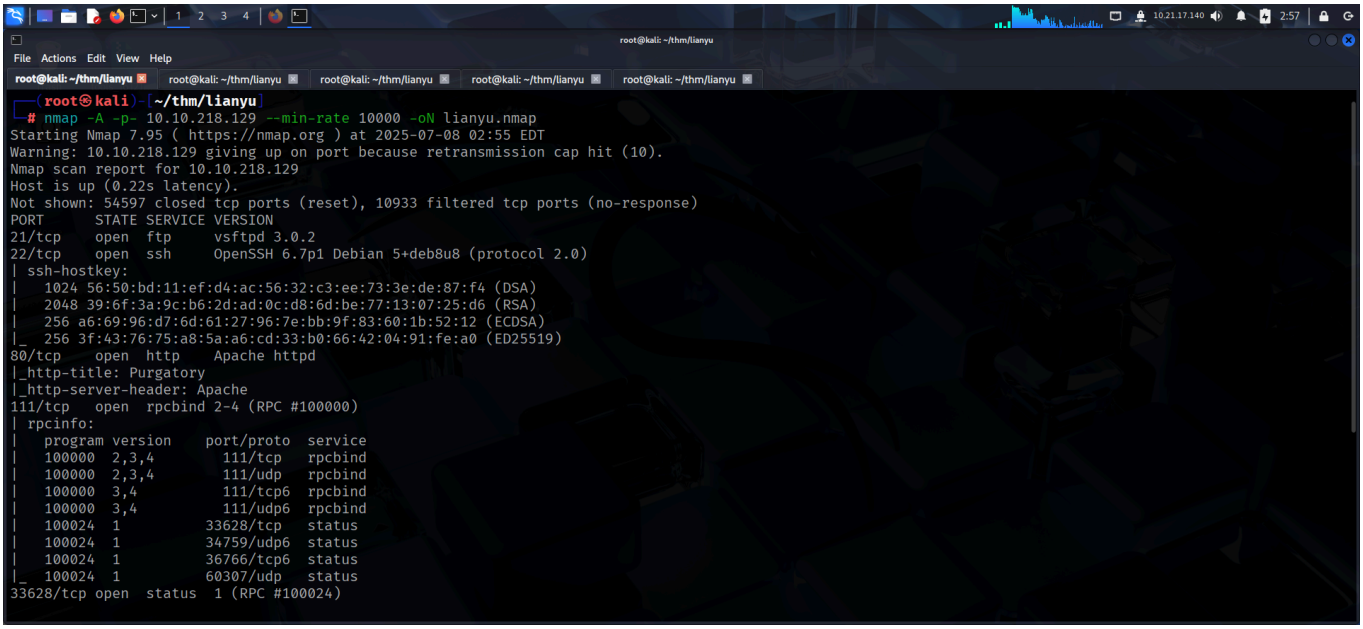
LIANYU

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

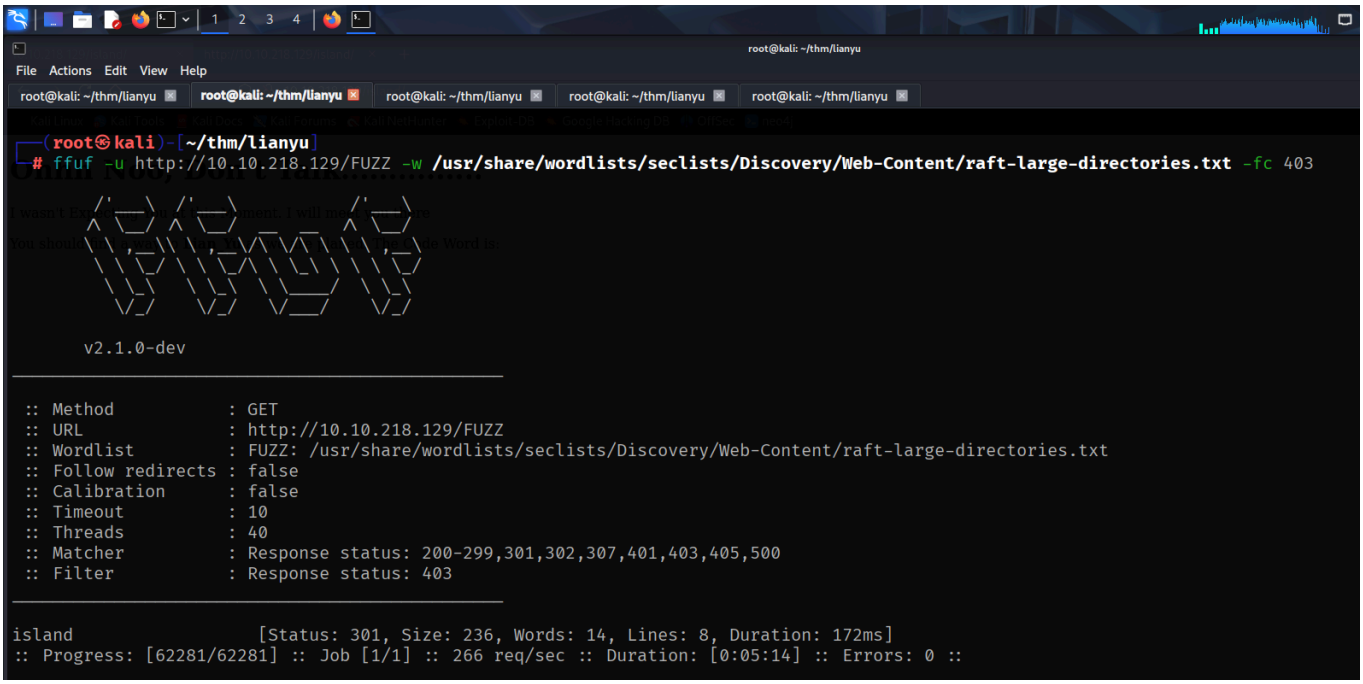
SCANNING

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

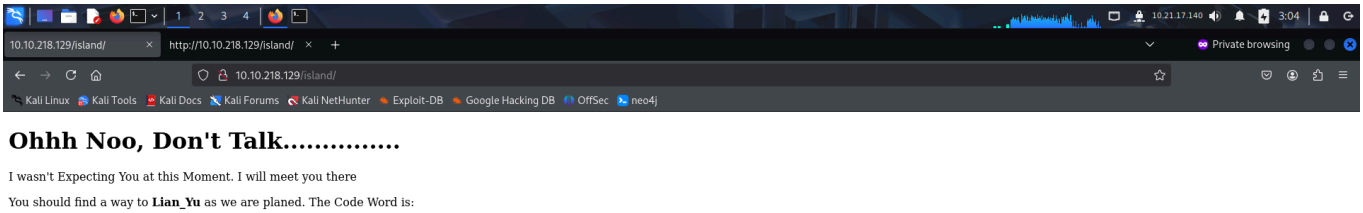


FOOTHOLD

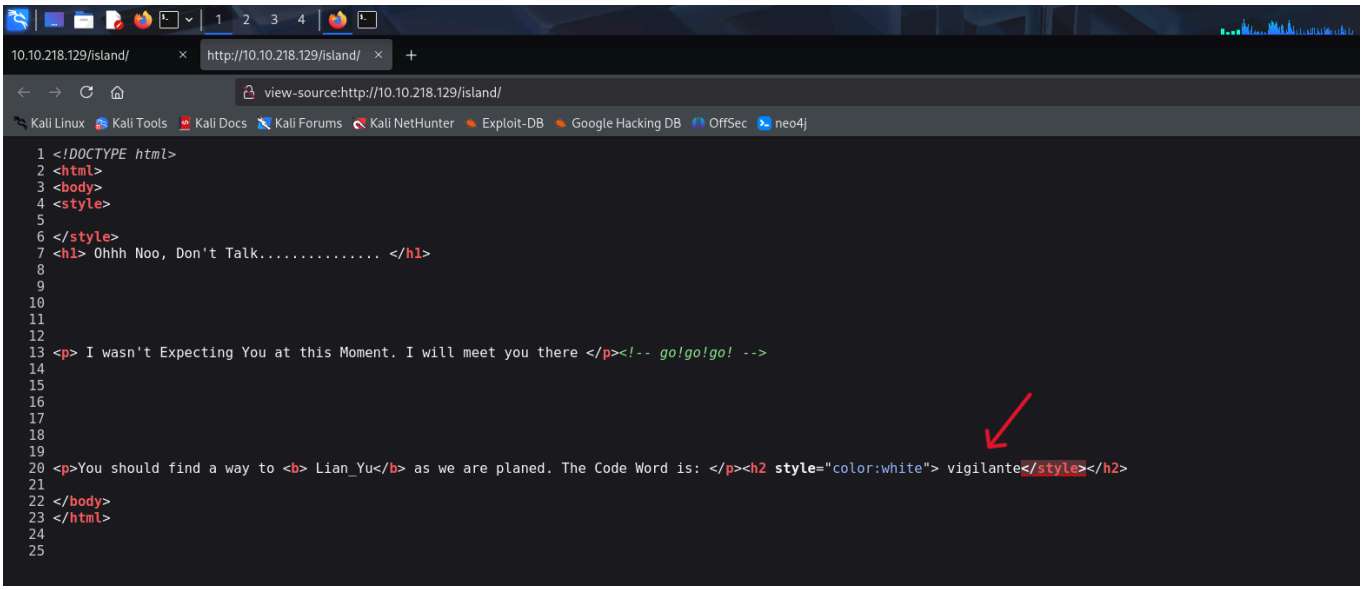
Since the target was running a web application, I fuzzed it for hidden directories and found an interesting endpoint.



