Biohazard

URL	
Created	@February 25, 2023 12:11 PM
Last edited	@April 28, 2023 10:32 AM
Progress	Done
Tools	Binwalk Steghide Strings exiftool

Task 1 Introduction

Enumeration

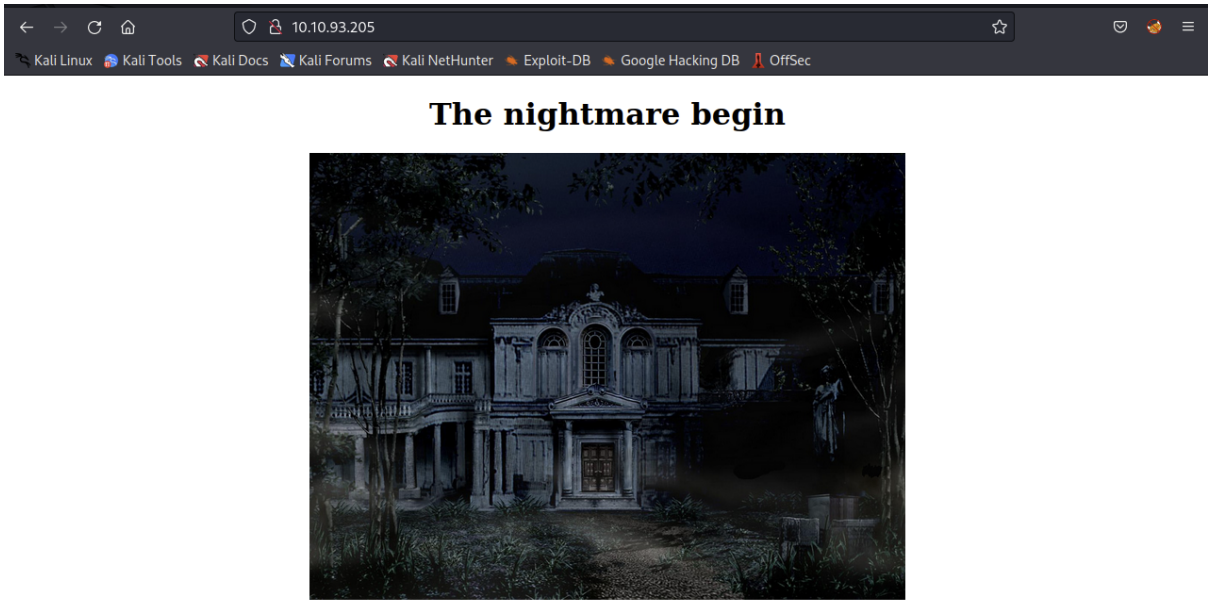
Using Nmap to enumerate ports

```
nmap -sV -p- -Pn 10.10.93.205 -oN Biohazard.nmap
```

```
Nmap scan report for 10.10.93.205
Host is up (0.074s latency).
Not shown: 65532 closed tcp ports (conn-refused)
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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Port	Service	Version
21	ftp	vsftpd 3.0.3
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29

Enumerating http web server



▼ Answer the questions below

📌 We saw on the nmap scan, that there's 3 ports open.
