Name: Konark patel

Mobile number: 8849492455

project: mainor

projectname: coldbox

In this project, we are going to solve the cold box lab. To solve this we are going to follow usual methodologies..

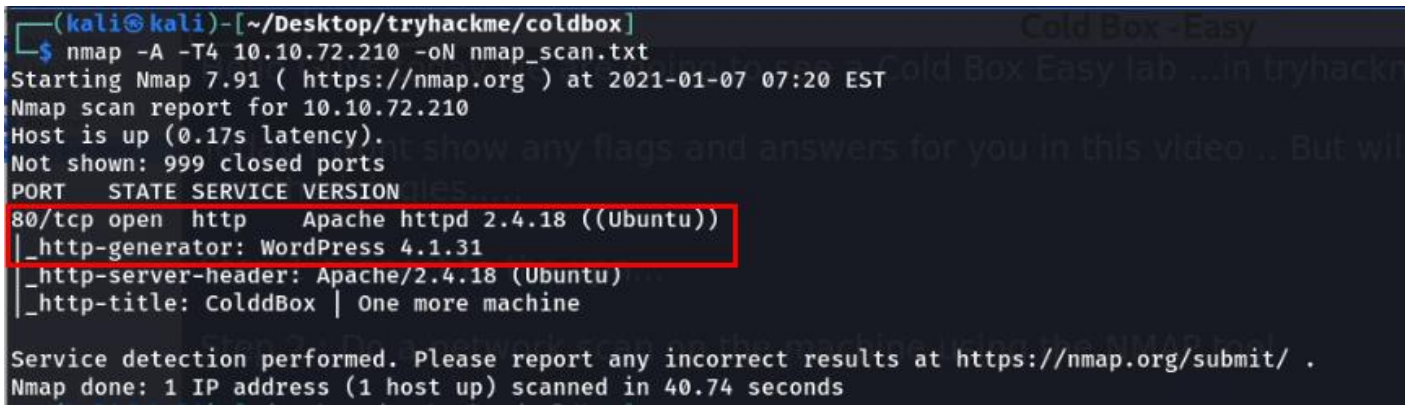
1. Information gathering
2. Scanning and enumeration
3. Exploitation
4. Privilege Escalation
5. User and root flags

Information gathering

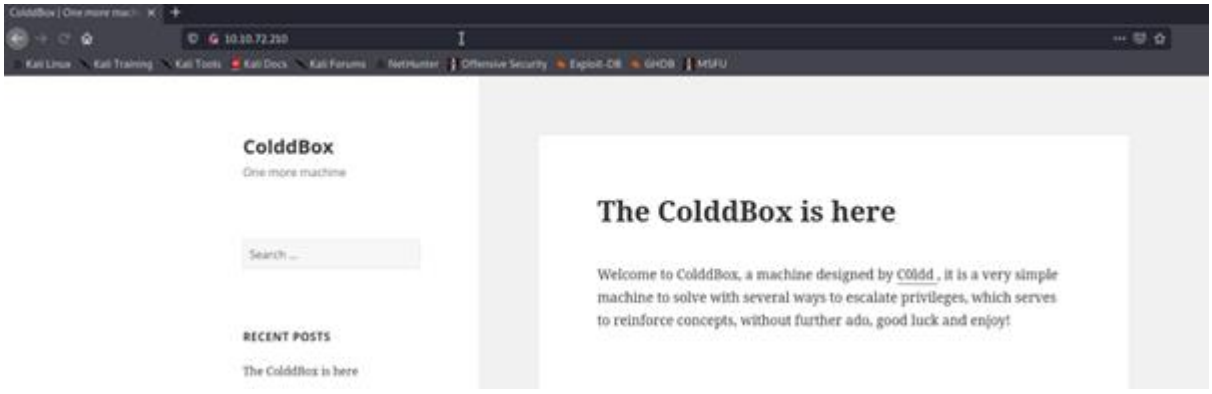
Let's start our Nmap scan using the following command

