Informe 2 – Segundo Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Septiembre 2025

Tabla de Contenido

Pag.

Tabla de Ilustraciones

Pag.

Introducción

En este informe se documenta el proceso de auditoría práctica realizado sobre la máquina objetivo **Lampaio**. El ejercicio incluye la importación y configuración de la máquina vulnerable, labores de reconocimiento y escaneo de puertos, recopilación de palabras para ataques por fuerza bruta, explotación de credenciales, escalada de privilegios locales, y finalmente la interacción con la aplicación web (Drupal) para crear usuarios en la base de datos y comprobar el acceso.

Objetivos

Objetivo General

Realizar una auditoría sobre la máquina **Lampaio** para identificar huecos de acceso, obtener credenciales válidas, escalar privilegios en el sistema operativo y crear usuarios en la aplicación web alojada, documentando el proceso y los hallazgos.

Objetivos Específicos

Importar y configurar la máquina objetivo **Lampaio** en el entorno de laboratorio, comprobando conectividad y asignación de IP.

Realizar reconocimiento y enumeración (escaneos Nmap, enumeración web y generación de diccionario con CeWL) para identificar servicios, usuarios y posibles vectores de ataque.

Obtener acceso inicial a la máquina (credenciales válidas por fuerza bruta o descubrimiento) y escalar privilegios localmente mediante técnicas y exploits apropiados.

Acceder a la base de datos de la aplicación (Drupal), crear dos cuentas de usuario en la tabla users, verificar el inicio de sesión y documentar resultados y recomendaciones de seguridad.

Entorno

Se trabajó en un entorno controlado (máquina virtual Kali Linux en VirtualBox) con la máquina objetivo **Lampaio** importada como VM vulnerable.

Las herramientas empleadas incluyeron: nmap, cewl, hydra, ssh, git, gcc/g++, LinEnum/, mysql/mariadb, y utilidades estándar de Linux.

Desarrollo

Importación y configuración de Lampaio

Se importó la máquina Lampaio en VirtualBox y se configuraron las redes necesarias para que la VM atacante (Kali) y la máquina objetivo estuvieran en el mismo segmento.

Ilustración 1 Importación de máquina virtual

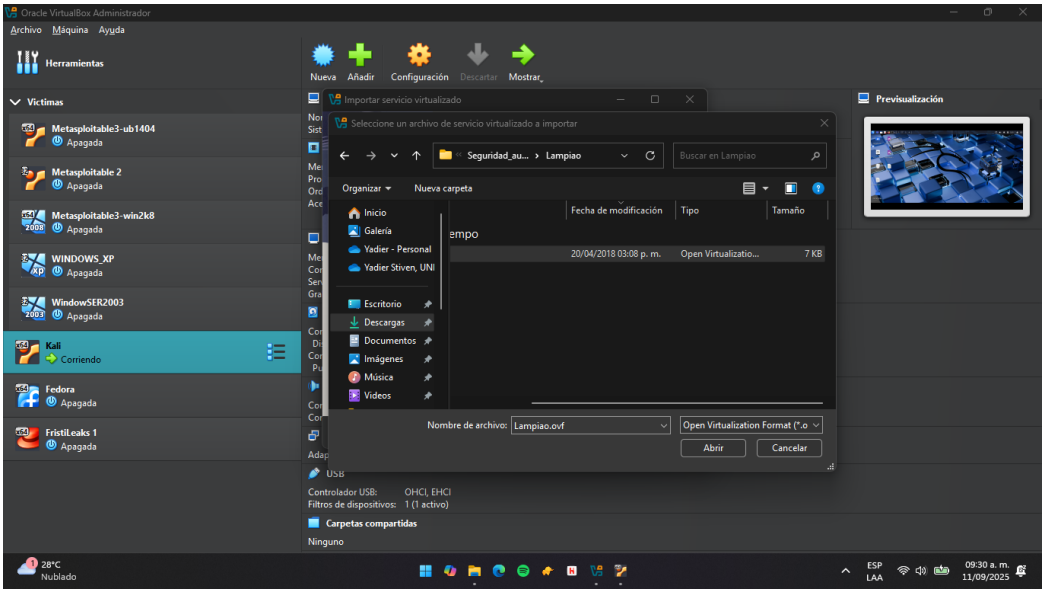
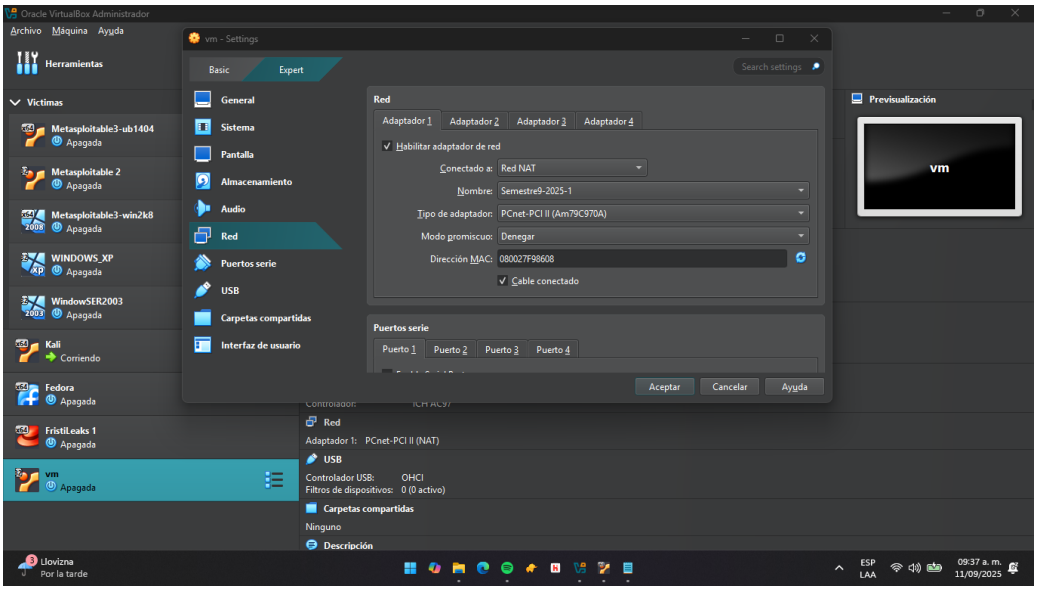


Ilustración 2 Configuración de red



Escaneo nmap

Una vez creada y configurada, se procede a realizar un escaneo desde Nmap donde se identifica que:

Lampaio adquirio la ip **192.168.5.13**

Tiene los siguientes puertos y servicios:

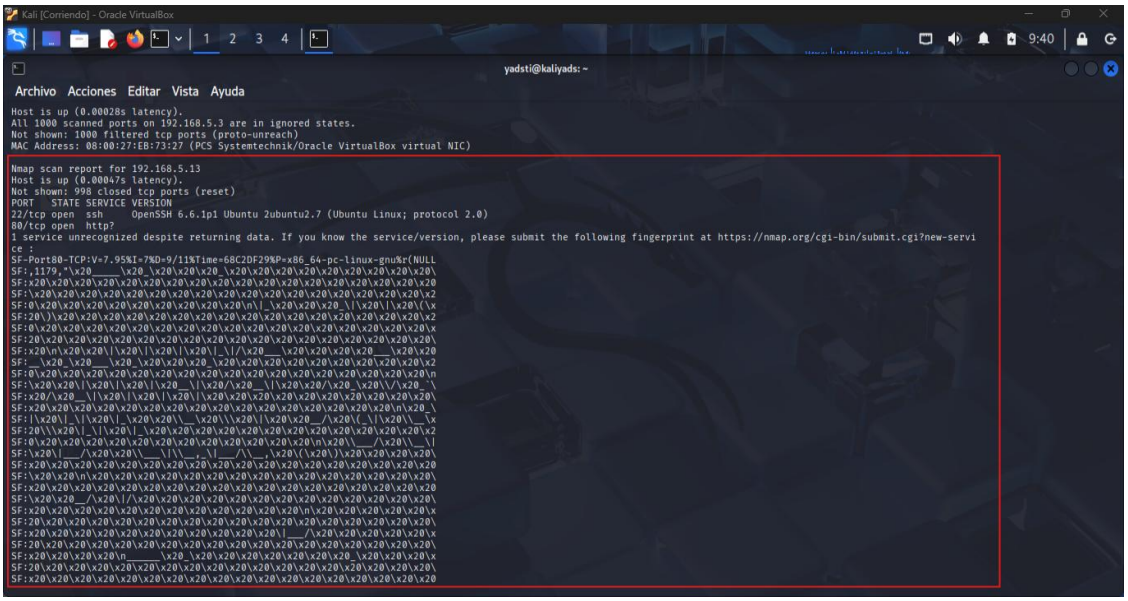
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)

80/tcp open http?

Se encuentra que el puerto 80 tiene un servicio que no se reconoce por lo que hay que escanearlo con mayor detalle.

Ilustración 3 Primer escaneo



Luego se vuelve a escanear, pero esta vez solo escanea la máquina de lampaio **nmap -p 1-2000 192.168.5.13,** con esto se escanean los puertos del 1 al 2000 y da como resultado:

Starting Nmap 7.95 (https://nmap.org) at 2025-09-11 09:46 -05

Nmap scan report for 192.168.5.13

Host is up (0.00057s latency).

Not shown: 1997 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh – servicio ssh

80/tcp open http – sitio web sencillo

1898/tcp open cymtec-port – sitio web con login

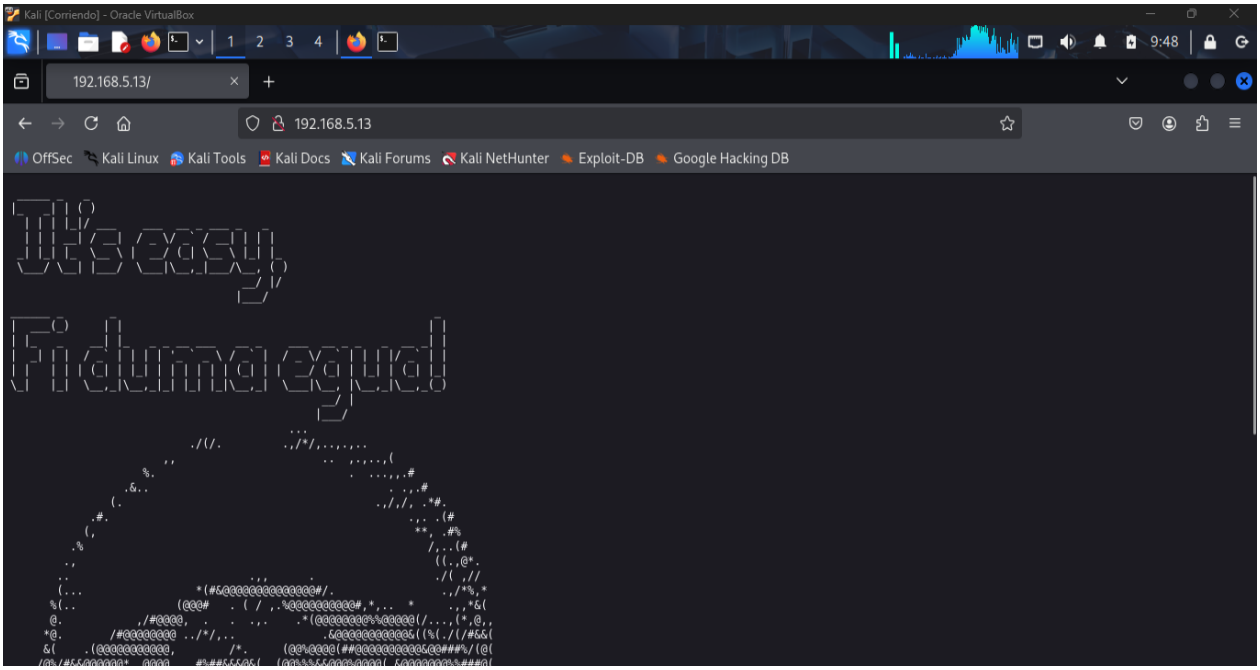
MAC Address: 08:00:27:F9:86:08 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.99 seconds

Inspección de dirección ip en navegador

Se ingresa a el navegador y se ingresa la dirección ip de lampaio para acceder al puerto 80, se observa un sitio web sencillo.

Ilustración 4 Sitio web

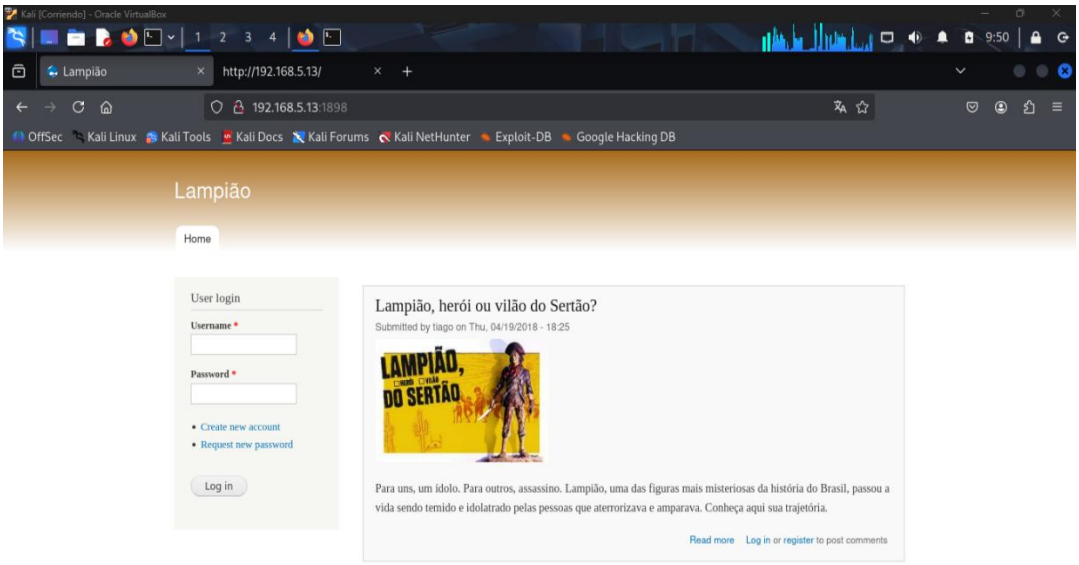


Luego se escanea el puerto 1898 y se observa una página con un login

Además, se encuentran unas publicaciones hechas por los siguientes usuarios:

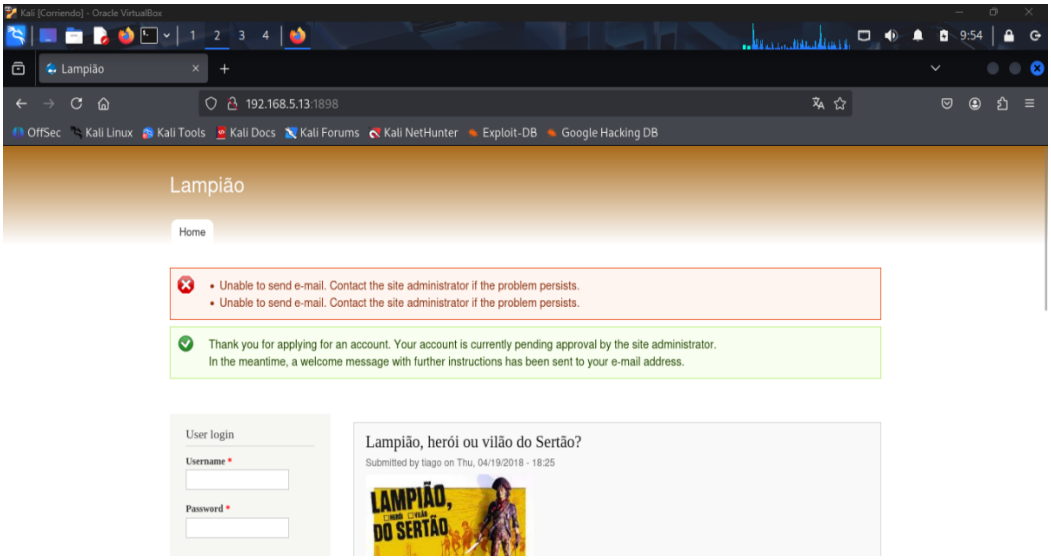
- tiago
- Eder
- LuisGonzaga
- LampaioFalou

Ilustración 5 Sitio web lamapio - login



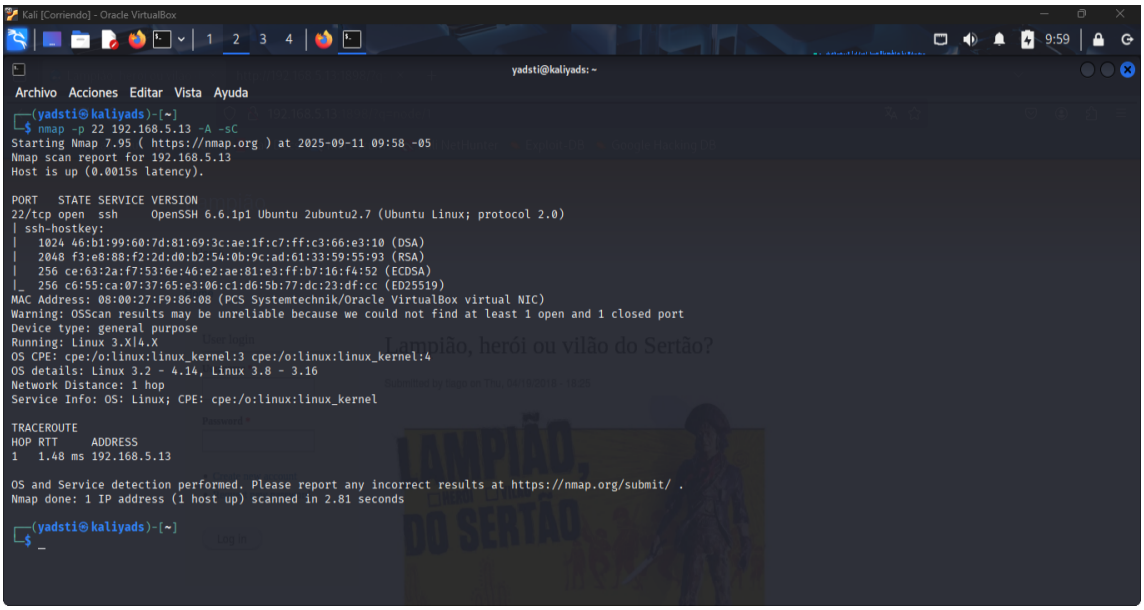
Se intenta iniciar sesión con esos usuarios, pero no es satisfactorio.

