

# Biohazard

## Introduction

Scan for open ports using nmap

//found 3 open ports

```
$ nmap -sC -sV -oN portscan 10.10.136.229
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-19 16:59 EST
Nmap scan report for 10.10.136.229
Host is up (0.19s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 c9:03:aa:aa:ea:a9:f1:f4:09:79:c0:47:41:16:f1:9b (RSA)
|_   256 2e:1d:83:11:65:03:b4:78:e9:6d:94:d1:3b:db:f4:d6 (ECDSA)
|_   256 91:3d:e4:4f:ab:aa:e2:9e:44:af:d3:57:86:70:bc:39 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ _http-server-header: Apache/2.4.29 (Ubuntu)
|_ _http-title: Beginning of the end
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

gaining access the rootpage of the web server

## 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 northwest 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.....

this is the team that in operation

The [STARS alpha team](#), Chris, Jill, Barry, Weasker and Joseph is in the operation on searching the STARS bravo team in the northwest of Racoon city.

## The Mansion

now we need to collect all the necessary items to advance to next level

Collect all necessary items and advanced to the next level. The format of the Item flag:

Item\_name{32 character}

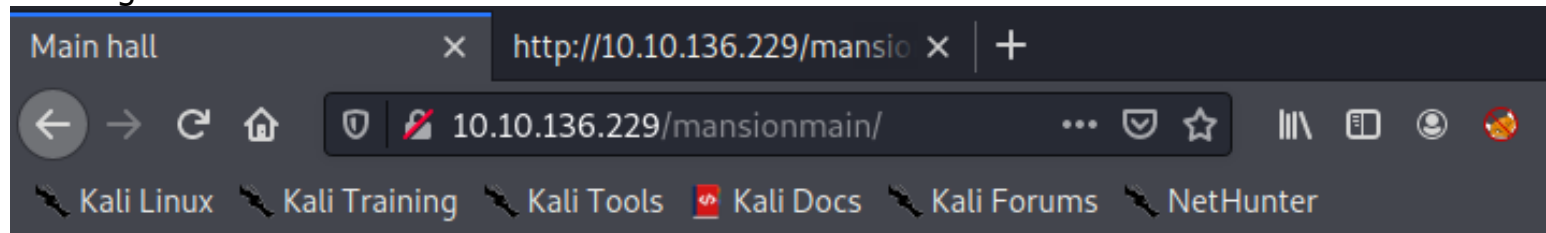
Some of the doors are locked. Use the item flag to unlock the door.

Tips: It is better to record down all the information inside a notepad

Finding the emblem

=====

entering into the mansion main hall



## Main hall



The team reach the mansion safe and sound. However, it appear that Chris is missing  
Jill try to open the door but stopped by Weaker

Suddenly, a gunshot can be heard in the nearby room. Weaker order Jill to make an  
investigate on the gunshot. Where is the room?

checking the source code, diningRoom?

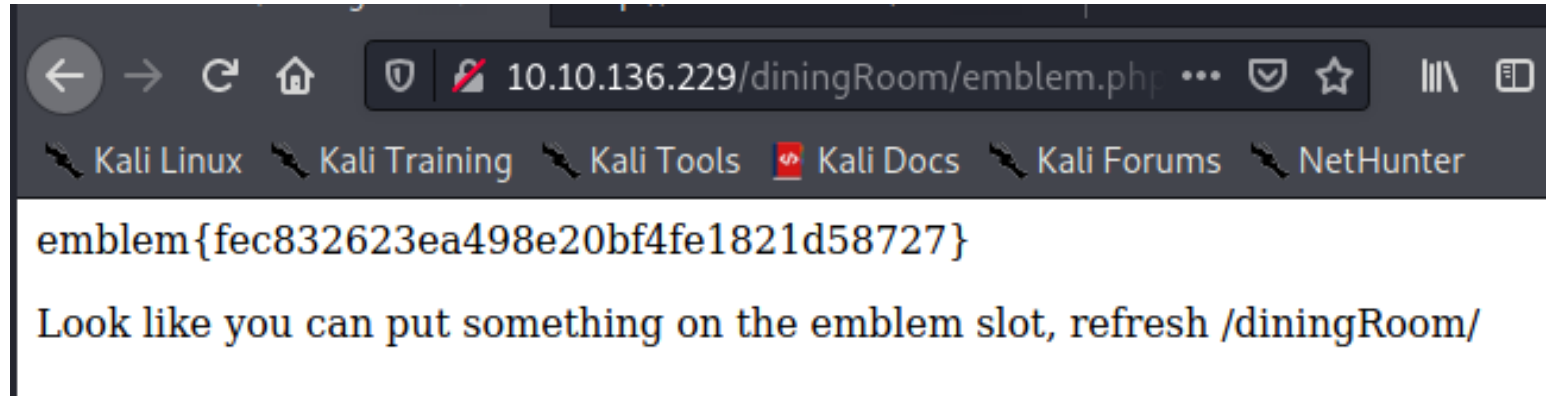
```
<p>Suddenly, a gunshot can be he  
<!-- It is in the /diningRoom/ -->  
</body>
```

in the /diningRoom directory, we found an emblem on the wall? let's take it

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](#)**

we've found the emblem



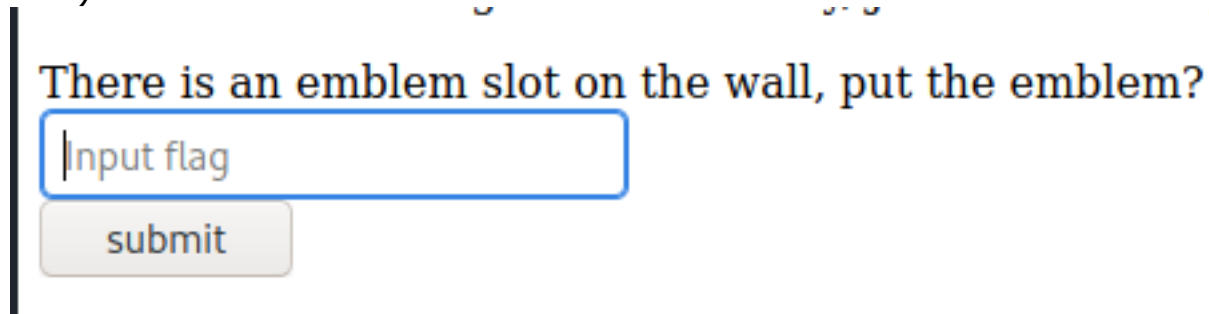
Finding Lock Pick Flag

=====

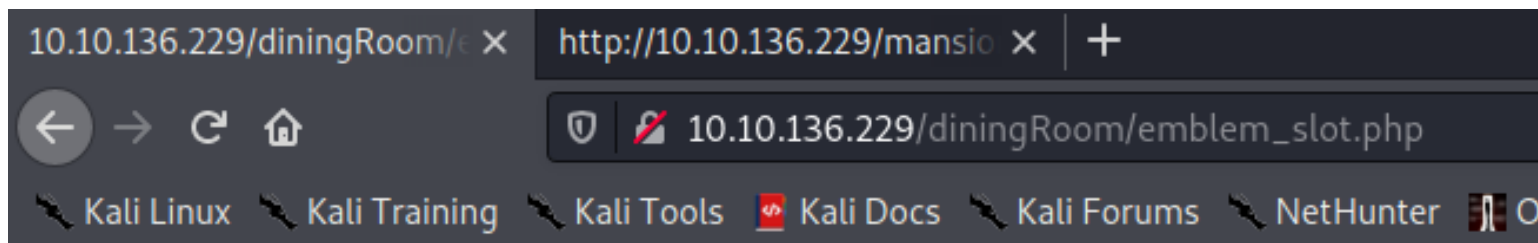
at the emblem.php, it does told us tht we can put something on the emblem slot, what could it be?

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

after refreshing the diningRoom directory, we found an input box (we can input our found emblem here)



we tried inputing the emblem flag into it but nothing happened



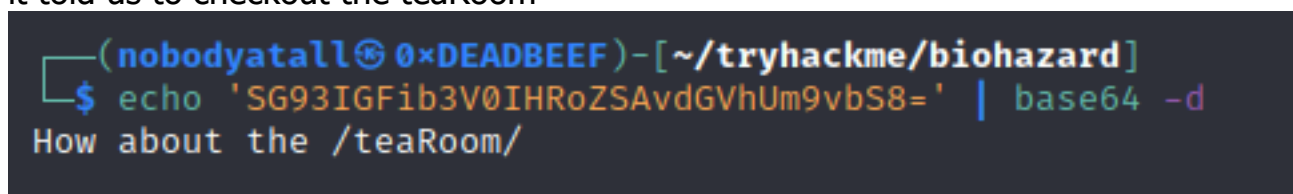
Nothing happen

checking the source code of diningRoom page again, we found base64 encoded string?