Nmap -A -T4 <IP Address>

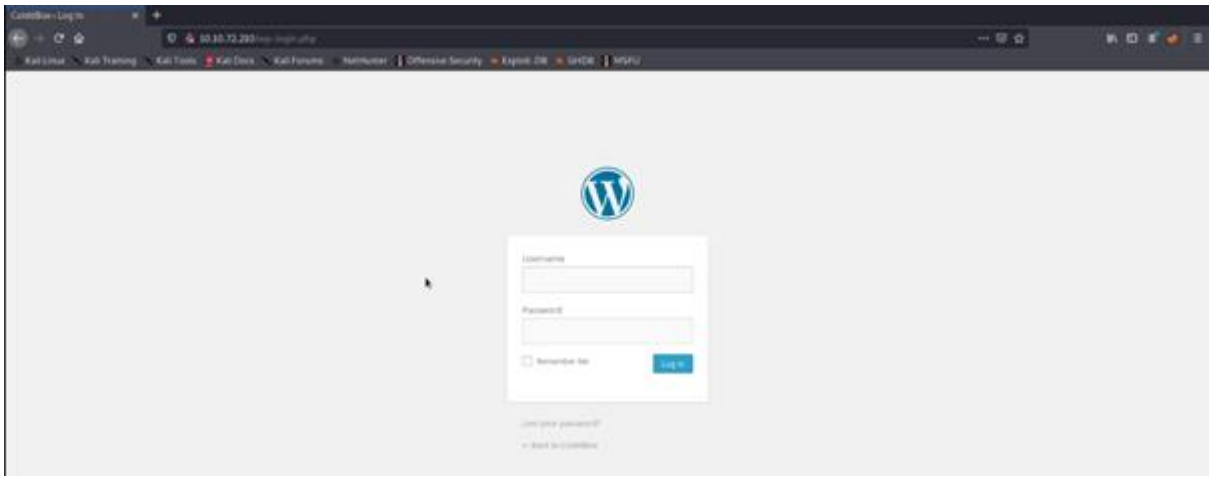
And using this command we got an output that there is only one port is opened in the TCP layer that is HTTP — 80



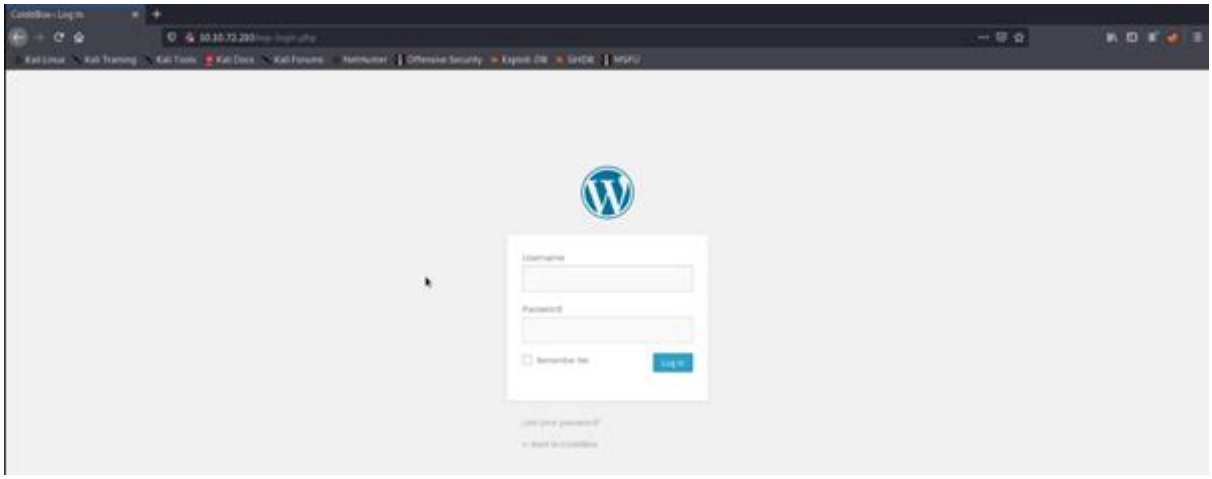
After finding out the http port is opened , I further enumerated and found there is a word press blog is running in this machine



So I checked for the login page for the wp-admin panel and I got a login portal for the WordPress blog



So I checked for the login page for the wp-admin panel and I got a login portal for the WordPress blog

