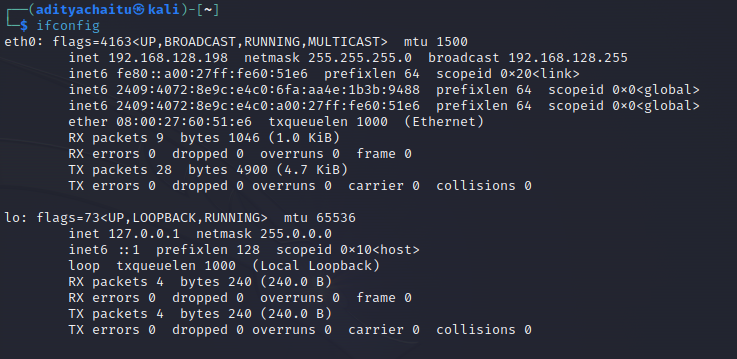
**CORIZO**

**Minor Project: Cold Box Easy**

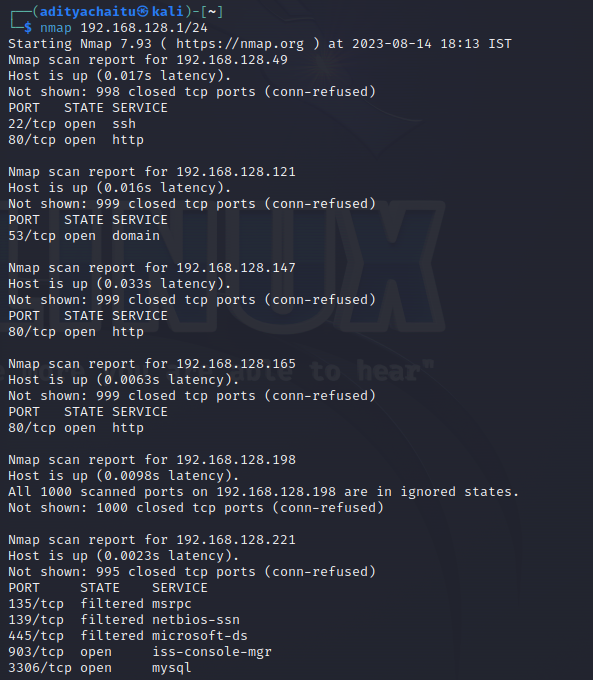
First Download the cold box from vulnweb.

Then setup the VM with network = “bridged” and usb port 1.1 version.

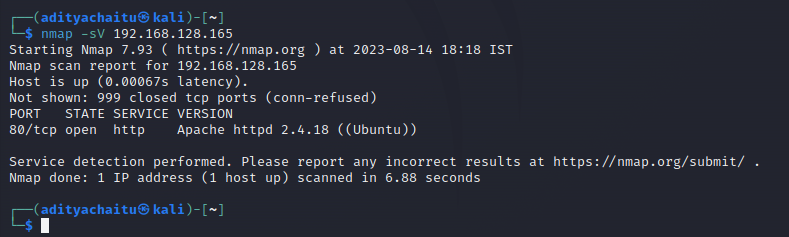
Do Ifconfig to find your IP.



Scan with nmap to find the IP of the target machine i.e Coldbox.

