

Report -1

Room: psychobreak

Progress : 76%

TASK 1: RECON

Tools: nmap

```
root@ip-10-10-49-169:~# nmap -O 10.10.138.34
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-11 17:41 BST
Nmap scan report for ip-10-10-138-34.eu-west-1.compute.internal (10.10.138.34)
Host is up (0.00058s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:9B:9C:EE:4E:B5 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/11%OT=21%CT=1%CU=33576%PV=Y%DS=1%DC=D%G=Y%M=029B9C%T
OS:M=68713ED5%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=Z%CI=I%II=I
OS:%TS=8)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11N
OS:W7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=6
OS:8DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=Y%DFI=N%T=40%CD=S)
```

Result: Open ports: 21 (FTP), 22 (SSH), 80 (HTTP)

This room is based on a video game called evil within. I am a huge fan of this game. So I decided to make a CTF on it. With my storyline :). Your job is to help Sebastian and his team of investigators to withstand the dangers that come ahead.

[Hints are provided as you progress through the challenge]

The VM might take up to 2-3 minutes to fully boot up.

Answer the questions below

Deploy the machine.

No answer needed ✓ Correct Answer

How many ports are open?

3 ✓ Correct Answer

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

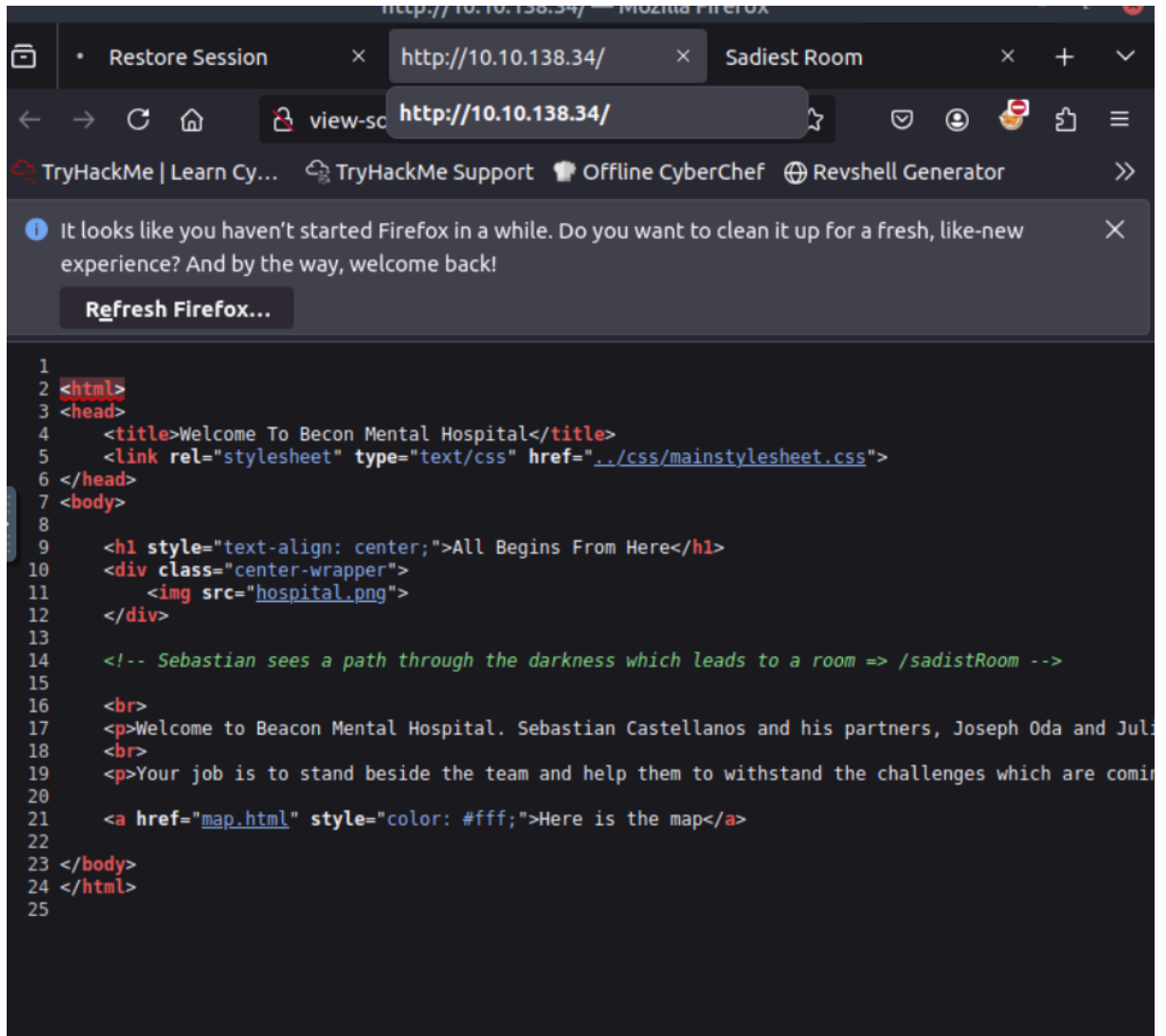
ubuntu ✓ Correct Answer

TASK 2: WEB

Tools: Web browser, go buster, Developer tools / View page source

2.1 Explore HTTP service

- Visit <http://<target-ip>>, view source
