RootMe

RootMe

A ctf for beginners, can you root me?

writeup

------------------------------------User-Flag---

-ran nmap scan and found 2 open ports, 22 and 80

-ran gobuster and found the following files and directories:

```
/css (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
```

-/panel/ contains an upload form, so I took php-reverse-shell.php, inserted my IP and port, and changed extension to .php5 to bypass the filter on .php files.

-uploaded php-reverse-shell.php5 to server

-started reverse netcat shell and navigated to /uploads/php-reverse-shell.php5 to kick off a shell

-ran cat user.txt and got flag:

THM{y0u_g0t_a_sh3ll}

------------------------------------Root-Flag---

--ran find / -user root -perm /4000 and found /usr/bin/python has SUID permissions

--ran the following command to get root shell /usr/bin/python -c 'import os; os.setuid(0); os.system("/bin/sh")' < -c 'import os; os.setuid(0); os.system("/bin/sh")'

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

THM{pr1v1l3g3_3sc4l4t10n}

[1] Deploy the machine

Connect to TryHackMe network and deploy the machine. If you don't know how to do this, complete the OpenVPN room first.

#1
Deploy the machine

No answer needed

[2] Reconnaissance

First, let's get information about the target.

#1

Scan the machine, how many ports are open?

2

#2

What version of Apache are running?

2.4.29

#3

What service is running on port 22?

ssh

#4

Find directories on the web server using the GoBuster tool.

No answer needed

#5

What is the hidden directory?

/panel/

[3] Getting a shell

Find a form to upload and get a reverse shell, and find the flag.

#1
user.txt

THM{y0u_g0t_a_sh3ll}

[4] Privilege escalation

Now that we have a shell, let's escalate our privileges to root.

#1
Search for files with SUID permission, which file is weird?

/usr/bin/python

#2
Find a form to escalate your privileges.

No answer needed

#3
root.txt

THM{pr1v1l3g3_3sc4l4t10n}