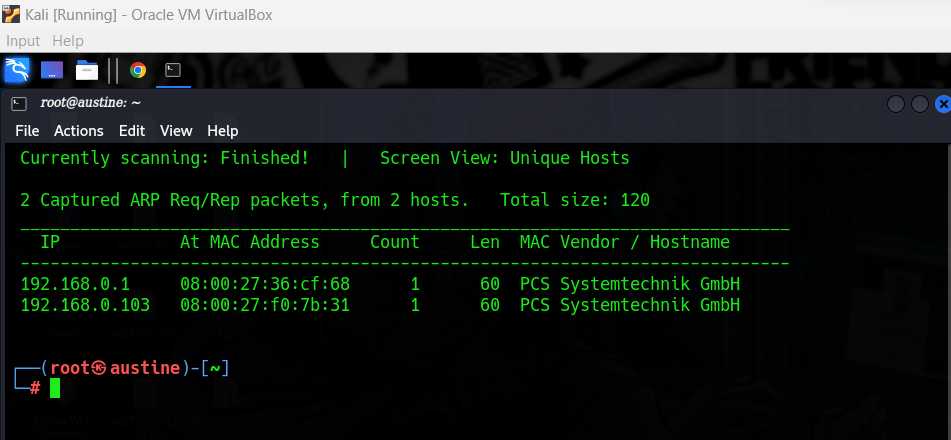
**ICA 1 (THE SECRET PROJECT) VULNHUB BREAKDOWN**

In very few steps, we will dive into unfolding the secret project found in the root directory of this Vuln Hub.

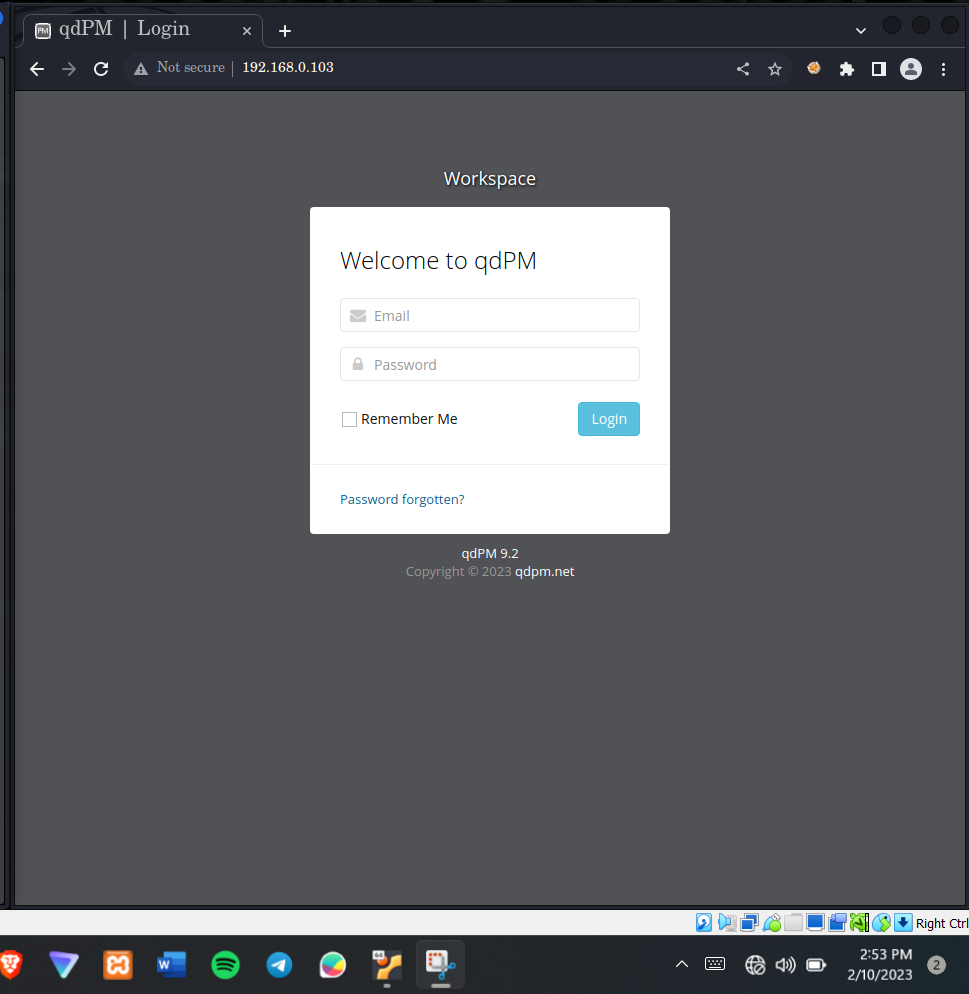
**Step 1: Using netdiscover to find the networks in our interface.**