- Find hidden link to </sadistRoom>
- Click it to reach the "Locker Room"



```

1
2 <html>
3 <head>
4   <title>Welcome To Beacon Mental Hospital</title>
5   <link rel="stylesheet" type="text/css" href="css/mainstylesheet.css">
6 </head>
7 <body>
8
9   <h1 style="text-align: center;">All Begins From Here</h1>
10  <div class="center-wrapper">
11    
12  </div>
13
14  <!-- Sebastian sees a path through the darkness which leads to a room => /sadistRoom -->
15
16  <br>
17  <p>Welcome to Beacon Mental Hospital. Sebastian Castellanos and his partners, Joseph Oda and Jul
18  <br>
19  <p>Your job is to stand beside the team and help them to withstand the challenges which are comin
20
21  <a href="map.html" style="color: #fff;">Here is the map</a>
22
23 </body>
24 </html>
25

```

2.2 Atbash Cipher Challenge

- Encrypted string found: `Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv`

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_zxxvhh_gl_gsv_nzk_kovzhv`" and get the key to access the map

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

- Use CyberChef

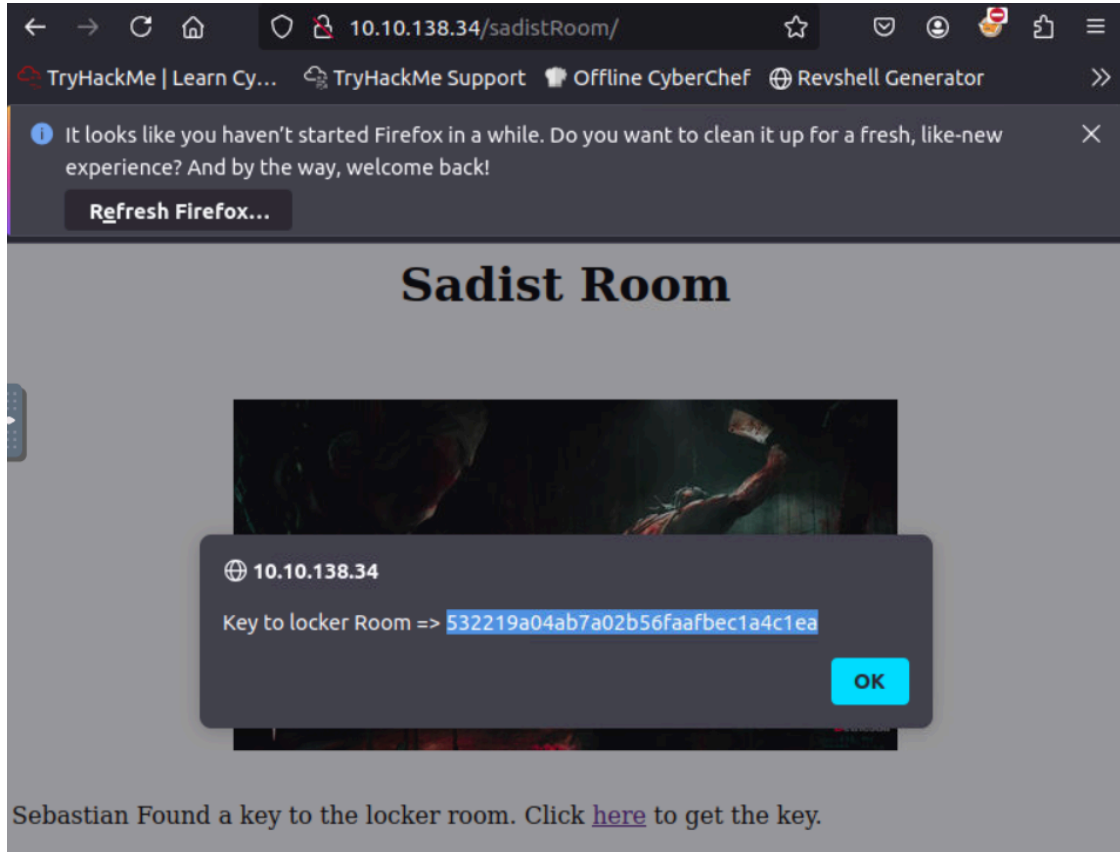
The screenshot shows the CyberChef interface. On the left, under the 'Recipe' tab, the 'Atbash Cipher' recipe is selected. On the right, the 'Input' field contains the encrypted string `Tizmg_nv_zxxvhh_gl_gsv_nzk_kovzhv`. Below the input, the 'Output' field displays the decoded string `Grant_me_access_to_the_map_please`. The interface also includes icons for saving, deleting, and pausing the recipe.

