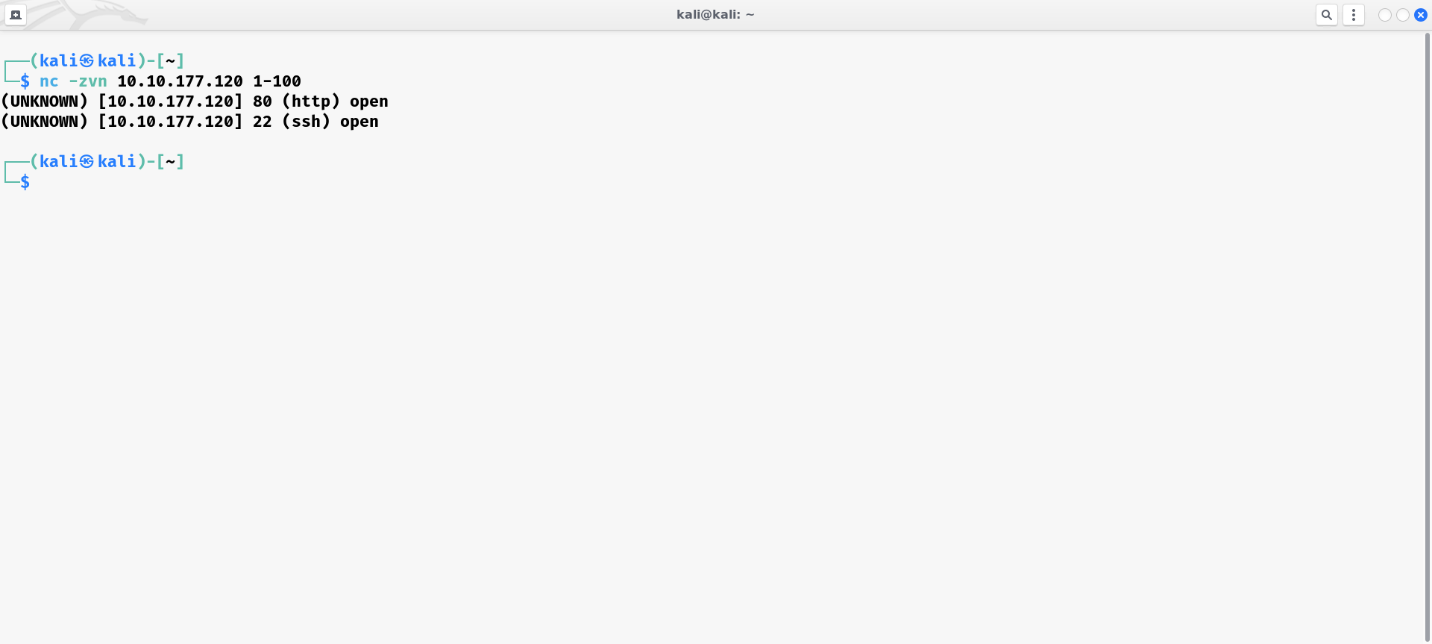
**Lab Practical #07:**

TryHackMe Room: - **Rootme**

Initially, we will try with the reconnaissance, so let’s start with the nc scan.



**nc results**

By looking at the above screenshot, we can see that we have found 2 ports open i.e. 22(SSH) and 80(HTTP).

1. **Scan the machine, how many ports are open?**

**Answer:** *2*

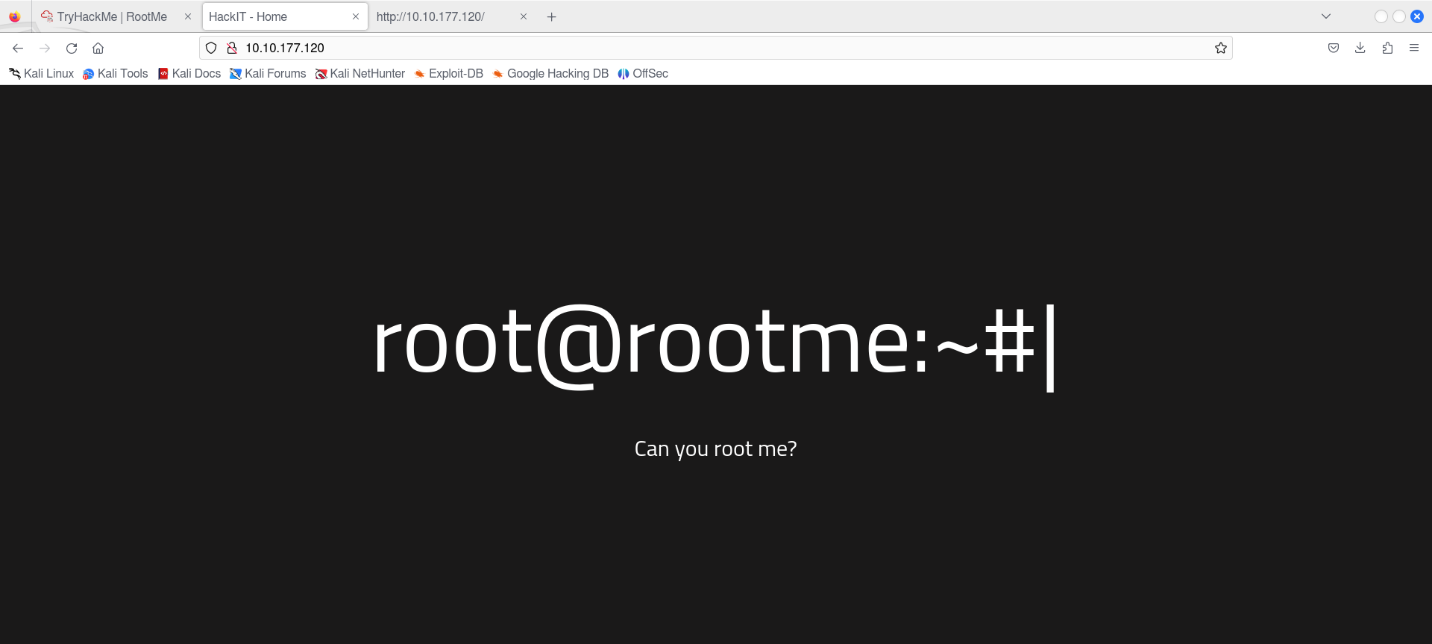
1. **What version of Apache is running?**