Our target machine has an IP of 192.168.0.103

****

**Step 2: Navigating to the IP address of our server. 192.168.0.103**

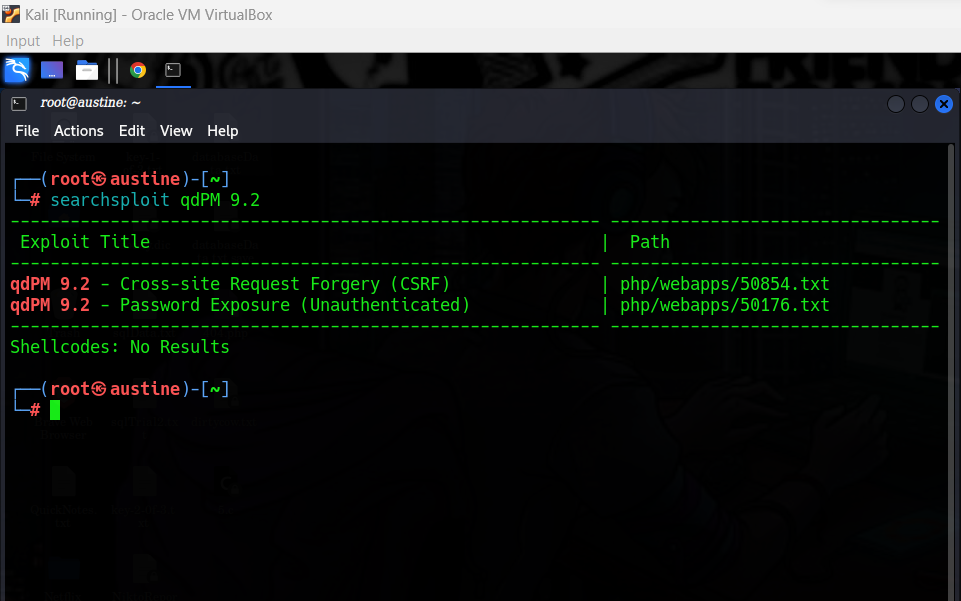
We get this page below. However, we don’t know the username or the password. Thus, we try to see if we can find an exploit for the **qdPM 9.2**

****

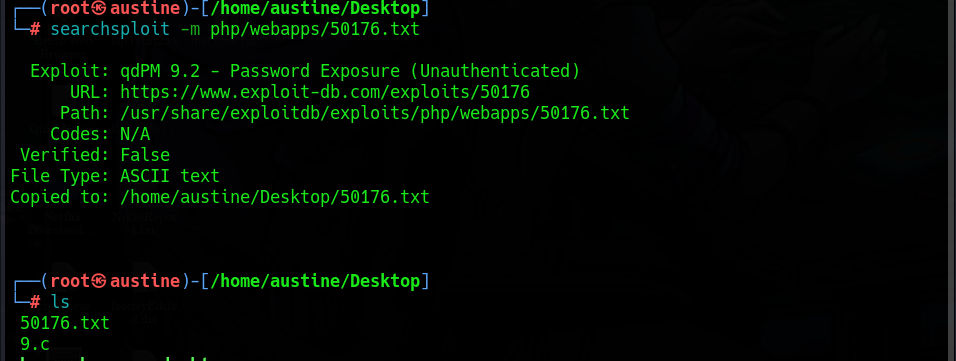
**Step 3: Using searchsploit we find that qdPM 9.2 has an exploit.**