On the web server, we can see a team name; STARS alpha team

Task 2 The Mansion

Main hall

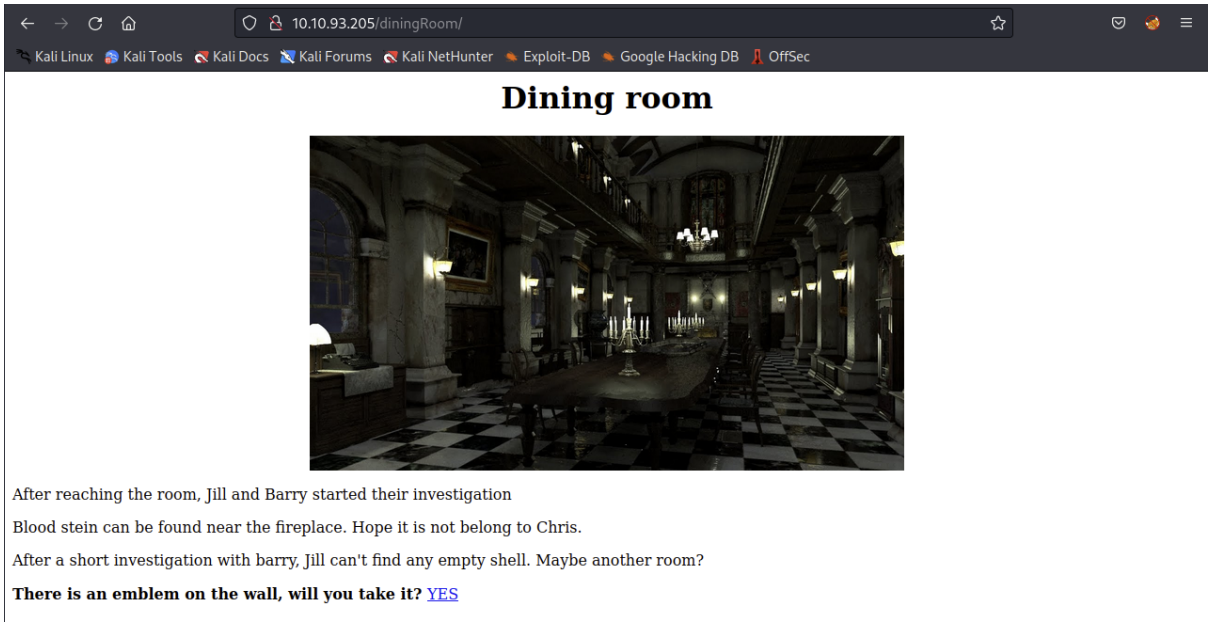
The team reach the mansion safe and sound. However, it appear that Chris is missing

Jill try to open the door but stopped by Weasker

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

The next room is the diningRoom. We can see this in the source code of the Main hall page.

Put the diningRoom in the url.

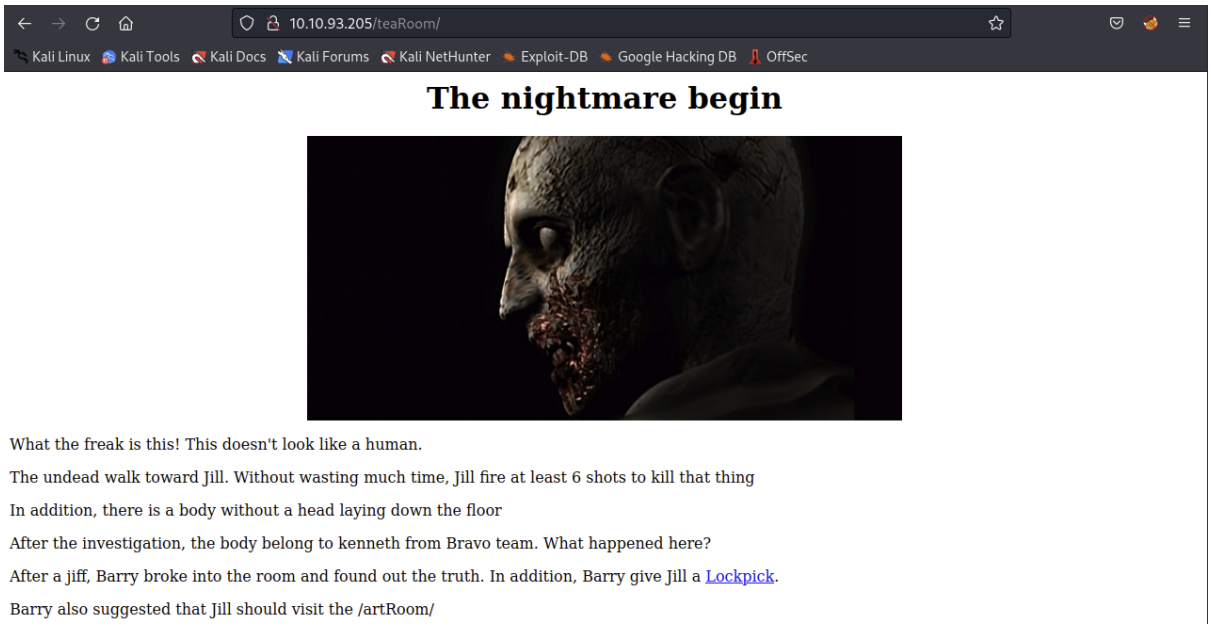


After taking the emblem, and refreshing the diningRoom, a input box has appeared.

Nothing really happens, but looking at the source code again, there's a base64 line

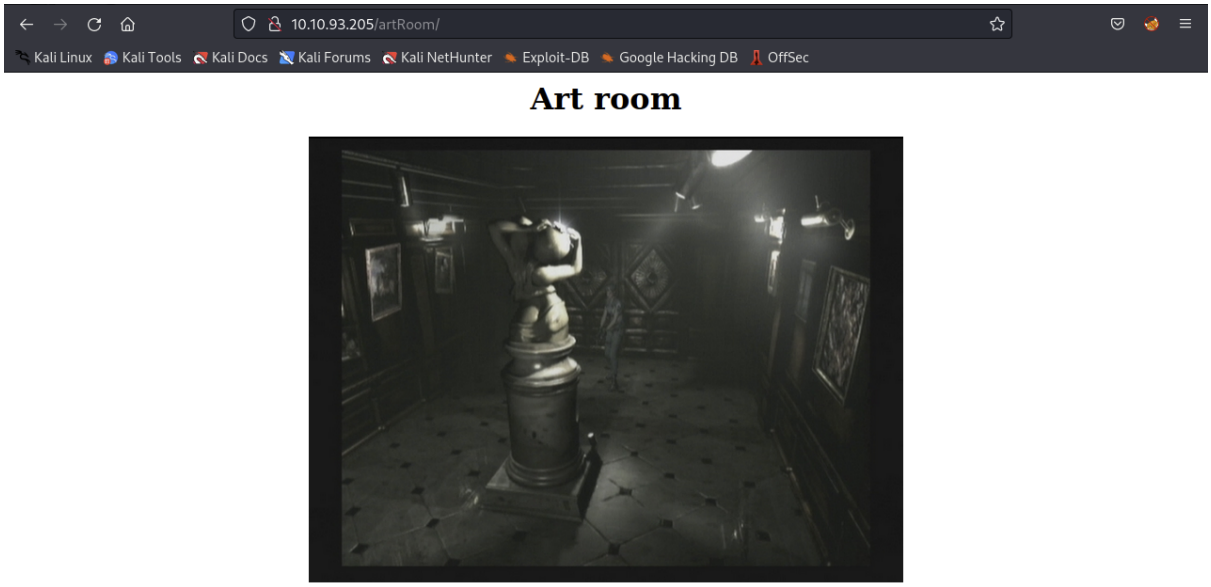
```
