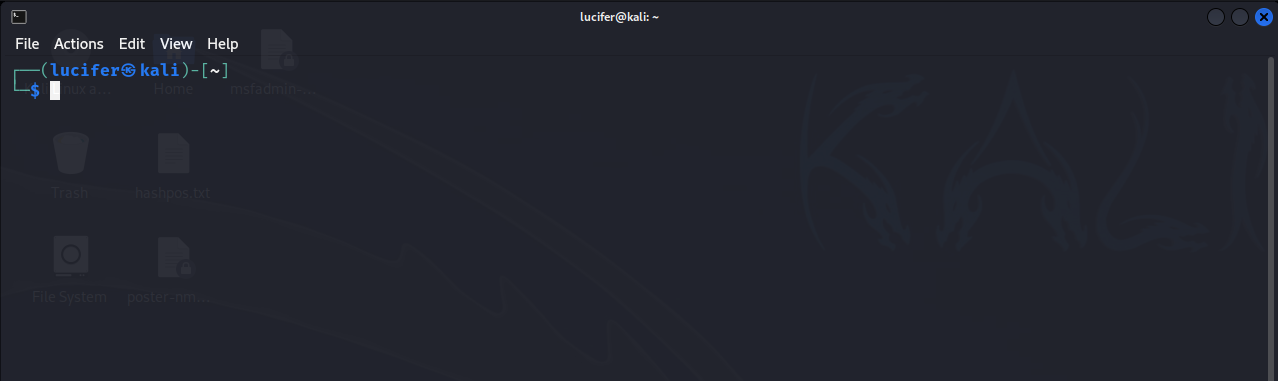
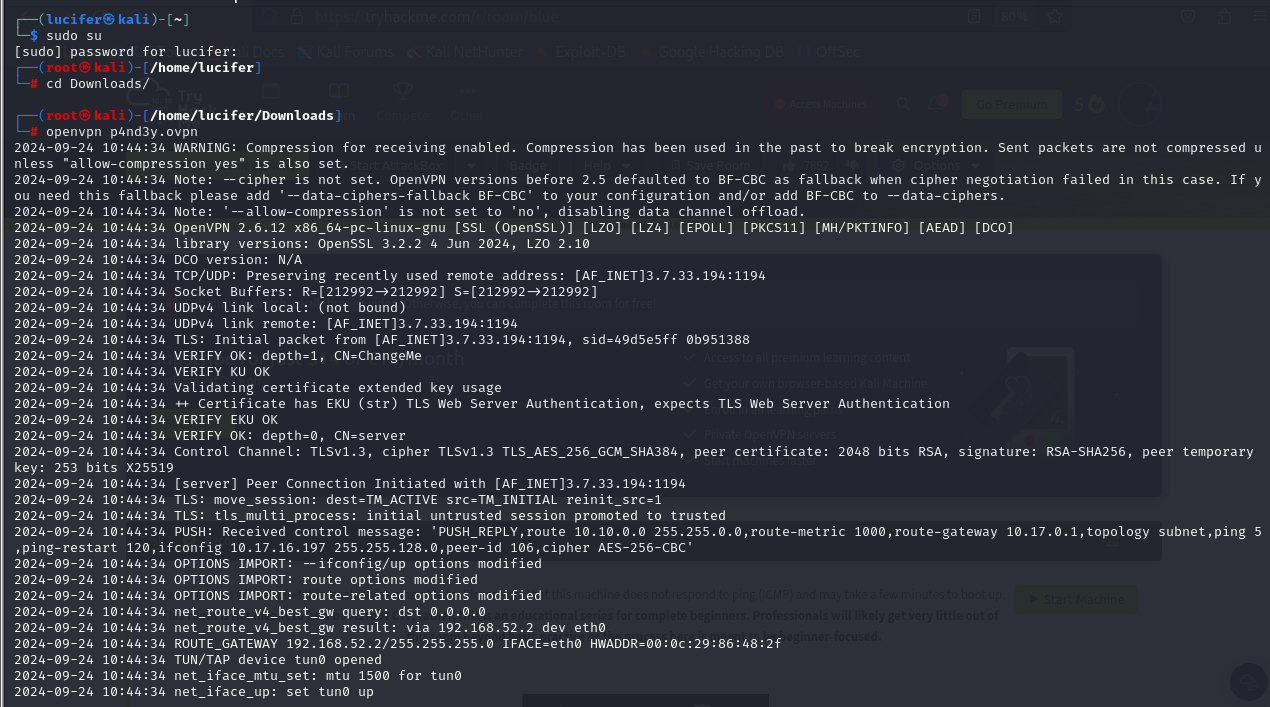
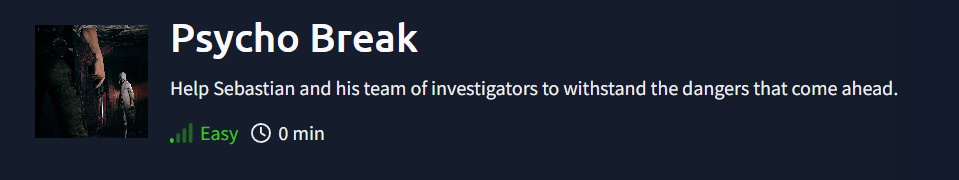
PsychoBreak is a box on tryhackme (<https://tryhackme.com/r/room/psychobreak> ) created by [**shafdo**](https://tryhackme.com/p/shafdo).

Here our **terminal**  is opened.