Command: **searchsploit qdPM 9.2**

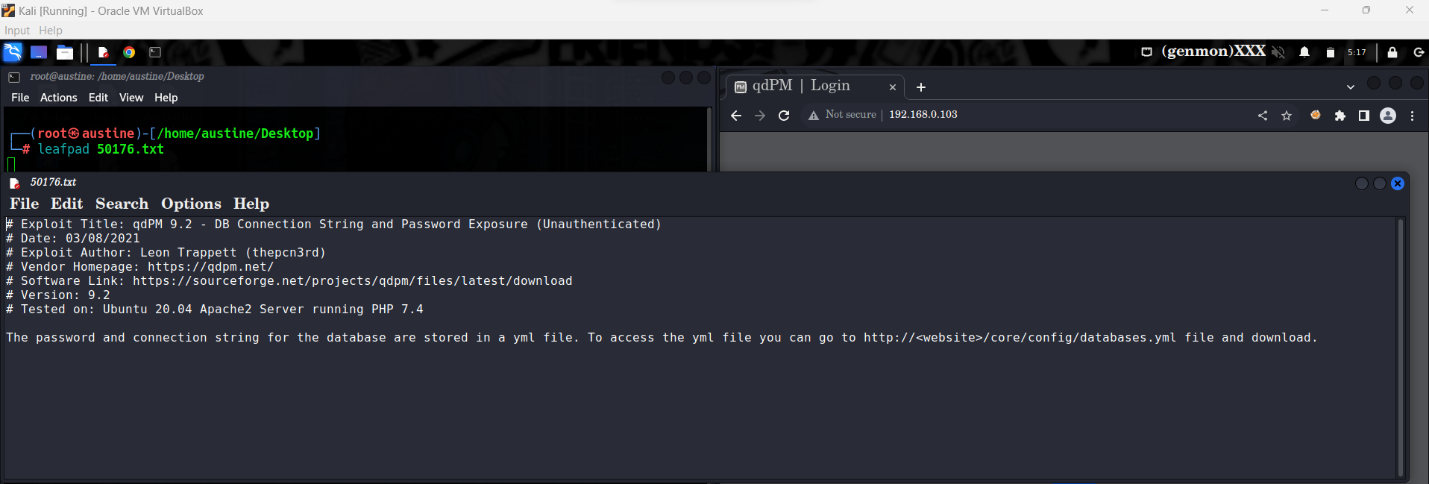
There are two exploits available. In this tutorial we shall use the password Exposure exploit

****

**Step 4:** Mirroring the exploit into our desired directory (Desktop in this case)

Command: searchsploit -m php/webapps/50176.txt

Using leafpad, to view the content of 50176.txt



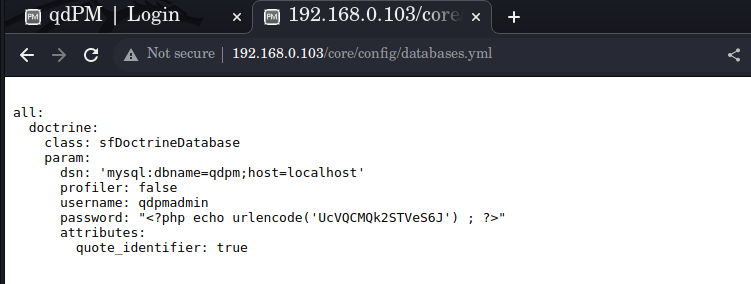
**Step 5 : Navigating to the URL found on the 50176.txt**

****

We have the username and the password

Email : [qdpmadmin@localhost.com](mailto:qdpmadmin@localhost.com)

