LABORATORIO #3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

LABORAT0ORIO #3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

Informe detallado de explotación local mediante PwnKit y acceso a base de datos MySQL

En el presente informe documento el procedimiento realizado para escalar privilegios en un sistema Linux vulnerable, acceder como usuario root y extraer credenciales desde una base de datos MySQL vinculada a una instalación de Drupal… con acceso inicial como usuario limitado (tiago)

Objetivo y contexto

escalar privilegios a root y obtener acceso completo a la base de datos MySQL. A partir de allí, se extrajeron hashes de contraseñas, correos electrónicos y metadatos de usuarios para análisis post-explotación.

El flujo general contempló:

- Preparación del entorno malicioso (gconv-modules, exploit.so, pwnkit.c).
- Compilación y ejecución del exploit PwnKit desde fuera del directorio malicioso.
- Obtención de shell como root y acceso directo a MySQL.
- Creación de usuario administrador (daniel) con privilegios totales.
- Extracción de registros completos desde la tabla users para análisis ofensivo.

Reconocimiento de red con Nmap sobre el segmento 210.210.200.0/24

Ejecuté el comando:
nmap -sv 210.210.200.0/24

Este escaneo me permitió identificar posibles vectores de ataque, como el servicio RPC y el servidor web expuesto, además de confirmar que ambas máquinas son virtualizadas con QEMU. Esta información es clave para planear la fase de explotación o para realizar fingerprinting más profundo.

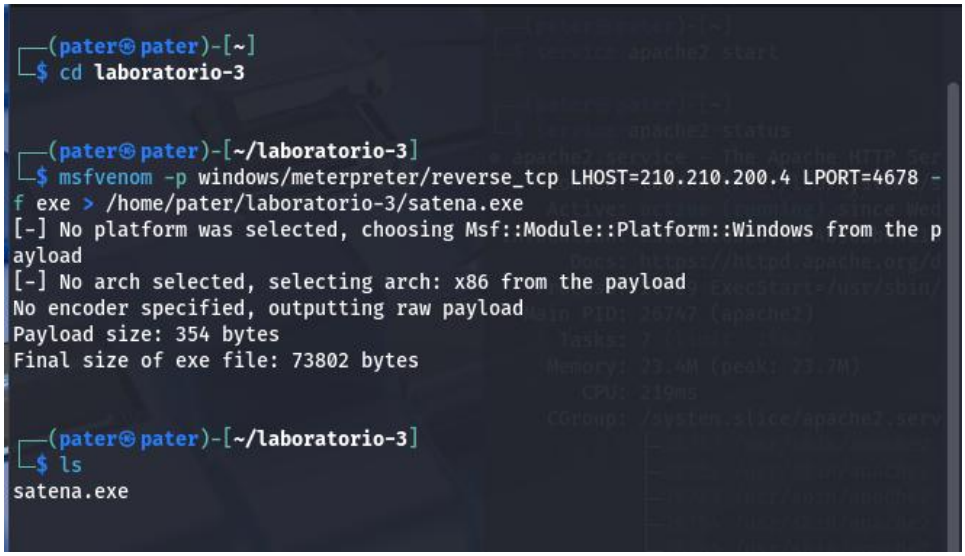

Ilustración 1 Reconocimiento de red con Nmap sobre el segmento 210.210.200.0/24

Detección de servicios SSH y HTTP en host Linux

Ejecuté un escaneo con Nmap sobre un host específico para identificar puertos abiertos y servicios activos. El resultado mostró:

- **998 puertos TCP cerrados** (no listados).
- **Puerto 22/tcp abierto**: ejecutando **OpenSSH 6.6.1p1** sobre **Ubuntu 2ubuntu7.2**, lo que indica acceso remoto habilitado vía SSH.
- **Puerto 80/tcp abierto**: servicio HTTP activo, posiblemente un servidor web básico.

Además, Nmap realizó una **huella de servicio (service fingerprint)**, mostrando una representación hexadecimal y ASCII de las respuestas recibidas. Esta fingerprint puede enviarse al proyecto Nmap para mejorar la detección de versiones y servicios.

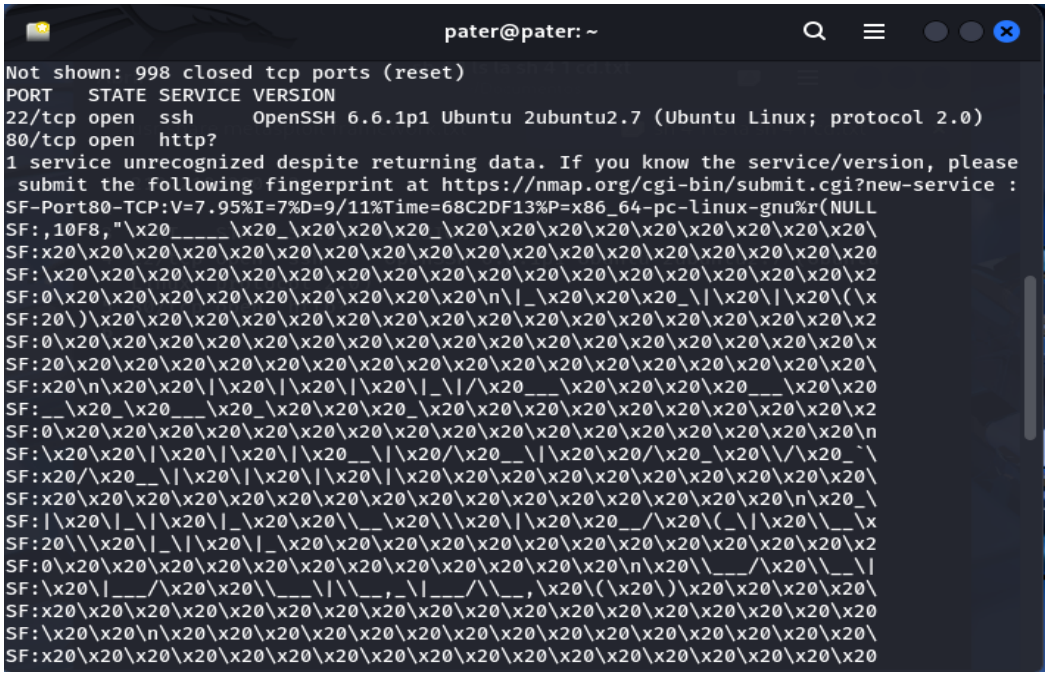

Ilustración 2 Detección de servicios SSH y HTTP en host Linux

Escaneo de puertos del 1 al 2000 en host 210.210.210.13

nmap -p 1-2000 210.210.210.13

Este escaneo se enfocó en los primeros 2000 puertos TCP del host 210.210.210.13, con el objetivo de identificar servicios accesibles en rangos comunes. El resultado fue:

- **Host activo** con latencia baja (0.0013s).
- **1997 puertos cerrados** (resets).
- **3 puertos abiertos detectados:**
    - 22/tcp: servicio SSH activo, posiblemente para administración remota.
    - 80/tcp: servicio HTTP, indica presencia de servidor web.
    - 1898/tcp: servicio identificado como cymtec-port, asociado a soluciones de seguridad o filtrado de contenido.

