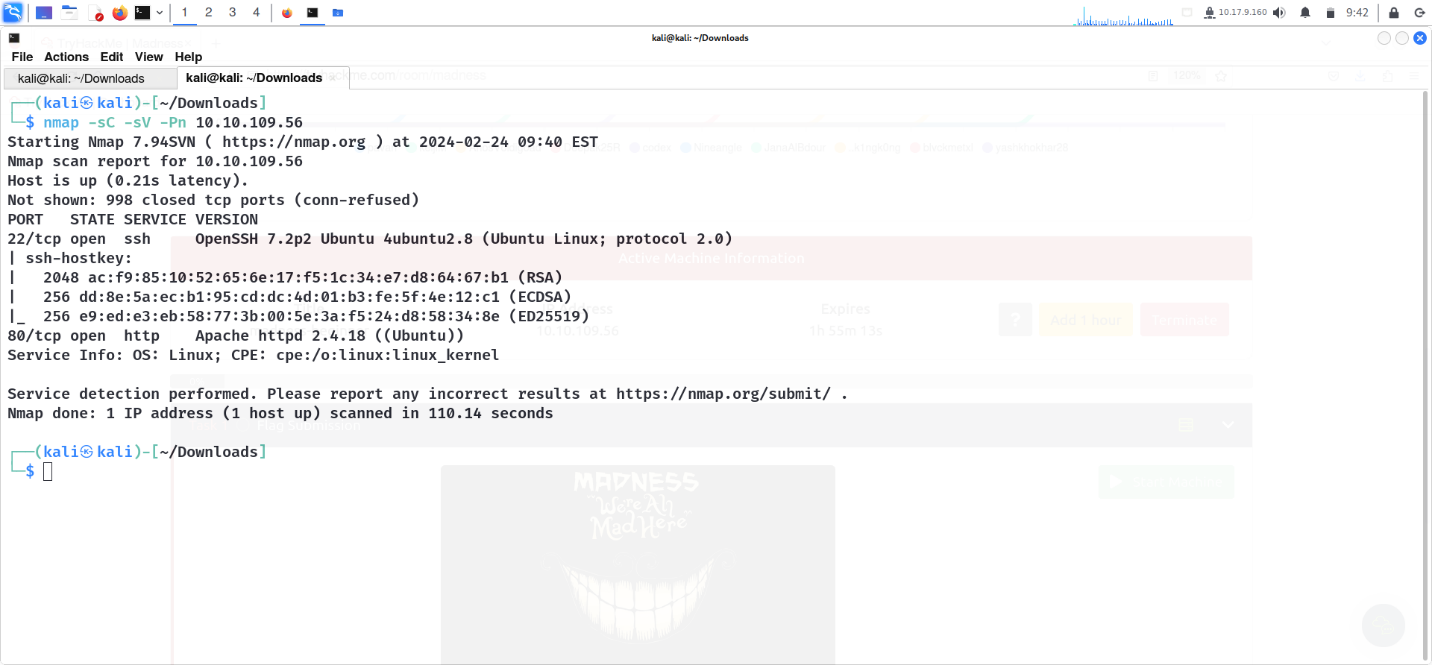
**Lab Practical #04:**

TryHackMe Room: - **madness**

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

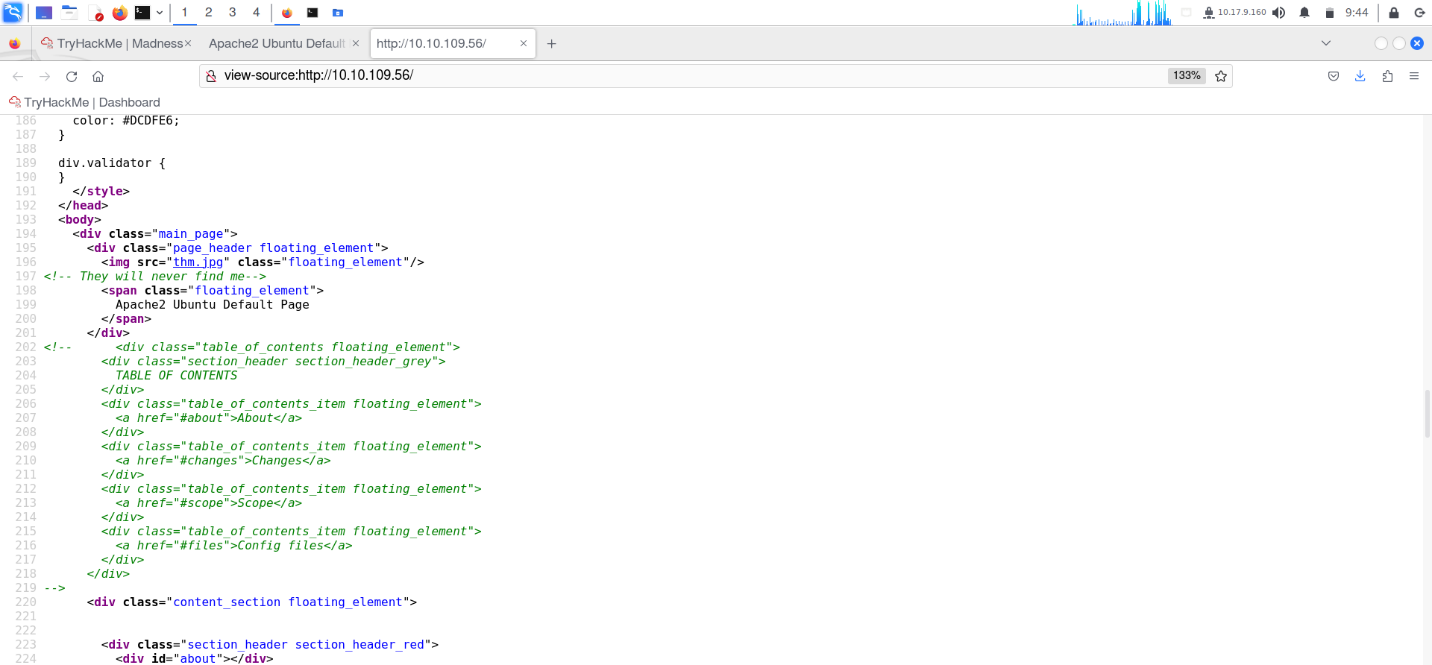
***nmap -sC -sV <10.10.109.56>***



**nmap results**

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

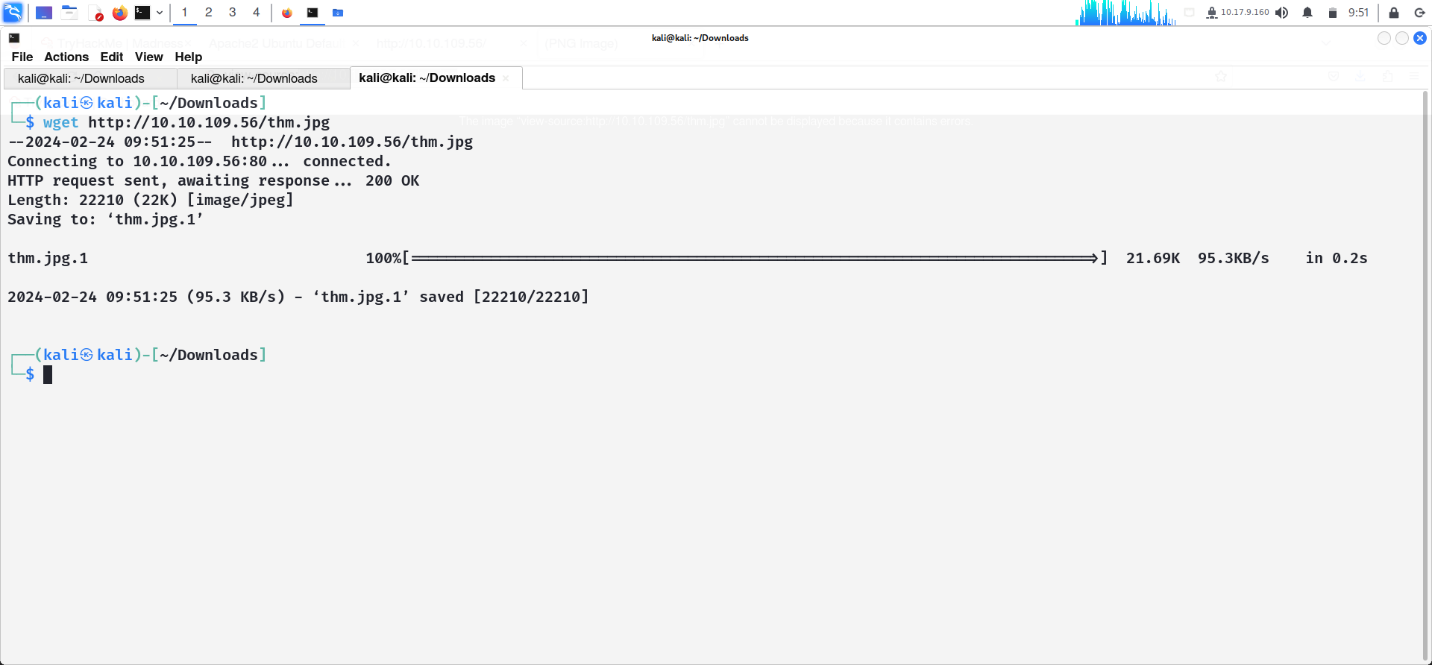
1. As port 80 is open, copy-paste the IP in the browser and check the source page of this.



**source page**

1. There is an interesting comment here, “They will never find me”, which seems to be under the thm.jpg

lets download the file.



When we try and open the file it cannot be displayed due to errors.

1. The first thing we can see is that the header is referencing a PNG file and not a JPG as per the file extension. We need to correct this but first we need to know what the HEX header is for a JPG.