Password **: UcVQCMQk25TVe56J**

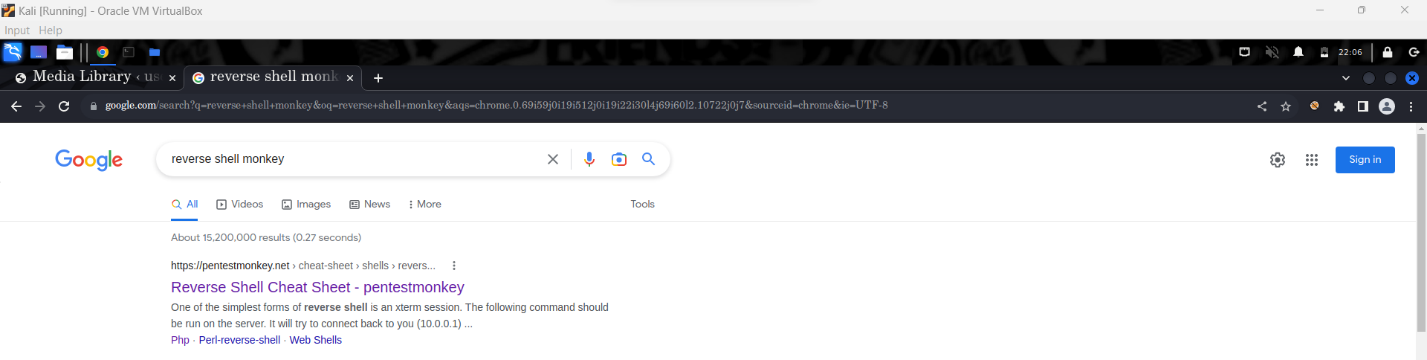


**Step 6: Adding a new user**

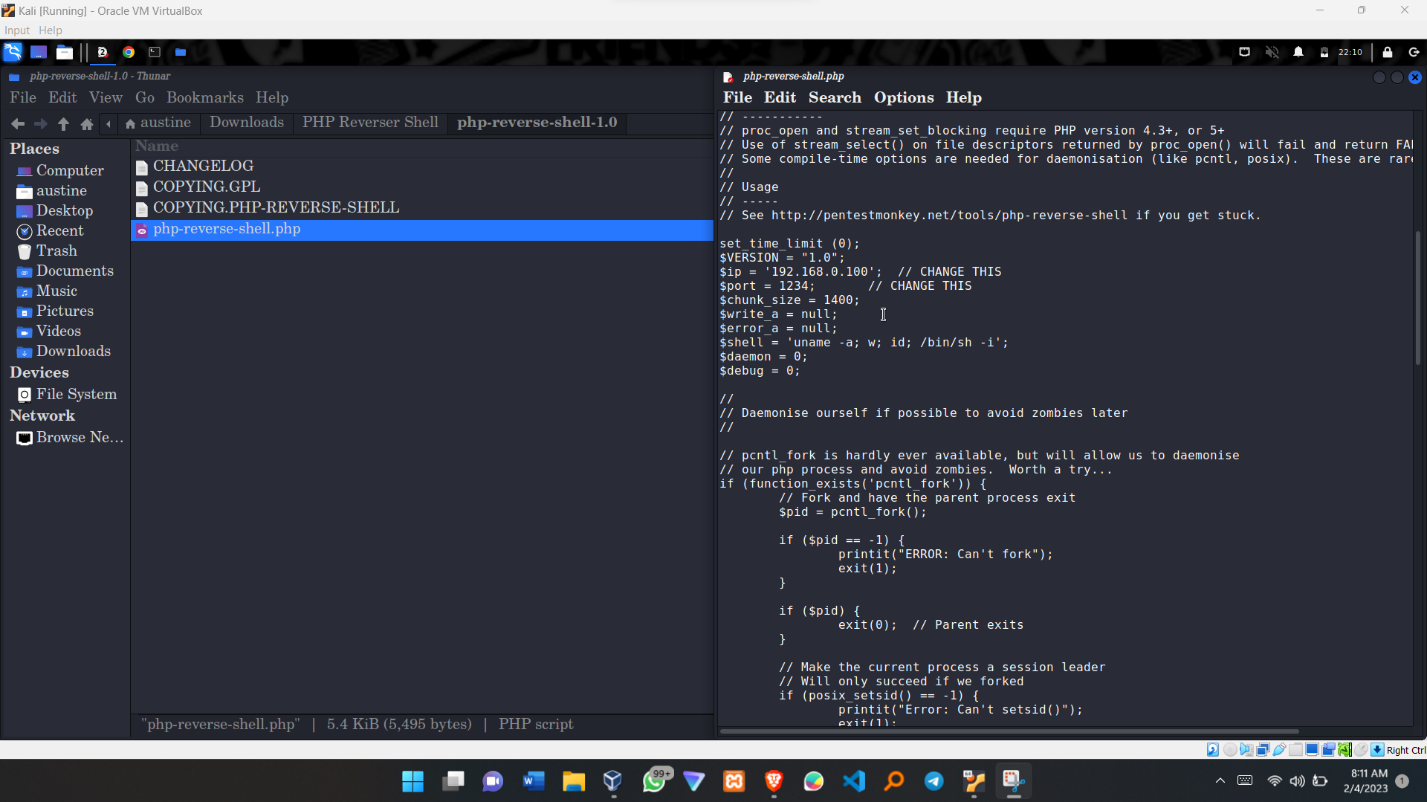
Navigate back to the <http://192.168.0.103> enter the above username and password, then once you login, navigate to Add user and add a new user with your desired email and password.