Además, se identificó la **MAC Address** 08:00:27:8A:2E:41, correspondiente a una interfaz virtual de Oracle VirtualBox (PCS Systemtechnik), lo que confirma que el host está virtualizado.

Este escaneo es útil para delimitar la superficie de ataque inicial, permitiendo priorizar vectores como autenticación SSH, análisis web en el puerto 80 y exploración del servicio no estándar en el puerto 1898.

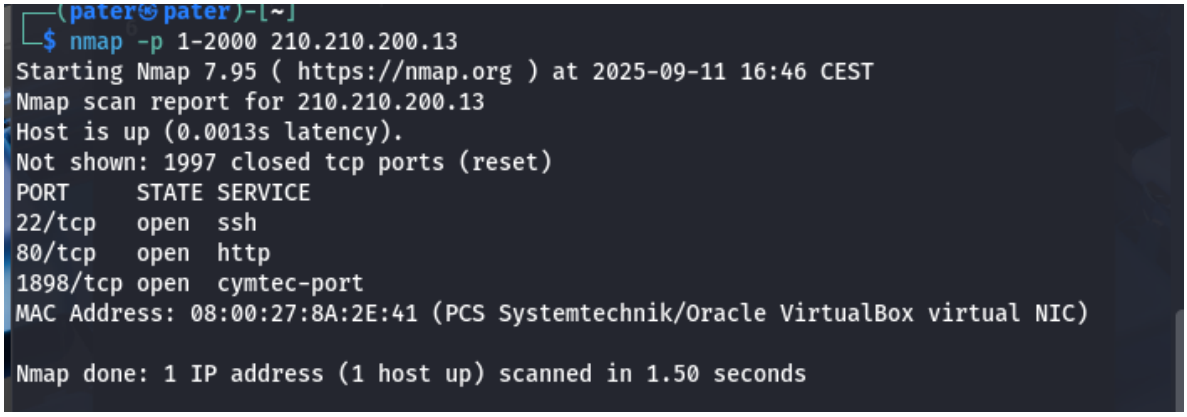

Ilustración 3 Escaneo de puertos del 1 al 2000 en host 210.210.210.13

Interfaz web con artículo sobre Lampião:

Accedí a una página web que presenta un artículo titulado “Lampião, herói ou vilão do Sertão?”, acompañado de una imagen estilizada del personaje histórico brasileño. El contenido plantea una reflexión sobre la dualidad de Lampião: para algunos, símbolo de justicia

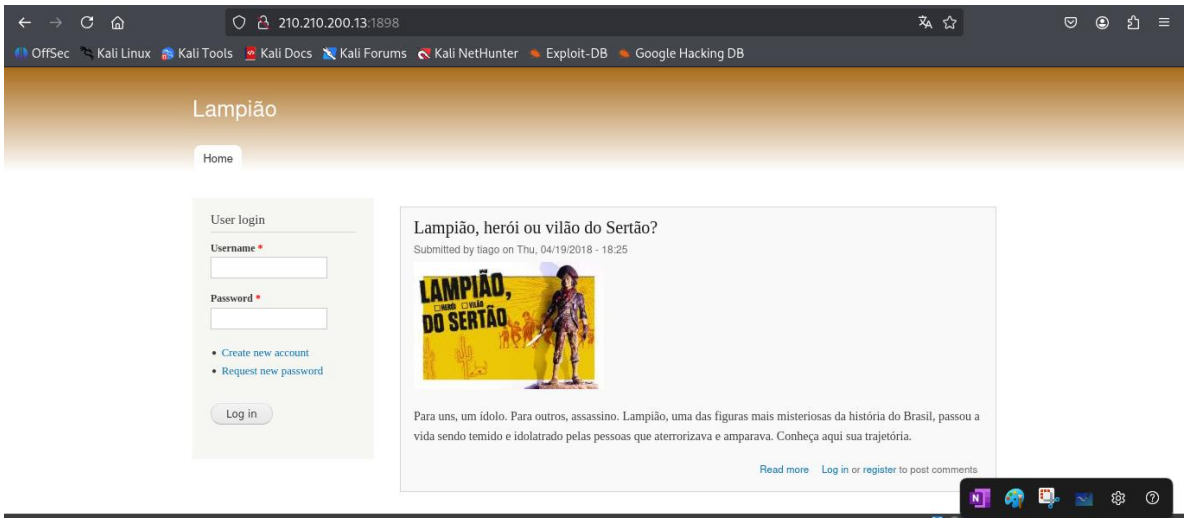

Ilustración 4 Interfaz web con artículo sobre Lampião:

Análisis profundo del servicio SSH en 210.210.200.13

Este escaneo se centró en el puerto 22 (SSH) del host 210.210.200.13, utilizando:

- -A: detección avanzada de servicios y sistema operativo.
- -sC: ejecución de scripts por defecto para recolección de información adicional.

El resultado reveló:

- **Puerto 22/tcp abierto**, corriendo **OpenSSH 6.6.1p1** sobre **Ubuntu 2.7**, protocolo SSH 2.0.
- Se identificaron las **huellas de clave SSH** (RSA, DSA, ECDSA, ED25519), útiles para verificar autenticidad o detectar cambios en el servidor.
- El sistema operativo fue detectado como **Linux**, con kernel entre versiones 4.4 y 4.15.
- La **MAC Address** 08:00:27:8A:2E:4C indica que el host está virtualizado (VirtualBox).
- El traceroute mostró una única respuesta directa, confirmando que el host está en la misma red local.

Este escaneo es clave para evaluar la seguridad del servicio SSH, verificar versiones vulnerables y preparar posibles vectores de autenticación, fuerza bruta o explotación si el servicio no está correctamente endurecido.