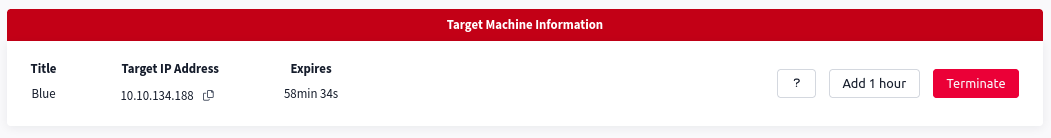


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

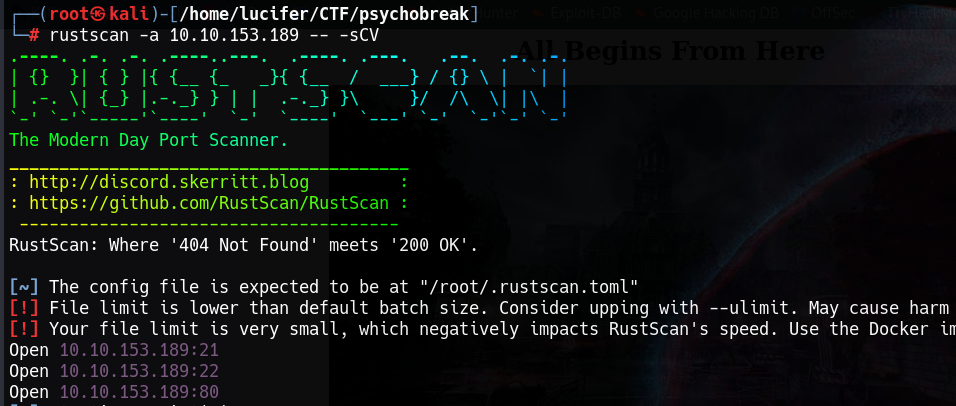


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. 

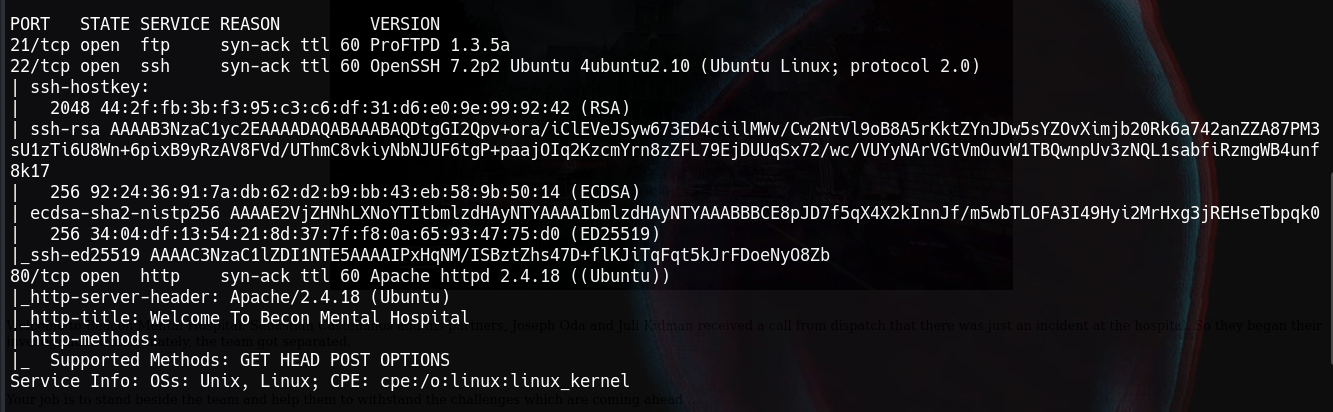
After starting the machine it’ll get one minute to show the ip.



After getting the target ip first thing we’ll do is **nmap** scan to see the open ports and more machine’s info.

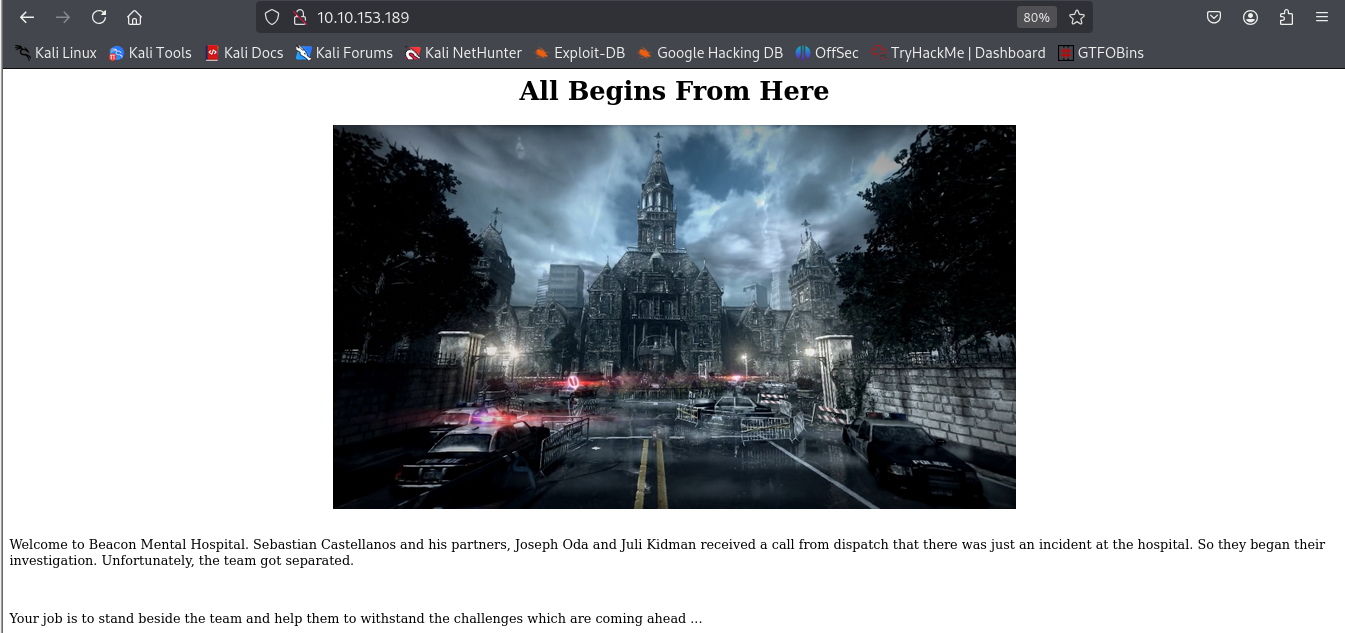
Here I am using **rustscan -a <IP> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