```
<p>After a short investigation with barry, .  
<!-- SG93IGFib3V0IHRoZSAvdGVhUm9vbS8= -->  
</body>
```

there is an emblem slot on the wall, put the emblem  
<input type="text" name="emblem slot" value="" />

it told us to checkout the teaRoom



in the teaRoom we found something about lockPick?

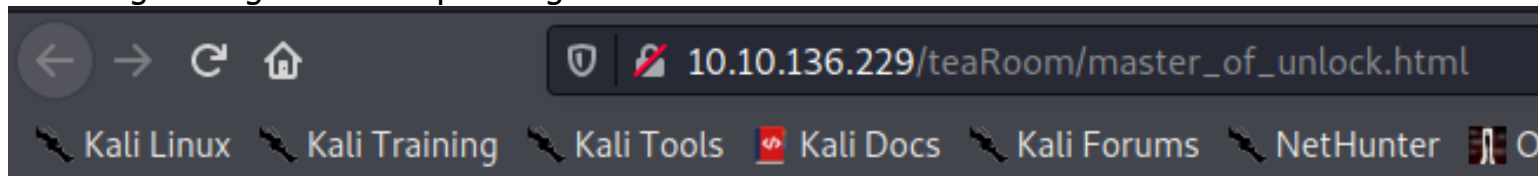
After the investigation, the body belong to kenneth from Bravo team. What happened here?

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/

10.10.136.229/teaRoom/master\_of\_unlock.html

& visiting it we got our lock pick flag



lock\_pick{037b35e2ff90916a9abf99129c8e1837}

Getting the Mansion Map

=====

in the teaRoom there's a notes suggesting Jill to visit the artRoom



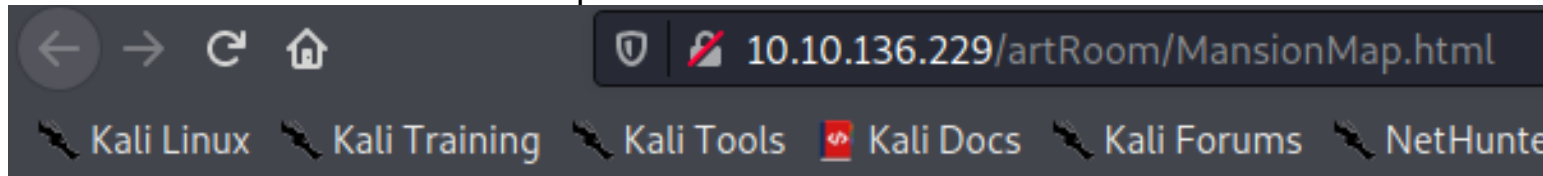
Barry also suggested that Jill should visit the /artRoom/

then we go to the artRoom & found something mentioned about paper stick that's on the wall?

A number of painting and a sculpture can be found inside the room

**There is a paper stick on the wall, Investigate it?** [YES](#)

& voila! we've found the mansion map



Look like a map

Location:

/diningRoom/

/teaRoom/

/artRoom/

/barRoom/

/diningRoom2F/

/tigerStatusRoom/

/galleryRoom/

/studyRoom/

/armorRoom/

/attic/

Finding Music Sheet Flag

=====

let's check out the barRoom first, okay we need a lockpick in order to open i

Look like the door has been locked

It can be open by a **lockpick**

using the lock\_pick flag that we've just found, we've entered the barRoom

## Bar room



in the barRoom, we need something in order to play the piano

what a messy bar room

A piano can be found in the bar room

**Play the piano?**

under the input box, we found a note, it seems to be the music sheet "moonlight somata" let's read it

**Also, you found a note that written as "moonlight somata", read it? [READ](#)**

it looks like music notes here

Look like a music note

NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVIRGIYZWGNSSGCZLDMU3GCMLGGY3TMZL5

using base32 & we've decoded it to our music\_sheet flag!