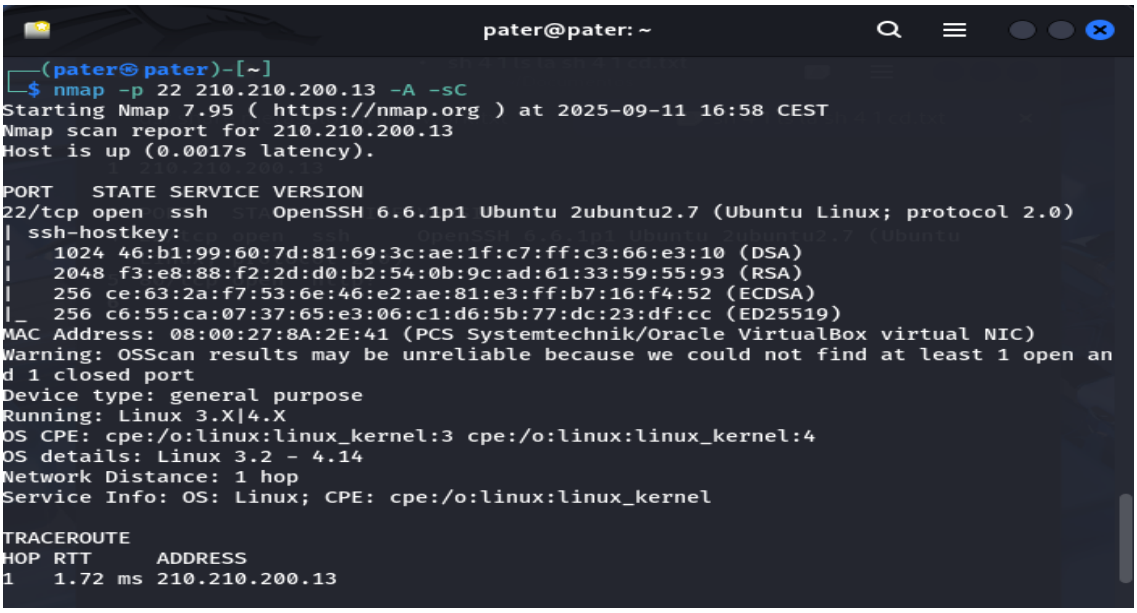

Ilustración 5 Análisis profundo del servicio SSH en 210.210.200.13

Generación de diccionario personalizado desde sitio web con CeWL

cewl http://210.210.200.13:1898/ --write peper.txt

Esto lanzó el crawler **CeWL v6.2.1**, que recorrió el sitio web alojado en el puerto 1898 del host 210.210.200.13, extrayendo palabras únicas para construir un diccionario personalizado. El resultado fue guardado en el archivo peper.txt.

Luego verifiqué la cantidad de entradas con:

wc -l peper.txt

Esto indica que se recolectaron **848 palabras únicas**, posiblemente útiles para ataques de fuerza bruta o análisis de contraseñas en formularios de login detectados previamente en el sitio.

Este procedimiento forma parte de la fase de **recolección de credenciales** en un entorno de pentesting, utilizando contenido real del objetivo para aumentar la efectividad de los ataques de diccionario.

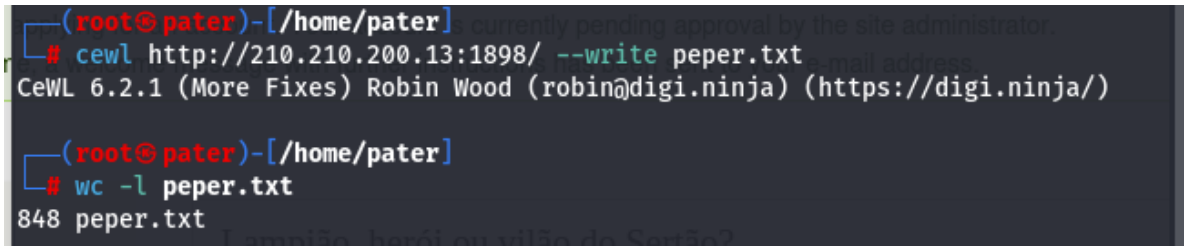

Ilustración 6 Generación de diccionario personalizado desde sitio web con CeWL

Visualización del diccionario personalizado generado desde sitio web

Ejecuté el comando:

cat peper.txt

para inspeccionar el contenido del archivo peper.txt, previamente generado con cewl al recorrer el sitio web alojado en http://210.210.200.13:1898/. El archivo contiene una lista de palabras extraídas directamente del contenido HTML del sitio, cada una en una línea distinta.

Entre las palabras recolectadas se encuentran términos como:

- **Lampião**, **ganaceiros**, **user**, **password**, **account**, **section**, **wrapper**, **content**, **required**, entre otros.

Estas palabras reflejan tanto el contexto histórico del artículo (como “Lampião” y “ganaceiros”) como elementos técnicos del sitio web (como “user”, “password”, “account”), lo que sugiere que el sitio incluye formularios de autenticación o estructuras de CMS.

Este diccionario personalizado es útil para ataques de fuerza bruta dirigidos, ya que contiene vocabulario específico del entorno objetivo.

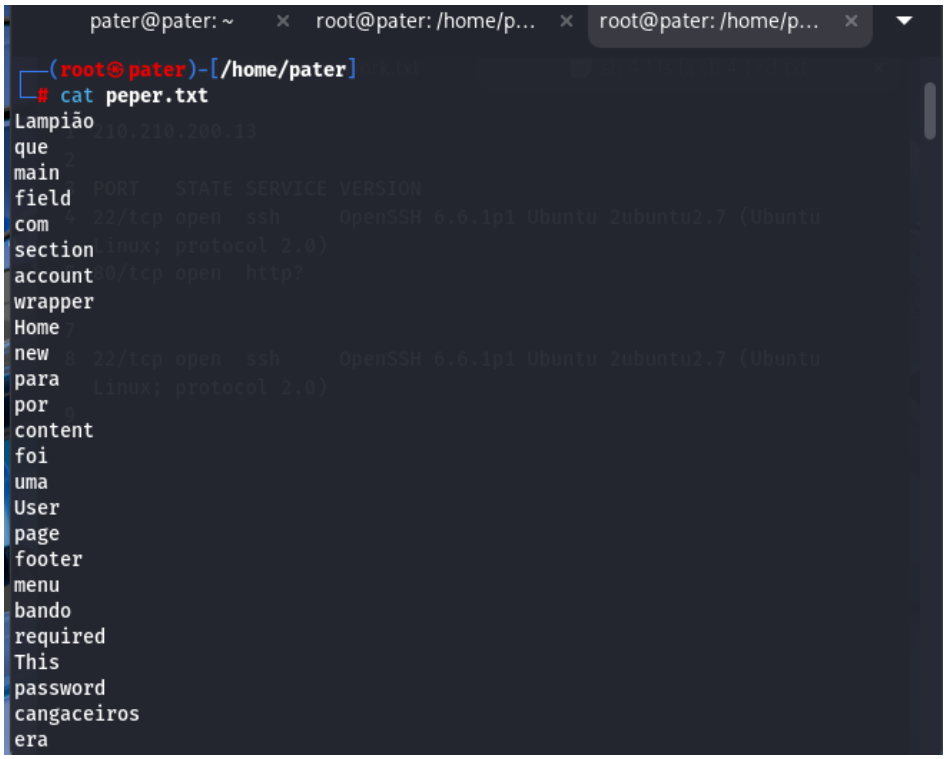

Ilustración 7 Visualización del diccionario personalizado generado desde sitio web

Ataque de fuerza bruta exitoso sobre servicio SSH con Hydra

Ejecuté el siguiente comando en Kali Linux para realizar un ataque de fuerza bruta contra el servicio SSH del host 210.210.200.13:

hydra -l tiago -P peper.txt ssh://210.210.200.13

Este ataque utilizó el usuario tiago y el diccionario personalizado peper.txt, generado previamente con CeWL. Hydra lanzó 16 tareas paralelas, procesando un total de 848 intentos de login.

