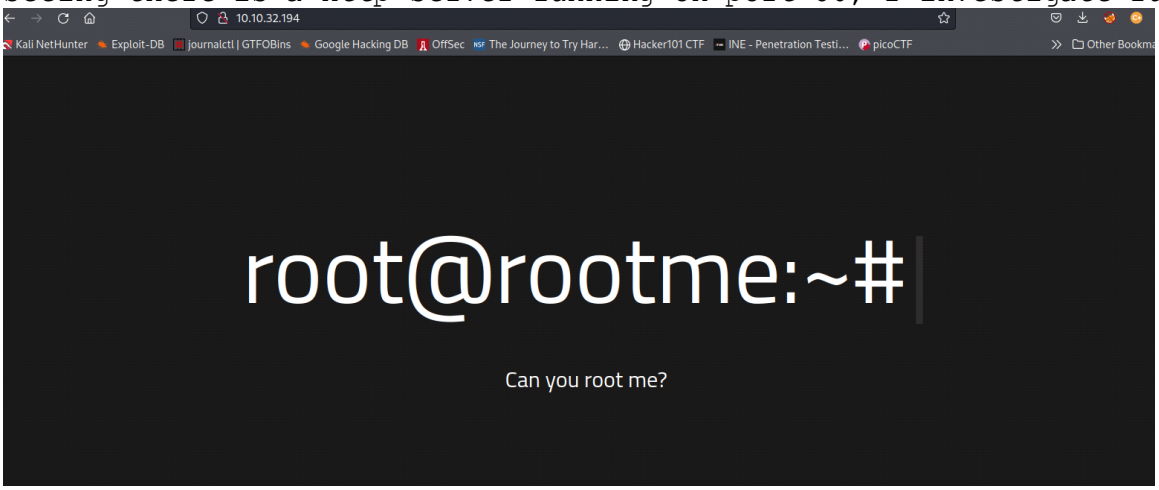
https://tryhackme.com/room/rrootme

After booting up the box I used Nmap to enumerate using the -A , -T4, and -Pn flags to attempt to find the ports even if they were not answering back.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T5 10.10.32.194 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-29 10:46 EDT
Nmap scan report for 10.10.32.194
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (conn-refused)
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-title: HackIT - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/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 23.35 seconds
```

Seeing there is a http server running on port 80, I investigate further



knowing there is a server serving php pages, i use Gobuster with Seclists's web-content directory list to further enumerate unknown pages and find two interesting things: Uploads, and Panel.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --url http://10.10.32.194 -w /home/kali/Downloads/SecLists-master/Discovery/Web-Content/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.32.194
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kali/Downloads/SecLists-master/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/08/29 10:51:36 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 314] [--> http://10.10.32.194/uploads/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.32.194/css/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.32.194/js/]
/panel                (Status: 301) [Size: 312] [--> http://10.10.32.194/panel/]
Progress: 11038 / 87665 (12.59%)
[!] Keyboard interrupt detected, terminating.
                                                             ^C
===============================================================
2022/08/29 10:55:38 Finished
===============================================================
```

Uploads is a directory page, and Panel is a page where one may uploads files.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
php.jpg	2022-08-29 15:14	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.32.194 Port 80

When there is a page to upload files, i attempt a reverse shell. From the Nmap read out we have a hit that Apache is running php - so i attempted the time tested https://pentestmonkey.net/tools/web-shells/php-reverse-shell