Seems like our scan is completed. Looks like there are total 3 ports open.



One of them is http web server. Now we will explore the webserver.

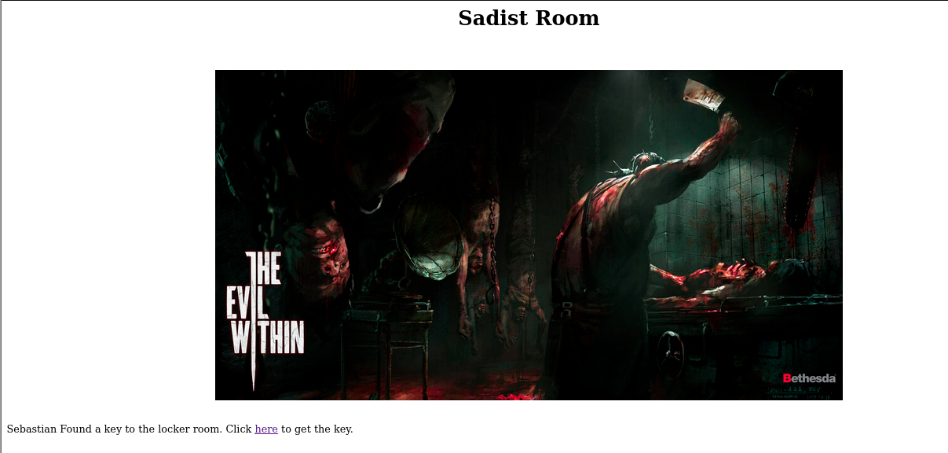
Our main page looks something like:



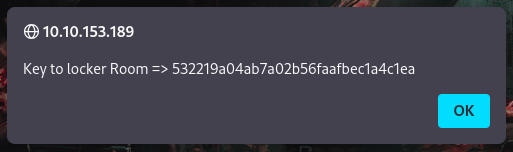
We can see a directory in oir souce code which is **sadistRoom**. We will explore it.



Here we have got another information.



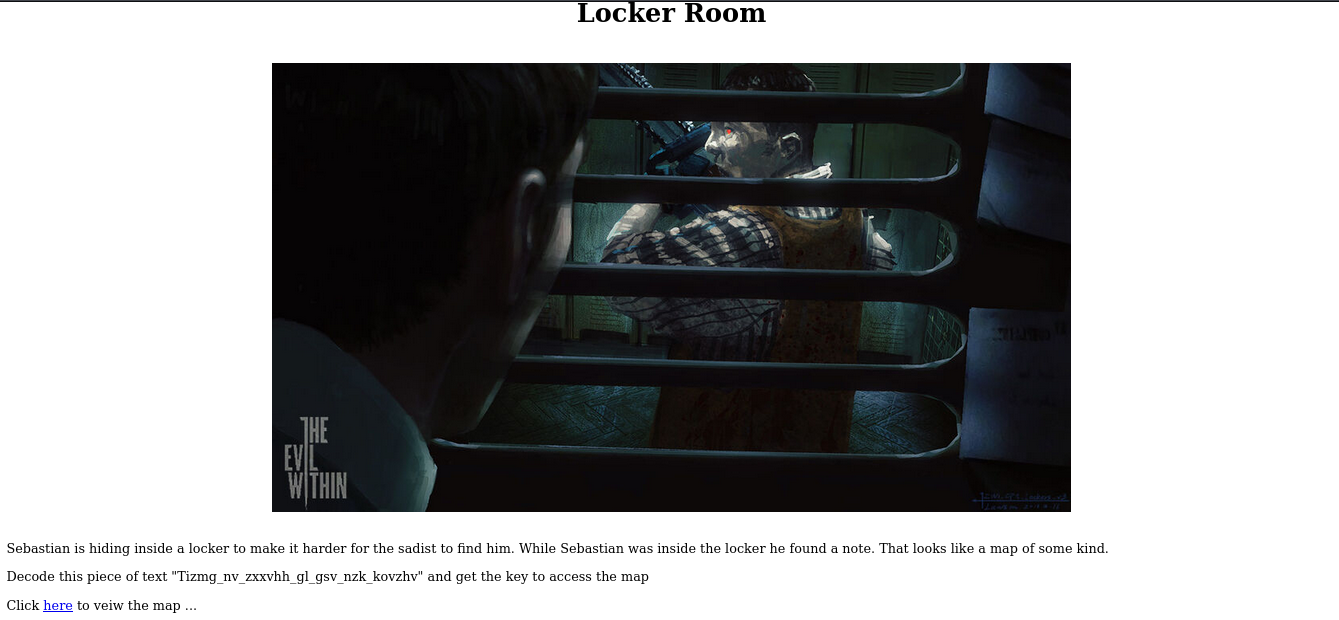
There is a redirect link to another page and it contains a key to the locker room.