<head> </head>
<body> scroll
  <h1 align="center">Dining room</h1> overflow
  <img alt="diningroom" src="../images/maxresdefault.jpg" style="display:
  block;margin-left: auto;margin-right: auto; width: 50%;"> overflow
  <p> </p>
  <p> </p>
  <p> </p>
  <!--SG93IGFib3V0IHRoZSAvdGVhUm9vbS8=-->
  There is an emblem slot on the wall, put the emblem?
  <form action="emblem_slot.php" method="POST">
    <input type="text" name="emblem_slot" col="100" placeholder="Input flag">
    <br>
    <input type="submit" value="submit">
  </form>
</body>
</html>
```

SG93IGFib3V0IHRoZSAvdGVhUm9vbS8=
How about the /teaRoom/



Taking the lock pick ()

And going to the artRoom

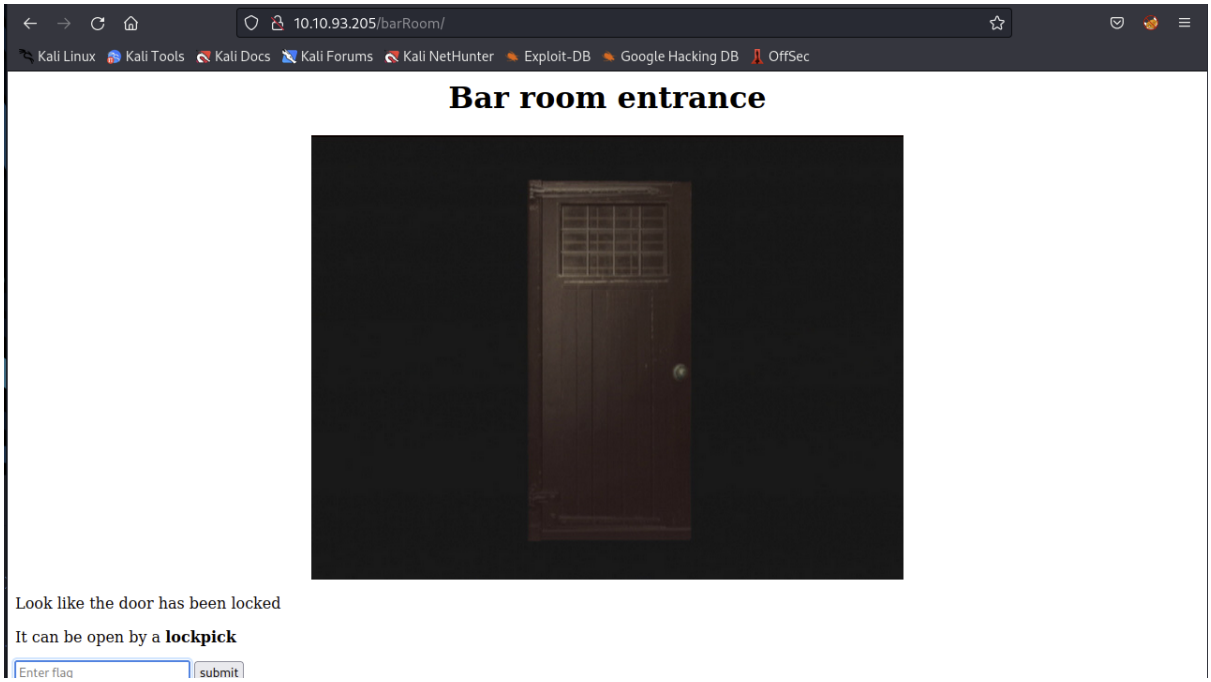


There is a map

