# *Biohazard*

## Biohazard

**A CTF room based on the old-time survival horror game, Resident Evil. Can you survive until the end?**

# *writeup*

## ----------[Task 1] Introduction----------

**--started off with sudo bash auto-recon.sh <IP-Address> and found 3 open ports 21, 22, and 80**
**--went to http://<IP-Address> and found the team name STARS alpha team and possible usernames Chris, Jill, Barry, Weasker and Joseph**

## ----------[Task 2] The-Mansion----------

**--went to /mansionmain/ and donloaded image, just incase (stego was one of the hints), and found /diningRoom/ in comment in source code**
**--went to /diningRoom/ and found a string and a flag:**
**SG93IGFib3V0IHRoZSAvdGVhUm9vbS8= decoded= 'How about the /teaRoom/'**
**emblem{fec832623ea498e20bf4fe1821d58727}**

**--/diningRoom/ now has an input form, so I entered the emblem flag and it returned 'Nothing happen'**
**--went to /teaRoom/ page and found /artRoom/ in source code and a link <a href="master_of_unlock.html">Lockpick</a> that contains a flag:**
**lock_pick{037b35e2ff90916a9abf99129c8e1837}**

**--went to /artRoom/ and found an embedded link 'YES', so I clicked it and got:**
**Look like a map**
**Location:**
**/diningRoom/**
**/teaRoom/**
**/artRoom/**
**/barRoom/**
**/diningRoom2F/**
**/tigerStatusRoom/**
**/galleryRoom/**
**/studyRoom/**
**/armorRoom/**
**/attic/**
**sapphire.html**
**barRoomHidden.php**

**--went to /barRoom/ and found a login form saying 'be open by a lockpick' so I entered 'lock_pick{037b35e2ff90916a9abf99129c8e1837}'**
**--login form took me to /barRoom357162e3db904857963e6e0b64b96ba7/ that has a link '"moonlight somata", read it? READ' that contains:**
**Look like a music note**
**NV2XG2LDL5ZWQZLFOR5TGNRSMQ3TEZDFMFTDMNLGGVRGIYZWGNSGCZLDMU3GCMLGGY3TMZL5**

**--decoded with base32:**
**music_sheet{362d72deaf65f5bdc63daece6a1f676e}**

**--entered music_sheet emblem in the form on /barRoom357162e3db904857963e6e0b64b96ba7/ took me to /barRoom357162e3db904857963e6e0b64b96ba7/barRoomHidden.php**
**--/barRoomHidden.php contains another form asking for an emblem slot, I inputted emblem{fec832623ea498e20bf4fe1821d58727} and it gave me:**
**rebecca**

**--went back to /diningRoom/ and entered gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843} and it gave me:**
**klfvg ks r wimgnd biz mpuiui ulg fiemok tqod. Xii jvmc tbkg ks tempgf tyi_hvgct_jljinf_kvc**
**decoded with viginere cipher and key of rebecca = there is a shield key inside the dining room. The html page is called the_great_shield_key**

**--tried /diningRoom/the_great_shield_key.html and found sheild key:**
**shield_key{48a7a9227cd7eb89f0a062590798cbac}**

**--went to /dinigRoom2F/ and in source code I found a ROT13 cipher 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**
**ROT13 decoded = You get the blue gem by pushing the status to the lower floor. The gem is on the diningRoom first floor. Visit sapphire.html**

--went to /diningRoom/sapphire.html and found blue gem flag:
blue_jewel{e1d457e96cac640f863ec7bc475d48aa}

--investigated the /galleryRoom/ and followed the link to /galleryRoom/note.txt and it gave me crest2(on crests page):
--went to /tigerStatusRoom/ entered blue_jewel{e1d457e96cac640f863ec7bc475d48aa} and it gave me crest1(on crests page):
--went to /armorRoom/ and entered sheild key to get crest3(on crests page)
--went to /attic/ page and entered shield key to get crest4(on crests page)
--decoded the crests on crest node and got:
FTP user: hunter, FTP pass: you_cant_hide_forever