**Answer:** *2.4.29*

1. **What service is running on port 22?**

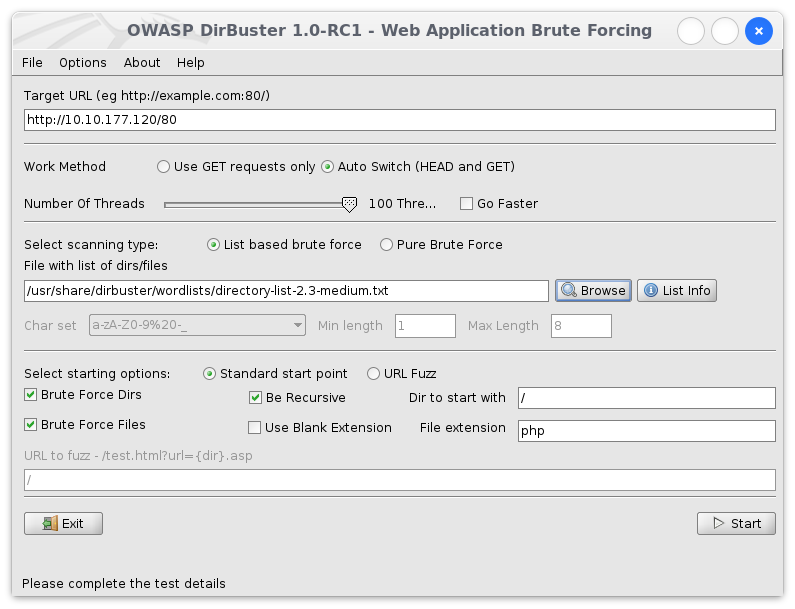
**Answer:** *2*

As port 80 is open, copy-paste the IP in the browser and check the source page of this.