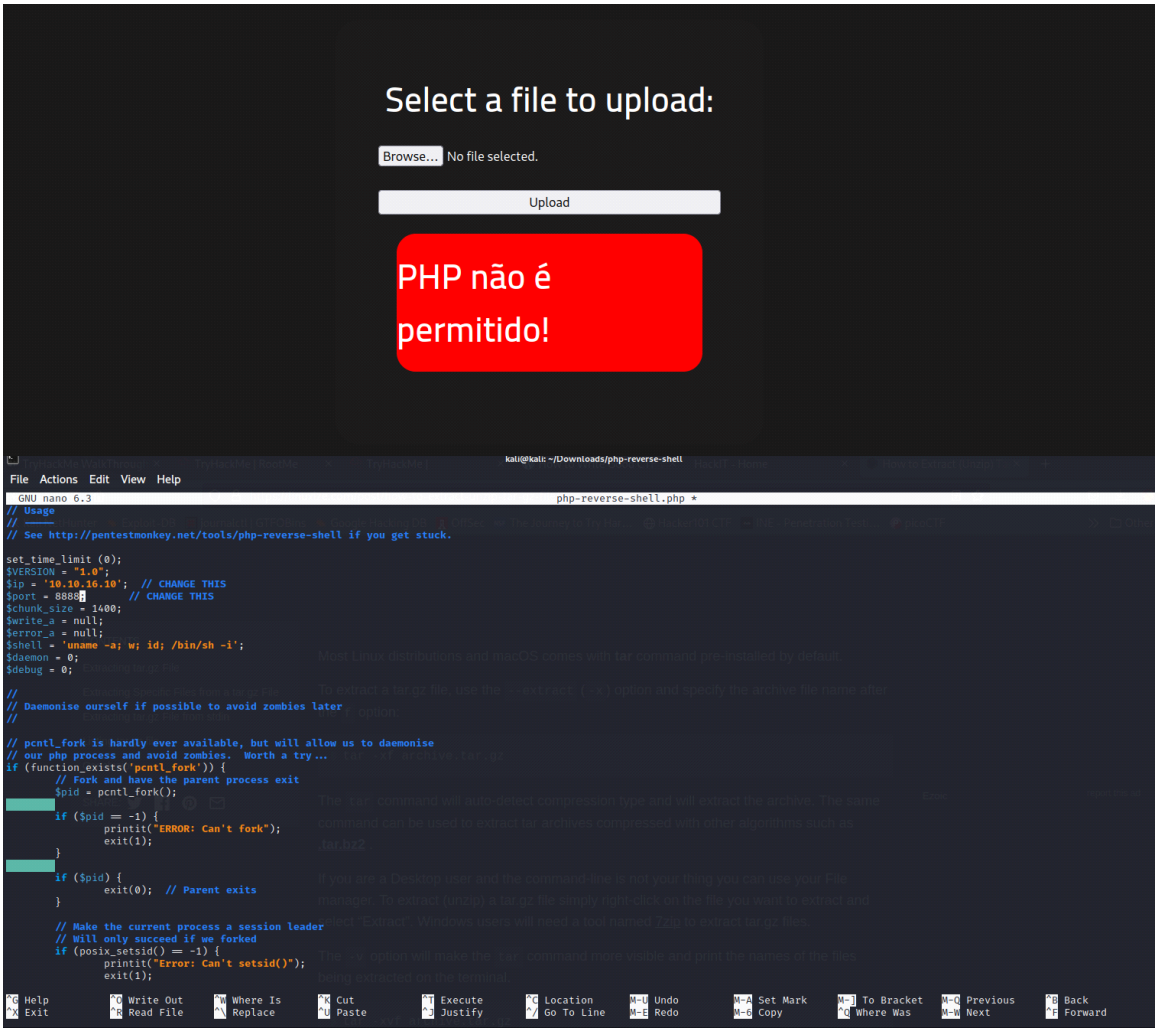
i change the script to my IP and the port i will be listening on