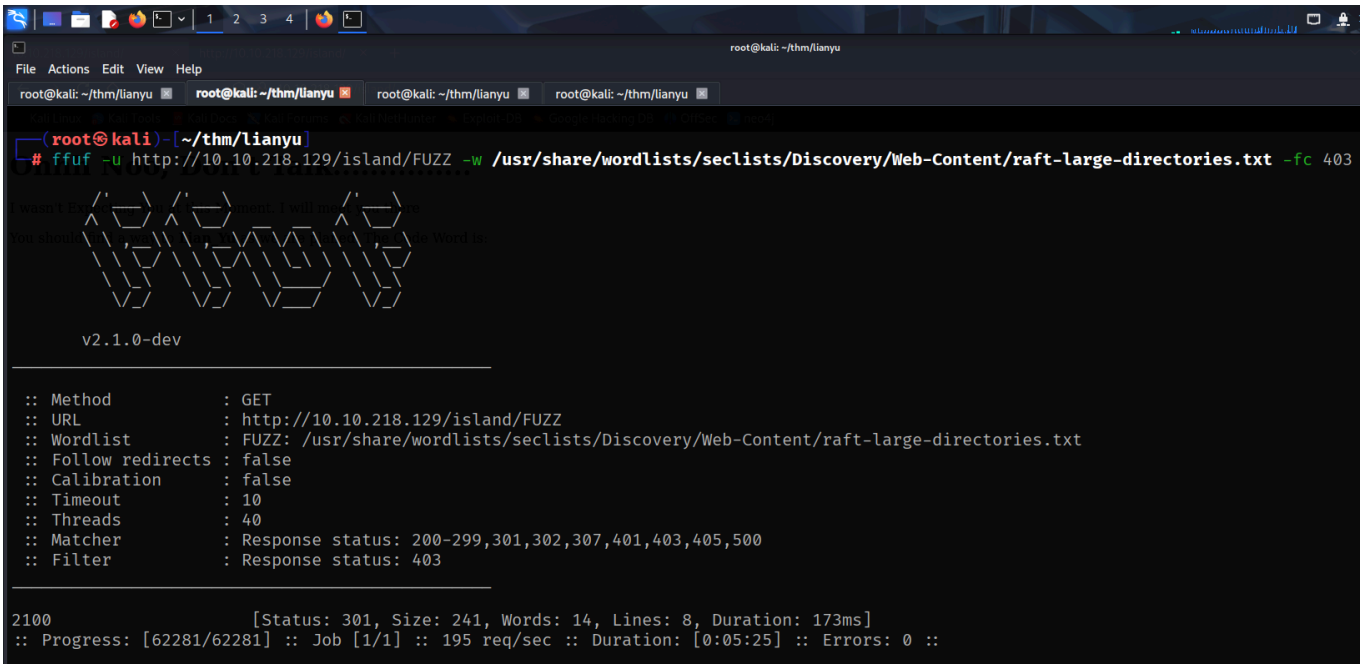
I visited the endpoint and felt that the information on the page was incomplete.



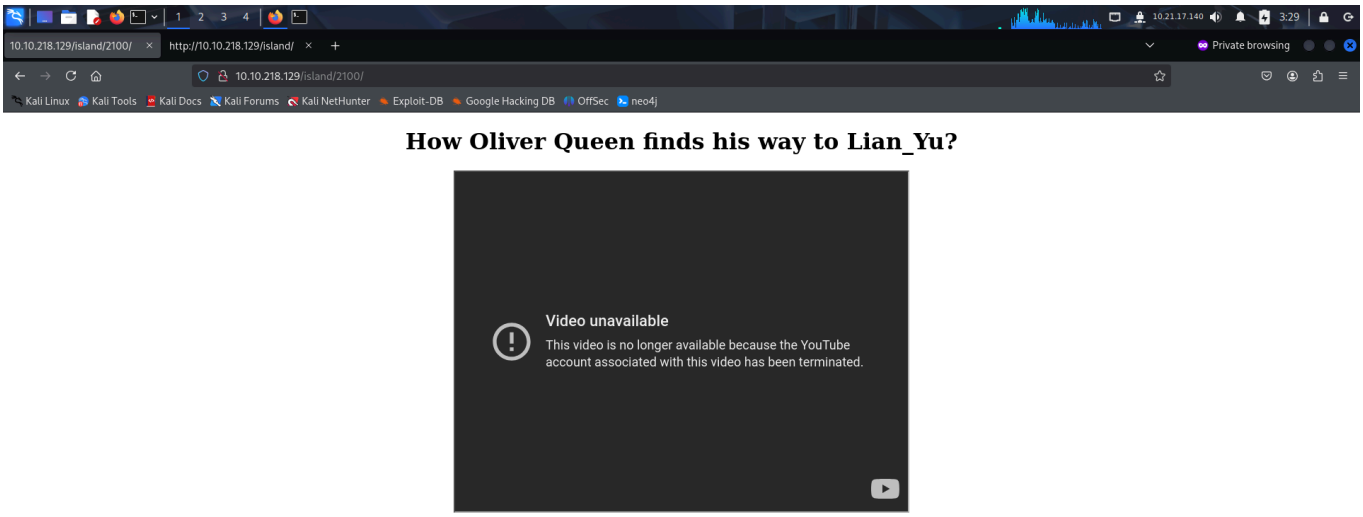
So, I viewed the source code and found a potential username/password.



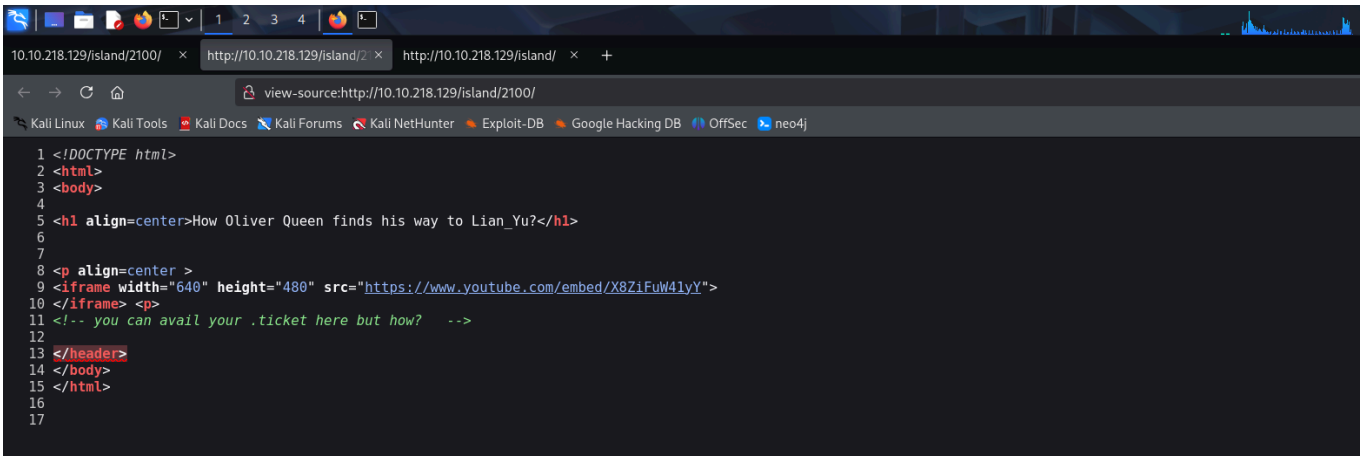
I then fuzzed for hidden directories inside the newly discovered endpoint and found another endpoint.