1. **Find directories on the web server using the GoBuster tool.**

**Answer:** *No Answer needed*



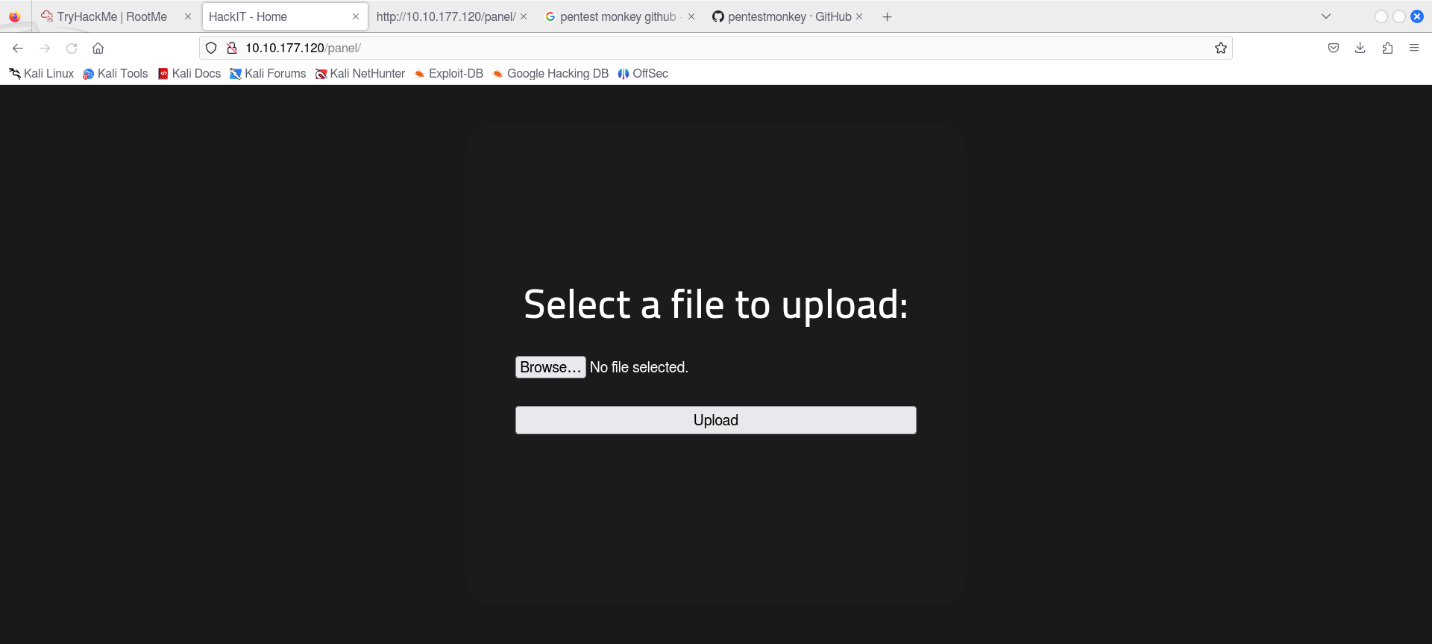
1. **What is the hidden directory?**

**Answer:***/panel/*

We have to find a form to upload and get a reverse shell, and find the flag.

As you can observe, there isn’t anything of interest in the source code for us. Therefore, we will proceed to investigate the directories discovered using Gobuster.

We discovered earlier that there is a hidden directory “/panel/”. Let’s open that to see if we find anything useful.

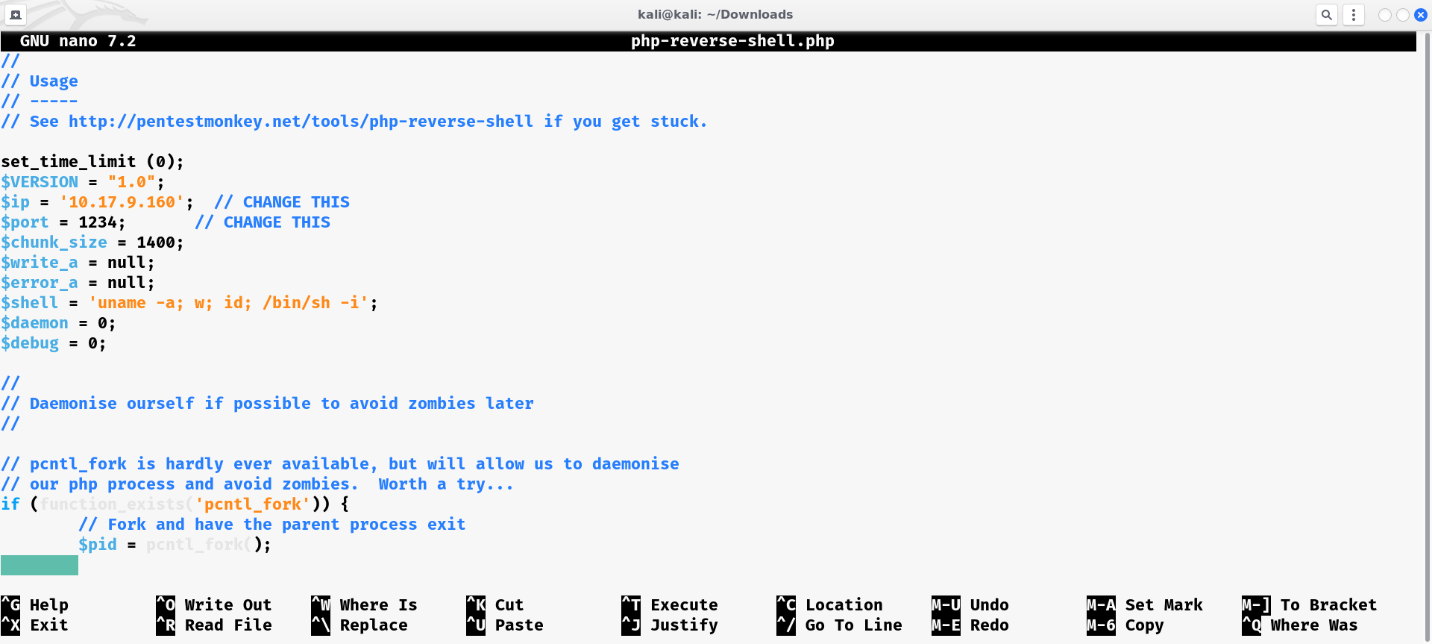


As you can see that we can upload a file to the /panel/ directory.