We can put it in our next page.

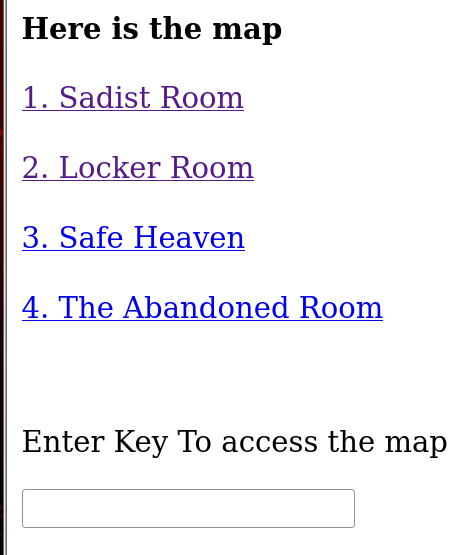


And we enter a new room i.e. locker room.

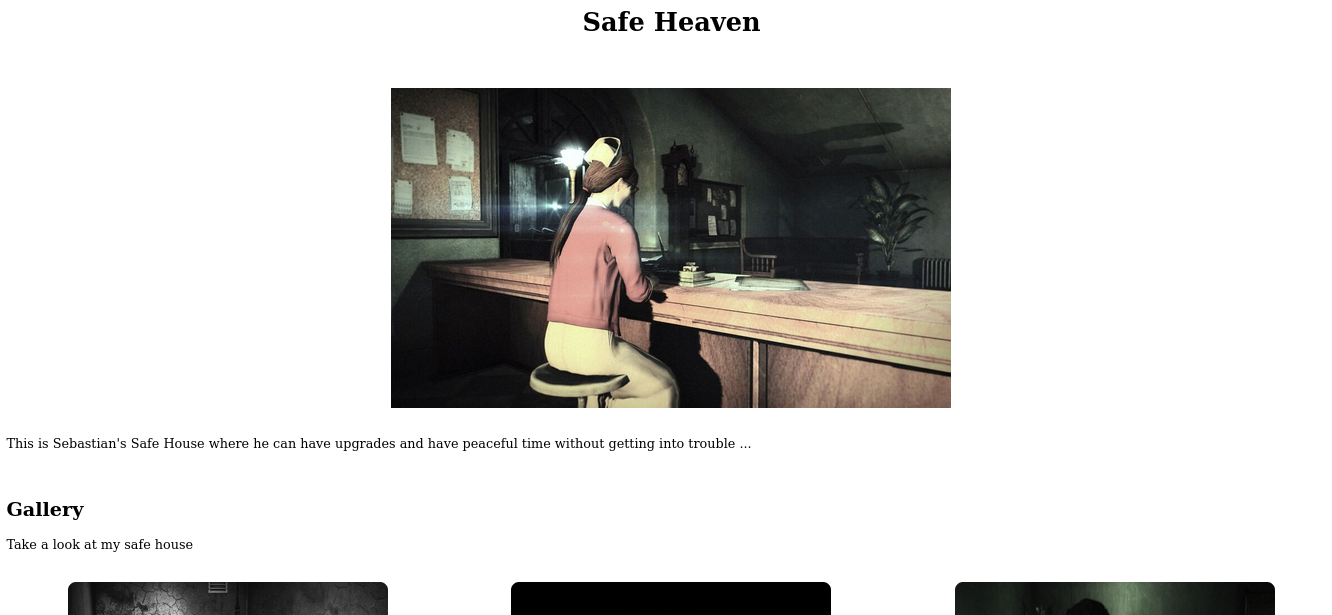


Here it contains a keeper key which is in Atbash cipher. After decoding it we get a key ie. **Grant\_me\_access\_to\_the\_map\_please**

After putting this key, We get access to the safe heaven. There were four rooms in total.



Safe heaven looks like:

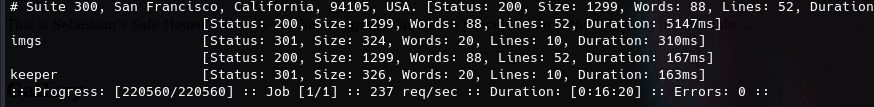


In the source code of this page, we get an information saying:

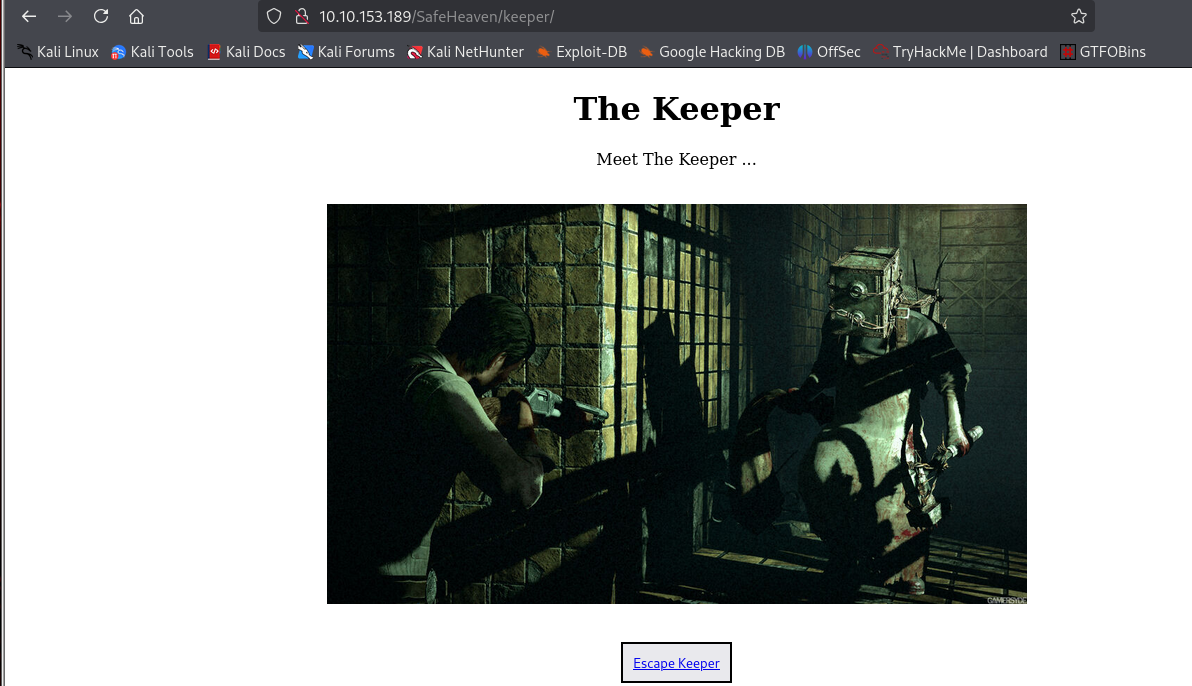


After much exploring I understood that we need to do FUZZING in this page for which we will use **ffuf** tool.





We will get a directory **keeper** after the completion of the process. Now we will go to the keeper directory and look for another key to abandoned room.



When we escape keeper, we see a page containing an image in which we have to do OSINT. We will google the image and find the next key.



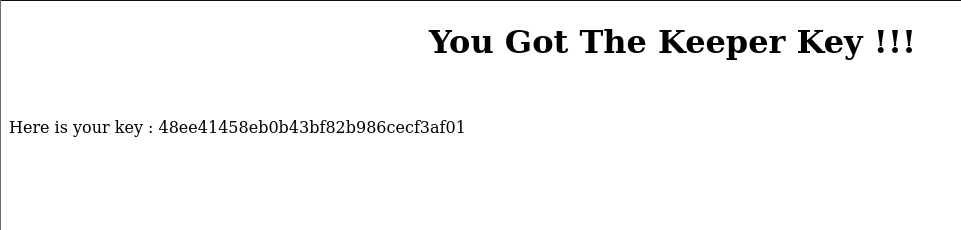
After googling we get that :

The image shows a spiral staircase with metal railings and intricate patterns, possibly from inside a lighthouse or a historical building. Spiral staircases like this are common in lighthouses because they allow for compact, efficient access to multiple levels.

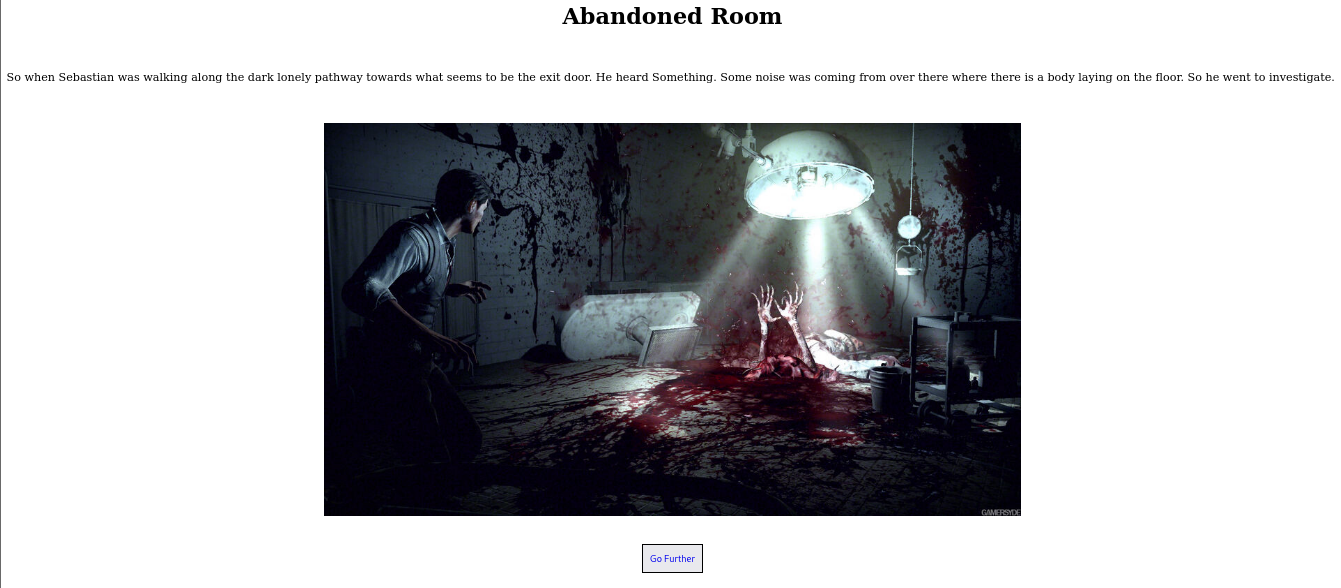
To help identify the exact location, more specific context about the area or additional clues in the image would be needed. This could be an iconic spiral staircase, such as those found in lighthouses like:

* **Ponce Inlet Lighthouse (Florida, USA)**
* **St. Augustine Lighthouse (Florida, USA)**
* **Currituck Beach Lighthouse (North Carolina, USA)**

According to the picture, we get the second option correct and get key to abandoned room.