```
Look like a map

Location:
/diningRoom/
/teaRoom/
/artRoom/
/barRoom/
/diningRoom2F/
/tigerStatusRoom/
/galleryRoom/
/studyRoom/
/armorRoom/
/attic/
```

Going to the barRoom

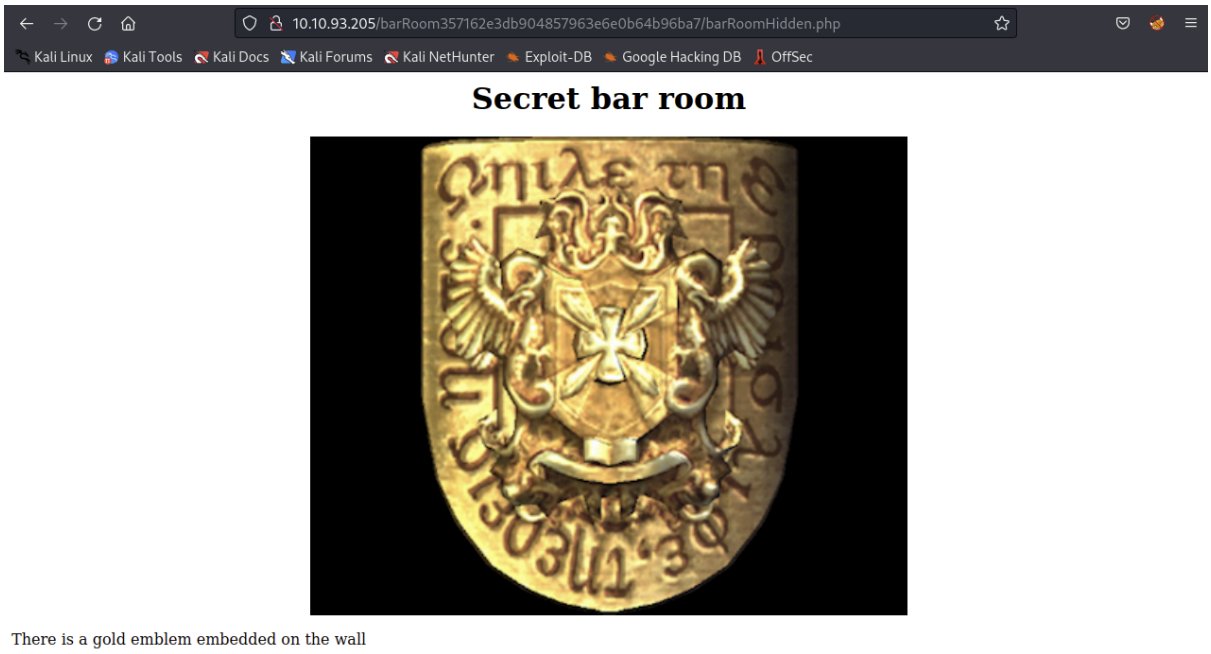


There's a piano in the barRoom - missing the key. There is a note though;

`NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5`

Putting it in CyberChef and using the Magic operations reveals it is a base32 string

```
music_sheet{362d72deaf65f5bdc63daece6a1f676e}
```



There's a gold emblem (`gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}`).

I'll try to use it in the diningRoom

This reveals another string
`klfvg ks r wimgnd biz mpuiui ulg fiemok tqod. Xii jvmc tbkg ks tempgf tyi_hvgct_jljinf_kvc`

I'm guessing this is a simple Caesar code… After some time, I checked the hint. Apparently it is a Vigenére cipher with a key of `rebecca` found later.

