Biohazard

> **Instructions**
> Welcome to Biohazard room, a puzzle-style CTF. Collecting the item, solving the puzzle and escaping the nightmare is your top priority. Can you survive until the end?

Because this room is a type of **puzzle-style CTF** → I will follow up the questions instead of going through normal phases of penetration testing. Let's start!

Deploy the machine and start the nightmare

No answer needed

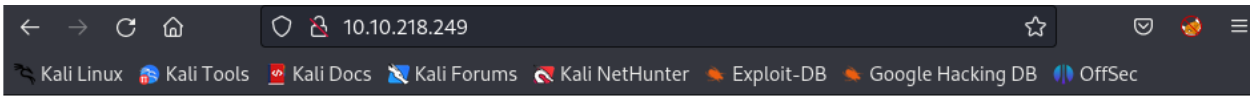
How many open ports?

Run `nmap` and you will find the answer ⇒ **3**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-22 09:53 EDT
Warning: 10.10.85.235 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.85.235
Host is up (0.19s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

What is the team name in operation

Visit the main page of the **http** service (port `80`):



The nightmare begin

July 1998, Evening

The STARS alpha team, Chris, Jill, Barry, Weasker and Joseph is in the operation on searching the STARS bravo team in the nortwest of Racoon city.

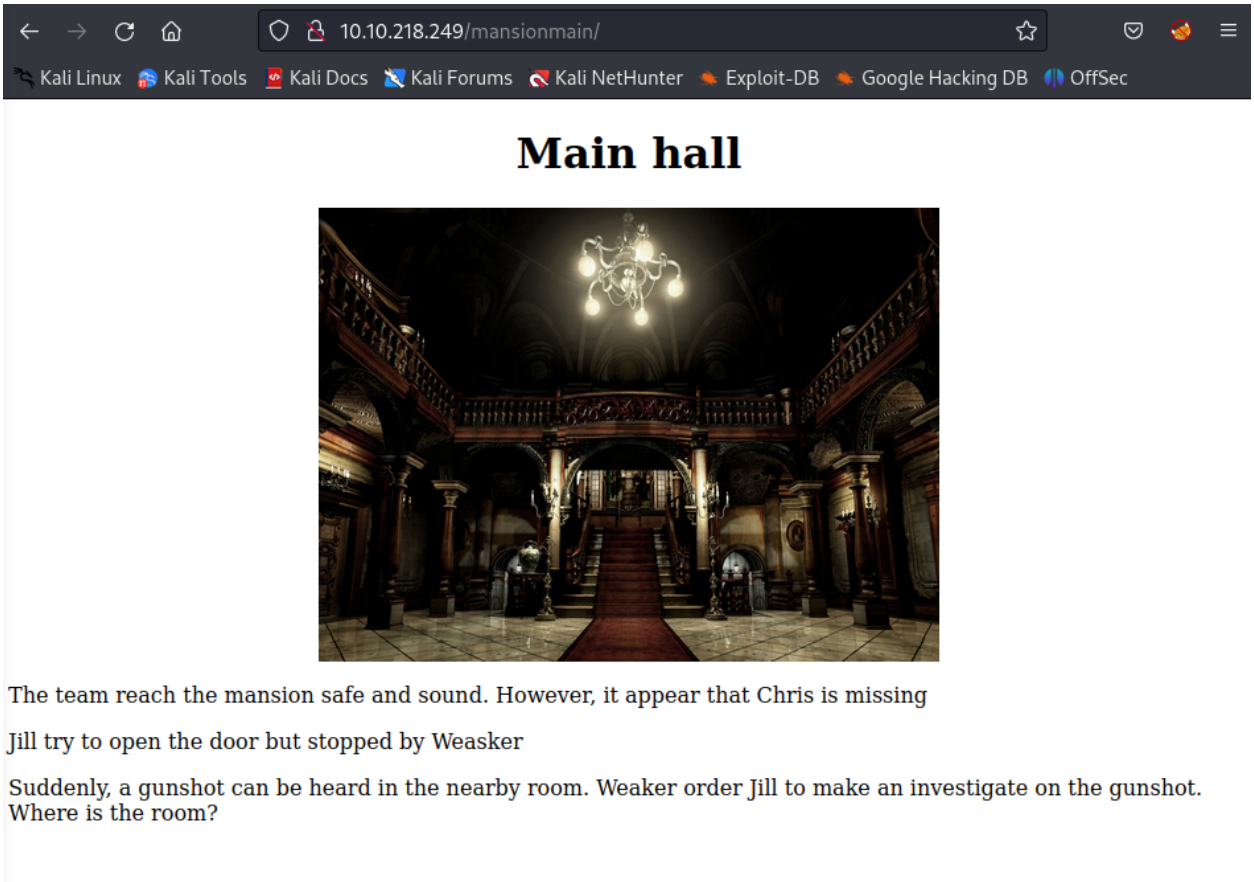
Unfortunately, the team was attacked by a horde of infected zombie dog. Sadly, Joseph was eaten alive.

The team decided to run for the nearby mansion and the nightmare begin.....

⇒ The answer is: **The STARS alpha team**

What is the emblem flag

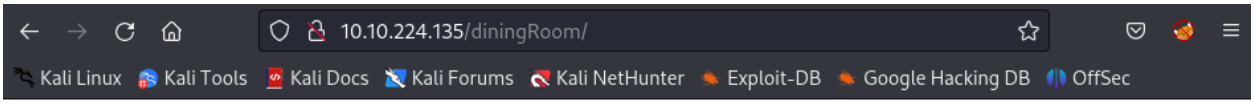
Click on the `mansion` and follow up its link:



Press `Ctrl + U` or right-click and view the Page's Source:

```
<!doctype html>
        <head>
                <title>Main hall</title>
                <h1 align="center">Main hall</h1>
        </head>

        <body>
        <img alt="mainhall" src="../images/Mainhall12.jpg" style="display: block;margin-left: auto;margin-right: auto; width: 50%;"/>

        <p>The team reach the mansion safe and sound. However, it appear that Chris is missing</p>
  <p>Jill try to open the door but stopped by Weasker</p>
        <p>Suddenly, a gunshot can be heard in the nearby room. Weaker order Jill to make an investigate on the gunshot. Where is the roo
m?</p>
  <!-- It is in the /diningRoom/ -->
        </body>

</html>
```

Notice at the comment line → Go to the `/diningRoom`



Dining room

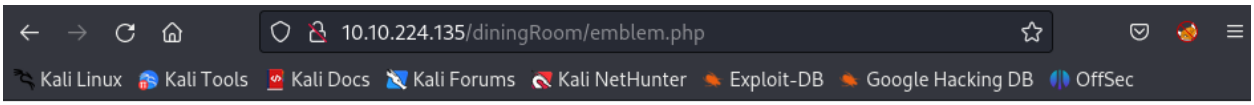
After reaching the room, Jill and Barry started their investigation

Blood stein can be found near the fireplace. Hope it is not belong to Chris.

After a short investigation with barry, Jill can't find any empty shell. Maybe another room?

There is an emblem on the wall, will you take it? YES

Click on **YES**



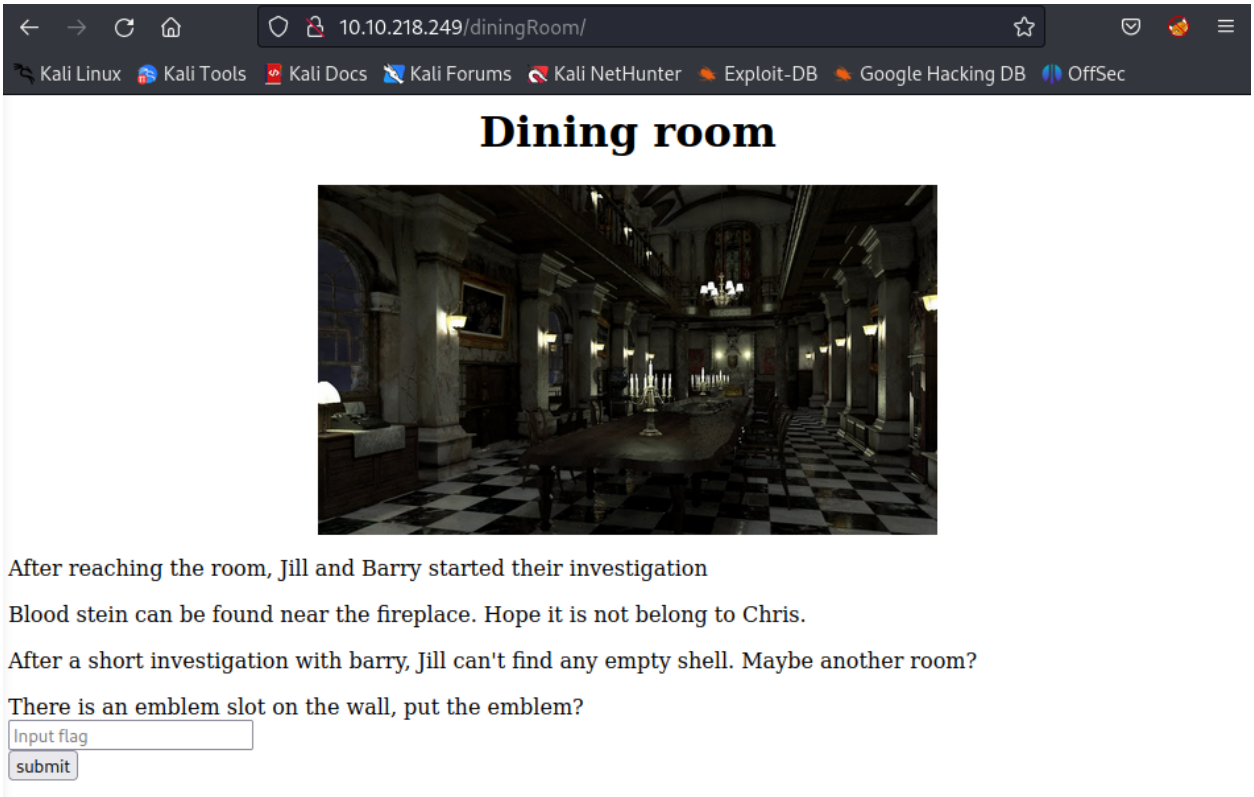
emblem{fec832623ea498e20bf4fe1821d58727}