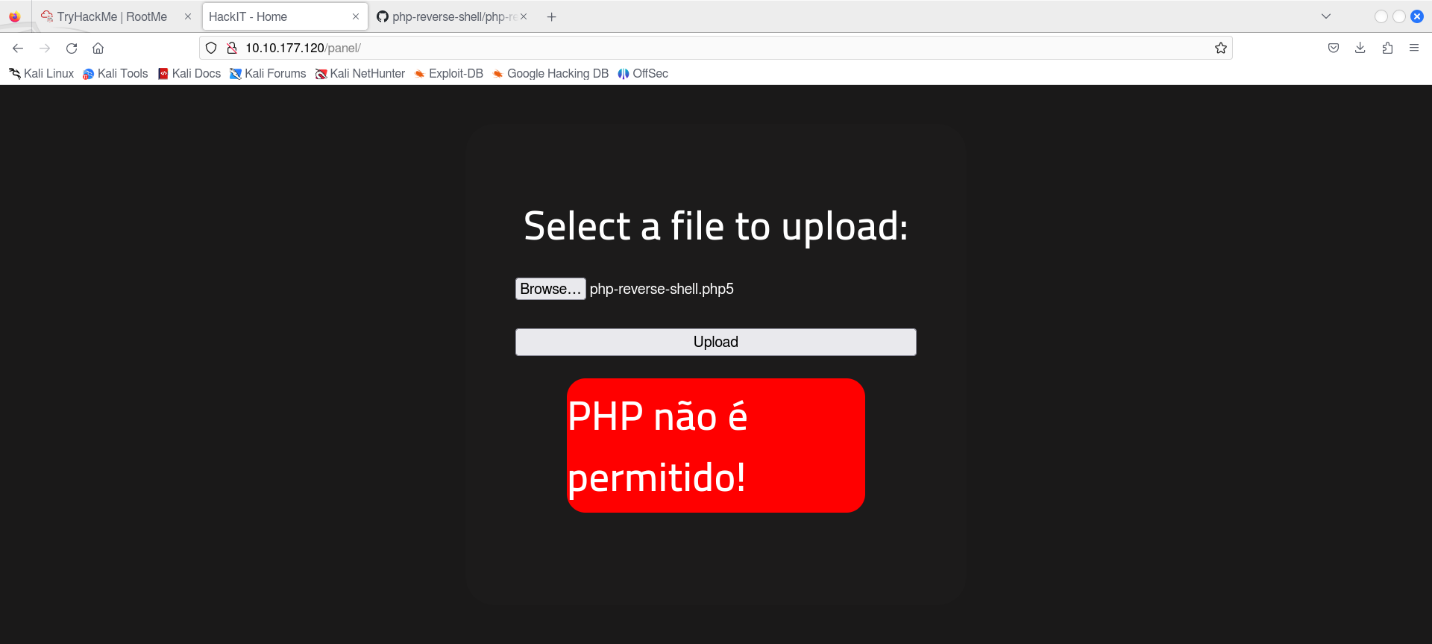
To accomplish this, we will upload a PHP reverse shell script.

I used php-reverse-shell.php script by Pentestmonkey.

Now the script has been downloaded in the directory,opening the script in editor and change the ip and port to my host machine’s IP and port.



Now we have configured the script . We will proceed furthur and upload the script.