```
there is a shield key inside the dining room. The html page is called the_great_shield_key
```

Going to http://10.10.93.205/diningRoom/the_great_shield_key.html

The gem is used in the tigerStatusRoom

Shield symbol is needed in the attic

Shield symbol is needed in the armourRoom

Helmet symbol is needed in the studyRoom

Note in the galleryRoom

```
crest 2:
GVFWK5KHK5WTGTCILE4DKY3DNN4GQQRTM5AVCTKE
Hint 1: Crest 2 has been encoded twice
Hint 2: Crest 2 contanis 18 letters
Note: You need to collect all 4 crests, combine and decode to reavel 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 decod
```

There's a blue gem on the 1. floor in the diningRoom (Mansion Key)

If we look at the source code in diningRoom2F we get a encoded string

```
Lbh trg gur oyhr trz ol chfuvat gur fgnghf gb gur ybjre sybbe. Gur trz vf ba gur qvavatEbbz svefg sybbe. Ivfvg fnccuver.ugzy
```

I used (guessing) ROT13 encoding

```
You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphire.html
```

Going to the url: http://10.10.93.205/diningRoom/sapphire.html

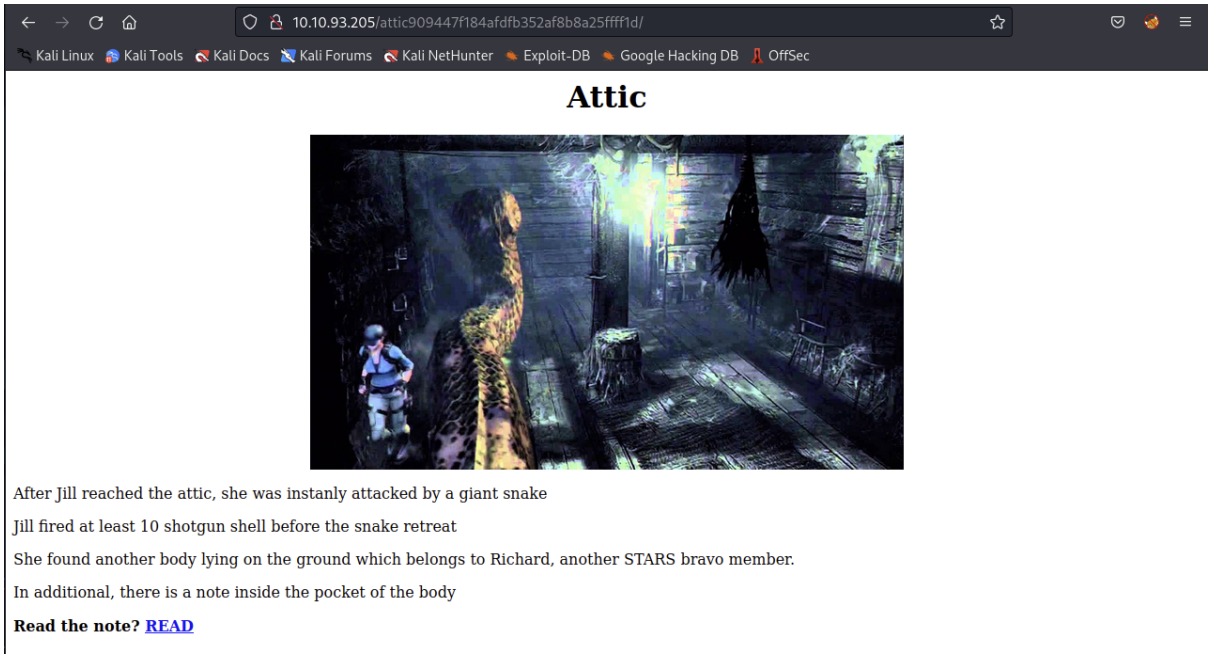
I got the blue_jewel key (`blue_jewel{e1d457e96cac640f863ec7bc475d48aa}`)

In the tigerStatusRoom we can put in the blue jewel

```
crest 1:
S0pXRkVVS0pKQkxIVVdTWUpFM0VTUlk9
Hint 1: Crest 1 has been encoded twice
Hint 2: Crest 1 contanis 14 letters
Note: You need to collect all 4 crests, combine and decode to reavel 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 decod
```

Putting in the first emblem flag (`emblem{fec832623ea498e20bf4fe1821d58727}`) we get the name `rebecca`

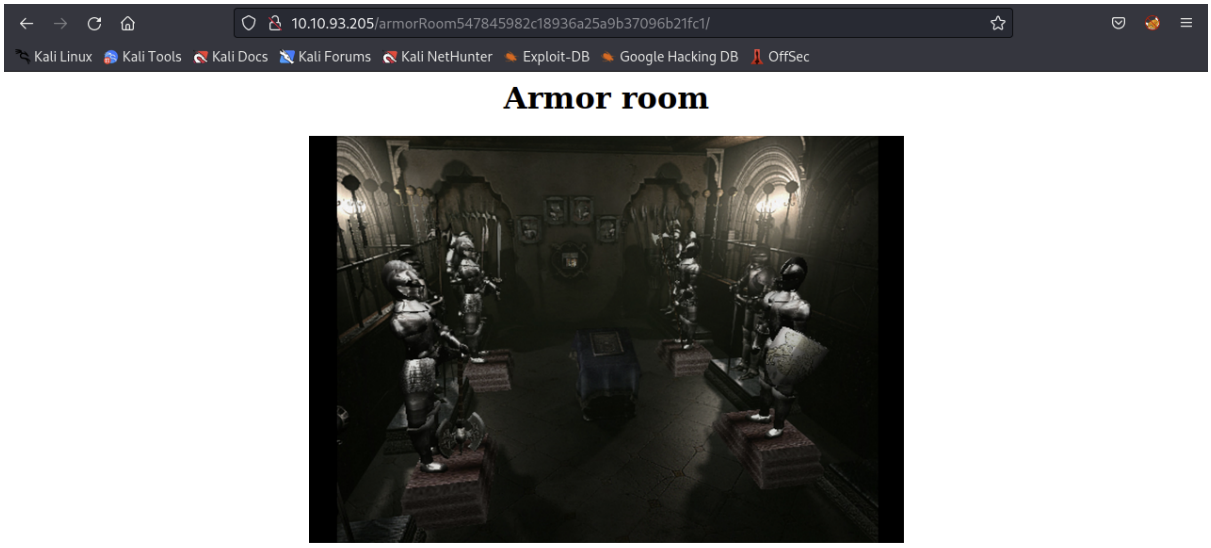
We can now enter the attic with the shield key (`shield_key{48a7a9227cd7eb89f0a062590798cbac}`)



Another note

```
crest 4:
gSUERauVpvKzRpyPpuYz66JDmRTbJubaoArM6CAQsnVwte6zF9J4GGYyun3k5qM9ma4s
Hint 1: Crest 2 has been encoded twice
Hint 2: Crest 2 contanis 17 characters
Note: You need to collect all 4 crests, combine and decode to reavel 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 decod
```

We can also go to the armourRoom with the shield key (`shield_key{48a7a9227cd7eb89f0a062590798cbac}`)




```
crest 3:
MDAxMTAxMTAgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAwMTEgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAxMDAgMDExMDAxMDAgMDAxMDAwMDAgMDAxMTAwMTEgMDAxMTAxMTAgMD
Hint 1: Crest 3 has been encoded three times
Hint 2: Crest 3 contanis 19 letters
```

```
Note: You need to collect all 4 crests, combine and decode to reavel 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 decod
```

```
Crest 1: From Base64 - From Base32
RlRQIHVzZXI6IG
```

```
Crest 2: From Base32 - From Base58
h1bnRlciwgRlRQIHBh
```

```
Crest 3: From Base64 - From Binary - From Hex
c3M6IHlvdV9jYW50X2h
```

```
Crest 4: From Base58 - From Hex
pZGVfZm9yZXZlcg==
```

```
RlRQIHVzZXI6IGh1bnRlciwgRlRQIHBhc3M6IHlvdV9jYW50X2hpZGVfZm9yZXZlcg==
This is Base64
FTP user: hunter, FTP pass: you_cant_hide_forever
```

Task 3 The guard house

Using ftp to enumerate the room

```
ftp 10.10.93.205
Connected to 10.10.93.205.
220 (vsFTPd 3.0.3)
Name (10.10.93.205:muninn): hunter
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53196|)
150 Here comes the directory listing.
-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
```

Got all the files and tried to read `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

From,
Barry
```

Used `binwalk` on `001-key.jpg` but nothing special.

Then tried steghide

```
steghide --extract -sf 001-key.jpg
```

This worked without any password

```
cat key-001.txt
cGxhbnQ0Ml9jYW
```

Also tried `binwalk` on `002-key.jpg` but nothing came up ether.