The abandoned room looks something like this:



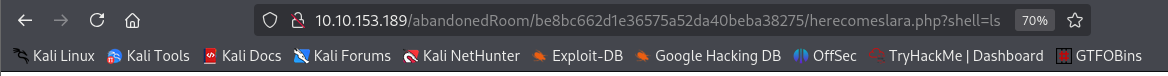
When we’ll go further, We see a page containing the spider lady.



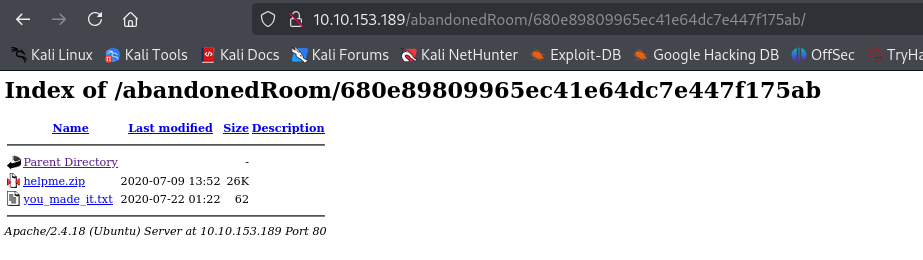
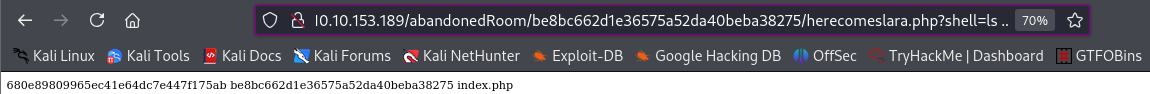
In the source code of the page we get the information regarding shell.



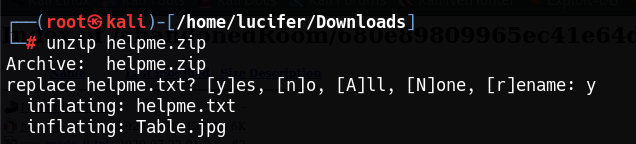
So I tried command injection on the site link using **php?shell=ls** and many more.



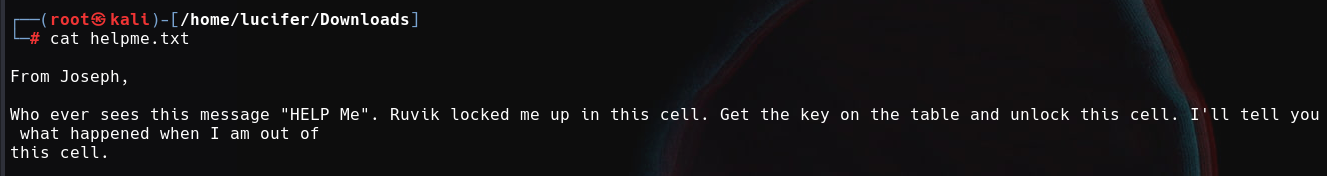
After further exploring and typing **ls ..** I got another directory and after pasting it into the link we get a page containing somethings.



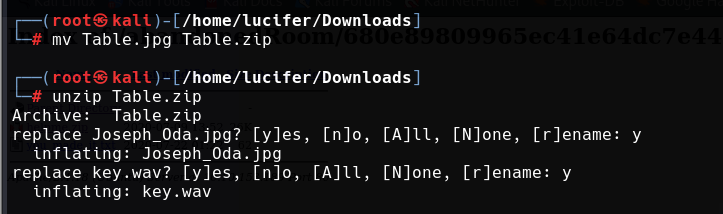
We will download the zip file and extract it.



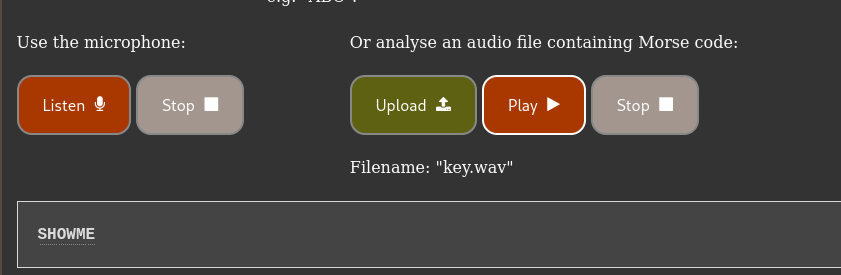
After extracting we get a helpme.txt file and Table.jpg image.



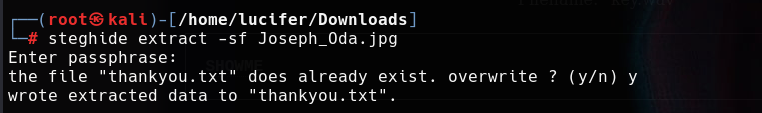
After much recon I got that the Table.jpg file is actually a zip file. So I converted it into Table.zip and extracted it.



