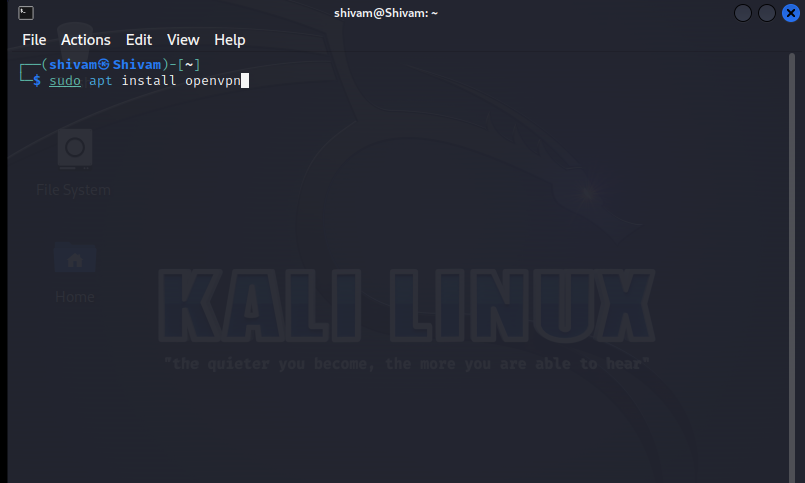
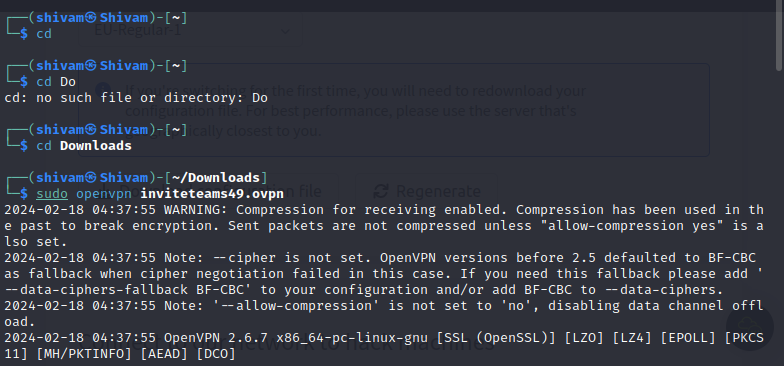
**Pen testing in ColddBox.**

After Starting the Machine of Colddbox (TryHackMe Website) from Kali Linux, we have to install openvpn for Kali Linux if it wasn’t already present. From Colddbox, go to read vpn access> download configuration and run terminal and run below mentioned commands present on screenshot

*Sudo apt install openvpn.*

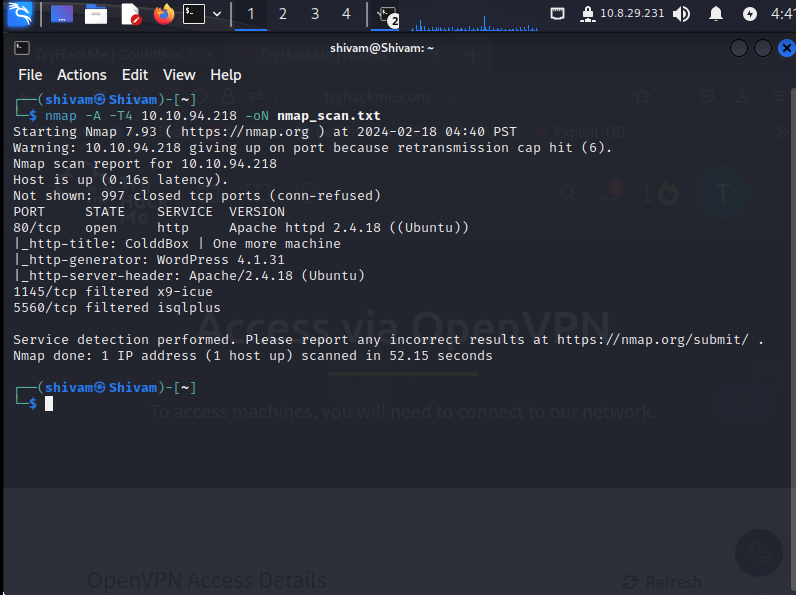
Download Configuration file and run *sudo openvpn username.ovpn*



After getting the IP address, begin the enumeration part.

