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 línea, con el objetivo de obtener información relevante para la seguridad del sistema y asegurar una configuración adecuada mediante hardening. Todos los comandos utilizados se presentan en el Anexo A (página 6).

3.1 Información del sistema

Se realizó la identificación del sistema operativo con el objetivo de conocer la distribución instalada, versión del kernel y arquitectura del sistema.

3.2 Gestión de usuarios y grupos

Se creó un usuario local y posteriormente se verificó su identificador de usuario (UID) y grupos al que pertenece (GID).

El análisis evidenció que el sistema asignó automáticamente un UID y GID dentro del rango usuario estándar, también así este usuario pertenece a grupos sin privilegios administrativos, confirmando que el usuario fue creado conforme a la configuración por defecto del sistema y sin acceso elevado. (ver Figura 1)

Desde una perspectiva de seguridad, la validación de UID y grupos resulta importante para detectar usuarios desconocidos o con privilegios elevados que podrían representar un riesgo para el sistema.

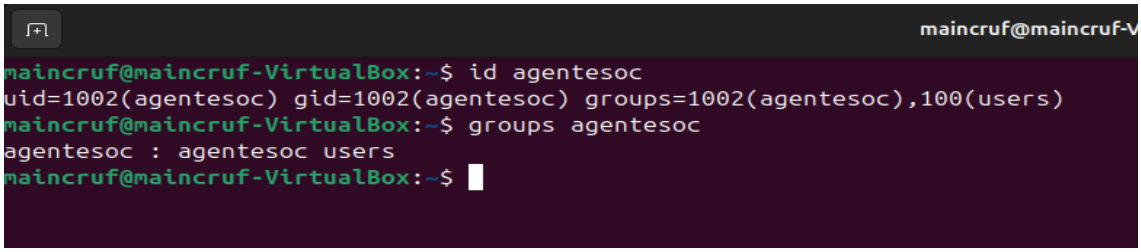

Figura 1. Identificación de un usuario y grupos al que pertenece.

3.3 Permisos de archivos

Se identificó y se modificó los permisos de un archivo de texto nuevo, con el objetivo de conocer las reglas que tienen.

Durante el proceso de análisis, al principio se identificó que el documento tenía permisos de uso compartido pero restringido. Posteriormente, se cambiaron los permisos para que el usuario que creó el archivo solo tenga acceso a él, verificando que los cambios tuvieron validez. (ver Figura 2)

Esto resulta relevante para proteger archivos críticos del sistema, reduciendo riesgos de seguridad.

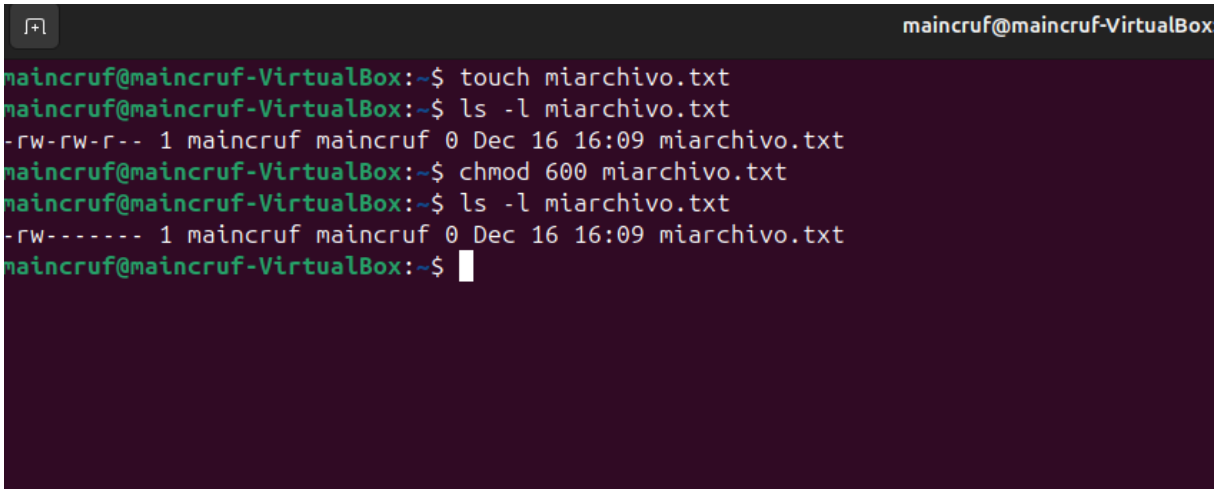

Figura 2. Creación y cambio de permisos de un archivo.