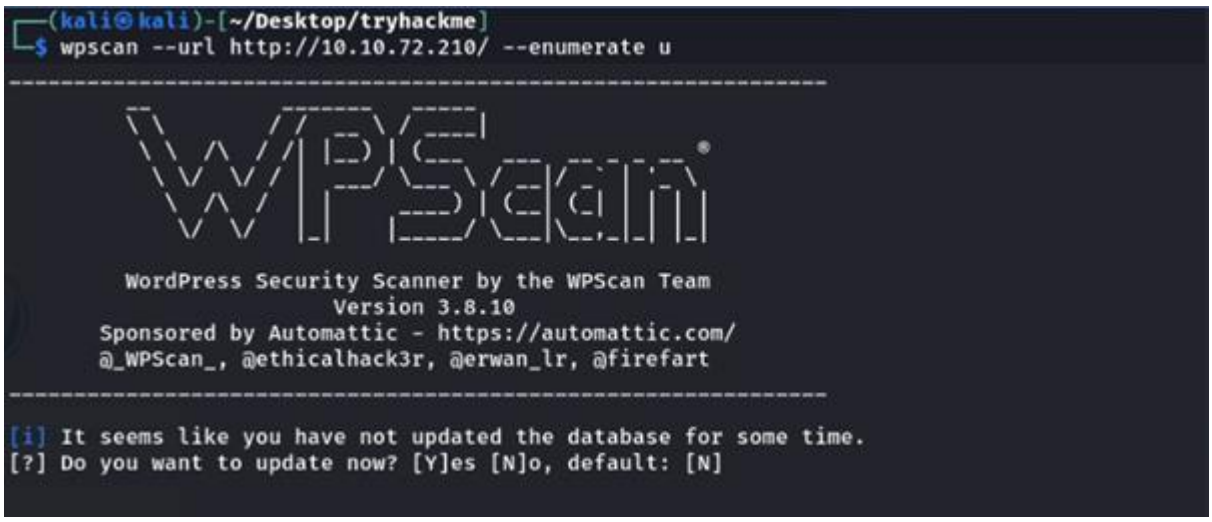


Scanning and Enumeration

Next I have an idea to enumerate the users credentials, for that we have an wonderful tool called wp-scan, the below command is used for to enumerate the users

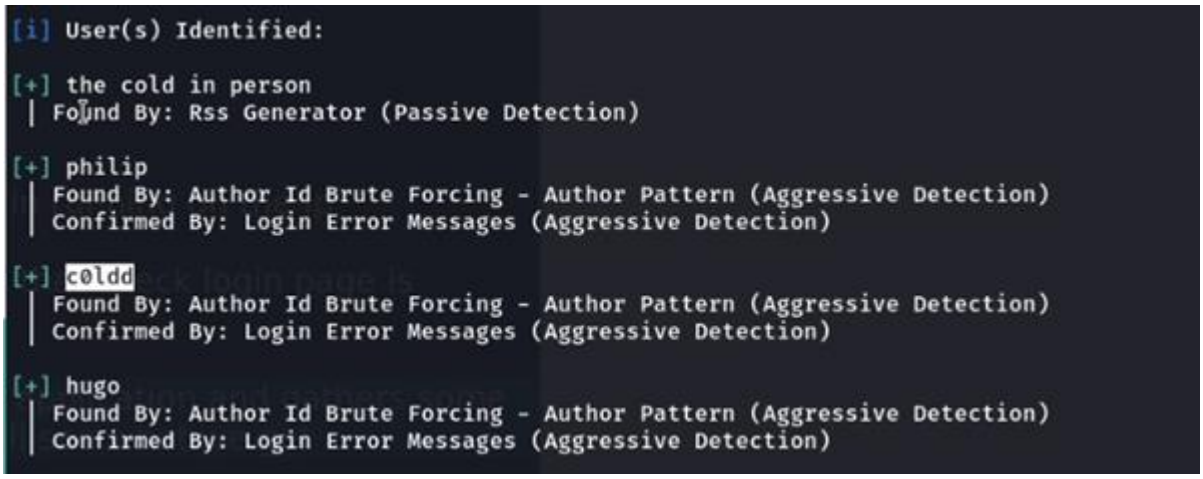
wp-scan –url http://IP Address –enumerate u

This command will enumerate all the users in the login portal.