**Recipe**

From Base32

Alphabet  
A-Z2-7=

☒ Remove non-alphabet chars

**Input**

length: 73  
lines: 1

NV2XG2LDL5ZWQZLF0R5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGN5GCZLDMU3GCMLGGY3TMZL5

**Output**

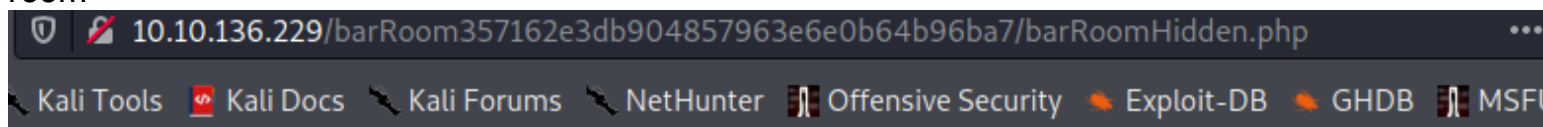
time: 3ms  
length: 45  
lines: 1

music\_sheet{362d72deaf65f5bdc63daece6a1f676e}

Finding Gold Emblem Flag

=====

entering the music\_sheet flag in the input box in barRoom & we've redirected into a secret bar room



## Secret bar room



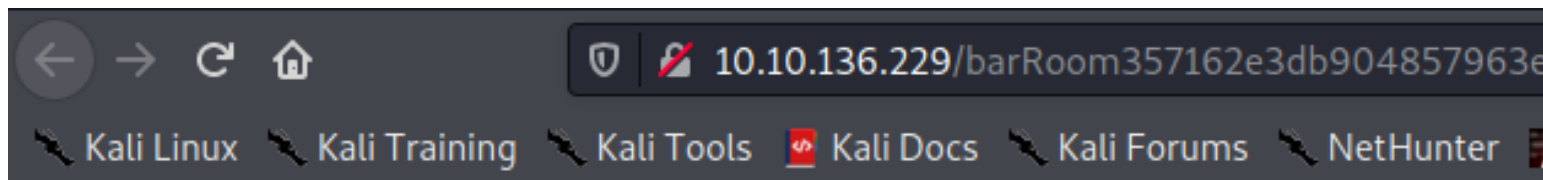
we found a gold emblem embedded on the wall let's take it \_\_\_\_\_

There is a gold emblem embedded on the wall

Will you take it? YES

now we've took the gold\_emblem





gold\_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}

Finding Shield\_Key flag

=====

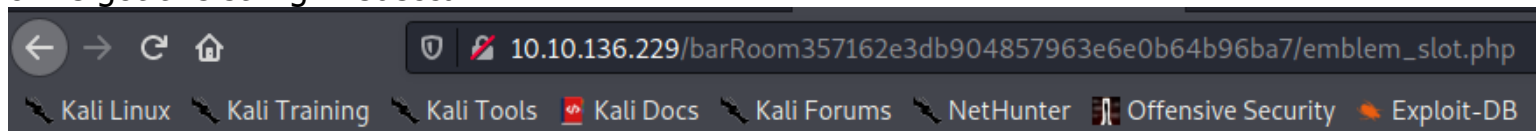
here it show us a notes that ask us to refresh previous page

now let's try out placing the emblem that we found in the diningRoom into the slot?

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

& we got this string "Rebecca"



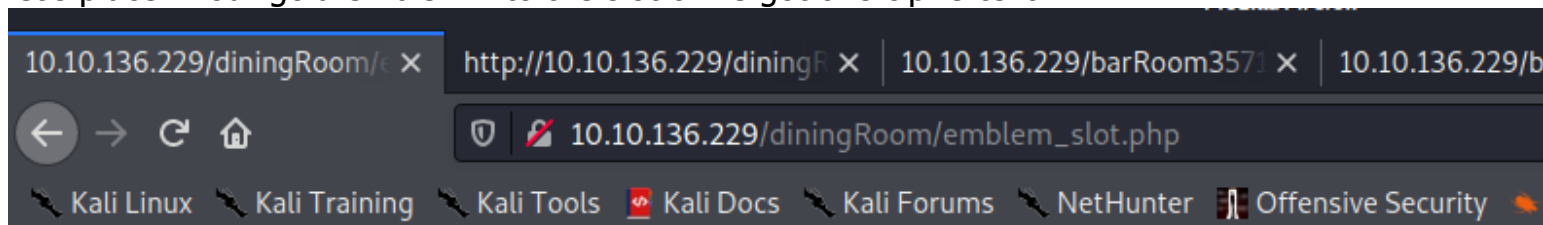
rebecca

still remember the emblem slot in diningRoom?

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

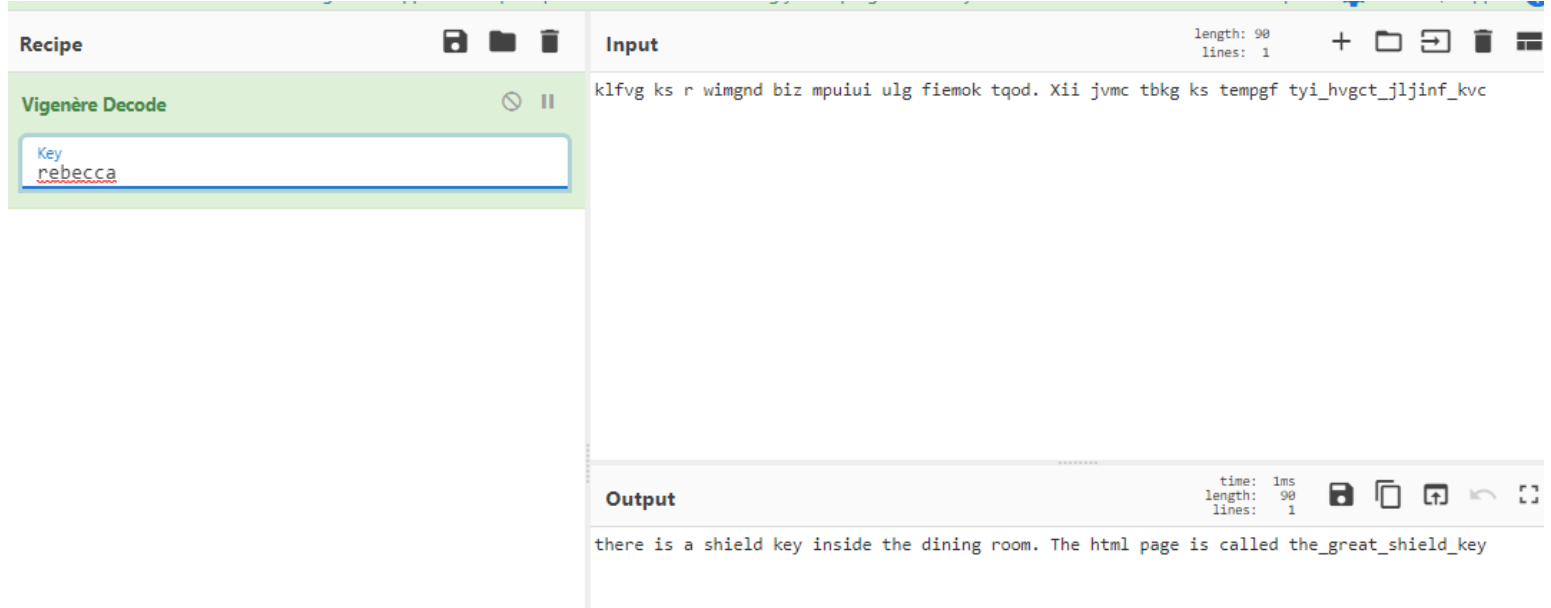
  

let's place in our gold emblem into the slot & we got this ciphertext



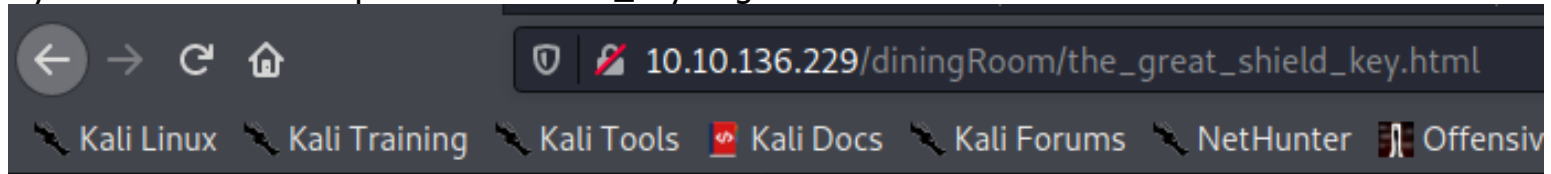
klfvg ks r wimgnd biz mpuiui ulg fiemok tqod. Xii jvmc tbkg ks tempgf tyi\_hvgct\_jljinf\_kvc

the ciphertext does look like vigenere cipher here, let's decrypt it with the key 'rebecca' & voila we got a notes



there's a shield\_key in the diningRoom uh with the\_great\_shield\_key html

try it out & voila we captured our shield\_key flag

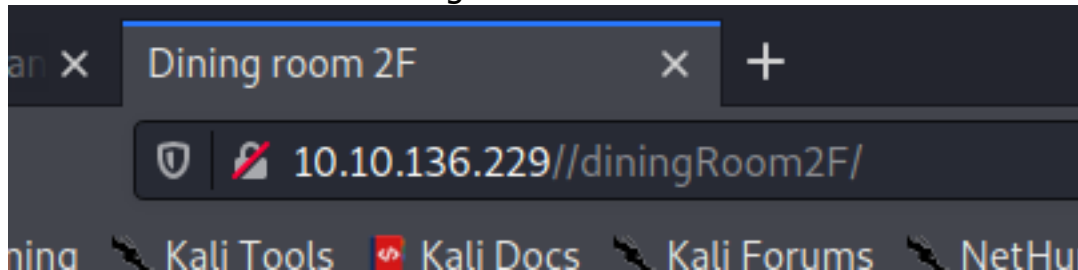


shield\_key{48a7a9227cd7eb89f0a062590798cbac}

### Finding Blue Gem Flag

=====

now let's check out the diningRoom2F



here it did mentioned something about blue gem

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

let's check out the page source code & we found another ciphertext