i then start a netcat listener on said port

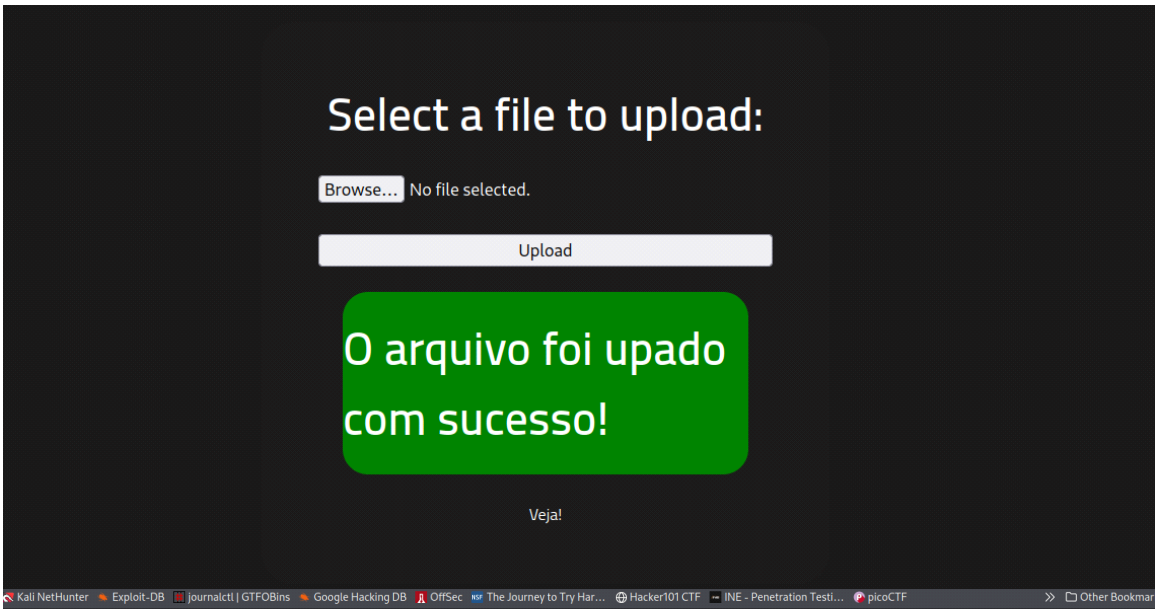
```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
```

i attempt to upload my php reverse shell on the /uploads page

my upload is denied - there may be a filter. i save it to another name of rev.phtml



after several VM issues, i go to the upload directory page and click on my reverse shell



Index of /uploads

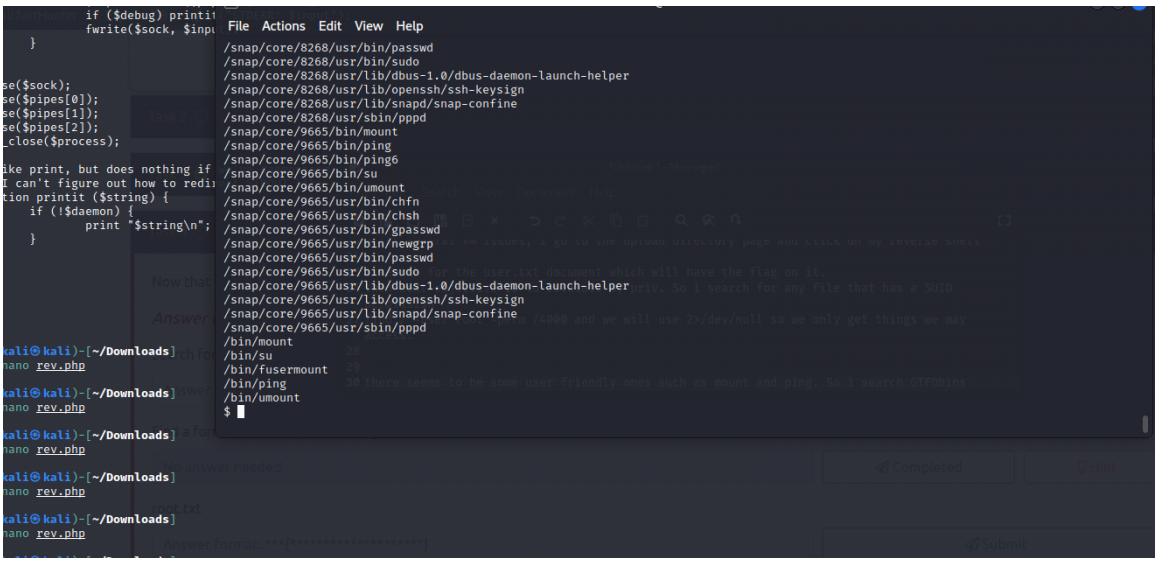
Name	Last modified	Size	Description
Parent Directory		-	
php.jpg	2022-08-29 15:21	5.4K	
php.phtml	2022-08-29 15:23	5.4K	
php2.phtml	2022-08-29 15:23	5.4K	
rev.phtml	2022-08-29 15:37	5.4K	
rev3.phtml	2022-08-29 15:38	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.32.194 Port 80

