**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](https://www.stationx.net/nmap-cheat-sheet/)

**Enumeration**

* gobuster : directory fuzzing (understand status codes)
  + [How to Scan Websites for Interesting Directories & Files with Gobuster](https://null-byte.wonderhowto.com/how-to/scan-websites-for-interesting-directories-files-with-gobuster-0197226/)
  + [HTTP - Status Codes](https://www.tutorialspoint.com/http/http_status_codes.htm)

**Exploitation**

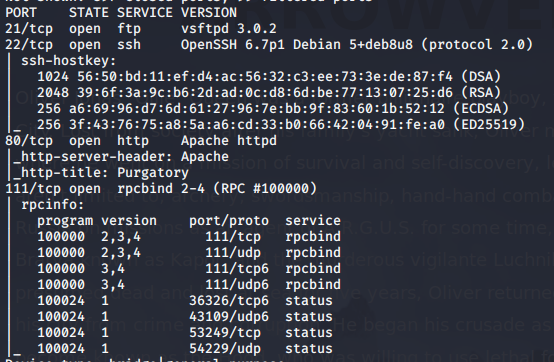
* steghide

**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

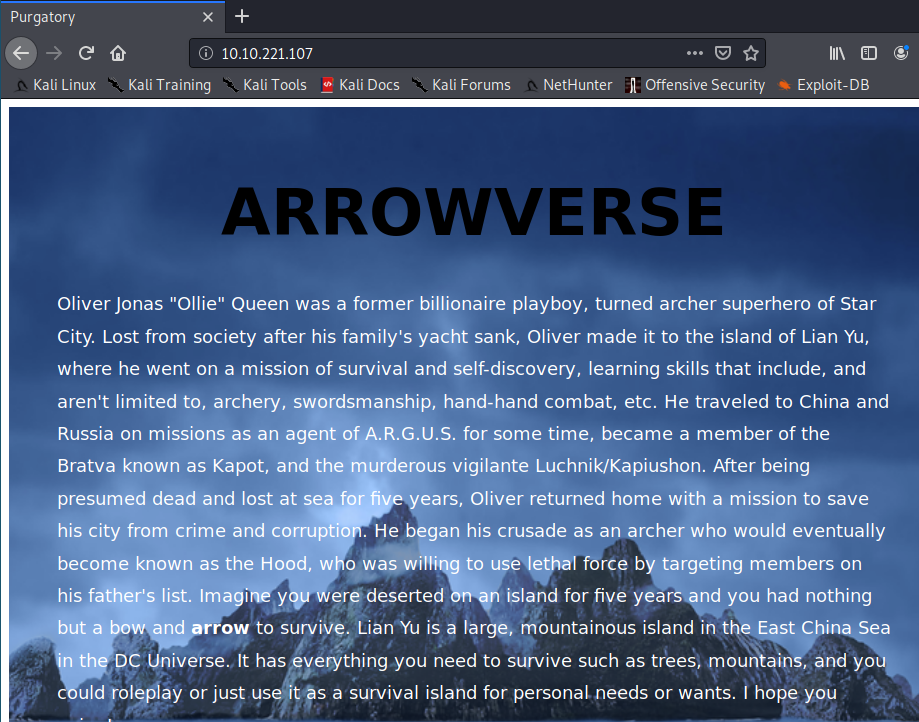
**-- 1. Port 21 running on TCP**

**-- 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!

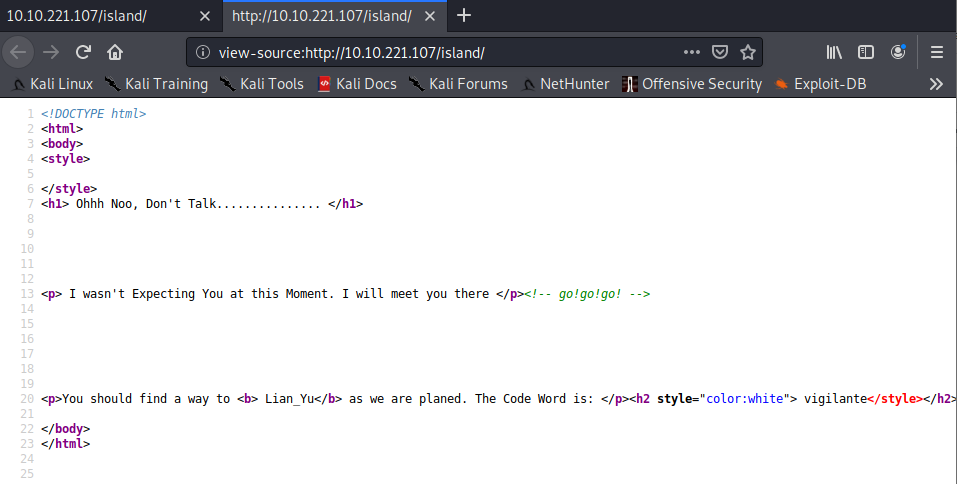


I am going to use gobuster to perform a dictionary attack to see if I can find any web directories.

gobuster dir -u http://10.10.221.107 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

**Found: /island (Status: 301)**

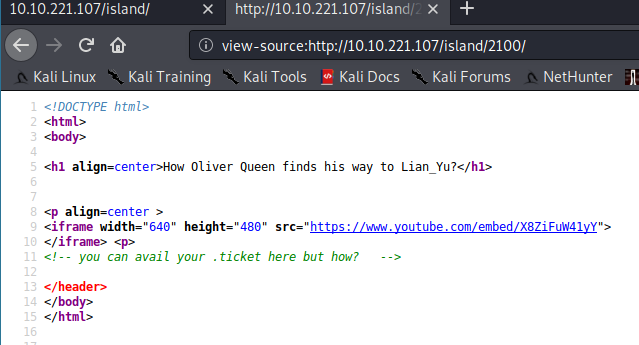
So I continued to *http://10.10.221.107/island* and viewed the page source. Guess what I found… ‘vigilante’ hidden due to its color being set to white. (This could be a possible user).



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*

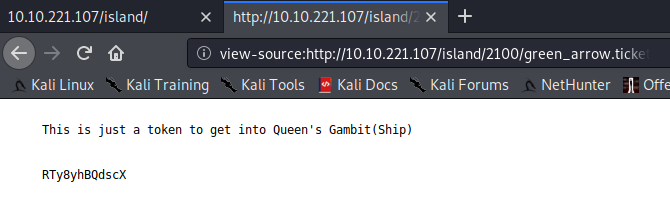
**Found: /2100 (Status: 301)**

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

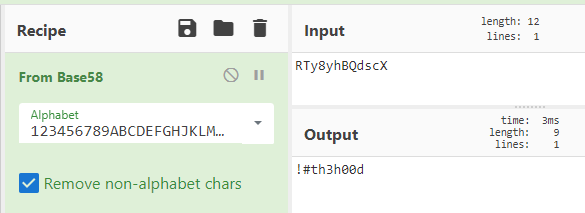


There is a comment with an extension .ticket, so I’m going to do another enumeration specifying the extension (-x) with gobuster.

**Found: /green\_arrow.ticket (Status: 301)**



This looks like a password, but it seems to be encrypted. Let’s fire up CyberChef ([GCHQ CyberChef](https://gchq.github.io/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.

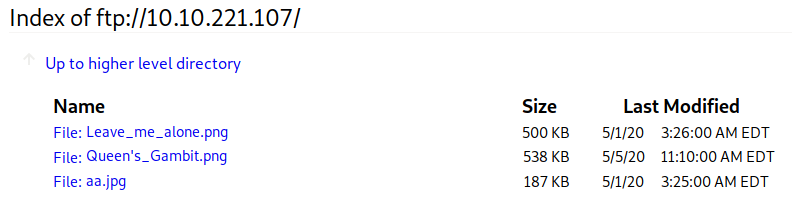
I saw Port 21 (ftp) up so lets try it with the possible credentials?

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:



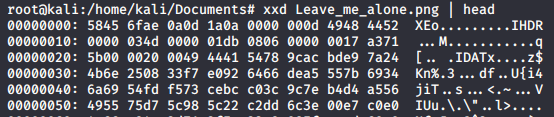
Well I’m curious to see what pictures they store so I start clicking on them. However “Leave\_me\_alone.png” has an error and is unable to display the picture. Time to find out why!

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](https://www.wikiwand.com/en/List_of_file_signatures))

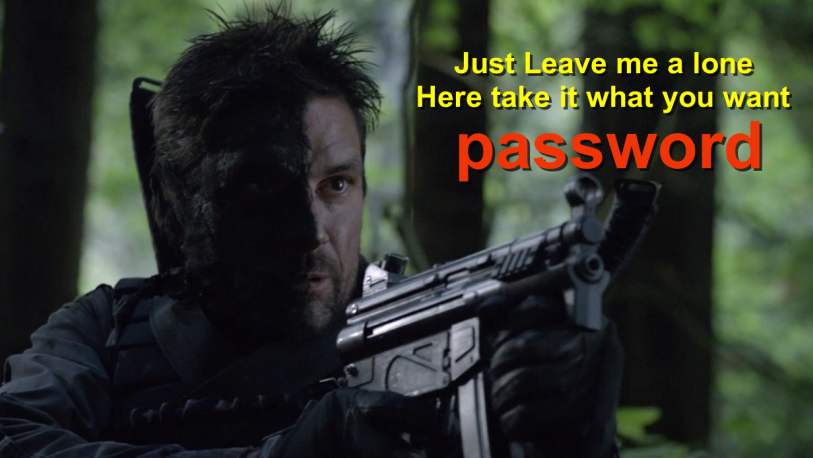
xxd Leave\_me\_alone.png | head

****

* 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:

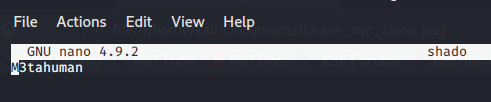
Well this seems to be like the perfect password :) I tried logging into SSH with vigilante and this new password but it didn’t work, so I have to keep searching.

steghide extract -sf aa.jpg

| wrote extracted data to “ss.zip”

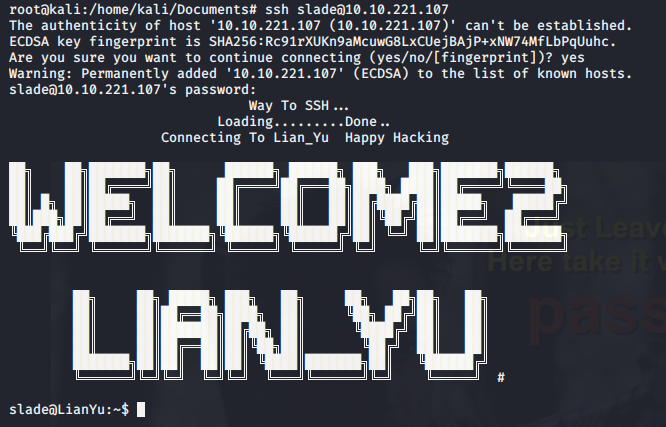
The passphrase was the password we found in “Leave\_me\_alone.png.” I then proceeded to unzip the file and found two text files.

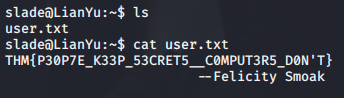
* passwd.txt
* shado



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





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

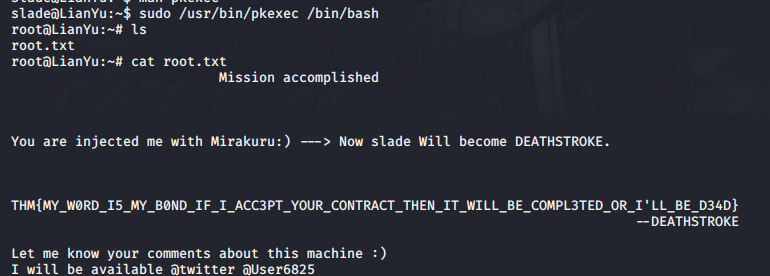
sudo -l

|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.





**By: Nicole Wong**