**Step 7: Login with the newly created user and navigate to Project > Add Project**

In the attachment section, its where we will attach our php reverse shell file.

Download the reverse shell from google, 

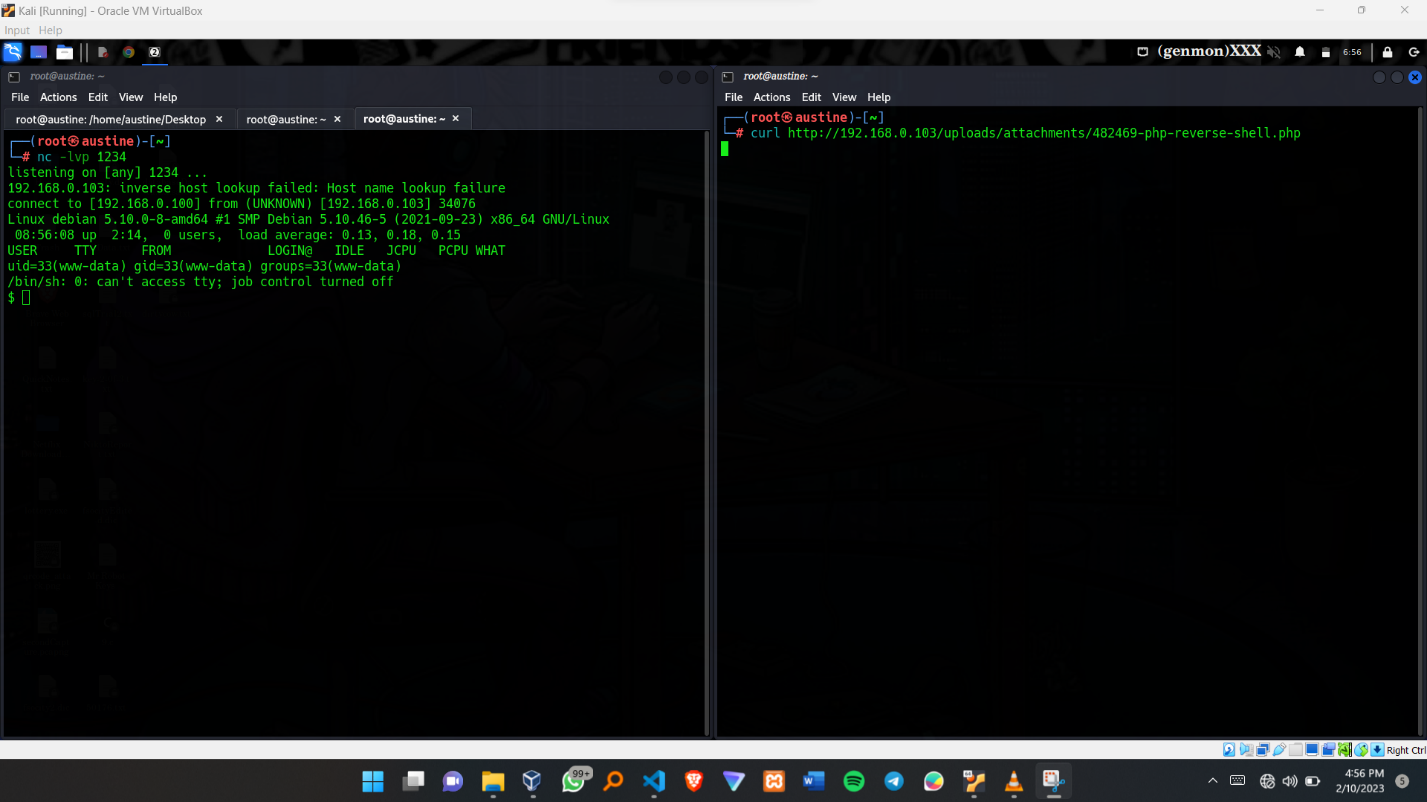
Open The file and change the IP (The Ip address of your attacking computer) and the port number of your choice.



Finally, upload this file as an attachment in the newly created project.