Look like you can put something on the emblem slot, refresh /diningRoom/

Answer: **emblem{fec832623ea498e20bf4fe1821d58727}**

What is the lock pick flag?

Get back and refresh the page:



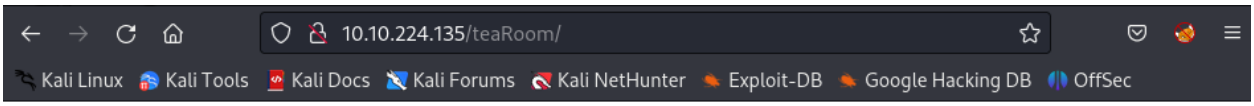
Enter the previous `emblem` flag but it's not correct. View the page source again and notice at the comment line:

```
<!-- SG93IGFib3V0IHRoZSAvdGVhUm9vbS8= -->
```

Decode the string with **base64**:

```
How about the /teaRoom/
```

Route to the `/teaRoom`



The nightmare begin

What the freak is this! This doesn't look like a human.

The undead walk toward Jill. Without wasting much time, Jill fire at least 6 shots to kill that thing

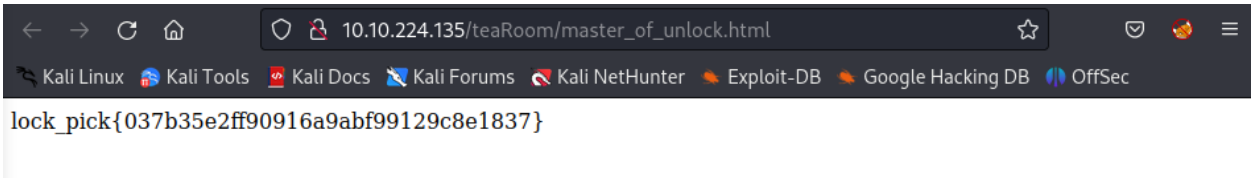
In addition, there is a body without a head laying down the floor

After the investigation, the body belong to kenneth from Bravo team. What happened here?

After a jiff, Barry broke into the room and found out the truth. In addition, Barry give Jill a Lockpick.

Barry also suggested that Jill should visit the /artRoom/

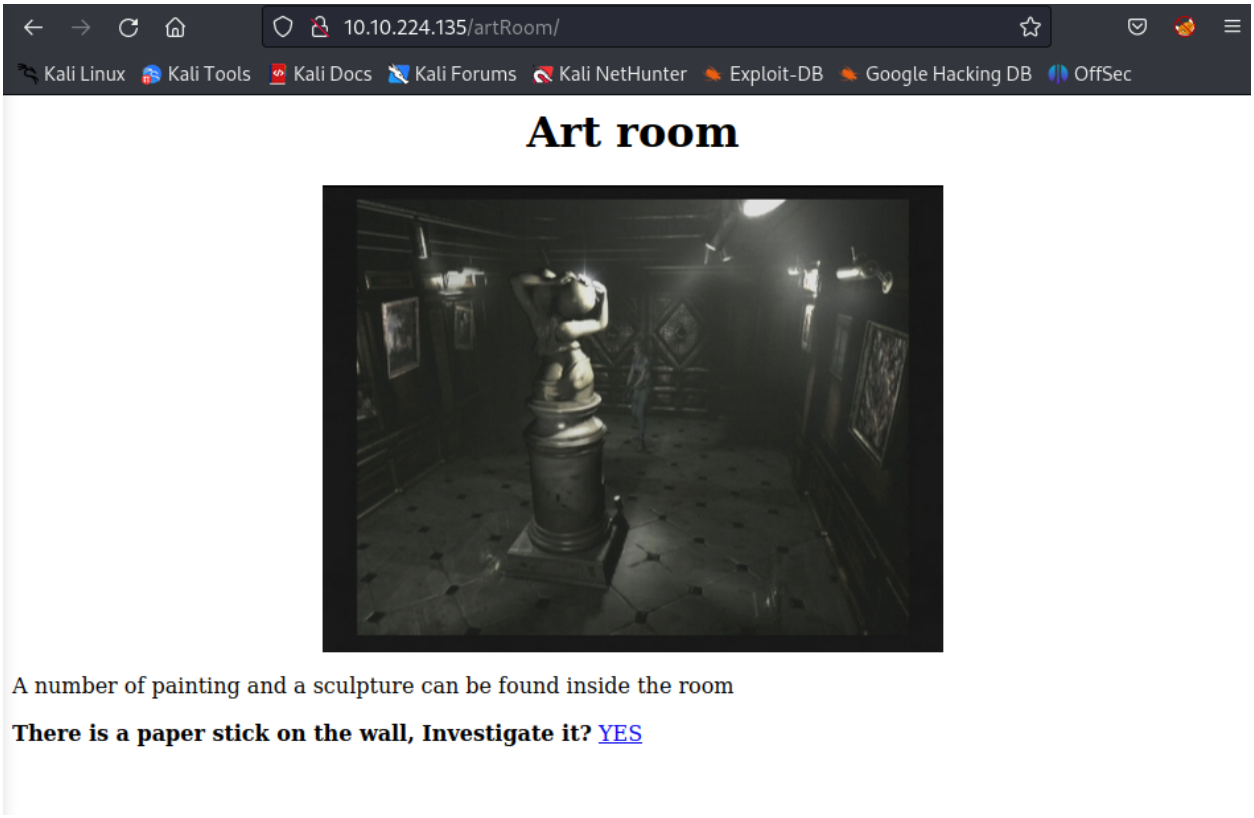
Click on the **Lockpick** and save the flag:

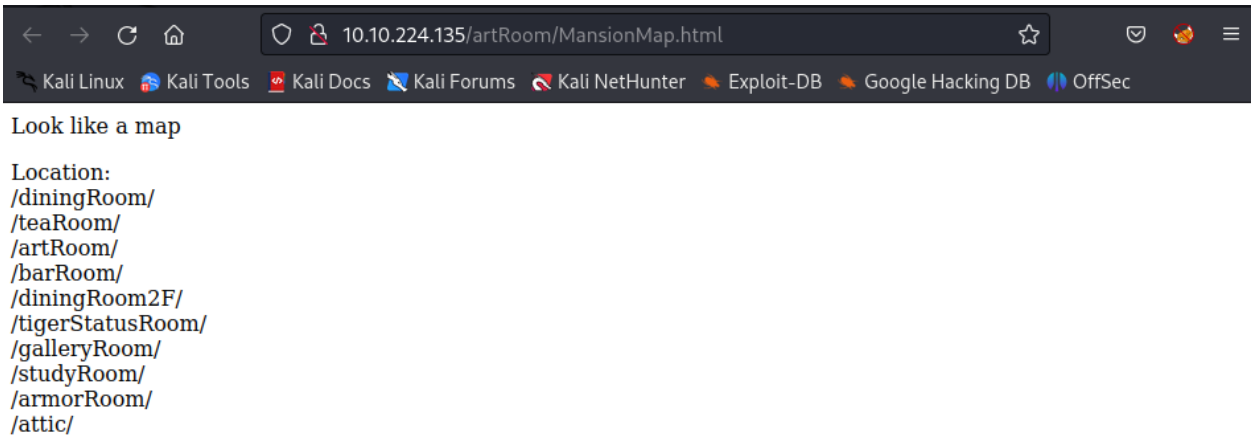


Asnwer: **lock_pick{037b35e2ff90916a9abf99129c8e1837}**

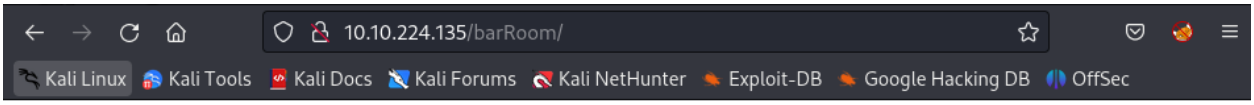
What is the music sheet flag?