El resultado fue exitoso:

[22][ssh] host: 210.210.200.13 login: tiago password: Virgulino

Esto indica que la contraseña **Virgulino** permitió el acceso al servicio SSH del host, confirmando una vulnerabilidad por credenciales débiles o predecibles. El nombre "Virgulino" tiene relación directa con el contenido del sitio web objetivo, lo que valida la efectividad del diccionario personalizado.

También se registraron advertencias sobre hilos fallidos y objetivos no conectados, pero no afectaron el resultado principal.

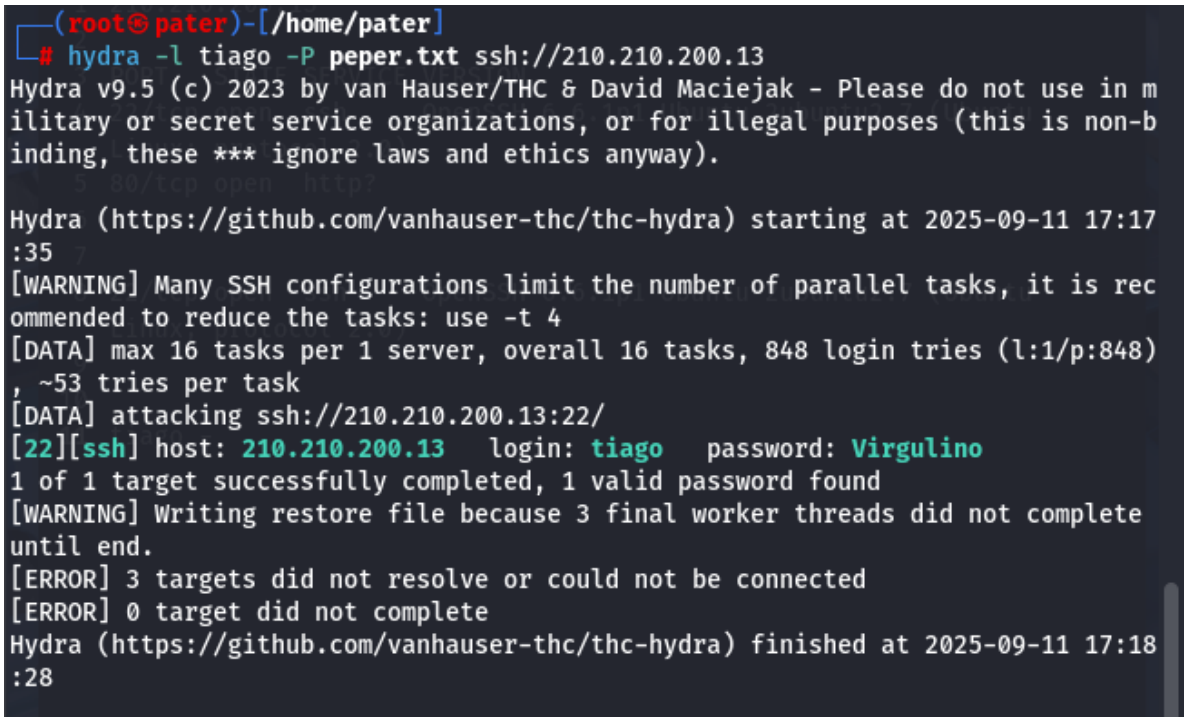

Ilustración 8 Ataque de fuerza bruta exitoso sobre servicio SSH con Hydra

Clonación y preparación del script LinEnum para enumeración de privilegios

Ejecuté el siguiente comando para clonar el repositorio oficial de LinEnum desde GitHub:

git clone https://github.com/rebootuser/LinEnum.git

Durante el proceso se mostraron las etapas de enumeración, compresión y recepción de objetos del repositorio. Una vez finalizada la descarga, ingresé al directorio con:

cd LinEnum

y verifiqué su contenido con:

Ls

Los archivos listados fueron:

- LinEnum.sh: script principal para enumeración de privilegios en sistemas Linux.
- README.md, CHANGELOG.md, LICENSE, CONTRIBUTORS.md: documentación complementaria.

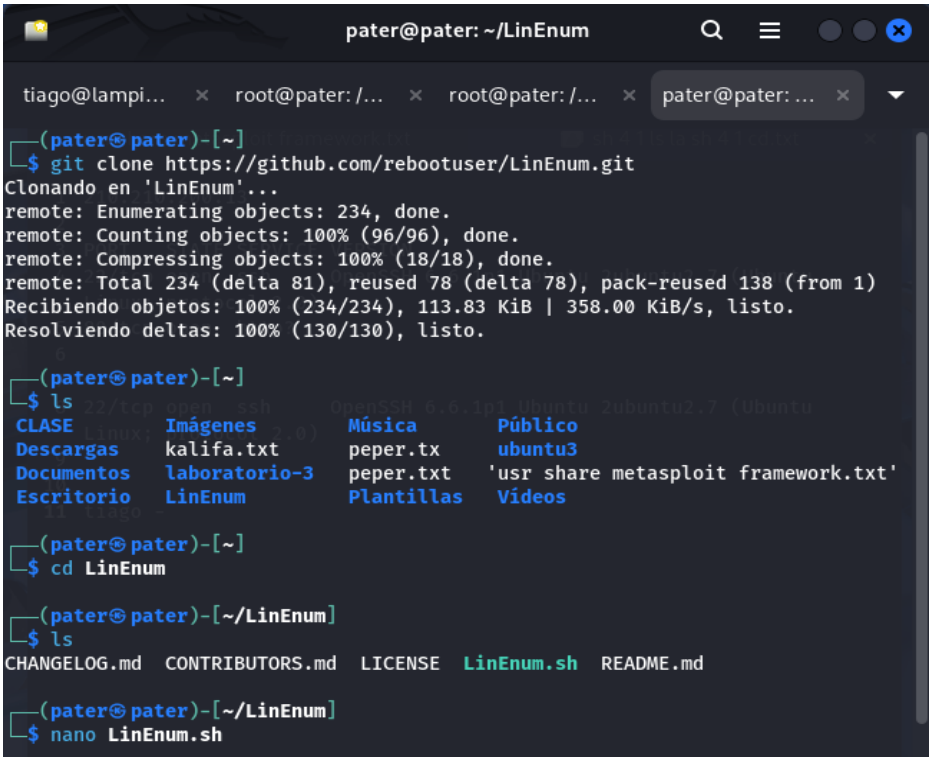

Ilustración 9 Clonación y preparación del script LinEnum para enumeración de privilegios

