LABORATORIO #03

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

LABORATORIO #03

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Tabla de contenido

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Lista de ilustraciones

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Introducción

En este laboratorio se realiza el proceso de explotación desde la máquina atacante Kali hacia la máquina víctima lampaio. El propósito es identificar configuraciones inseguras que permitan realizar escalada privilegios y, navegar rutas seguras que permita crear dos nuevas cuentas de usuarios.

Alcance

El laboratorio abarca la identificación de posibles configuraciones inseguras que permitan escalada de privilegios en la víctima.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Objetivos

General: Comprender la utilidad de los procedimientos aplicados en el laboratorio para la identificación de vulnerabilidades en sistemas informáticos.

Específicos:

- Realizar ataque a lampaio
- Crear dos usuarios en la máquina vulnerable lampaio

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Planteamiento del problema

Se plantea la necesidad de acceder al sistema víctima lampaio y verificar si, partiendo de un acceso con SSH, con un usuario sin privilegios, es posible obtener los permisos necesarios para crear usuarios adicionales.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 DESARROLLO DEL PROBLEMA

1.1 Capítulo 1: Ataque a Lampaio

Se inicia el laboratorio poniendo en ejecución dos máquinas virtuales: **Kali Linux**, y la máquina objetivo **Lampaio.**

Ilustración 1Ejecución simultánea de Kali Linux y la máquina objetivo Lampaio