- Decoded: `Grant_me_access_to_the_map_please`

- Submit as key → unlocked map

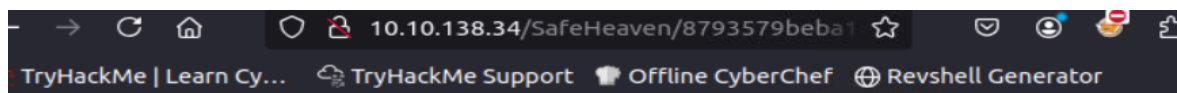
2.3 Discover Keeper Challenge

- Use Gobuster to enumerate `/safeheaven`



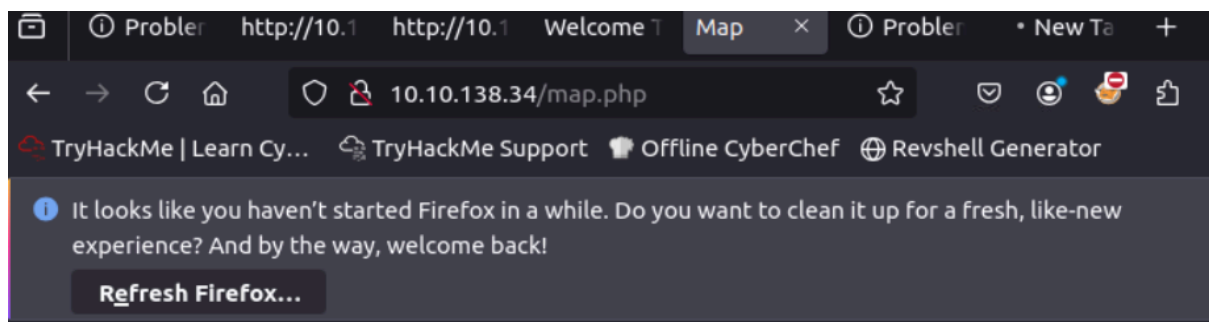
Command: `gobuster dir -u http://<target-ip>/safeheaven -w /usr/share/wordlists/dirb/common.txt`

- Find `/keeper/`, visit → shows image puzzle
- Reverse image search using **Google Images** or **TinEye**
- Answer: `St. Augustine Lighthouse` → gives **Keeper Key**





You Got The Keeper Key !!!

Here is your key : 48ee41458eb0b43bf82b986cecf3af01



Enter Key To access the map

Access to the map please

Task 2  Web 

Here comes the web.

Answer the questions below

Key to the locker room

532219a04ab7a02b56faafbec1a4c1ea

✓ Correct Answer

Key to access the map

Grant_me_access_to_the_map_please

✓ Correct Answer

The Keeper Key


48ee41458eb0b43bf82b986cecf3af01

✓ Correct Answer

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

you_made_it

✓ Correct Answer

 Hint

Limited Remote Code Execution

Tools:

- Go to `/abandonedRoom?shell=ls ..`
- Try: `curl "http://<target-ip>/abandonedRoom?shell=ls%20.."`