Ilustración 6 Intento de login fallido



Después se procede a hacer un escaneo agresivo al puerto 22 y se obtiene la versión del servicio la que será útil para la búsqueda de exploit con el comando nmap -p 22 192.168.5.13 -A sC es un escaneo agresivo con scripts

Ilustración 7 Escaneo agresivo

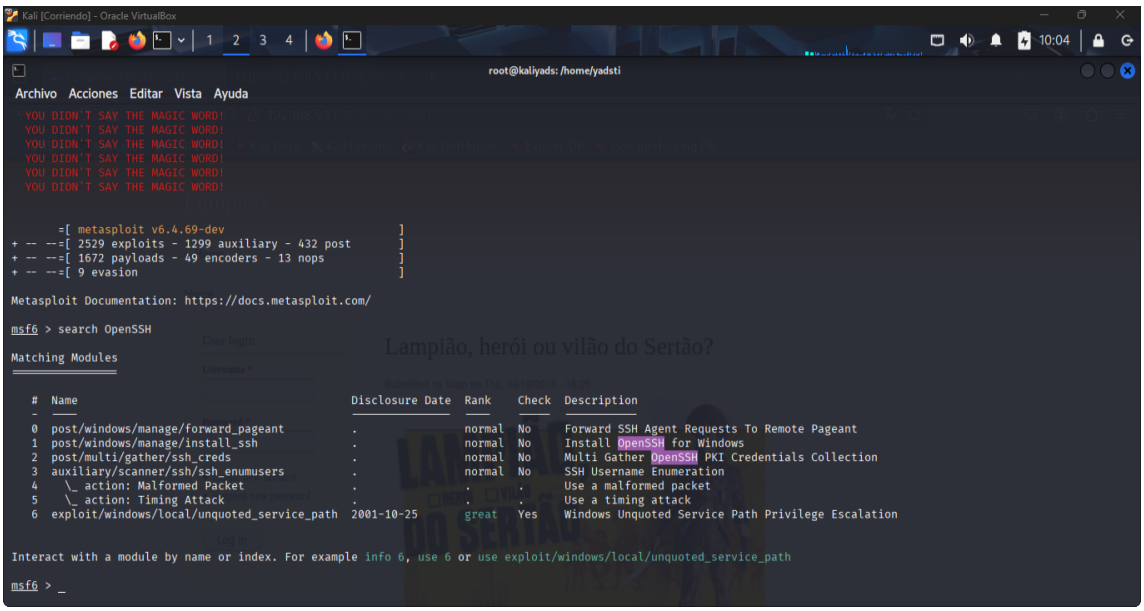


Búsqueda de exploits msfconsole

Se ingresa a la consola de metasploitable framework

Los exploits que aparecen son para Windows por lo tanto no sirven.

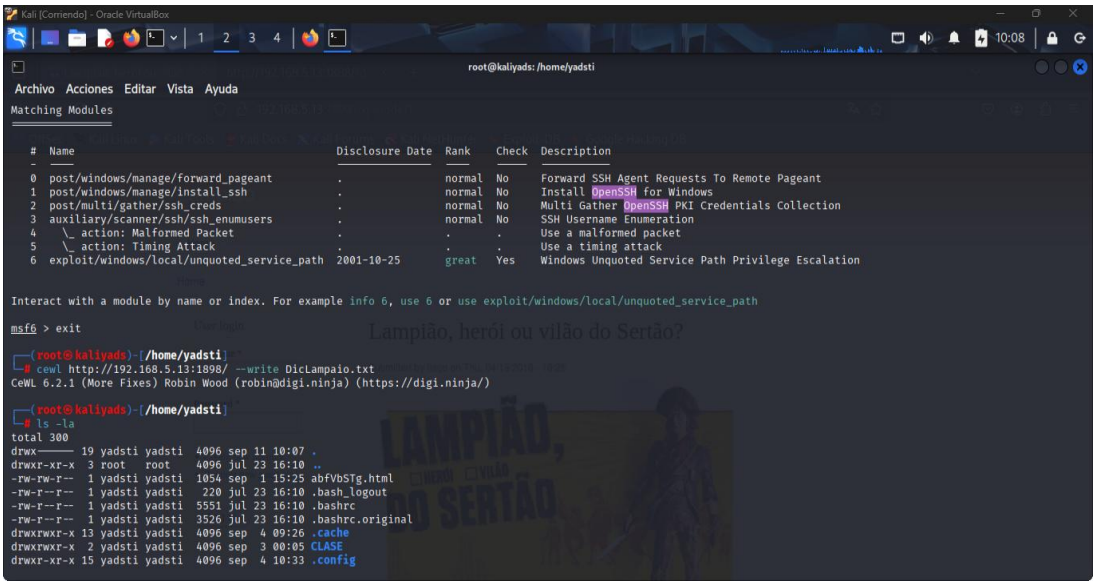
Ilustración 8 Búsqueda de exploits msfconsole



Enumeración y recolección de palabras claves del sitio

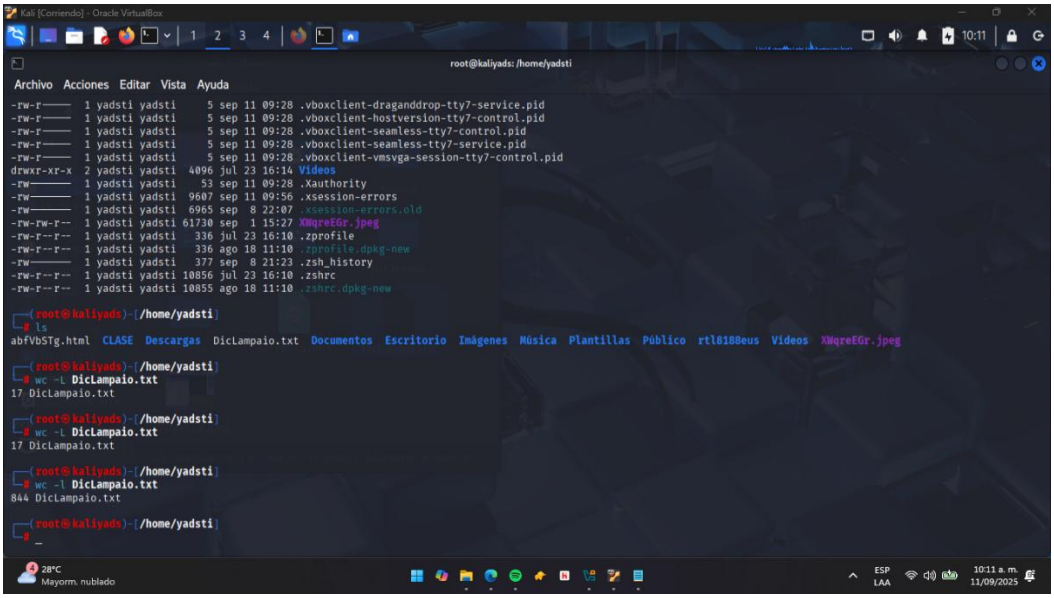
Se procede a crear un diccionario de toda la página con el siguiente comando cewl http://192.168.5.13:1898/ --write DicLampaio.txt, este comando lo que hace es escribir todo el contenido de la página en un diccionario

Ilustración 9 Creación de diccionario palabras de sitio web



Eso genera un archivo con 844 palabras que se pueden utilizar en ataques de fuerza bruta.

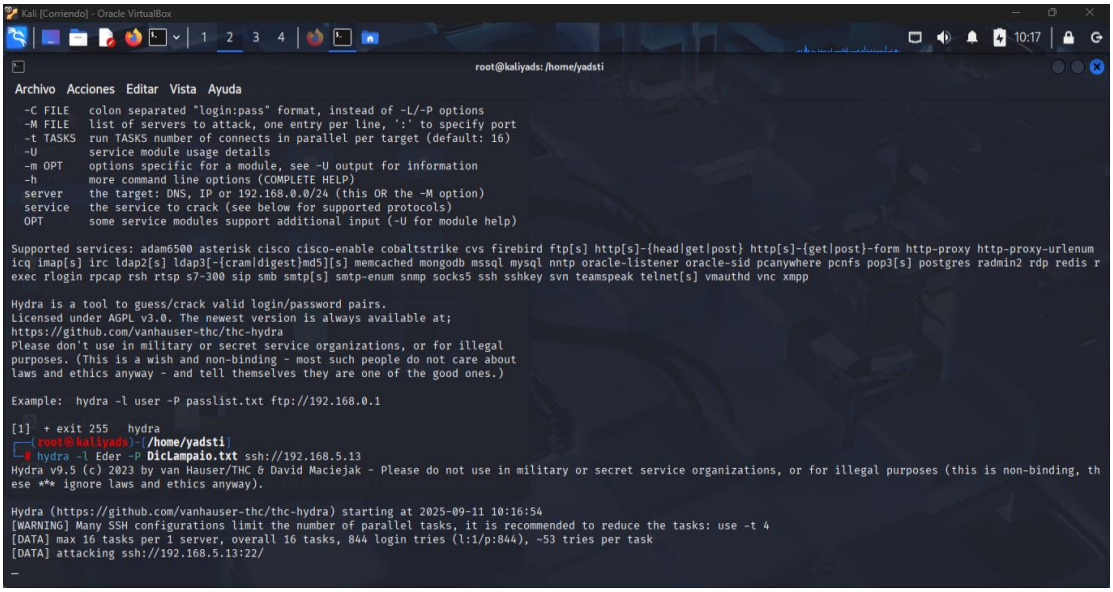
Ilustración 10 Diccionario creado



Fuerza bruta (Hydra)

Luego se utiliza el service Hydra para hacer una comparación de posibles usuarios y contraseñas en base al diccionario generado, con el usuario Eder no se obtiene contraseña.

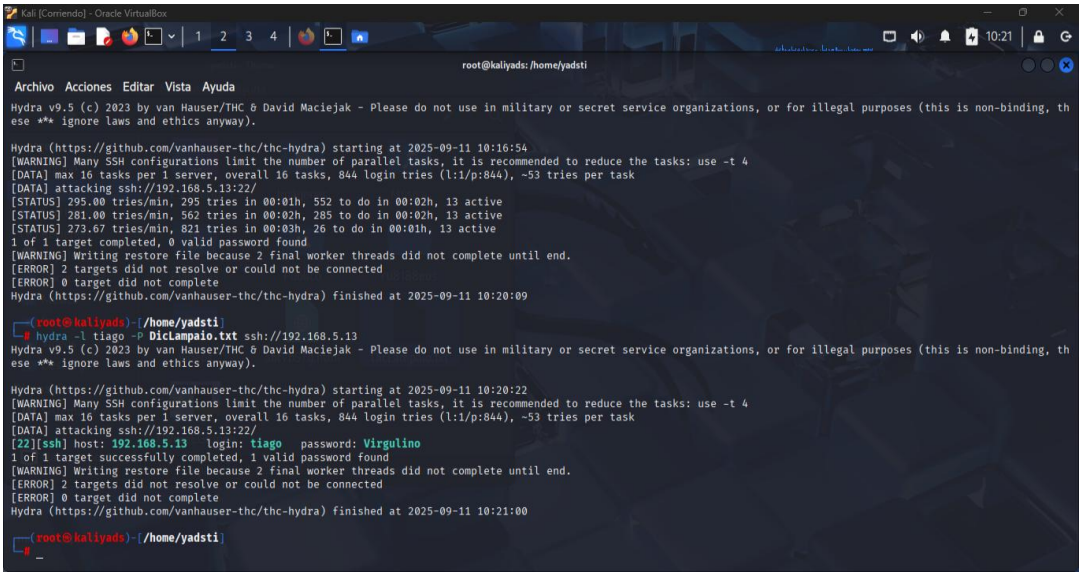
Ilustración 11 Hydra Eder



Se continua con tiago y se obtiene lo siguiente:

[22][ssh] host: 192.168.5.13 login: tiago password: Virgulino

Ilustración 12 Hydra tiago



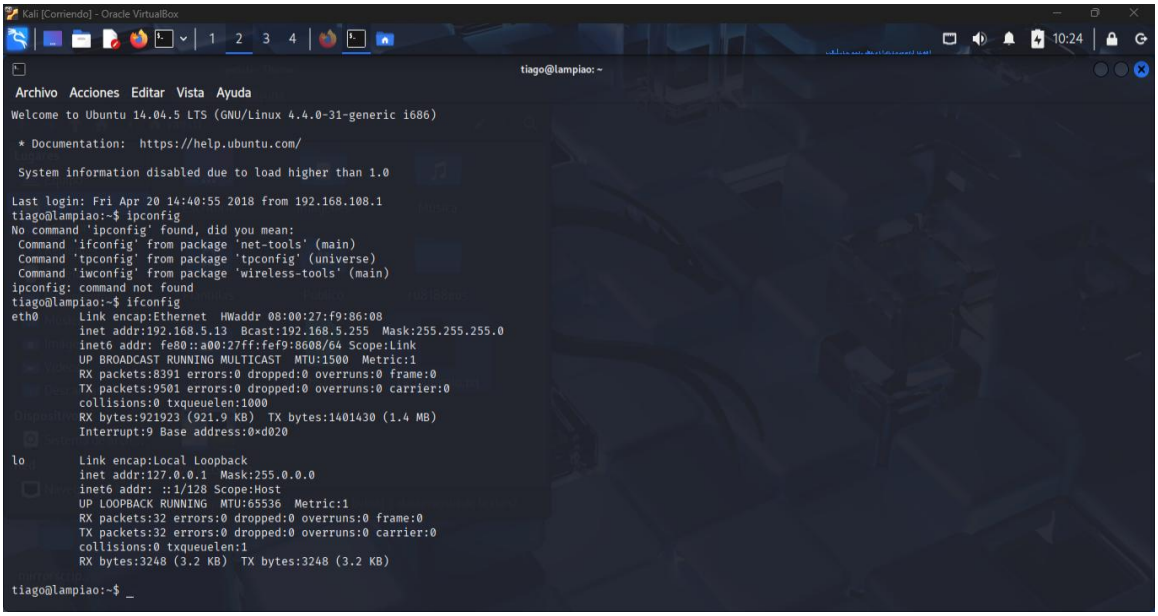
Prueba de credenciales y acceso SSH

Con esas credenciales se ingresa por SSH y se accede al sistema como se evidencia a continuación.

Ilustración 13 Ingreso SSH

Se verifica la dirección ip para confirmar que si es la de lampaio.

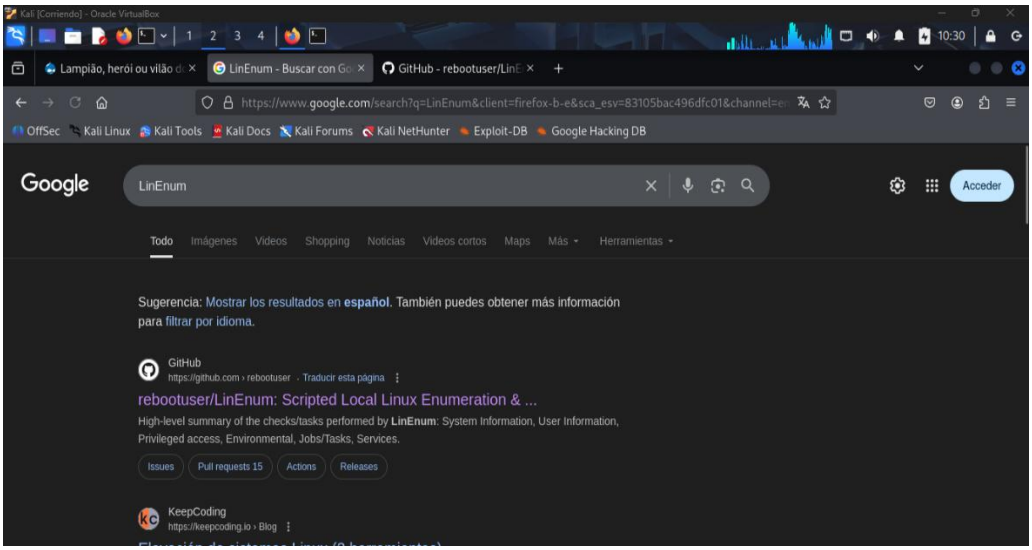
Ilustración 14 Confirmación ip acceso SSH



Herramienta LinEnum

Se buscó y clonó el repositorio de herramientas de enumeración (LinEnum) para automatizar la búsqueda para escalar privilegios.

Ilustración 15 Búsqueda LinEnum

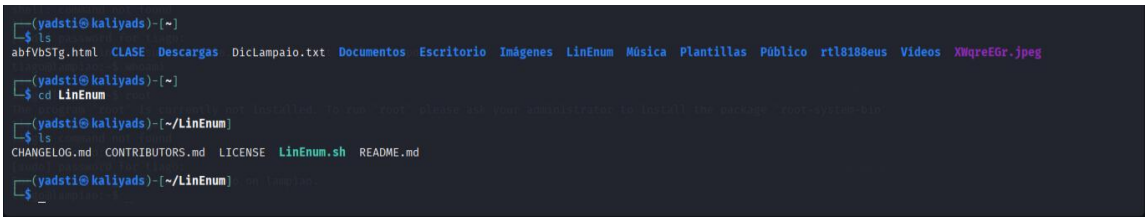


Se clona el repositorio, con el fin de tener el script de la herramienta.

Ilustración 16 Clonación de herramienta

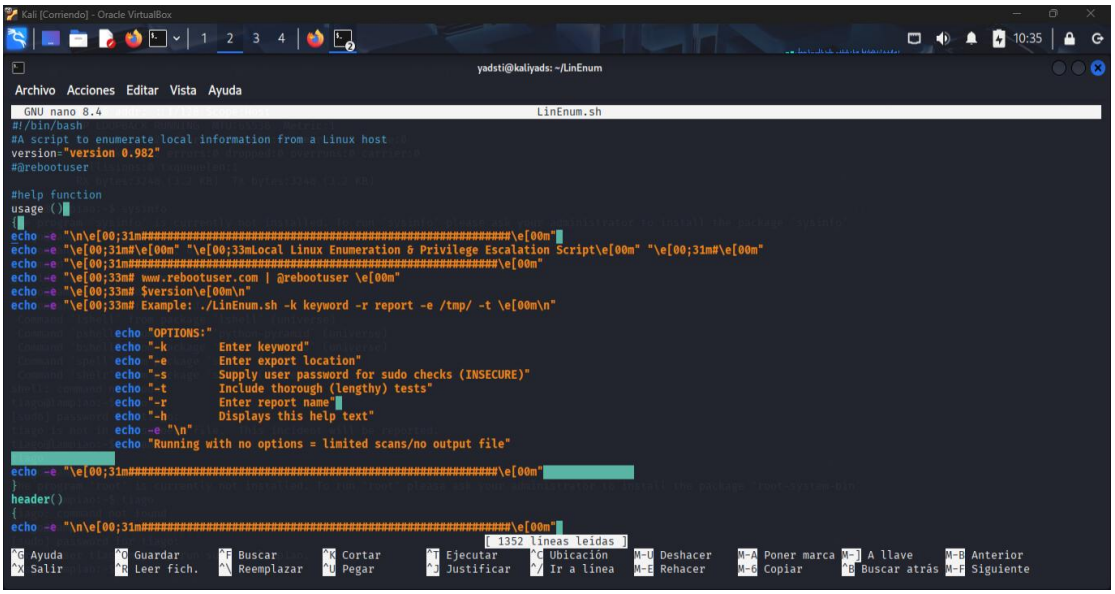
Una vez clonado se utiliza el comando ls para verificar que el repositorio se clonó satisfactoriamente y para conocer su ruta.

Ilustración 17 Ruta LinEnum



Se selecciona el directorio y se revisa el contenido del archivo LinEmun.sh que es el que contiene el script para revisar sus funciones y funcionamiento de este, además por si hay que hacer alguna modificación de algún parámetro.

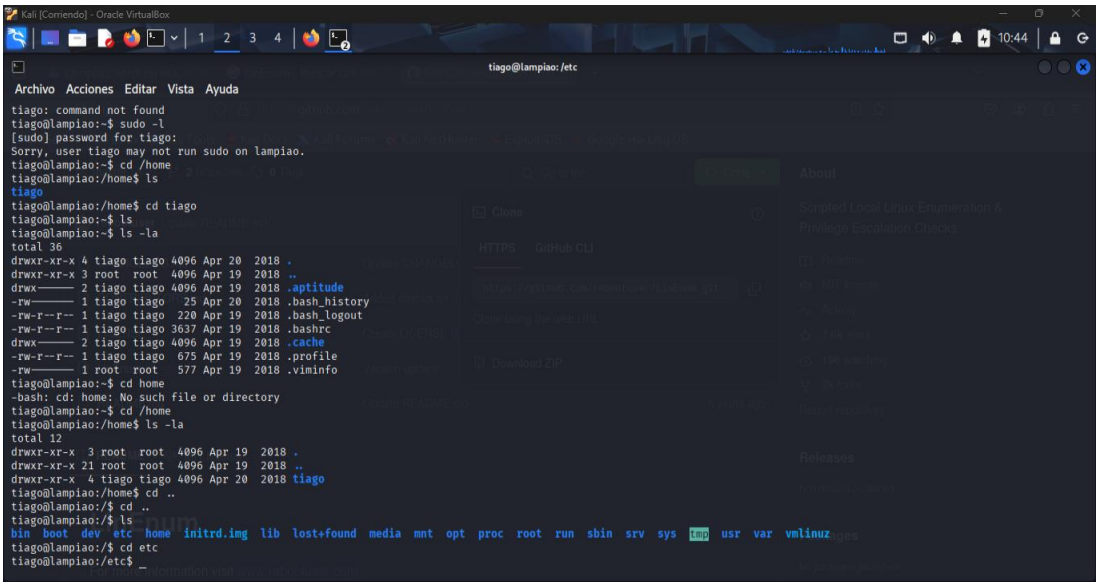
Ilustración 18 Inspección LinEnum



Escalada de privilegios

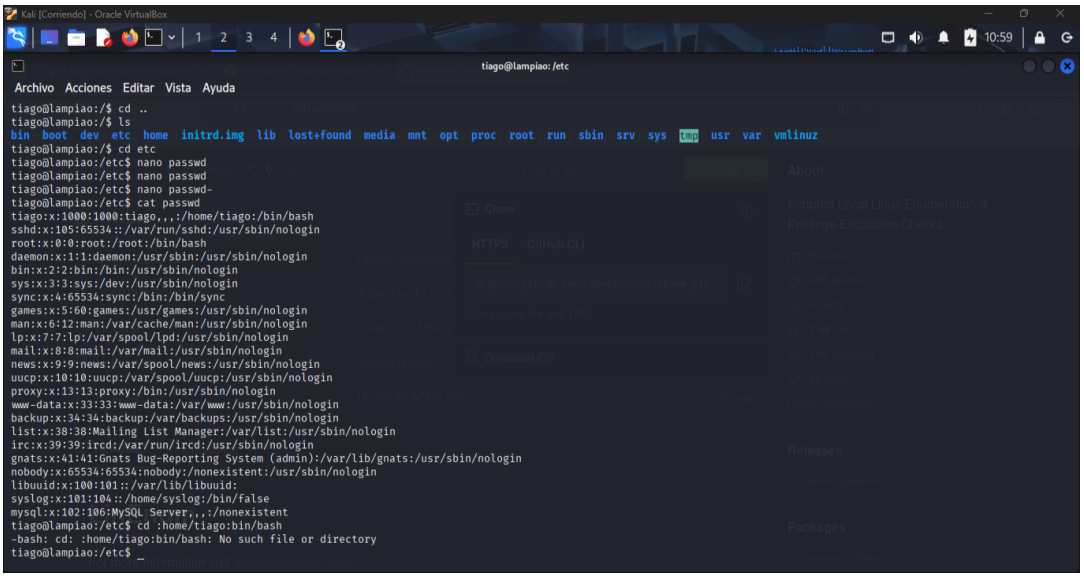
Luego se regresa a Lampaio para verificar la ruta del usuario creado y sus permisos.

Ilustración 19 Inspección de ruta de usuario



Se revisa el archivo etc/passwd con el fin de encontrar información que sea de ayuda.

Ilustración 20 Inspección archivo passwd

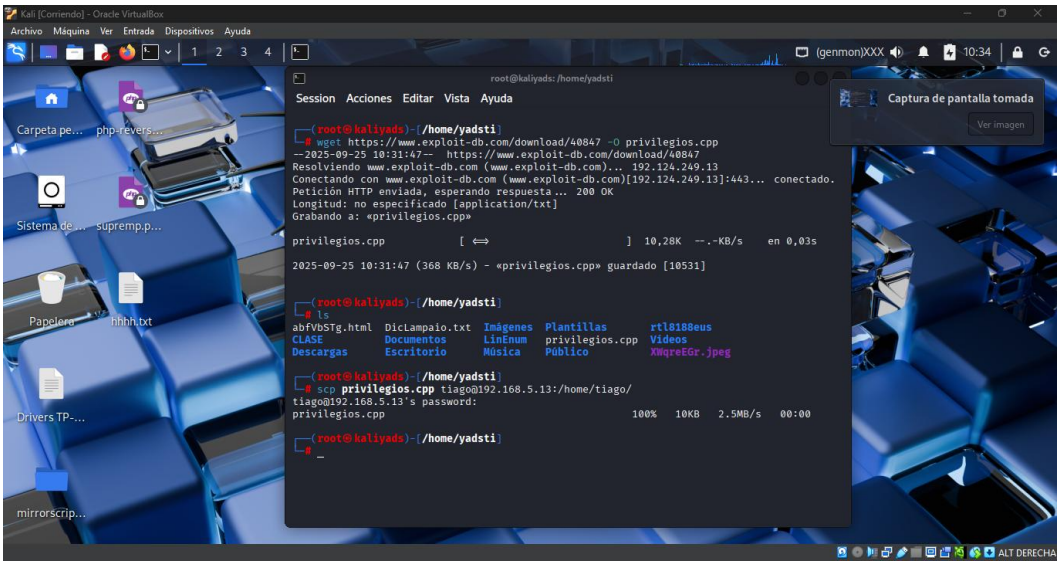


Una vez se conoce información de usuarios como Tiago, root, Daemon, entre otros se procede a descargar un exploit o herramienta que ayudará con la escalada de privilegios y permisos. Utilizando los siguientes comandos:

wget https://www.exploit-db.com/download/40847 -O privilegios.cpp

scp privilegios.cpp tiago@192.168.5.13:/home/tiago/ - se envía el archivo a lampaio

Ilustración 21 Descarga y envió de exploit a lampaio

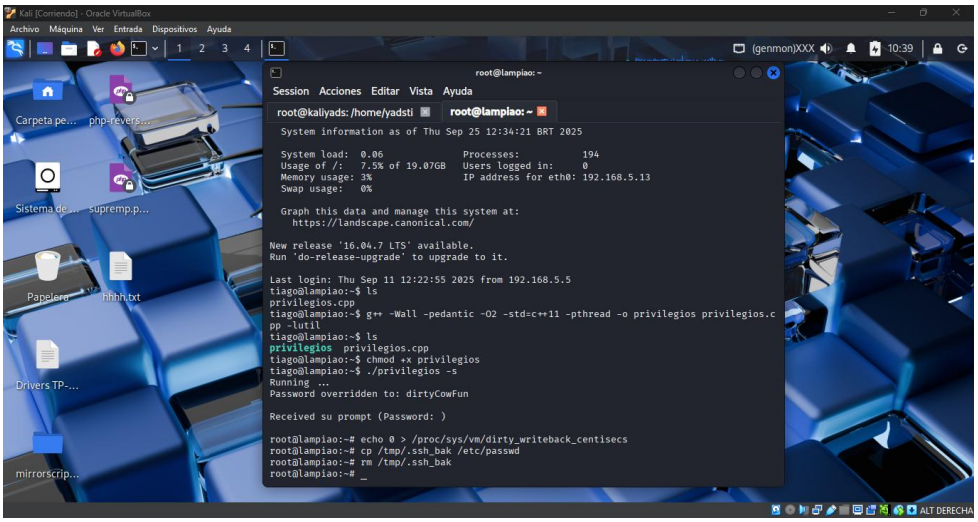


Luego se procede a enmascarar el ejecutable y adicionarle los permisos correspondientes, para posteriormente ejecutar el exploit que este contiene con el siguiente comando:

g++ -Wall -pedantic -O2 -std=c++11 -pthread -o privilegios privilegios.cpp -lutil

El exploit fue satisfactorio y ahora se opera dentro del sistema como usuario root.

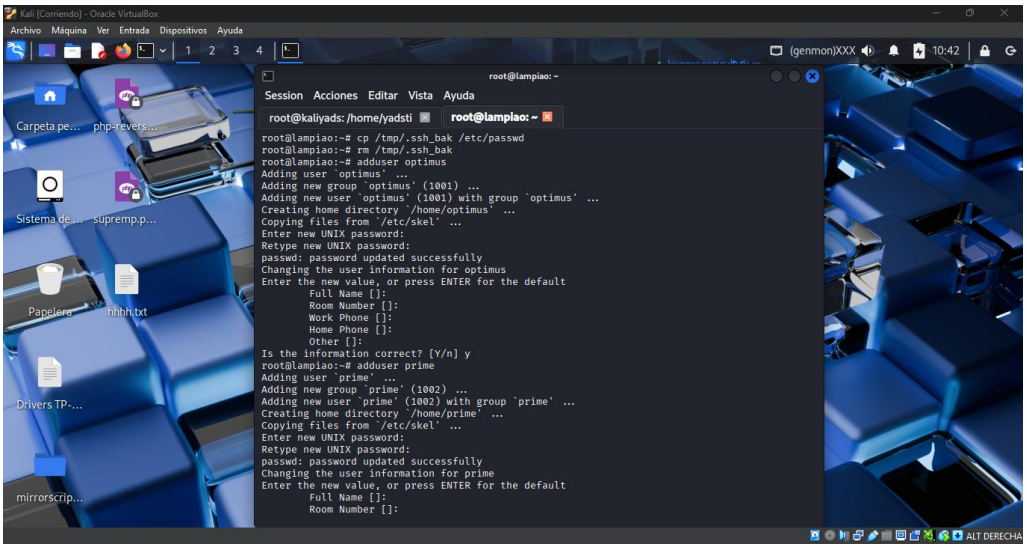
Ilustración 22 Escalada de privilegios



Creación de usuarios

Con privilegios de root se procede con la creación de dos usuarios. Usuario **optimus** y usuario **prime**.

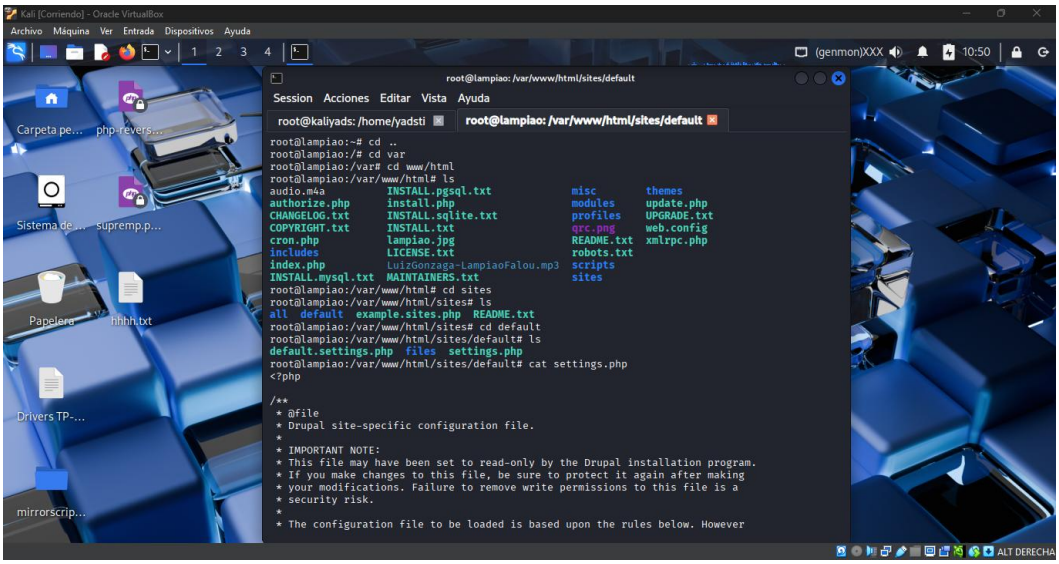
Ilustración 23 Creación de usuarios



Inspección de directorio sitio web

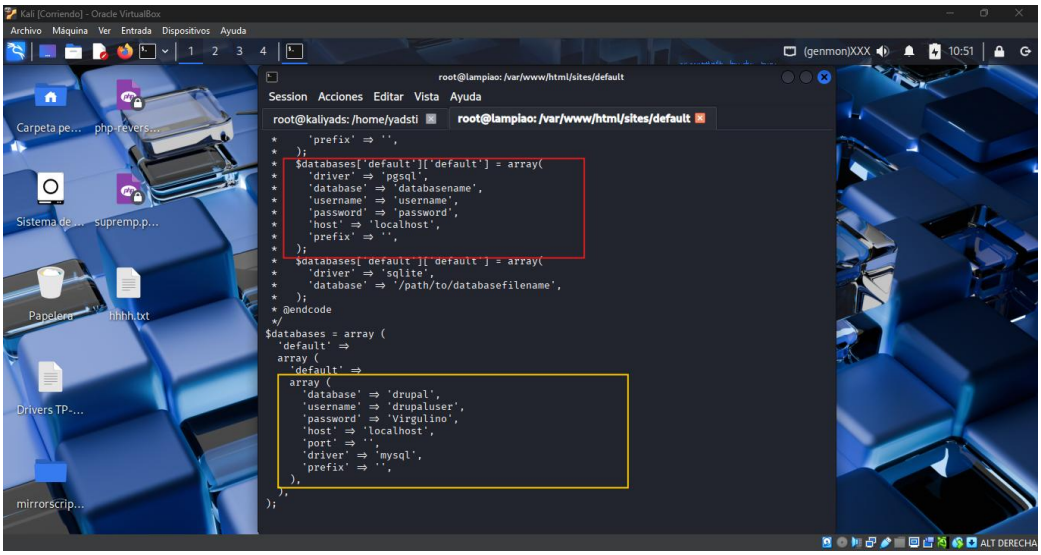
Luego de crear los usuarios, se procede a escalarle privilegios y permisos. Se procede a explorar el directorio donde está almacenado el sitio web con el fin de encontrar información que permita la creación de nuevos usuarios para el sitio, insertándolo en la base de datos. Se navega a **var/www/html/sites/default** y ahí encuentra el archivo **settings.php** el cual contiene información importante de la base de datos.

Ilustración 24 Inspección de directorio



En el recuadro rojo se encuentra la sintaxis o estructura que debería tener la configuración de conexión a la base de datos. Mientras que en el recuadro amarillo se encuentra la información real de la conexión a la base de datos.

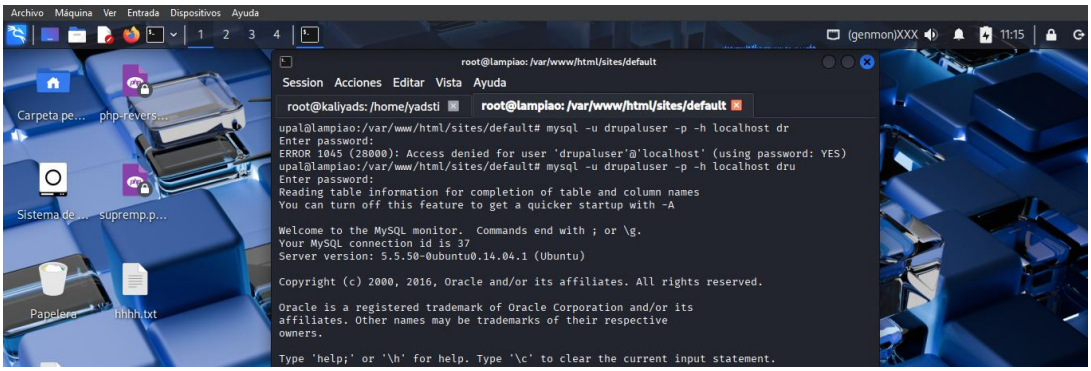
Ilustración 25 Revisión archivo settings



Teniendo esta información se observa que la base de datos está alojada en **MySQL**, la base de datos se llama **drupal**, el usuario es **drupaluser**, la contraseña es **Virgulino** y está en el **localhost**.

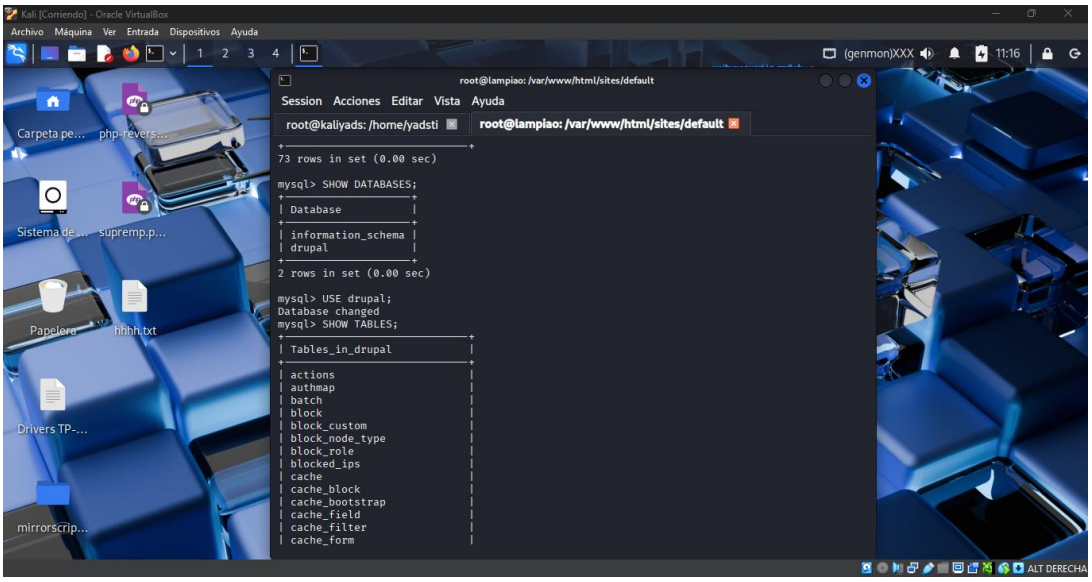
Con esta información se procede a iniciar sesión en MySQL para inspeccionar la base de datos y crear los usuarios.

Ilustración 26 Inicio de sesión MySQL



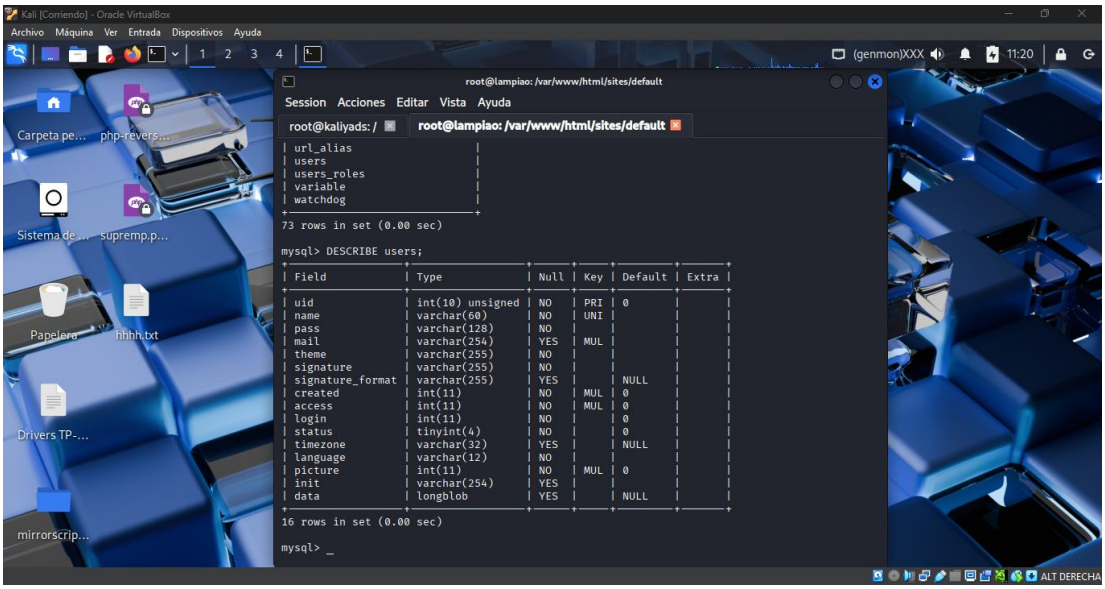
Se observa que hay dos bases de datos, la de MySQL por defecto y drupal. Se selecciona drupal y se revisan sus tablas.

Ilustración 27 Revisión de base de datos



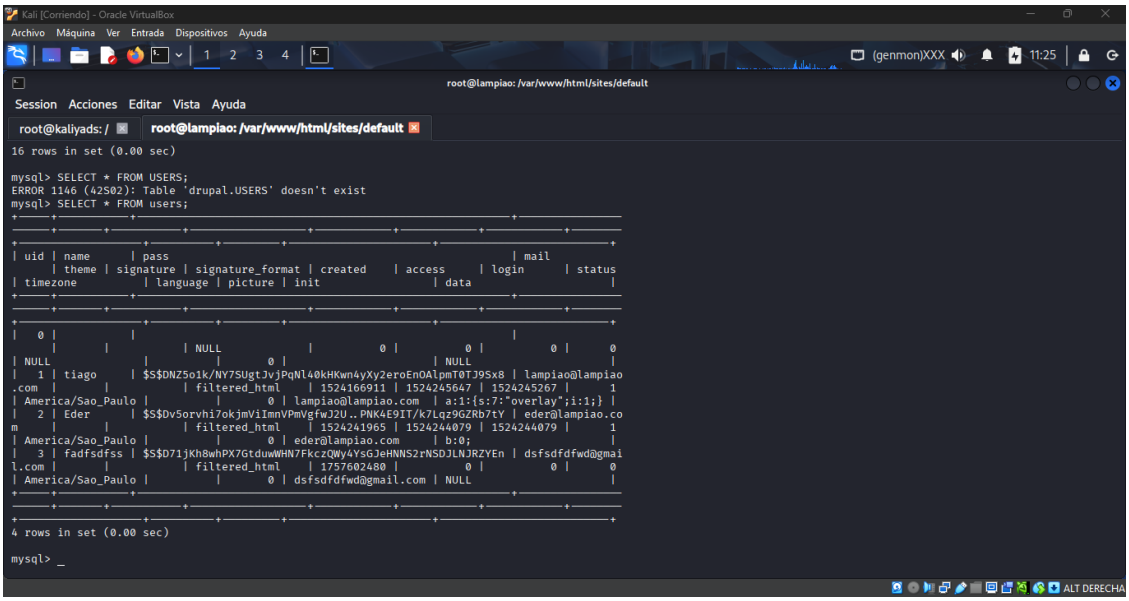
La tabla que interesa es **users**, se procede a describir su estructura para revisar que campos se necesitan para crear los usuarios.

Ilustración 28 Descripción tabla users



Luego se inspecciona para ver que hay en ella y se encuentran 4 registros, que son los usuarios que pueden ingresar al sitio.

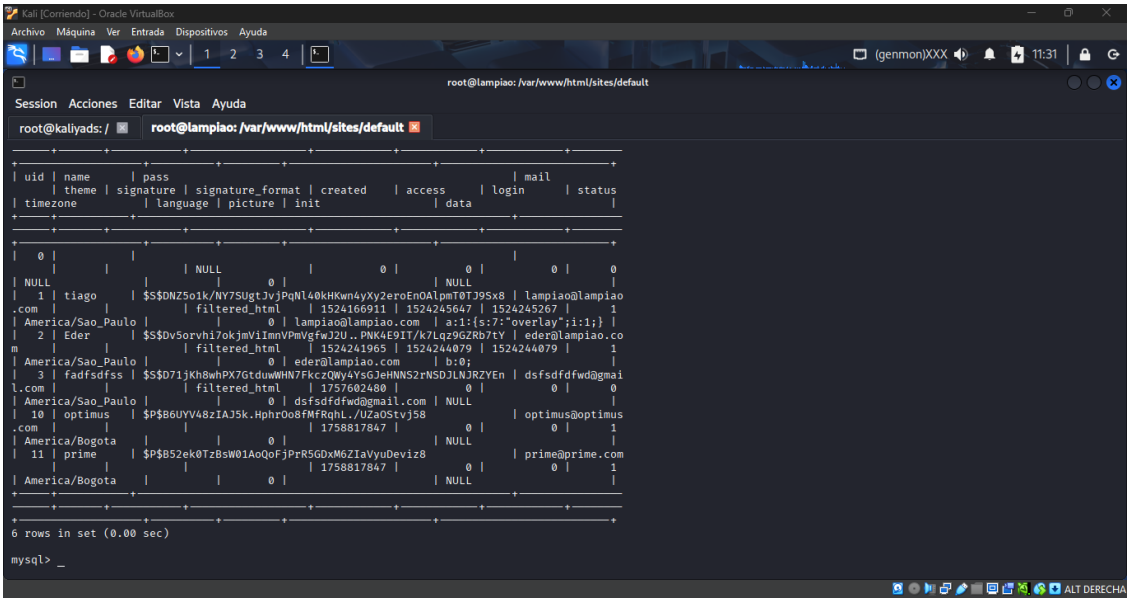
Ilustración 29 Usuarios existentes



Creación de usuarios

Se insertan los dos usuarios en la tabla.

Ilustración 30 Creación de usuarios



Ahora se procede a verificar que si se pueda iniciar sesión.

Ilustración 31 Inicio sesión optimus

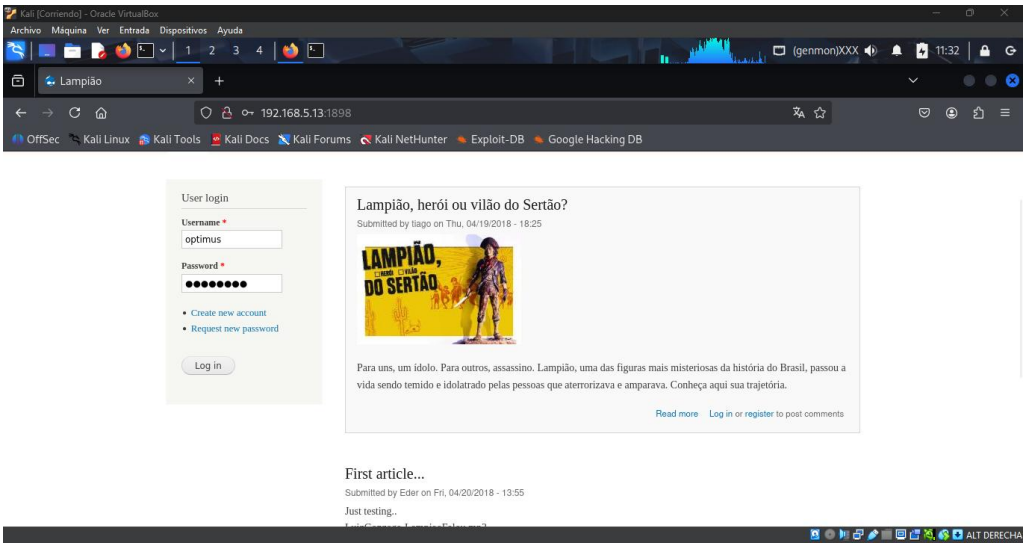


Ilustración 32 Inicio de sesión optimus exitoso

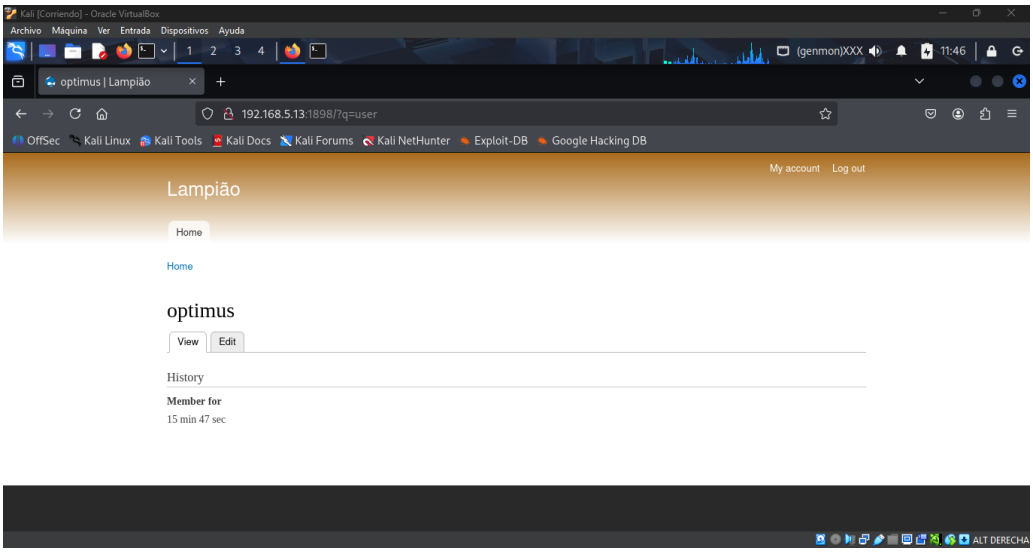


Ilustración 33 Comentario optimus

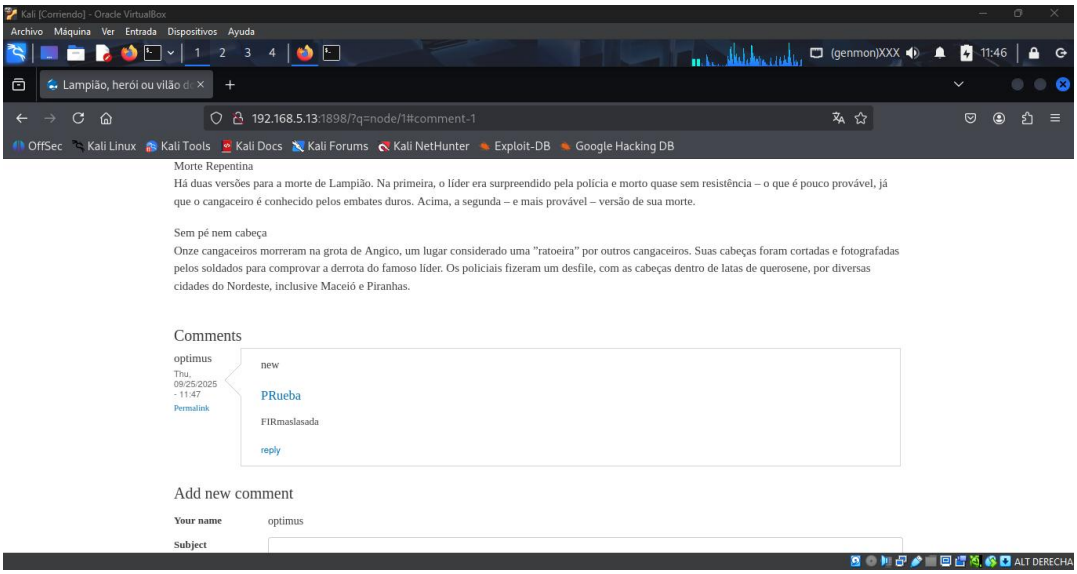


Ilustración 34 Inicio sesión prime

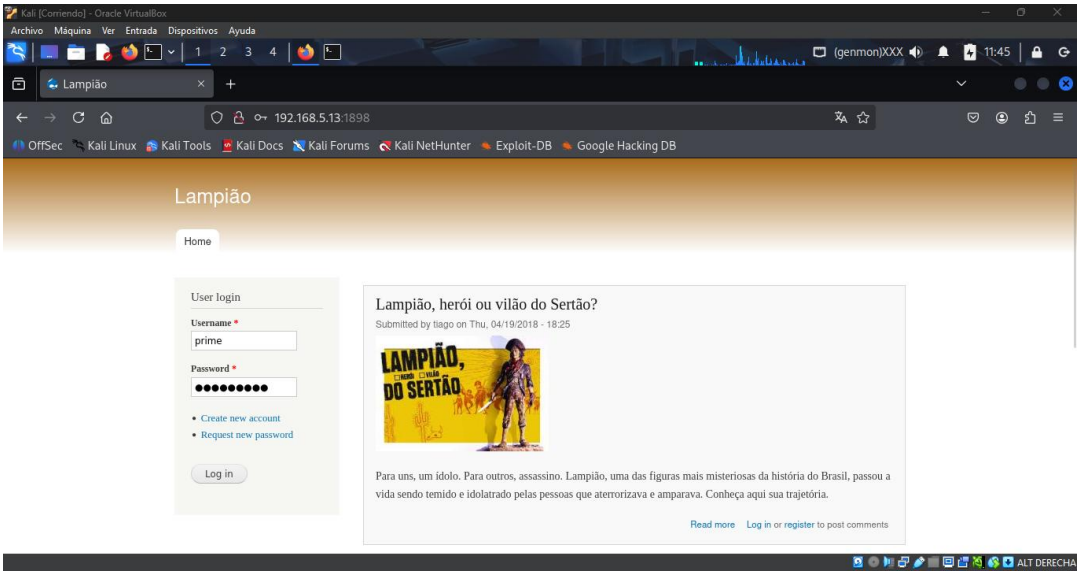


Ilustración 35 Inicio de sesión exitoso prime

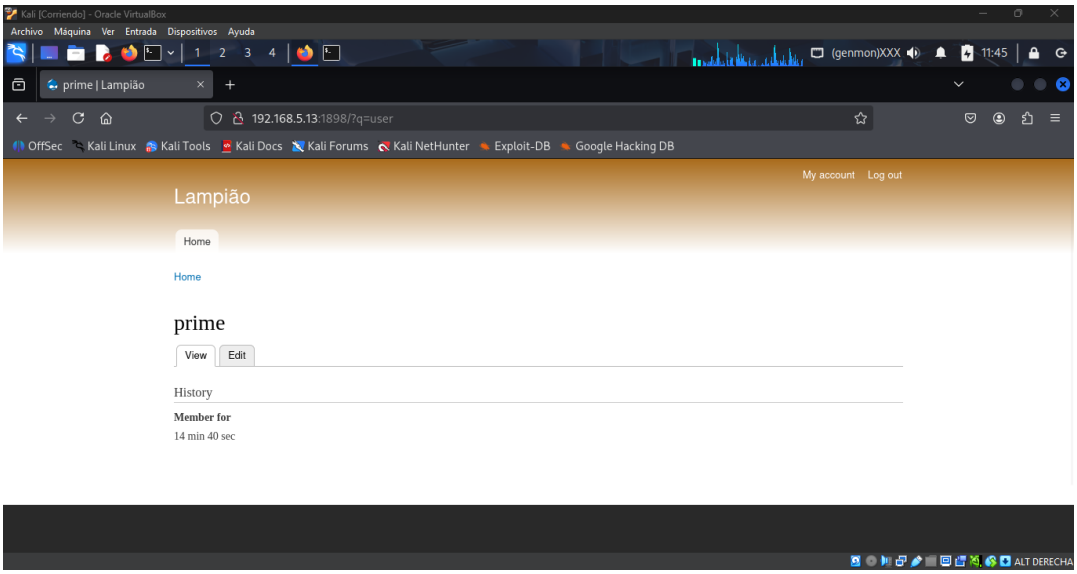
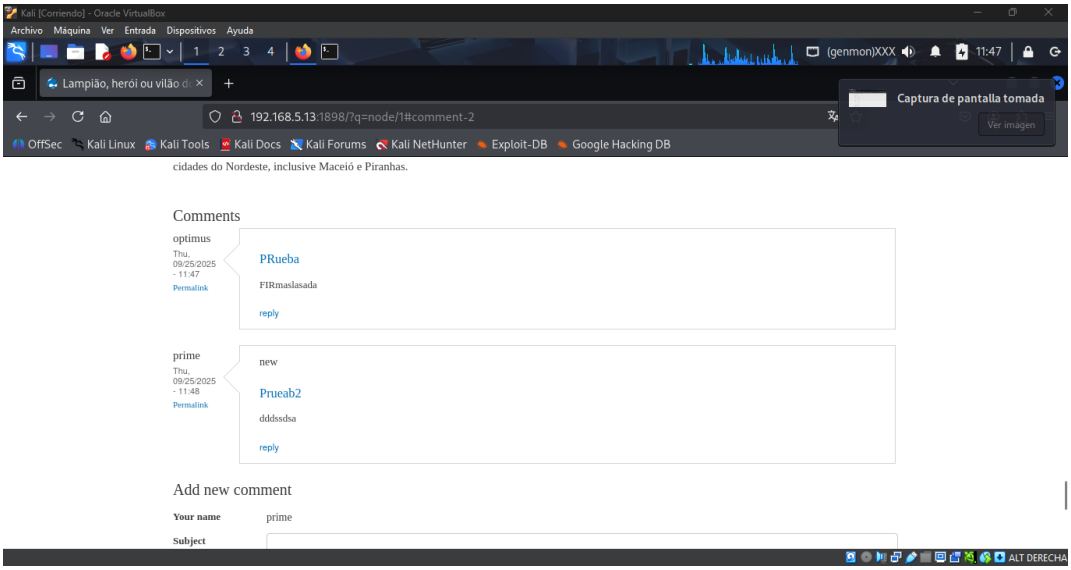


Ilustración 36 Comentario prime



Finalmente, el inicio de sesión es satisfactorio para los dos usuarios creados, adicionalmente se hacen comentarios en la publicación del sitio y como se evidencia los usuarios son publicados correctamente.

Conclusión

La práctica permitió aplicar un flujo completo de auditoría en un entorno controlado: reconocimiento, recolección de información, generación de diccionarios a partir de contenido real, ataques de fuerza bruta dirigidos, acceso inicial, enumeración local, y explotación para escalada de privilegios. El hallazgo principal es que configuraciones desactualizadas (servicios y kernels antiguos), combinadas con información pública en la web y credenciales predecibles, facilitan la intrusión y la elevación de privilegios.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*

netcat | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/netcat/

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos - ochobitshacenunbyte*. Ochobitshacenunbyte. https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.). https://es.linux-console.net/?p=20171