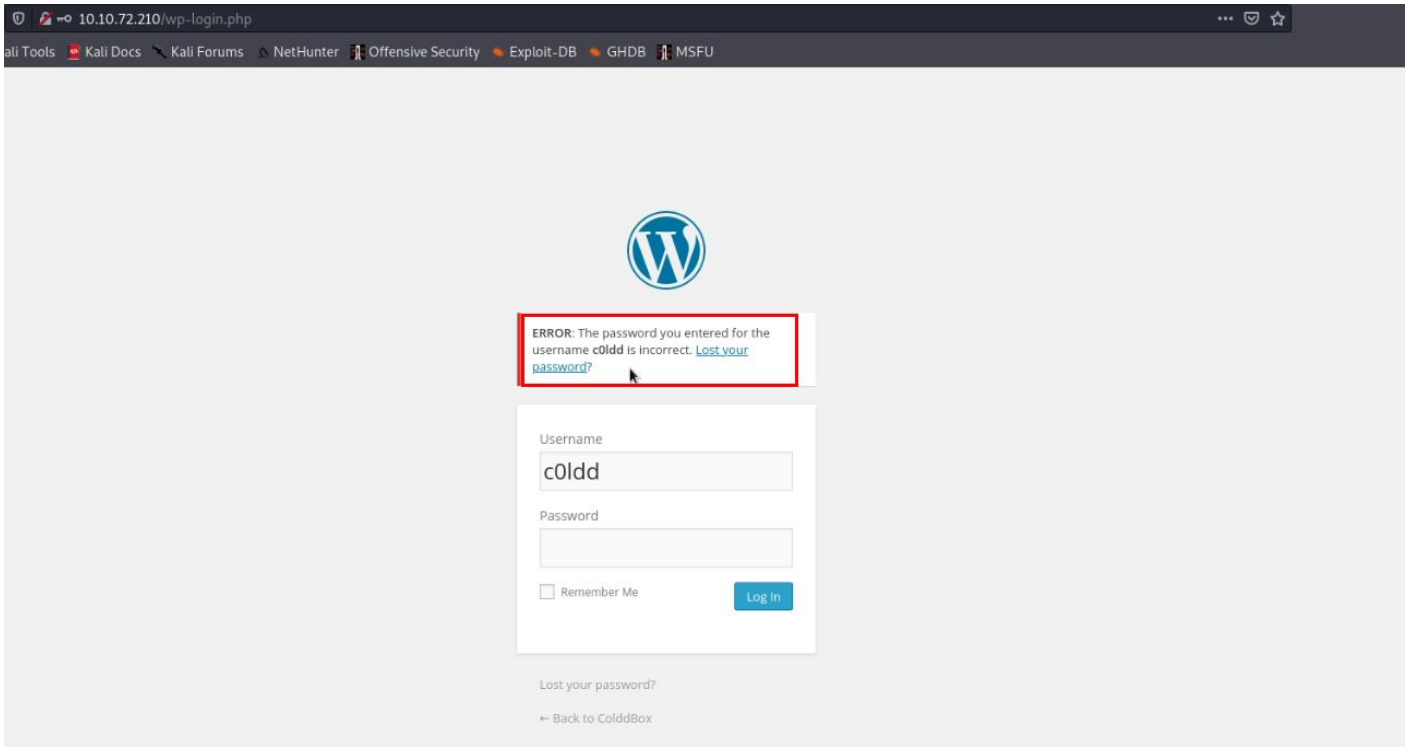


After some time the the scan completed and given a results of 4 valid users

After viewing the results I confirmed that the user is c0ldd because the machine name also cold so having that as a hint I used this username in the login portal and again confirmed the user is valid with the error thrown by the portal

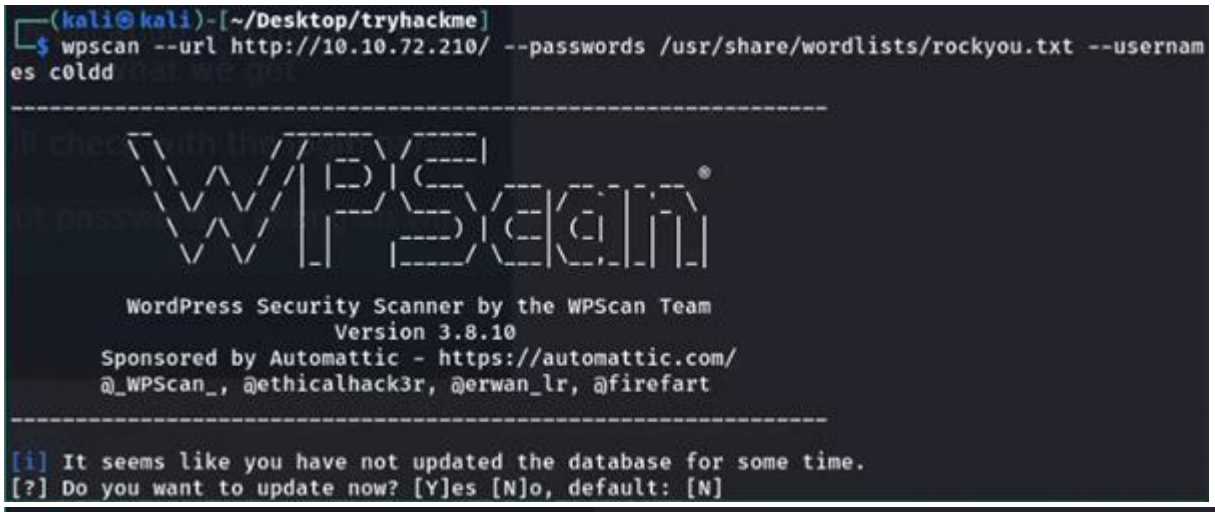


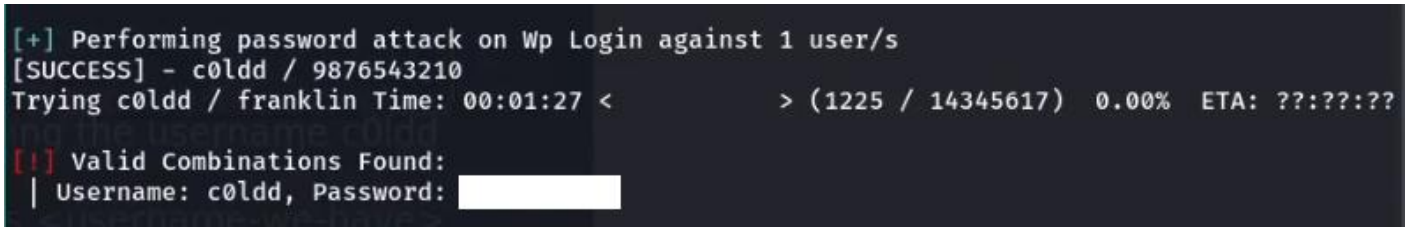
After viewing the results I confirmed that the user is c0ldd because the machine name also cold so having that as a hint I used this username in the login portal and again confirmed the user is valid with the error thrown by the portal