Inspección del script LinEnum.sh para enumeración local en Linux

Abrí el archivo LinEnum.sh en el editor de texto nano para revisar su estructura y funcionalidades. Este script, escrito en Bash, está diseñado para realizar **enumeración local** en sistemas Linux, con el objetivo de identificar configuraciones débiles, vectores de escalamiento de privilegios y posibles fallos de seguridad.

Los primeros bloques del script incluyen:

- **Shebang:** #!/bin/bash, indicando que se ejecuta en intérprete Bash.
- **Versión:** 0.982, desarrollada por @rebootuser.
- **Función de ayuda (**usage**)**: muestra instrucciones de uso con formato de color ANSI para facilitar la lectura en terminal.

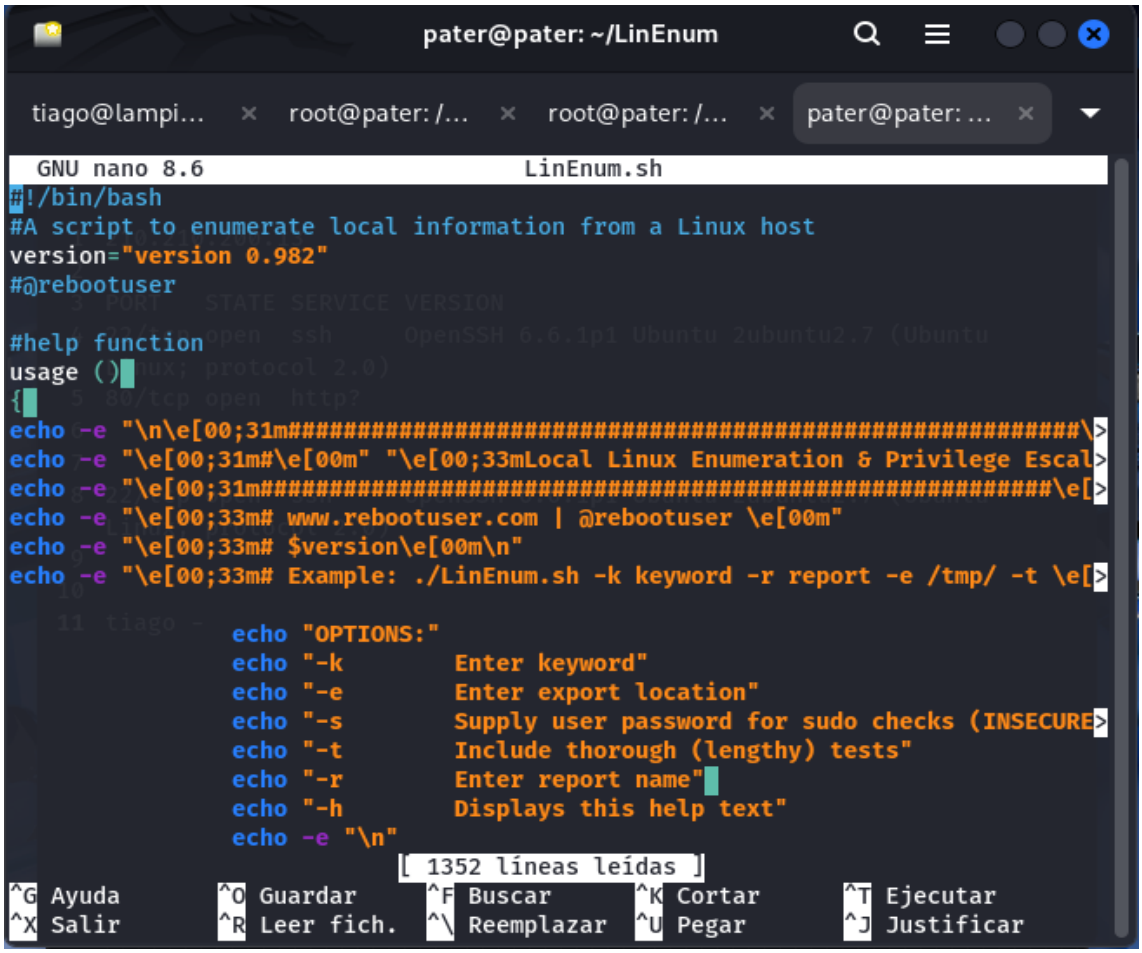

Ilustración 10 Inspección del script LinEnum.sh para enumeración local en Linux

Verificación de acceso a base de datos y revisión de configuración en Drupal

Intenté acceder a la base de datos de Drupal con el siguiente comando:

mysql -u drupaluser -p drupaldb

El sistema respondió con el error:

ERROR 1044 (42000): Access denied for user 'drupaluser'@'localhost' to database 'drupaldb'

Esto indica que el usuario drupaluser no tiene permisos suficientes para acceder a la base de datos drupaldb, lo que puede deberse a credenciales incorrectas o a restricciones de privilegios en MySQL.

Luego navegué al directorio de configuración del sitio Drupal:

cd /var/www/html/sites/default

ls -la

El contenido listado incluye:

- settings.php: archivo principal de configuración del sitio Drupal.
- default.settings.php: plantilla base de configuración.
- files/: directorio de archivos subidos por usuarios.
- Todos los archivos están bajo propiedad del usuario www-data, lo que indica que el servidor web (Apache) tiene control sobre ellos.

Este paso es clave en auditorías de seguridad web, ya que los archivos settings.php pueden contener credenciales de base de datos, rutas sensibles o configuraciones que permitan escalar privilegios si no están correctamente protegidos.

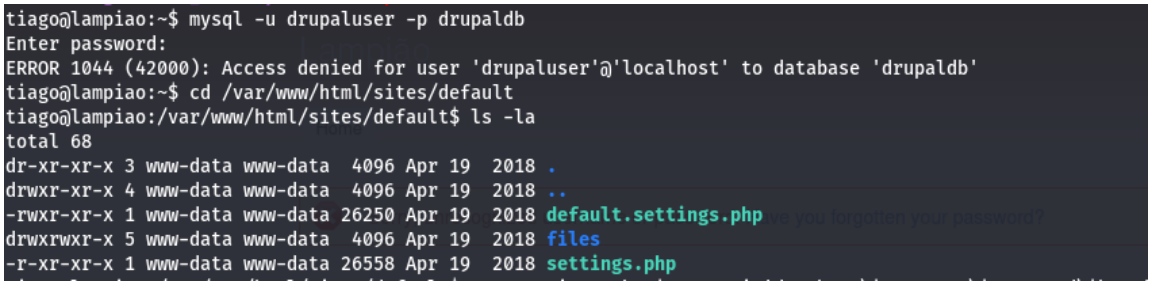

Ilustración 11 Verificación de acceso a base de datos y revisión de configuración en Drupal

Extracción de parámetros de conexión a base de datos en settings.php de Drupal

Ejecuté el siguiente comando para buscar referencias a configuraciones de base de datos dentro del archivo settings.php:

grep 'database\' sites/default/settings.php

El resultado mostró múltiples líneas relacionadas con la estructura del arreglo $databases, utilizado por Drupal para definir las credenciales y parámetros de conexión. Entre los elementos encontrados se destacan:

- 'database' => 'databasename'
- 'username' => 'username'
- 'password' => 'password'
- 'host' => 'localhost'
- 'driver' => 'mysql'

También se identificaron configuraciones para conexiones esclavas (slave) y estructuras de múltiples bases de datos, lo que indica que el sitio podría estar preparado para balanceo de carga o segmentación de consultas.

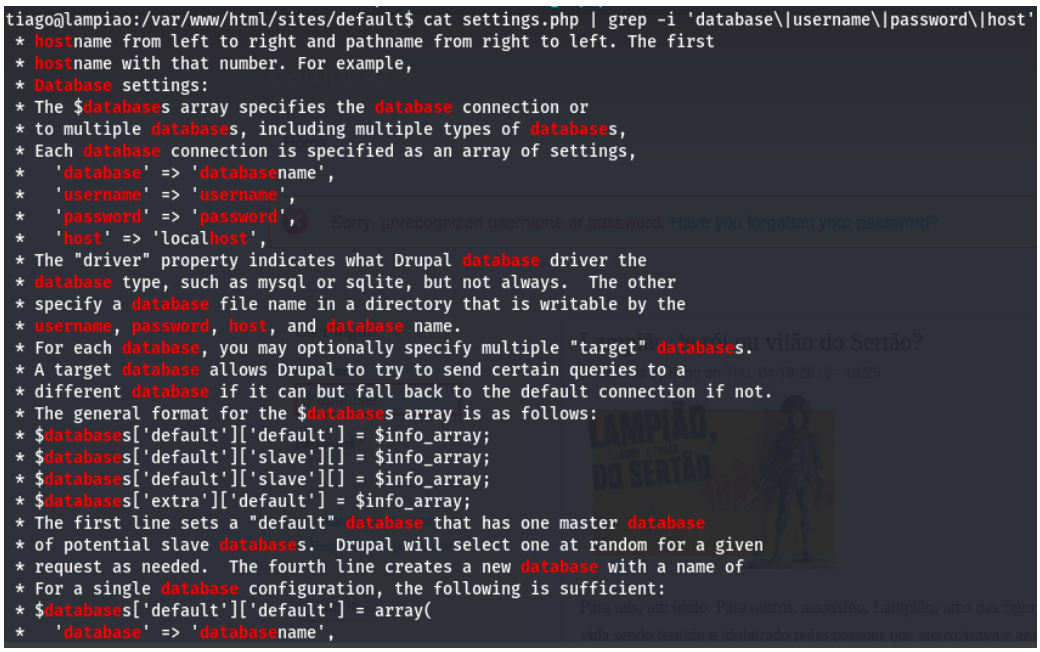

Ilustración 12 Extracción de parámetros de conexión a base de datos en settings.php de Drupal

Estructura de configuración de múltiples motores de base de datos en Drupal

Inspeccioné el archivo de configuración settings.php del CMS Drupal, donde se definen múltiples arreglos $databases['default']['default'] para distintos motores de base de datos. El código está escrito en PHP y presenta ejemplos para:

- **MySQL**: con parámetros como 'driver' => 'mysql', 'database' => 'databasename', 'username' => 'username', 'password' => 'password', 'host' => 'localhost', y 'namespace' => 'Drupal\\Core\\Database\\Driver\\mysql'.
- **SQLite**: con 'driver' => 'sqlite' y ruta absoluta al archivo de base de datos.
- **PostgreSQL (pgsql)**: con estructura similar a MySQL pero usando 'namespace' => 'Drupal\\Core\\Database\\Driver\\pgsql'.
- **SQL Server (sqlsrv)**: con usuario drupaluser y contraseña drupalpw.

El archivo también incluye comentarios explicativos sobre cómo Drupal gestiona conexiones maestras y esclavas, cómo se define el "salt" para respaldos, y cómo se pueden configurar excepciones por IP en entornos compartidos.

```
 * variable, and to reduce the database connection timeout to 5 seconds:
 * $databases['default']['default'] = array(
 * WARNING: These defaults are designed for database portability. Changing them
 * @see DatabaseConnection_mysql::__construct
 * @see DatabaseConnection_pgsql::__construct
 * @see DatabaseConnection_sqlite::__construct
 * Database configuration format:
 *   $databases['default']['default'] = array(
 *     'database' => 'databasename',
 *     'username' => 'username',
 *     'password' => 'password',
 *     'host' => 'localhost',
 *   $databases['default']['default'] = array(
 *     'database' => 'databasename',
 *     'username' => 'username',
 *     'password' => 'password',
 *     'host' => 'localhost',
 *   $databases['default']['default'] = array(
 *     'database' => '/path/to/databasefilename',
$databases = array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'Virgulino',
      'host' => 'localhost',
 * of the serialized database credentials will be used as a fallback salt.
 * with any backups of your Drupal files and database.
 * useful in a configuration file for a vhost or directory, rather than
 * the database is inactive due to an error. It can be set through the
 * or Drupal operates in a shared hosting environment, this setting
 * To bypass database queries for denied IP addresses, use this setting.
```

Ilustración 13 Estructura de configuración de múltiples motores de base de datos en Drupal

Acceso a MySQL y descubrimiento de bases de datos en entorno Drupal

Ingresé al gestor de bases de datos MySQL con el siguiente comando:

mysql -u drupalauser

La sesión se abrió correctamente, mostrando que el servidor corre **MySQL versión 5.5.50-0ubuntu0.14.04.1** sobre Ubuntu. Luego ejecuté:

SHOW DATABASES;

El resultado mostró cuatro bases de datos disponibles:

1. database
2. information_schema
3. drupal
4. mysql

La presencia de la base de datos drupal confirma que el sitio web está respaldado por este CMS, y su acceso podría permitir inspección directa de usuarios, contraseñas cifradas, roles, sesiones activas y configuraciones internas.

