LABLINUX 1 – Administración básica + Hardening

1. Objetivo. – Analizar el sistema operativo Linux mediante comandos de línea para identificar información relevante desde el punto de vista de la seguridad.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

3. Metodología / Análisis Realizado

Esta sección describe el análisis realizado sobre el sistema Linux mediante comandos de linea, con el objetivo de obtener información relevante para la seguridad del sistema.

3.1 Información del Sistema

Se consultó la información completa y detallada del sistema operativo utilizando los siguientes comandos:

- **lsb_realease -a** permite obtener toda la información detallada acerca de la distribución del sistema operativo, basándose en Linux Standard Base (lbs).
- **Uname -a** es una abreviatura de (UNIX NAME), el cual sirve para mostrar una información completa del software y hardware, como ser el nombre y la versión del kernel, nombre del host, procesador, sistema operativo.

Conocer la información del equipo es vital, ya que permite identificar sistemas desactualizados o vulnerables.

3.2 Gestión de usuarios y grupos

Se realizó la revisión de usuarios existentes en el sistema ejecutando el siguiente comando:

“cat /etc/passwd”

Este comando visualiza el contenido del archivo **“passwd”,** el cual contiene la información de los usuarios del sistema, incluyendo el nombre, identificador de usuario (UID), directorio personal y grupos al que pertenece. Este enlistado es muy útil para identificar usuarios desconocidos o con privilegios elevados, destacando su importancia en el área de seguridad.

El conocimiento de como se crea un usuario nuevo es de suma importancia, ya que permite separar entornos de trabajo, asignar permisos y usar el sistema sin interferir con otros. En este laboratorio se creó un nuevo usuario llamado “agentesoc”, utilizando el siguiente comando:

“sudo add user agentesoc”

Con el nuevo usuario creado, se utilizaron comandos que permitan conocer el UID del usuario nuevo y a los grupos que pertenece, entendiendo de lo que puede y no puede hacer un usuario en el sistema, siendo fundamental para la seguridad y administración. (ver Figura 1)

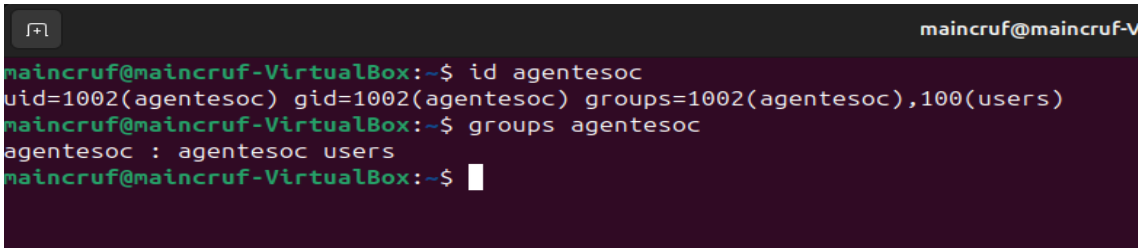

Figura 1. Identificación de un usuario y grupos al que pertenece.

3.3 Permisos de archivos

La gestión de permisos de archivos en Linux es un aspecto crucial para la seguridad y administración del sistema, ya que se permite definir que usuarios pueden leer, escribir o ejecutar un archivo.

Durante este laboratorio, se creó un archivo de prueba y modificó sus permisos con el comando **“chmod 600”**. En la notación octal de permisos, el valor **6** corresponde a la suma de los permisos de lectura (4) y escritura (2) del propietario del archivo, mientras que el valor **0** indica ausencia de permisos para el grupo y resto de usuarios. Posteriormente se verificó la configuración de los cambios realizados. (ver Figura 2)

Los permisos de los archivos se representan mediante la cadena **“-rwxrwxrwx”**, donde los nueve caracteres finales se dividen en tres grupos de tres. El primer grupo corresponde a los permisos del propietario del archivo, el segunda al grupo que pertenece y el tercer grupo al resto de los usuarios. El carácter **“r”** corresponde a permisos de lectura (read), **“w”** a escritura (write) y **“x”** a ejecución (execute). La correcta configuración de estos permisos es esencial para proteger archivos críticos del sistema, reduciendo riesgos de seguridad.

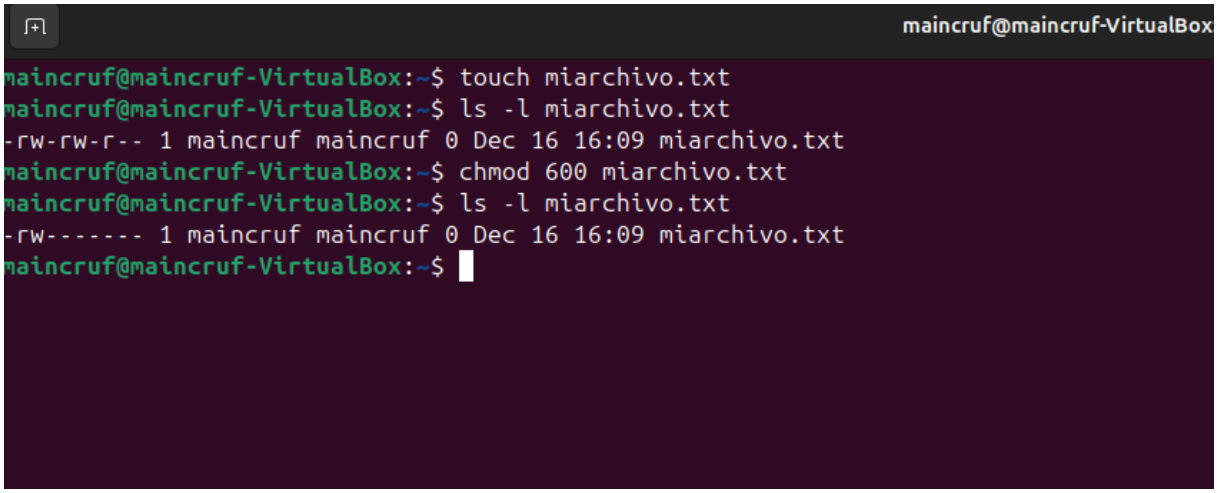

Figura 2. Creación y cambio de permisos de un archivo.

3.4 Procesos del sistema

Se realizó la revisión de los procesos en ejecución que se encuentran en el sistema mediante el comando:

1. “ps aux”

Este comando da a conocer una gran lista detallada de todos los procesos activos, identificando a sus respectivos usuarios, lo cual resulta útil para distinguir procesos desconocidos o potencialmente sospechosos.

Debido a que la lista de los procesos en ejecución es extensa, se utilizó el comando **“grep”** para filtrar y encontrar coincidencias con el proceso que se desea analizar, en este caso los procesos ssh. (ver Figura 3)

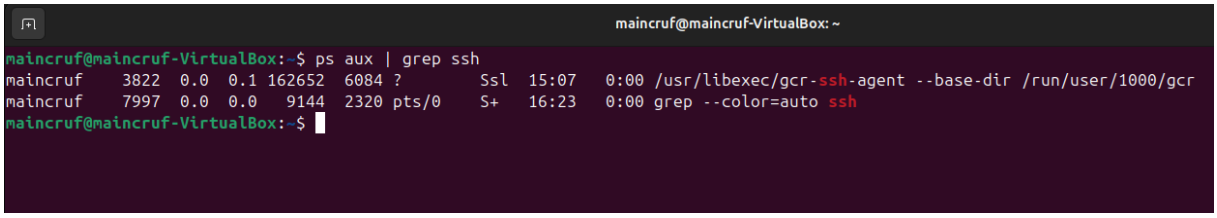

Figura 3. Identificación un proceso en especifico.

3.5 Servicios del sistema

Conocer el estado de los servicios en ejecución es fundamental para la administración y seguridad del sistema. Para ello se ejecutó el comando:

“systemctl status ssh”

A partir de la salida de este comando se observó que el servicio SSH se encuentra instalado pero inactivo **(inactive (dead))**, y no configurado para iniciarse

automáticamente al arranque del sistema **(disabled)**, ademas se identificó que el servicio puede activarse mediante **ssh.socket**, manteniendo la disponibilidad del servicio cuando es requerido. (ver Figura 4)

Asimismo, se ejecutó el comando:

“sudo systemctl disable cups”

Este permite deshabilitar el inicio automático de servicios innecesarios. Esta práctica contribuye a reducir la superficie de ataque del sistema, evitando que servicios no requeridos se ejecuten al iniciar el sistema. No obstante se observó que el servicio puede activarse bajo demanda a través de sus unidades asociadas **(cups.socket y cups.path).** (ver Figura 4)