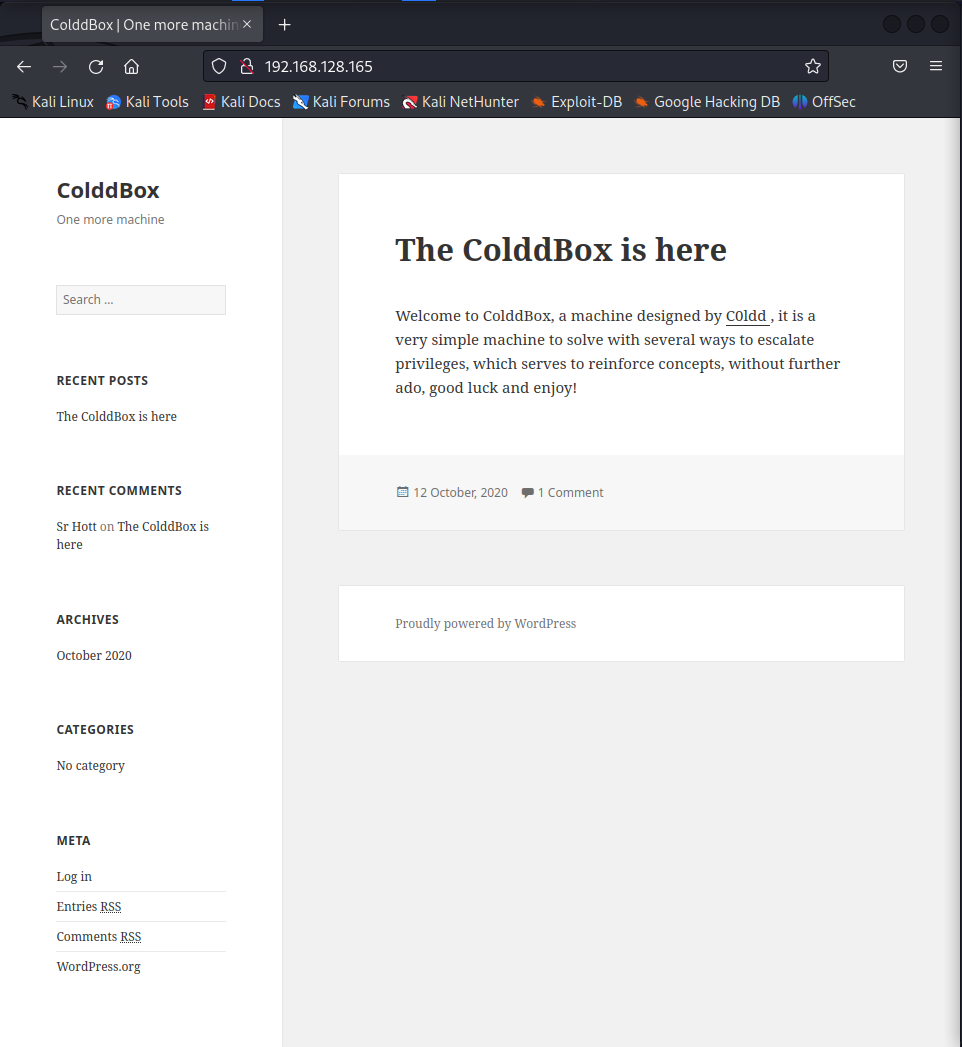


Now Do the port scanning on the targeted machine.



We find that there is Apache httpd is running on port 80. That mean there is a web server running the system.

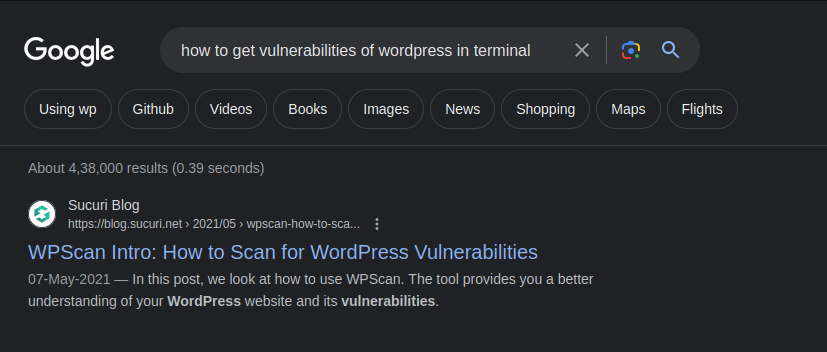
Now open web browser and enter target IP.



You find a web page with colddBox name.

And you can see that the server is running a service named Wordpress.

Now scan for the vulnerabilities that can be found on wordpress.



You can find that there is a scanning tool for the wordpress. Go on and install wpscan in your system by using following commands in terminal.

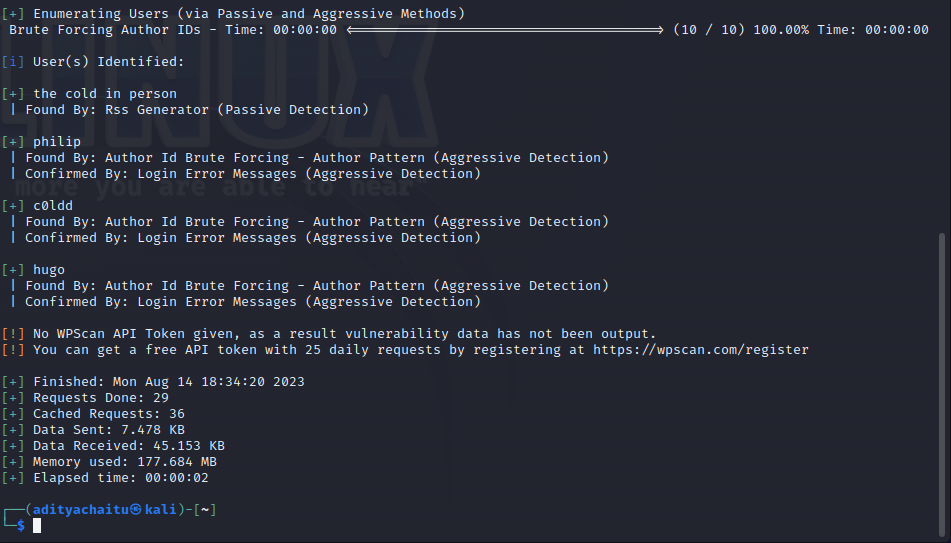


Once you install type “wpscan –help” to find the options we can use.



Now try to find the valid users of the server by using the option “–enumerate u”

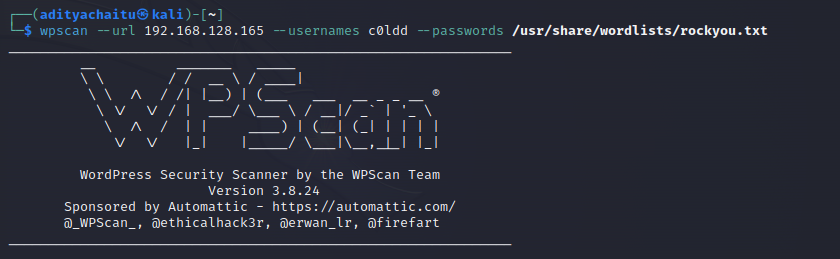


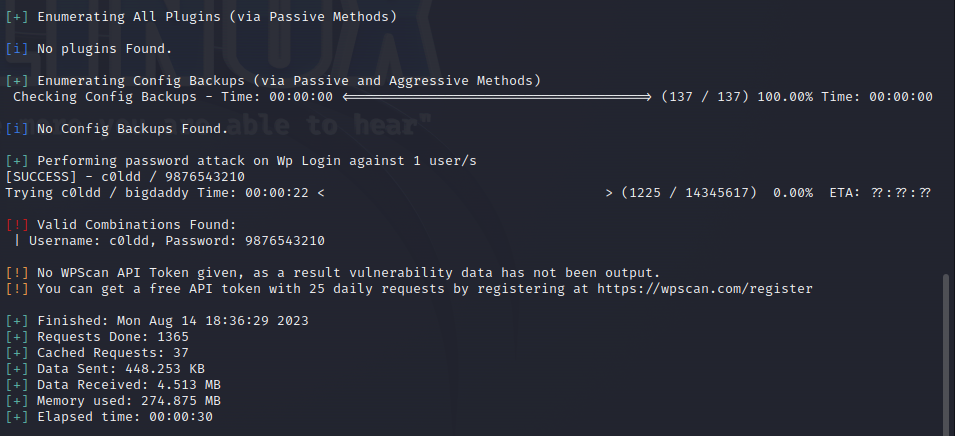


In the above screenshot you can find the valid users of the website.