Visit the `/artRoom`





Save the list for easier following up all the directions. Then move on with the `/barRoom/`



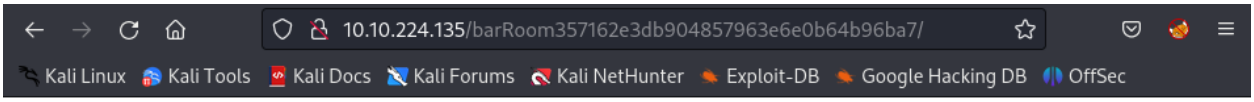
Bar room entrance

Look like the door has been locked

It can be open by a **lockpick**

Enter flag submit

Enter the previous **lockpick** flag:



Bar room

what a messy bar room

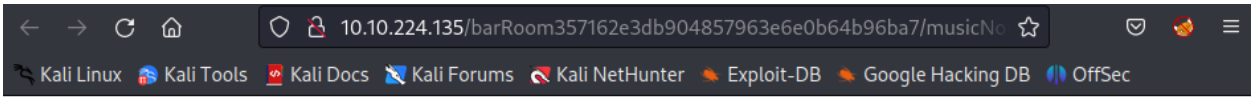
A piano can be found in the bar room

Play the piano?

Enter flag submit

Also, you found a note that written as "moonlight somata", read it? READ

Click on **READ**:



Look like a music note

NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5

Decode the string with **base32**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ echo "NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5" | base32 -d
music_sheet{362d72deaf65f5bdc63daece6a1f676e}
```

Answer: **music_sheet{362d72deaf65f5bdc63daece6a1f676e}**

What is the gold emblem flag?

Get back to the browser and enter the **music sheet** flag:

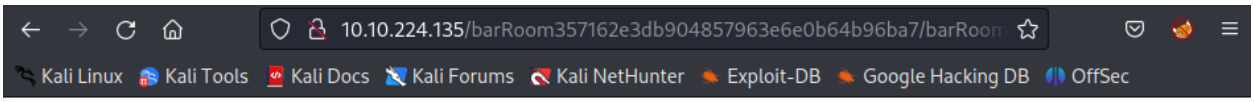
what a messy bar room

A piano can be found in the bar room

Play the piano?

music_sheet{362d72deaf65f5l submit

Also, you found a note that written as "moonlight somata", read it? READ

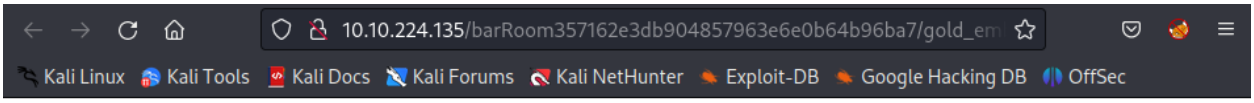


Secret bar room

There is a gold emblem embedded on the wall

Will you take it? YES

Click YES:



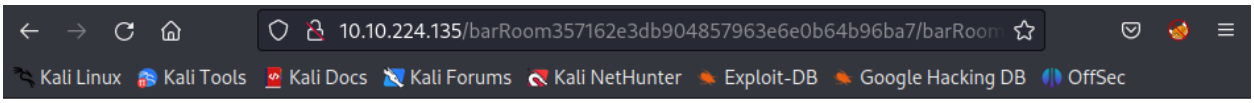
gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}

Look like you can put something on the emblem slot, refresh the previous page

Answer: **gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}**

What is the shield key flag

Go back and refresh the **Secret bar room** page then enter the flag:

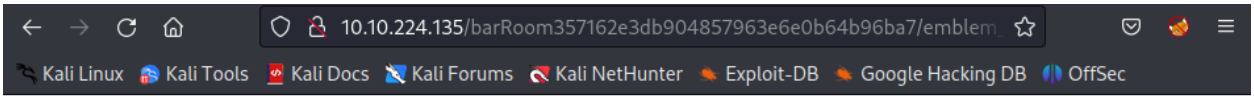


Secret bar room

There is an emblem slot on the wall, put the emblem?

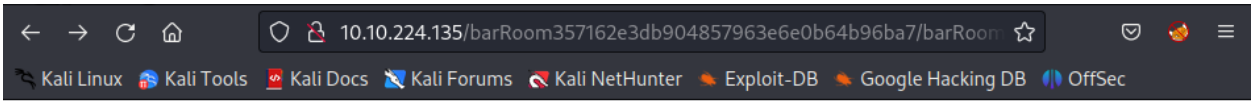
gold_emblem{58a8c41a9d08l

submit



Nothing happen

The **gold_emblem** key is not the right one, remember the first **emblem** key? Use it!

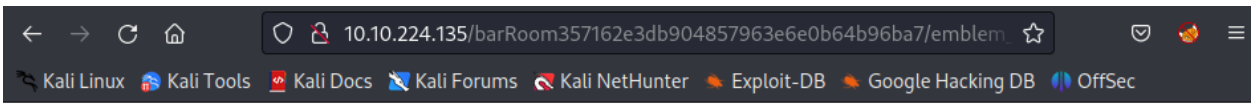


Secret bar room

There is an emblem slot on the wall, put the emblem?

emblem{fec832623ea498e20l

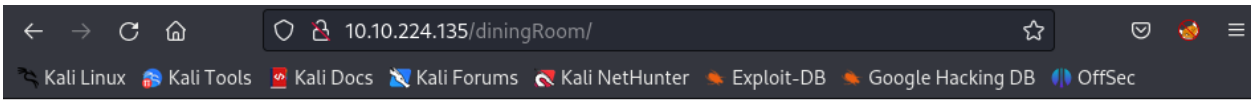
submit



rebecca

The `rebecca` might be an username or a key for decrypt/decode something. Save it for later use.

Go back to the first found room `/diningRoom/` and enter the **gold_emblem** key:



Dining room

After reaching the room, Jill and Barry started their investigation

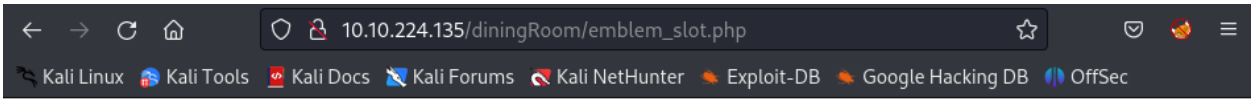
Blood stein can be found near the fireplace. Hope it is not belong to Chris.

After a short investigation with barry, Jill can't find any empty shell. Maybe another room?

There is an emblem slot on the wall, put the emblem?

gold_emblem{58a8c41a9d08b

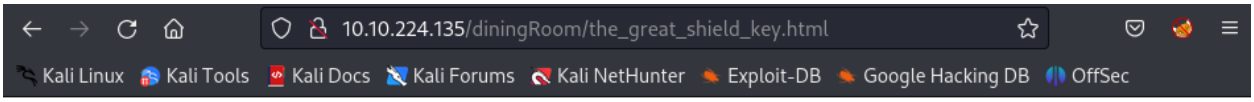
submit



klfvg ks r wimgnd biz mpuiui ulg fiemok tqod. Xii jvmc tbkg ks tempgf tyi_hvgct_jljinf_kvc

Decode the string with **Vigenere Cipher** and the key is **rebecca**:

Go to `/the_great_shield_key.html`:

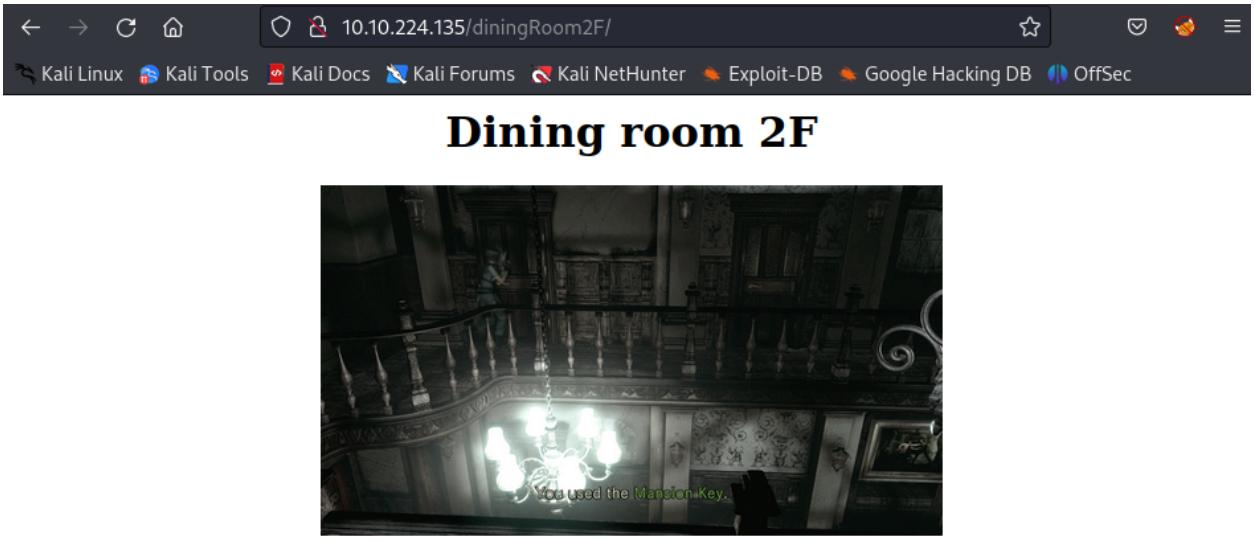


shield_key{48a7a9227cd7eb89f0a062590798cbac}

Answer: **shield_key{48a7a9227cd7eb89f0a062590798cbac}**

What is the blue gem flag?

Open the list `MansionMap` and move on to the next one `/diningRoom2F/`



Once Jill reach the room, she saw a tall status with a shiining blue gem on top of it. However, she can't reach it

View it's source:

```
<html>
        <head>
                <title>Dining room 2F</title>
                <h1 align="center">Dining room 2F</h1>
        </head>

        <body>
        <img alt="dining room 2F" src="../images/Vlcsnap-2015-01-26-08h54m37s183.png" style="display: block;margin-left: auto;margin-righ
t: auto; width: 50%;"/>

  <p>Once Jill reach the room, she saw a tall status with a shiining blue gem on top of it. However, she can't reach it</p>
  <!-- Lbh trg gur oyhr trz ol chfuvat gur fgnghf gb gur ybjre sybbe. Gur trz vf ba gur qvavatEbbz svefg sybbe. Ivfvg fnccuver.ugzy -->
        </body>

</html>
```

Decode the comment text with **ROT13:**

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ hURL --rot13 -f diningRoom2F_comment.txt

Original file   :: diningRoom2F_comment.txt
ROT13 decoded   :: You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphir
e.html
```

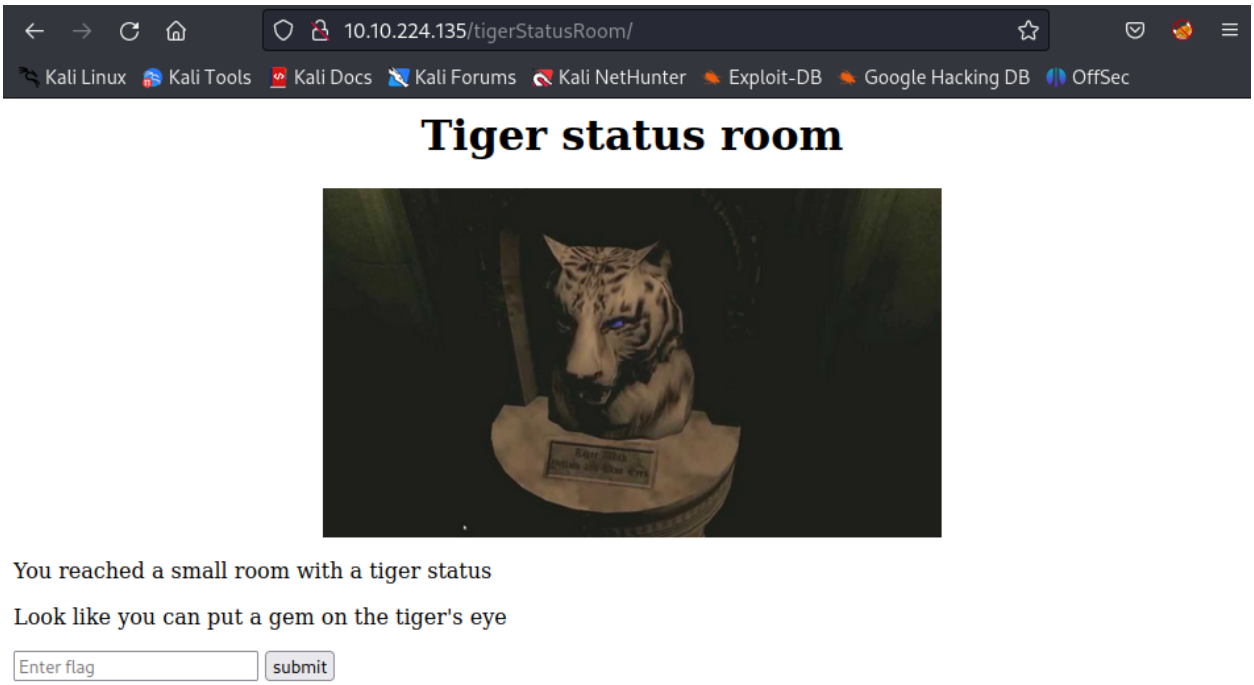
Visit the `sapphire.html` from the `/diningRoom/`:

blue_jewel{e1d457e96cac640f863ec7bc475d48aa}

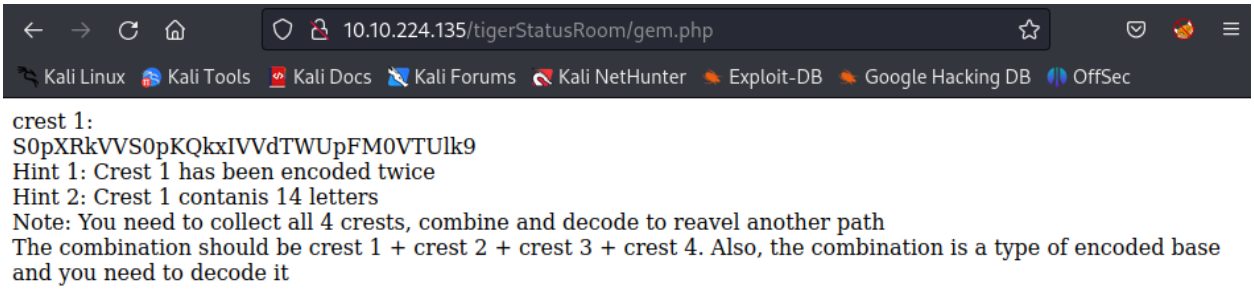
Answer: **blue_jewel{e1d457e96cac640f863ec7bc475d48aa}**

What is the FTP username? What is the FTP password?

Take a look at the list of rooms again (`MansionMap.html`) → Visit the room `/tigerStatusRoom/`



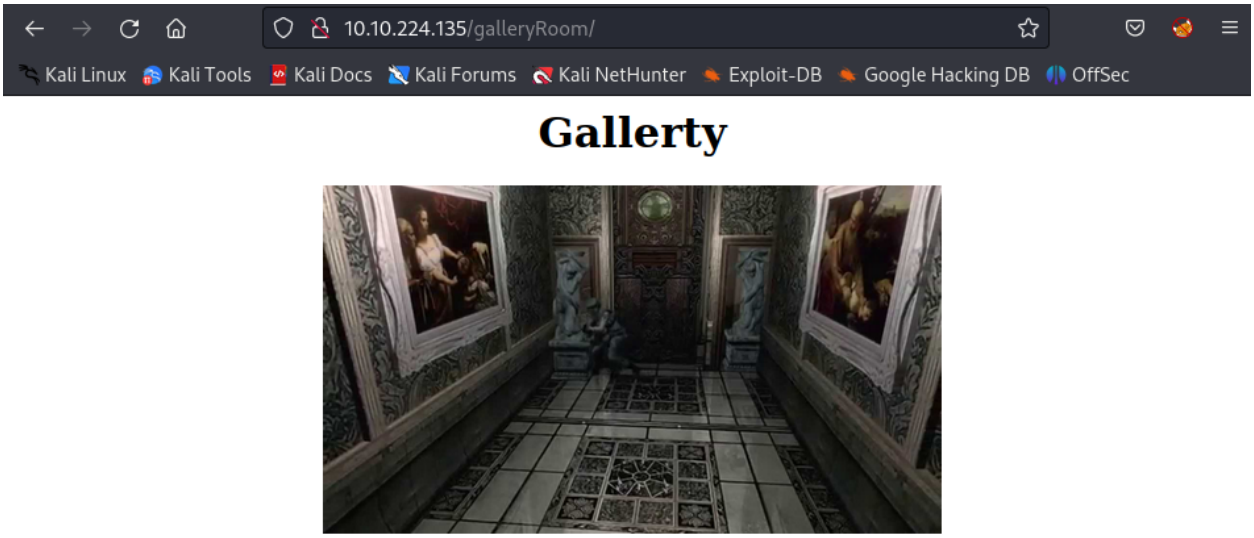
gem is a kind of jewel and notice at the tiger's eye in the picture with blue color → Enter the **blue_jewel** flag:

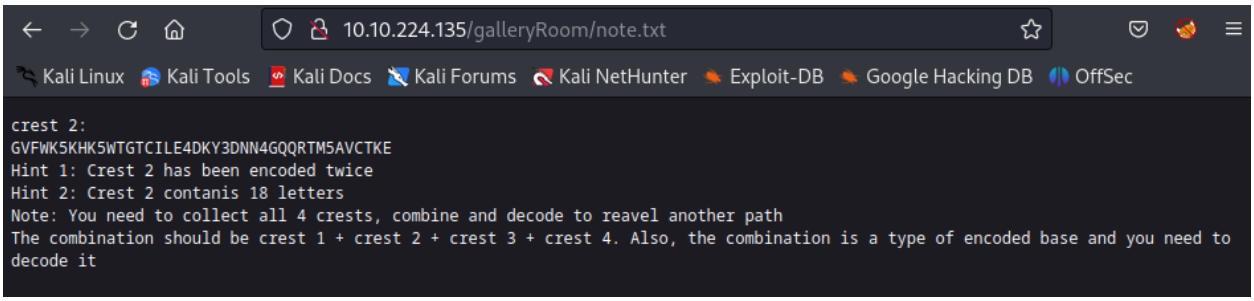


There are totally 4 **crests**! Let's decode the **crest1** with **base64** and **base32**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ echo "S0pXRkVVS0pKQkxIVVdTWUpFM0VTUlk9" | base64 -d | base32 -d
RlRQIHVzZXI6IG
```

The **crest2** is in the `/galleryRoom/`

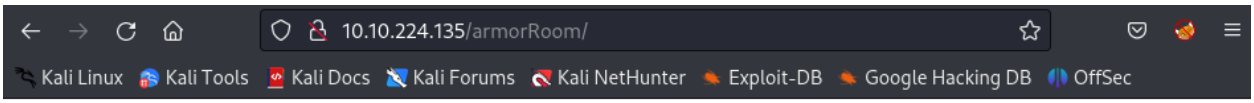




Decode it with **base32** and **base52**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ echo "GVFWK5KHK5WTGTCILE4DKY3DNN4GQQRTM5AVCTKE" | base32 -d | base58 -d
h1bnRlciwgRlRQIHBh
```

The **crest3** is in the `/armorRoom/` by using the **shield key** flag:

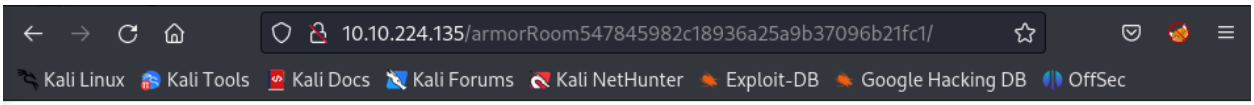


Armor room entrance

Look like the door has been locked

A **shield symbol** is embedded on the door

shield_key{48a7a9227cd7eb8 submit

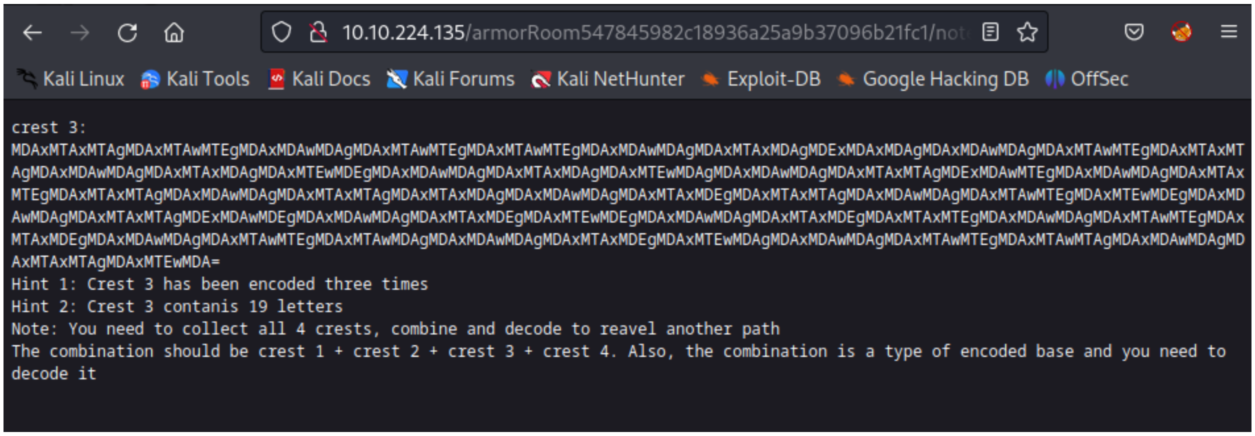


Armor room

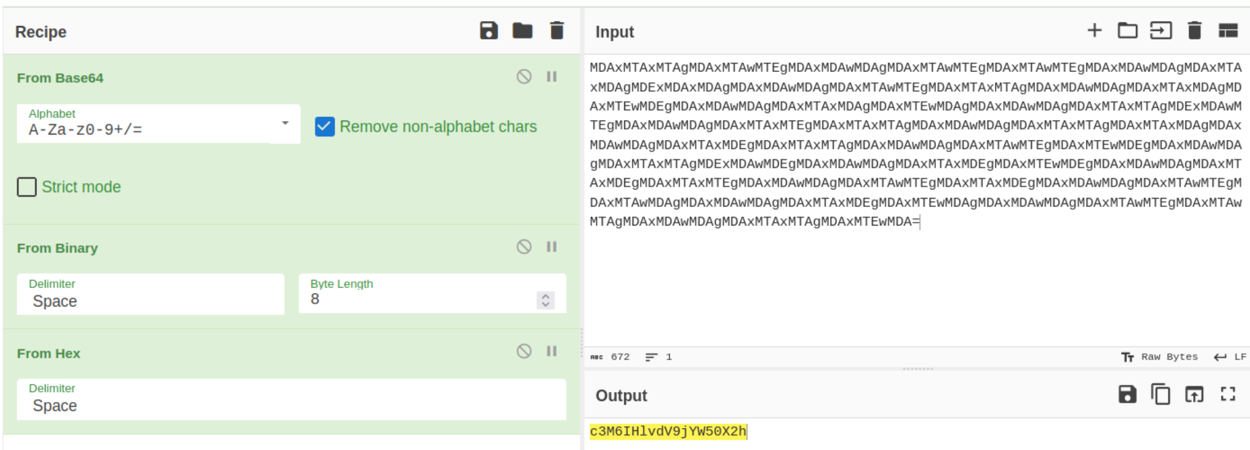
Jill saw a total 8 armor stands on the right and left of the room

Jill examine the armor one by one and found a note hidden inside one of it

Read the note? READ

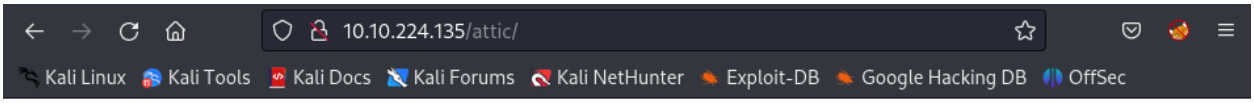


Decode the **crest3** with **base64** + **binary** + **hex**:



→ **Crest3**: c3M6IHlvdV9jYW50X2h

The final **crest4** could be found from the `/attic/` using the **shield key** flag too:

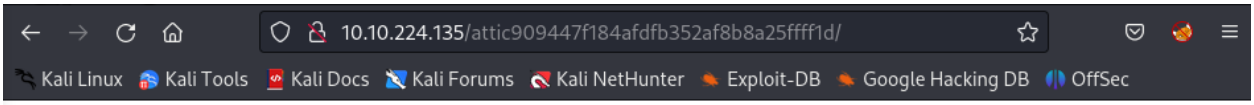


Attic entrance

Look like the door has been locked

A **shield symbol** is embedded on the door

shield_key{48a7a9227cd7eb8! submit



Attic

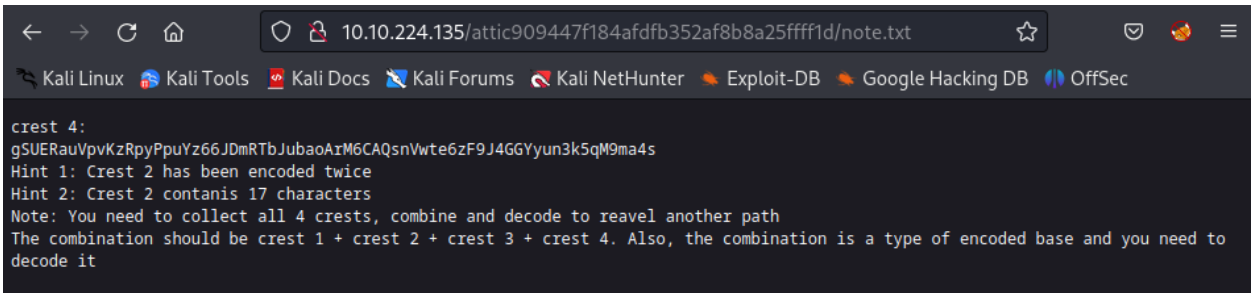
After Jill reached the attic, she was instanly attacked by a giant snake

Jill fired at least 10 shotgun shell before the snake retreat

She found another body lying on the ground which belongs to Richard, another STARS bravo member.