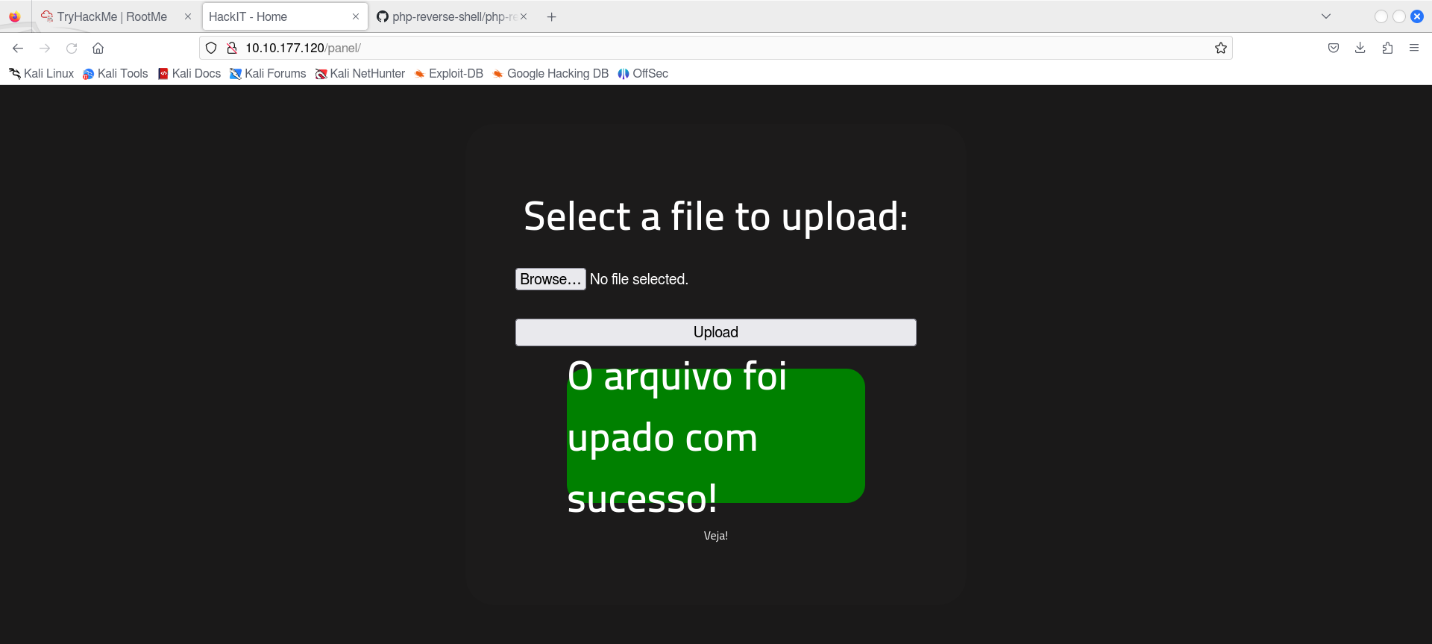


Upload failed!! This is because .php file is not allowed to be uploaded here. So we will try to bypass the upload by changing the file extension.

We will rename the script using the command:***mv php\_reverse\_shell.php php\_reverse\_shell.php5***

This will change the file extension from .php to .php5

Now let’s try to upload the script again to see if it works.

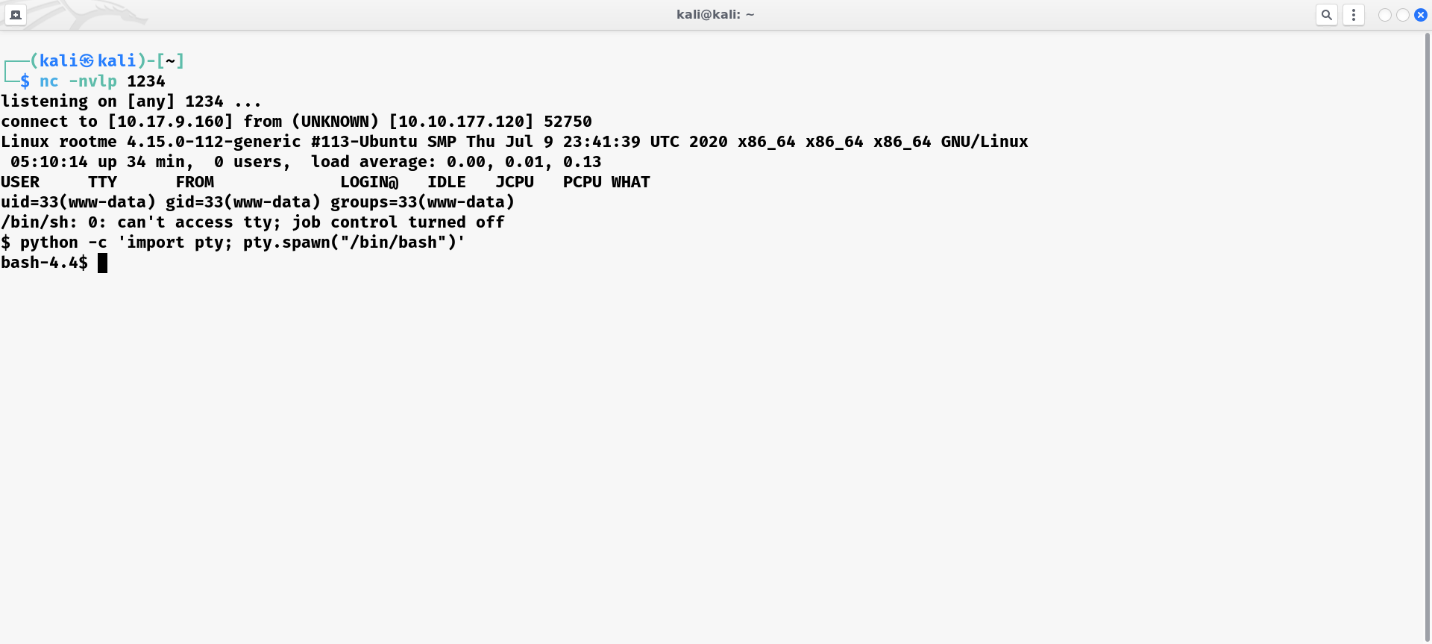


The script has been uploaded successfully.

Moving on to the next step, i will initiate a listener using Netcat. I am using 1234 port which was already inserted in the script that i uploaded.