**Enumeration:**

I used **nmap** to get the open port and the version of service running on that port.



*Nmap –A –T4 <ip address> -oN nmap\_scan.txt*

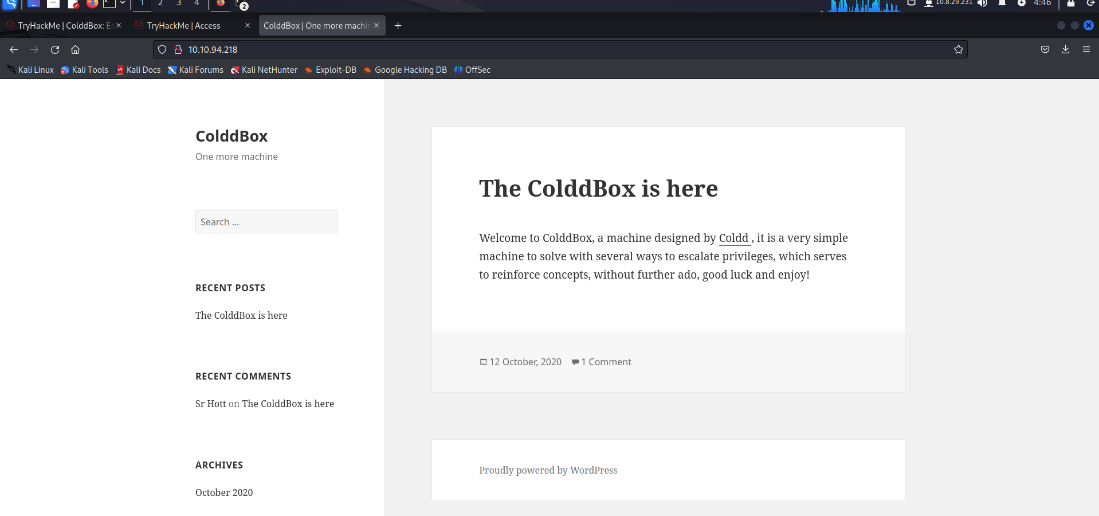
From this nmap scan, I found there are three open ports.

Port: 80/tcp | Service: http | Version: Apache httpd 2.4.18

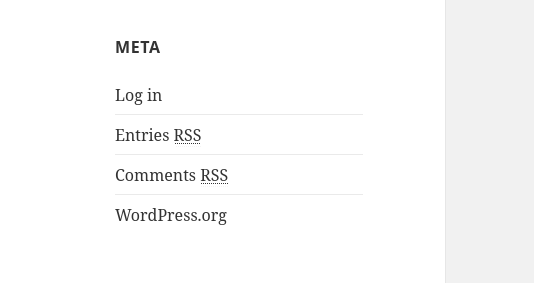
Port 1145/tcp| Service: x9-icue

Port: 5560/tcp| Service: isqlplus

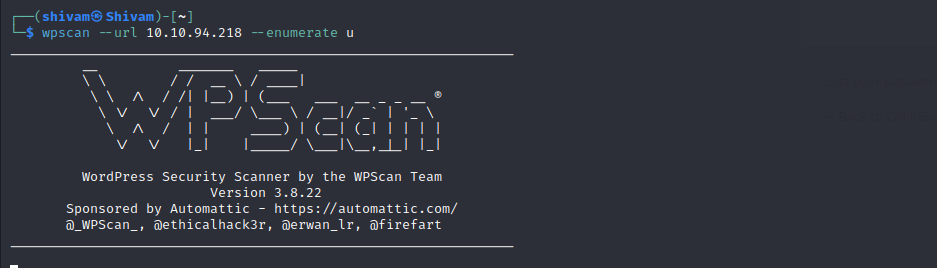
From this scan result I identified port 80 is opened then it really works with the browser. And I enter the target IP into the browser.



