INFORME DE LABORATORIO 01

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

INFORME DE LABORATORIO 01

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 6

2. OBJETIVOS 7

2.1 Objetivo general 7

2.2 Objetivos específicos 7

3. ALCANCE 8

4. LAMPIAO 9

4.1 Iniciar máquina Lampião 9

4.2 Escaneo de red con el comando Nmap 9

4.3 Ver IP de máquina atacante (Kali Linux) 10

4.4 Escaneo de puertos específicos 11

4.5 Acceso al servicio web (puerto 80) 11

4.6 Acceso a Lampião (puerto 1898) 12

4.7 Página de registro de Lampião 12

4.8 Escaneo avanzado de SSH 13

4.9 Inicio de Metasploit 13

4.10 Lista de módulos de Metasploit 14

4.11 Generación de diccionario con CeWL 14

4.12 Verificación del diccionario 15

4.13 Uso de Hydra para fuerza bruta en SSH 15

4.14 Intento de login en Lampião con credenciales 16

4.15 Conexión SSH exitosa 17

4.16 Verificación de red 18

4.17 Búsqueda de LinEnum en Google 18

4.18 Página de GitHub de LinEnum 19
4.19 Clonación de LinEnum 19
4.20 Navegación y preparación de LinEnum 19
4.21 Enumeración manual del sistema 20
4.22 Visualización del archivo /etc/passwd 21
5. PROBLEMAS ENCONTRADOS 22
6. CONCLUSIÓN 23
7. BIBLIOGRAFIA 24

TABLA DE ILUSTRACIONES

Ilustración 1. Inicio de la máquina Lampião 9
Ilustración 2. Escaneo de red con Nmap 10
Ilustración 3. Verificación de IP local 10
Ilustración 4. Escaneo de puertos específicos 11
Ilustración 5. Acceso al servicio web (puerto 80) 11
Ilustración 6. Acceso a Lampião (puerto 1898) 12
Ilustración 7. Página de registro de Lampião 12
Ilustración 8. Escaneo avanzado de SSH 13
Ilustración 9. Inicio de Metasploit 13
Ilustración 10. Lista de módulos de Metasploit 14
Ilustración 11. Generación de diccionario con CeWL 14
Ilustración 12. Verificación del diccionario 15
Ilustración 13. Validar el contenido del diccionario. 15
Ilustración 14. Uso del comando Hydra 16
Ilustración 15. Intento de login en Lampião con credenciales 16
Ilustración 16. Error de login en Lampião 17
Ilustración 17. Conexión SSH exitosa 17
Ilustración 18. Verificación de red 18
Ilustración 19. Búsqueda de LinEnum en Google 18
Ilustración 20. Página de GitHub de LinEnum 19
Ilustración 21. Clonación de LinEnum 19
Ilustración 22. Navegación y preparación de LinEnum 20
Ilustración 23. Archivo LinEnum 20
Ilustración 24. Enumeración manual del sistema 21
Ilustración 25. Visualización del archivo /etc/passwd 21

1. INTRODUCCIÓN

El presente informe de laboratorio tiene como propósito documentar las prácticas realizadas en el entorno de seguridad informática con la máquina virtual Lampião. A través de diferentes fases de exploración, análisis y explotación de vulnerabilidades, se buscó afianzar los conocimientos adquiridos en la asignatura de Seguridad Informática y Auditoría de Redes, aplicando herramientas como Nmap, Hydra, CeWL, Metasploit y LinEnum.

Este ejercicio se desarrolló en un entorno controlado y académico, lo cual permitió identificar y comprender los riesgos que representan los servicios mal configurados, así como la importancia de las contraseñas seguras y los procesos de escalamiento de privilegios.

2. OBJETIVOS

2.1 Objetivo general

Aprender técnicas básicas de seguridad informática mediante la práctica con la máquina virtual Lampião.

2.2 Objetivos específicos

- Reconocer los servicios activos en la máquina Lampião usando herramientas de escaneo de red.
- Identificar puntos débiles en el sistema mediante análisis de puertos y servicios.
- Practicar el uso de herramientas éticas de hacking como Nmap, Hydra y CeWL.
- Comprender la importancia de las contraseñas seguras mediante ataques de diccionario.
- Crear dos usuarios dentro del sistema como evidencia de la administración total conseguida.

3. ALCANCE

El alcance de este laboratorio se limitó a el reconocimiento de servicios y puertos activos en la máquina Lampião, la generación y verificación de diccionarios personalizados para ataques de fuerza bruta, el acceso inicial al sistema a través del protocolo SSH, la utilización de scripts de enumeración para análisis de configuraciones y usuarios, y la exploración de vulnerabilidades del kernel mediante intentos de explotación con DirtyCow. Todas las actividades se realizaron con fines académicos.

4. LAMPIAO

4.1 Iniciar máquina Lampião

Se muestra la consola de la máquina virtual Lampião (Ubuntu 14.04.5) iniciándose, esperando el login. El propósito es confirmar que la máquina está corriendo.

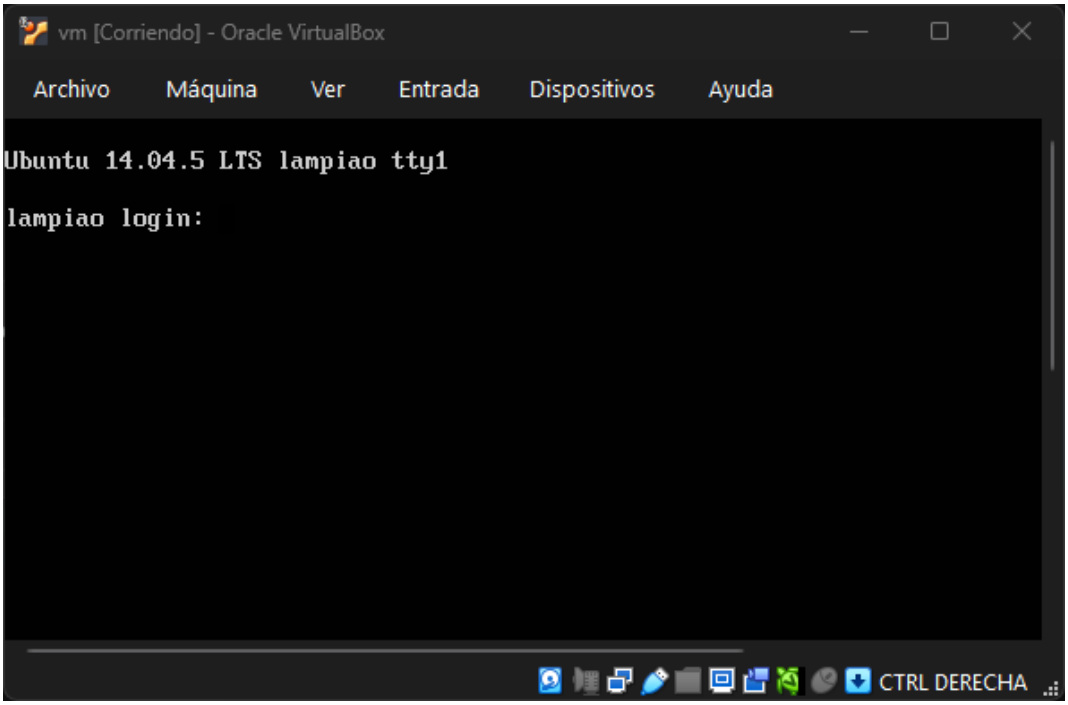


Ilustración 1. Inicio de la máquina Lampião

4.2 Escaneo de red con el comando Nmap

Escaneo de toda la red para descubrir hosts activos y servicios. Se identifica la IP 192.168.10.7 con puertos abiertos (SSH en 22 y HTTP en 80).

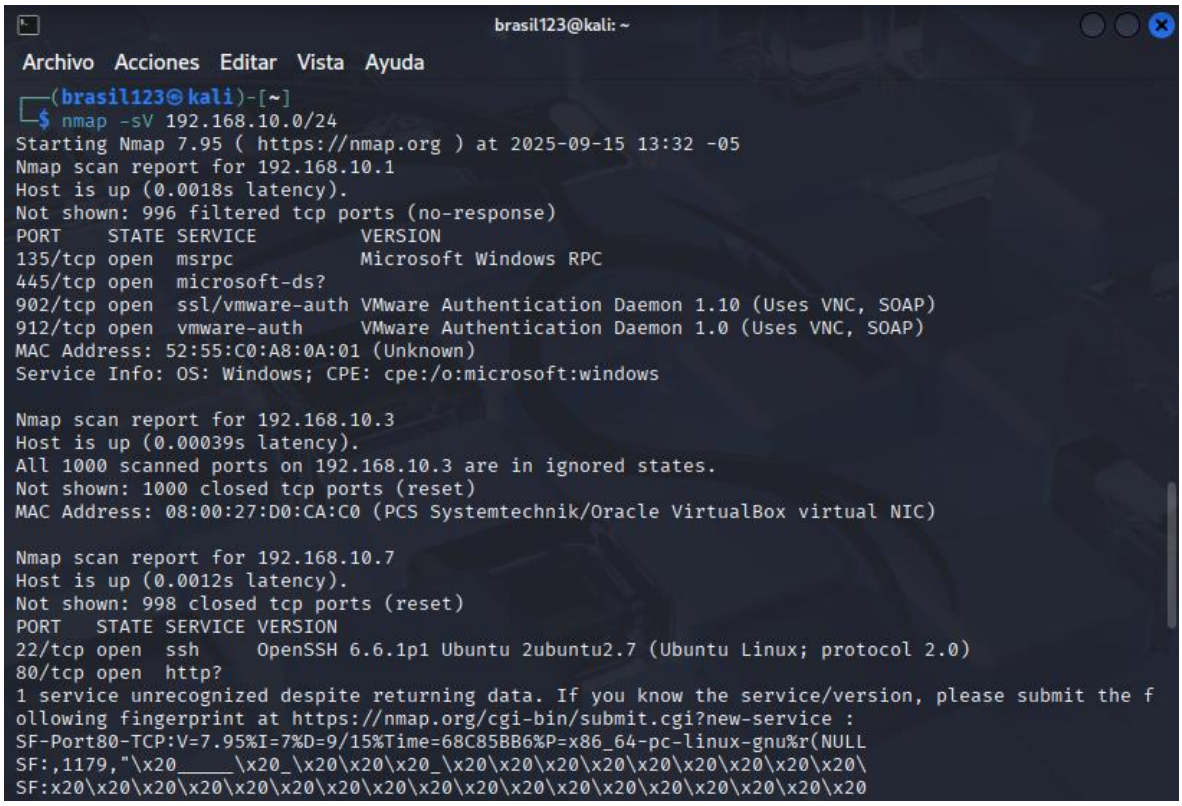


Ilustración 2. Escaneo de red con Nmap

4.3 Ver IP de máquina atacante (Kali Linux)

Mediante el comando **ifconfig** se verifica la configuración de red de la máquina atacante (Kali Linux), confirmando que tiene la dirección IP 192.168.10.6.

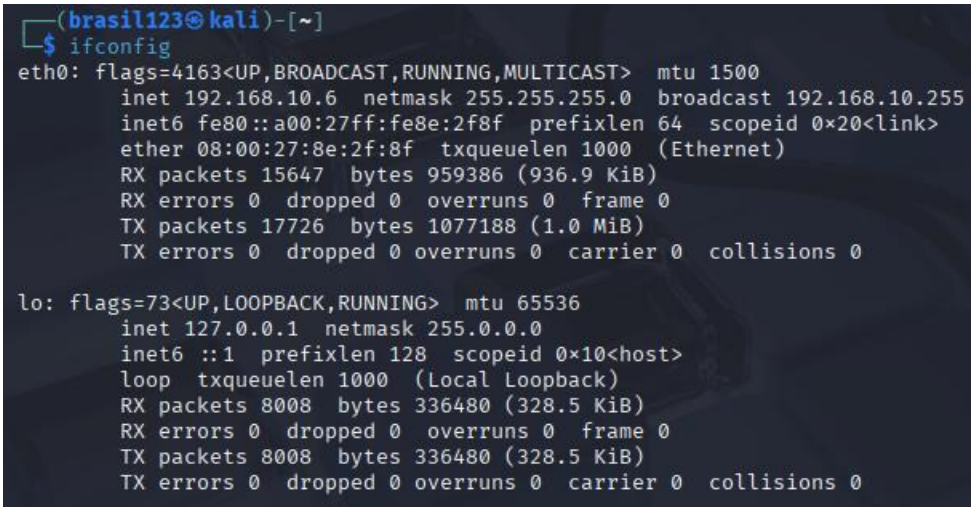


Ilustración 3. Verificación de IP local

4.4 Escaneo de puertos específicos

Un escaneo más específico con **nmap -p 1-2000** revela tres puertos abiertos: 22 (SSH), 80 (HTTP) y el puerto 1898, que posteriormente se identificará como un servicio HTTP adicional.

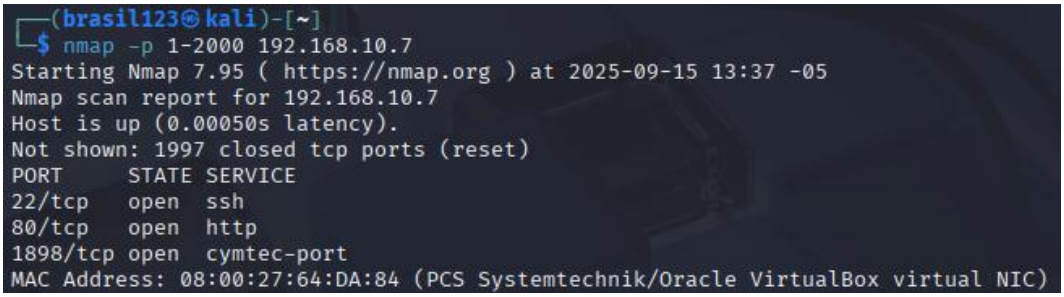


Ilustración 4. Escaneo de puertos específicos

4.5 Acceso al servicio web (puerto 80)

Acceso mediante navegador web al servicio HTTP del puerto 80, se visita **http://192.168.10.7** en el navegador. Muestra una página genérica.

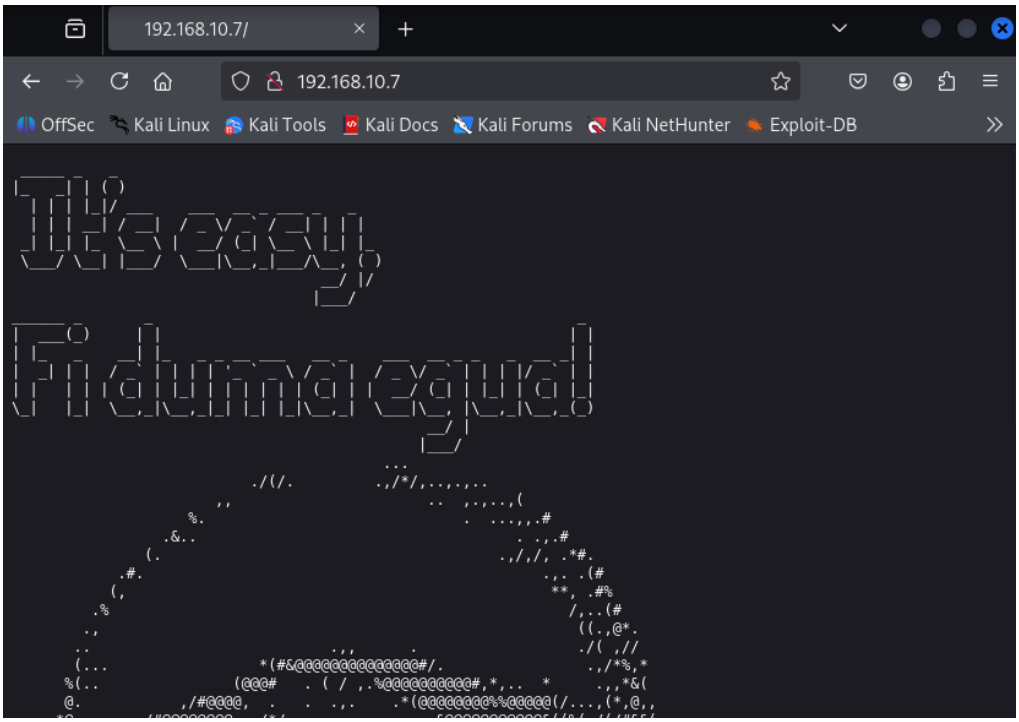


Ilustración 5. Acceso al servicio web (puerto 80)

4.6 Acceso a Lampião (puerto 1898)

Se visita **http://192.168.10.7:1898.** Se identifica el sitio de Lampião con un artículo publicado por el usuario tiago.

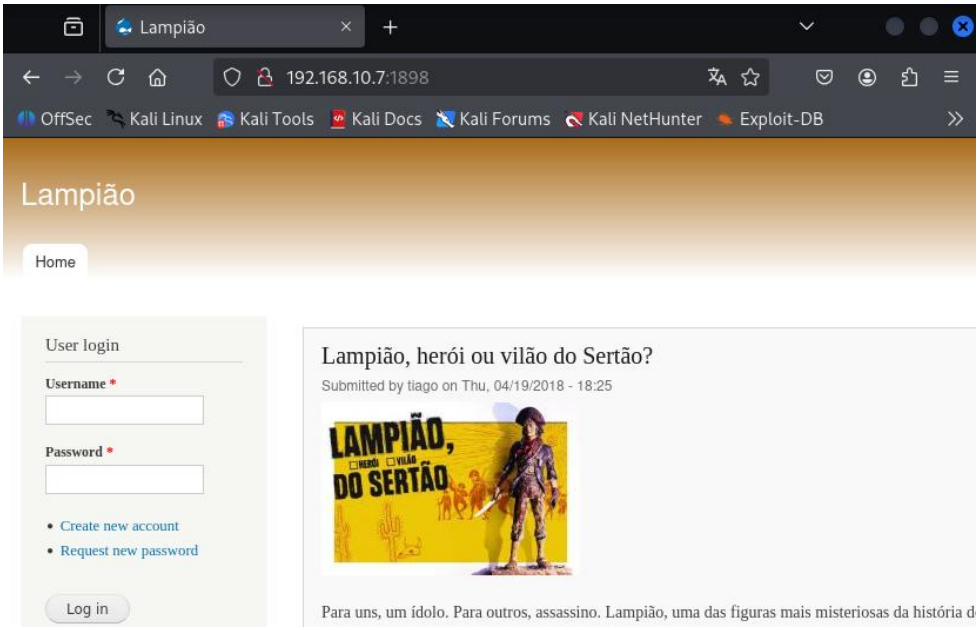


Ilustración 6. Acceso a Lampião (puerto 1898)

4.7 Página de registro de Lampião

Se intenta crear una cuenta, pero requiere aprobación del administrador.

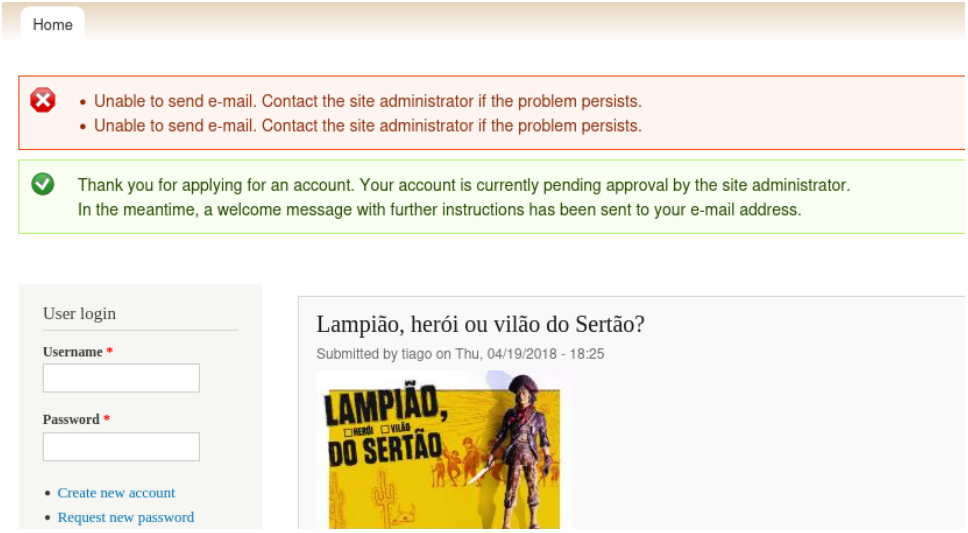


Ilustración 7. Página de registro de Lampião

4.8 Escaneo avanzado de SSH

Escaneo avanzado con nmap -A -sC específico sobre el puerto SSH (22), obteniendo información detallada de versiones (OpenSSH 6.6.1).

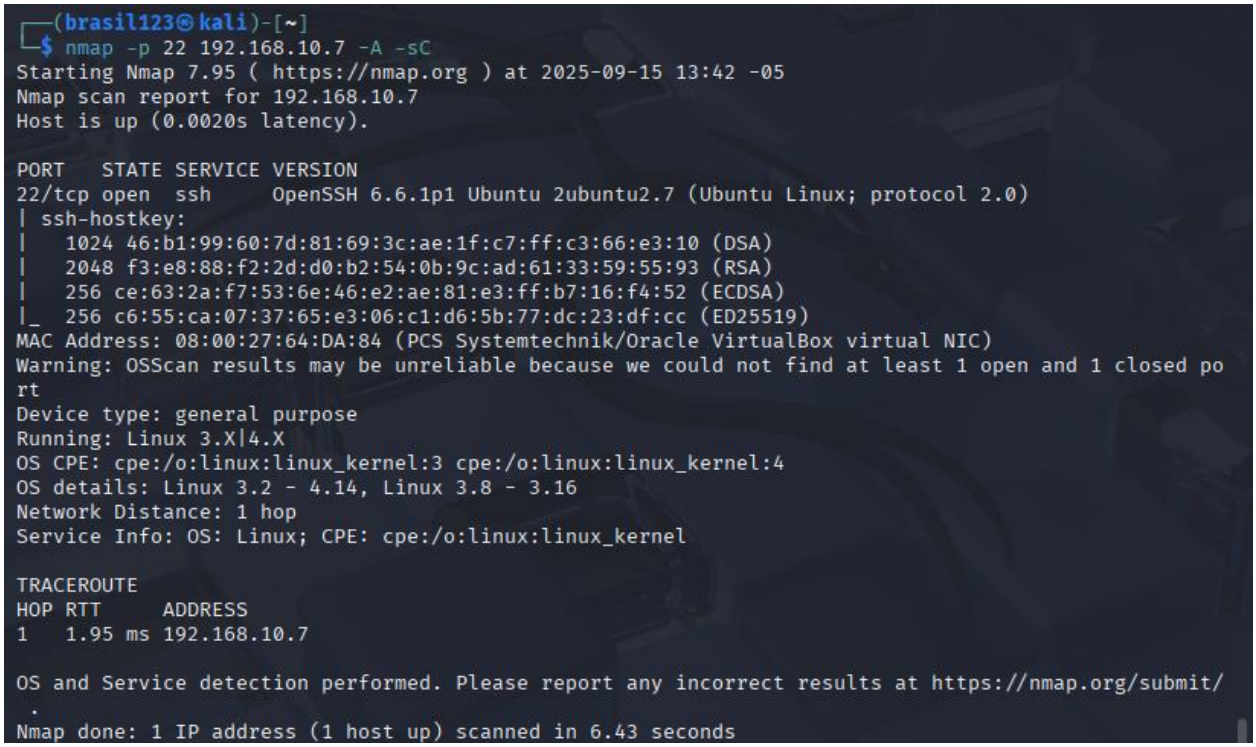


Ilustración 8. Escaneo avanzado de SSH

4.9 Inicio de Metasploit

Se inicia sesión como superusuario en Kali con **sudo su** y se ejecuta el framework de explotación Metasploit mediante el comando **msfconsole**.

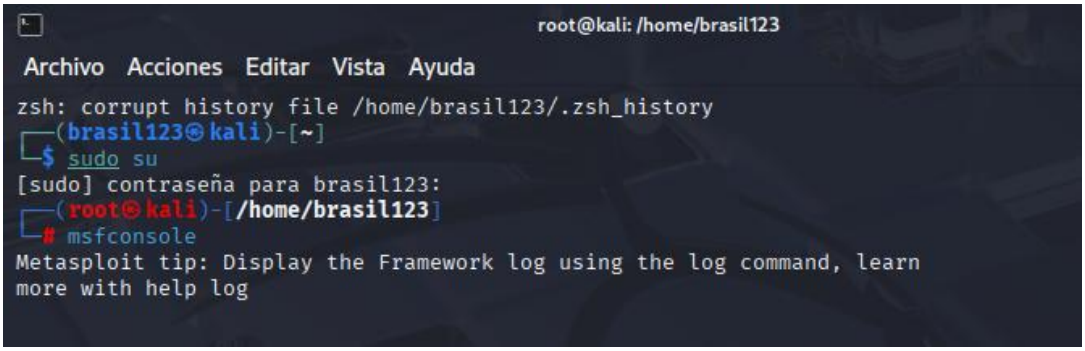


Ilustración 9. Inicio de Metasploit

4.10 Lista de módulos de Metasploit

Navegación por la interfaz de Metasploit, mostrando diversos módulos de post-explotación y exploits auxiliares disponibles para su uso.

Ilustración 10. Lista de módulos de Metasploit

4.11 Generación de diccionario con CeWL

Ejecución del comando **ceWL http://192.168.10.7:1898/ --write DicLampiao.txt** para generar un diccionario personalizado basado en palabras extraídas del contenido del sitio web de Lampião.

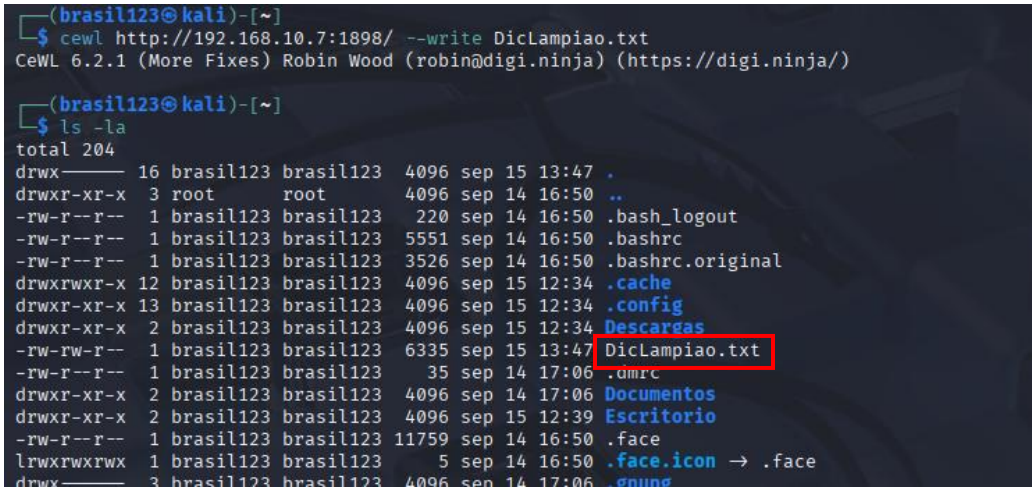


Ilustración 11. Generación de diccionario con CeWL

4.12 Verificación del diccionario

Verificación exitosa del archivo de diccionario generado (DicLampiao.txt), confirmando que contiene 844 palabras extraídas del sitio.

Ilustración 12. Verificación del diccionario

Se visualizan las primeras palabras que contiene el diccionario.

Ilustración 13. Validar el contenido del diccionario.

4.13 Uso de Hydra para fuerza bruta en SSH

Ataque de fuerza bruta con el comando **hydra -l tiago -P DicLampiao.txt ssh://192.168.10.7** que resulta en el descubrimiento exitoso de la contraseña **"Virgulino"** para el usuario **"tiago"** por SSH.

```
┌──(root㉿kali)-[/home/brasil123]
└─# hydra -l tiago -P DicLampiao.txt ssh://192.168.10.7
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2025-09-15 13:56:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.168.10.7:22/
[22][ssh] host: 192.168.10.7   login: tiago   password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 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 2025-09-15 13:56:53
```

Ilustración 14. Uso del comando Hydra

4.14 Intento de login en Lampião con credenciales

Se intenta logear en Lampião con el usuario **tiago** y la contraseña **Virgulino**, pero falla.

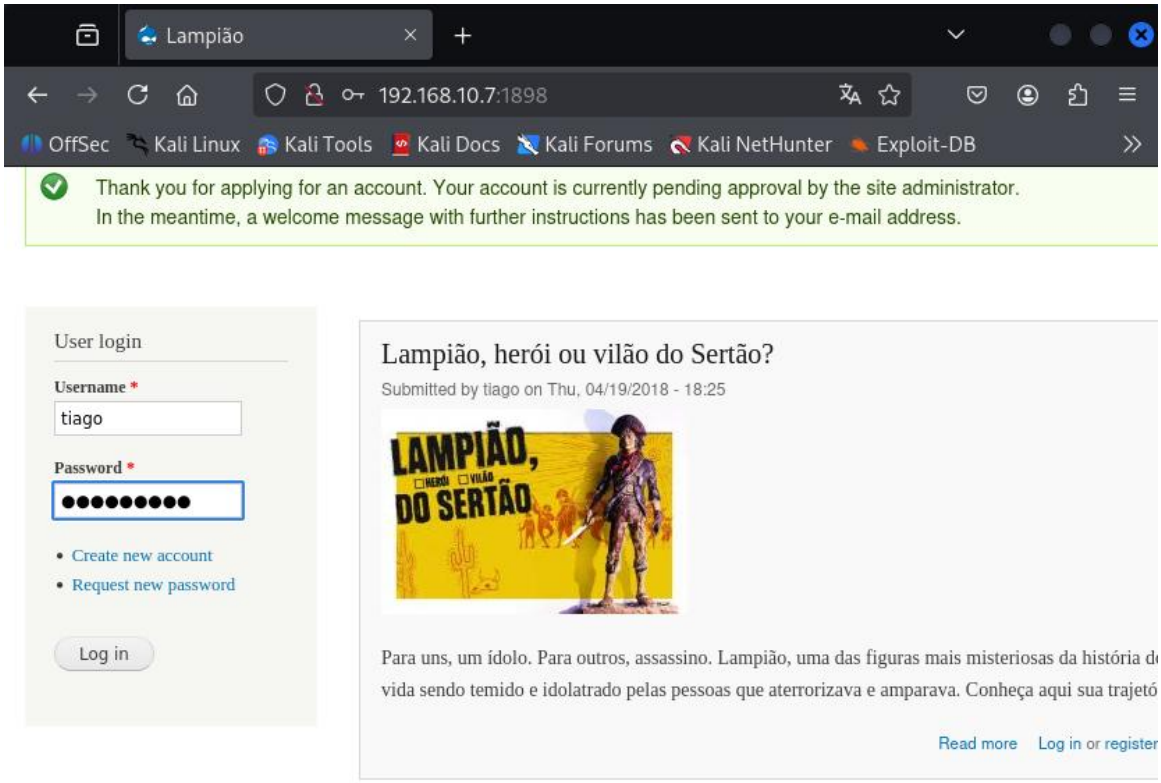


Ilustración 15. Intento de login en Lampião con credenciales

Ilustración 16. Error de login en Lampião

4.15 Conexión SSH exitosa

Conexión SSH exitosa a la máquina Lampião utilizando el comando **ssh tiago@192.168.10.7** y la contraseña **"Virgulino",** obteniendo acceso inicial al sistema.

```
┌──(root㉿kali)-[/home/brasil123]
└─# ssh tiago@192.168.10.7
The authenticity of host '192.168.10.7 (192.168.10.7)' can't be established.
ED25519 key fingerprint is SHA256:GGW0ASyjbhMycAKiglcXcsa0HvSwkLHZP9bQBtVrPs8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.7' (ED25519) to the list of known hosts.
tiago@192.168.10.7's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

  System information as of Mon Sep 15 15:56:53 BRT 2025

  System load:  0.98              Processes:           177
  Usage of /:   7.5% of 19.07GB   Users logged in:     0
  Memory usage: 18%               IP address for eth0: 192.168.10.7
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Thu Sep 11 12:24:55 2025 from 192.168.10.4
tiago@lampiao:~$
```

Ilustración 17. Conexión SSH exitosa

4.16 Verificación de red

Ejecución del comando **ifconfig** dentro de la sesión SSH para confirmar la configuración de red de la máquina victima la cual es **192.168.10.7**.

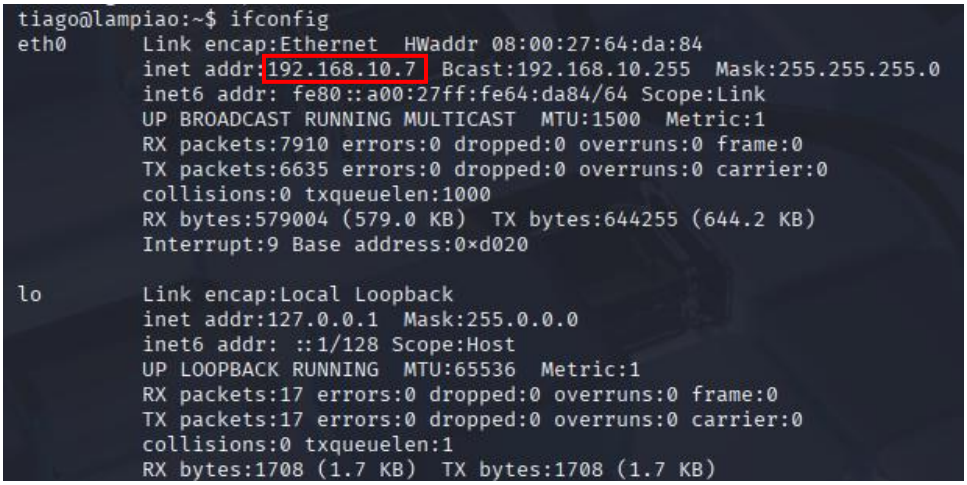


Ilustración 18. Verificación de red

4.17 Búsqueda de LinEnum en Google

Búsqueda en internet de LinEnum, un script de enumeración y escalada de privilegios para sistemas Linux.

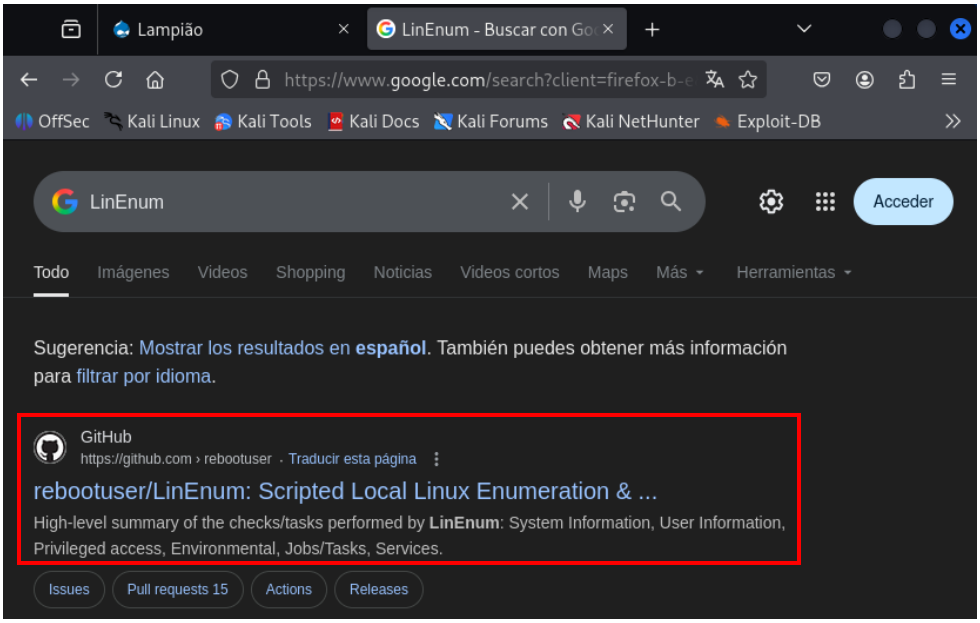


Ilustración 19. Búsqueda de LinEnum en Google

4.18 Página de GitHub de LinEnum

Se copia el repositorio oficial de LinEnum.

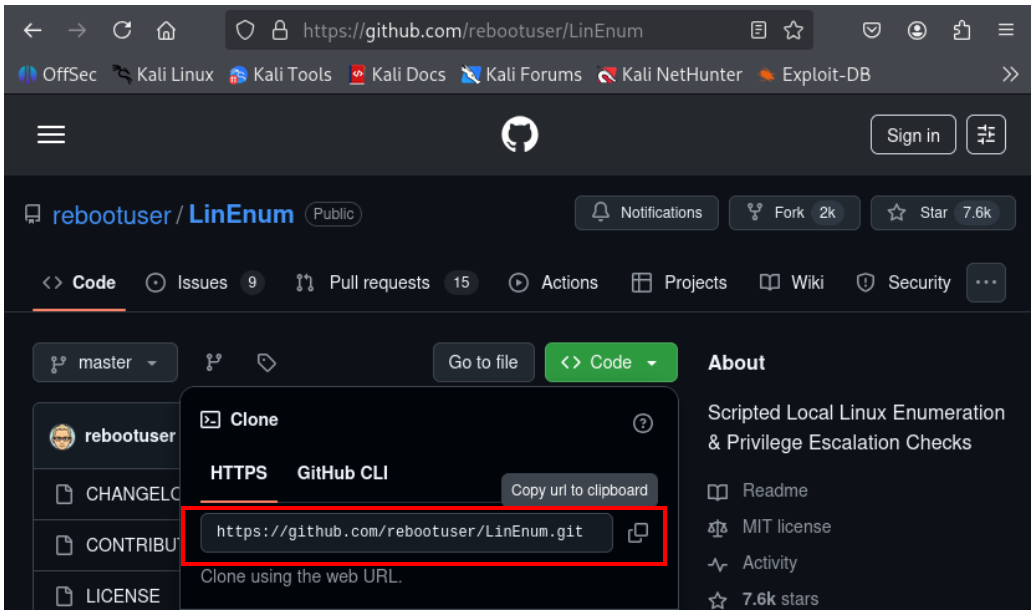


Ilustración 20. Página de GitHub de LinEnum

4.19 Clonación de LinEnum

Clonación del repositorio de LinEnum mediante el comando **git clone https://github.com/rebootuser/LinEnum.git** para obtener la herramienta en el sistema atacante.

```
┌──(root㉿kali)-[/home/brasil123]
└─# git clone https://github.com/rebootuser/LinEnum.git
Clonando en 'LinEnum' ...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Recibiendo objetos: 100% (234/234), 113.83 KiB | 539.00 KiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.
```

Ilustración 21. Clonación de LinEnum

4.20 Navegación y preparación de LinEnum

Navegación al directorio clonado de LinEnum y revisión del script principal **LinEnum.sh** utilizando el editor **nano**.

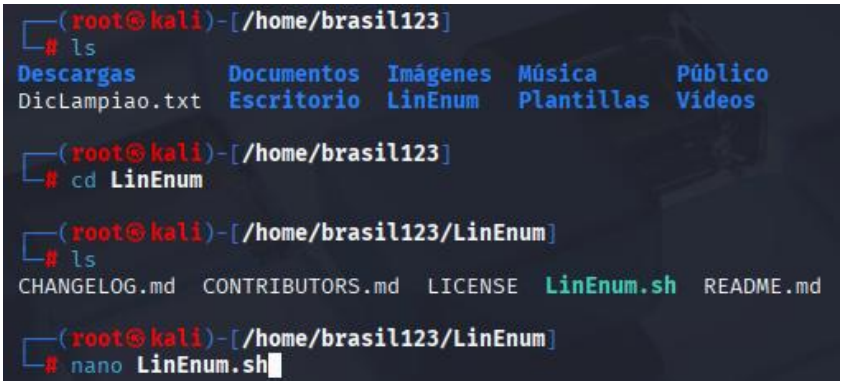


Ilustración 22. Navegación y preparación de LinEnum

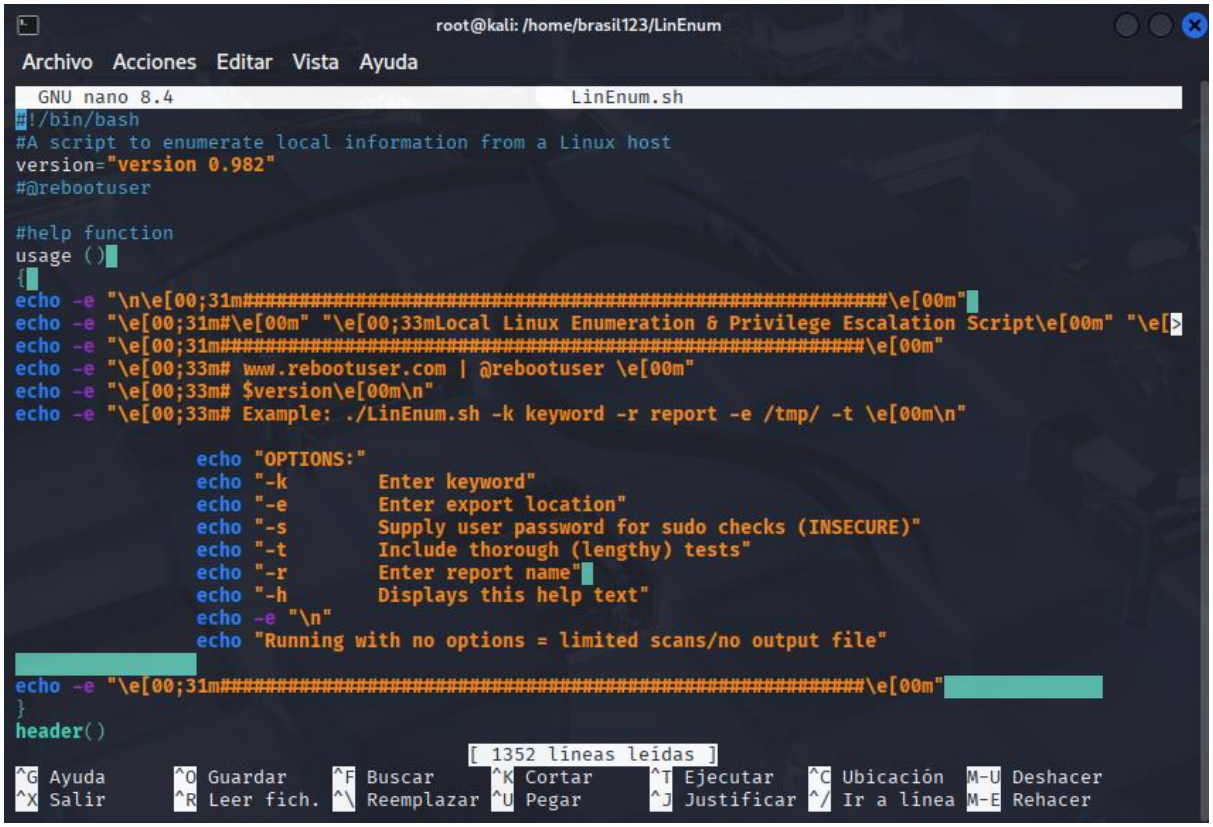


Ilustración 23. Archivo LinEnum

4.21 Enumeración manual del sistema

Exploración manual del sistema comprometido, navegando por directorios como **/home/tiago** y **/etc** en busca de información sensible o configuraciones vulnerables.

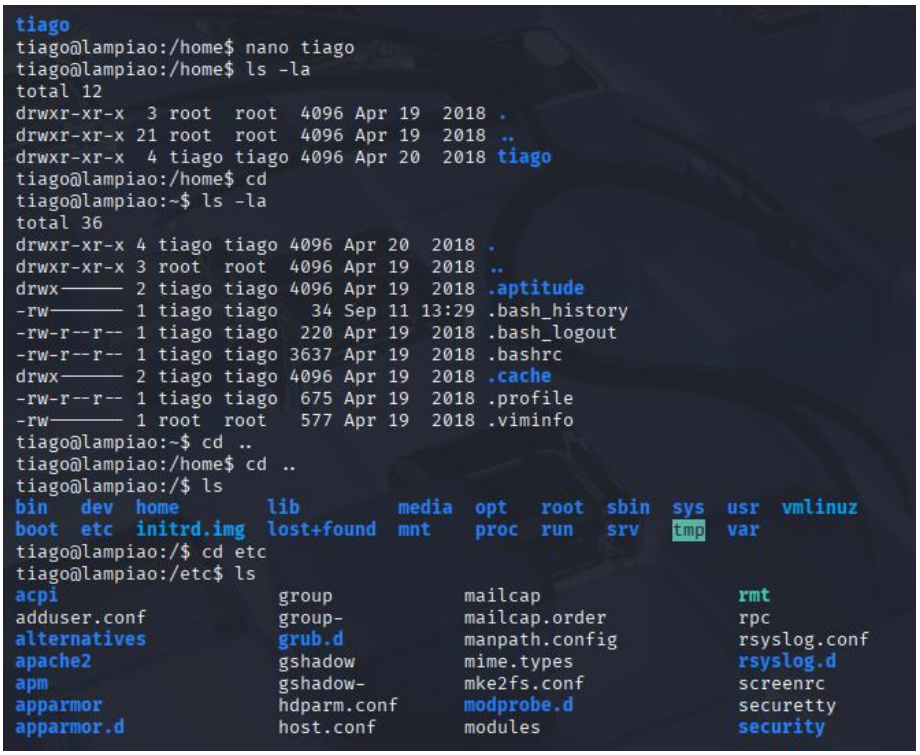


Ilustración 24. Enumeración manual del sistema

4.22 Visualización del archivo /etc/passwd

Visualización del contenido del archivo /etc/passwd para identificar usuarios del sistema, confirmando la presencia de "tiago", "root" y otros usuarios del servicio.

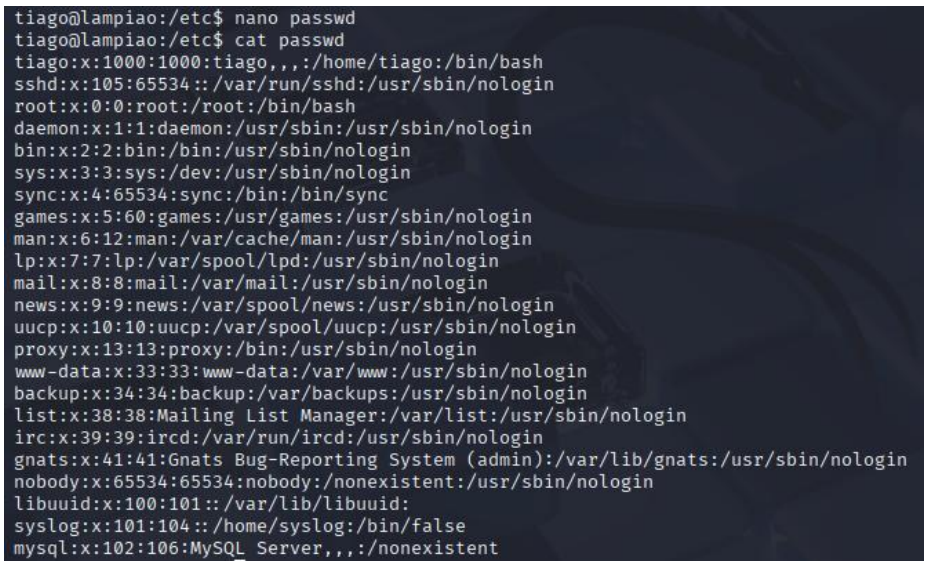
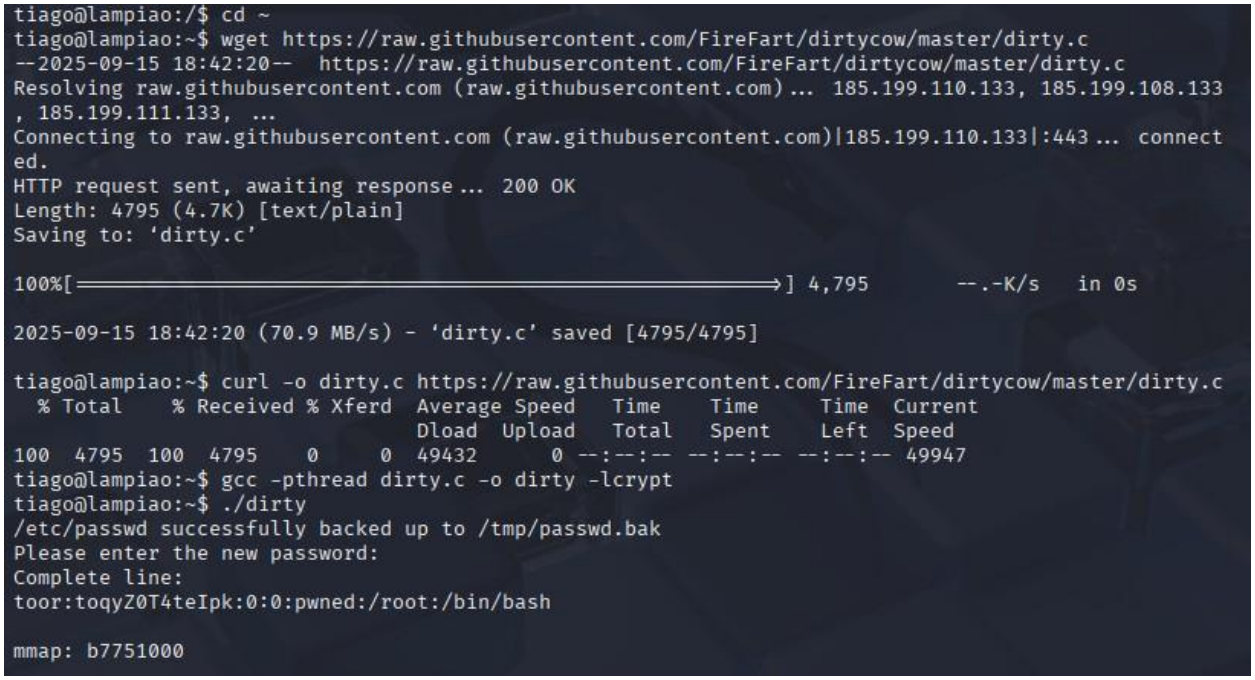


Ilustración 25. Visualización del archivo /etc/passwd

5. PROBLEMAS ENCONTRADOS

Durante la fase de escalada de privilegios, se procedió a explotar la conocida vulnerabilidad DirtyCow en el kernel de Lampião. El proceso inició correctamente con la descarga y compilación del exploit, sin embargo, al momento de la ejecución, el sistema mostró inestabilidad, el exploit se detiene abruptamente en la línea mmap: b7751000, lo que impidió completar la escalada de privilegios mediante este método.

El hecho de que el sistema se bloquee en la función mmap sugiere que el kernel objetivo, aunque vulnerable, presenta inestabilidades adicionales que previenen la explotación exitosa, requiriendo reinicios manuales de la máquina virtual para recuperar la funcionalidad, pero al volver a hacer el proceso se presenta de nuevo el mismo problema.



6. CONCLUSIÓN

El laboratorio permitió comprender de manera práctica los proceso desde el descubrimiento de servicios hasta la obtención de acceso al sistema. Aunque la explotación de DirtyCow no se ejecutó de manera exitosa debido a inestabilidades en el kernel, la práctica evidenció la realidad de los entornos de seguridad, donde no siempre los exploits funcionan de manera inmediata o predecible.

Se logró acceder a la máquina Lampião por medio de técnicas de enumeración y ataques de diccionario, lo que demostró la importancia de implementar contraseñas seguras y mantener actualizados los sistemas.

7. BIBLIOGRAFIA

Morales, R. S. (25). *INFORME DE LABORATORIO 01*. Quibdó, Colombia: Universidad Tecnologia del Chocó Diego Luis Córdoba. Recuperado el 23 de 09 de 2025