Now I will gain shell by executing the uploaded script in the 10.10.177.120/uploads/

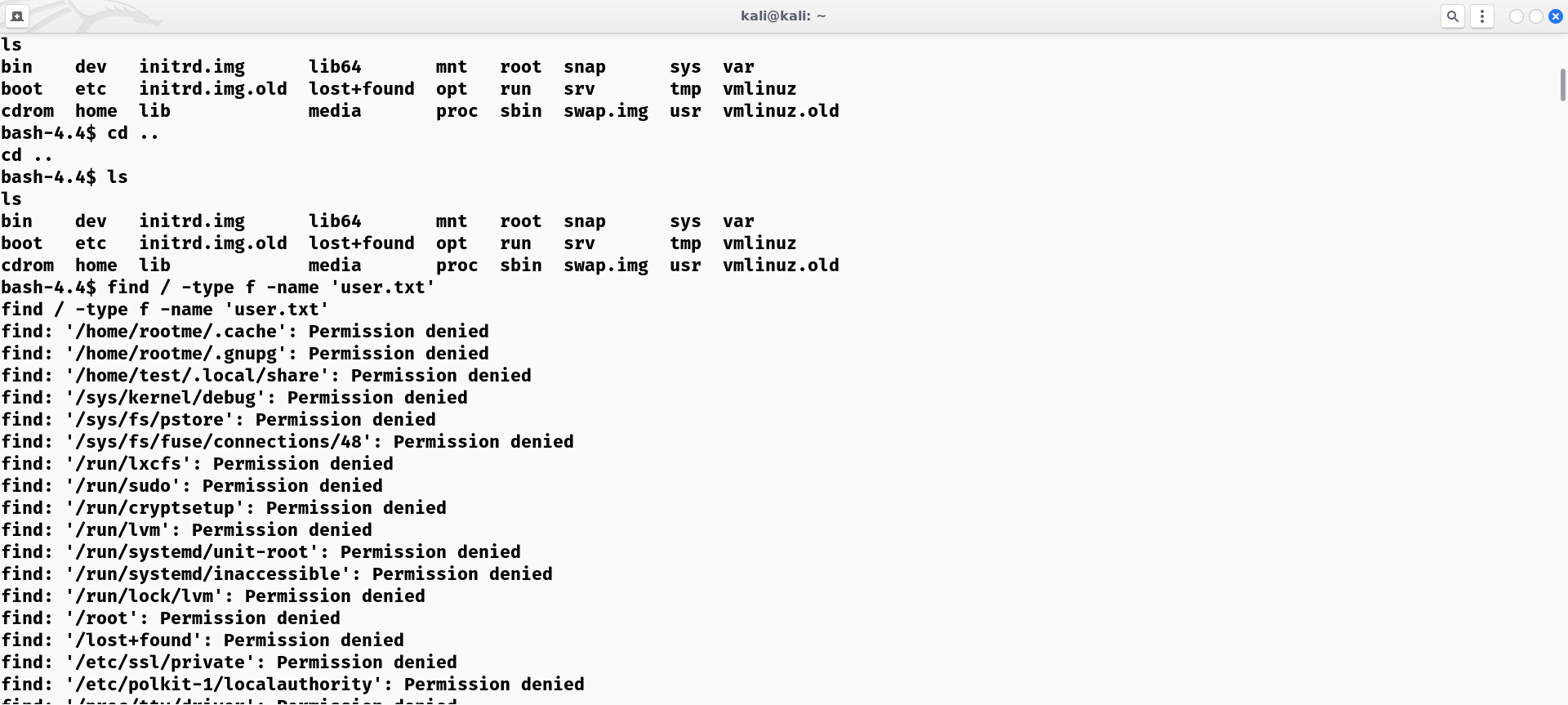
Executing the script and check back to see my netcat listener.



we have successfully gained the shell.