**Step 8: Setting up a listener using netcat**

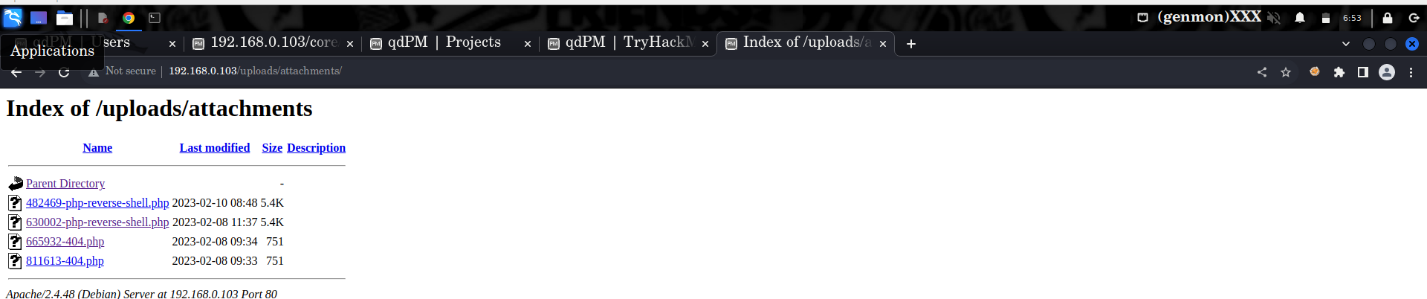
Command**: nc -lvp 1234**



Additionally you can curl the URL from the code in the picture above or navigate to step 9 below and click one of the reverse shell created. NB: Make sure your listener is running and listening with the same port number as the one in the reverse shell php file.

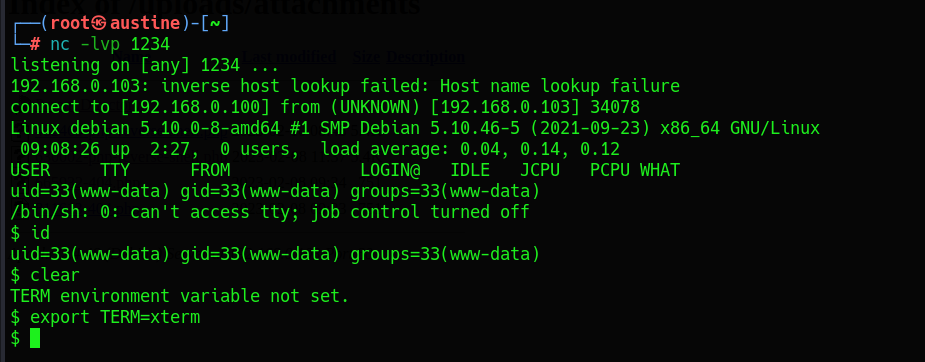
**Step 9: Navigate to this URL to get the attachments.**

**URL: http://192.168.0.103/uploads/attachments/**

The use of command: **nikto -h 192.168.0.103** can come in handy to discover the various subdirectories in the server.

**Step 10: We are inside the system!!!!**

However, we are logged into as (www-data). Also, the terminal we get is not fully interactive and thus we setup a good working environment. Command: **export TERM=xterm**

****

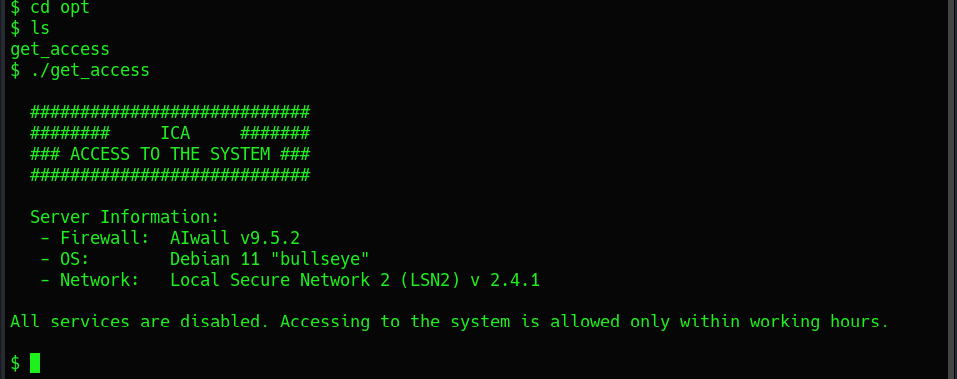
**Step 11: We navigate into the opt directory.**

**NB:** To keep this tutorial short, I went straight to the point where I was able to be successful, however, I navigated to various directories in search for anything valuable