## ----------[Task 3] The-Guard-House----------

--went to ftp://<IP-address> and downloaded all 5 files to my local machine - 001-key.jpg, 002-key.jpg, 003-key.jpg, helmet_key.txt.gpg, important.txt
--while reading important.txt I found the hidden directory /hidden_closet/
--ran exiftool on image files and image 2 and 3 have comments containing:
002-key.jpg - 5fYmVfZGVzdHJveV9
003-key.jpg - 'Compressed by jpeg-recompress'

--found data in 001-key.jpg by running steghide extract -sf 001-key.jpg:
cGxhbnQ0Ml9jYW

--found hidden files in 003-key.jpg with binwalk -e 003-key.jpg, and the new file key-003.txt contains:
3aXRoX3Zqb2x0

--combine the 3 strings found and decode using base64 to get password:
cGxhbnQ0Ml9jYW5fYmVfZGVzdHJveV93aXRoX3Zqb2x0
plant42_can_be_destroy_with_vjolt

--decrypt gpg file with the password above and get helmet key flag:
helmet_key{458493193501d2b94bbab2e727f8db4b}

## ----------[Task 4] The-Revisit----------

--since the /studyRoom/ is the only room from earlier I haven't been to yet, I decided to start there
--entered helmet_key to get to next room /studyRoom28341c5e98c93b89258a6389fd608a3c/ that contains a link 'EXAMINE'
--upon clicking 'EXAMINE' a file is downloaded called doom.tar.gz, extract it to get eagle_medal.txt that contains SSH username:
umbrella_guest

--only place left to check is /hidden_closet/ from previous task
--room contains 2 links, 1 to MO_DISK1.txt, and another to wolf_medal.txt:
wolf_medal.txt contains - SSH password: T_virus_rules
MO_DISK1.txt contains - 'wpbwbxr wpkzg pltwnhro, txrks_xfqsxrd_bvv_fy_rvmexa_ajk'
--tried decrypting by brute forcing the viginere cipher, but had no success, so I moved on to SSH

## ----------[Task 5] Underground Labratory----------

--logged in to SSH with command ssh umbrella_guest@<IP-address> and password T_virus_rules
--running ls -al I found a hidden directory called /.jailcell/ that contains file chris.txt
--ran cat chris.txt and got:
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**

**--according to chris, weasker is the traitor**
**--and the key to decode the viginere cipher is 'albert' and it decodes to:**
**weasker login password, stars_members_are_my_guinea_pig**

**--logged in to SSH with ssh weasker@<IP-address> and password stars_members_are_my_guinea_pig**
**--ran ls -al and found weasker_note.txt containing the following text:**
**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**

**--according to weasker tyrant is the ultimate form**
**--ran sudo -l and got:**
**User weasker may run the following commands on umbrella_corp:**
**    (ALL : ALL) ALL**

**--ran sudo bash to get root shell since we can run anything as root and it is the easiest**
**--ran cat /root/root.txt and got the flag inside of the following note:**
**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.**
**The Tyrant shredded into pieces and the Mansion was blowed. The survivor able to escape with the helicopter and prepare for their next fight.**
**The End**

# flag: 3c5794a00dc56c35f2bf096571edf3bf

# *recon-scans*

## NMAP Scan

```
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-
methods:
|_  Supported Methods: OPTIONS HEAD GET
POST
|_http-server-header: Apache/2.4.29
(Ubuntu)
|_http-title: Beginning of the end          100
```

## buster-scan

```
DirBuster 1.0-RC1 - Report
-----------------------------
```

### Directories:

```
Dirs found with a 200 response:
/
/diningRoom2F/
/teaRoom/
/armorRoom/
/tigerStatusRoom/
/barRoom/
/artRoom/
/diningRoom/
/galleryRoom/
/studyRoom/
/attic/
/barRoom357162e3db904857963e6e0b64b96ba7/
/images/
/barRoom357162e3db904857963e6e0b64b96ba7/barRoomHidden.php/
/mansionmain/

Dirs found with a 403 response:
/icons/
--------------------------------
```

### Files:

```
Files found with a 200 responce:
/galleryRoom/note.txt
/artRoom/MansionMap.html
/teaRoom/master_of_unlock.html
/barRoom357162e3db904857963e6e0b64b96ba7/musicNote.html
/attic/unlock_door.php
/armorRoom/unlock_door.php
/images/maxresdefault.jpg.3
/images/maxresdefault.jpg.2
/barRoom/unlock_door.php
```

**/studyRoom/unlock_door.php**
**/diningRoom/emblem_slot.php**
**/tigerStatusRoom/gem.php**
**/images/maxresdefault.jpg.1**
**/barRoom357162e3db904857963e6e0b64b96ba7/piano.php**
**/images/maxresdefault.jpg.4**
**/images/zombie**
**/images/maxresdefault.jpg.5**

**Files found with a 301 responce:**
**/mansionmain**
**---------------------------------**

# *crests*

**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 decode it**
**base64 > base32**
**RlRQIHVzZXI6IG**

**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 decode it**
**base32 > base58**
**h1bnRlciwgRlRQIHBh**

**crest 3:**
**MDAxMTAxMTAgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAwMTEgMDAxMTAwMTEgMDAxMDAwMDAgMDAxMTAxMD**
**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 decode it**
**base64 > binary > hex**
**c3M6IHIvdV9jYW50X2h**

**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 decode it**
**base58 > hex**
**pZGVfZm9yZXZlcg==**

**RlRQIHVzZXI6IGh1bnRlciwgRlRQIHBhc3M6IHIvdV9jYW50X2hpZGVfZm9yZXZlcg==**
**FTP user: hunter, FTP pass: you_cant_hide_forever**

# *[Task 1] Introduction*

**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?**
**If you have any question, do not hesitate to DM me on the discord channel.**

| **#1** |
| --- |
| Deploy the machine and start the nightmare |

## No answer needed

| **#2** |
| --- |
| How many open ports? |

## 3

| **#3** |
| --- |
| What is the team name in operation |

## STARS alpha team

# *[Task 2] The Mansion*

**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**

| **#1** |
| --- |
| What is the emblem flag |

**emblem{fec832623ea498e20bf4fe1821d58727}**

| **#2** |
| --- |
| What is the lock pick flag |

**lock_pick{037b35e2ff90916a9abf99129c8e1837}**

| **#3** |
| --- |
| What is the music sheet flag |

**music_sheet{362d72deaf65f5bdc63daece6a1f676e}**

| **#4** |
| --- |
| What is the gold emblem flag |

**gold_emblem{58a8c41a9d08b8a4e38d02a4d7ff4843}**

| **#5** |
| --- |
| What is the shield key flag |

**shield_key{48a7a9227cd7eb89f0a062590798cbac}**

| **#6** |
| --- |
| What is the blue gem flag |

**blue_jewel{e1d457e96cac640f863ec7bc475d48aa}**

| **#7** |
| --- |
| What is the FTP username |

**hunter**

| **#8** |
| --- |
| What is the FTP password |

**you_cant_hide_forever**

# *[Task 3] The guard house*

**After gaining access to the FTP server, you need to solve another puzzle.**

**FTP Credentials:**
**hunter**:**you_cant_hide_forever**

| **#1** |
| --- |
| Where is the hidden directory mentioned by Barry |

## /hidden_closet/

| **#2** |
| --- |
| Password for the encrypted file |

## plant42_can_be_destroy_with_vjolt

| **#3** |
| --- |
| What is the helmet key flag |

## helmet_key{458493193501d2b94bbab2e727f8db4b}

## *[Task 4] The Revisit*

**Done with the puzzle? There are places you have explored before but yet to access.**

| #1 |
| --- |
| What is the SSH login username |

**umbrella_guest**

| #2 |
| --- |
| What is the SSH login password |

**T_virus_rules**

| #3 |
| --- |
| Who the STARS bravo team leader |

**Enrico**

## *[Task 5] Underground laboratory*

**Time for the final showdown. Can you escape the nightmare?**

| #1 |
| --- |
| Where you found Chris |

**.jailcell**

| #2 |
| --- |
| Who is the traitor |

**weasker**

| #3 |
| --- |
| The login password for the traitor |

**stars_members_are_my_guinea_pig**

| #4 |
| --- |
| The name of the ultimate form |

**tyrant**

| #5 |
| --- |
| The root flag |

**3c5794a00dc56c35f2bf096571edf3bf**