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

TABLA DE ILUSTRACIONES

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.

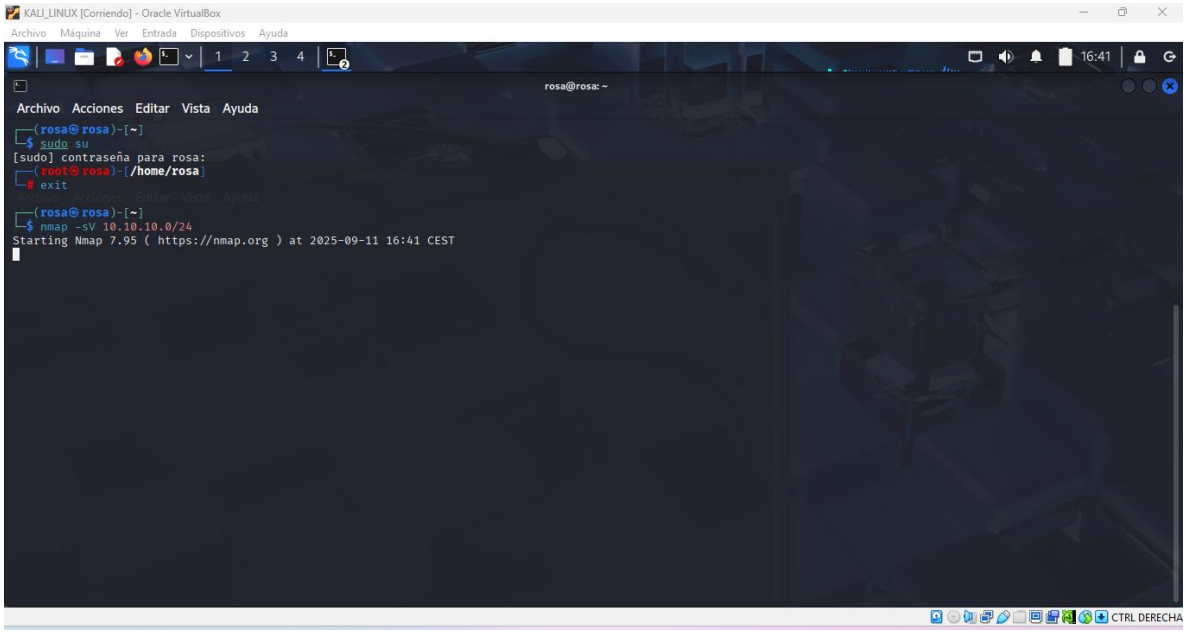
3.1 Descripción del problema

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>



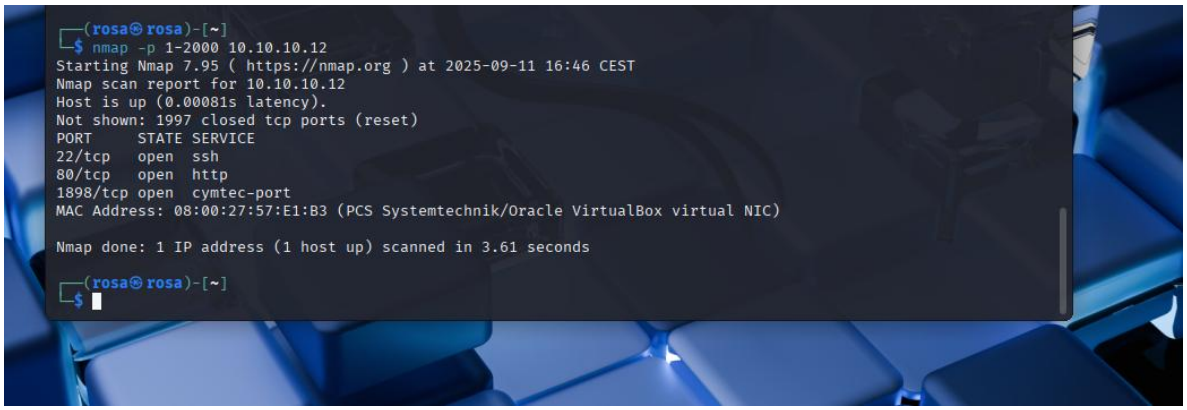
Descripción 1

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



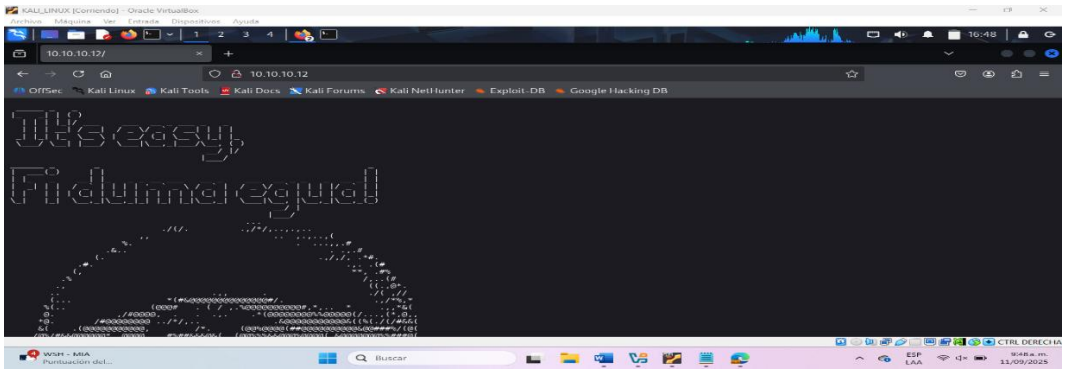
Descripción 2

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

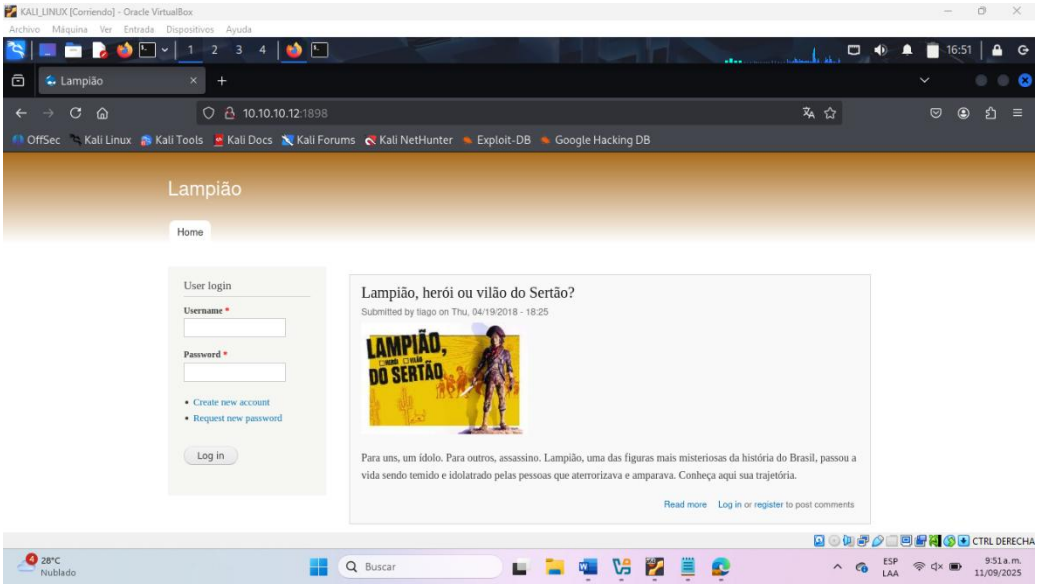


Descripción 3

3.5 Acceso al Servicio Web Descubierto

Visualización del servicio web encontrado tras la enumeración de directorios.

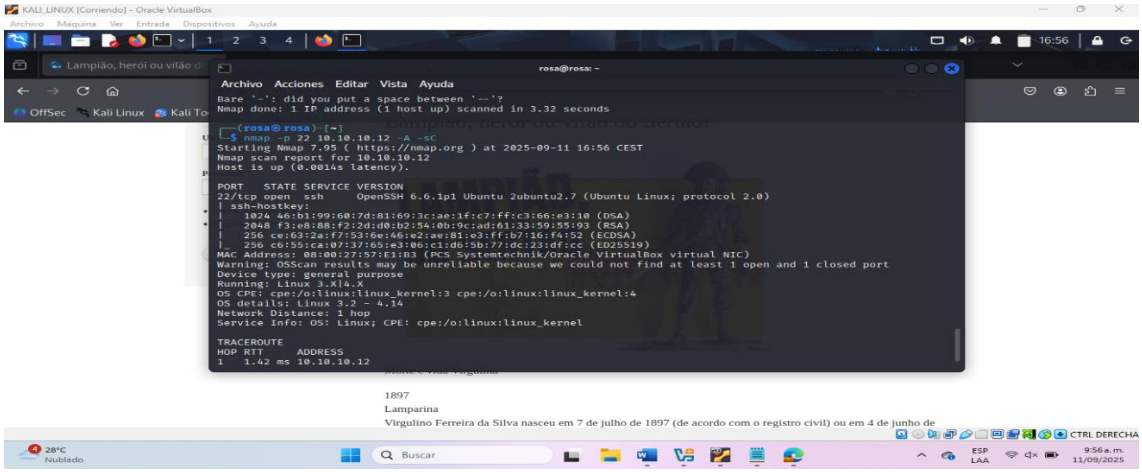
Permite interacción con el sistema objetivo.



Descripción 4

3.6 Página de Autenticación en la Aplicación Web

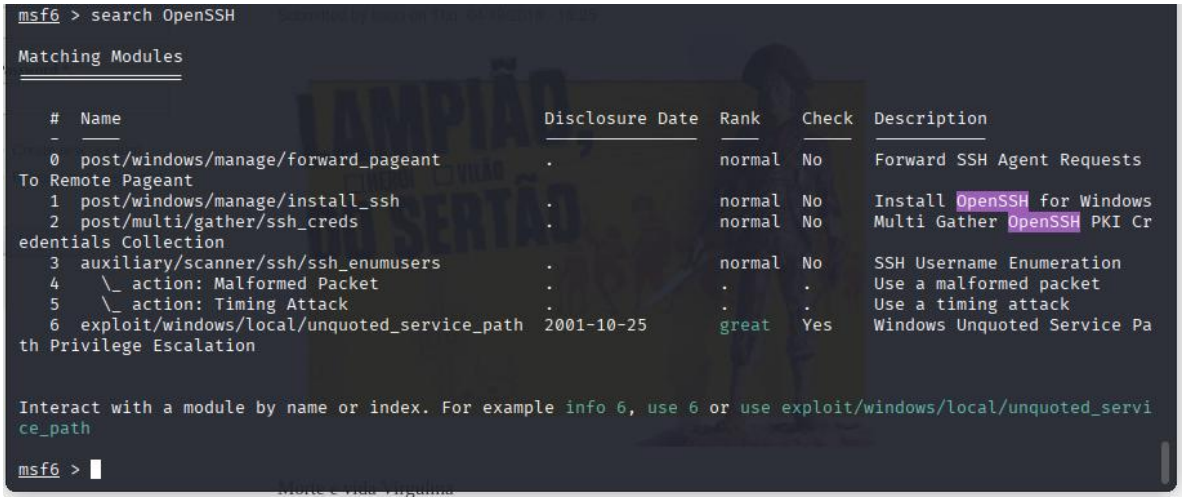
Captura de la página de login donde se probarán usuarios y contraseñas obtenidos con CeWL y otras técnicas de fuerza bruta.



Descripción 5

3.7 Intento de Acceso con Credenciales

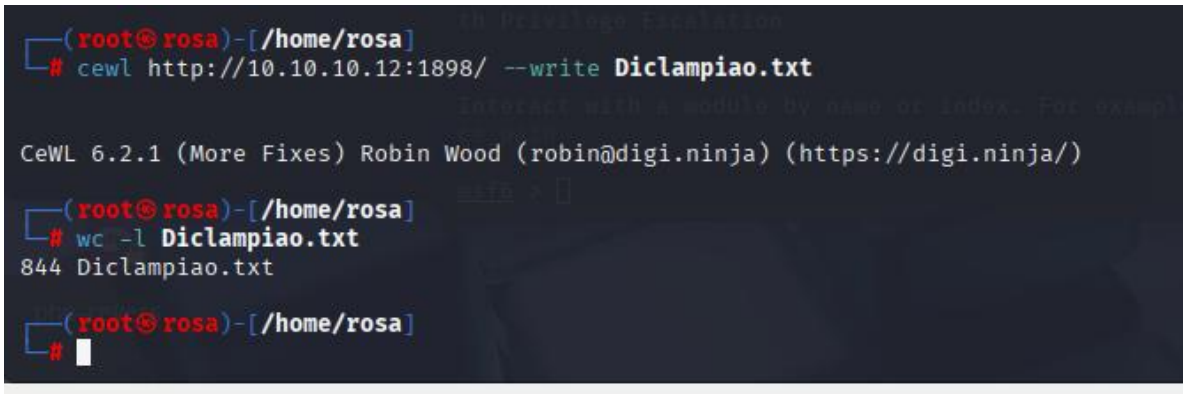
Prueba de credenciales sobre el formulario de inicio de sesión.



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.

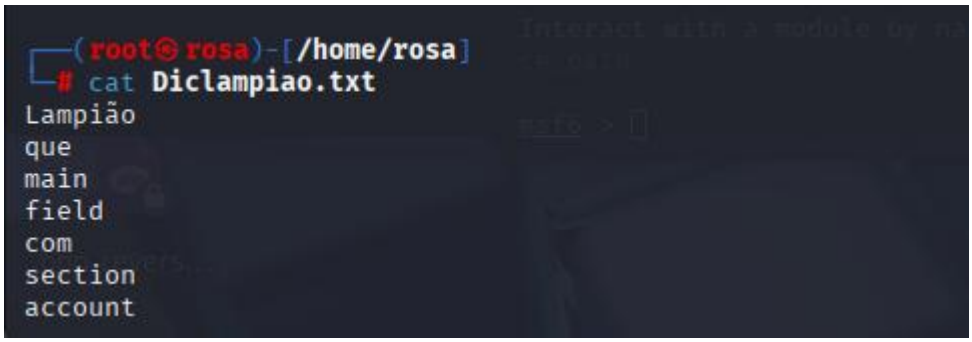


Descripción 7

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.

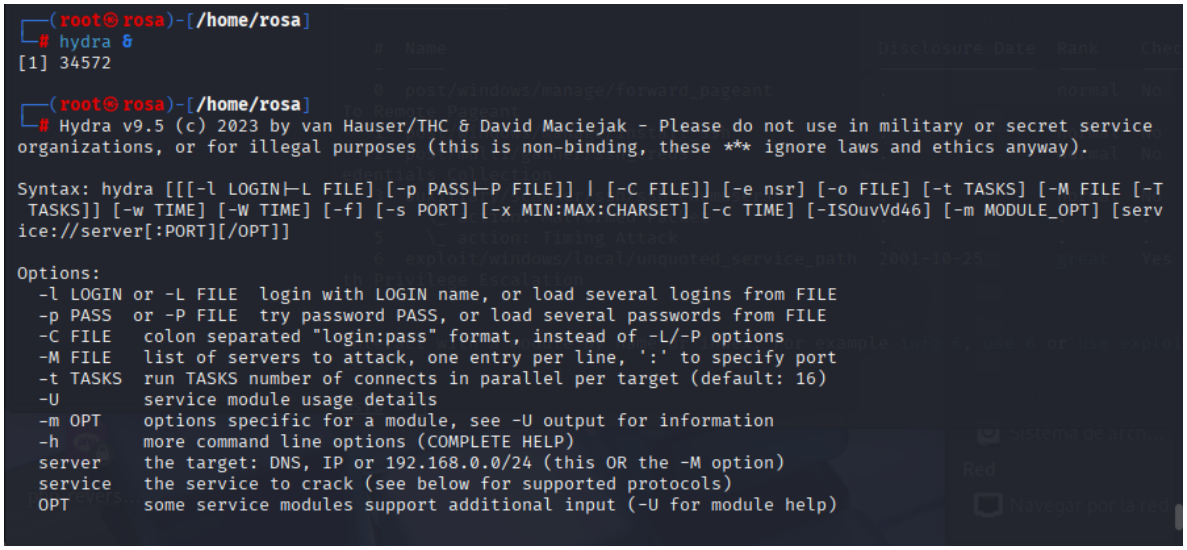


Descripción 8

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.).



Descripción 9

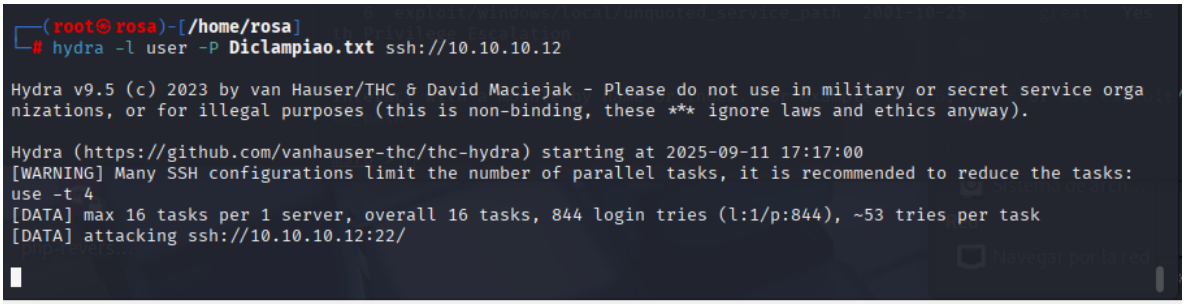
3.11 Ataque con Hydra seguido de análisis con LinEnum

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.



Descripción 10

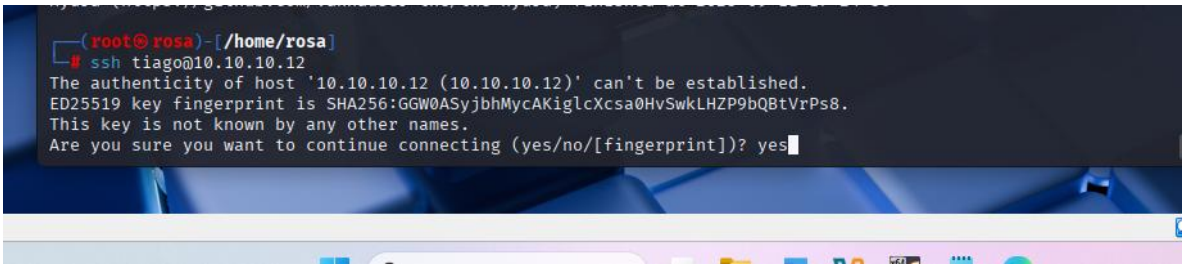
3.12 Compromiso inicial y reconocimiento post-explotación

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.



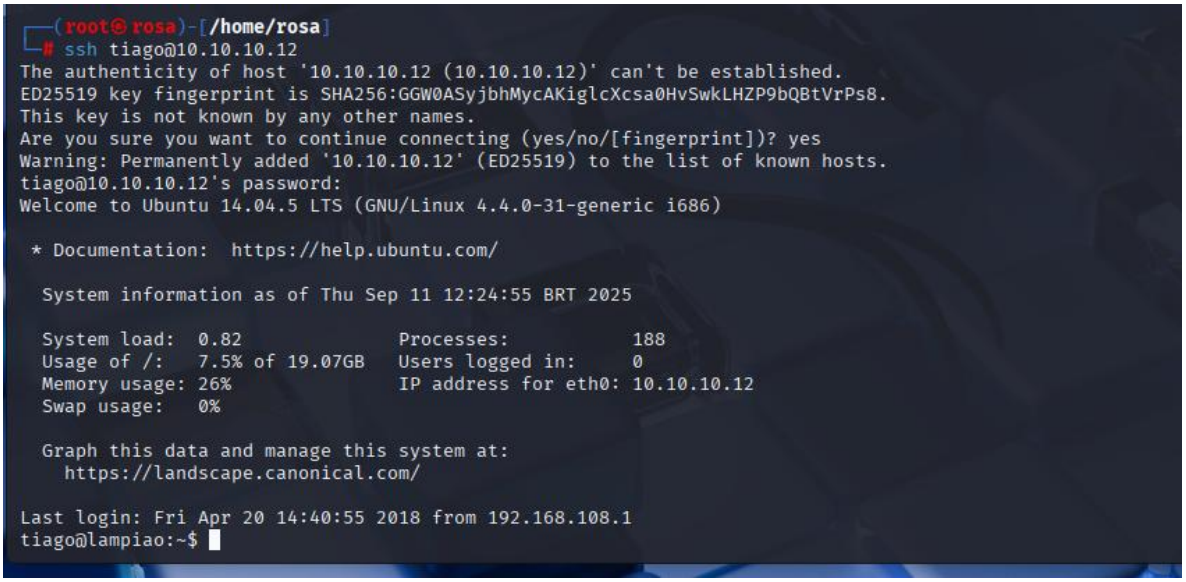
Descripción 11

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.).



Descripción 12

3.14 Secuencia: diccionario → Hydra → SSH → LinEnum

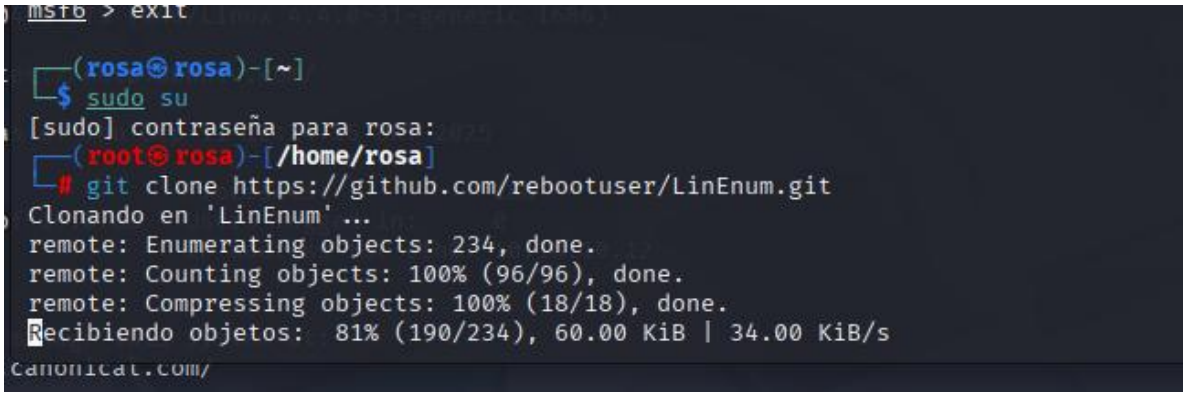
Se cambia de usuario rosa a root usando:

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**.



Descripción 13

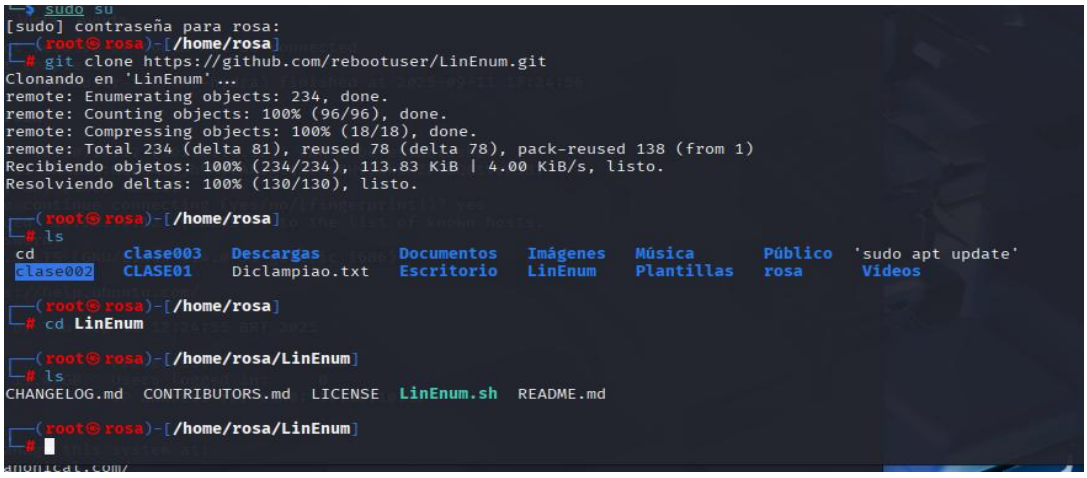
3.15 Operaciones de pentesting — fuerza bruta y enumeración

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.

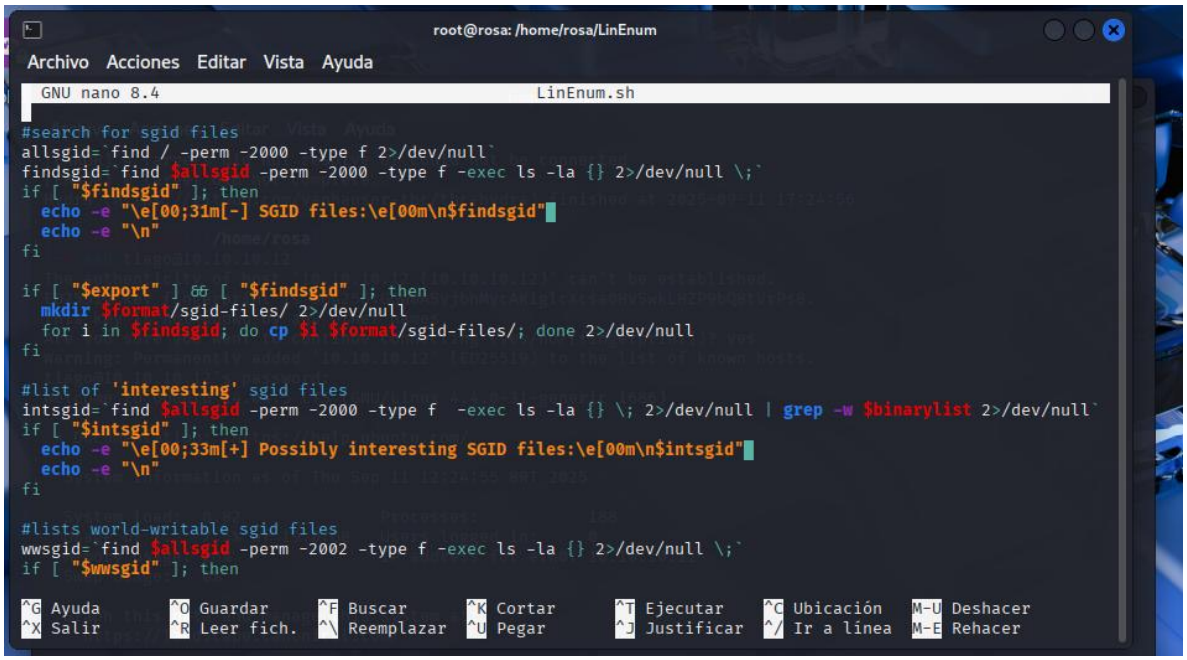


Descripción 14

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.ggggggggggggggggg



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.

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.

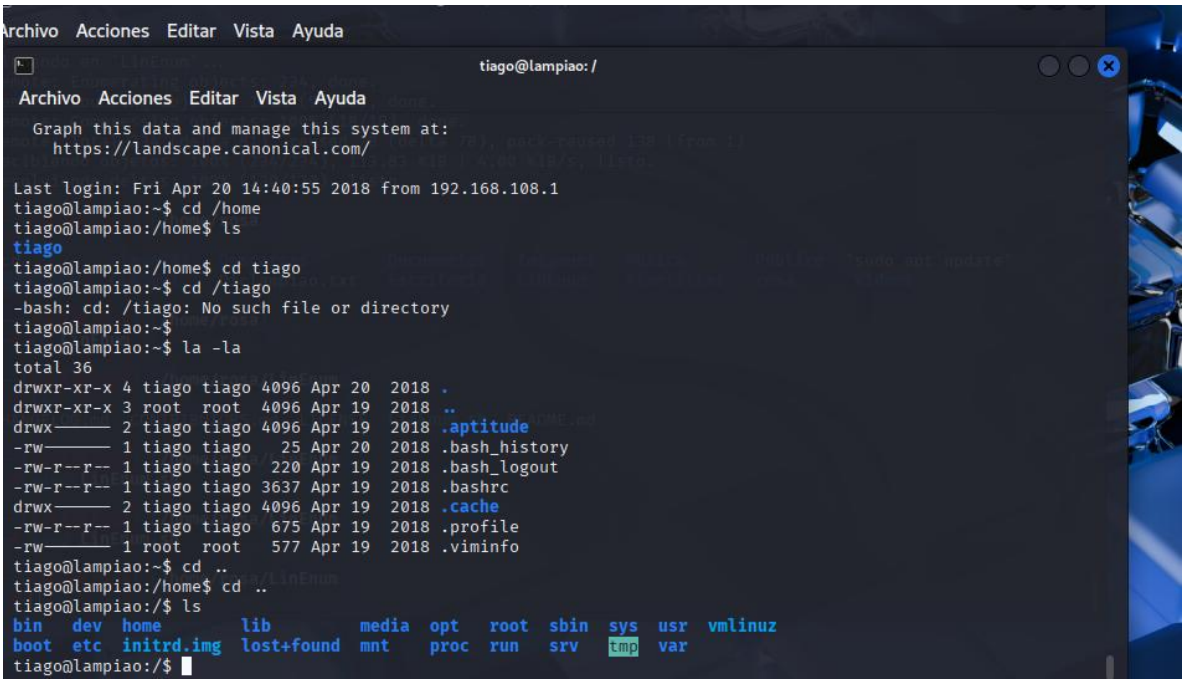
  - .viminfo — historial/estado de vim.

  - .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.



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 ...

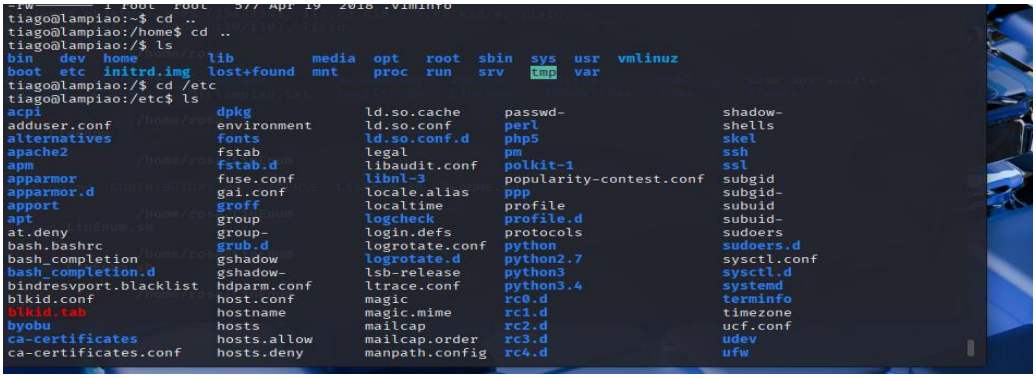
Qué representa cada tipo de entrada (resumen rápido):

- 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 /).



Descripción 18

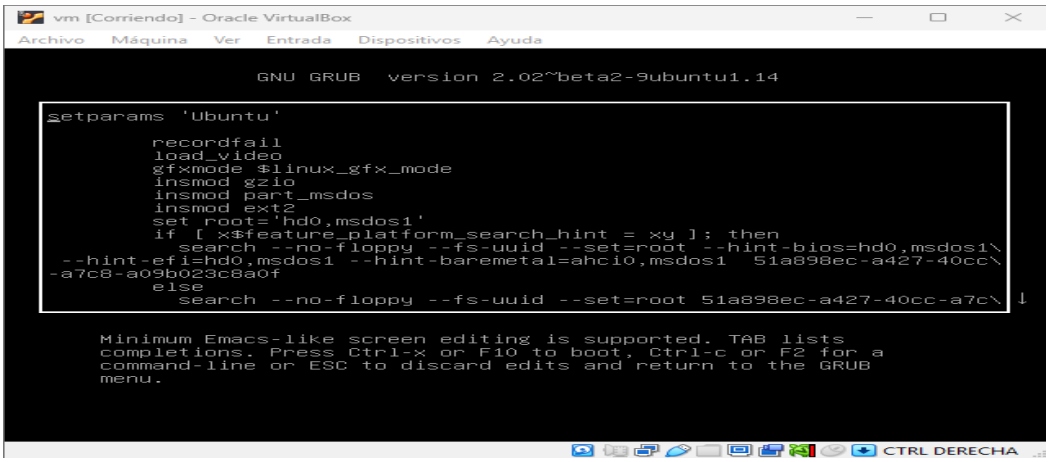
3.20 Convertir a Tiago como sudo

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

1. Reinicia lampiao.

2. En el menú de GRUB, selecciona la entrada de Ubuntu y pulsa e.

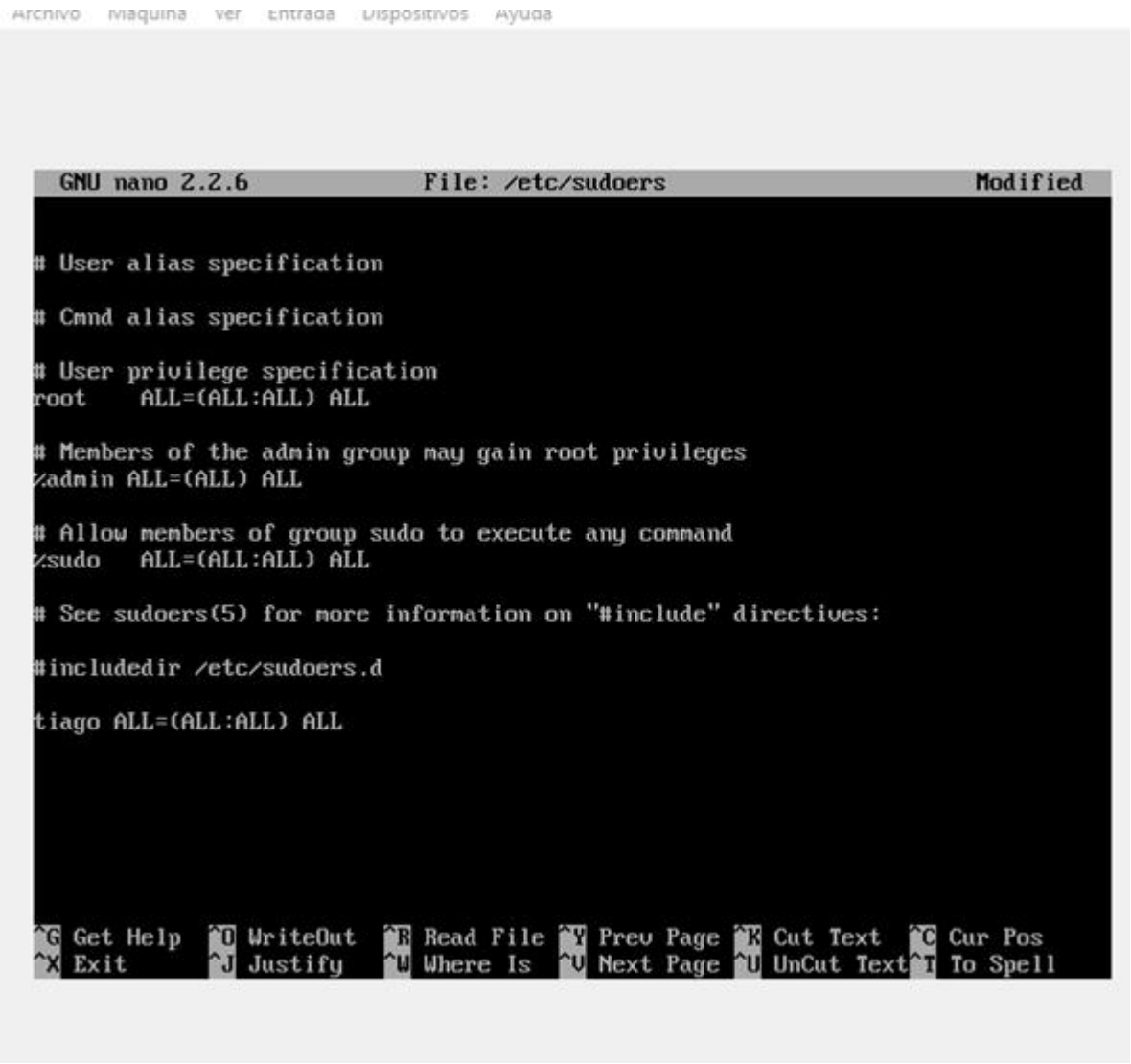
3. Busca la línea que empieza con linux y al final agrega:



Descripción 19

3.20.2 se le dan los privilegios a tiago

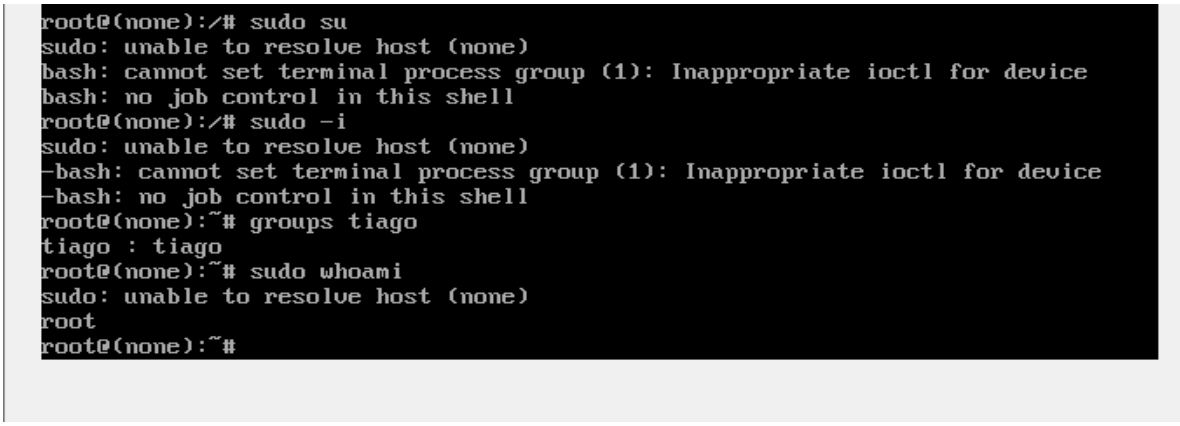
dentro de nano, se agrega la siguiente línea en modo lectura. Solo tienes que remontar el sistema de archivos con permisos de escritura (mount -o remount,rw /) y ya podrás usar usermod.



Descripción 20

3.20.3 Inicializa como root

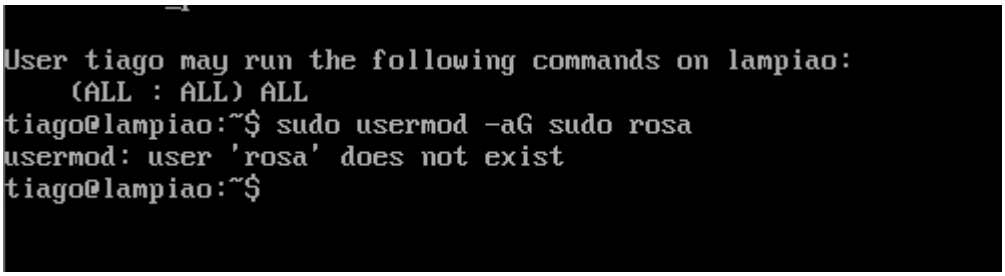
Se inicializa como root provisional para que darle los acesso como supe usuario a tiago



Descripción 21

3.20.4 Confirmamos si Tiago tiene el modo sudo

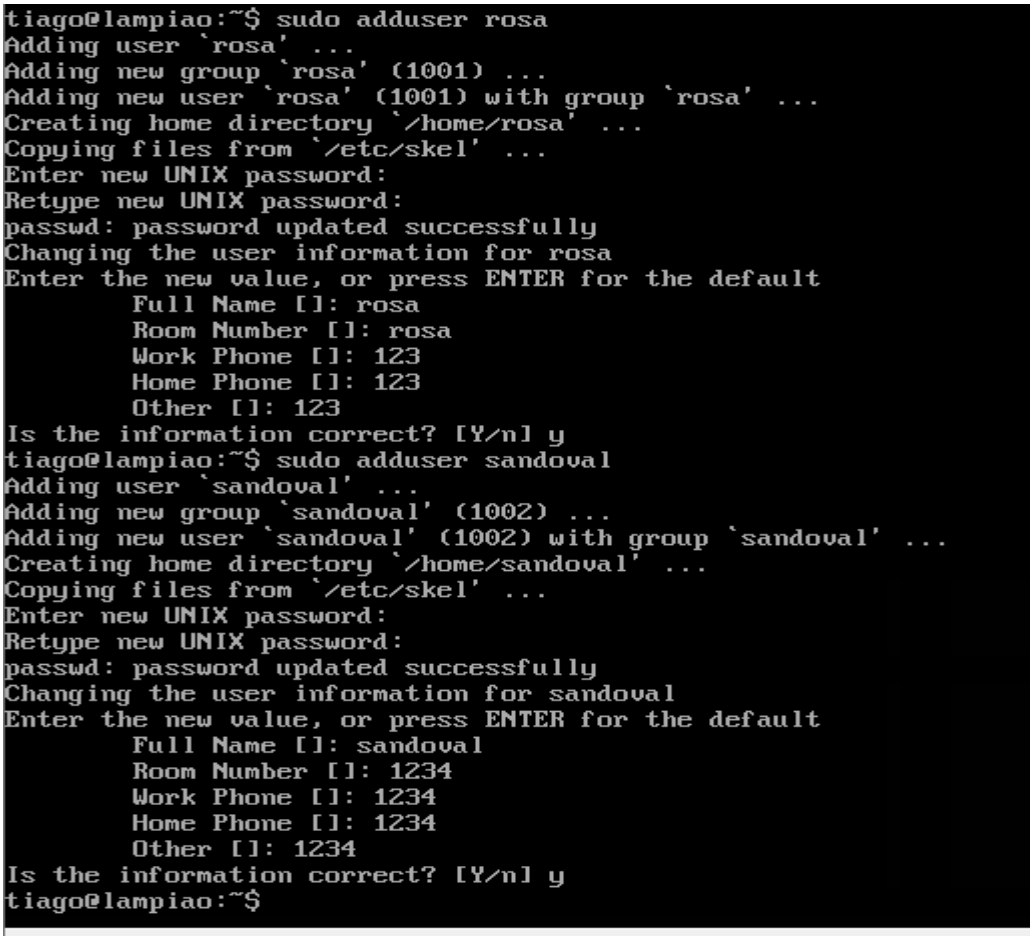
Aplicamos el comando sudo usermod -aG sudo rosa para que probar si tiago esta en modo sudo y efectivamente esta en modo sudo, ya que nos dice que el usuario rosa no existe



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



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

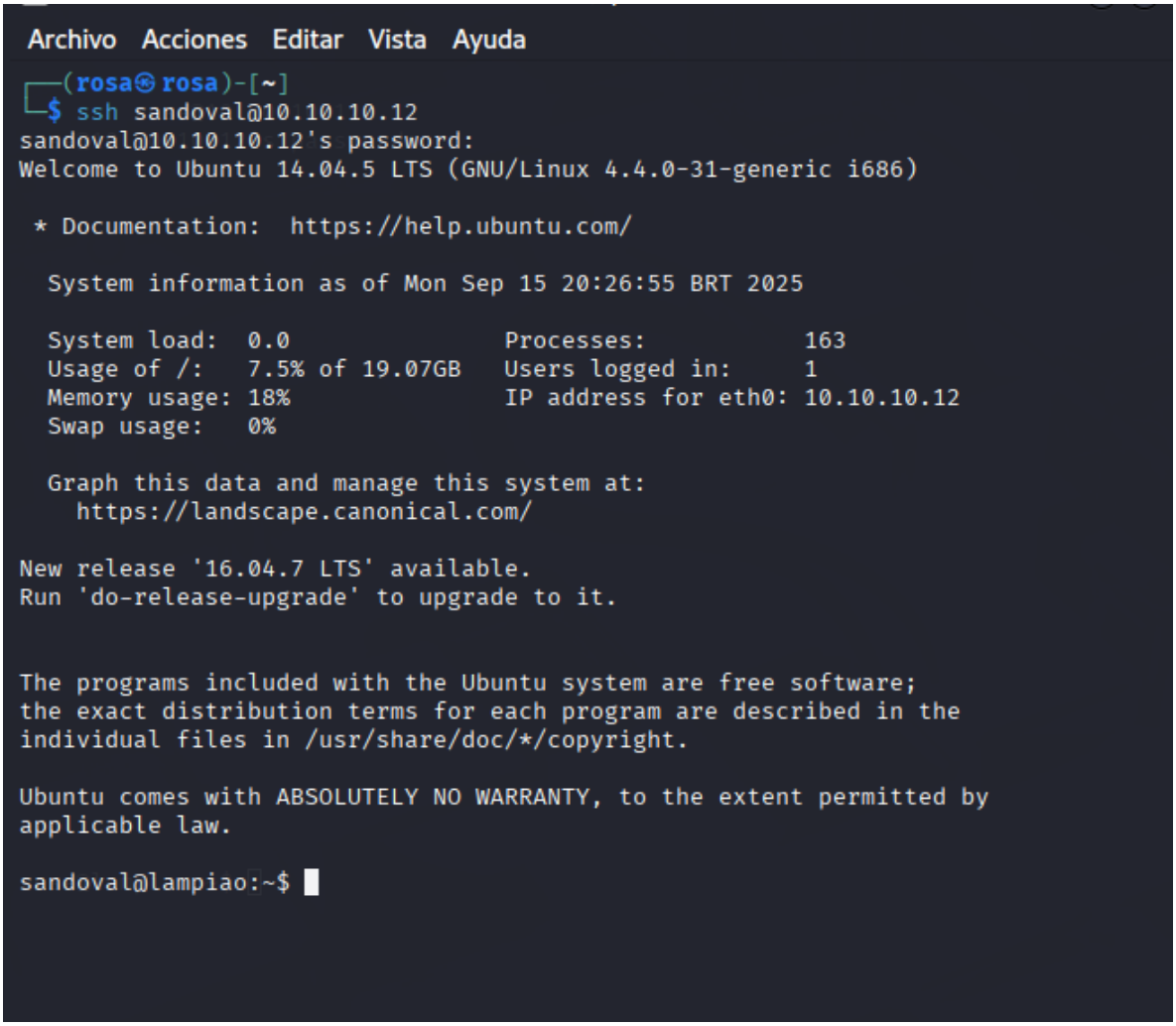
3.20.7 Accedemos a SSH con el usuario ROSA recién creado

```
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



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).