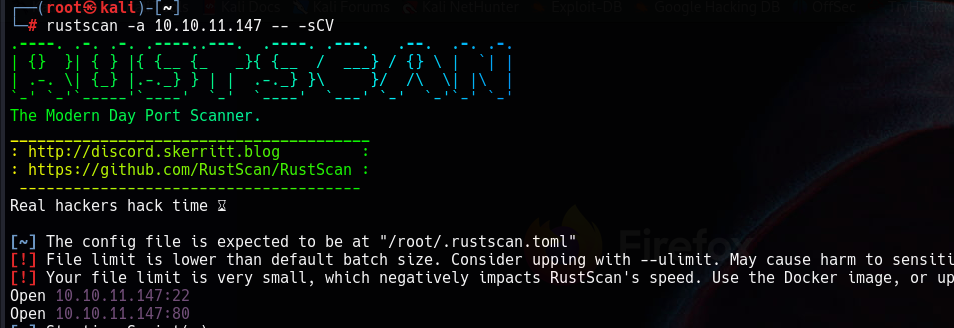
Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

****

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

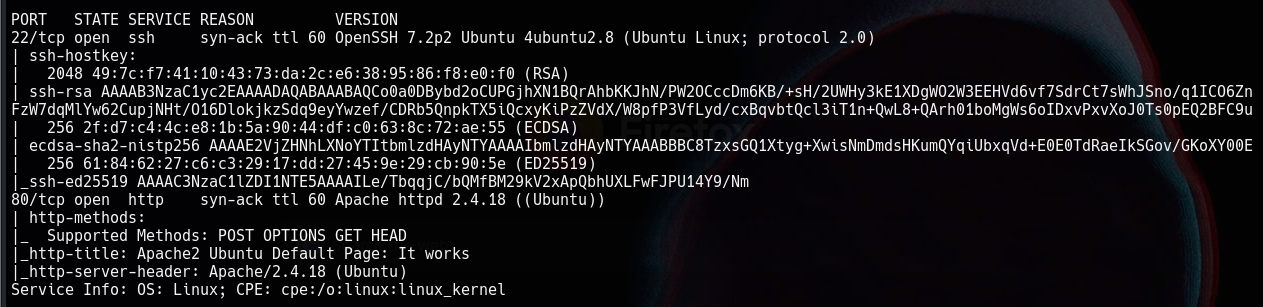


After getting the target ip first thing we’ll do is **rustscan** to see the open ports and more machine’s info.

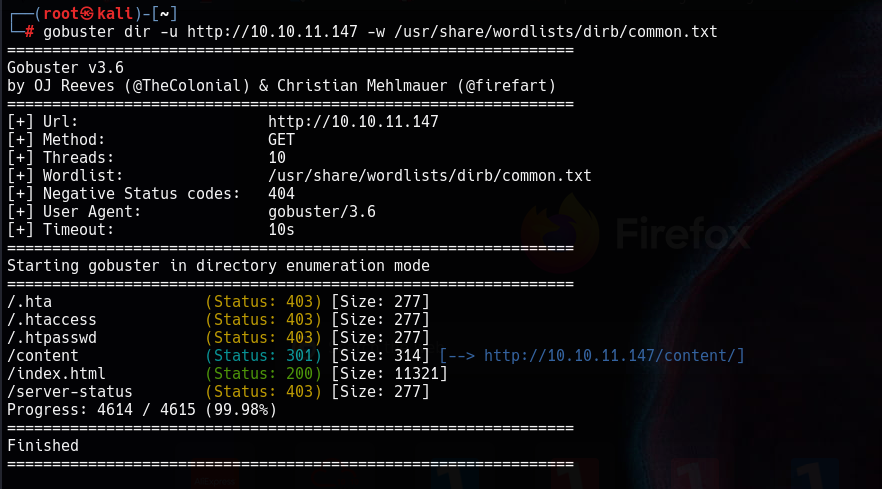


Here I am using **rustscan -a <IP> -- -sCV** to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