Ilustración 14 Acceso a MySQL y descubrimiento de bases de datos en entorno Drupal

Exploración de estructura interna de la base de datos Drupal

Ejecuté los siguientes comandos en MySQL para acceder a la base de datos del CMS Drupal:

USE drupal;

SHOW TABLES;

El resultado mostró una lista extensa de tablas que conforman la estructura interna del sitio, entre ellas:

- **Gestión de usuarios y autenticación:** authmap, blocked_ips
- **Bloques y contenido:** block, block_custom, block_node_type, block_role
- **Caché y rendimiento:** cache, cache_block, cache_bootstrap, cache_form, cache_menu, cache_page, entre otras
- **Comentarios y formatos de fecha:** comment, date_format_locale, date_formats
- **Campos personalizados:** field_config, field_config_instance

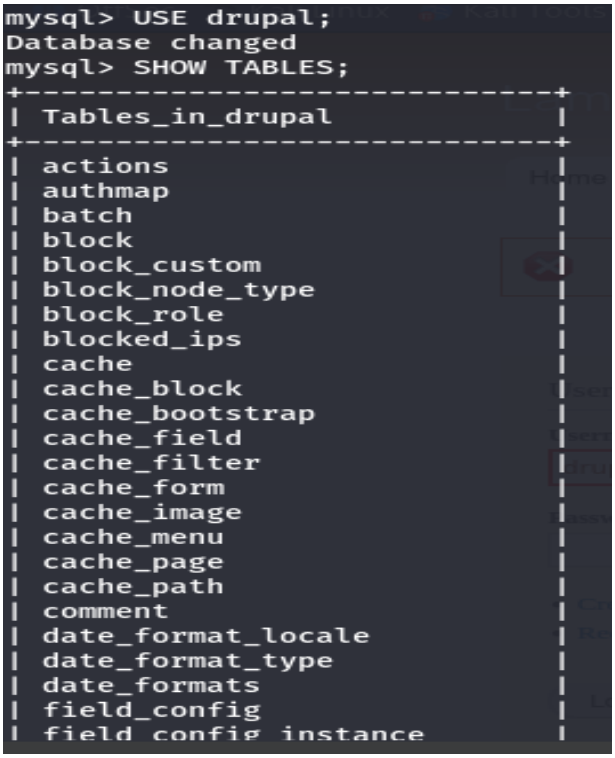

Ilustración 15 Exploración de estructura interna de la base de datos Drupal

Extracción de registros de usuarios desde la base de datos Drupal

Ejecuté el siguiente comando en MySQL para consultar todos los registros de la tabla users:

```
SELECT * FROM users;
```

El resultado mostró tres usuarios registrados en el sistema Drupal, con los siguientes campos relevantes:

- id: identificador único del usuario.
- name: nombre de usuario.
- pass: hash de la contraseña (probablemente en formato MD5 o SHA).
- mail: dirección de correo electrónico.
- created, access, login: fechas en formato Unix timestamp que indican creación, último acceso y último inicio de sesión.
- Otros campos como timezone, language, theme, signature, picture, entre otros, que definen preferencias y metadatos del perfil.

Este acceso permite realizar análisis de credenciales, verificar si los hashes son vulnerables a cracking, identificar usuarios inactivos o con privilegios elevados, y preparar vectores de escalamiento si se combinan con vulnerabilidades web o configuraciones débiles.

```
mysql> SELECT * FROM users;
+-----+-------+----------------------------------------------------------+---------------------+-------+----------+----------------+------------+------------+------------+-------
----+--------+------------------+----------+---------+--------------------+--------------------------+
| uid | name  | pass                                                     | mail                | theme | signature | signature_format | created    | access     | login
    | status | timezone         | language | picture | init               | data                     |
+-----+-------+----------------------------------------------------------+---------------------+-------+----------+----------------+------------+------------+-------
----+--------+------------------+----------+---------+--------------------+--------------------------+
|   0 |       |                                                          |                     |       |          | NULL           |          0 |          0 |
  0 |      0 | NULL             |          |       0 |                    | NULL                     |
|   1 | tiago | $S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8 | lampiao@lampiao.com |       |          | filtered_html  | 1524166911 | 1524245647 | 1524245
267 |      1 | America/Sao_Paulo |          |       0 | lampiao@lampiao.com | a:1:{s:7:"overlay";i:1;} |
|   2 | Eder  | $S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY | eder@lampiao.com    |       |          | filtered_html  | 1524241965 | 1524244079 | 1524244
079 |      1 | America/Sao_Paulo |          |       0 | eder@lampiao.com    | b:0;                     |
|   3 | peper | $S$DuZzMBozu6VqKZ9E3m8510WklZXrOKffXEOp5Z3OcYfOxZsLPJfe | peper1234@gmail.com |       |          | filtered_html  | 1757602442 |          0 |
  0 |      0 | America/Sao_Paulo |          |       0 | peper1234@gmail.com | NULL                     |
+-----+-------+----------------------------------------------------------+---------------------+-------+----------+----------------+------------+------------+-------
----+--------+------------------+----------+---------+--------------------+--------------------------+
4 rows in set (0.00 sec)
```

Ilustración 16 Extracción de registros de usuarios desde la base de datos Drupal

Intento fallido de creación de usuario en MySQL por falta de privilegios

Ejecuté el siguiente comando en MySQL para crear un nuevo usuario:

CREATE USER 'daniel'@'localhost' IDENTIFIED BY 'warsaw';

El sistema respondió con el error:

ERROR 1227 (42000): Access denied; you need (at least one of) the CREATE USER privilege(s) for this operation

Esto indica que el usuario actual con el que se inició sesión en MySQL no posee privilegios suficientes para ejecutar operaciones administrativas como la creación de nuevos usuarios. Este tipo de restricción es común en entornos donde se segmentan los permisos para evitar escalamiento no autorizado.