```
<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 fgngfh gb gur ybjre sybbe. Gur trz vf ba gur qvavatEbbz svefg sybbe. Ivfvg fnccuver.ugzy -->
</body>
```

it seems like ROT13 encryption here

The screenshot shows a web-based ROT13 encryption tool. On the left, under the heading "Recipe", there are two checked options: "Rotate lower case chars" and "Rotate upper case chars". A text box labeled "Amount" contains the value "13". On the right, the "Input" section contains the ROT13-encoded text: "Lbh trg gur oyhr trz ol chfuvat gur fgnghf gb gur ybjre sybbe. Gur trz vf ba gur qvavatEbbz svefg sybbe. Ivfvg fnccu|ver.ugzy". The "Output" section shows the decoded text: "You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphire.html".

here it mentioned the gem is on the diningRoom 1st floor & we need to get it by visiting sapphire.html

The screenshot shows a web browser window with the URL "10.10.136.229//diningRoom/sapphire.html". The page content displays the decoded message: "You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphire.html".

let's capture our blue gem flag!

The screenshot shows a web browser window with the URL "10.10.136.229//diningRoom/sapphire.html". The page content displays the blue gem flag: "blue\_jewel{e1d457e96cac640f863ec7bc475d48aa}".

Finding FTP Credential

=====

now let's check out the tigerStatusRoom

The screenshot shows a web browser window with the URL "10.10.136.229/tigerStatusRoom/". The page title is "Tiger status room". The browser's address bar shows the URL. The page content is partially visible, showing the text "Tiger status room".

**Tiger**

here we found an input box for us to insert the blue gem flag

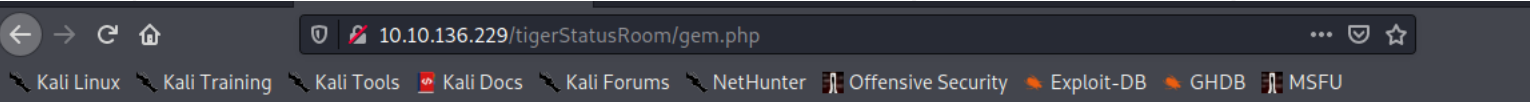
You reached a small room with a tiger status

Look like you can put a gem on the tiger's eye

Enter flag

submit

inserting it & we end up in this page with some notes  
//here it provided us crest1, we need to find other 3 crests (combine it & decode)



crest 1:  
S0pXRkVVS0pKQkxIVVdTWUpFM0VTUlk9  
Hint 1: Crest 1 has been encoded twice  
Hint 2: Crest 1 contains 14 letters  
Note: You need to collect all 4 crests, combine and decode to reveal another path  
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

by decoding the crest 1, we use this decoding types

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

From Base32

Alphabet  
A-Z2-7=

☒ Remove non-alphabet chars

Input

S0pXRkVVS0pKQkxIVVdTWUpFM0VTUlk9

Output

R1RQIHVzZXI6IG

& it matched the 2nd hint 14 letters

```
ui >>> x = "RlRQIHVzZXI6IG"
rt >>> len(x)
ot 14
kl >>> _
```

checking out the gallery room & we can examine some note

Upon Jill walk into the room, she saw a bunch of gallery and zombie crow in the room  
Nothing is interesting, expect the note on the wall

**Examine the note?** [EXAMINE](#)

& we've found the crest2!

crest 2:  
GVFWK5KHK5WTGTCILE4DKY3DNN4GQQRTM5AVCTKE  
Hint 1: Crest 2 has been encoded twice  
Hint 2: Crest 2 contains 18 letters  
Note: You need to collect all 4 crests, combine and decode to reveal another path  
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it

let's decode it again

Recipe

From Base32

Alphabet  
A-Z2-7=

☒ Remove non-alphabet chars

From Base58

Alphabet  
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefgh...

☒ Remove non-alphabet chars

Input

GVFWK5KHK5WTGTCILE4DKY3DNN4GQQRTM5AVCTKE

Output

h1bnRlciwgRlRQIHh

& it matched the 2nd hint 18 letters



```
>>> x = "h1bnRlciwgRlRQIHh"
>>> len(x)
18
>>>
```

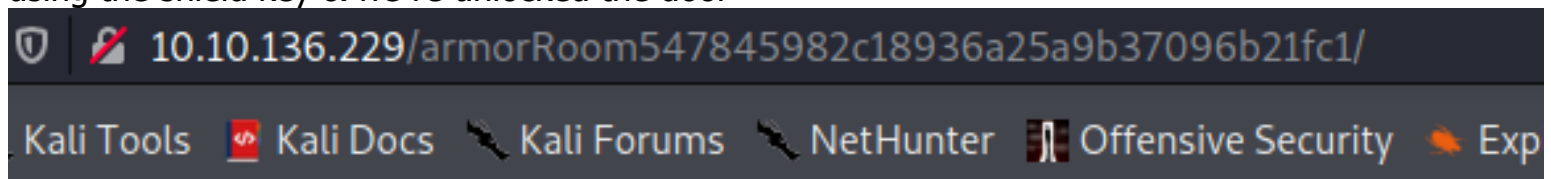
checking the armorRoom & we need the key to unlock the door  
//it shows a shield symbol embedded on the door

Look like the door has been locked

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

using the shield key & we've unlocked the door



in the armorRoom there's a note again let's read it

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

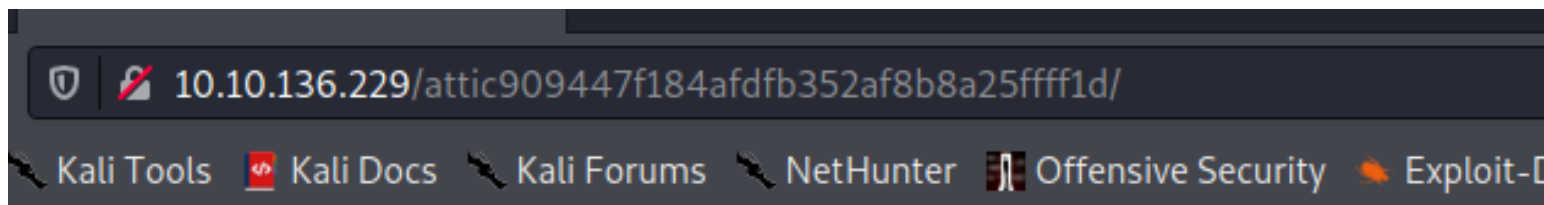
Read the note? [READ](#)

& we've found the crest 3

[illegible]

decoding it with the hints provided & we got this





# Attic



& there's a note found down there too

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

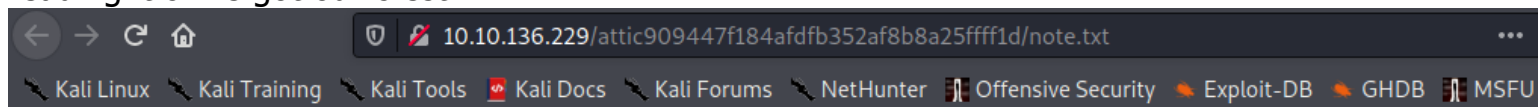
Jill fired at least 10 shotgun shells before the snake retreated

She found another body lying on the ground which belongs to Richard, another STA

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

**Read the note? [READ](#)**

reading it & we got our crest4



```
crest 4:
gSUEraUvPvKzRpyPpuYz66JDmRTbJubaoArM6CAQsnVwte6zF9J4GGYyun3k5qM9ma4s
Hint 1: Crest 2 has been encoded twice
Hint 2: Crest 2 contains 17 characters
Note: You need to collect all 4 crests, combine and decode to reveal another path
The combination should be crest 1 + crest 2 + crest 3 + crest 4. Also, the combination is a type of encoded base and you need to decode it
```

decoding it again & we got the following text

**Recipe**

From Base58

Alphabet

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefg...

☒ Remove non-alphabet chars

From Hex

Delimiter

Auto

Input

length: 68  
lines: 1

gSUErauVpvKzRpyPpuYz66JDmRTbJubaoArM6CAQsnVwte6zF9J4GGYyun3k5qM9ma4s

Output

start: 0    time: 4

end: 17    length: 4

length: 17    lines:

pZGVfZm9yZXZlcg==

& it matched the hint 2 too 17 characters

```
>>> x = 'pZGVfZm9yZXZlcg=='
>>> len(x)
17
>>>
```

now by combining the 4 crest & we'll have an encoding text

```




Crest
=====
crest1: R1RQIHVzZXI6IG
crest2: h1bnRlciwgR1RQIHBh
crest3: c3M6IH1vdV9jYW50X2h
crest4: pZGVfZm9yZXZlcg==

R1RQIHVzZXI6IGh1bnRlciwgR1RQIHBhc3M6IH1vdV9jYW50X2hpZGVfZm9yZXZlcg==

```

decoding the encoded text, we got the FTP credential

**Recipe**



**From Base64**

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

**Input**

length: 68  
lines: 1

R1RQIHVzZXI6IGh1bnRlcwR1RQIHBhc3M6IHlvdV9jYW50X2hpZGVfZm9yZXZlcg==

**Output**

time: 5ms  
length: 49  
lines: 1

FTP user: hunter, FTP pass: you\_cant\_hide\_forever

FTP credential

```
FTP user: hunter, FTP pass: you_cant_hide_forever
```

## The Guard House

now let's access the FTP using the credential we found

18/29



```

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$ ftp 10.10.136.229
Connected to 10.10.136.229.
220 (vsFTPd 3.0.3)
Name (10.10.136.229:nobodyatall): hunter
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
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.
ftp>

```

use mget to download all the files to our local host

```

ftp> mget *
mget 001-key.jpg?
200 PORT command successful.
150 Opening BINARY mode data
226 Transfer complete.
7994 bytes received in 0.00
mget 002-key.jpg?
200 PORT command successful.

```

there's an important.txt

// barry mentioned that there's a /hidden\_closet/ door locked

// and the helmet key might be inside the text file which might be encrypted

```

(nobodyatall@0xDEADBEEF)-[~/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

```

checking helmet key file, it's encrypted

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ cat helmet_key.txt.gpg
eiC[h[9_dFw?nH@(\
\Xqyu
H[H0,m\{Q
R4by a giant snake
6\W?sU?y^f?q$
snake retreat
```

this is a gpg symmetrically encrypted data, we need the secret key to decrypt it

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ file helmet_key.txt.gpg
helmet_key.txt.gpg: GPG symmetrically encrypted data (AES256 cipher)
```

there's jpg files, check is there any stegano hidden stuff behind? found key-001.txt  
//it's encoded

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ steghide extract -sf 001-key.jpg
Enter passphrase:
wrote extracted data to "key-001.txt".

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ cat key-001.txt
cGxhbnQ0Ml9jYW
```

for 002-key.jpg, we check using exiftool & notice the comment section looks kinda sus

```

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ exiftool 002-key.jpg
ExifTool Version Number      : 12.09
File Name                    : 002-key.jpg
Directory                    : .
File Size                    : 2.2 kB
File Modification Date/Time   : 2020:12:19 18:24:37-05:00
File Access Date/Time        : 2020:12:19 18:28:08-05:00
File Inode Change Date/Time   : 2020:12:19 18:24:37-05:00
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

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]

```

for 003-key.jpg we use binwalk to observe, it seems to have a .zip file in it with key-003.txt

```

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ binwalk 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

the key-003.txt

```

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ cat key-003.txt
3aXR0X3Zqb2x0

```

let's combine the keys we found & decode it using base64, it seems to be a passphrase

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

cGxhbnQ0M19jYW5fYmVfZGVzdHJveV93aXR0X3Zqb2x0

Output

plant42\_can\_be\_destroy\_with\_vjolt

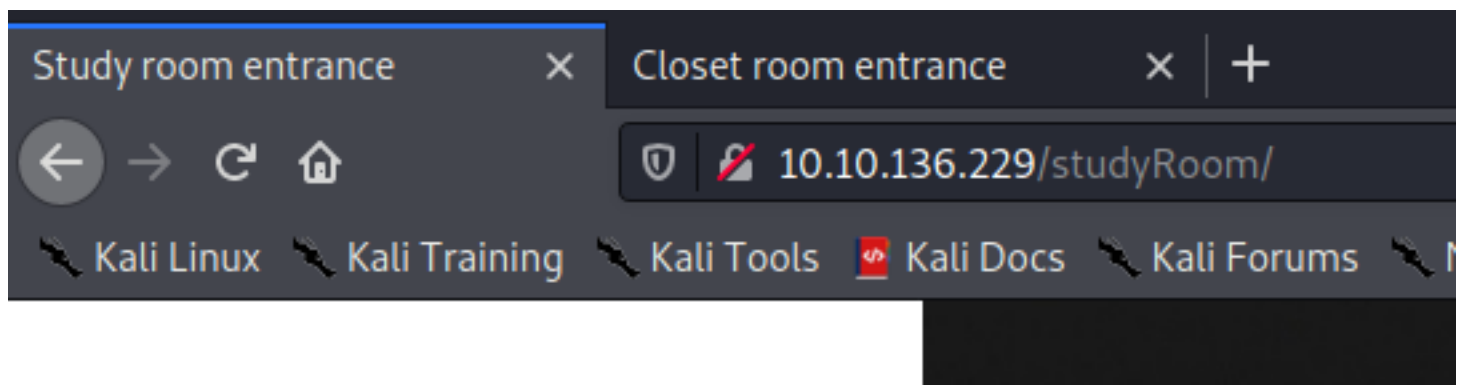
voila using the passphrase with gpg to decrypt it & we got our helmet key flag

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
$ gpg --decrypt helmet_key.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
helmet_key{458493193501d2b94bbab2e727f8db4b}
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard/ftp]
```

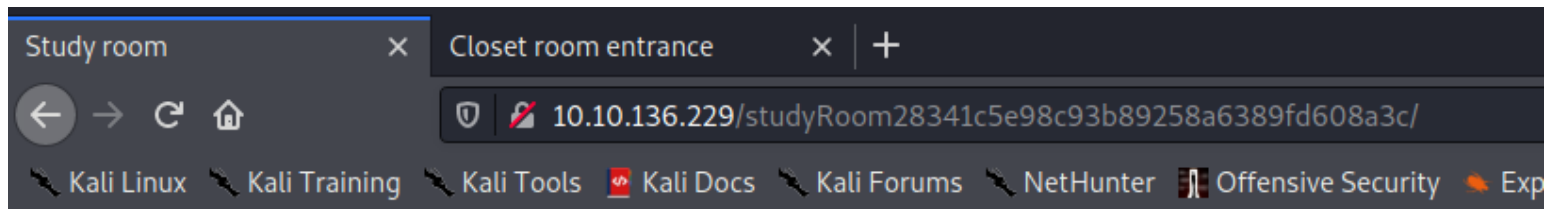
## The Revisit

Still remember the places that we visit before in the mansion map that needs helmet key to unlock?

now let's visit again



& we've unlocked the door



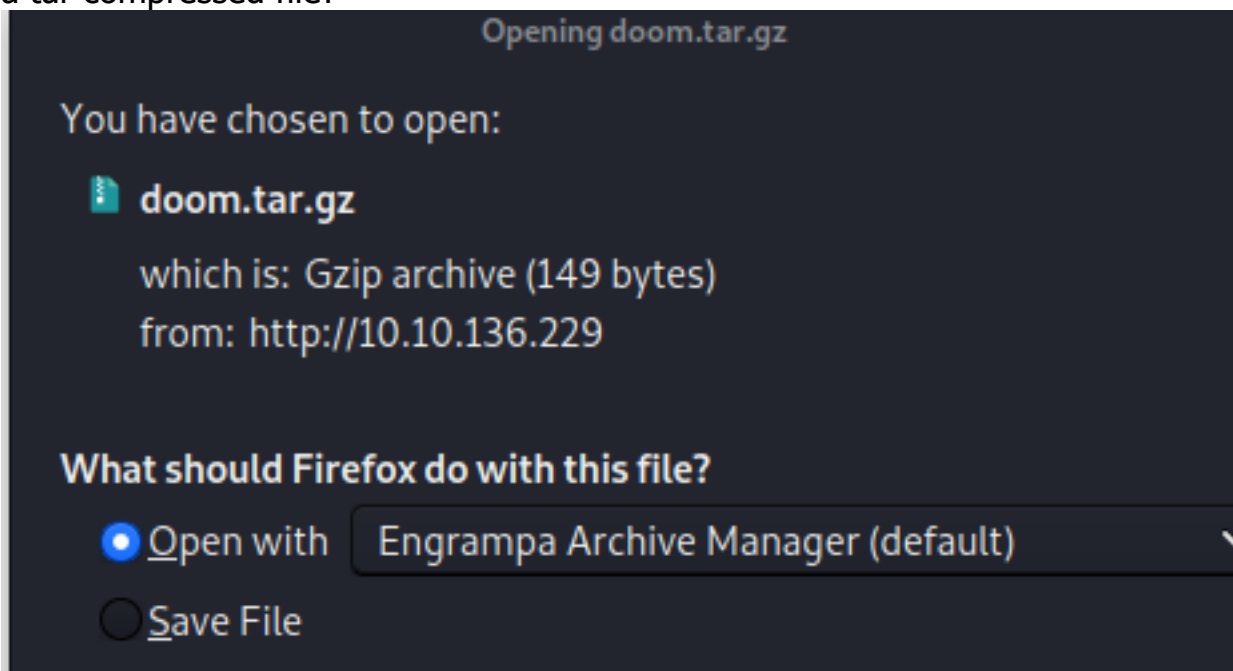
there's a book for us to examine let's check it out

Jill saw a messy table upon enter the room

After a short search, Jill managed to find a sealed book

**Examine the book?** EXAMINE

a tar compressed file?