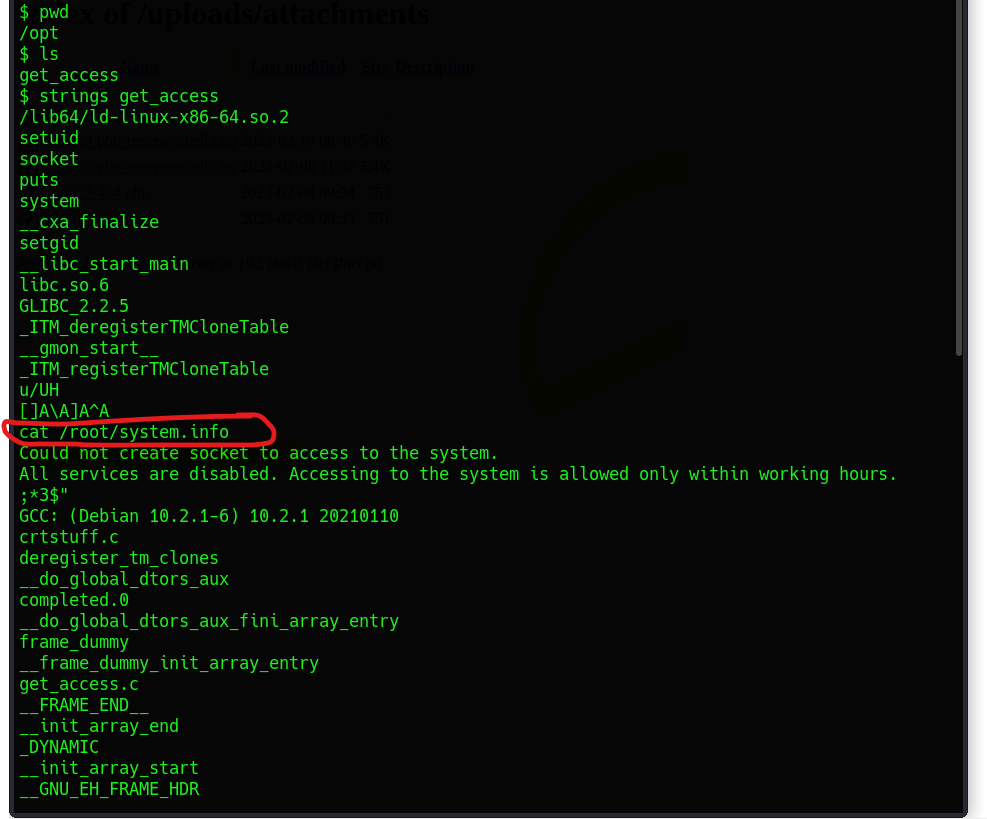
Command: **ls -l**

Using this command above, we find that the get\_access file is of type, || -rwsr -xr -x || meaning that it can be run using the with root privileges.