3.4 Procesos del sistema

Se realizó la revisión de los procesos en ejecución que se encuentran en el sistema. Además, dado que el archivo es extenso, se utilizó un filtro para solo mostrar los procesos ssh. El análisis reflejó que los procesos ssh funcionan en segundo plano, indicando el usuario al cual están asociados, el PID asignado, los recursos que consume del sistema y finalmente la hora de su ejecución. (ver Figura 3)

A nivel de monitoreo de seguridad, es crucial conocer qué procesos están activos, y asimismo conocer la información completa para un mayor control.

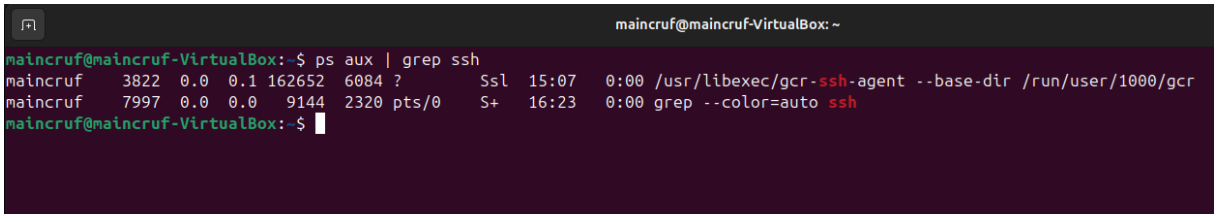

Figura 3. Identificación un proceso en específico.

3.5 Servicios del sistema

Se verificó el estado del servicio SSH, además de desactivar servicios innecesarios, con el fin de incrementar la seguridad del sistema.

Los resultados mostraron que el servicio SSH está instalado, pero inactivo. Además, no está configurado para iniciarse automáticamente cuando arranque el sistema, identificando que el servicio puede activarse solo cuando haya una conexión (socket), manteniendo la disponibilidad cuando es requerido. Por otra parte, se deshabilitó un servicio vulnerable y no activo (CUPS), configurando que el servicio de impresión solo puede activarse bajo demanda a través de sus unidades asociadas. (ver Figura 4)

Este tipo de verificación permite reducir la superficie de ataque del sistema, evitando servicios no requeridos se ejecuten al iniciar el sistema.

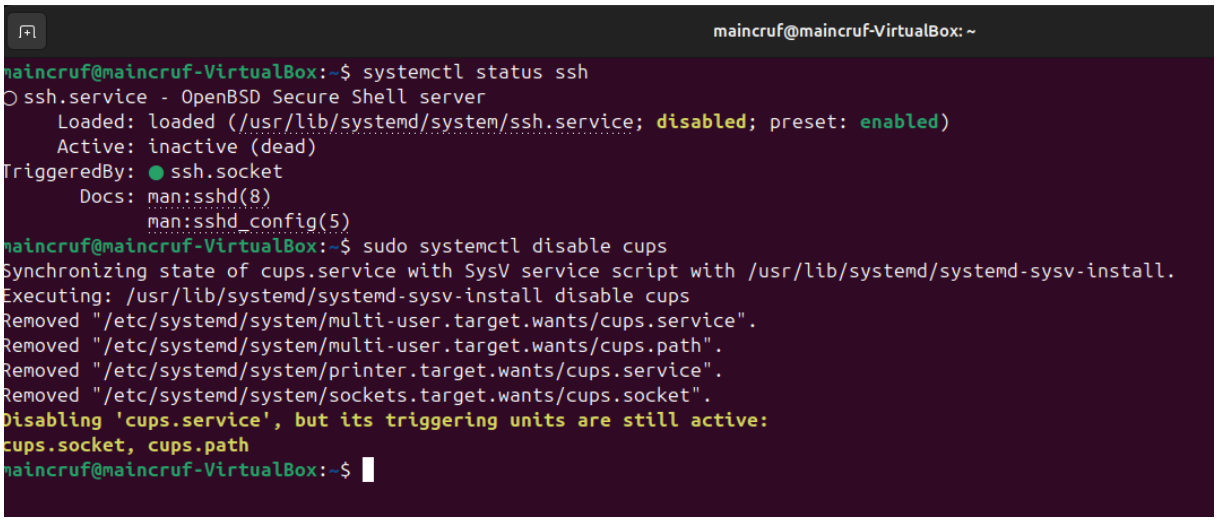

Figura 4. Verificación del estado del servicio ssh y desactivación de servicios.

3.6 Actualizaciones y revisión de firewall

Se actualizó el sistema con los más recientes repositorios. Por otra parte, se examinó el estado y las reglas actuales del Firewall con el propósito de encontrar algunas vulnerabilidades.