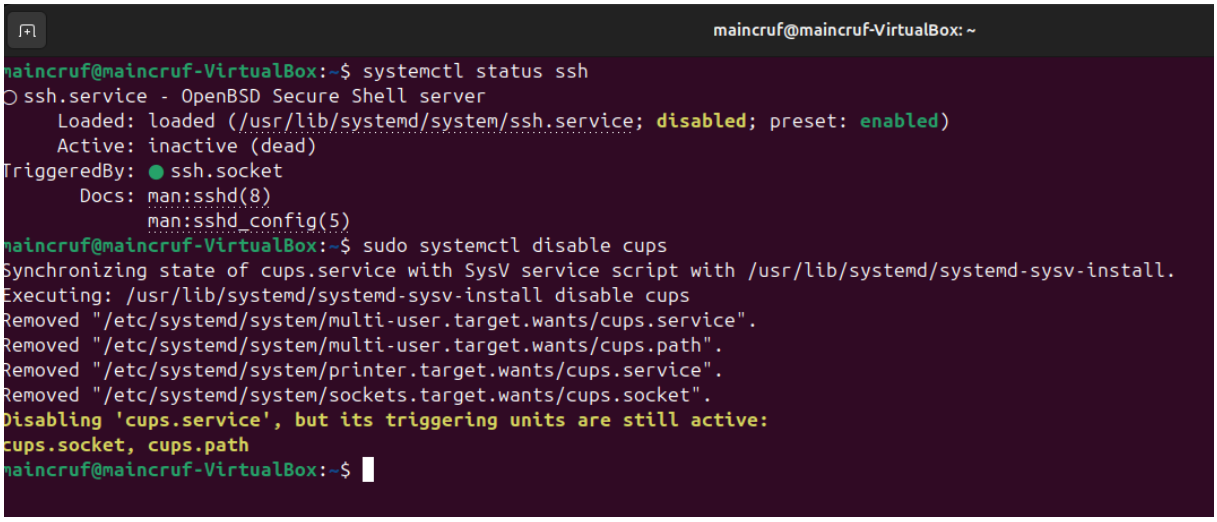

Figura 4. Verificación del estado del servicio ssh y desactivación de servicios.

3.6 Hardening básico + firewall

Tener actualizado el equipo es crucial para la administración de la seguridad, para esto se ejecutó el siguiente comando:

sudo apt update && sudo apt upgrade

Este comando primero actualiza la data del equipo acerca de los mas recientes repositorios, y después compara la lista de paquetes locales con los paquetes instalados, actualizando los que son antiguos.

Asimismo es necesario mantener activo el firewall. Para verificar el estado y las reglas activas del firewall se ejecutó el siguiente comando:

sudo afw status verbose

La salida de este comando permite conocer los detalles acerca del firewall. En este caso se observa que el firewall está activo y que el registro de eventos solo registra eventos básicos de la actividad de firewall (logging : on (low)).

Ademas, se identifican las políticas por defecto del firewall como ser conexiones entrantes que se bloquean por defecto, conexiones salientes que se permiten por defecto y el firewall no afecta el trafico que se ruta entre interfaces. Finalmente, los nuevos perfiles de aplicaciones que se instalan son ignorados automáticamente, por lo que no se crea reglas por defecto para ellos. (ver Figura 5)