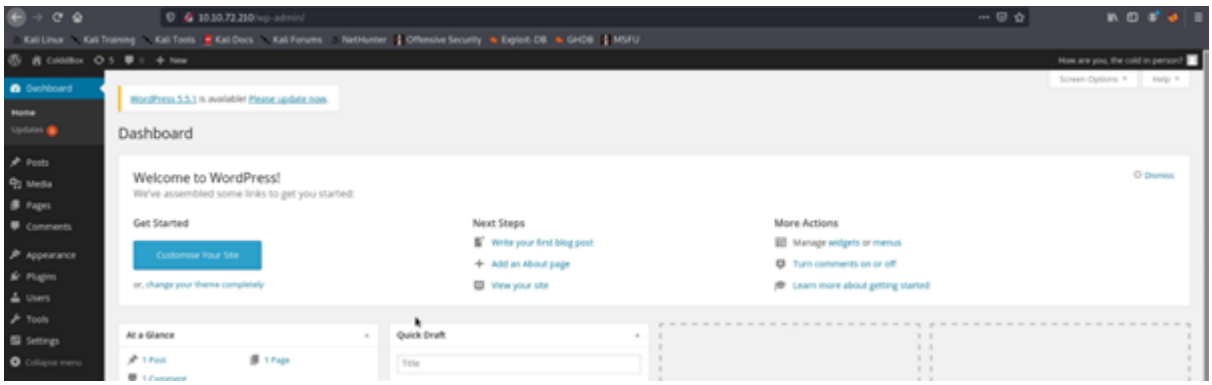
It's great we found the user and now I am going to brute force this login portal with a favorite pass list called rockyou.txt, the tool which I am going to use here is same wp-scan and the below command is used to enumerate the passwords of the mentioned users

> wp-scan –url http://ipaddress/wp-login.php — passwords <password file > — usernames <username>