In additional, there is a note inside the pocket of the body

Read the note? READ




```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ echo "gSUERauVpvKzRpyPpuYz66JDmRTbJubaoArM6CAQsnVwte6zF9J4GGYyun3k5qM9ma4s" | base58 -d > crest4_hex

┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ hURL --hex -f crest4_hex

Original file     :: crest4_hex
ASCII/RAW DEcoded :: pZGVfZm9yZXZlcg==
```

Combine all the **crests** and we have:

```
RlRQIHVzZXI6IGh1bnRlciwgRlRQIHBhc3M6IHlvdV9jYW50X2hpZGVfZm9yZXZlcg==
```

Decode it with **base64**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ cat crest_combination.txt | base64 -d
FTP user: hunter, FTP pass: you_cant_hide_forever
```

Where is the hidden directory mentioned by Barry?

Use the **FTP creds** to login FTP:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ ftp 10.10.224.135
Connected to 10.10.224.135.
220 (vsFTPd 3.0.3)
Name (10.10.224.135:kali): hunter
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||38340|)
150 Here comes the directory listing.
drwxrwxrwx    2 1002     1002         4096 Sep 20  2019 .
drwxrwxrwx    2 1002     1002         4096 Sep 20  2019 ..
-rw-r--r--    1 0        0            7994 Sep 19  2019 001-key.jpg
-rw-r--r--    1 0        0            2210 Sep 19  2019 002-key.jpg
-rw-r--r--    1 0        0            2146 Sep 19  2019 003-key.jpg
-rw-r--r--    1 0        0             121 Sep 19  2019 helmet_key.txt.gpg
-rw-r--r--    1 0        0             170 Sep 20  2019 important.txt
226 Directory send OK.
```

Transfer all the files to local machine. Then read the `important.txt`:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat important.txt
Jill,

I think the helmet key is inside the text file, but I have no clue on decrypting stuff. Also, I come across a /hidden_closet/ door but it was locked.
```

```
From,
Barry
```

Answer: **/hidden_closet/**

Password for the encrypted file?

Use `steghide` to extract the `001-key.jpg` to get the **key1**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ steghide --extract -sf 001-key.jpg
Enter passphrase:
wrote extracted data to "key-001.txt".
```

Use `exiftool` to get the **key 2** from the **Comment** field:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ exiftool 002-key.jpg
ExifTool Version Number         : 12.57
File Name                       : 002-key.jpg
Directory                       : .
File Size                       : 2.2 kB
File Modification Date/Time     : 2019:09:19 02:08:31-04:00
File Access Date/Time           : 2023:08:23 07:07:35-04:00
File Inode Change Date/Time     : 2023:08:23 07:07:35-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : 5fYmVfZGVzdHJveV9
Image Width                     : 100
Image Height                    : 80
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 100x80
Megapixels                      : 0.008

┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat key-002.txt
5fYmVfZGVzdHJveV9
```

Use `binwalk` to extract the `003-key.jpg`:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ binwalk -e 003-key.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
1930          0x78A           Zip archive data, at least v2.0 to extract, uncompressed size: 14, name: key-003.txt
2124          0x84C           End of Zip archive, footer length: 22
```

Get the **key 3** inside the extracted folder:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cd _003-key.jpg.extracted

┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp/_003-key.jpg.extracted]
└─$ cat key-003.txt
3aXRoX3Zqb2x0
```

Combine **3 keys** and decode it with **base64**:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat key* | tr -d "\n" > keys

┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat keys
cGxhbnQ0Ml9jYW5fYmVfZGVzdHJveV93aXRoX3Zqb2x0
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat keys | base64 -d
plant42_can_be_destroy_with_vjolt
```

Answer: **plant42_can_be_destroy_with_vjolt**

What is the helmet key flag?

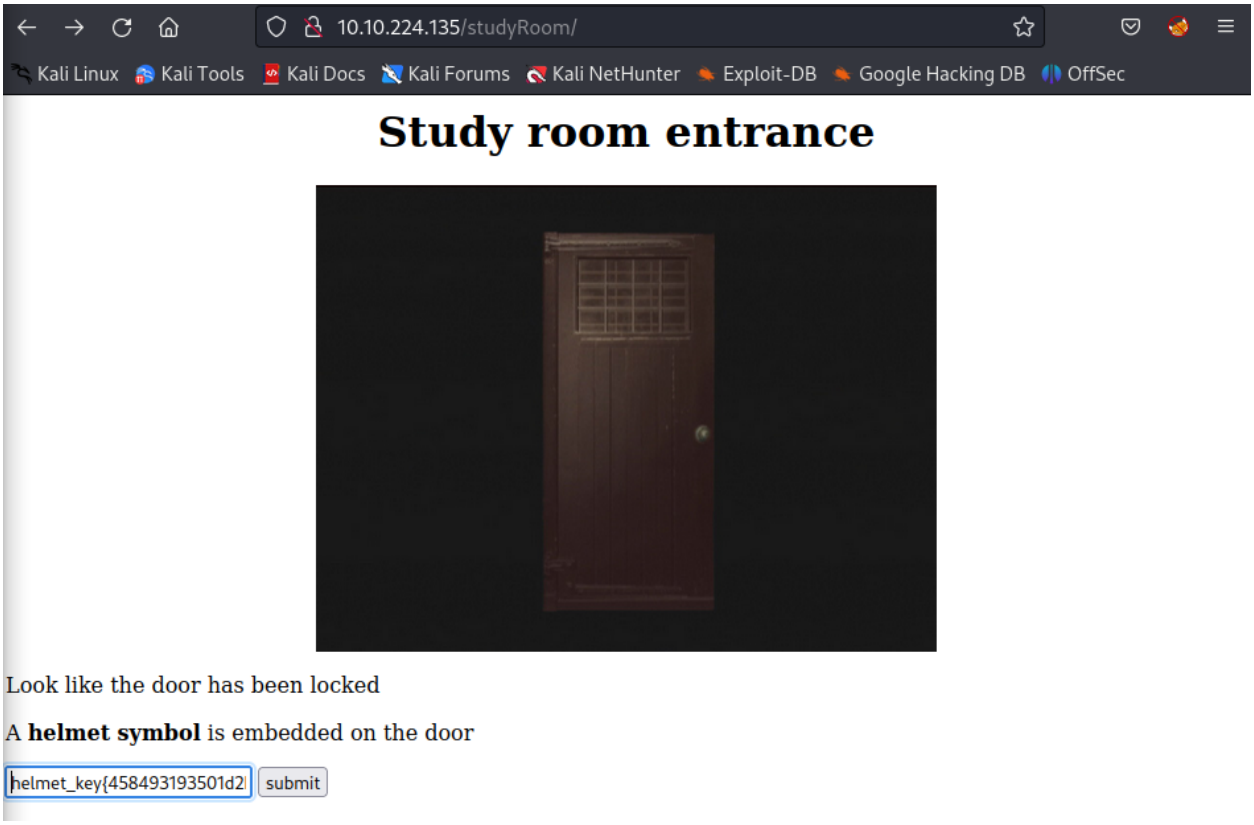
Use the result as the key to extract the `helmet_key.txt.gpg` and get the key:

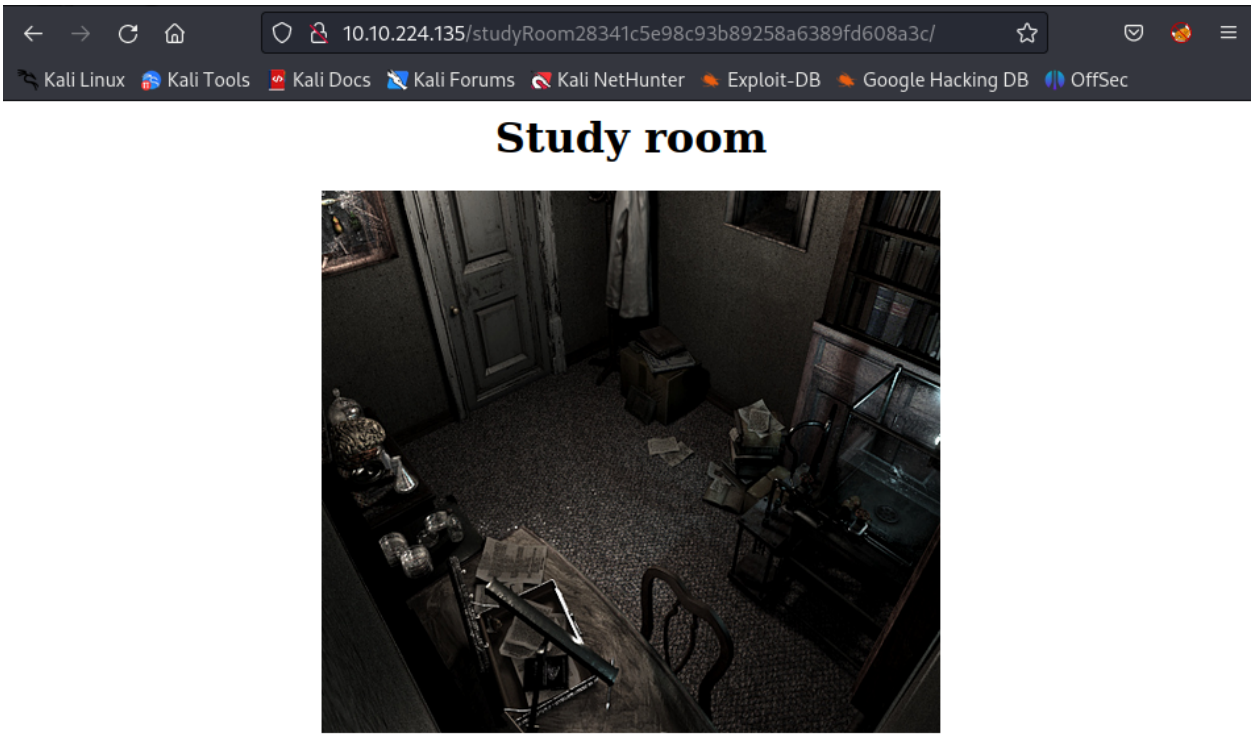
```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ gpg helmet_key.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
```

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard/ftp]
└─$ cat helmet_key.txt
helmet_key{458493193501d2b94bbab2e727f8db4b}
```

What is the SSH login username?

Re-visit the left room in the `MansionMap.html` which is `/studyRoom/` and enter the **helmet key** flag:





Click **EXAMINE** or copy its link and use `wget` to download a file:

```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ wget http://10.10.224.135/studyRoom28341c5e98c93b89258a6389fd608a3c/doom.tar.gz
--2023-08-23 07:20:28--  http://10.10.224.135/studyRoom28341c5e98c93b89258a6389fd608a3c/doom.tar.gz
Connecting to 10.10.224.135:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 149 [application/x-gzip]
Saving to: ‘doom.tar.gz’

doom.tar.gz                 100%[=============================================>]     149  --.-KB/s    in 0s

2023-08-23 07:20:29 (24.6 MB/s) - ‘doom.tar.gz’ saved [149/149]
```

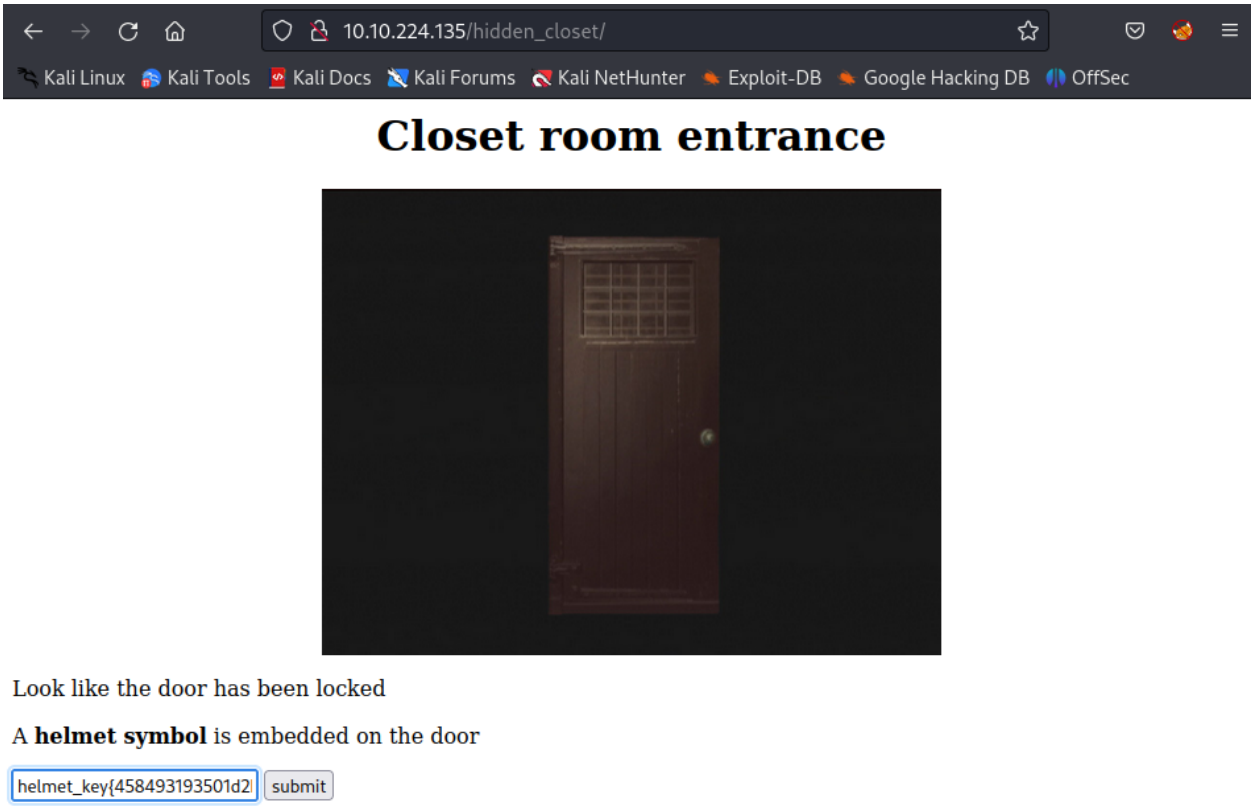
Use `gunzip` to unzip the file and then use `tar -xvf` to extract the data inside:

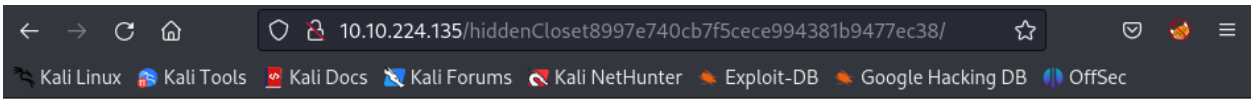
```
┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ gunzip doom.tar.gz

┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ tar -xvf doom.tar
eagle_medal.txt

┌──(kali㉿kali)-[~/TryHackMe/Biohazard]
└─$ cat eagle_medal.txt
SSH user: umbrella_guest
```

Answer: **umbrealla_guest**

What is the SSH login password?

Visit the `/hidden_closet/` and enter the **helmet key** flag:





Closet room

The closet room lead to an underground cave

In the cave, Jill met injured Enrico, the leader of the STARS Bravo team. He mentioned there is a traitor among the STARTS Alpha team.

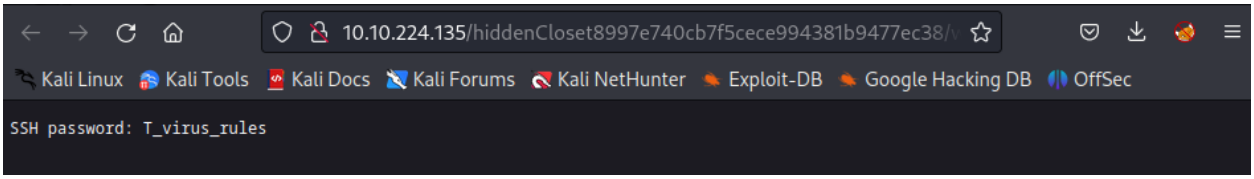
When he was about to tell the traitor name, suddenly, a gun shot can be heard and Enrico was shot dead.

Jill somehow cannot figure out who did that. Also, Jill found a MO disk 1 and a wolf Medal

Read the MO disk 1? READ

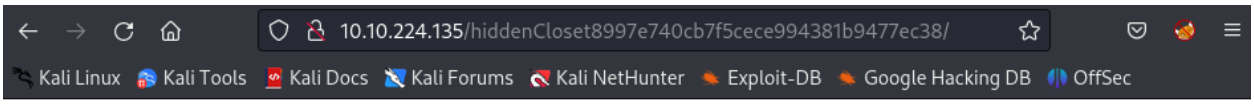
Examine the wolf medal? EXAMINE

Click **EXAMINE:**



Answer: **T_virus_rules**

Who the STARS bravo team leader



Closet room

The closet room lead to an underground cave

In the cave, Jill met injured Enrico, the leader of the STARS Bravo team. He mentioned there is a traitor among the STARTS Alpha team.

When he was about to tell the traitor name, suddenly, a gun shot can be heard and Enrico was shot dead.

Jill somehow cannot figure out who did that. Also, Jill found a MO disk 1 and a wolf Medal

Read the MO disk 1? READ

Examine the wolf medal? EXAMINE

Answer: **Enrico**

Where you found Chris?

SSH to the target system using the found creds:

```
umbrella_guest@umbrella_corp:~$ id
uid=1001(umbrella_guest) gid=1001(umbrella) groups=1001(umbrella)
umbrella_guest@umbrella_corp:~$ ls -l
total 0
umbrella_guest@umbrella_corp:~$ ls -la
total 64
drwxr-xr-x  8 umbrella_guest umbrella 4096 Sep 20  2019 .
drwxr-xr-x  5 root           root     4096 Sep 20  2019 ..
-rw-r--r--  1 umbrella_guest umbrella  220 Sep 19  2019 .bash_logout
-rw-r--r--  1 umbrella_guest umbrella 3771 Sep 19  2019 .bashrc
drwxrwxr-x  6 umbrella_guest umbrella 4096 Sep 20  2019 .cache
drwxr-xr-x 11 umbrella_guest umbrella 4096 Sep 19  2019 .config
-rw-r--r--  1 umbrella_guest umbrella   26 Sep 19  2019 .dmrc
drwx------  3 umbrella_guest umbrella 4096 Sep 19  2019 .gnupg
-rw-------  1 umbrella_guest umbrella  346 Sep 19  2019 .ICEauthority
drwxr-xr-x  2 umbrella_guest umbrella 4096 Sep 20  2019 .jailcell
drwxr-xr-x  3 umbrella_guest umbrella 4096 Sep 19  2019 .local
-rw-r--r--  1 umbrella_guest umbrella  807 Sep 19  2019 .profile
drwx------  2 umbrella_guest umbrella 4096 Sep 20  2019 .ssh
-rw-------  1 umbrella_guest umbrella  109 Sep 19  2019 .Xauthority
-rw-------  1 umbrella_guest umbrella 7546 Sep 19  2019 .xsession-errors
```

Go to `.jailcell`:

```
umbrella_guest@umbrella_corp:~$ cd .jailcell/
umbrella_guest@umbrella_corp:~/.jailcell$ ls -la
total 12
drwxr-xr-x 2 umbrella_guest umbrella 4096 Sep 20  2019 .
```

```
drwxr-xr-x 8 umbrella_guest umbrella 4096 Sep 20  2019 ..
-rw-r--r-- 1 umbrella_guest umbrella  501 Sep 20  2019 chris.txt
```

Answer: **jailcell**

Who is the traitor?

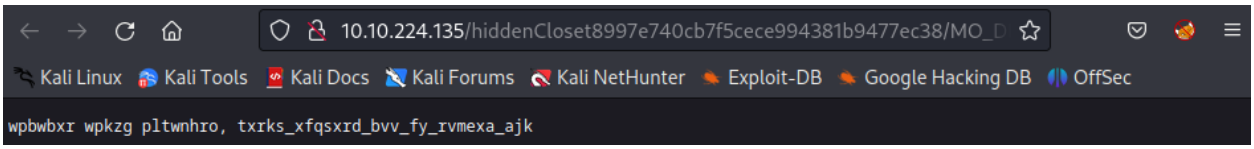
Read the file `christ.txt`

```
umbrella_guest@umbrella_corp:~/.jailcell$ cat chris.txt
Jill: Chris, is that you?
Chris: Jill, you finally come. I was locked in the Jail cell for a while. It seem that weasker is behind all this.
Jil, What? Weasker? He is the traitor?
Chris: Yes, Jill. Unfortunately, he play us like a damn fiddle.
Jill: Let's get out of here first, I have contact brad for helicopter support.
Chris: Thanks Jill, here, take this MO Disk 2 with you. It look like the key to decipher something.
Jill: Alright, I will deal with him later.
Chris: see ya.

MO disk 2: albert
```

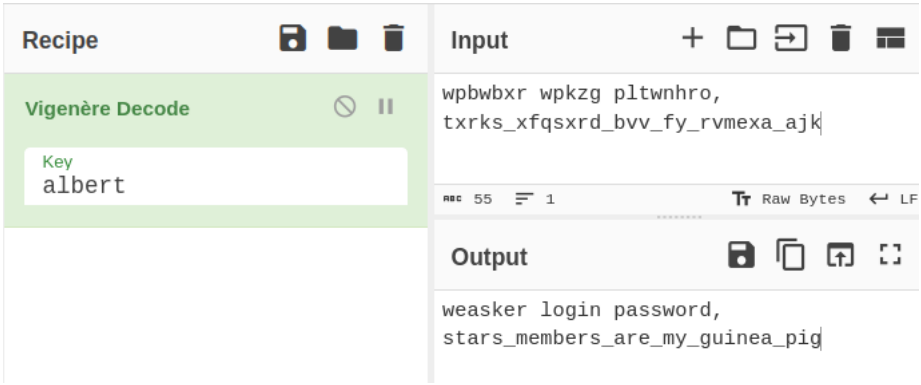
Answer: **weasker**

The login password for the traitor?

Re-visit the `/hidden_closet/` and enter the **helmet key** flag. Then click **READ**:



Use the key `ablert` from the `chrits.txt` and decode the string with **Vigenere Cipher**:



Answer: **stars_members_are_my_guinea_pig**

The name of the ultimate form

Switch to user `weasker` using the login password found:

```
umbrella_guest@umbrella_corp:~/.jailcell$ su weasker
Password:
weasker@umbrella_corp:/home/umbrella_guest/.jailcell$ cd
weasker@umbrella_corp:
```

Read the note of `weasker`:

```
weasker@umbrella_corp:~$ ls -la
total 80
drwxr-xr-x  9 weasker weasker 4096 Sep 20  2019 .
drwxr-xr-x  5 root    root    4096 Sep 20  2019 ..
-rw-------  1 weasker weasker   18 Sep 20  2019 .bash_history
-rw-r--r--  1 weasker weasker  220 Sep 18  2019 .bash_logout
-rw-r--r--  1 weasker weasker 3771 Sep 18  2019 .bashrc
drwxrwxr-x 10 weasker weasker 4096 Sep 20  2019 .cache
drwxr-xr-x 11 weasker weasker 4096 Sep 20  2019 .config
drwxr-xr-x  2 weasker weasker 4096 Sep 19  2019 Desktop
drwx------  3 weasker weasker 4096 Sep 19  2019 .gnupg
-rw-------  1 weasker weasker  346 Sep 20  2019 .ICEauthority
drwxr-xr-x  3 weasker weasker 4096 Sep 19  2019 .local
drwx------  5 weasker weasker 4096 Sep 19  2019 .mozilla
-rw-r--r--  1 weasker weasker  807 Sep 18  2019 .profile
drwx------  2 weasker weasker 4096 Sep 19  2019 .ssh
-rw-r--r--  1 weasker weasker    0 Sep 20  2019 .sudo_as_admin_successful
-rw-r--r--  1 root    root     534 Sep 20  2019 weasker_note.txt
-rw-------  1 weasker weasker  109 Sep 20  2019 .Xauthority
-rw-------  1 weasker weasker 5548 Sep 20  2019 .xsession-errors
-rw-------  1 weasker weasker 6749 Sep 20  2019 .xsession-errors.old
weasker@umbrella_corp:~$ cat weasker_note.txt
Weaker: Finally, you are here, Jill.
Jill: Weasker! stop it, You are destroying the  mankind.
Weasker: Destroying the mankind? How about creating a 'new' mankind. A world, only the strong can survive.
Jill: This is insane.
Weasker: Let me show you the ultimate lifeform, the Tyrant.

(Tyrant jump out and kill Weasker instantly)
(Jill able to stun the tyrant will a few powerful magnum round)

Alarm: Warning! warning! Self-detruct sequence has been activated. All personal, please evacuate immediately. (Repeat)
Jill: Poor bastard
```

Answer: **Tyrant** *(Weasker: Let me show you the ultimate lifeform, the Tyrant.)*

The root flag

```
weasker@umbrella_corp:~$ sudo -l
[sudo] password for weasker:
Matching Defaults entries for weasker on umbrella_corp:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User weasker may run the following commands on umbrella_corp:
    (ALL : ALL) ALL
```

The `weasker` user can run all `sudo` commands → Simply type `sudo su` to switch to the **root** user:

```
weasker@umbrella_corp:~$ sudo su
root@umbrella_corp:/home/weasker# id
uid=0(root) gid=0(root) groups=0(root)
root@umbrella_corp:/home/weasker# cd /root
root@umbrella_corp:~# cat root.txt
In the state of emergency, Jill, Barry and Chris are reaching the helipad and awaiting for the helicopter support.

Suddenly, the Tyrant jump out from nowhere. After a tough fight, brad, throw a rocket launcher on the helipad. Without thinking twice, Ji
ll pick up the launcher and fire at the Tyrant.

The Tyrant shredded into pieces and the Mansion was blowed. The survivor able to escape with the helicopter and prepare for their next fi
ght.

The End

flag: 3c5794a00dc56c35f2bf096571edf3bf
```