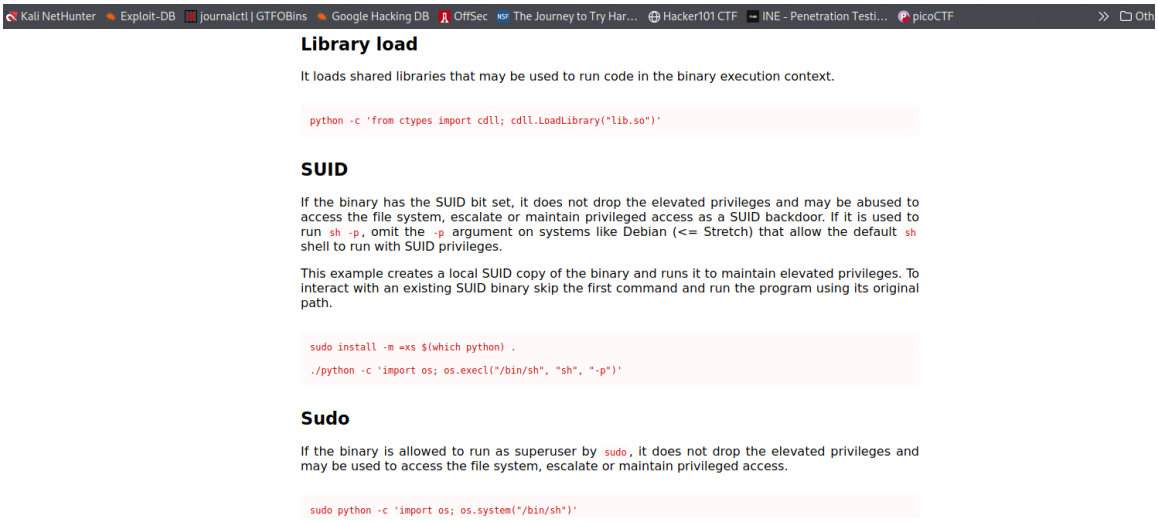
i search for the user.txt document which will have the flag on it.

then next objective is to escalate my priv. So i search for any file that

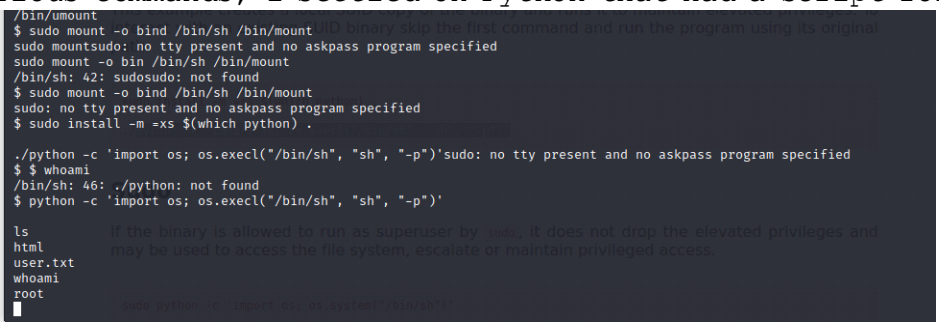
has a SUID permission
find / -user root -perm /4000 and we will use 2>/dev/null so we only get things we may access.



there seems to be some user friendly ones such as mount and ping. So i search GTFObins



searching various commands, i settled on Python that had a script for SUID



and root was achieved

rootme questions:

Scan the machine, how many ports are open? 2

What version of Apache is running? 2.4.29

What service is running on port 22? ssh

What is the hidden directory? /panel/

what was in user.txt? THM{y0u_g0t_a_sh3ll}

earch for files with SUID permission, which file is weird? /usr/bin/python

Find a form to escalate your privileges. gtfobins

root.txt
THM{pr1v1l3g3_3sc4l4t10n}