Se observó que el firewall se encuentra activo, y que le registro de eventos solo registra eventos básicos de la actividad firewall. Además, se identificaron las políticas por defecto del firewall como ser conexiones entrantes que se bloquean por defecto, conexiones salientes que se permiten por defecto, el firewall no afecta el tráfico que existe entre interfaces y 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)

Desde una perspectiva de seguridad, mantener el sistema actualizado es crucial para reducir la exposición a vulnerabilidades, mientras que la correcta configuración y revisión del firewall ayuda a controlar el tráfico de red y prevenir accesos no autorizados.

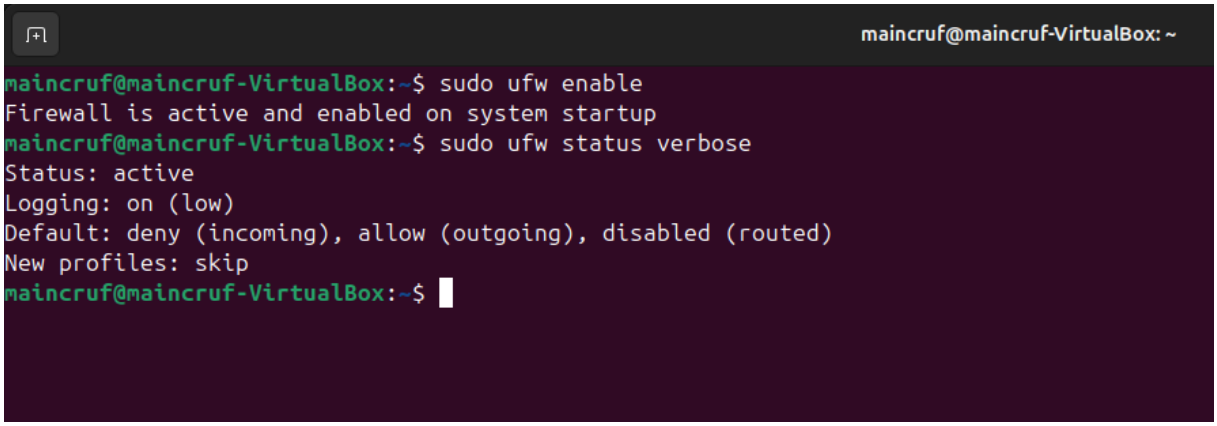

Figura 5. Estado del Firewall

3.7 Registro de eventos (logs)

Se consultaron las últimas líneas del archivo auth.log, con el objetivo de identificar actividades sospechosas.

Se identificó que el usuario maincruf inicio sesiones como sudo, además de ejecutar la consulta en una terminal interactiva para la consulta del archivo auth.log. Posteriormente, se observaron servicios automatizados CRON, dando como resultado que no se identificaron intentos fallidos de autenticación ni comportamientos extraños, revelando un uso legítimo del sistema. (ver Figura 6)

Conocer los logs de un archivo importante como este, logra facilitar la identificación de posibles ataques o eventos sospechosos ejecutándose.

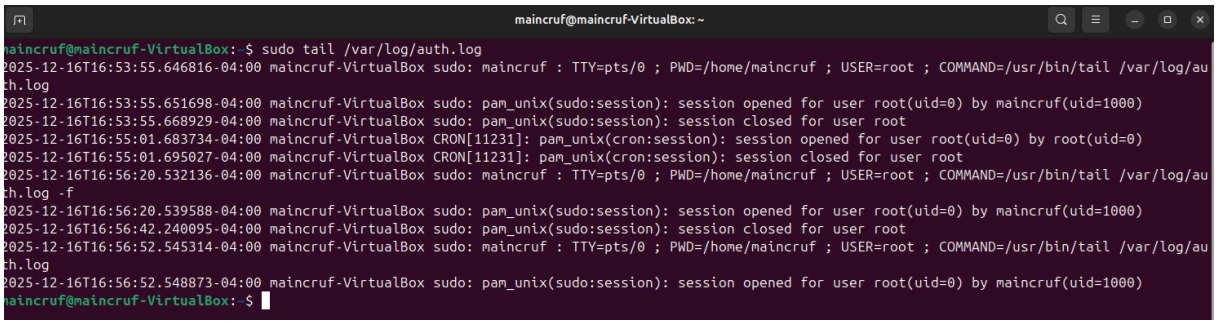

Figura 6. Registros de autenticación

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. Aparte 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.

Anexo A – Comandos Utilizados

lsb_realease -a

Uname -a

cat /etc/passwd

sudo add user agentesoc

id agentesoc

groups agentesoc

touch miarchivo.txt

ls -l miarchivo.txt

chmod 600 miarchivo.txt

ps aux

ps aux | grep ssh

systemctl status ssh

sudo systemctl disable cups

sudo apt update && sudo apt upgrade

sudo afw status verbose

sudo tail var/log/auth.log