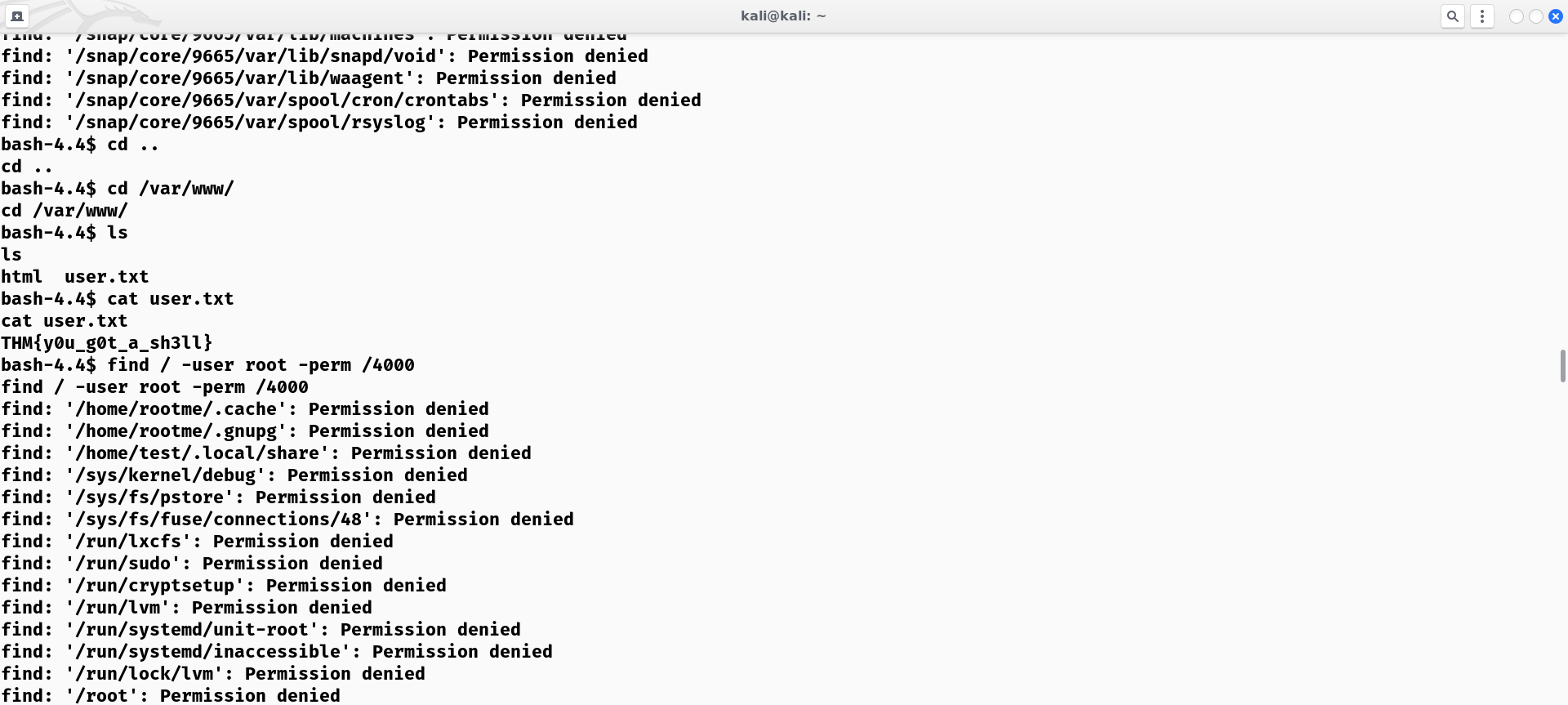
Now let’s search for the flag. We know that it is in user.txt as it is mentioned in the question.

Run the command: ***find / -type f -name user.txt 2> /dev/null***



We can see where the file is located (/var/www/user.txt)

To open the file, run the command: ***cat /var/www/user.txt***



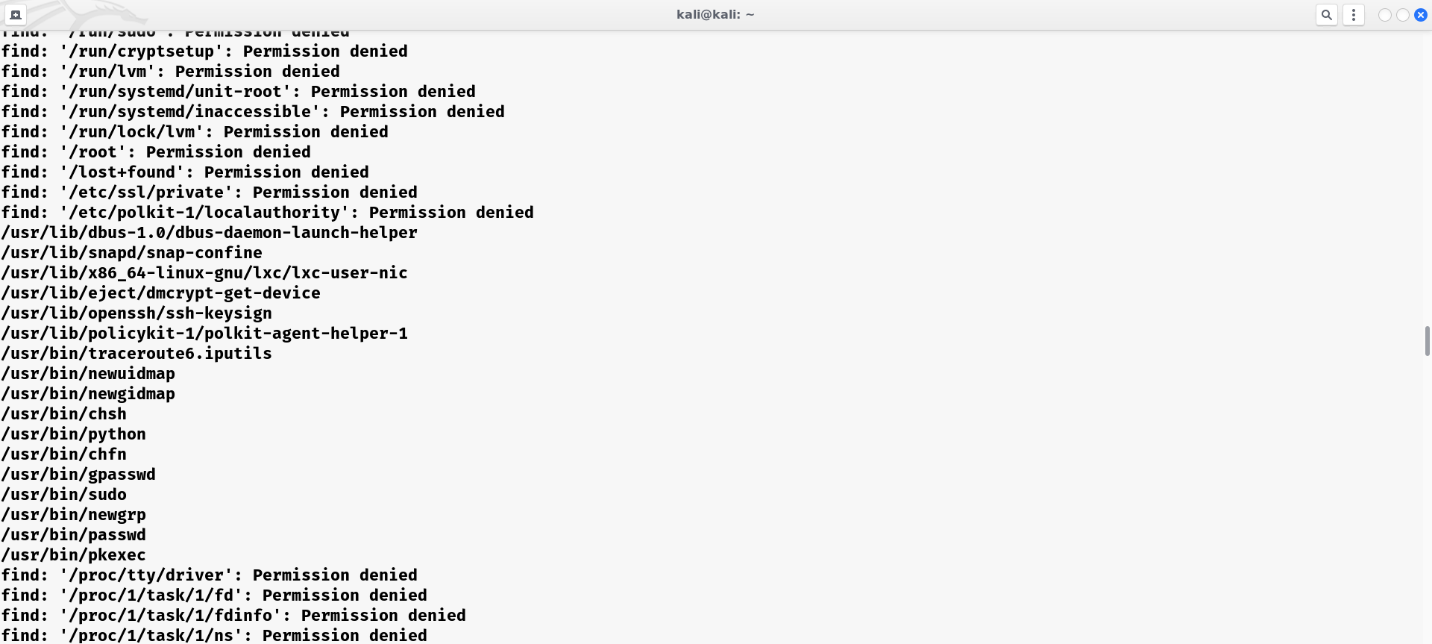
We found our flag which is “***THM{y0u\_g0t\_a\_sh3ll}”.***