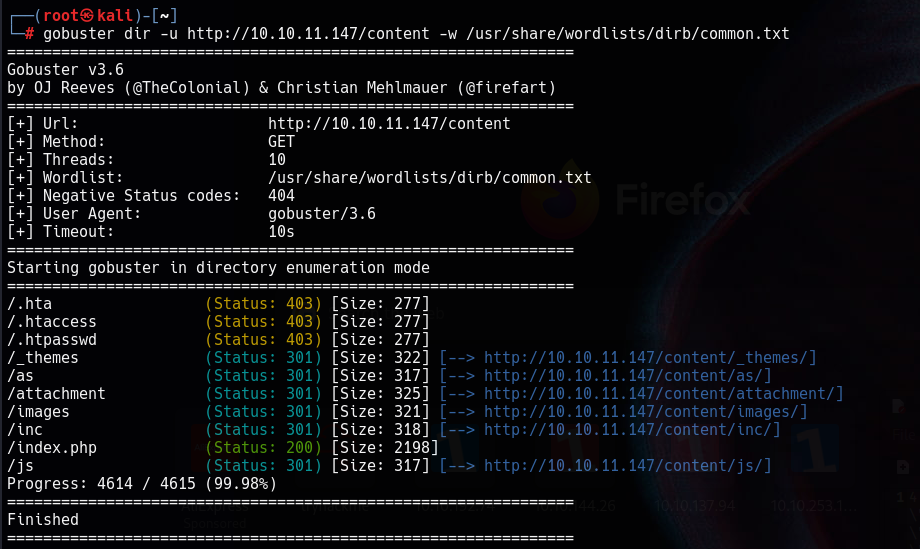
Seems like our scan is completed. Looks like there are total 2 ports open.



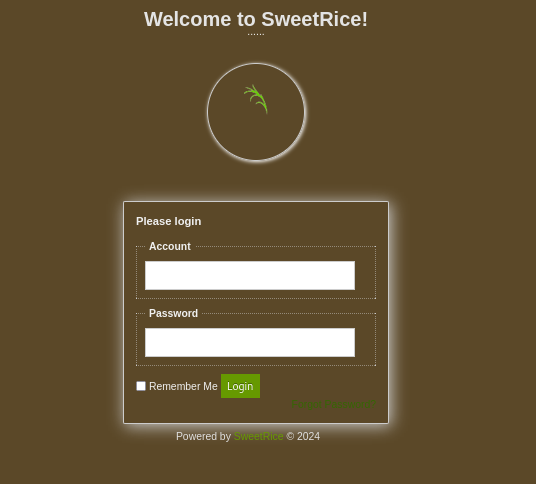
Now we will explore the web server after the directory brute force.



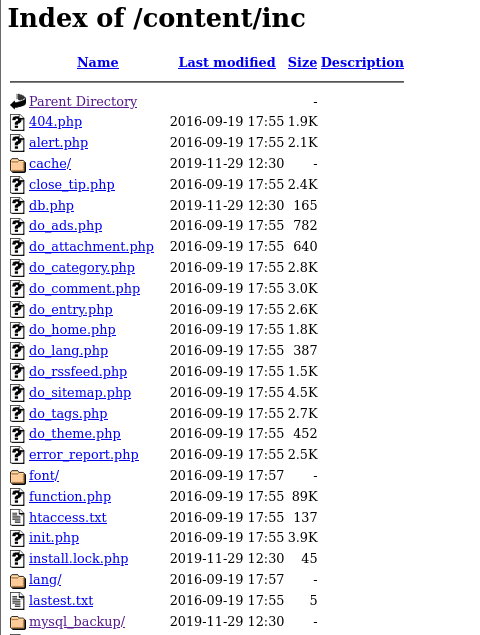
Here **content** directory gives us redirect. We will brute-force it further.



Now we will explore the directories one by one. After further recon we found a sweetrice login page on **/content/as** directory.



On the other hand we found a sql\_backup file which contains the admin username and it’s password hash.