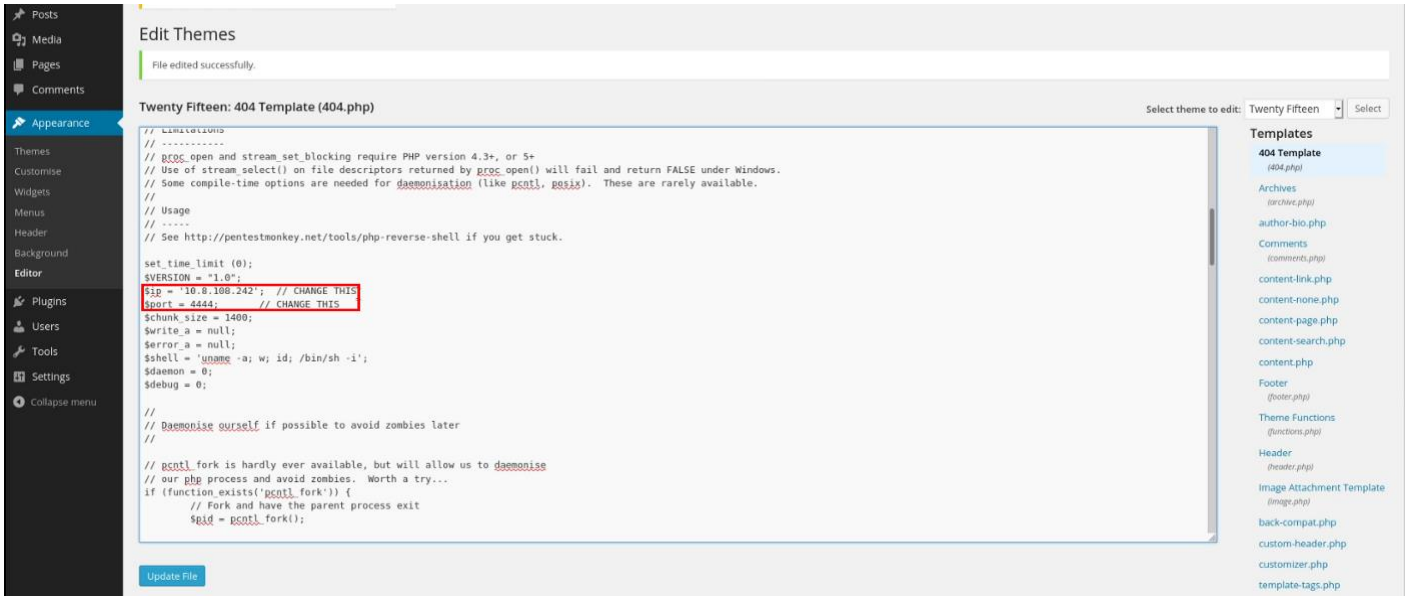


Then using this I logged into the WordPress dashboard

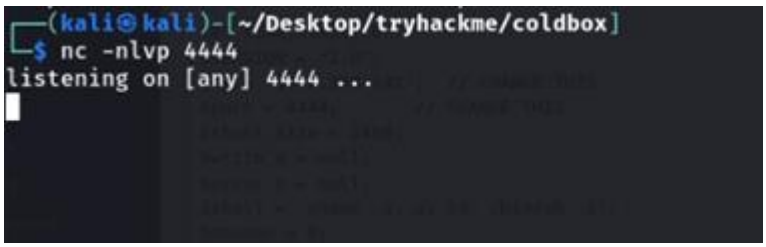


Exploitation

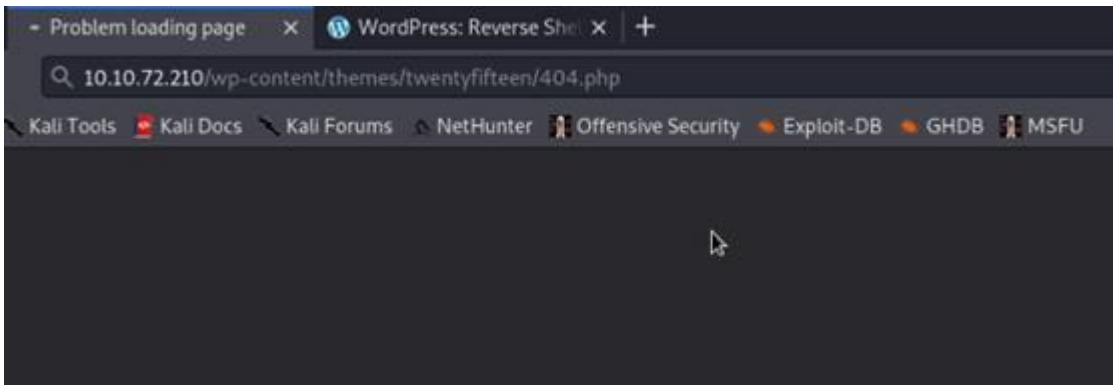
And in WordPress pentesting we knew that if we can able to change the theme editor code then we can able to get the reverse shell easily so I also did the same just edited the 404.php page with my php reverse shellcode and updated the 404.php page. To know more about the WordPress pentesting visit [hacking articles](#) blog



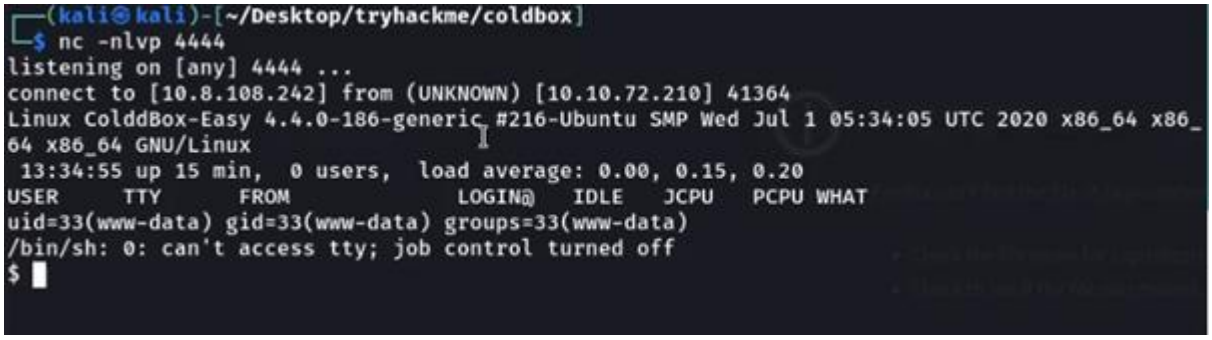
Then after the success update, I started my net cat listener