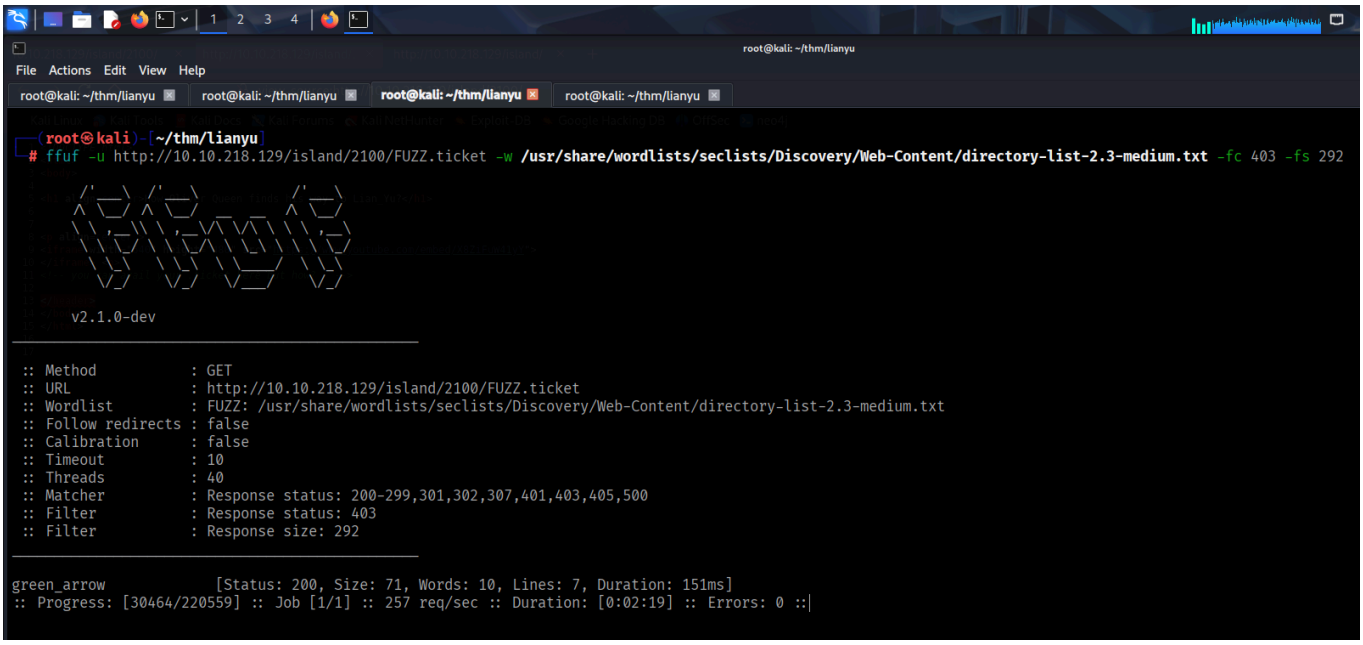
Upon visiting the page, I viewed the source code and found an interesting comment left by the developer.



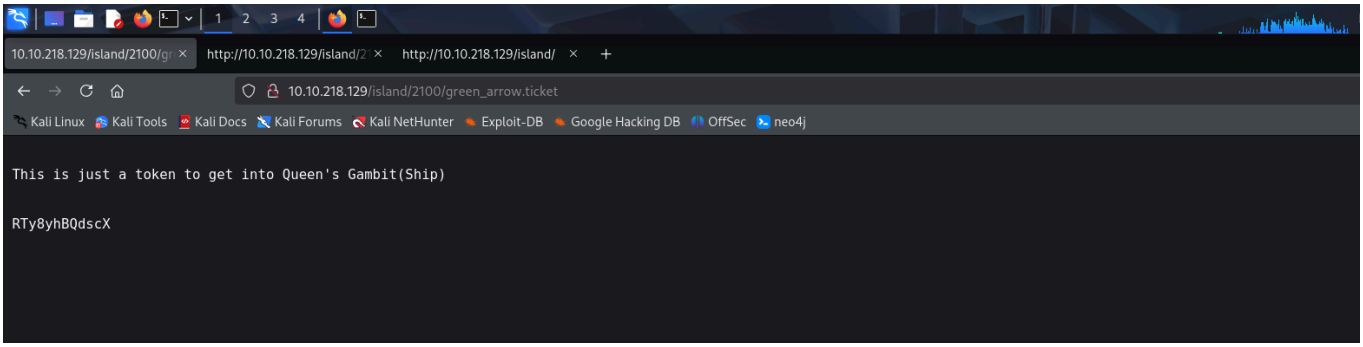
The comment said we could avail our `.ticket` ... Maybe, there could be a file or directory on this endpoint with the `.ticket` extension.



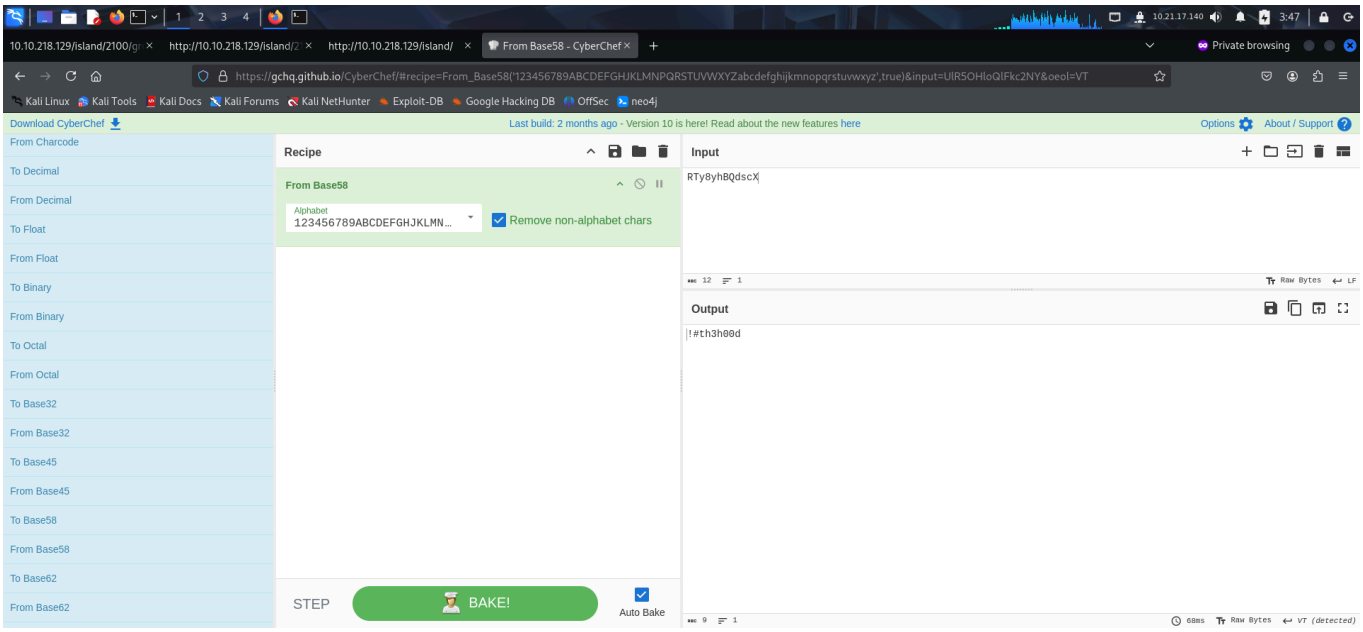
So, I fuzzed for `.ticket` endpoints inside the hidden directory.



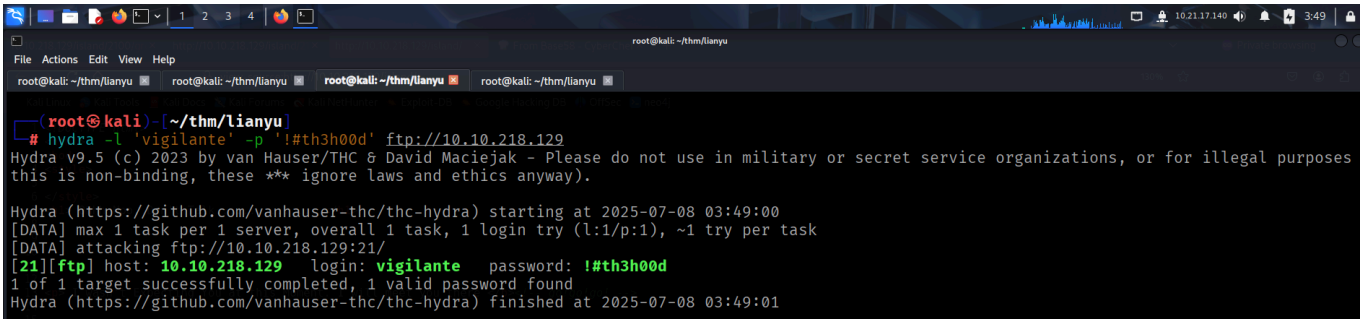
I accessed the newly discovered endpoint and found an encoded piece of string.



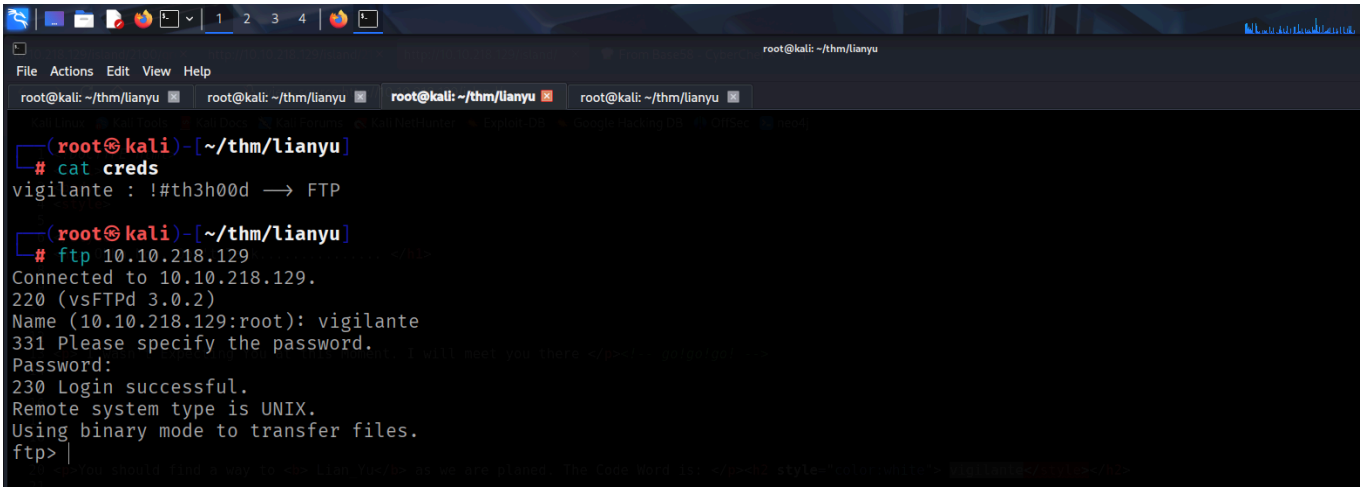
I tried various methods to decode the string and successfully decoded it when I used the *From Base58* decoder from **cyberchef**.



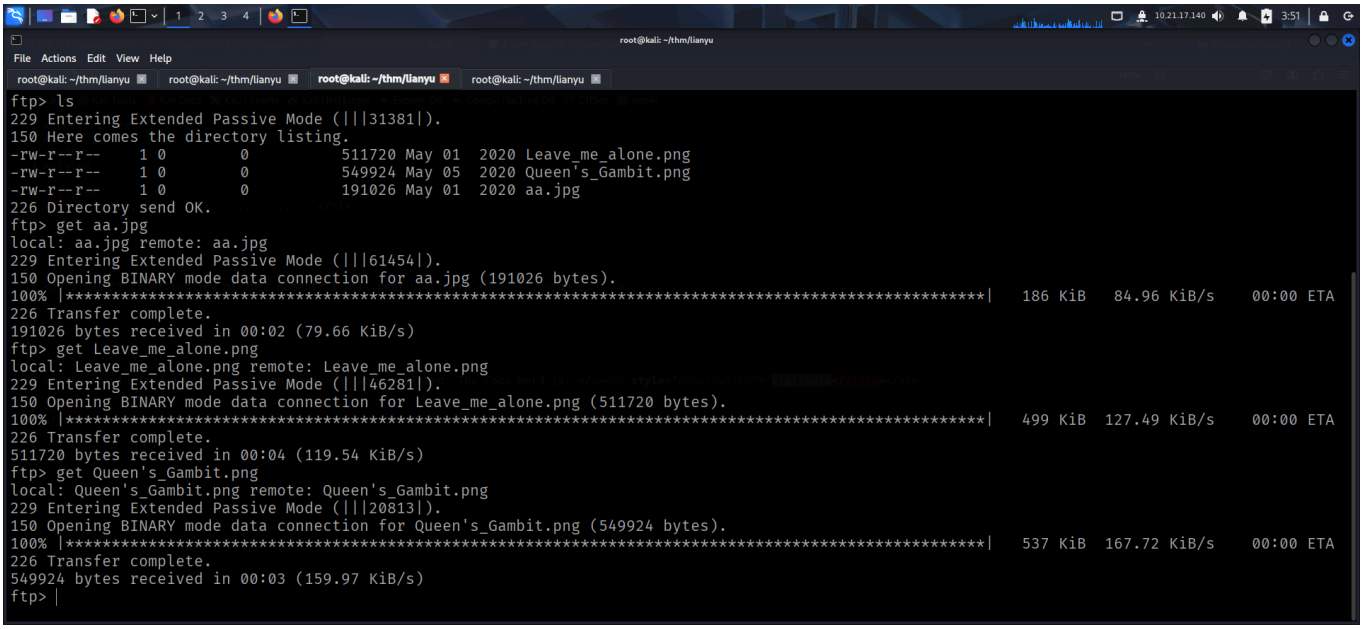
This looked like a password so I checked if this could be used with the username that I had found earlier on the other services running on the target i.e **ssh** or **ftp**. The credentials worked with **ftp*.



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



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



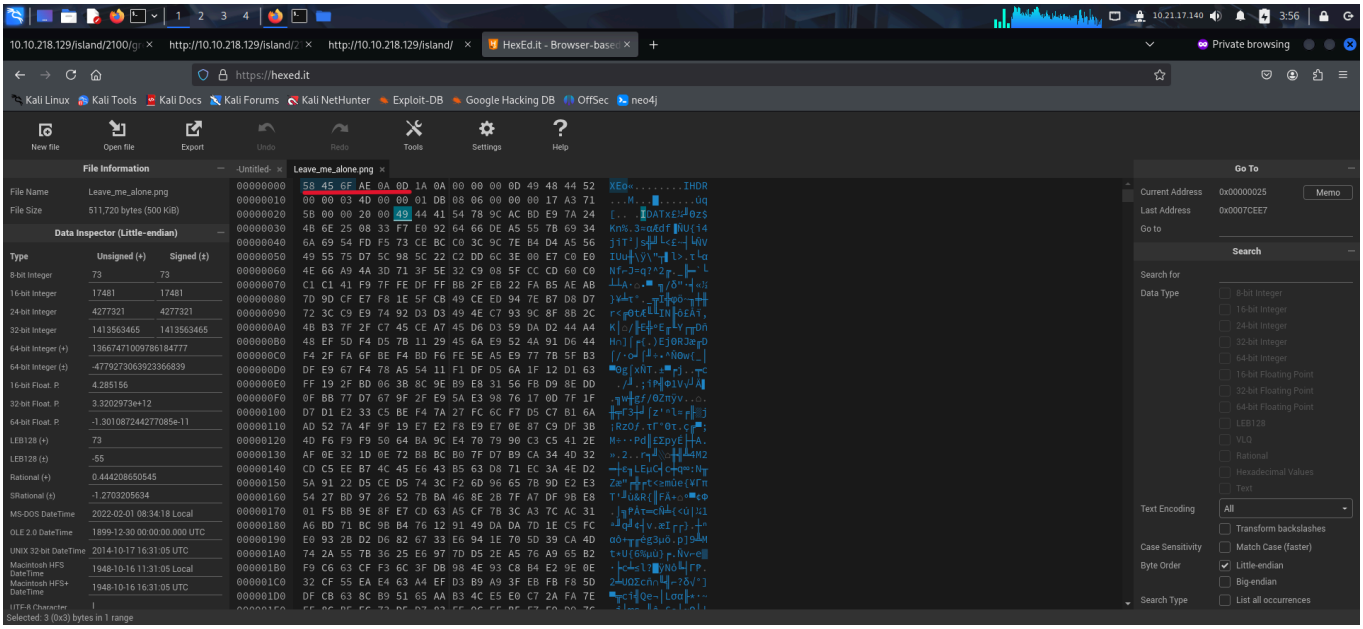
The `leave_me_alone.png` file seemed to have some problem.

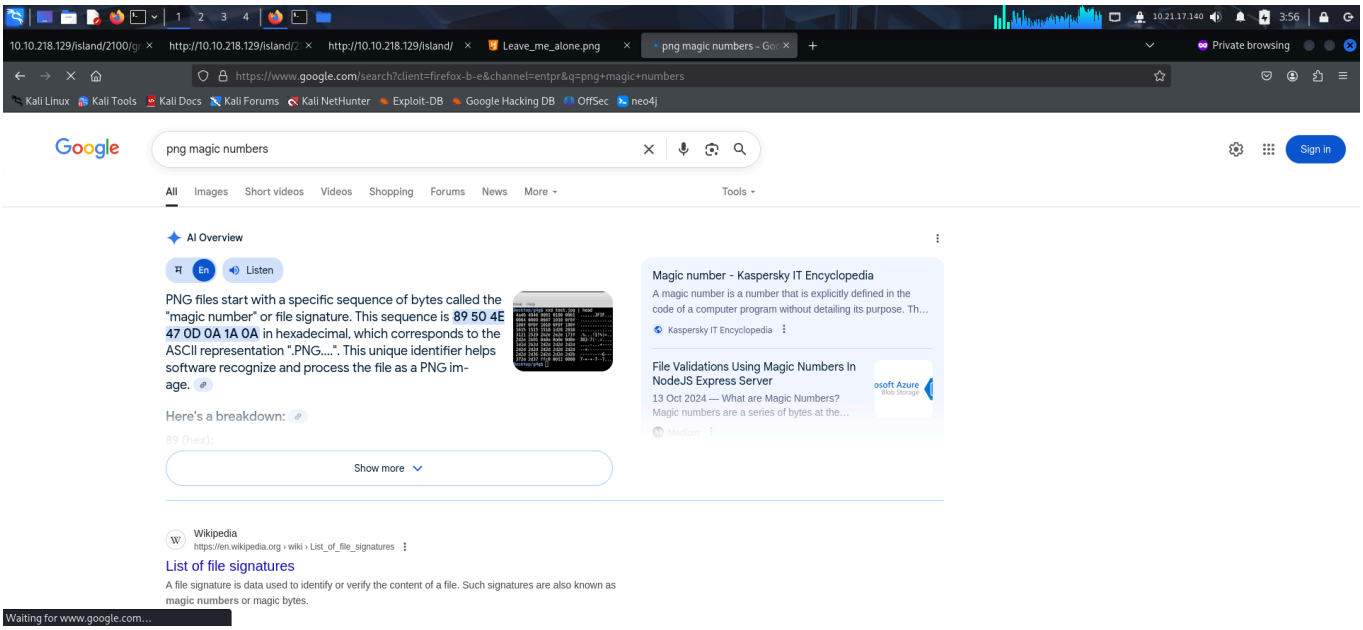
```
┌──(root㉿kali)-[~/thm/lianyu]
└─# file aa.jpg
aa.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1×1, segment length 16, baseline, precision 8, 1200×1600, components 3

┌──(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.

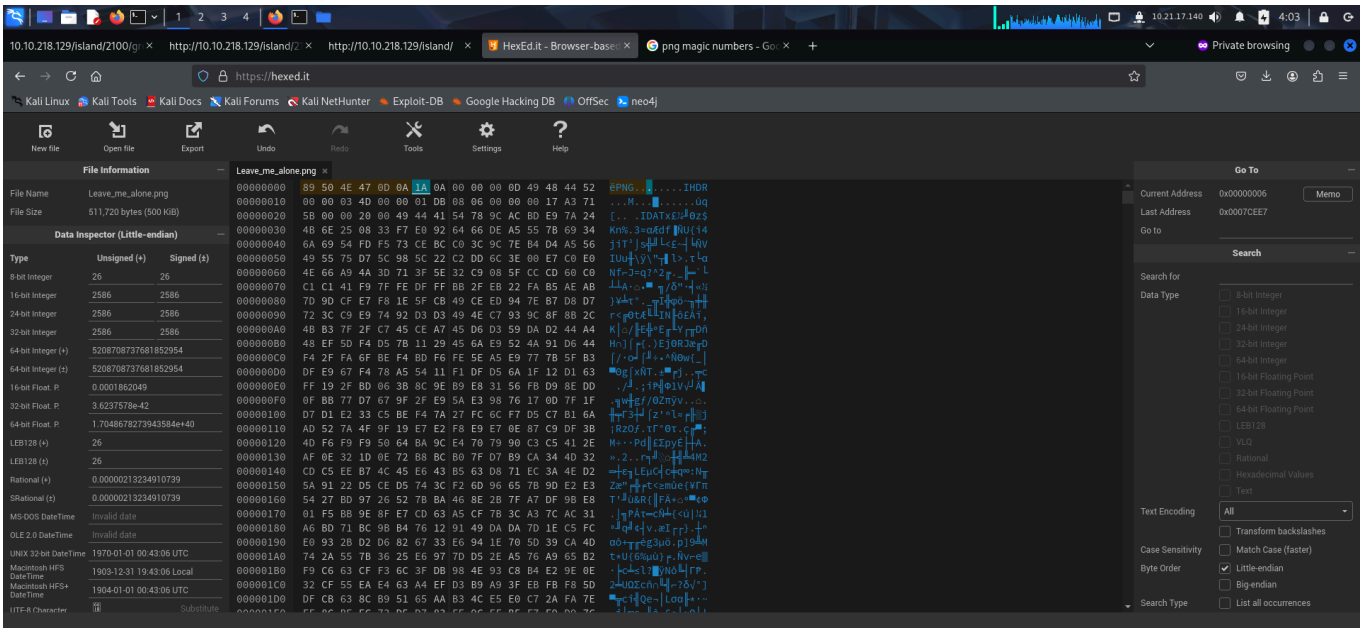
```
┌──(root㉿kali)-[~/thm/lianyu]
└─# exiftool Leave_me_alone.png
ExifTool Version Number         : 13.25
File Name                       : Leave_me_alone.png
Directory                       : .
File Size                       : 512 kB
File Modification Date/Time     : 2020:04:30 23:26:06-04:00
File 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.

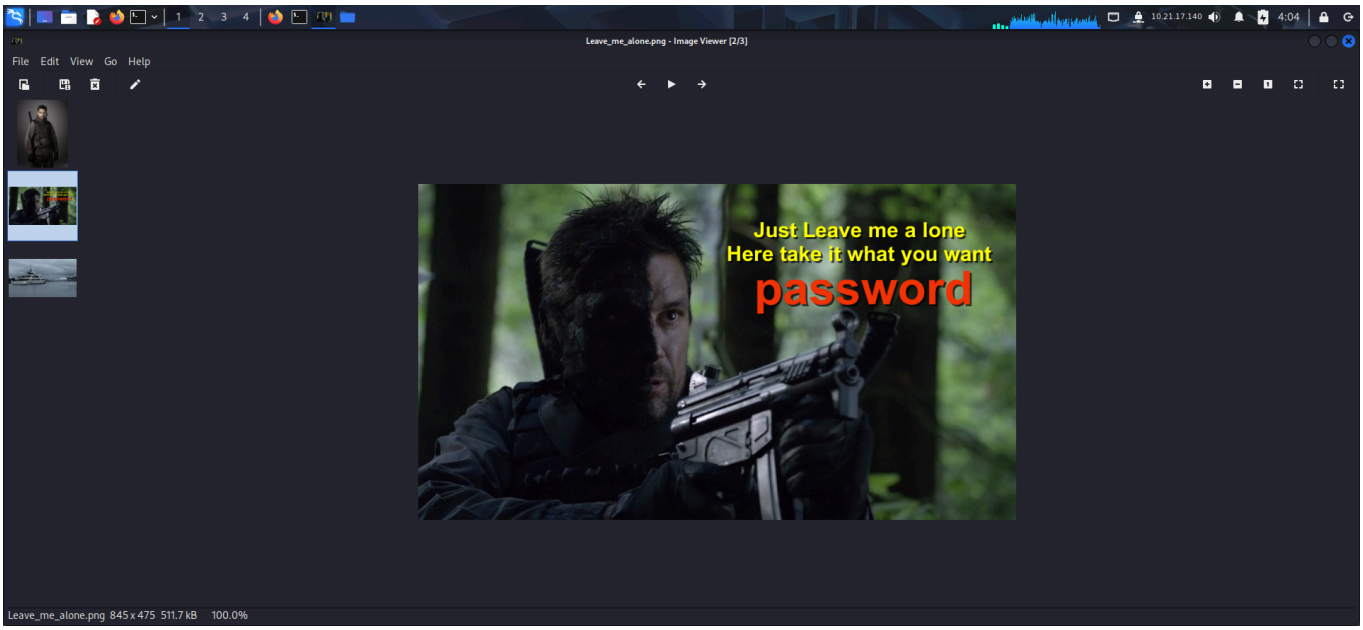




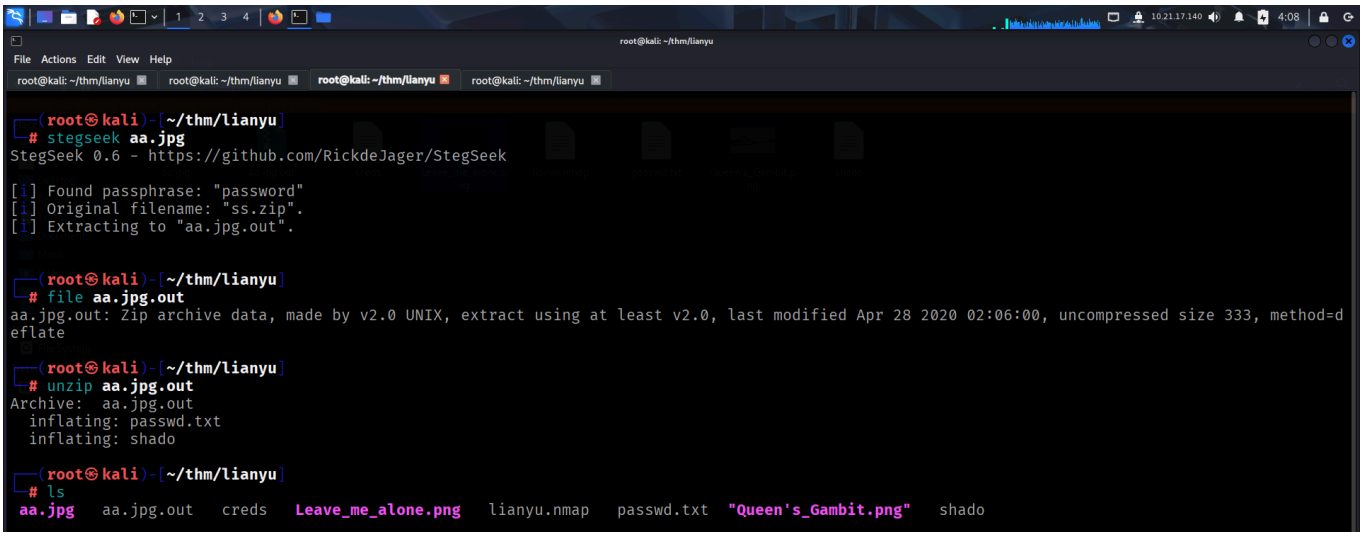
I fixed the headers and downloaded the image.



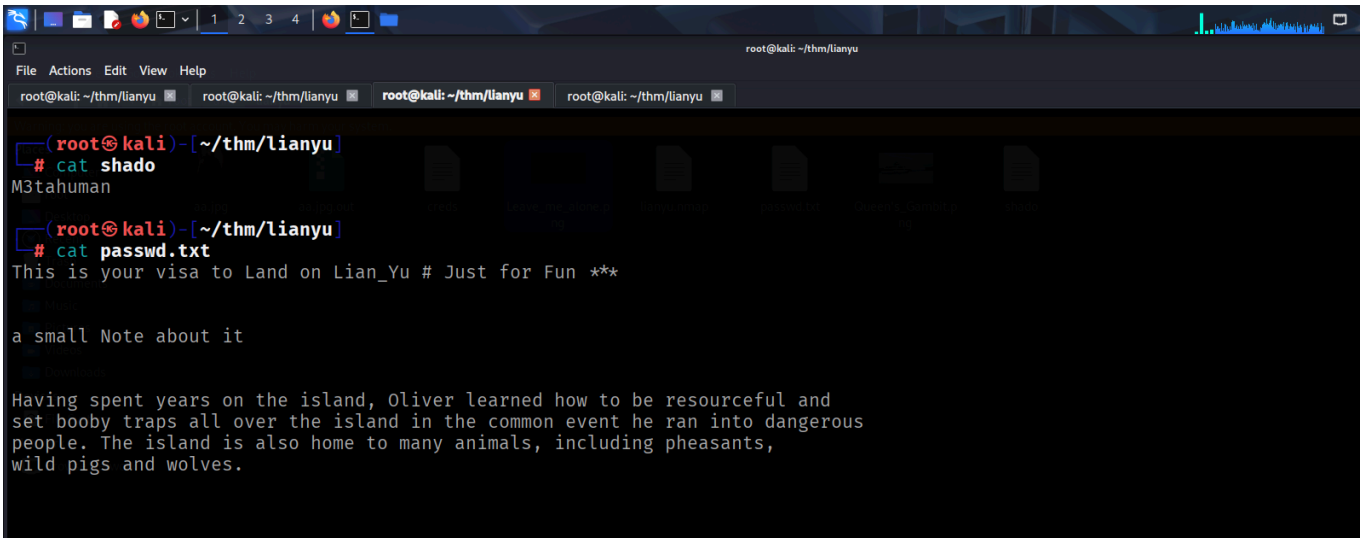
However, the image contained nothing interesting.



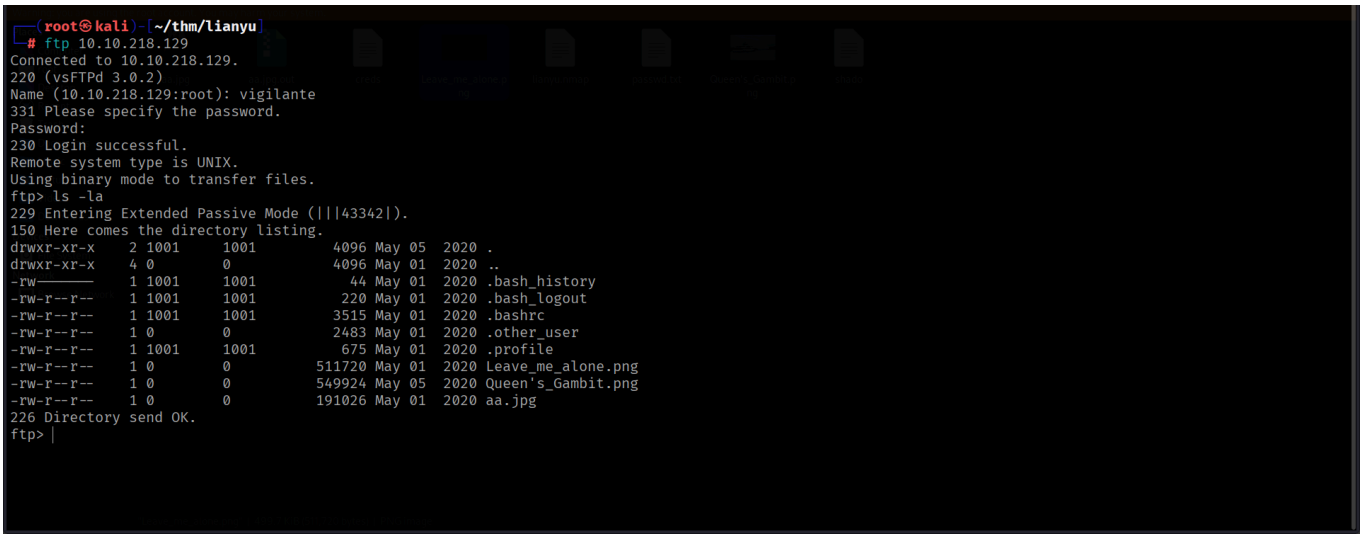
I then tried extracting data from `aa.jpg` and found out it contained a zip file. In uncompressed the file and found 2 files.



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

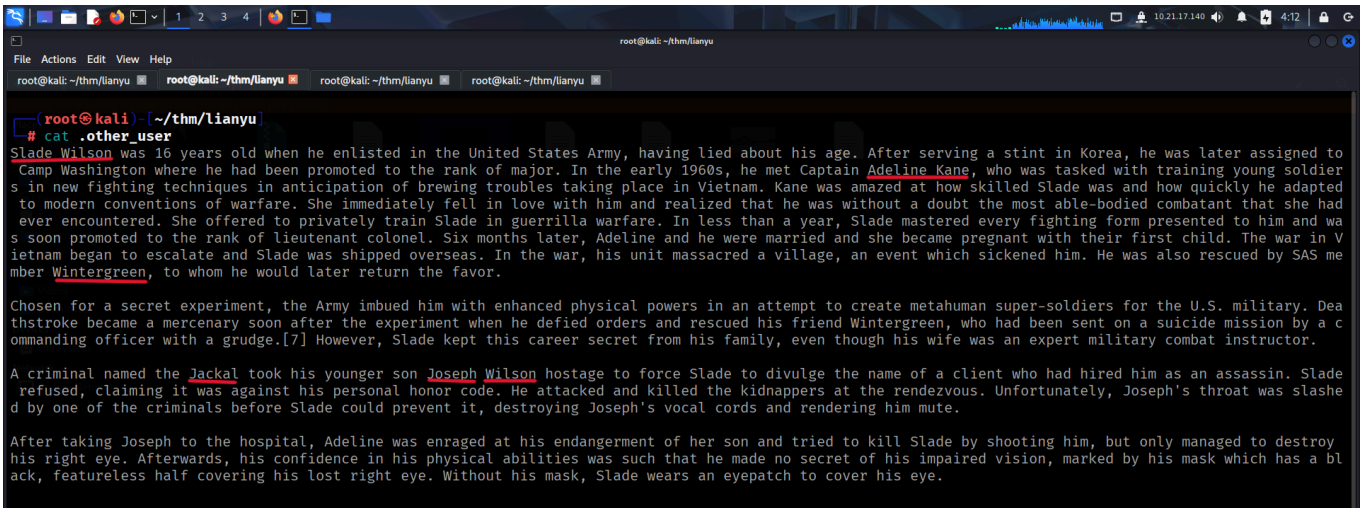


At this point, I tried tried fuzzing spraying this password with the potential usernames that I had found so far, however, nothing worked. I went back to the **ftp** server and listed the hidden files as well to find an interesting hidden file called `.other_user`.

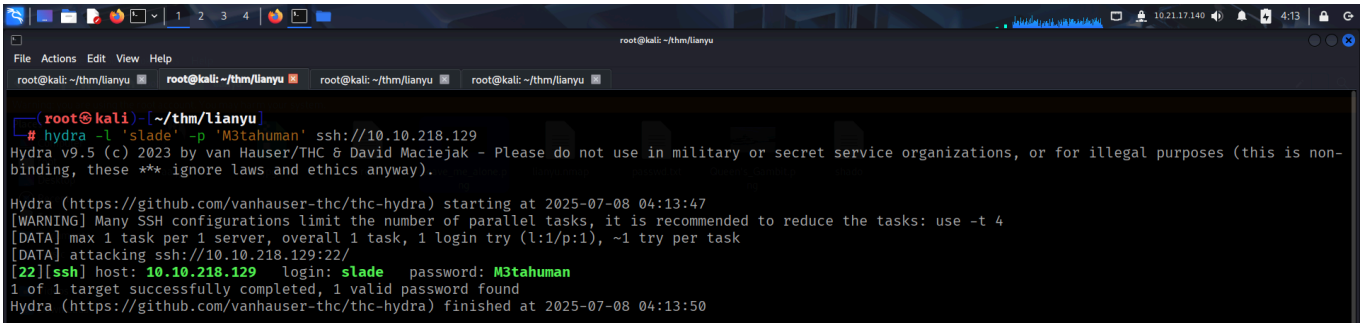


I downloaded the file on my local system.

The file contained a bunch of potential usernames.

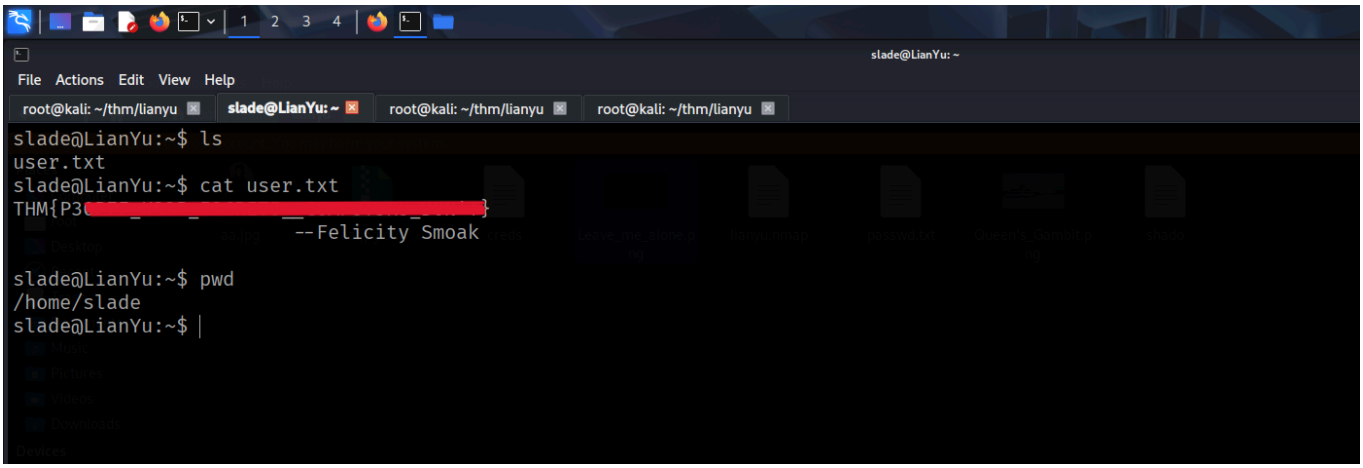


I tried the password with these usernames aswell and found a valid ssh credential.



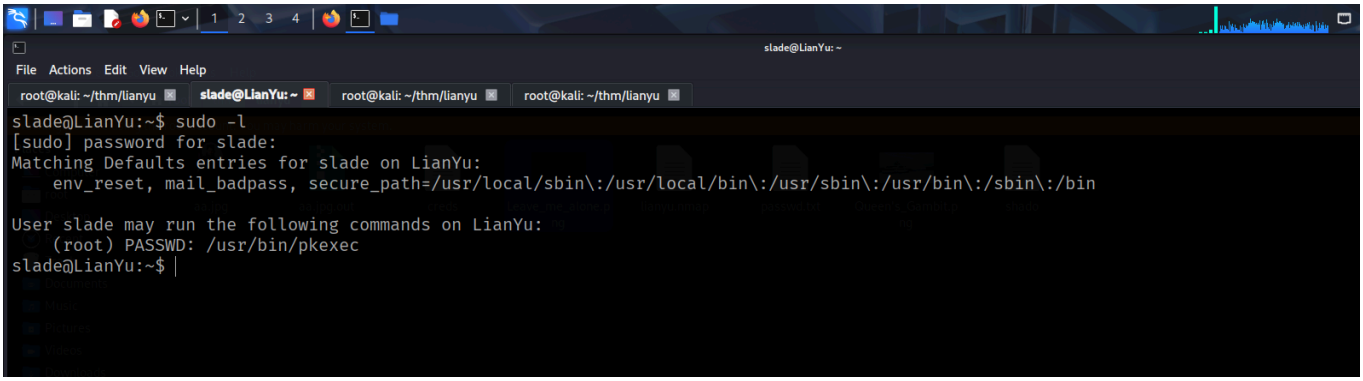
I connected to the machine using the discovered credentials through **ssh**.

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

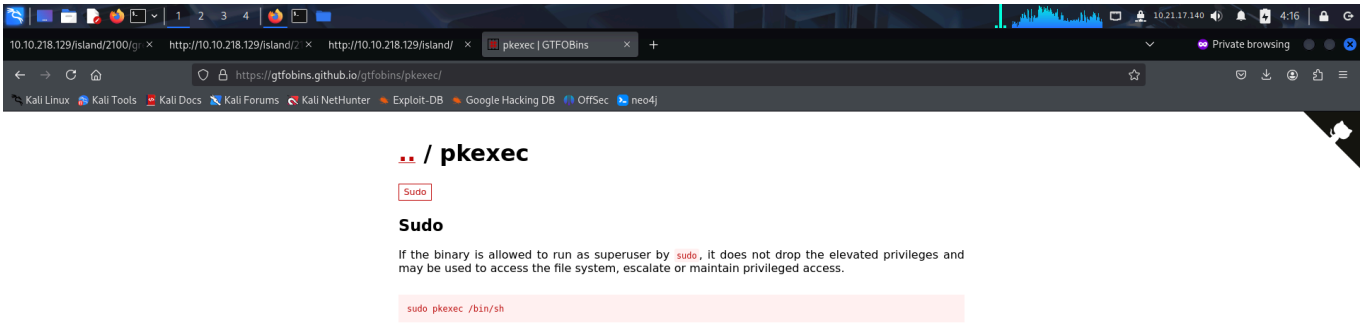


PRIVILEGE ESCALATION

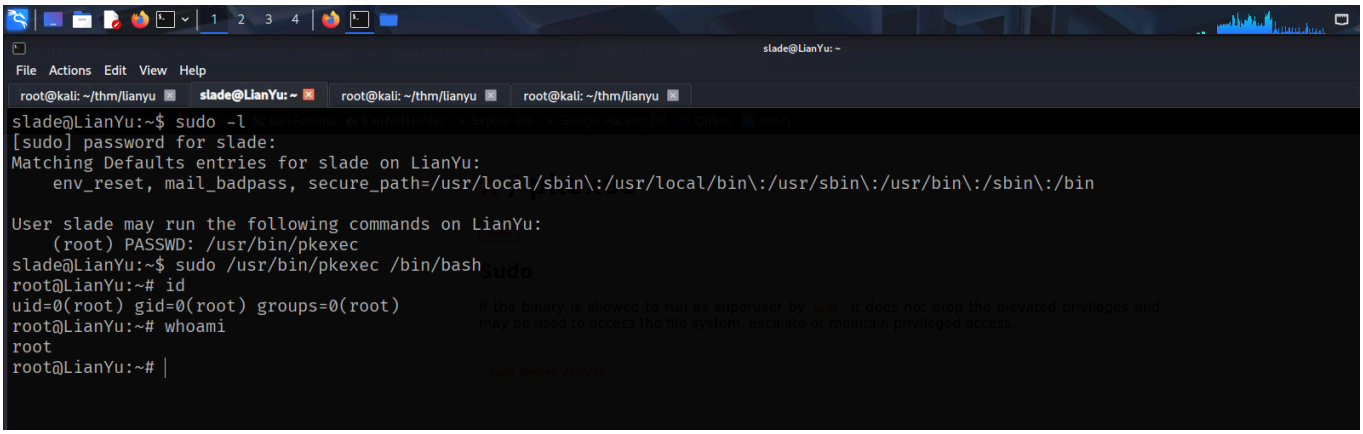
I then listed my **sudo** privileges and found that I was allowed to run the **pkexec** binary as root without password.



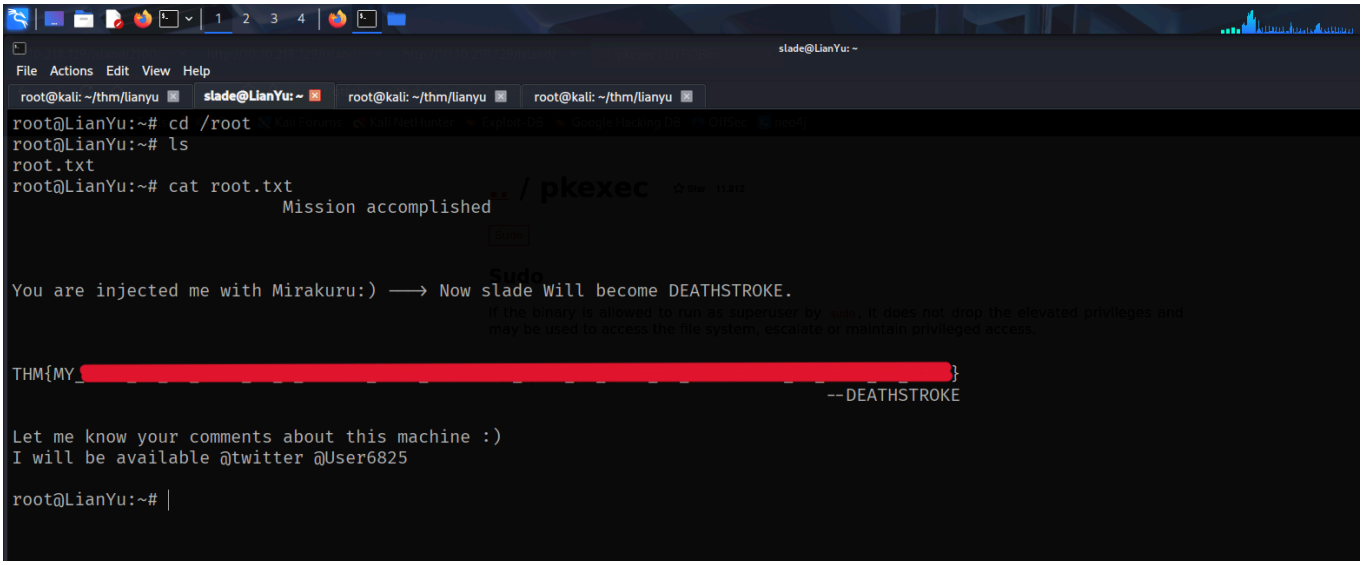
I referred to **gtfobins** and found a way to exploit this to get root access.



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



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



That's it from my side!
Until next time :)