Apology: I only used the **ls** command instead of the **ls -l**

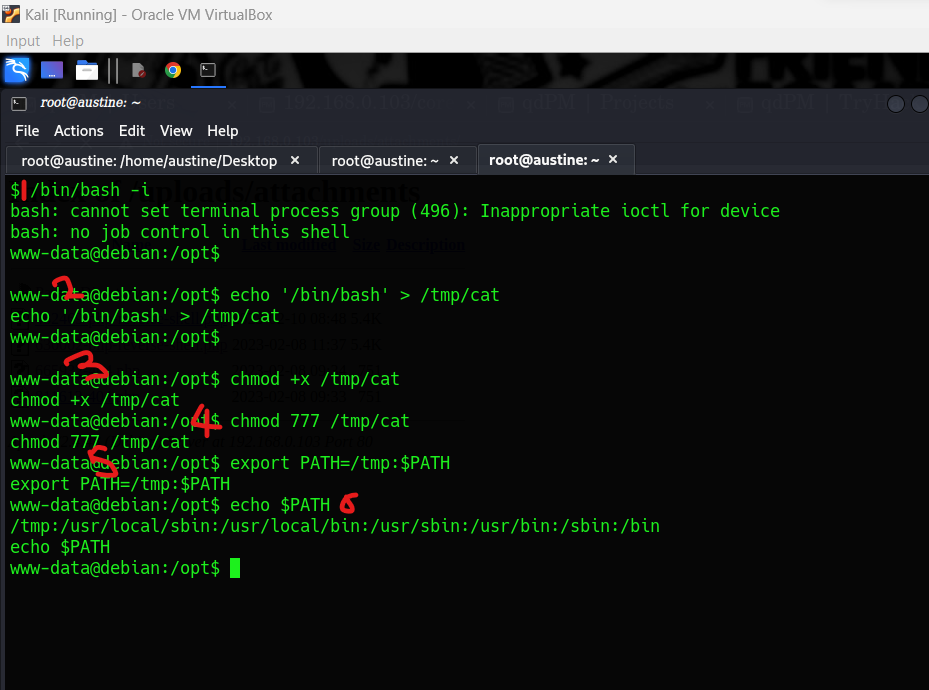
****

**Step 12: The strings command**

****

**Step 13 : Privilege escalation**

We use the PATH privilege escalation tactic to escalate from being (www-data) to being root



Explanation:

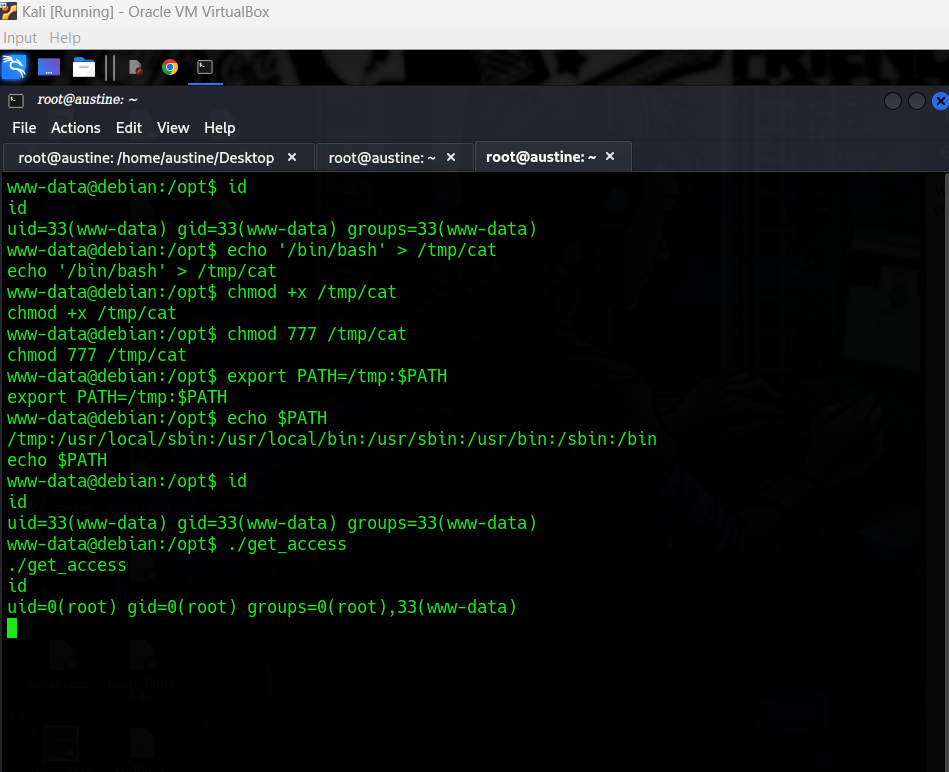
1. We install the /bin/bash using the command: **/bin/bash -i**
2. Push the path /bin/bash into the /tmp.cat command: **echo ‘/bin/bash’ > /tmp/cat**
3. Changing mode of the file to be executable. Command: **chmod +x /tmp/cat**
4. The command chmod -R 777 / makes every single file on the system under / (root) have rwxrwxrwx permissions. Command: chmod 777 /tmp/cat
5. Ensuring that the current path we are in comes after the /tmp/$$PATH FOLLLOWS hence the command will be able to first look into the tmp for the cat command

**Command: echo PATH=/tmp: $PATH**

1. Print out the path, the /tmp should appear at the front Command: **echo $PATH**

**Step 14 : Final step, WE ARE NOW ROOT**

If we check the current user using command: **id,** we are root and cd we can cd into any director in the system and thus we are able to unfold the root.txt project found in the root folder



**STEP 15: MAKE SURE YOU LEAVE YOUR FEEDBACK OR A THANK YOU NOTE**

**[[1]](#footnote-1)**

**THANK YOU**

1. [↑](#footnote-ref-1)