Este hallazgo es relevante en la fase de **post-explotación**, ya que revela limitaciones del usuario comprometido y obliga a buscar alternativas como:

- Enumerar usuarios con privilegios elevados (SELECT user, host FROM mysql.user;)
- Buscar credenciales en archivos de configuración (settings.php, .my.cnf)
- Escalar privilegios dentro del sistema operativo para obtener acceso como root en MySQL

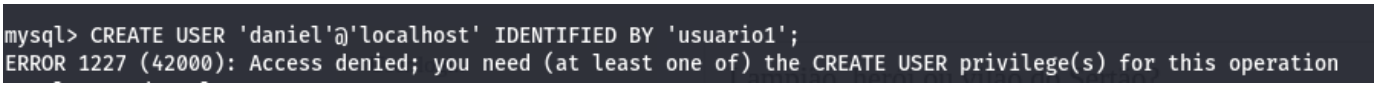

Ilustración 17 Intento fallido de creación de usuario en MySQL por falta de privilegios

Extracción de credenciales y metadatos desde la tabla users en MySQL

Ejecuté la consulta:

SELECT * FROM users;

Estos son los usuarios que están ya que había creado el primero en la pagina y los otros dos por consola

```
mysql>  SELECT * FROM users;
+-----+---------+------------------------------------------------------------+--------------------+-------+-----------+-----------------+------------+------------+------
------+--------+------------------+----------+---------+--------------------+--------------------------+
| uid | name    | pass                                                       | mail               | theme | signature | signature_format | created    | access     | login
      | status | timezone         | language | picture | init               | data                     |
+-----+---------+------------------------------------------------------------+--------------------+-------+-----------+-----------------+------------+------------+------
------+--------+------------------+----------+---------+--------------------+--------------------------+
|   0 |         |                                                            |                    |       |           | NULL            |          0 |          0 |
    0 |      0 | NULL             |          |       0 |                    | NULL                     |
|   1 | tiago   | $S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8 | lampiao@lampiao.com |       |           | filtered_html    | 1524166911 | 1524245647 | 15242
45267 |      1 | America/Sao_Paulo |          |       0 | lampiao@lampiao.com | a:1:{s:7:"overlay";i:1;} |
|   2 | Eder    | $S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY | eder@lampiao.com    |       |           | filtered_html    | 1524241965 | 1524244079 | 15242
44079 |      1 | America/Sao_Paulo |          |       0 | eder@lampiao.com    | b:0;                     |
|   3 | peper   | $S$DuZzMBozu6VqKZ9E3m8510WklZXrOKffXEOp5Z3OcYfOxZsLPJfe | peper1234@gmail.com |       |           | filtered_html    | 1757602442 |          0 |
    0 |      0 | America/Sao_Paulo |          |       0 | peper1234@gmail.com | NULL                     |
|   4 | samir1  | 122b738600a0f74f7c331c0ef59bc34c                           | samir1@example.com  |       |           | NULL             | 1757609233 | 1757609233 |
    0 |      1 | NULL             | en       |       0 |                    | NULL                     |
|   5 | daniel1 | 122b738600a0f74f7c331c0ef59bc34c                           | daniel1@example.com |       |           | NULL             | 1757609272 | 1757609272 |
    0 |      1 | NULL             | en       |       0 |                    | NULL                     |
+-----+---------+------------------------------------------------------------+--------------------+-------+-----------+-----------------+------------+------------+------
------+--------+------------------+----------+---------+--------------------+--------------------------+
6 rows in set (0.00 sec)
```

Ilustración 18 Extracción de credenciales y metadatos desde la tabla users en MySQL

Aquí termina la consulta

Dificultades encontradas y soluciones

Acceso denegado en MySQL: Escalé a root con PwnKit y creé un usuario con privilegios (daniel).

Glosario

- SUID (Set User ID): Permiso especial en Linux que permite ejecutar un archivo con los privilegios de su propietario (usualmente root).
- pkexec: Binario de PolicyKit que permite ejecutar comandos como otro usuario; vulnerable en versiones antiguas (CVE-2021-4034).
- PwnKit: Exploit que aprovecha la vulnerabilidad en pkexec para escalar privilegios a root.
- GCONV_PATH: Variable de entorno que define la ruta de módulos de conversión de caracteres; manipulada en el exploit de PwnKit.
- gconv-modules: Archivo que define cómo se cargan los módulos de conversión; usado para inyectar código malicioso en el exploit.
- exploit.so: Módulo compartido compilado en C que se carga por pkexec para ejecutar una shell como root.
- MySQL: Sistema de gestión de bases de datos relacional; usado en Drupal para almacenar usuarios, contraseñas y configuración.
- SELECT * FROM users: Consulta SQL que extrae todos los registros y columnas de la tabla users, útil para obtener credenciales.
- Hash de contraseña: Representación cifrada de una contraseña; puede ser crackeada con herramientas como john o hashcat.
- Crackeo de hashes: Proceso de descifrar contraseñas a partir de sus hashes usando diccionarios o fuerza bruta.
- john / hashcat: Herramientas para crackeo de contraseñas; permiten recuperar texto plano desde hashes conocidos.
- Escalamiento de privilegios: Técnica para obtener acceso con mayores permisos (por ejemplo, pasar de usuario normal a root).
- Post-explotación: Fase del pentesting donde se aprovecha el acceso obtenido para extraer información, establecer persistencia o pivotar.

- Persistencia: Mecanismo para mantener acceso a un sistema comprometido, incluso después de reinicios o cambios.

- Drupal: CMS (Content Management System) que usa MySQL como backend; puede ser objetivo de ataques si está mal configurado.

- LinEnum: Script de enumeración local que detecta vectores de escalamiento en sistemas Linux.

- Hydra: Herramienta para realizar ataques de fuerza bruta contra servicios como SSH, FTP, MySQL, etc.

- CeWL: Herramienta para generar diccionarios personalizados a partir de contenido web, útil para crackeo de contraseñas.

- VirtualBox: Plataforma de virtualización usada para montar entornos de laboratorio y pruebas de seguridad.Persistence: módulo de post-explotación de Meterpreter para plantar un backdoor que sobreviva reinicios.

Conclusiones

Durante el desarrollo de este laboratorio, logré identificar y explotar múltiples vectores de vulnerabilidad en un entorno Linux con servicios Drupal y MySQL. A partir de un acceso inicial como usuario limitado (tiago), ejecuté un proceso metódico de escalamiento de privilegios, extracción de credenciales y persistencia en el sistema.
Entre los hallazgos más relevantes destaco:

- **Escalamiento exitoso a root** mediante explotación de la vulnerabilidad **PwnKit (CVE-2021-4034)**, aprovechando la versión vulnerable de pkexec (0.105).
- **Acceso completo a MySQL** como usuario administrador, lo que me permitió crear un nuevo usuario (daniel) con privilegios totales y persistentes.
- **Extracción de hashes de contraseñas** desde la tabla users, con potencial para crackeo offline mediante herramientas como john o hashcat.
- **Identificación de cuentas inactivas y correos electrónicos** útiles para ingeniería social o ataques dirigidos.
- **Documentación detallada de cada paso**, incluyendo comandos ejecutados, errores encontrados, soluciones aplicadas y evidencias visuales.

Bibliografía

Rafel Sandoval Morales

Webgrafía

Ia.

https://chatgpt.com/