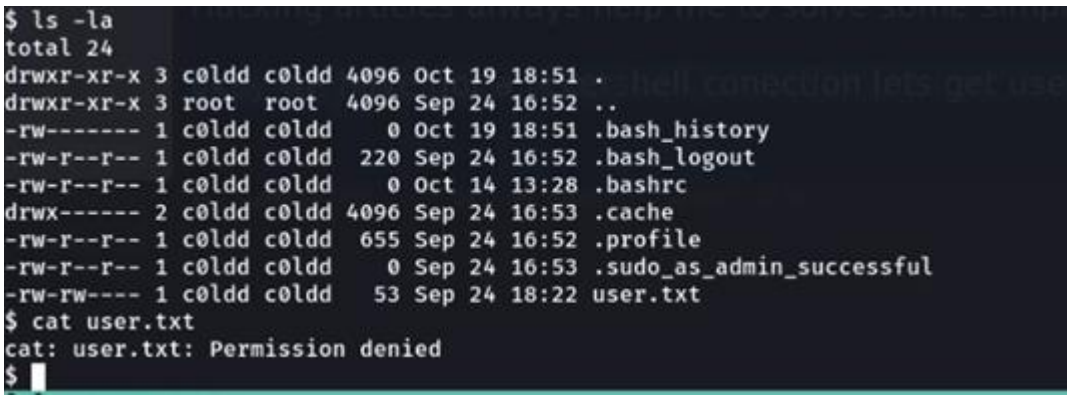
Then I accessed the page in the browser and I got a reverse connection from the webserver



We successfully got a shell of the www-data user



After this step I thought I easily get the user flag but unfortunately I can able to get that because the machine saying that permission is denied for the www-data user



So our next step is to enumerate the internal configuration files and need to get the credentials for any user, so I finalized that this is the WordPress application so it has a wp-config .php file that contains some basic information and sometimes it has hardcoded the password with the file. So I enumerated the file and found a password for the user c0ldd

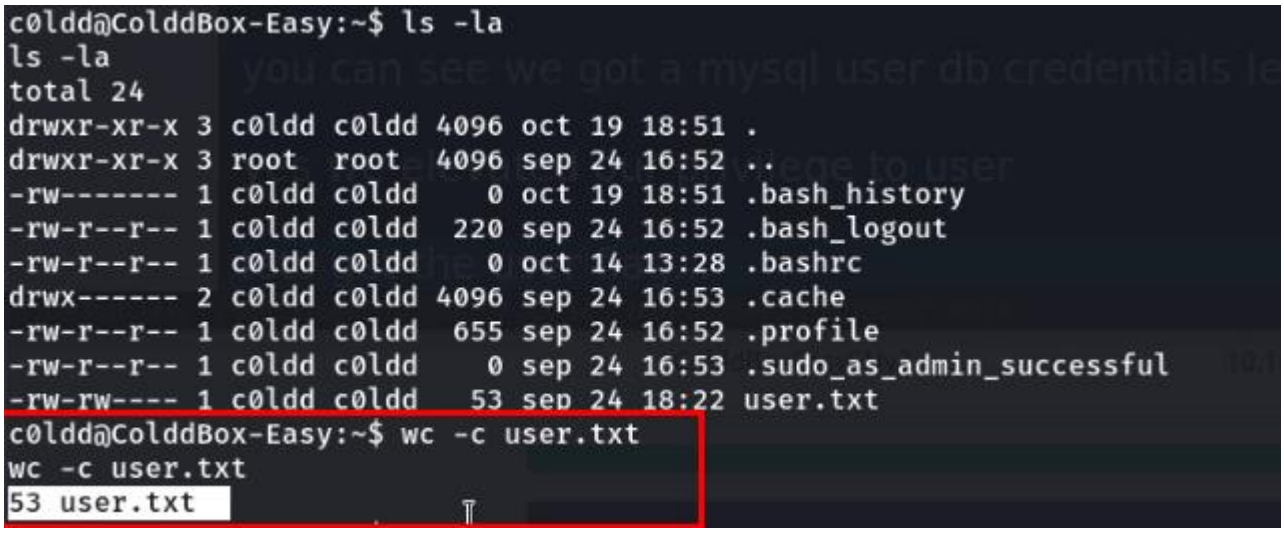
```
$ cd /var/www/html/
$ ls
hidden
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
```

```
// ** 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', [redacted]);

/** 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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
```