At the bottom of this page it has a login link



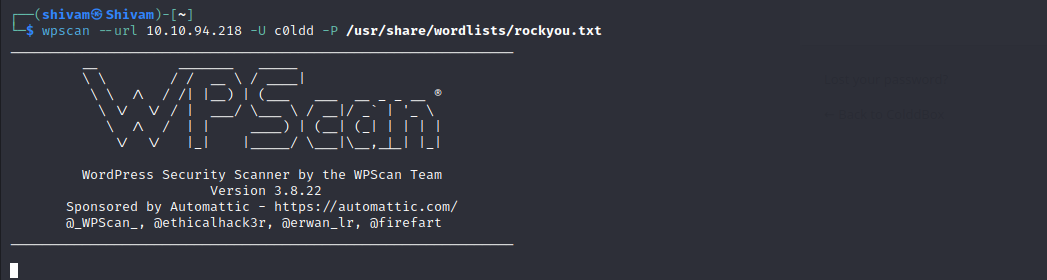
After clicking that link it redirects to the wordpress login screen. So, I used wpscan tool to enumerate the wordpress login user.



*Wpscan –url <ip-address> --enumerate u*



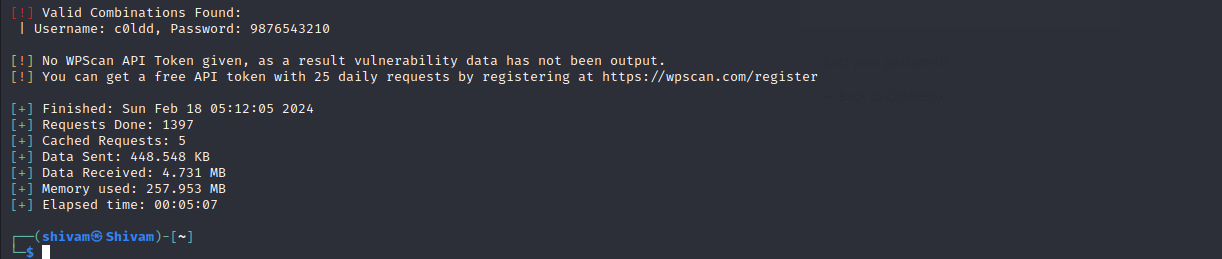
I chose the **c0ldd** username because the name of the machine is also similar to this. After choosing the username we use wpscan tool to get the password of the user



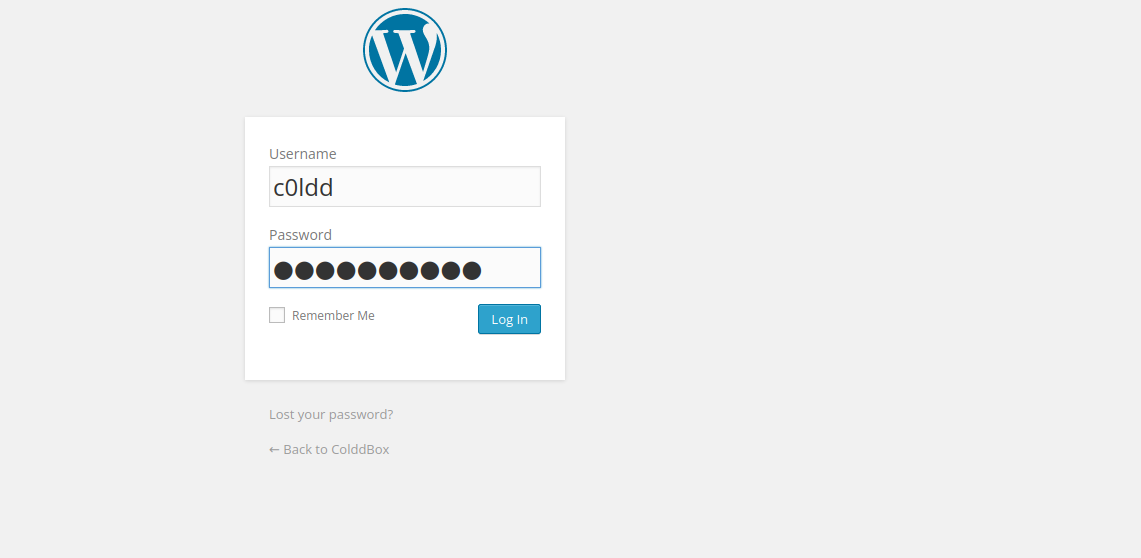
*Wpscan –url <ip-address> -U c0ldd –P /usr/share/wordlists/rockyou.txt*