decompress it & we got a text file



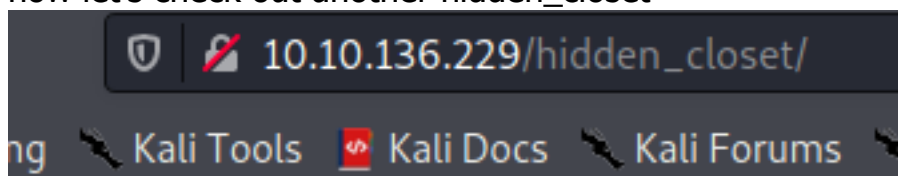
```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$ tar -xvf doom.tar.gz
eagle_medal.txt

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$
```

voila! we got our ssh user!

```
(nobodyatall@0xDEADBEEF)-[~/t
$ cat eagle_medal.txt
SSH user: umbrella_guest
```

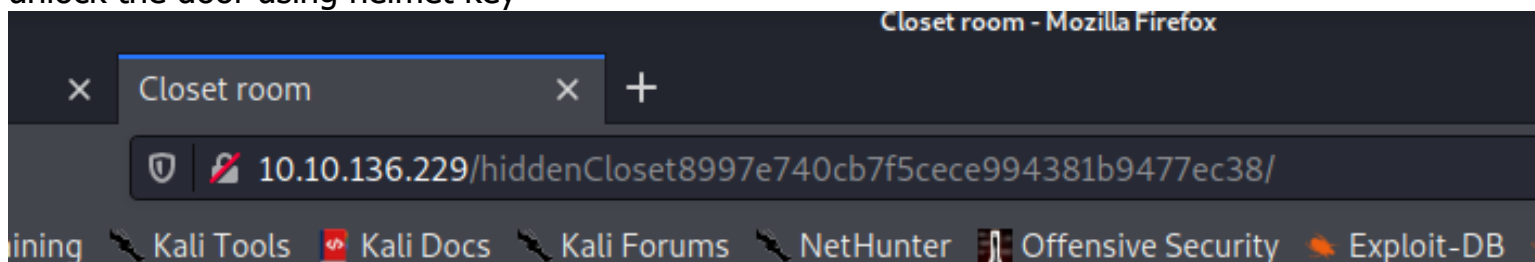
now let's check out another hidden\_closet



Look like the door has been locked

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

unlock the door using helmet key



in the hidden\_closet it'll lead us to an underground cave & we found Enrico

The closet room lead to an underground cave

In the cave, Jill met injured Enrico, the **leader of the STARS Bravo team**. H

seems like there's 2 stuff for us to examine

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](#)

MO disk 1 seems like a ciphertext

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$ cat MO_DISK1.txt
wpbwbxr wpkzg pltwnhro, txrks_xfqsxrd_bvv_fy_rvmexa_ajk
```

wold\_mode.txt content will be our ssh password

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$ cat wolf_medal.txt
SSH password: T_virus_rules

(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
```

## Underground laboratory

gaining access into the remote host using the ssh credential provided & we got our initial foothold

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/biohazard]
$ ssh umbrella_guest@10.10.136.229
umbrella_guest@10.10.136.229's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

320 packages can be updated.
58 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Fri Sep 20 03:25:46 2019 from 127.0.0.1
umbrella_guest@umbrella_corp:~$ id
uid=1001(umbrella_guest) gid=1001(umbrella) groups=1001(umbrella)
umbrella_guest@umbrella_corp:~$
```

in here we noticed that there's a hidden jailcell  
//in there, there's a text file chris.txt

```
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
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
umbrella_guest@umbrella_corp:~/.jailcell$ cat chris.txt
```

the content of chris.txt

/\*

chris was locked in jailcell

weasker was the traitor

Chris gave Jill MO Disk 2 that looks like a key deciphering something

MO disk 2: albert

\*/

```

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 see
m that weasker is behind all this.
Jill, What? Weasker? He is the traitor? S Alpha team.
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
umbrella_guest@umbrella_corp:~/.jailcell$

```

still remember the MO disk 1 that we found it's encrypted? let's use vigenere cipher to decrypt it  
 //now we've the traitor's credential!

Recipe	Input
<b>Vigenère Decode</b> <div> Key  albert </div>	wpbwbxr wpkzg pltwnhro, txrks_xfqsrxd_bvv_fy_rvmexa_ajk
	<b>Output</b> weasker login password, stars_members_are_my_guinea_pig

su into weasker user with the credential found

```

umbrella_guest@umbrella_corp:/home$ su weasker
Password:
weasker@umbrella_corp:/home$ id
uid=1000(weasker) gid=1000(weasker) groups=1000(weasker),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),118(lpadmin),126(sambashare)
weasker@umbrella_corp:/home$

```

weasker user can run any command as root with sudo

```

weasker@umbrella_corp:/home$ sudo -l
[sudo] password for weasker:
Sorry, try again.
[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\
n\:/snap/bin

User weasker may run the following commands on umbrella_corp:
    (ALL : ALL) ALL
weasker@umbrella_corp:/home$

```

now we're root now

```

weasker@umbrella_corp:/home$ sudo /bin/bash
root@umbrella_corp:/home# id
uid=0(root) gid=0(root) groups=0(root)
root@umbrella_corp:/home#

```

in weasker's home directory found a note

```

-rw-r--r--  1 root    root      534 Sep 20  2019 weasker_note.txt

```

the content of the note

//ultimate form Tyrant?

```

root@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, on
ly 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

```

check the root directory & we found our root flag!



```
root@umbrella_corp:/root# ls -la
total 36
drwx----- 4 root root 4096 Sep 20 2019 .
drwxr-xr-x 24 root root 4096 Sep 18 2019 ..
-rw----- 1 root root 76 Sep 20 2019 .bash_history
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwx----- 2 root root 4096 Apr 26 2018 .cache
drwxr-xr-x 3 root root 4096 Sep 19 2019 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 493 Sep 20 2019 root.txt
-rw-r--r-- 1 root root 207 Sep 19 2019 .wget-hsts
root@umbrella_corp:/root# 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, Jill pick up the launcher and fire at the Tyrant.

price was shot dead
The Tyrant shredded into pieces and the Mansion was blowed. The survivor able to escape with the helicopter and prepare for their next fight.

Medal

The End

flag: [REDACTED]
root@umbrella_corp:/root#
```