1. **Search for files with SUID permission, which file is weird?**

**Answer:***/usr/bin/python*

To look for the files with SUID permission run the command:  
*find / -type f -user root -perm -4000 2>/dev/null*

We have the /usr/bin/python with SUID permission.



Now I will try to escalate our privileges. Let’s go to <https://gtfobins.github.io/> and look for possible privilege escalation commands for elevating the privileges.  
Searching python in the search bar and choose “SUID”.

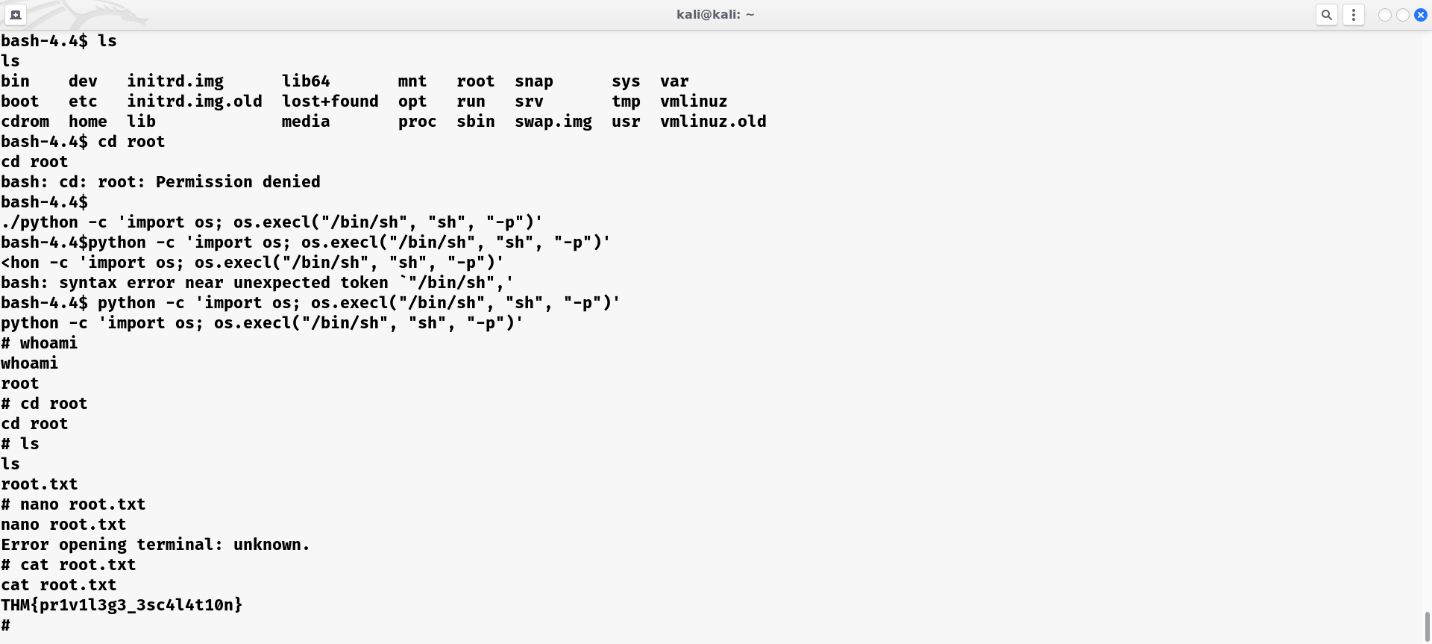
i need the command that has been highlighted above.i can skip the first command as the binary has already SUID permission.

Copying the second command and run it on terminal.

***python -c ‘import os; os.execl(“/bin/sh”, “sh”, “-p”)’***

After running this command,typing ***whoami*** to get confirmation that i indeed as a root user now.

Now, **cat /root/root.txt**



There we found the flag “THM{pr1v1l3g3\_3sc4l4t10n}”.

TryHackMe Tutorial