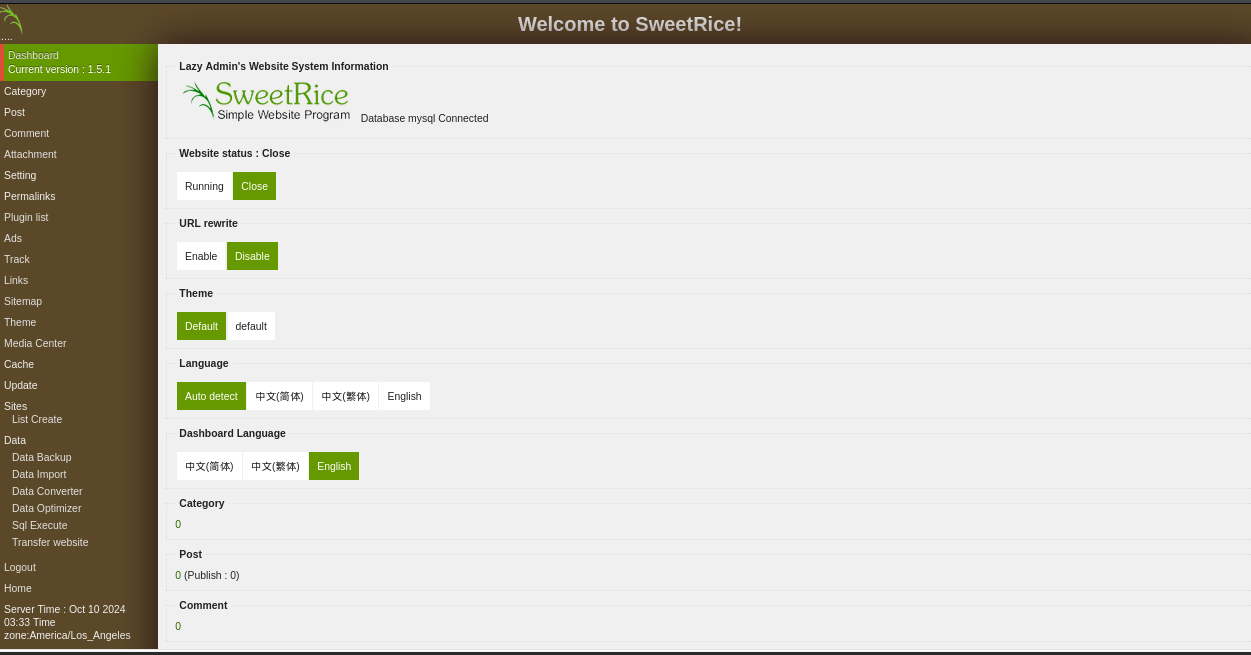


The file contents are something like:

**\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\**

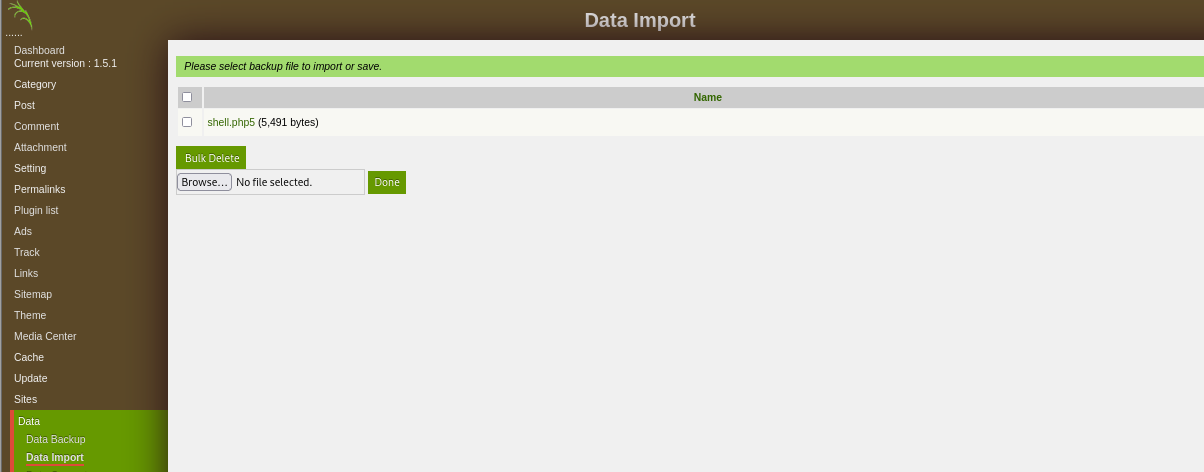
We will decrypt the password and get new password which is **Password123. (manager:Password123)** and try to login on that login page we found previously.

We get a successful login and our dashboard looks like this:

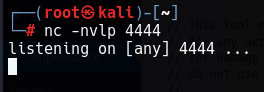


Now we will explore the website and try to exploit it. After further exploration and recon we found that we can upload **php5** files on data import page.

So we will upload a **php reverse shell file by pentestmonkey** and try to get a reverse shell.



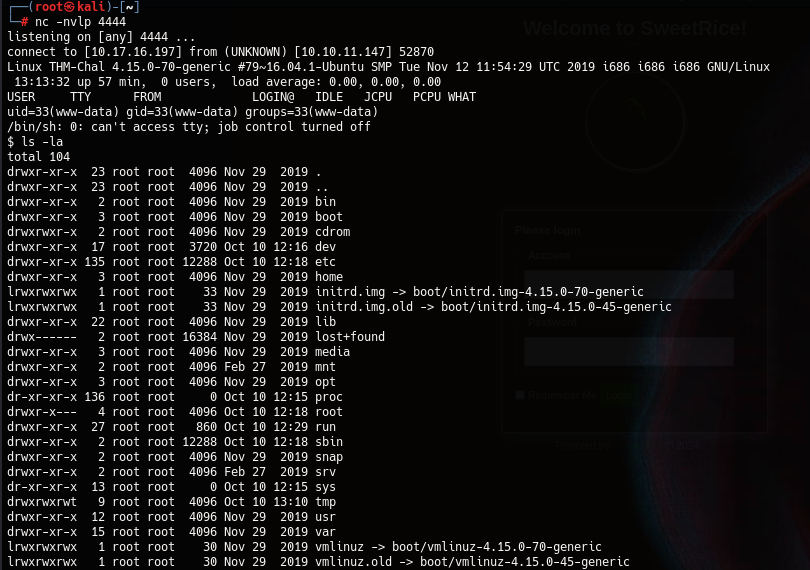
Now we start a listener on our kali machine to get the shell.



And we will reload the link

(<http://10.10.11.147/content/inc/my_sql_backup/shell.php5> )

We got a reverse shell.



Now we will look for the flags. The user.txt flag will be in user’s folder i.e. **/home/user.**

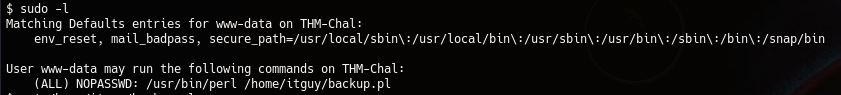
We found a user **itguy**  and it contains the first flag.



Now our next flag will be in root folder but we don’t have access to root folder.

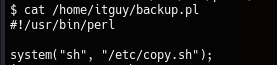
We need to escalate our privileges to get root.

We will run **sudo -l**  to see the processes run by sudoers and what we have got.



Here we can see that there is a perl process running which has root access and it has both read-write access to the user.

We can see the **/home/itguy/backup.pl** file.



We can see another directory here **(/etc/copy.sh).**

It’s a bash file and we can edit it because user has the permission to both read-write.

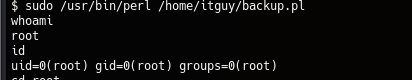
We will go to the /etc directory and use the following command to edit the copy.sh file:



Now we can see that our new copy.sh file contains **/bin/bash** which will help us gain root.

Now we will run the full process which we have already seen in the sudo -l output i.e.

**sudo /usr/bin/perl /home/itguy/backup.pl** and it’ll give us root.



Now we can get our second flag from the root folder.