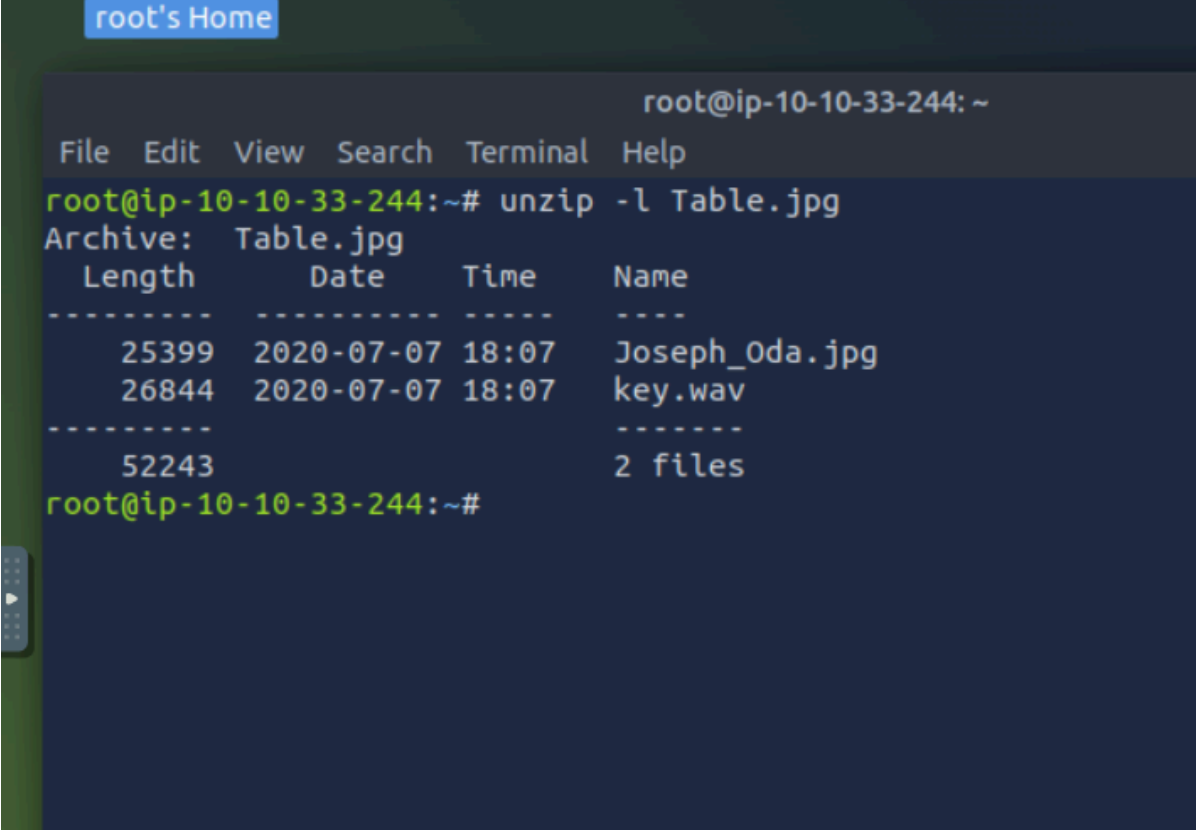
Analyzing the Download

Files: `helpme.zip`

Steps:

1. Extract `helpme.zip`
2. We'll get:
 - `Joseph_Oda.jpg`

- key.wav



```
root's Home
root@ip-10-10-33-244: ~
File Edit View Search Terminal Help
root@ip-10-10-33-244:~# unzip -l Table.jpg
Archive:  Table.jpg
  Length      Date    Time    Name
-----
 25399  2020-07-07  18:07  Joseph_Oda.jpg
 26844  2020-07-07  18:07  key.wav
-----
 52243
2 files
root@ip-10-10-33-244:~#
```

3. Use the Morse audio decoder on key.wav → get password: SHOWME
4. Use steghide to extract data from the image:

Username: joseph

Password: intotheterror445

```
root@ip-10-10-33-244: ~
File Edit View Search Terminal Help
Archive: /root/Downloads/helpme.zip
Length      Date       Time       Name
-----
191 2020-07-07 18:43 helpme.txt
-----
191
1 file
root@ip-10-10-33-244:~# ^C
root@ip-10-10-33-244:~# unzip -l ~/Downloads/helpme.zip helpme.txt
Archive: /root/Downloads/helpme.zip
Length      Date       Time       Name
-----
191 2020-07-07 18:43 helpme.txt
-----
191
1 file
root@ip-10-10-33-244:~# unzip -p ~/Downloads/helpme.zip 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.

root@ip-10-10-33-244:~#
```

FTP Enumeration

Tools:

- ftp or lftp

Commands: ftp <target-ip>

- Login with joseph / intotheterror445
- Download program and random.dic

Index of / abandonedRoom/680e89809965ec41e64dc

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	

Apache/2.4.18 (Ubuntu) Server at 10.10.68.94 Port 80

Task 3 Help Mee

Get that poor soul out of the cell.

Answer the questions below

Who is locked up in the cell?

joseph

✓ Correct Answer

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

SHOWME

✓ Correct Answer

What is the FTP Username

joseph

✓ Correct Answer

What is the FTP User Password

intotheterror445

✓ Correct Answer