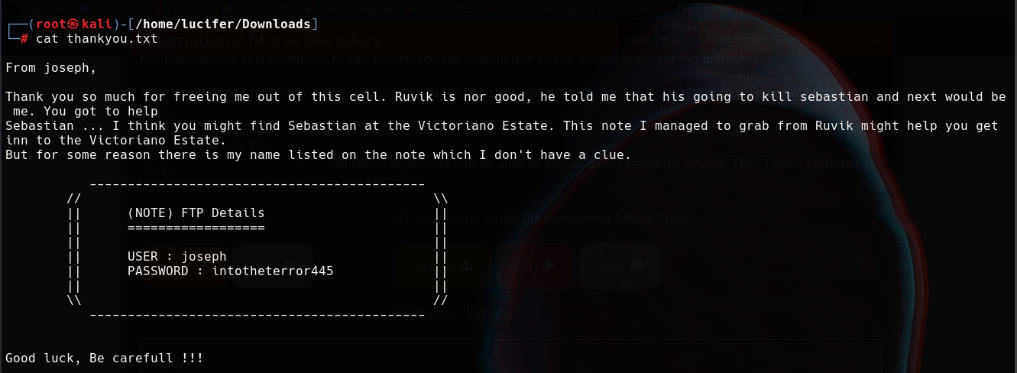
It contains a **key.wav** file which is some kind of morse code file and **Joseph\_0da.jpg** file is a jpg file with steganography in it. So first I got the text from the audio file from a morse code converting site.



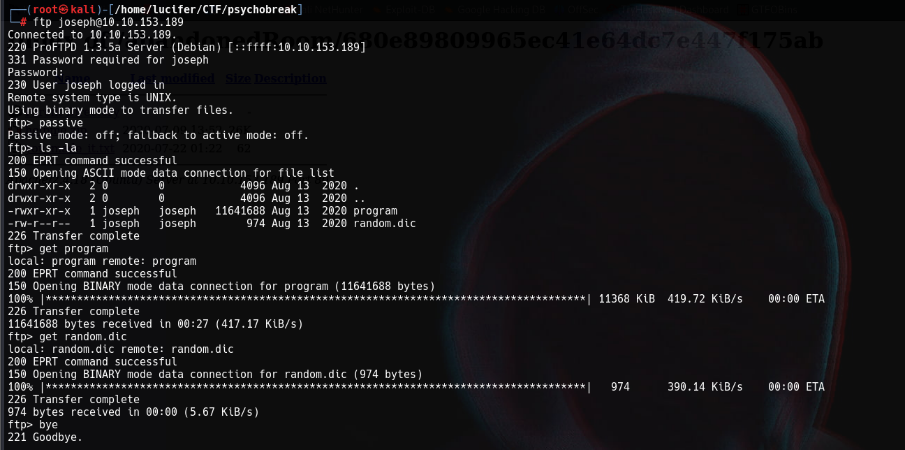
Now as we got a word it could be passphrase of the image file to open it. I used **steghide** to extract the files from the image with the passphrase **SHOWME.**



It contains a **thankyou.txt** file. When we read this file we get credentials for **ftp** for user **joseph.**



Following the credentials we will log into ftp using command **ftp joseph@ip** and get the files present there.



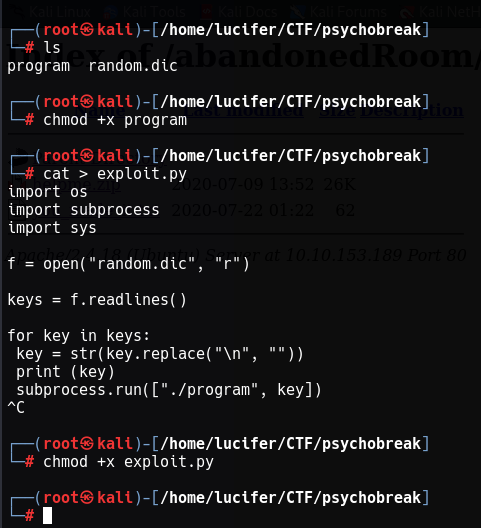
We will get a **program** file and **random.dic** which is dictionary file. After much recon I got that the there is some sort of code in the program which needs a phrase from the random.dic file to execute. So we will write a simple python code for the program and run it. We will wait until the program gets the right code.

The python script will be something like:

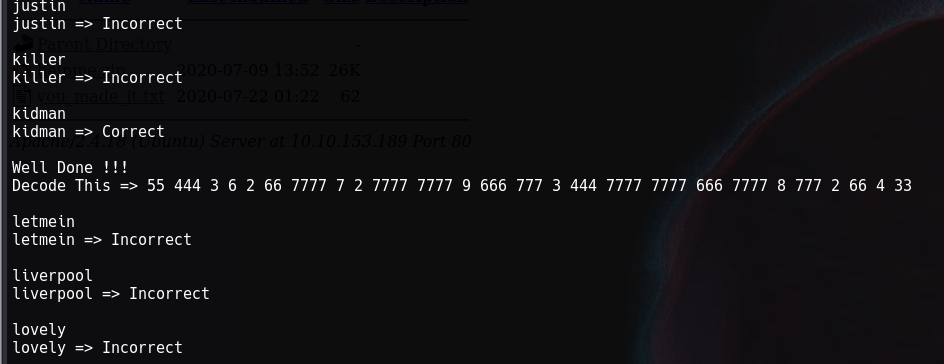


We will run it in the same directory where program and dic file is stored.

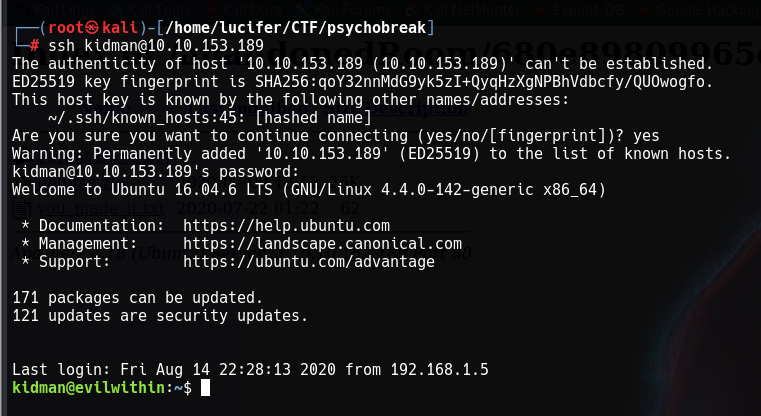
**Note: Change permissions of the program file**



Now we will execute the **exploit.py** file using **python exploit.py** and we will wait until we get the correct combination.

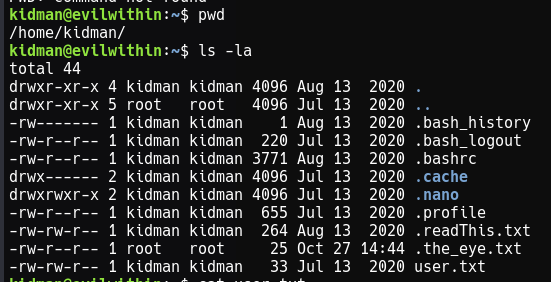


After getting the combination we get some sort of code which is in phone keypad cipher format. We will decode it and get **KIDMANSPASSWORDISSOSTRANGE.** It contains credentials of user **kidman** which we can use for ssh login. The username will be kidman and password will be the decoded code.

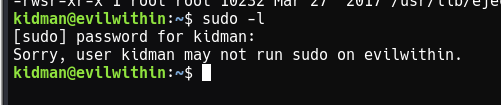


And we got a successful login!!

Now we will get the user.txt file from the user’s directory.

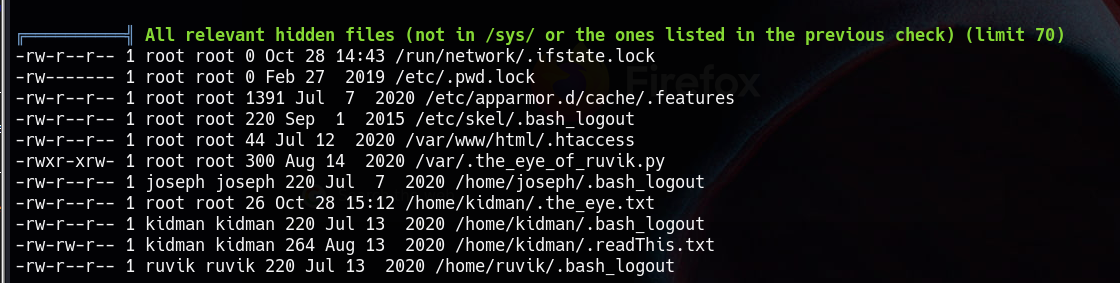


For the root.txt file we need to escalate privileges. We will run **sudo -l**  as we know user’s password.

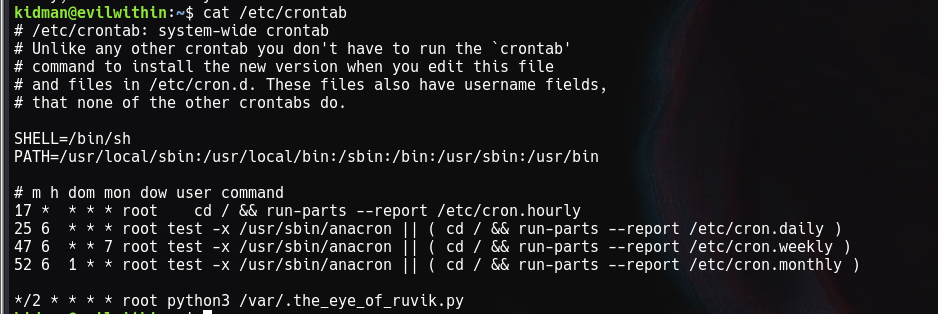


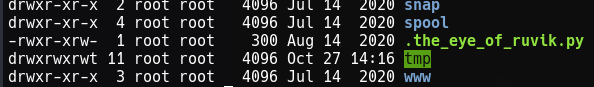
We get that user kidman can’t run sudo. So we will explore different measures to get root.

After much recon and running **linpeas** on target system I found a suspicious python script which had root permissions and permissions to edit it.



After sometime I located it in **/etc/crontab** file.



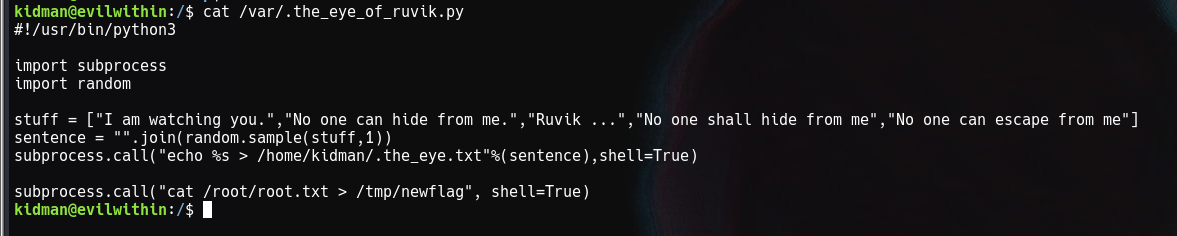


It contains a file which has permission to edit. So we will edit the **.the\_eye\_of\_ruvik.py** file. To do this we will first make a folder in **/tmp** directory and give it needed permissions.



Now we will add some script in the **.the\_eye\_of\_ruvik.py file** which is:





As we know the file is running, we are adding a subprocess in the code to output the **root.txt** file in the new directory we formed **newflag.**

Now we will wait for sometime to run the script automatically and give us the output file. After sometime we will get the **root.txt** in the **newflag** file.