Couldn't use `steghide` on `002-key.jpg` ether, but using `strings` i fount a string that looks like the string from `key-001.txt` and `key-003.txt`.

```
strings 002-key.jpg
JFIF
5fYmVfZGVzdHJveV9
...
```

we could also have used `exiftool 002-key.jpg`

Using `binwalk` on `003-key.jpg`

```
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
```

Extracting the ziped archive

```
binwalk 003-key.jpg -e

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
```

In the archive I wound a key-003.txt

```
cat key-003.txt
3aXRoX3Zqb2x0
```

Combining them all and decoding it from Base64, we get

```
plant42_can_be_destroy_with_vjolt
```

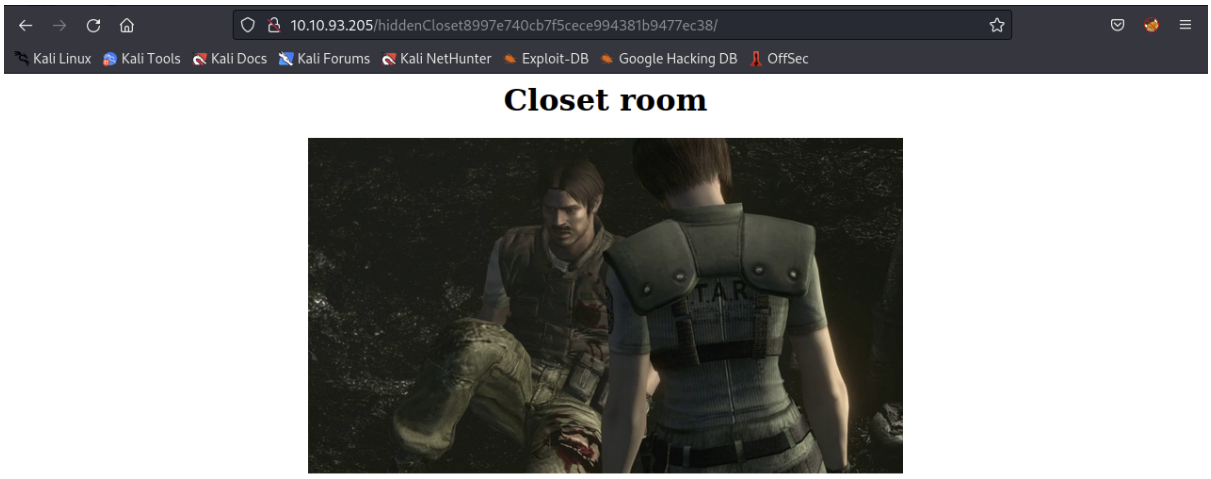
Which is the password for the encrypted `helmet_key.txt.gpg` file. Now we can unencrypt the file:

```
gpg --decrypt helmet_key.txt.gpg > helmet_key.txt
gpg: keybox '/home/muninn/.gnupg/pubring.kbx' created
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase

cat helmet_key.txt
helmet_key{458493193501d2b94bbab2e727f8db4b}
```

Task 4 The Revisit

Enter the hiddenCloset directory



The MO_DISK1.txt

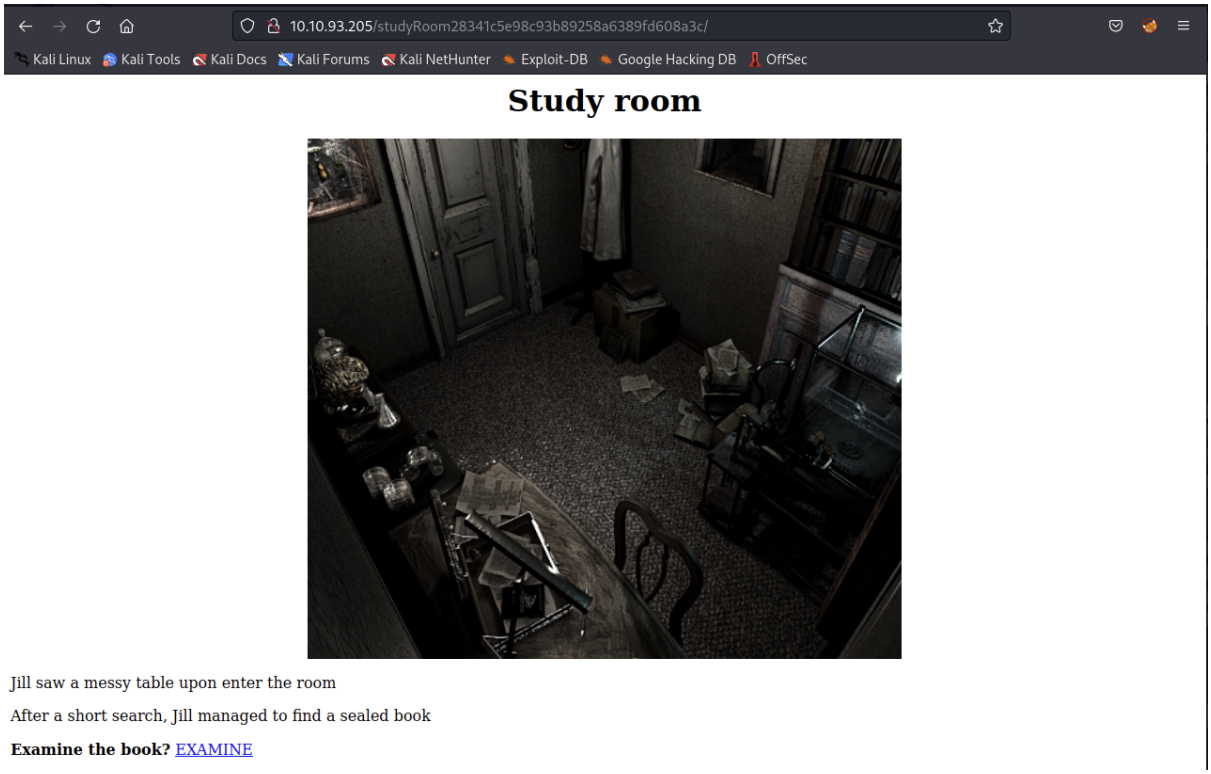
```
wpbwbxr wpkzg pltwnhro, txrks_xfqsxrd_bvv_fy_rvmexa_ajk
```