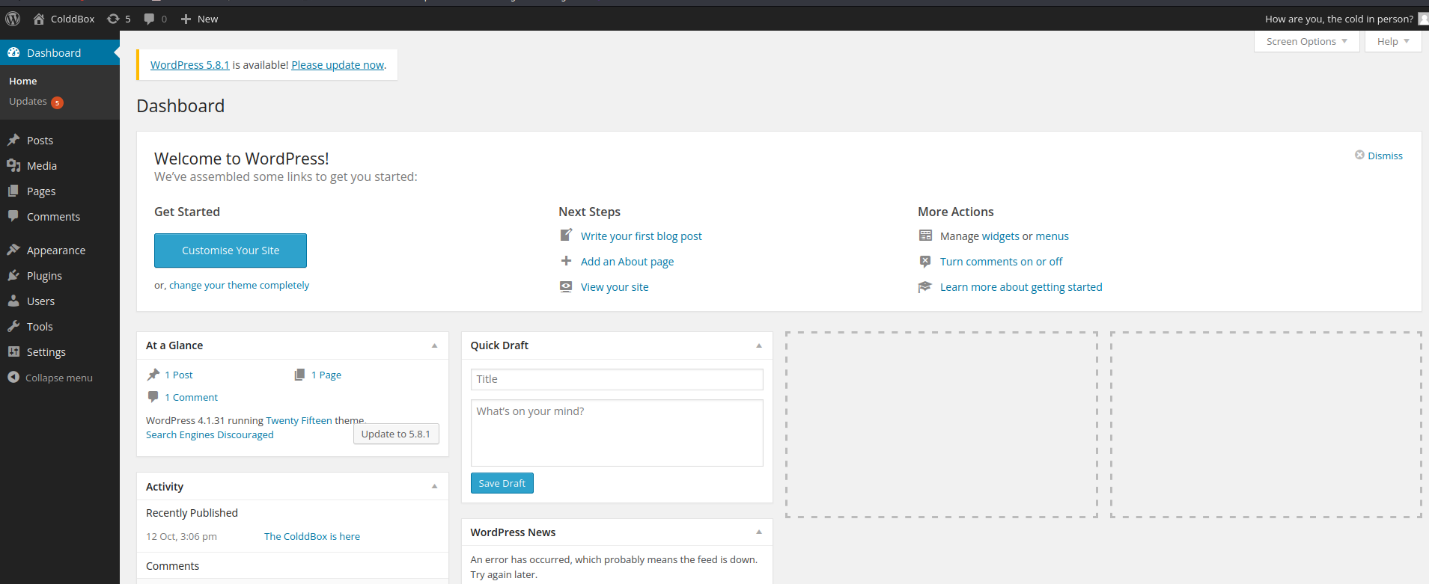
If rockyou zip is not unzip, kindly unzip it.

By this command I got the valid password of this user: Password is - 9876543210

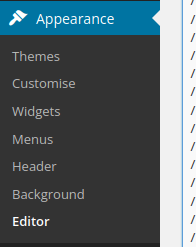


Now using this username and password I log in to WordPress admin dashboard.

Now I am in admin dashboard



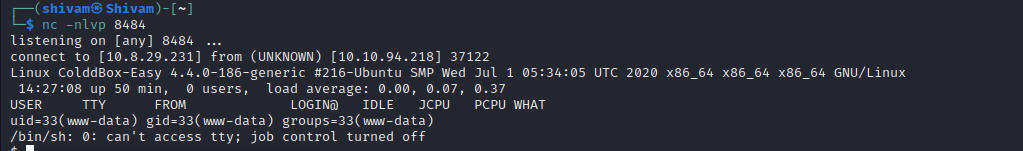
Uploading a Reverse Shell - We can add a reverse shell by modifying the header.php



I will be using the php-reverse-shell by the pentestmonkey. This is the GitHub repo for that. I copy pasted the content of reverse-shell.php to header.php in WordPress. For getting the reverse-shell I have to change the IP and Port



After changing this I open my Terminal and used Netcat tool.

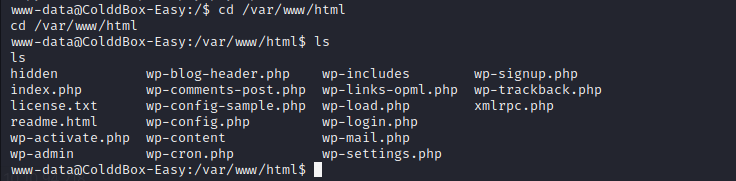


While listening to the port we have to revisit the Target-IP on browser. Now we get a shell in our terminal.

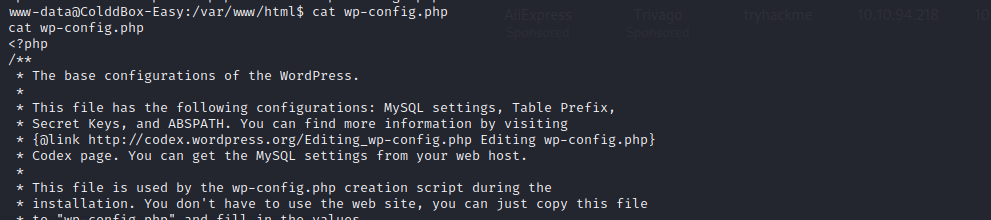
Now I opened the python spawned shell. Using this command to it:

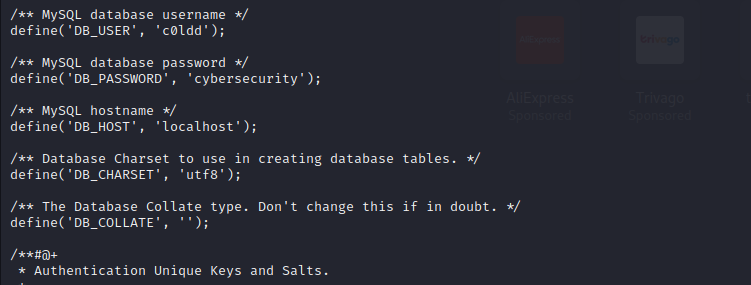


Now here we can see php files. The most important one is the wp-config.php file because it contains the user name and password for the database.

