**ANEXO I**

**Práctica 1: Hardening.**

**Trabajo preparatorio**

* **Revisar y explicar de manera breve comandos básicos para gestionar usuarios y permiso en Linux.**

La administración de usuarios y permisos en Linux es clave para garantizar la seguridad y el control del sistema. A continuación, se detallan algunos comandos fundamentales para gestionar usuarios y permisos:

**Tabla 5.1.** Comandos fundamentales

|  |  |
| --- | --- |
| Comando [36] | Uso [36] |
| sudo adduser nombre\_usuario | Añade un nuevo usuario al sistema y crea su directorio personal. |
| sudo userdel nombre\_usuario | Elimina una cuenta de usuario del sistema. |
| sudo chmod 755 archivo\_o\_directorio | Modifica los permisos de lectura, escritura y ejecución para el propietario, grupo y otros. |
| sudo chown usuario:grupo archivo\_o\_directorio | Cambia el propietario y/o el grupo de un archivo o directorio |

* **Explicar y detallar para que sirve el comando chmod, sus especificaciones y las formas o modos para asignar permisos.**

El comando chmod, abreviatura de "change mode" (cambiar modo), se utiliza para modificar los permisos de acceso a archivos y directorios en sistemas operativos basados en Unix, como Linux. Estos permisos definen quién tiene autorización para leer, escribir o ejecutar un archivo o directorio [37].

En sistemas Linux, cada archivo o directorio tiene asociados permisos para tres categorías de usuarios:

* Propietario (u - user): El usuario que posee el archivo.
* Grupo (g - group): Usuarios que pertenecen al mismo grupo que el propietario.
* Otros (o - others): Todos los demás usuarios.

Los tipos de permisos que se pueden asignar son:

Lectura (r - read): Permite ver el contenido del archivo o listar el directorio.

* Escritura (w - write): Permite modificar el contenido del archivo o añadir/eliminar archivos en un directorio.
* Ejecución (x - execute): Permite ejecutar el archivo como un programa o acceder al directorio.
* Existen dos métodos principales para asignar permisos con chmod:

**Notación Simbólica [37]**

Utiliza letras y símbolos para representar los cambios de permisos. La sintaxis básica es chmod [categoría][operador][permisos] archivo\_o\_directorio donde:

**Tabla 5.2.** Notación Simbólica

|  |  |  |
| --- | --- | --- |
| Categoría | Operador | Permisos |
| u: Propietario. | +: Añadir permiso. | r: Lectura. |
| g: Grupo. | -: Quitar permiso | w: Escritura. |
| o: Otros. | =: Asignar permiso específico, eliminando los demás | x: Ejecución. |
| a: Todos |  |  |

**Notación Numérica (Octal) [37]**

Cada permiso se representa con un valor numérico:

* r (lectura) = 4
* w (escritura) = 2
* x (ejecución) = 1

Los permisos se suman para cada categoría de usuario y se expresan en un número de tres dígitos, donde cada dígito representa los permisos del propietario, grupo y otros, respectivamente. Por ejemplo, el comando chmod 754 archivo.txt representa rwxr-xr— donde:

* Propietario: rwx = 4+2+1 = 7
* Grupo: r-x = 4+0+1 = 5
* Otros: r-- = 4+0+0 = 4
* **Definir que es tráfico saliente y entrante, además explicar su diferencia.**

**Tráfico Entrante:**

El tráfico entrante hace referencia a todos los datos que ingresan a un dispositivo o red desde fuentes externas. Esto incluye, por ejemplo, solicitudes de páginas web recibidas por un servidor, correos electrónicos entrantes o cualquier conexión externa dirigida hacia la red interna. Una gestión adecuada de este tráfico es esencial para protegerse contra amenazas externas y asegurar que solo conexiones autorizadas puedan acceder a los recursos internos.[38]

**Tráfico Saliente:**

El tráfico saliente comprende todos los datos enviados desde un dispositivo o red hacia destinos externos. Esto incluye actividades como visitar sitios web, enviar correos electrónicos o cargar archivos a servidores remotos. Controlar este tipo de tráfico es crucial para prevenir la filtración de información sensible y garantizar que las comunicaciones externas se realicen de forma segura. [38]

La diferencia fundamental entre estos dos tipos de tráfico se basa en la dirección en la que se transmiten los datos:

* Tráfico Entrante: Corresponde a los datos que llegan a la red desde fuentes externas.
* Tráfico Saliente: Se refiere a los datos que se envían desde la red hacia destinos externos.
* **Investigar que es SSH, configuración básica y la seguridad en SSH en un sistema operativo Linux.**

SSH (Secure Shell) es un protocolo de red diseñado para establecer conexiones seguras y encriptadas entre dos dispositivos, permitiendo tanto la administración remota de sistemas como la transferencia de archivos de manera segura en entornos Linux y otros sistemas operativos compatibles [39].

Para configurar el servicio SSH primero se debe tener instalado en el sistema con sudo apt install openssh-server, luego iniciar y habilitar el servicio con los comandos sudo systemctl start sshd, sudo systemctl enable sshd [39]. Después se debe configurar el archivo sshd\_config de acuerdo con la personalización que se desee dar y por último se reinicia el servicio para guardar los cambios con el comando sudo systemctl restart sshd

Por otra parte, se configura el firewall para permitir el puerto SSH configurado con el comando sudo ufw allow puerto/tcp:

* **Consultar que es Lynis y su propósito en la auditoría de seguridad.**

Lynis es una herramienta de código abierto para auditorías de seguridad, enfocada en sistemas operativos basados en Unix, como Linux y macOS. Su objetivo principal es analizar la seguridad del sistema, detectar vulnerabilidades y ofrecer sugerencias para optimizar la configuración y reforzar la protección frente a posibles amenazas[40].

El propósito de Lynis en la auditoría de seguridad es el siguiente:

* Auditorías de seguridad: Lleva a cabo análisis detallados del sistema para identificar configuraciones vulnerables, software desactualizado y posibles fallas de seguridad.
* Pruebas de penetración: Facilita a los profesionales de seguridad la identificación y evaluación de vulnerabilidades que podrían ser aprovechadas por atacantes.
* Fortalecimiento del sistema: Ofrece recomendaciones específicas para optimizar la configuración del sistema, mejorando su capacidad de resistir ataques.
* Cumplimiento normativo: Ayuda a comprobar el cumplimiento de estándares y regulaciones de seguridad, garantizando que el sistema siga las mejores prácticas y normativas vigentes.