Se realizo un reconocimiento de servicios mediante la herramienta Nmap, dirigido a la dirección IP 100.10.2.14 que es la víctima.

```
└─# nmap -p 1-2000 100.10.2.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 02:26 -05
Nmap scan report for pool-100-10-2-14.prvdri.fios.verizon.net (100.10.2.14)
Host is up (0.00090s latency).
Not shown: 1997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port
MAC Address: 08:00:27:D8:84:F6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

Ilustración 2Resultado del escaneo de puertos con Nmap

El resultado del escaneo indicó la detección de tres puertos abiertos: el 22, asociado al servicio SSH; el 80, correspondiente al servicio HTTP; y el 1898.

Luego, se accedió a la dirección IP de la máquina objetivo mediante el navegador web desde Kali Linux. Como resultado, el servidor respondió mostrando la página principal alojada en el puerto 80.

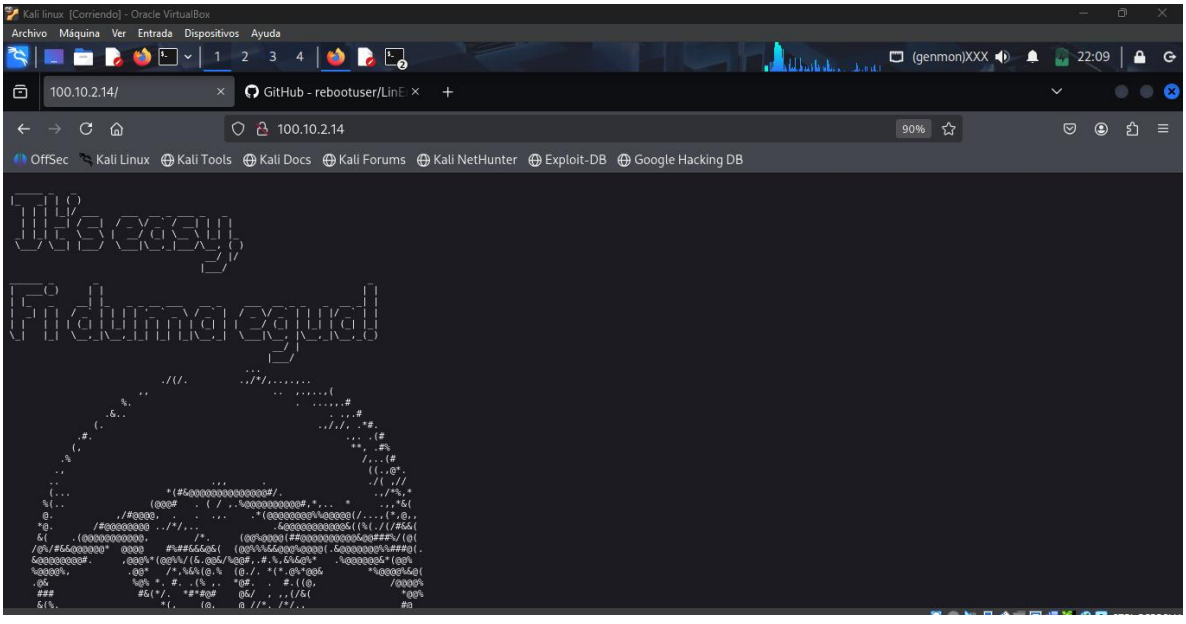


Ilustración 3Visualización de la página web de la máquina objetivo

Como se identificó durante el escaneo que el puerto 1898 se encontraba abierto y ofrecía un servicio HTTP basado en Apache, se procedió a acceder a la dirección IP de la máquina objetivo especificando dicho puerto en el navegador.

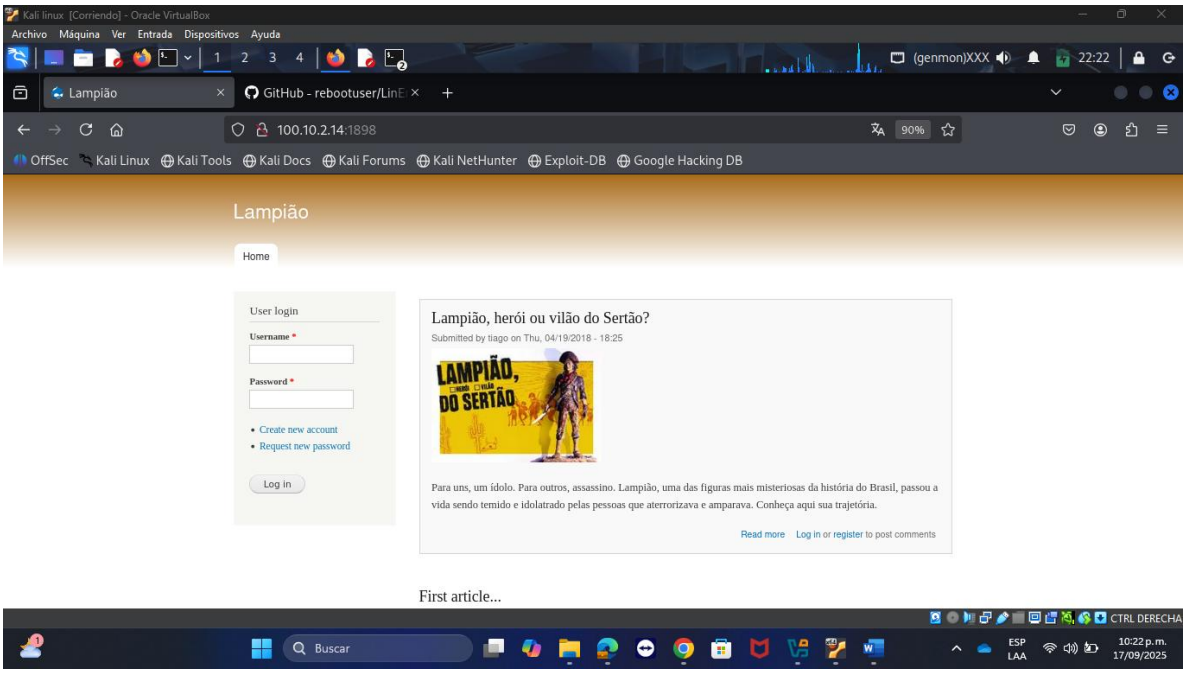


Ilustración 4 Acceso al servicio HTTP en el puerto 1898

Como resultado, se visualizó la interfaz principal de un sitio web denominado **Lampião**, que incluye un formulario de inicio de sesión y contenido informativo.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Se identificaron nombres y palabras clave que podrían corresponder a usuarios válidos del sistema

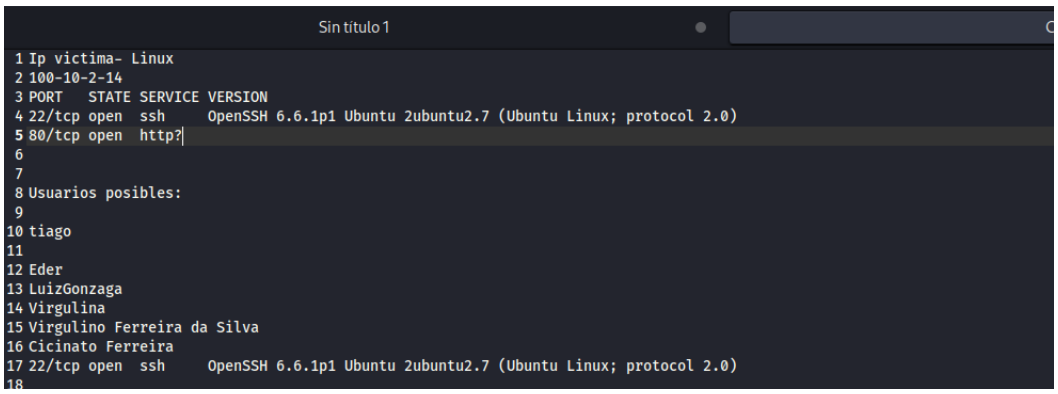