I found the DB credentials so I tried these credentials to switch to the user c0ldd using su command and I successfully logged in as a c0ldd user

```
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: [redacted]

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

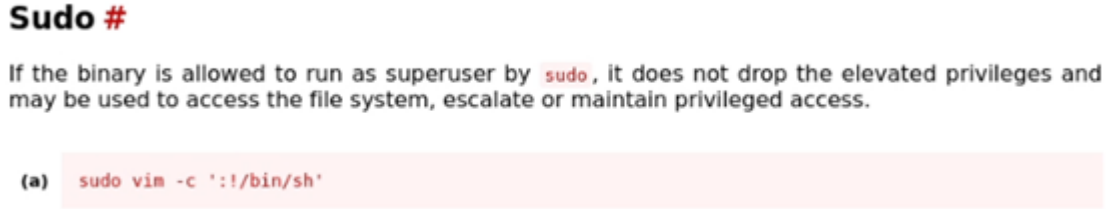
Now we need to get the user flag, but I will not show the user flag here. But you can view the user flag now without any issues



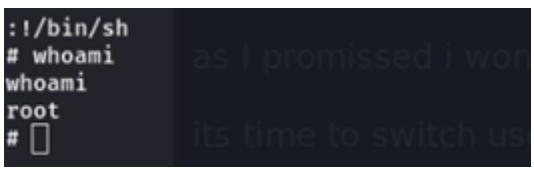
Privilege Escalation

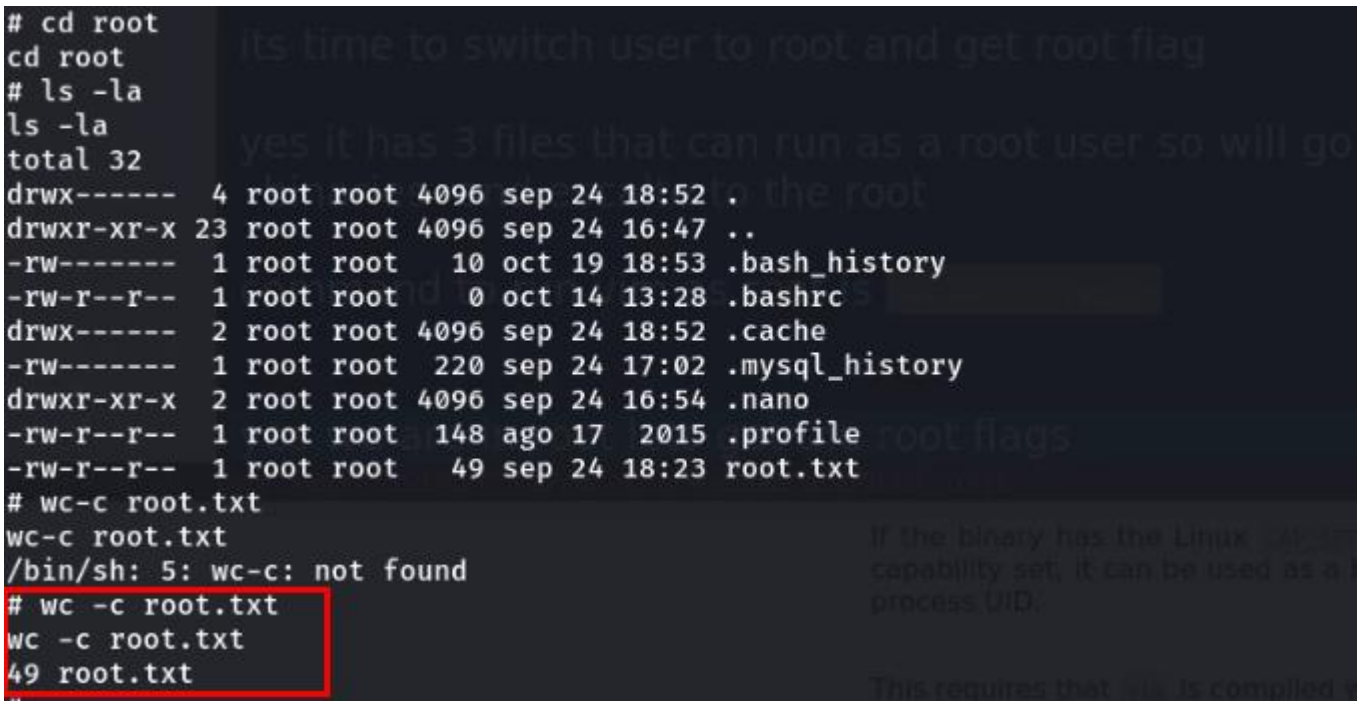
Now we need to escalate our privilege to root to get the root user flag

Great we have found that vim is able to run with root permissions, so will go for our favorite website called GTFOBIN and form there I found a command to run vim as sudo root



By this command, I escalated as root and got a root flag




cd root
cd root
ls -la
ls -la
total 32
drwx------ 4 root root 4096 sep 24 18:52 .
drwxr-xr-x 23 root root 4096 sep 24 16:47 ..
-rw------- 1 root root   10 oct 19 18:53 .bash_history
-rw-r--r-- 1 root root   0 oct 14 13:28 .bashrc
drwx------ 2 root root 4096 sep 24 18:52 .cache
-rw------- 1 root root 220 sep 24 17:02 .mysql_history
drwxr-xr-x 2 root root 4096 sep 24 16:54 .nano
-rw-r--r-- 1 root root 148 ago 17 2015 .profile
-rw-r--r-- 1 root root   49 sep 24 18:23 root.txt
wc-c root.txt
wc-c root.txt
/bin/sh: 5: wc-c: not found
wc -c root.txt
wc -c root.txt
49 root.txt