The wolf_medal.txt

```
SSH password: T_virus_rules
```

I missed a room

The helmet key is also used in the studyRoom



There's a doom,.tar.gz file

```
tar -ztvf doom.tar.gz
-rw-r--r-- root/root        25 2019-09-20 09:02 eagle_medal.txt

tar -zxf doom.tar.gz

cat eagle_medal.txt
SSH user: umbrella_guest
```

Task 5 Underground laboratory

Looking around the machine (through ssh)

There is a note `weasker_note.txt` in the `/home/weasker` directory

```
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
```

Trying to find Chris

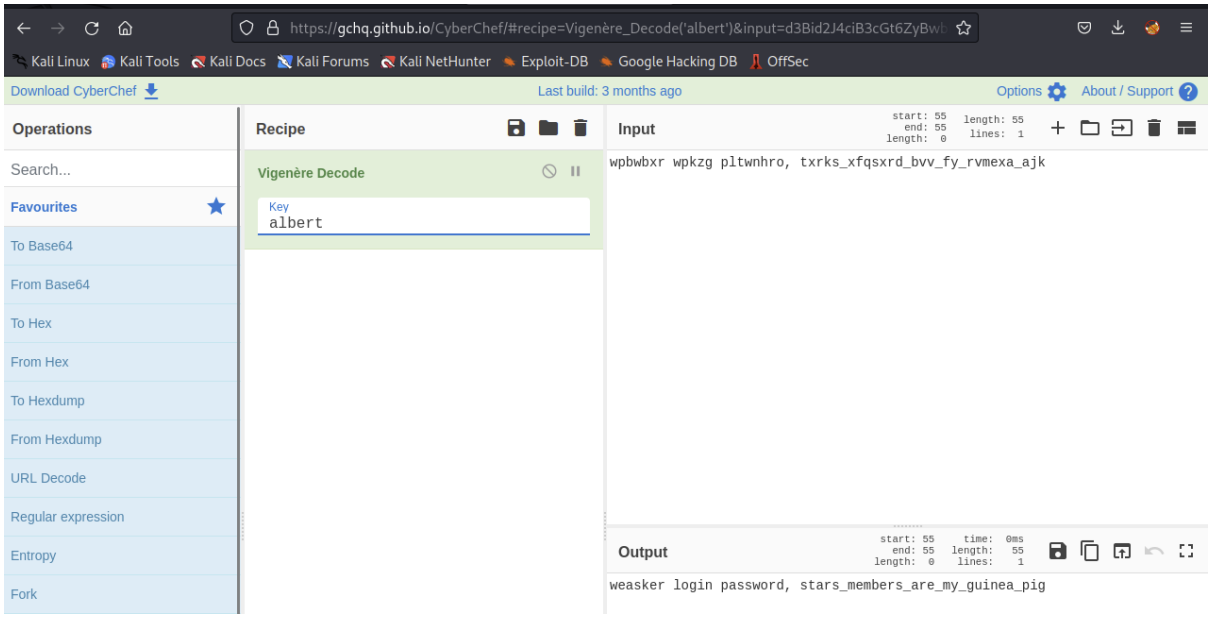
```
find / -type f -name "chris*" 2>/dev/null
```

```
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
```

We still haven't decrypt the MO disk 1 text

```
wpbwbxr wpkzg pltwnhro, txrks_xfqsxrd_bvv_fy_rvmexa_ajk
```



Changing user to weasker

```
su weasker
```

Now, I'll try to elevate the user to root

```
groups
weasker adm cdrom sudo dip plugdev lpadmin sambashare
```

```
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 use all `sudo` commands

```
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
```