Ilustración 5 Listado de usuarios potenciales

Se ejecutó una herramienta de generación de diccionarios sobre la dirección http://100.10.2.14:1898/ con el objetivo de extraer términos y palabras clave presentes en la página web. La salida se guardó en el archivo DicLampiao.txt.

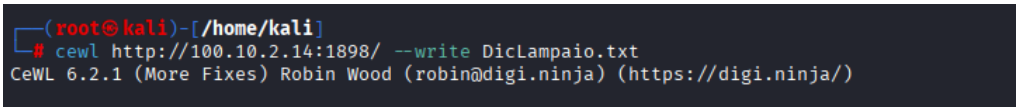


Ilustración 6Generación de un diccionario de palabras a partir del contenido del sitio web

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Se verificó la cantidad de entradas generadas en el diccionario DicLampiao.txt mediante el comando wc -l. El resultado indicó un total de **848 líneas**, lo que corresponde al número de palabras recolectadas desde el sitio web.

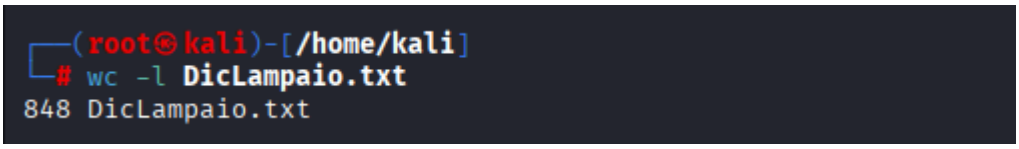


Ilustración 7Conteo de palabras en el archivo DicLampiao.txt

Se ejecutó la herramienta Hydra contra el servicio SSH de la máquina objetivo (100.10.2.14) empleando como usuario inicial el nombre tiago(obtenido de la página web) y el diccionario DicLampiao.txt

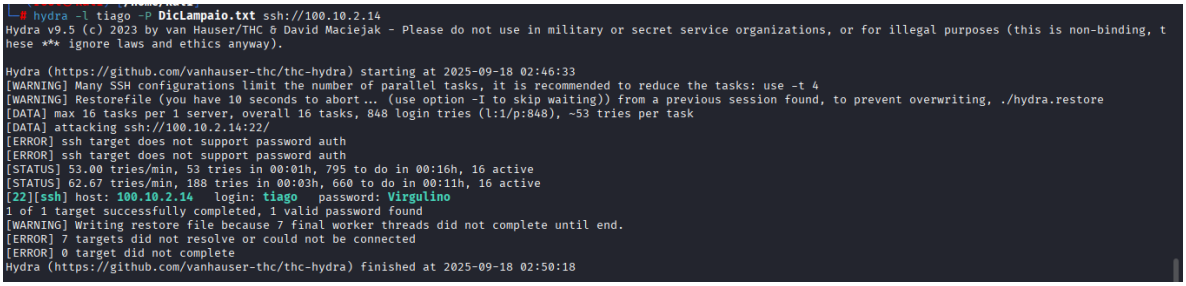


Ilustración 8Ejecución de Hydra

El proceso permitió identificar credenciales válidas de acceso, correspondiendo al usuario **tiago** con la contraseña **Virgulino**

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Se estableció una sesión SSH hacia la máquina objetivo (100.10.2.14) empleando credenciales previamente obtenidas durante la ejecución de hydra.

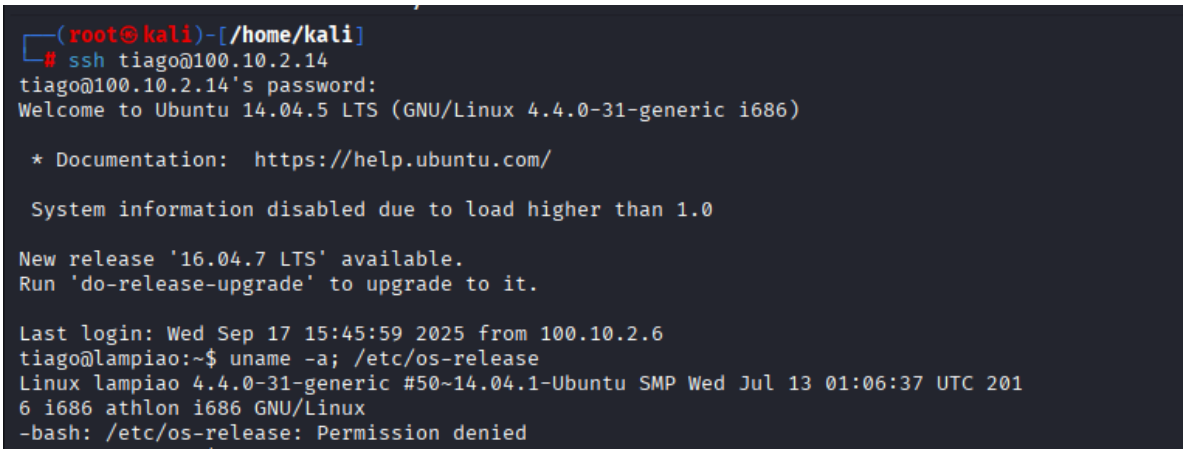


Ilustración 9Acceso SSH exitoso