As we see the website is having user c0ldd in it, we can go ahead with the user “c0ldd”.

Now we are brute forcing the password by using the inbuilt wordlist file in the “/usr/share/wordlists” named “rockyou.txt”. ( This consists of most of the commonly used passwords)

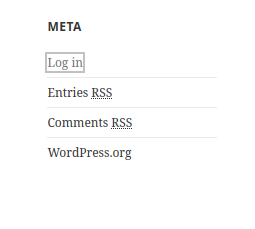


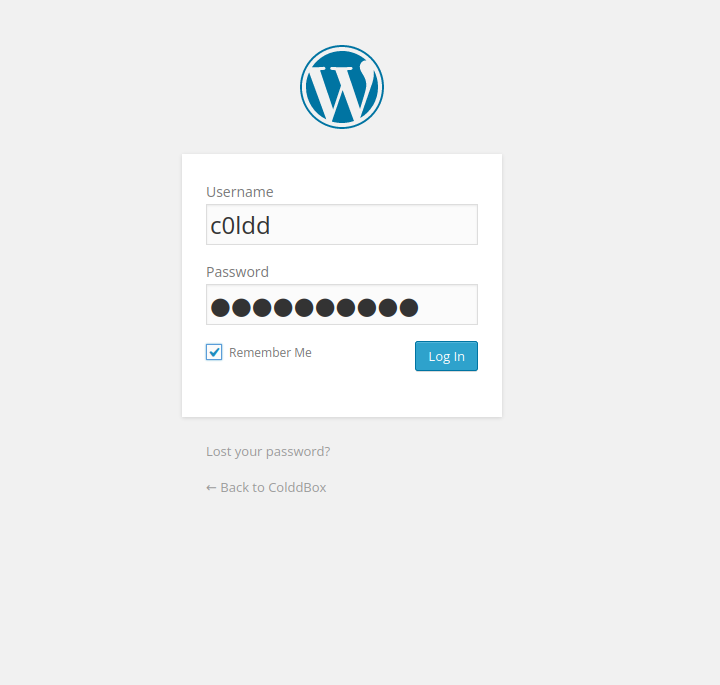


You can see that there is a “Valid Combination Found”.

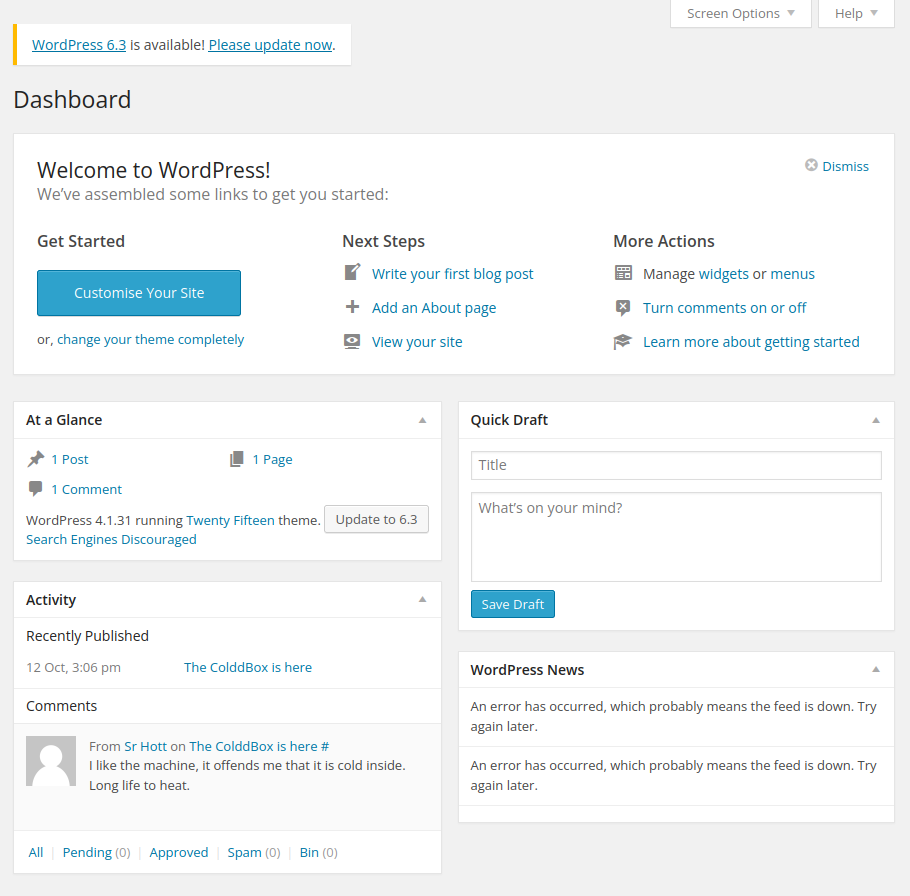
With username = c0ldd and password = 9876543210

Now go back to the website and login with the c0ldd user from login.

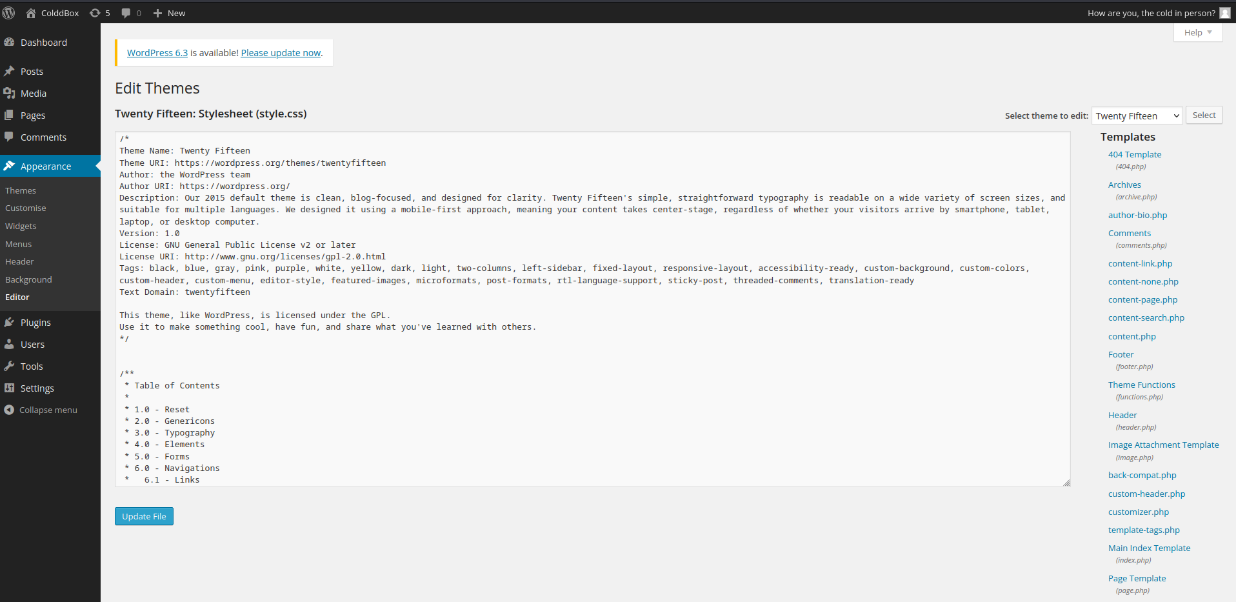




Now you will get the administrator access to the server and now you can see the following dashboard.



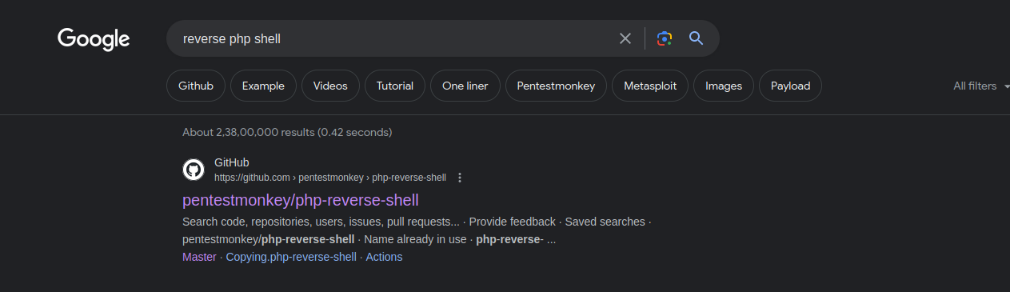
In the “appearance” section you can find “editor” option, click on that.



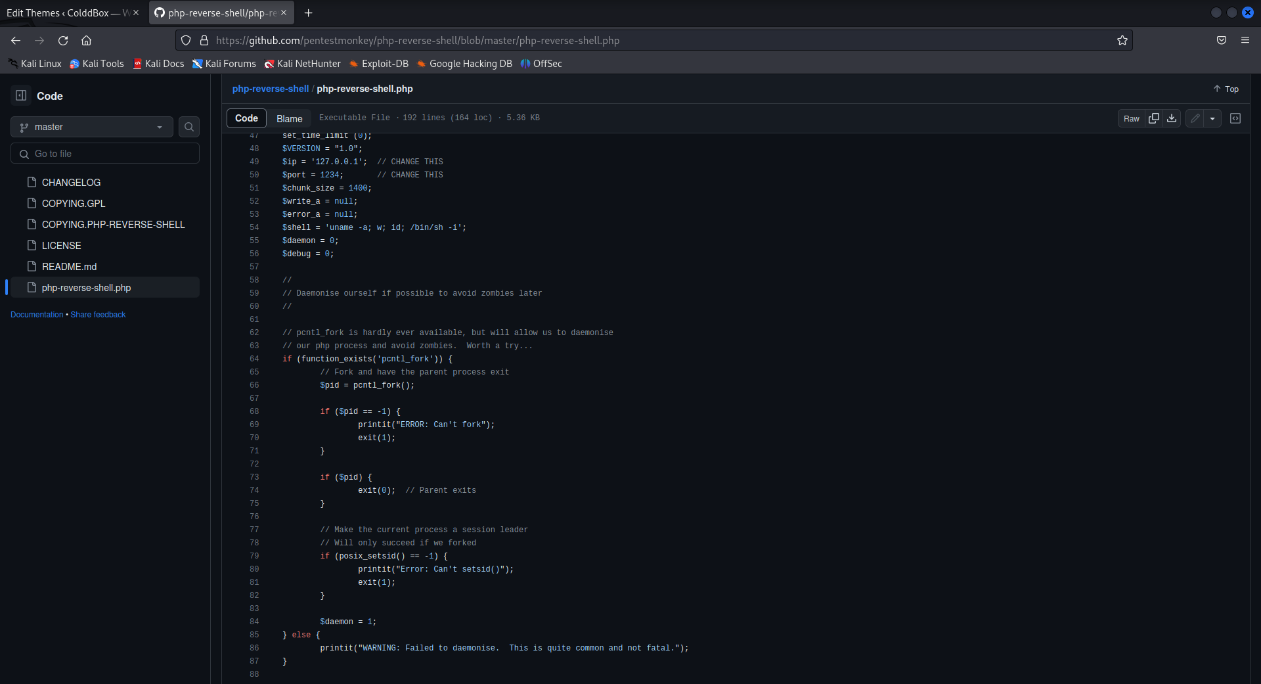
You can find different files that you can edit as you are the administrator.

At this rate you can find header.php file in the Templates with can be edited.

As we can edit this we can use “php reverse shell” technique to get the shell access.

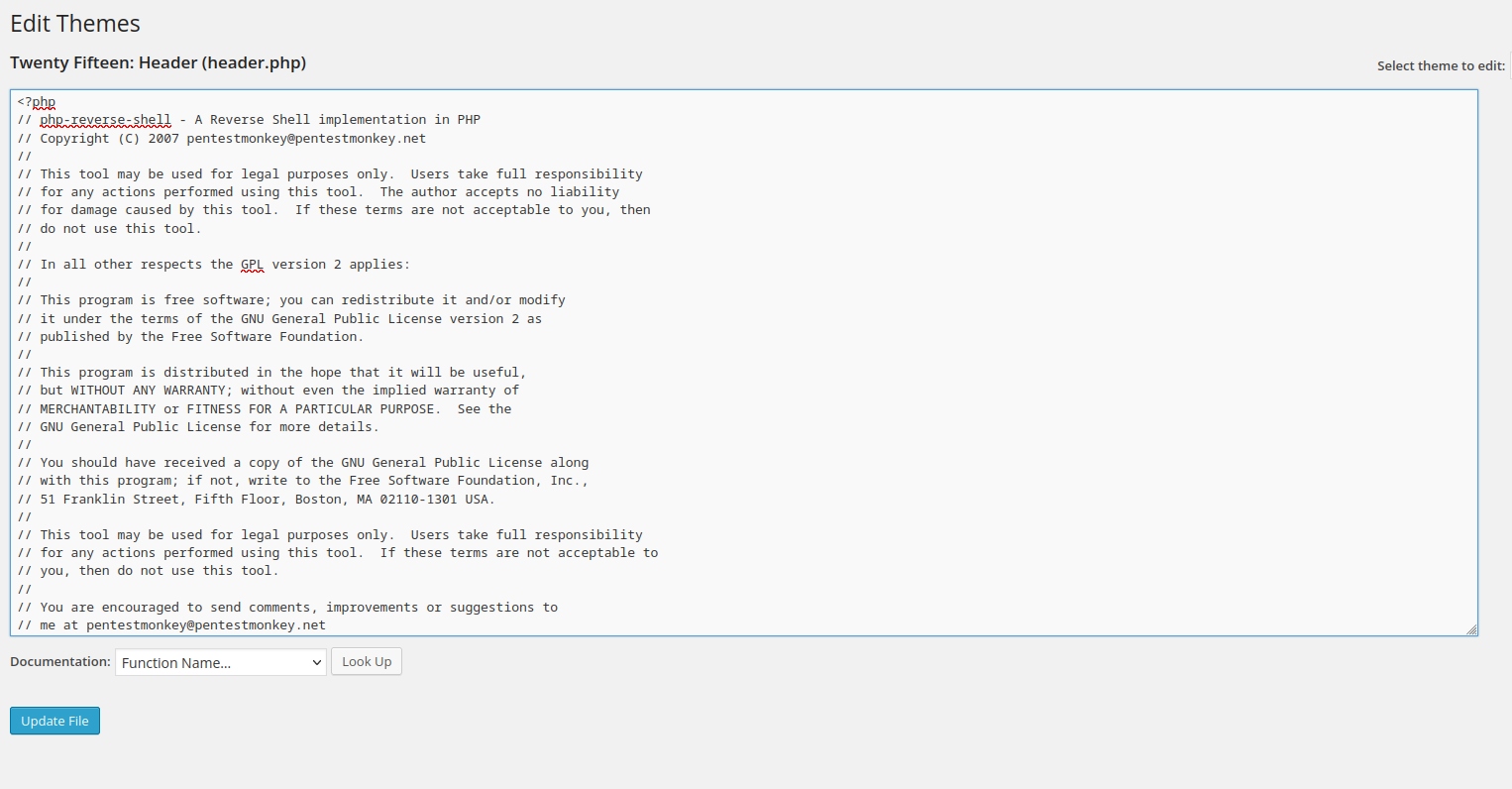


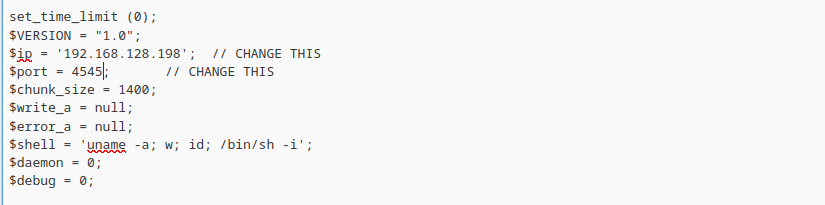
You can search for the php reverse shell so you can find the script.



Copy and paste the php script there in the header.php.

And change the Ip address in the php script to your IP address and port number of your choice that is not currently on use.





I used 4545 port.

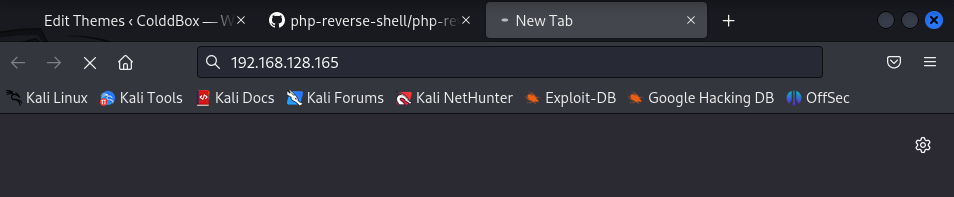
Now update the file by clicking the update file at the bottom.

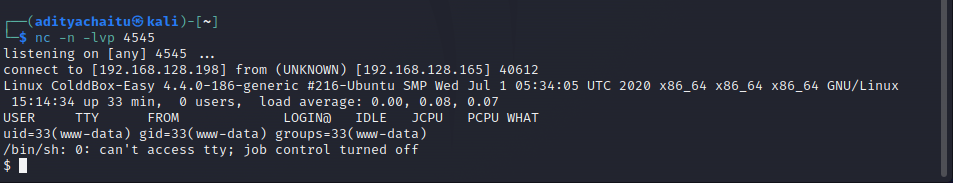
Now open your terminal and type the command “nc -n -lvp 4545”

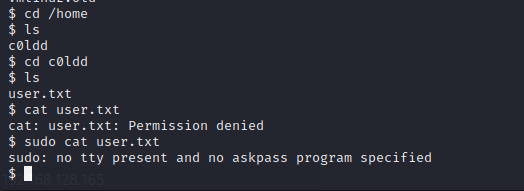
This mean we are listening the input from the 4545 port.



And now go to the browser and type the target IP address, now a connection will be established from the port 4545 now you are inside the target systems bash.

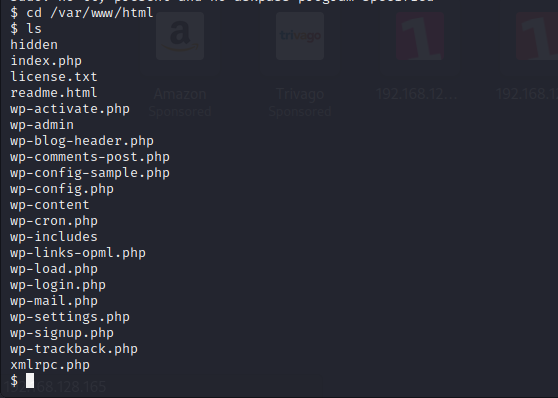






Now I went to “/home/c0ldd” to check for any leads and found a user.txt which cannot be read as it has no access other than “c0ldd” and “root”.

So now I went to “/var/www/html” as it is the place for websites and everything that works on port 80 in linux.



You can find the above files in the specified locations.

And the important one of the above files is “wp-config.php” it contains the information about the users.

I used “cat” command to show the data in the file.

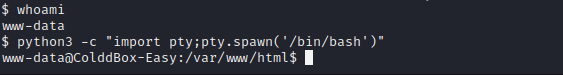


And in the above we can find the DB\_USER and DB\_PASSWORD i.e we got the user password.

We got the password but we need the terminal to enter the c0ldd user.

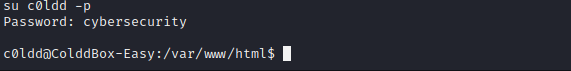
I got that there is python running on the system.

Using python we can gain the pseudo access of the terminal by using pty library.

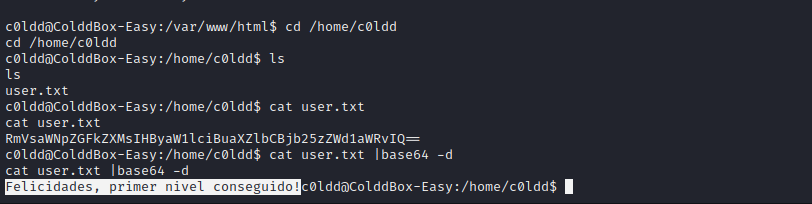


Now use su c0ldd -p command to login to the c0ldd user as we know the password from the above type the password and login.

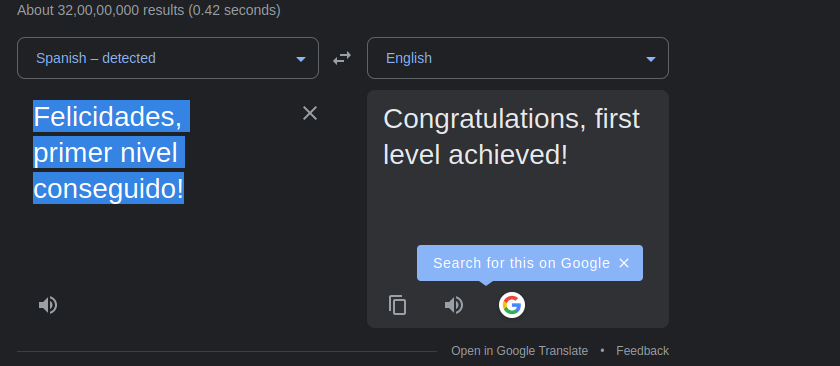


Now you gain the access of the c0ldd

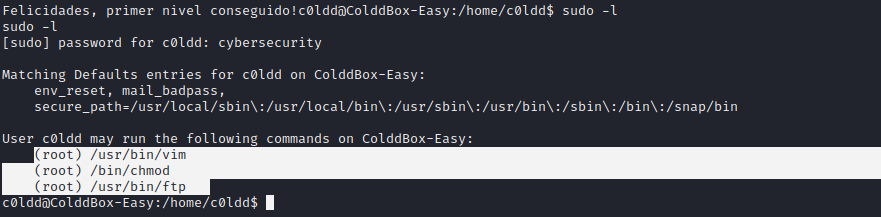
Go to the “/home/c0ldd” and use “cat user.txt | base64 -d” as we get the encrypted form if we do not use base64 decryption.



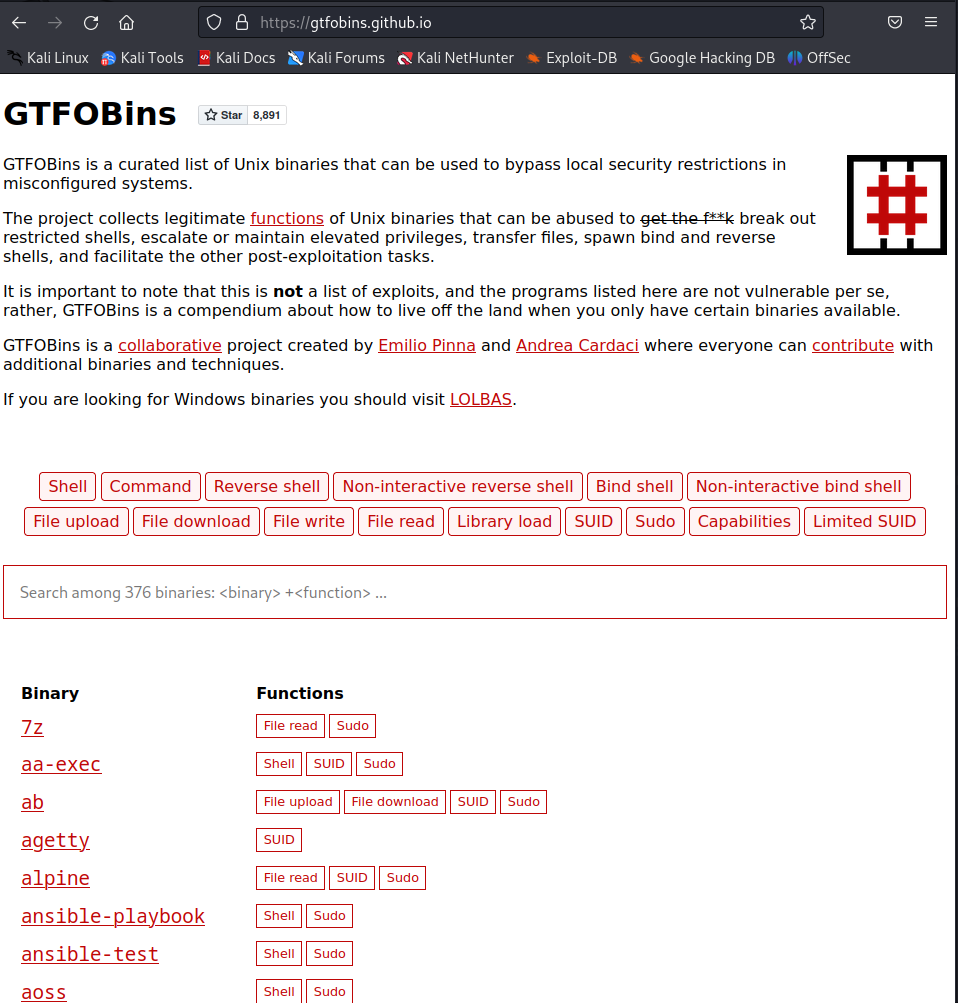
Use google translator to get the meaning.



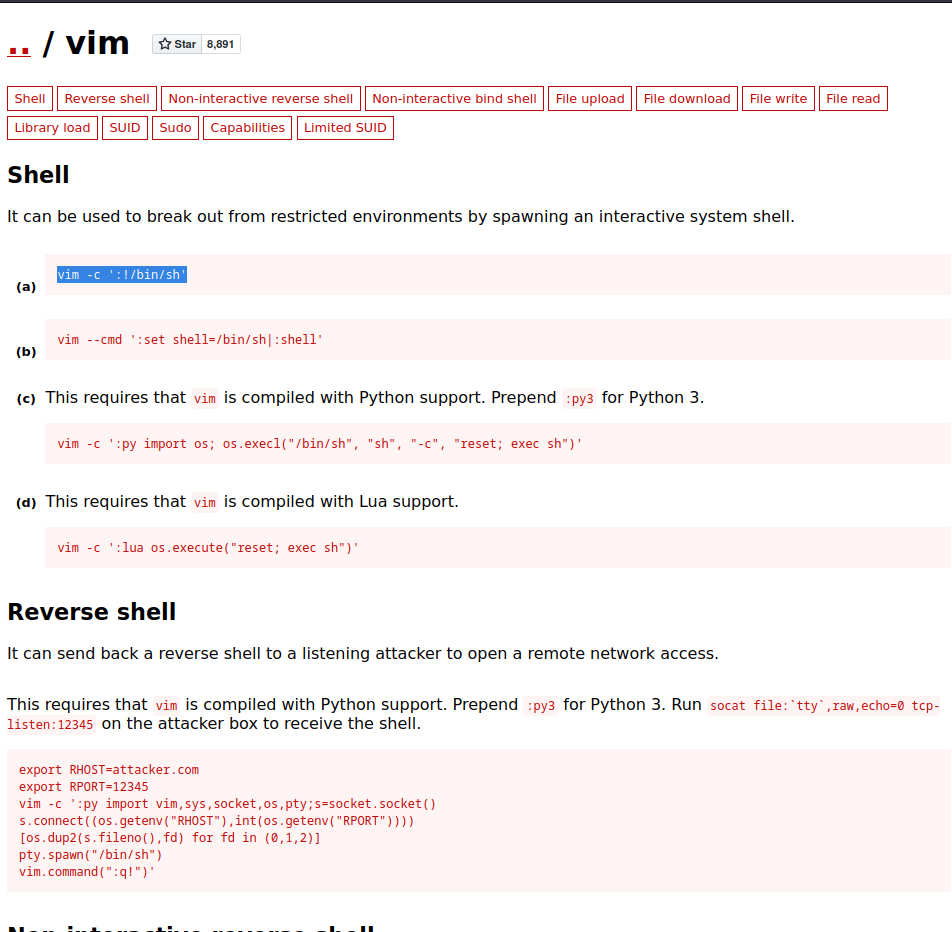
Now Gaining the root access of the machine, the c0ldd user do not have the root privileges but you can find that it has root privileges for some of the applications.



Go to the website “gtfobins” where you can find different local bypasses possible using different applications.

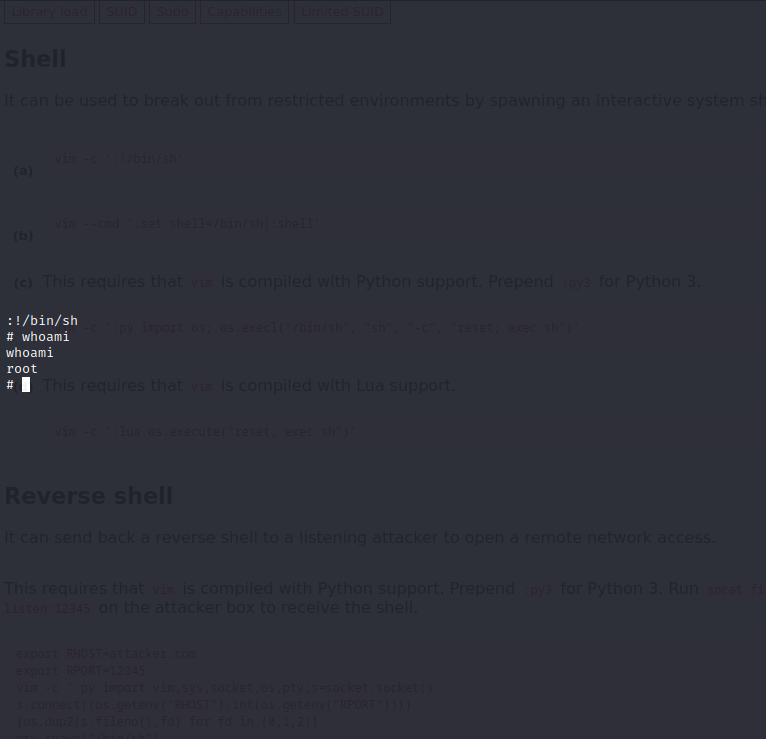


I choose “vim” to bypass into the root.

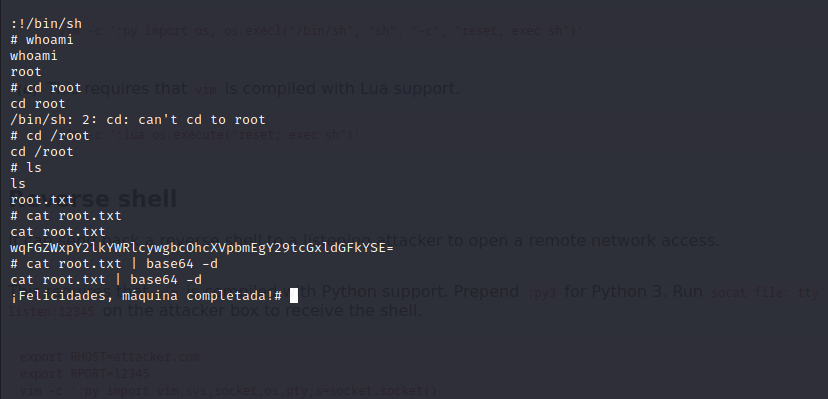


Now use the command “ sudo vim -c ‘:!/bin/sh’ “.

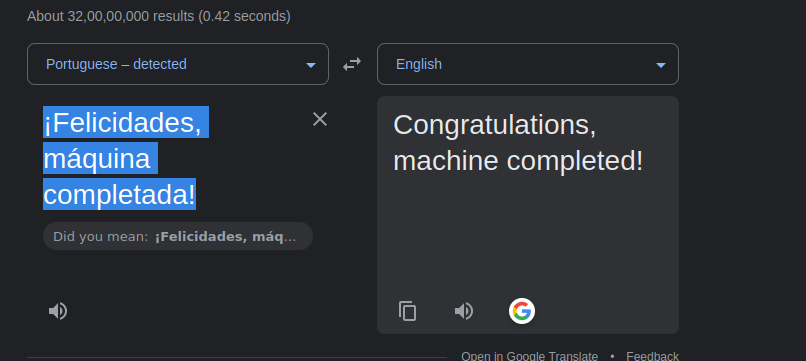
Now you got the root access.



Now you can goto “/root” where you can find “root.txt”.



Use Google Translator again.



Now the machine is done.

MITIGATIONS:

The password policy should prevent using too common and easy to guess passwords.

First do not use the web services like “wordpress”.

Misconfigurations with the SUID bit should be avoided.

Maintain a firewall.

Do not give the root privileges of unwanted applications to other users.