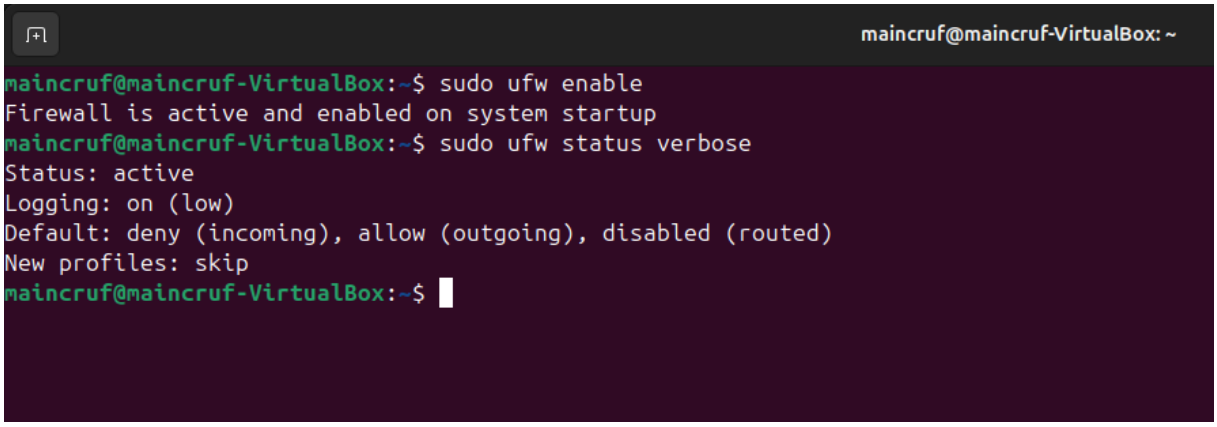

Figura 5. Estado del Firewall

3.7 Registro de eventos (logs)

El registro de eventos en una herramienta muy importante para la seguridad del sistema, ya que permite identificar actividades relevantes y posibles incidentes. Para acceder a esta información, se consulta el archivo **auth.log**, el cual registra el evento de autenticación, como inicio de sesión de usuarios e intentos fallidos.

Al consultar el archivo, se observan eventos relacionados con la autenticación y el uso de privilegios elevados en el sistema. En los registros se identifica que el usuario maincruf ejecutó el comando **sudo** desde una terminal interactiva **(TTY=pts/0)**, con el objetivo de acceder al archivo logs.

Los mensajes generados por el modulo **pam_unix** indican la apertura y cierre correctos de sesiones con privilegios elevados, confirmado que la autenticación fue exitosa y controlada. Asimismo, se registra eventos asociados al servicio **CRON** que corresponden a tareas automáticas por el usuario **root**, consideradas como actividad normal del sistema.

En base a los análisis de los registros, no se identificaron intentos fallidos de autenticación ni comportamientos extraños, mostrando un uso legitimo del sistema en este laboratorio. (ver Figura 6)

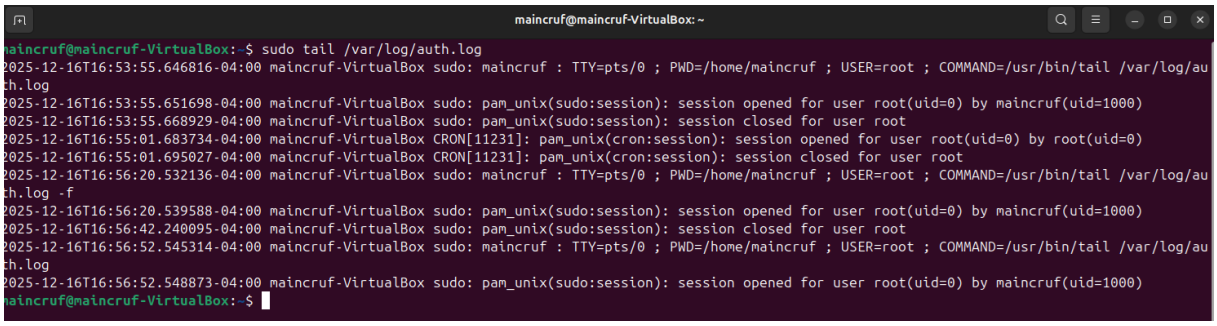

Figura 6. Registros de autenticación

4. Resultados Obtenidos. – En este laboratorio se utilizaron distintos comandos básicos en Linux para obtener la información general del sistema y realizar su actualización. Asimismo, se observaron y analizaron servicios, procesos y registros del sistema, con el objetivo de identificar posibles eventos sospechosos. Adicionalmente, se crearon usuarios y administraron permisos, comprendiendo como el control de accesos influye en la seguridad del sistema. Finalmente, se verificó el estado del firewall, sus políticas y reglas activas. En conjunto, estas actividades permitieron aplicar conceptos de seguridad en entornos Linux y comprender su importancia en la protección del sistema.

5. Reflexión final. – Este laboratorio permitió comprender la importancia de conocer la información básica del sistema. Ademas de tener la capacidad de analizar procesos, servicios, permisos y registros identificando comportamientos extraños o eventos potencialmente sospechosos, para lograr mantener un entorno seguro. Si bien un SIEM correctamente configurado visualiza este tipo de eventos fácilmente, la ausencia de este entorno de seguridad, hace indispensable el conocimiento y uso de comandos nativos del sistema. Esto permite responder y tomar decisiones oportunas ante posibles incidentes y fortalecer la seguridad del sistema de manera efectiva.