Una vez establecida la conexión con la máquina objetivo, se intentó comprobar la posibilidad de ejecutar comandos con privilegios administrativos a través de la utilidad **sudo**. El sistema indicó que el usuario autenticado no posee permisos para realizar operaciones con elevación de privilegios, lo cual no permitió la creación de nuevos usuarios en esta fase del laboratorio.

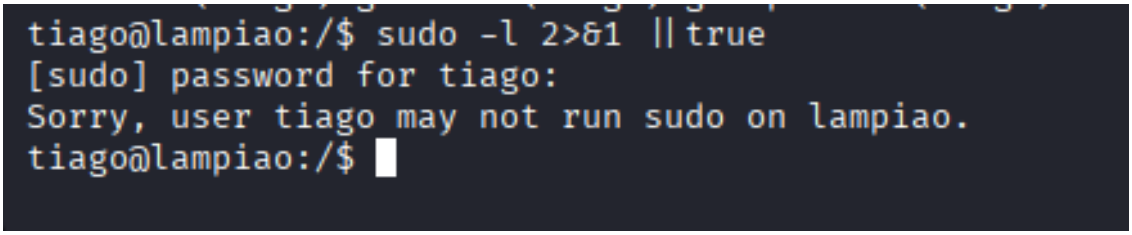


Ilustración 10Comprobación de privilegios

2 Problemas encontrados

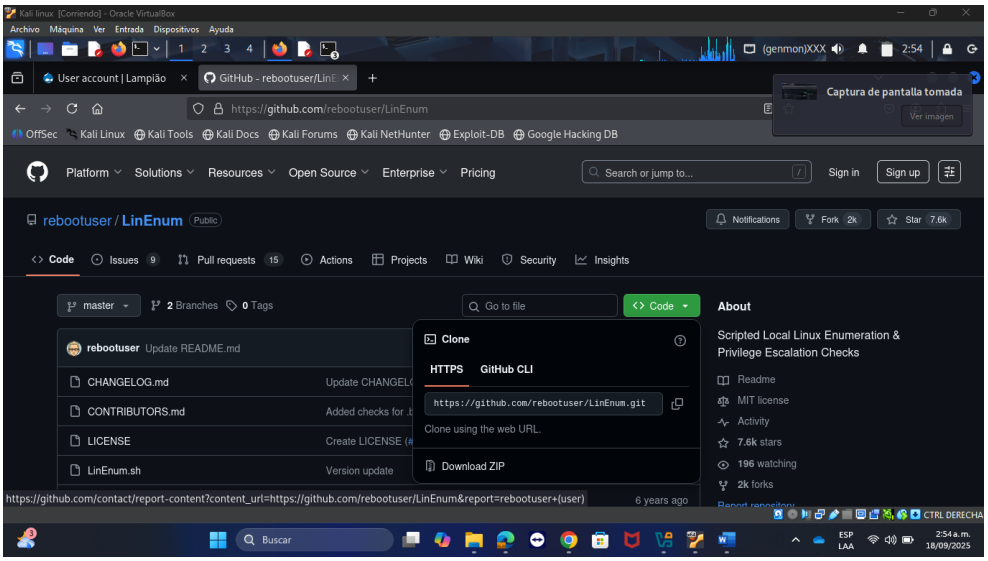
El usuario obtenido no disponía de privilegios sudo, impidiendo crear usuarios directamente.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

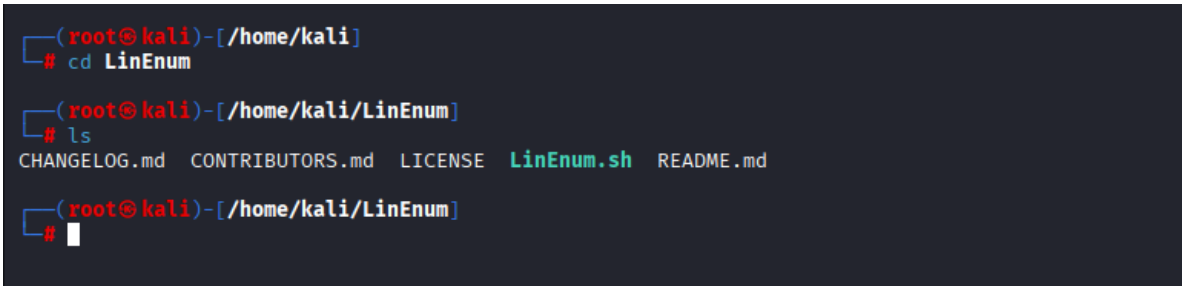
3 Soluciones de los problemas

Se llevaron a cabo pruebas utilizando el repositorio **LinEnum** con el fin de enumerar posibles vectores de escalamiento de privilegios; sin embargo, hasta el momento no se ha logrado identificar una solución efectiva.

Se busco el repositorio en internet:



Se clono en Kali Linux:



4 Recomendaciones

Se recomienda documentar cada paso del proceso para evitar confusiones y verificar cuidadosamente las rutas y directorios antes de ejecutar cualquier comando. Asimismo, es fundamental prestar atención a la correcta escritura de los comandos, ya que los errores tipográficos pueden ocasionar fallos en la ejecución. También resulta conveniente investigar y familiarizarse con los comandos básicos de navegación en la terminal, como salir, retroceder o cambiar de directorio.

5 Conclusiones

Hasta el momento no se han alcanzado los objetivos planteados; sin embargo, se continúan explorando alternativas que permitan cumplirlos, a la vez que se adquiere experiencia valiosa durante el desarrollo del laboratorio.

6 Glosario

- Kali **Linux:** Distribución de Linux orientada a pruebas de seguridad y hacking ético, con múltiples herramientas de análisis y explotación.