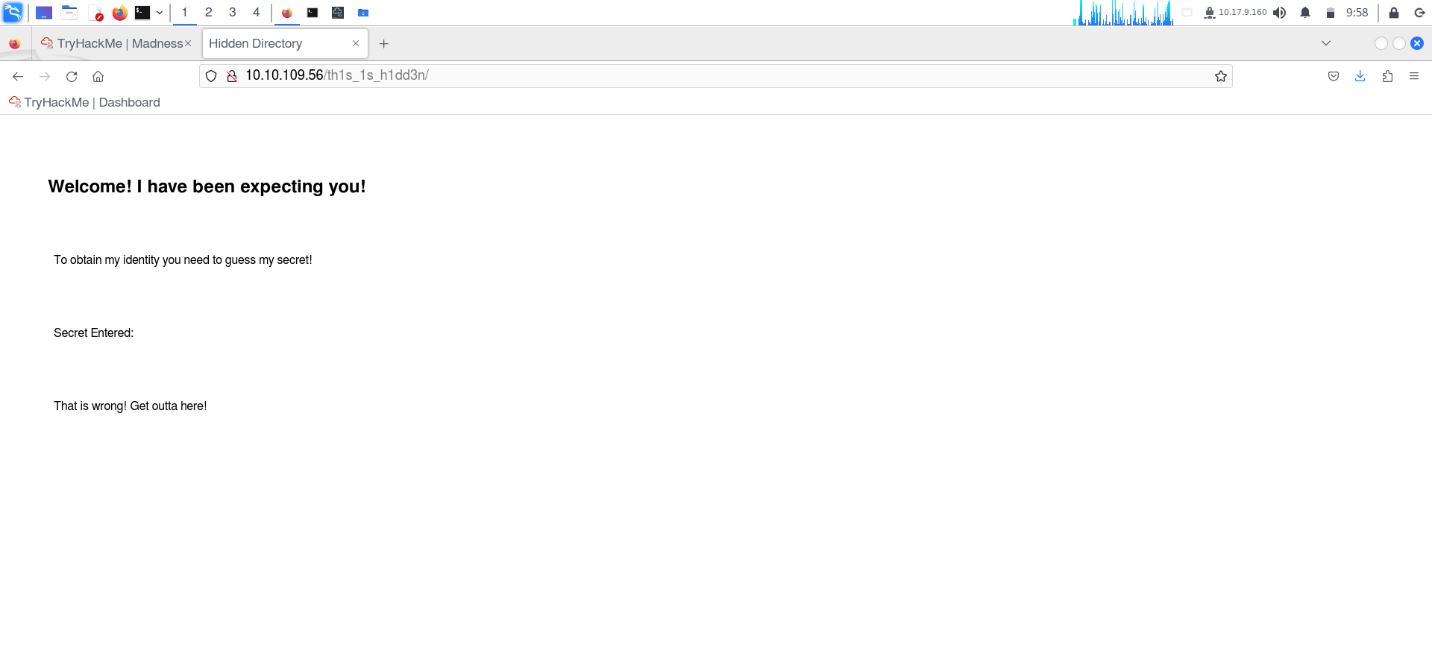
The HEX for the downloaded image starts 89,50,4E,47,0D,0A,1A,0A,00 and as can be seen in the ASCII refers to .PNG. Using the header information from the above site we can see that the HEX code for a JPG is FF D8 FF E0 00 10 4A 46 49 46 00 01.

Replacing the HEX code with the JPEG HEX code using GHex and saving the file works.

We can now load the .jpg and it gives us a hidden directory.



1. Navigating to the secret directory we land on the following page



Checking the source code we find that this is another directory, as there is no additional code in the source. So we know it is between 0–99.

1. So now we will check from 0 upto 99 for the secret using following python code.

import requests

i=0

while(i<100):

    a = requests.get("http://10.10.109.56/th1s\_1s\_h1dd3n/?secret="+str(i))

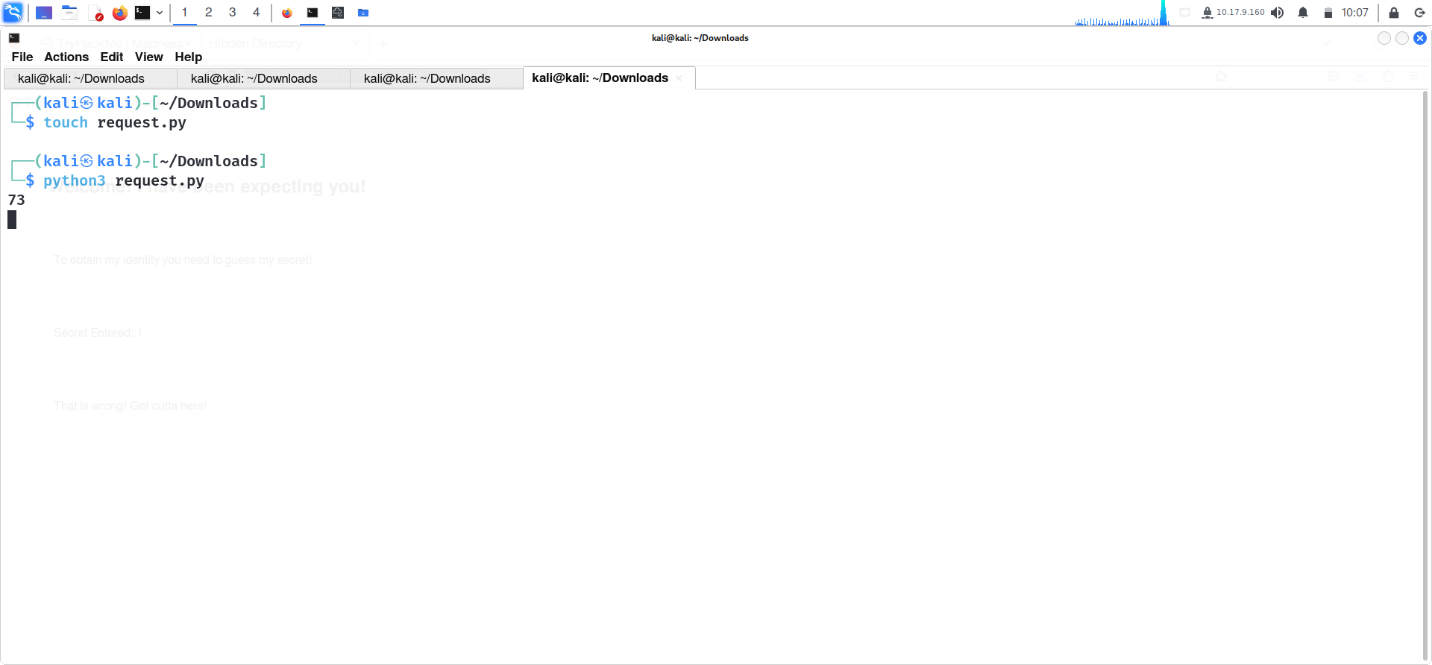
    b = a.text

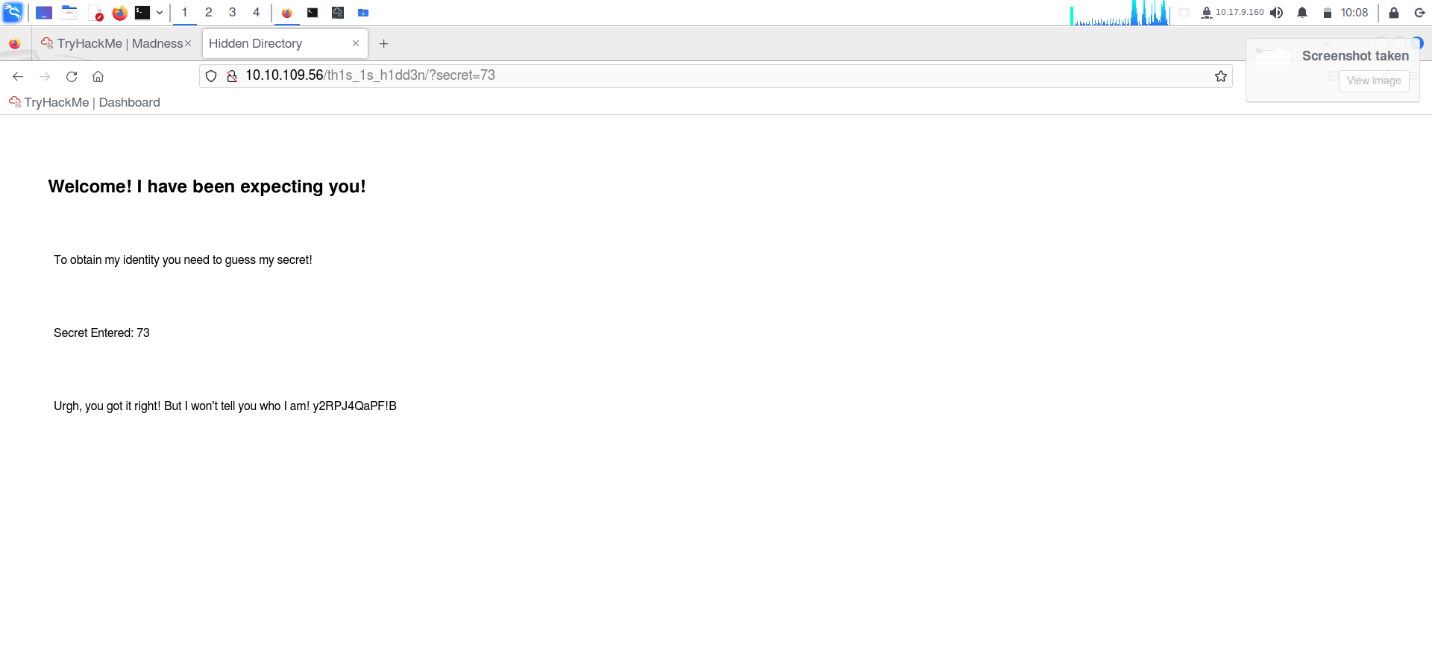
    if("wrong" not in b):

        print(i)

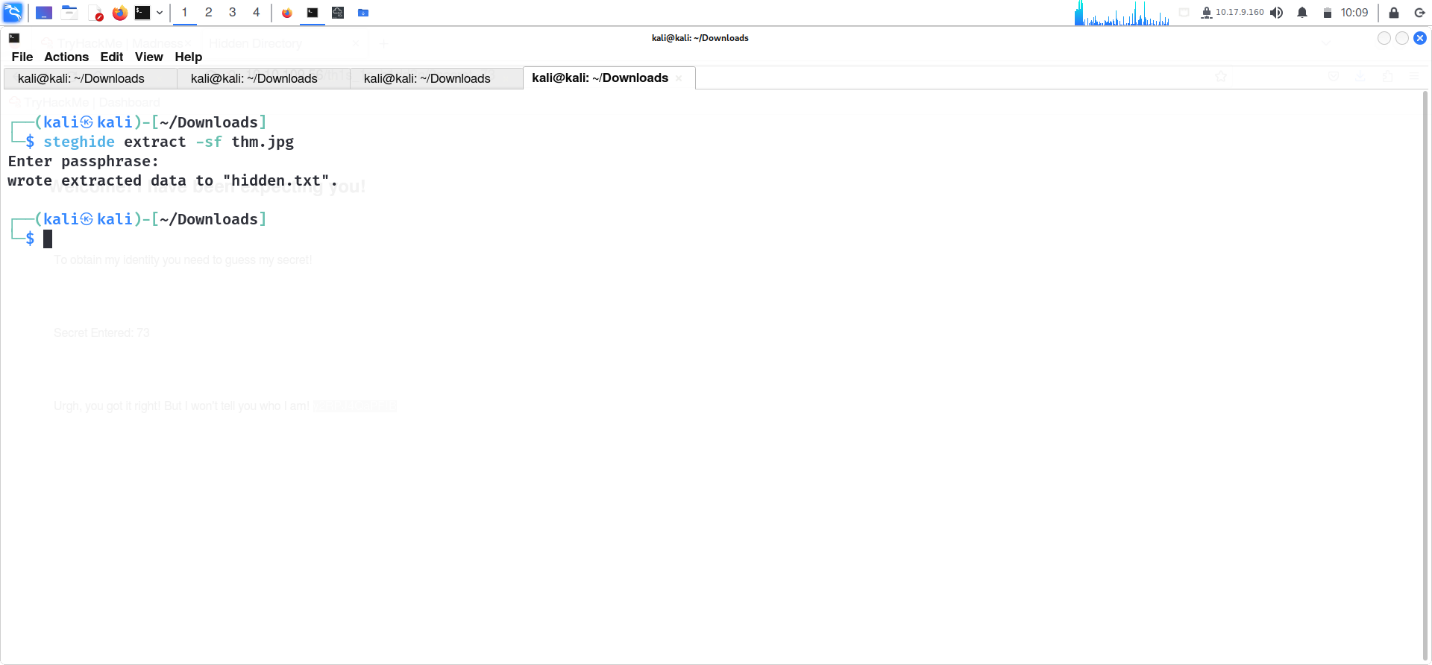
    i=i+1

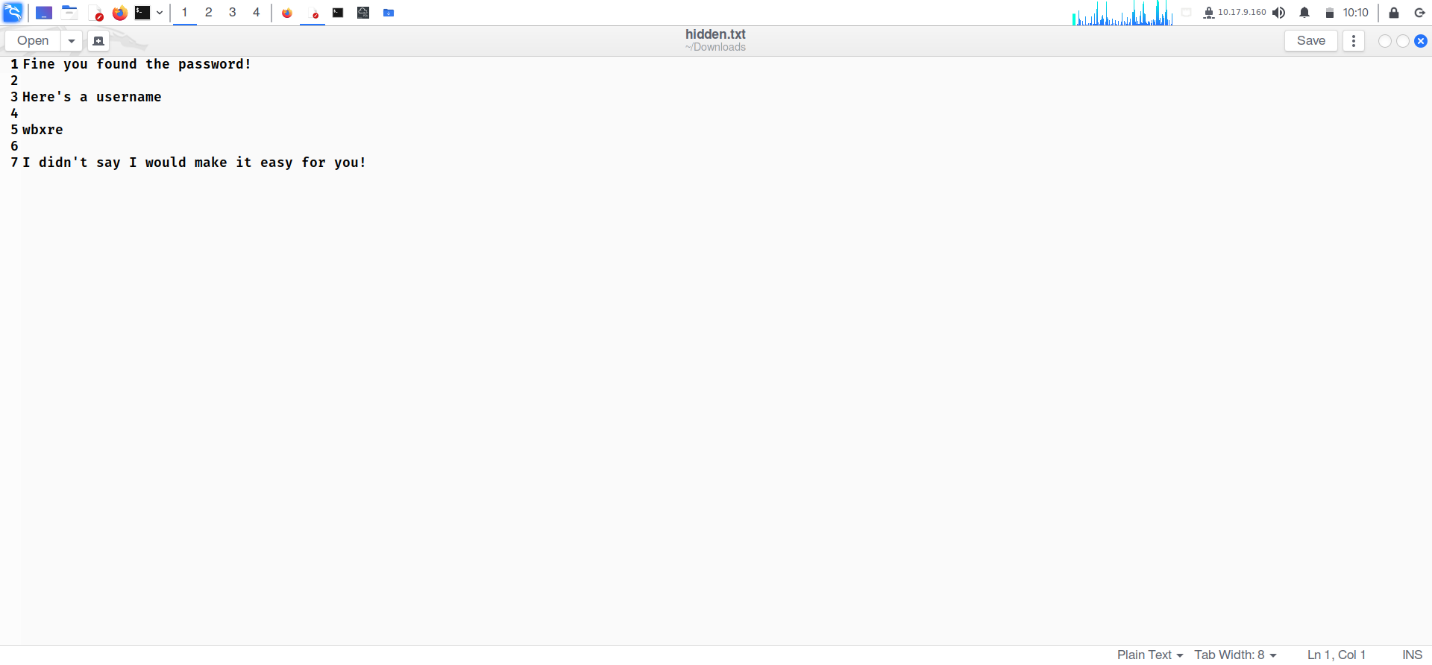
1. Here, we found the value 73.



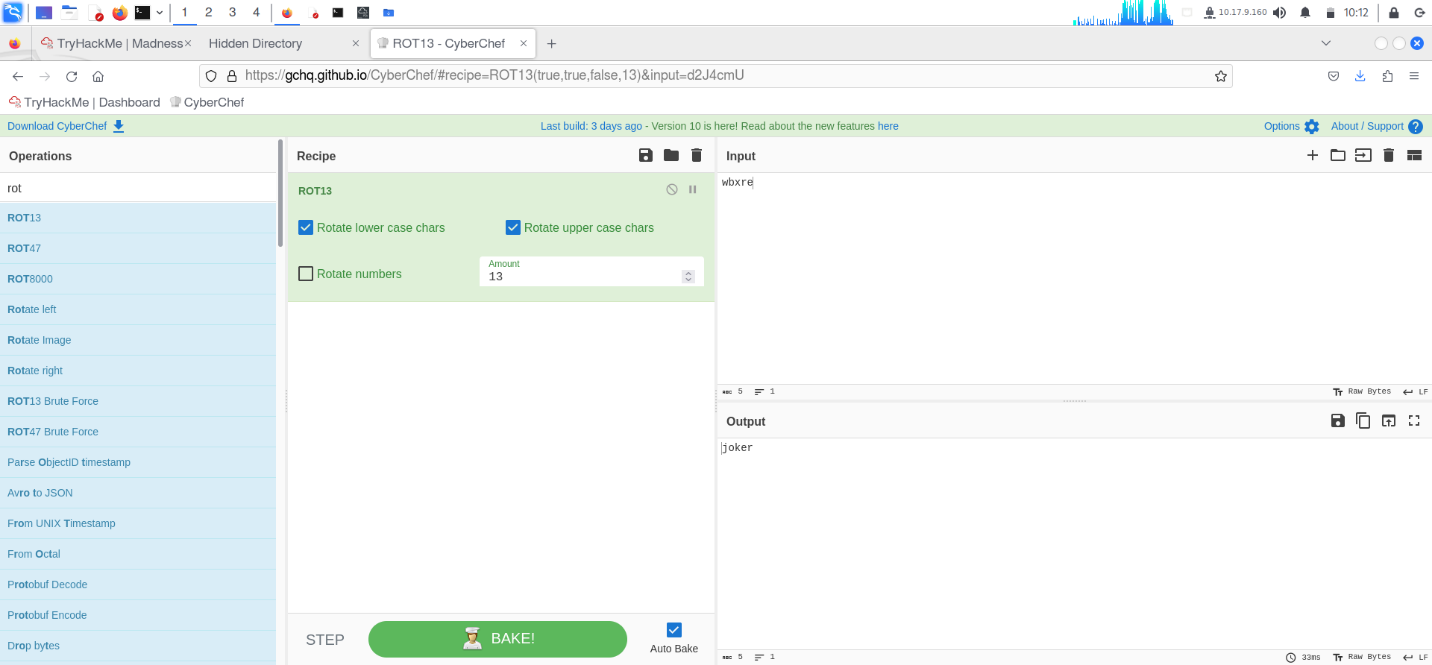


1. Using steghide, we extracted the hidden text from the modified JPEG file, revealing a username.



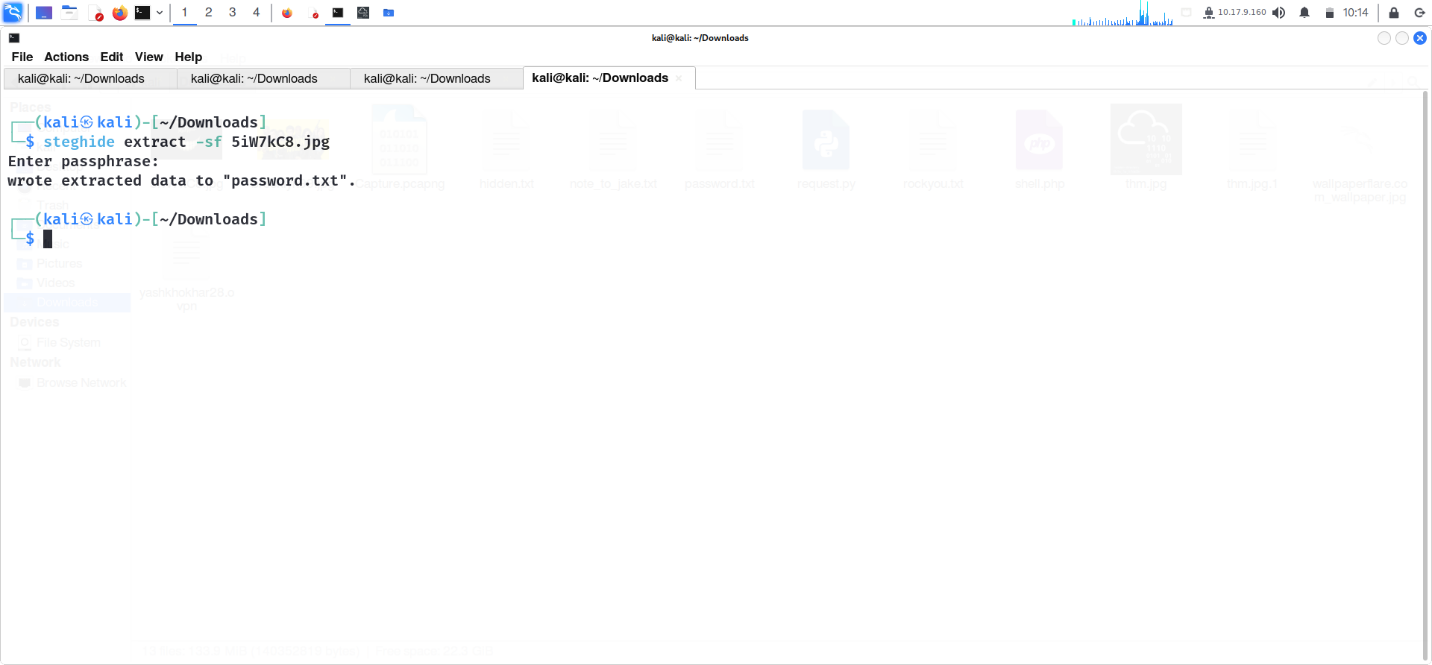


1. As the username still appeared strange, I attempted to decode the text and obtained the plain text username.



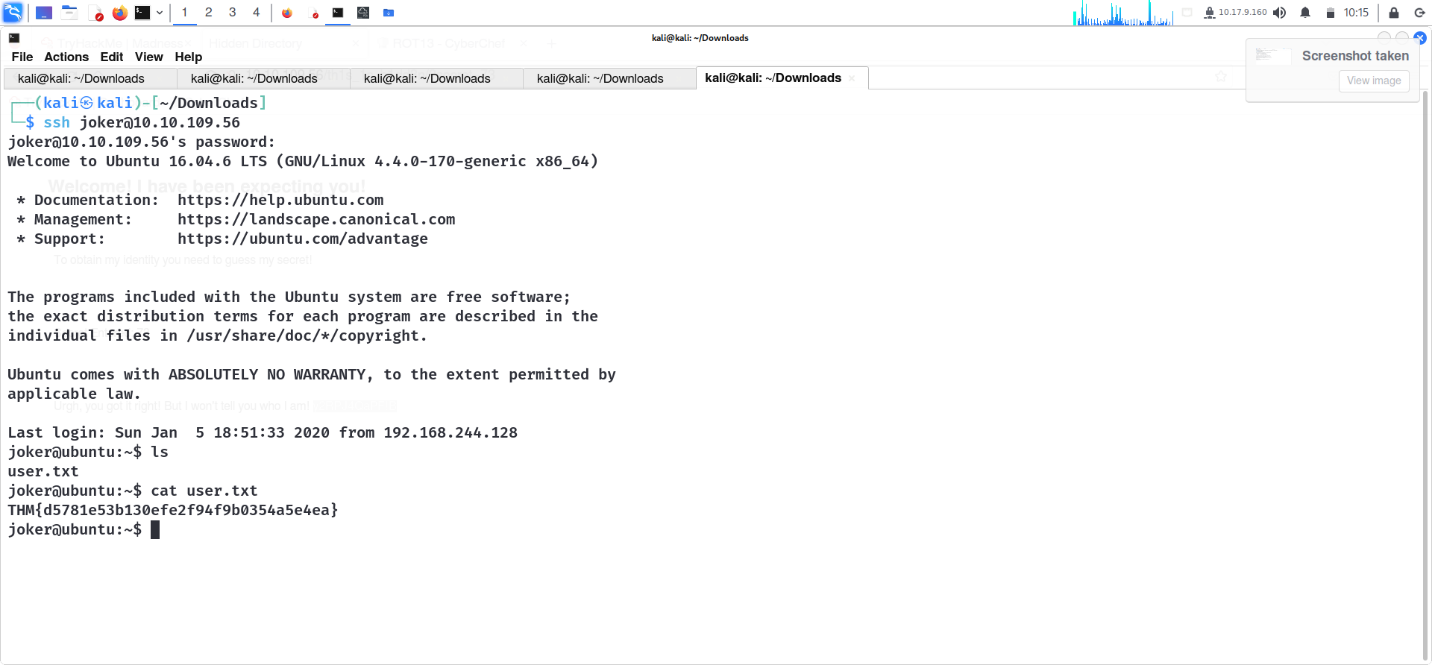
 I attempted to download the banner image from the TryHackMe website.

1. I tried extracting the image using steghide, and indeed, I found text containing a password!!!



1. I accessed port 21 SSH using the username and password we obtained.

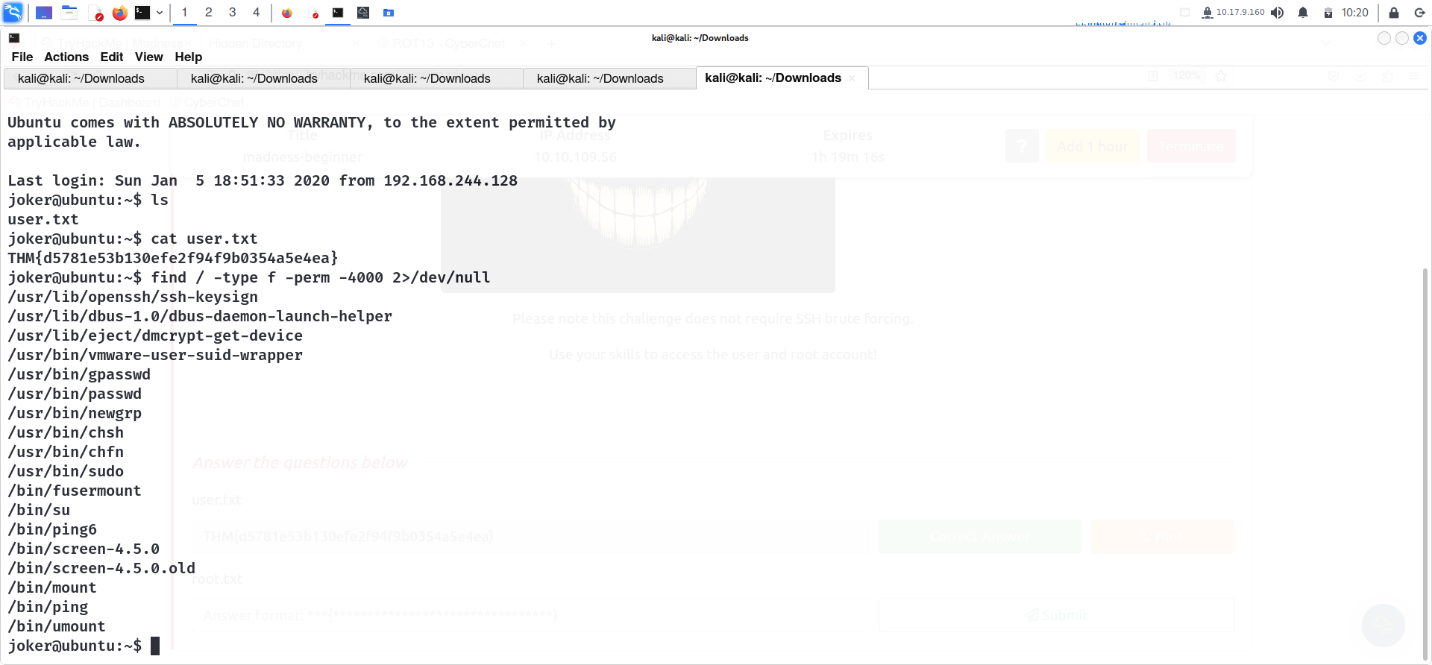
Here, we obtained the first flag.



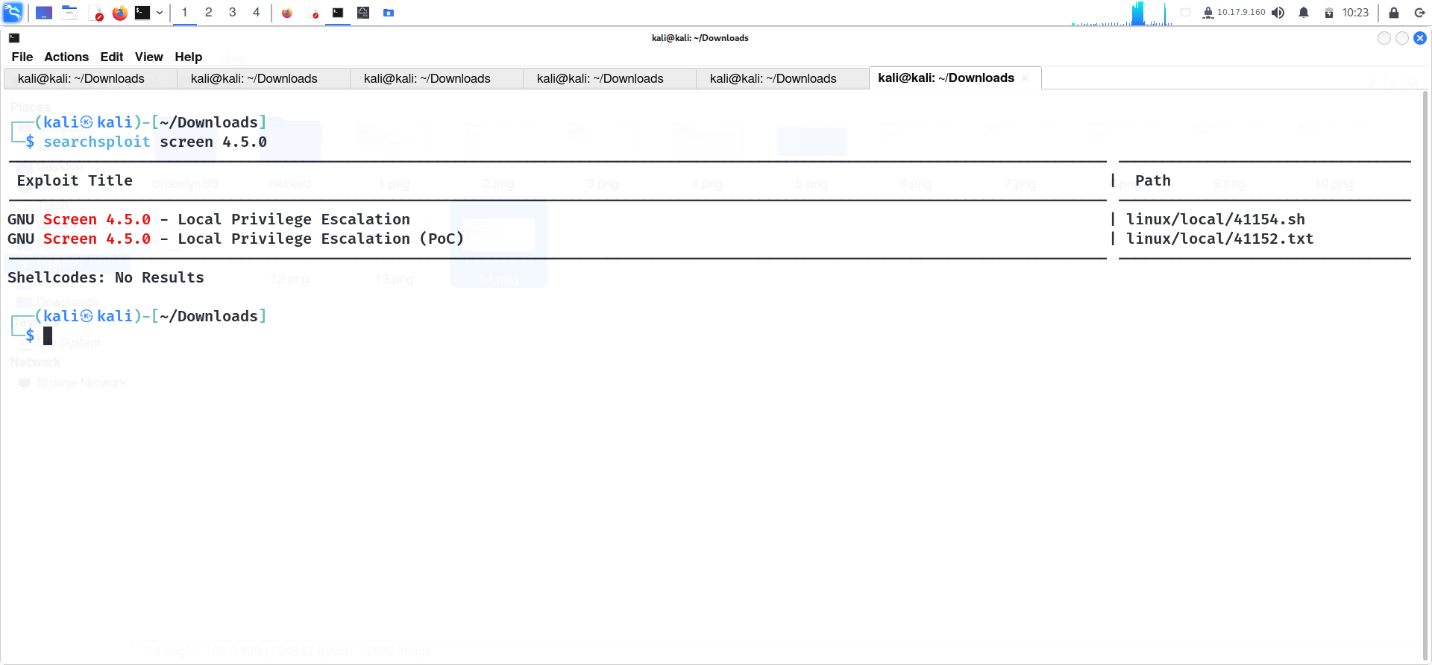
*User.txt*

*Answer: THM{d5781e53b130efe2f94f9b0354a5e4ea}*

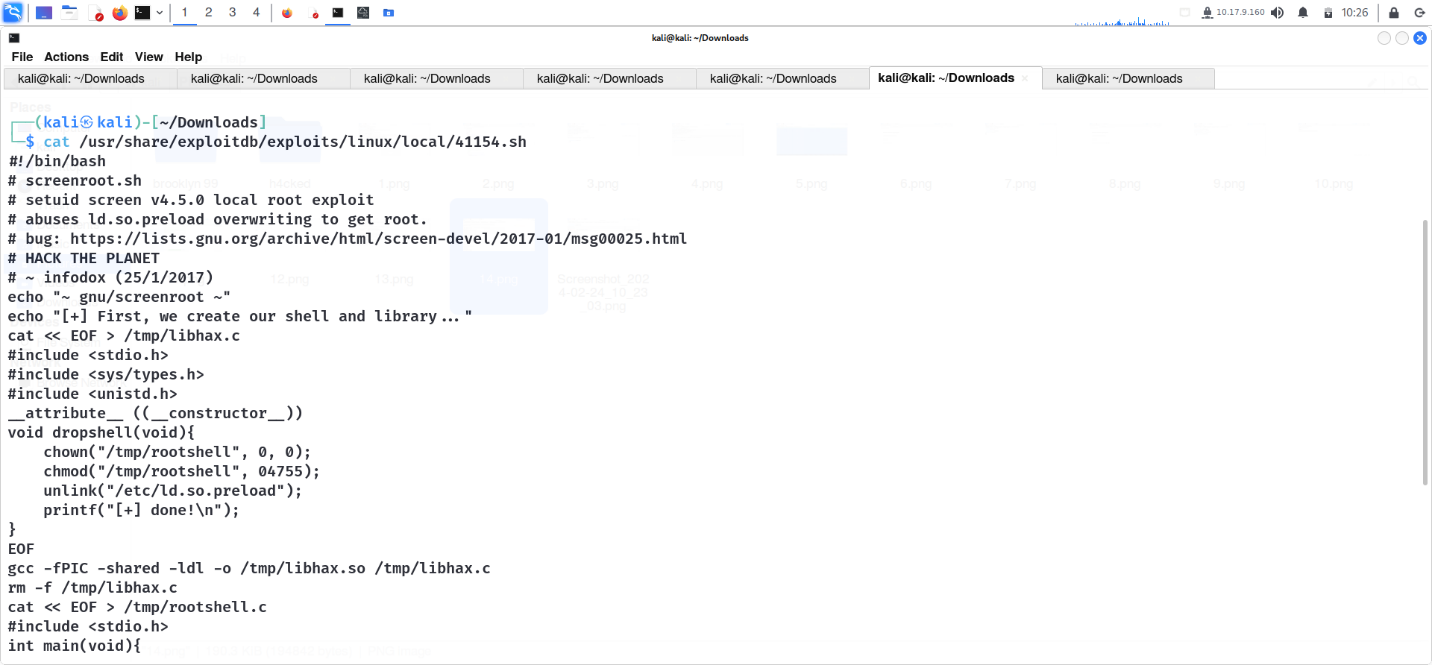
1. I attempted to perform privilege escalation, and I noticed something strange with screen-4.5.0.

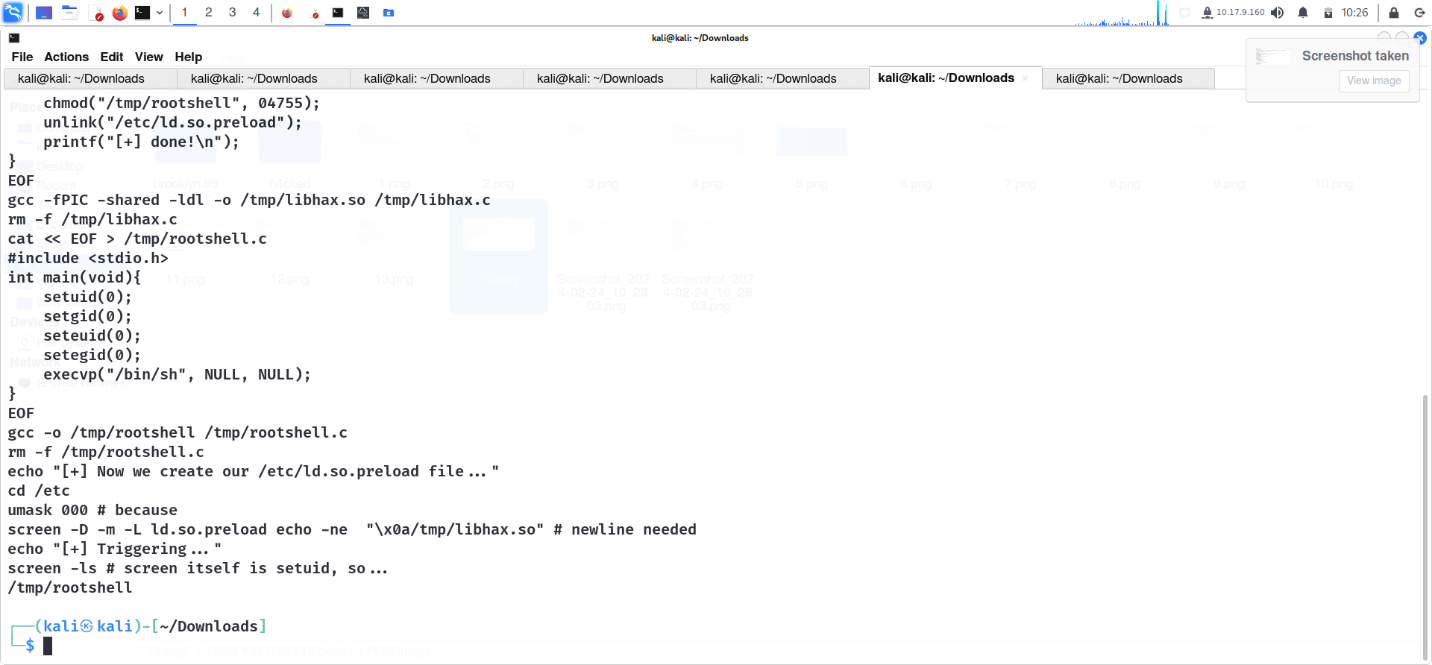


1. I searched for vulnerabilities using searchsploit.

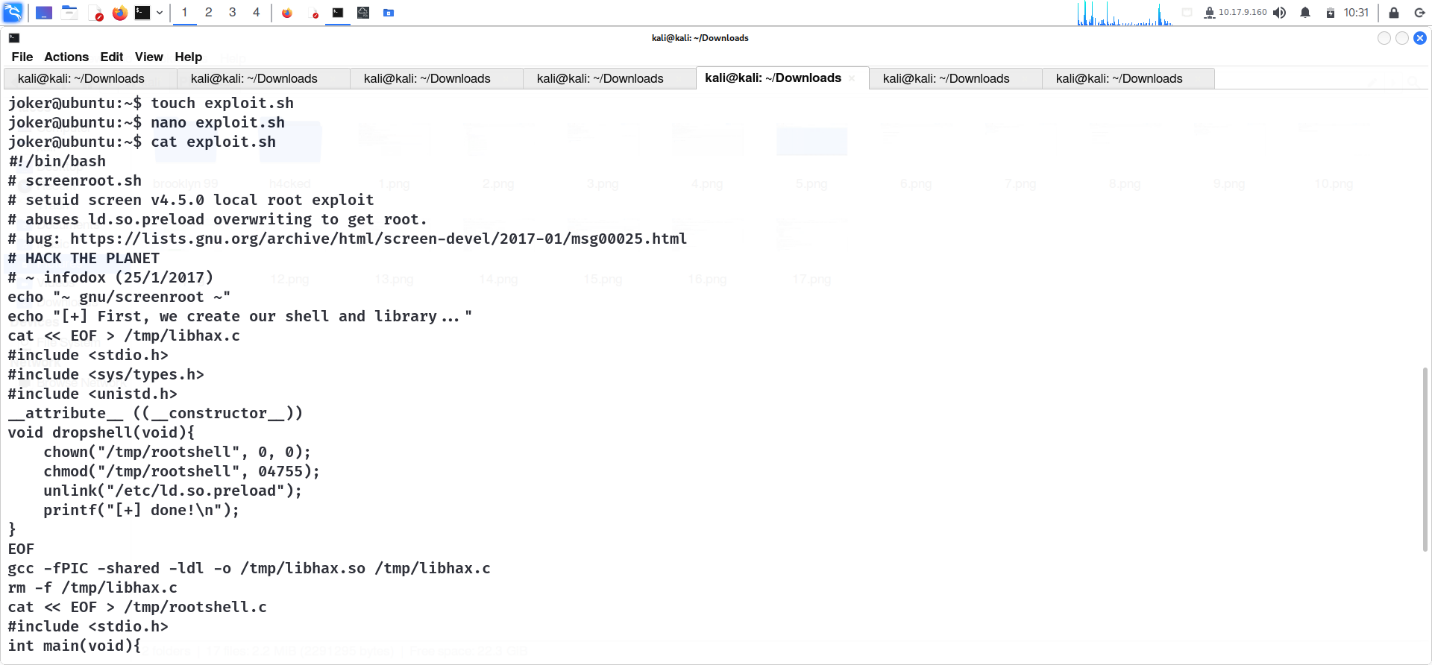


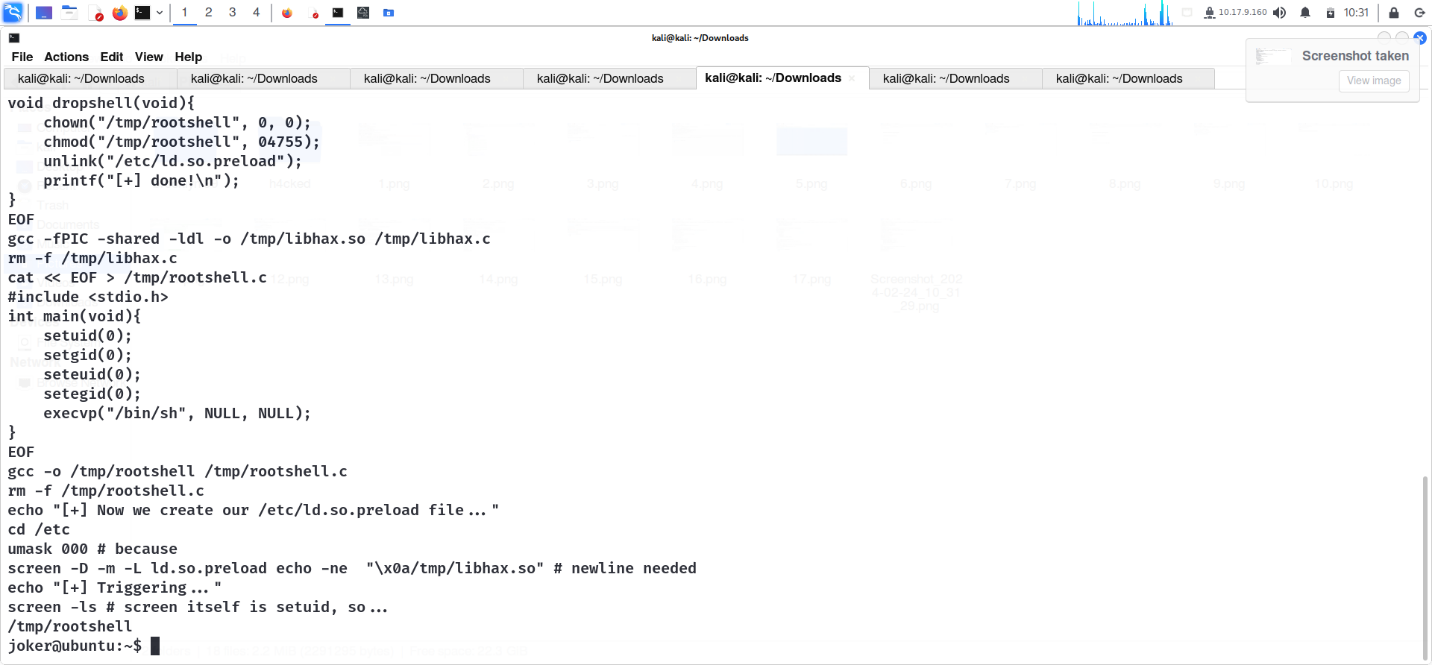
1. open the .sh file.

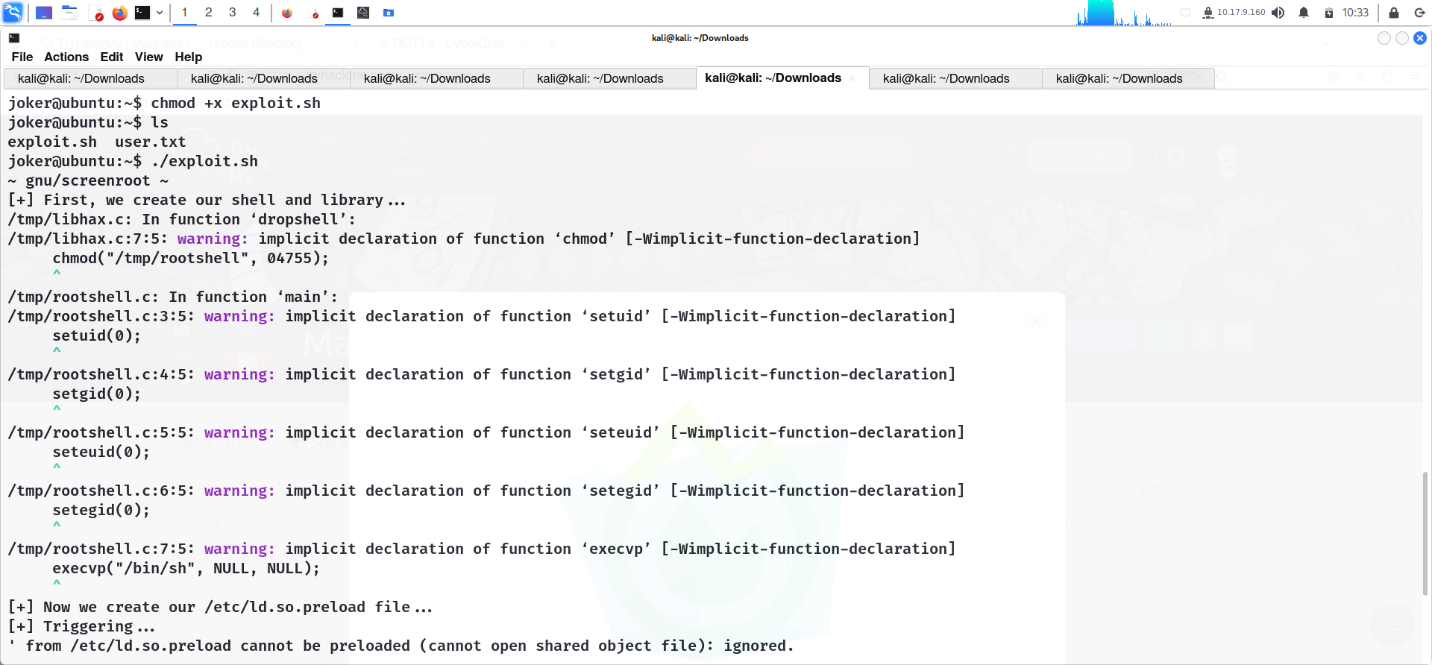


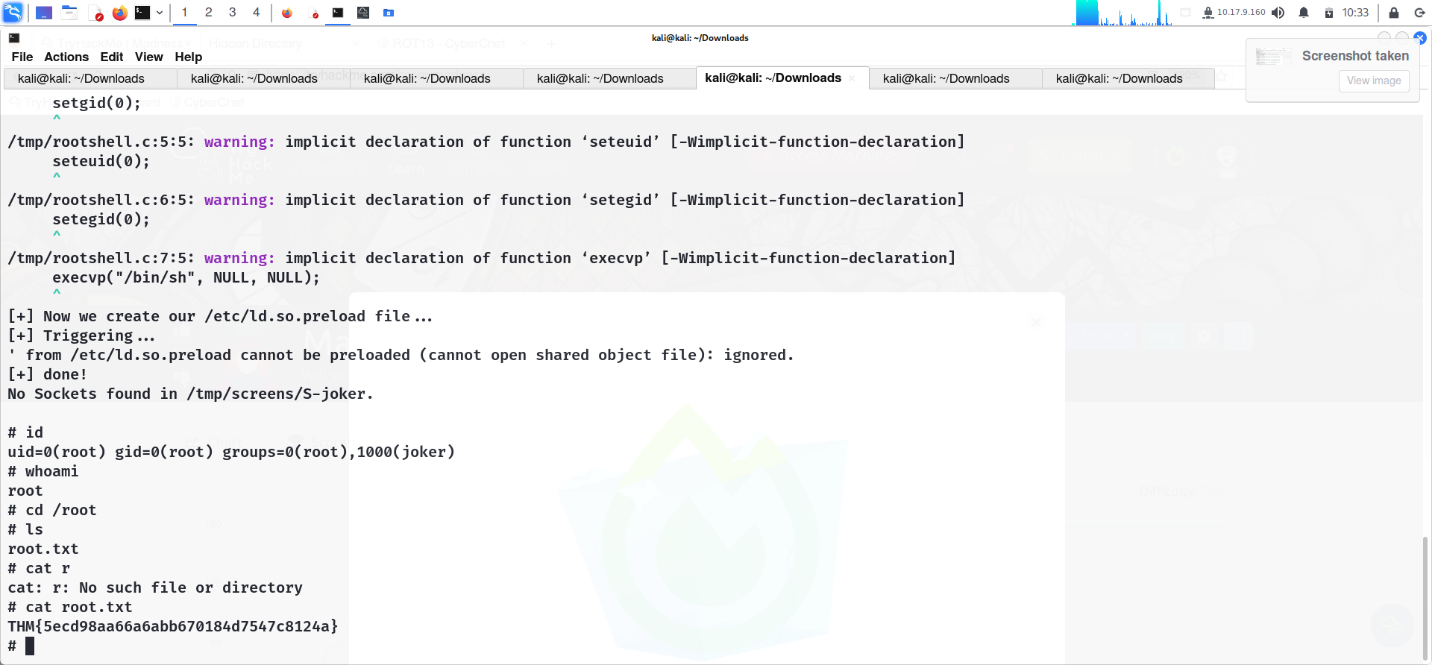


1. I copied the .sh file to the target computer, added executable permissions to the file, and ran the .sh file. And voila, we gained root access.









1. TryHackMe Tutorial