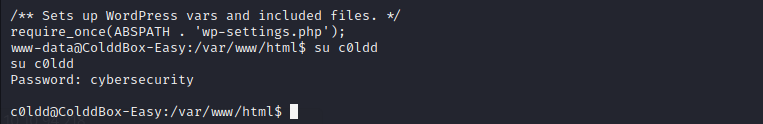


I used cat to see the content of wp-config.php file

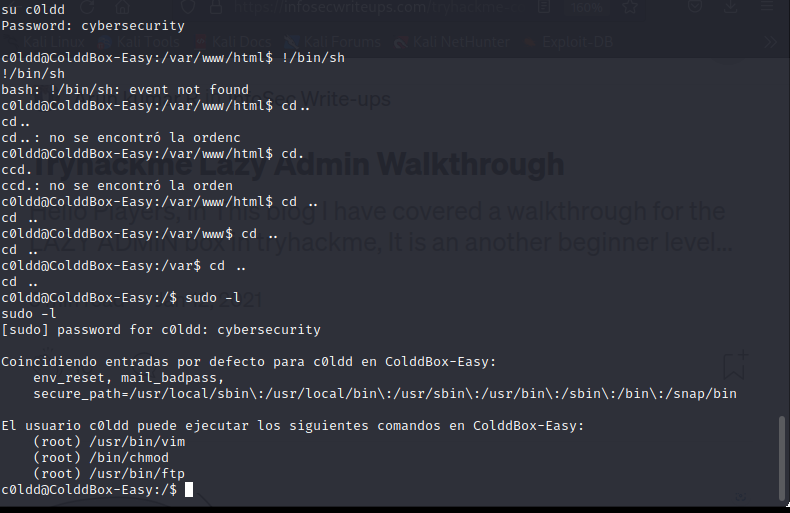
From this file I obtained the credentials:



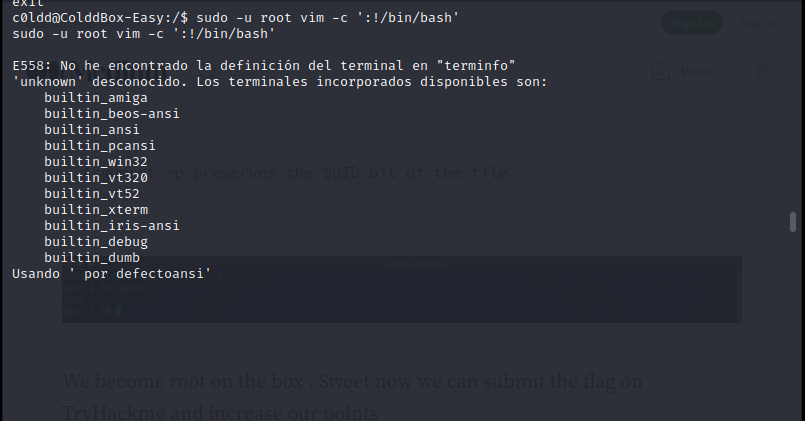
Now I used this credentials to login the account:

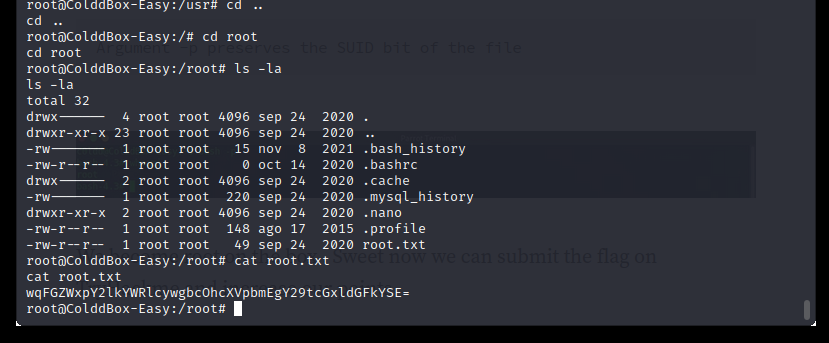


So, now I’m in the c0ldd account. But I didn’t get root privileges. Now I perform the ls command to know what are the files in there.



By above screenshot attached command enter to the root privileges.





Got the root.txt file for colddbox, submit the code as it is.

Now type

cd ..

cd Home

Cat user.txt file

And wohoo everything works well.

Thanks,

Shivam Roy.