- Nmap**:** Herramienta utilizada para el escaneo de puertos y detección de servicios en una red.

- SSH **(Secure Shell):** Protocolo seguro de comunicación remota que permite administrar sistemas mediante línea de comandos.

- HTTP **(HyperText Transfer Protocol):** Protocolo de comunicación que permite la transferencia de páginas web.

- Hydra**:** Aplicación diseñada para realizar ataques de fuerza bruta a servicios de autenticación.

- Diccionario **de contraseñas:** Archivo de texto que contiene múltiples combinaciones de palabras utilizadas para probar credenciales en ataques de autenticación.

- Privilegios **sudo:** Permisos especiales en sistemas Linux que permiten ejecutar comandos con privilegios de administrador.

- Escalamiento **de privilegios:** Técnica empleada para obtener mayores permisos en un sistema tras un acceso inicial.

- LinEnum**:** Script de automatización que enumera configuraciones y posibles vulnerabilidades en sistemas Linux para facilitar la búsqueda de vectores de escalamiento de privilegios.

- Hacking **ético:** Práctica controlada y legal que busca identificar vulnerabilidades en sistemas informáticos con fines educativos o de seguridad.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

7 Bibliografía

IONOS, E. e. (11 de 2023 de Agosto). *ionos.Comando de Linux wc*. Obtenido de ionos.com: https://www.ionos.com/es-us/digitalguide/servidores/configuracion/comando-de-linux-wc/

phoenixnap.com. (4 de Mayo de 2022). Obtenido de phoenixnap.Comando nc: https://phoenixnap-com.translate.goog/kb/nc-command?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc