Registros de eventos de autenticación y control de acceso.

1. Objetivo. – Analizar los diferentes registros de eventos de autenticación en Linux, para detectar posibles funciones anómalas y accesos no autorizados.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

3. Metodología / Análisis realizado

Esta sección describe el análisis realizado sobre los logs de autenticación del sistema Linux mediante comandos de línea, monitoreando y simulando acciones sospechosas. Todos los comandos utilizados se presentan en el Anexo A (página 6).

3.1 Verificación de la existencia de logs.

Se identificaron los principales registros de eventos del sistema ubicados en el directorio estándar de logs. Entre los más relevantes se encuentran auth.log, encargado de registrar eventos de autenticación y control de acceso; syslog, que almacena eventos generales del sistema; kern.log, relacionado con eventos del kernel; y ufw.log, que registra actividades del firewall. (ver Figura 1)

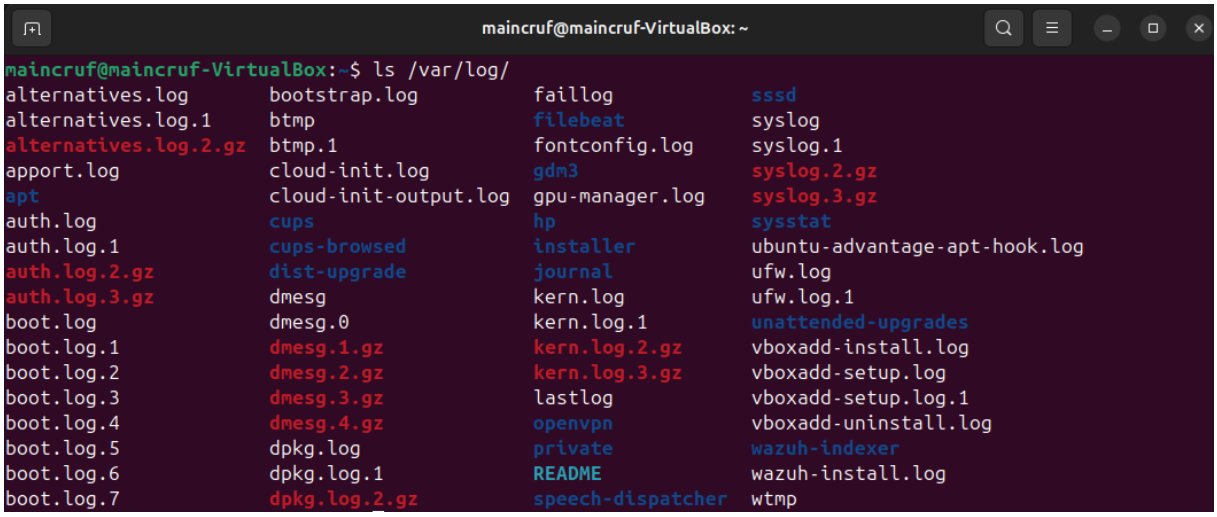

Figura 1. Logs existentes en el sistema

3.2 Análisis de eventos de autenticación y control de acceso

Se analizaron los registros de autenticación del sistema con el objetivo de identificar el uso de privilegios elevados, aperturas y cierres de sesión, así como posibles intentos de acceso no autorizado.

Durante el análisis se observaron eventos asociados a la ejecución legítima de comandos mediante el uso de sudo, así como la apertura y cierre controlado de sesiones privilegiadas. No se identificaron intentos fallidos de autenticación ni actividades que sugieran abuso de privilegios. (ver Figura 2)

El análisis de este registro resulta fundamental para detectar accesos no autorizados, escaladas de privilegios indebidas y otros comportamientos anómalos relevantes para la seguridad del sistema.

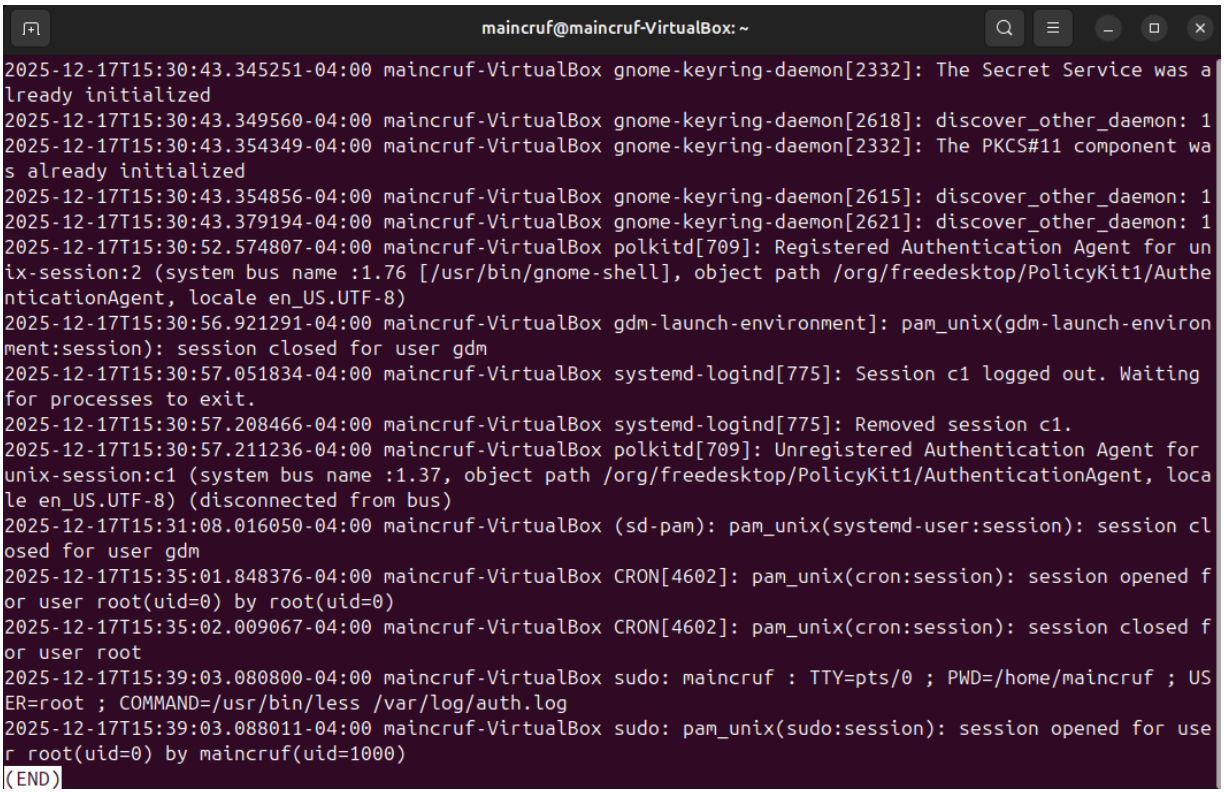

Figura 2. Identificación de un usuario y grupos al que pertenece.

3.3 Simulación y monitoreo de eventos de autenticación sospechosos.

Se simularon varios intentos fallidos de autenticación, con el objetivo de generar eventos para lograr visualizarlos. Por otra parte, se utilizó un filtro en el que solo se muestre los eventos de autenticación fallidos para facilitar el monitoreo.

El análisis permitió identificar varios intentos fallidos de autenticación del usuario Maincruf en un lapso de tiempo demasiado corto, pretendiendo subir sus privilegios a

usuario root, utilizando una terminal virtual como medio. Finalmente, se catalogó como un evento sospechoso leve. (ver Figura 3)

Esto resulta relevante desde el punto de vista de la seguridad, ya que permite diferenciar ataques potencialmente peligrosos de falsos positivos.

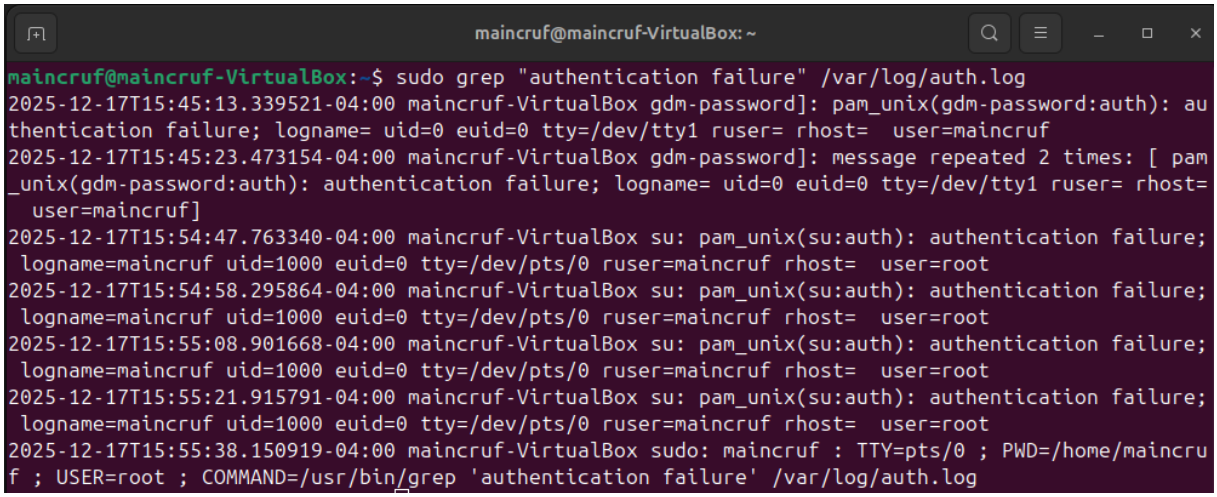

Figura 3. Autenticaciones fallidas.

3.4 Identificación de usuarios inexistentes

Se realizaron varios intentos de autenticación SSH con un usuario inexistente con el propósito de analizar los eventos generados. Posteriormente, se consultó el archivo auth.log con el filtro de usuario no válido para observar dichos eventos, los resultados mostraron la cantidad de intentos, así como la IP y el puerto de origen del usuario no válido, y finalmente el servicio ssh cerró la conexión. (ver Figura 4)

A nivel de un monitoreo de seguridad, estos eventos son muy relevantes para identificar el origen de un ataque malicioso.

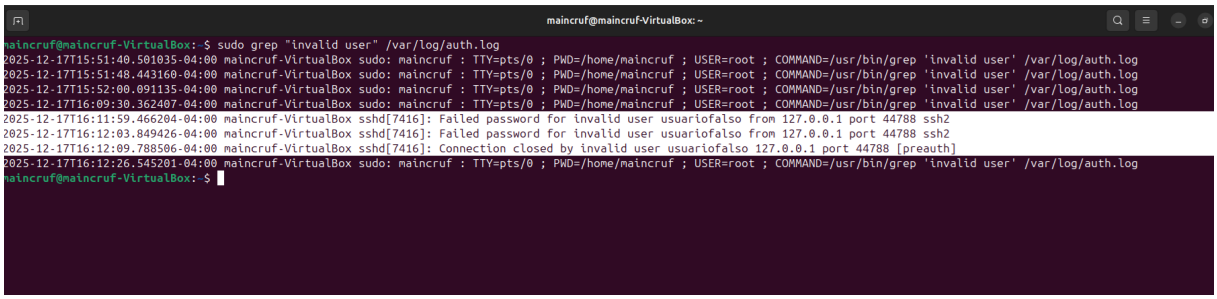

Figura 4. Detección de usuario no válido

3.5 Monitoreo en tiempo real

Se consultaron las últimas líneas del archivo auth.log en tiempo real. Por otra parte, en una segunda terminal, se simularon varios intentos de autenticación fallida para

generar los eventos. Finalmente, se pudieron observar los eventos de autenticación fallida en tiempo real. (Ver Figura 5)

En un escenario de detección temprana, un monitoreo en tiempo real es clave, para una toma de decisiones rápida y oportuna, mejorando así el nivel de seguridad del sistema.

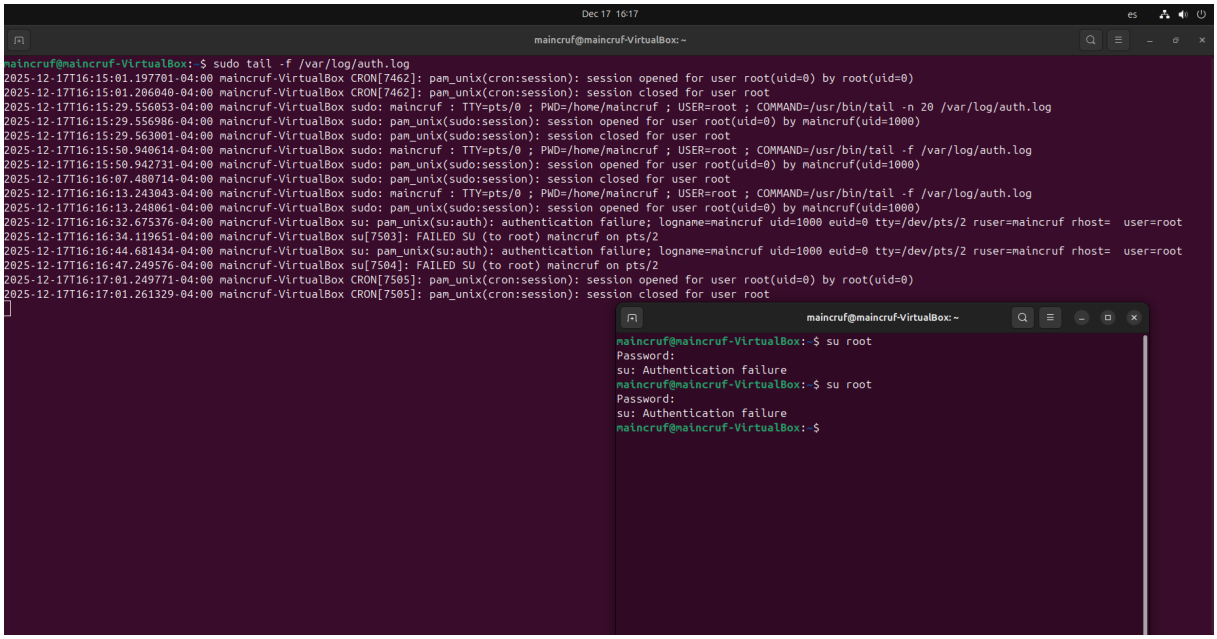

Figura 5. Monitoreo en tiempo real.

3.6 Identificación de fuerza bruta

Se simularon conexiones SSH con un usuario falso para generar un evento de fuerza bruta. Asimismo, se pudo identificar el origen del ataque y el número de veces que se realizó. (ver Figura 6)

En un contexto de monitoreo, esta información es altamente relevante, ya que se pueden tomar medidas preventivas sobre la IP de origen del ataque, además de analizar si es un falso positivo.

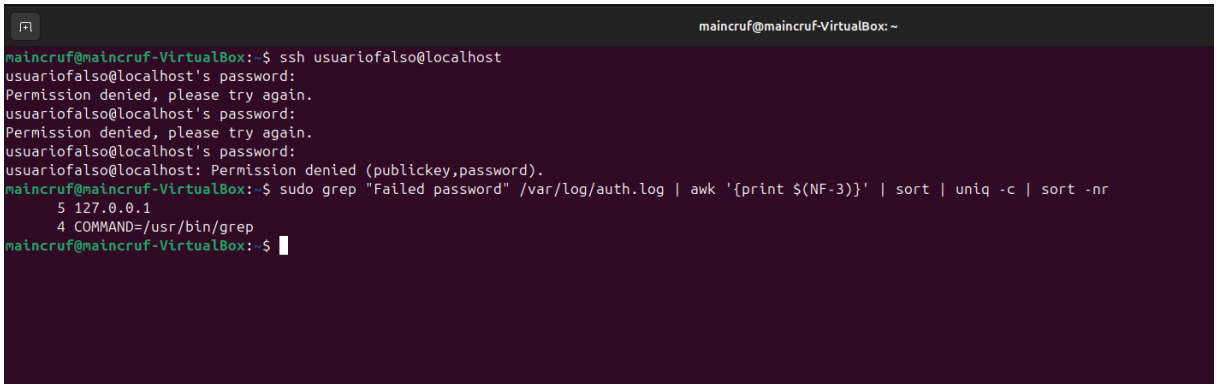

Figura 6. Origen IP del ataque y cantidad de autenticaciones fallidas.

4. Acciones recomendadas

Ante la detección de múltiples autenticaciones fallidas e intentos de fuerza bruta, se recomienda aplicar las siguientes medidas:

- Confirmar si hubo accesos exitosos posteriores a los intentos fallidos.
- Bloquear temporalmente la IP origen del ataque.
- Forzar cambio de credenciales del usuario afectado.
- Deshabilitar el login SSH para el usuario root.
- Implementar un mecanismo de protección contra fuerza bruta (fail2ban).

5. Resultados obtenidos

En este laboratorio se identificaron varios archivos de registros en el sistema, enfocándose principalmente en el análisis del archivo auth.log para diferenciar los eventos relevantes del ruido. Además, se utilizaron varios comandos en Linux y varias simulaciones de intentos fallidos de autenticación, con el fin de comprender el comportamiento de los eventos que se registran en el sistema.

Como resultado, fue posible identificar distintos registros importantes al momento de detectar posibles ataques o intentos de fuerza bruta, observando tanto el origen como la cantidad de intentos realizados. Si bien un número reducido de intentos fallidos puede corresponder a errores del usuario, patrones repetitivos o distribuidos en el tiempo pueden indicar intentos de fuerza bruta, especialmente cuando afectan a servicios expuestos como SSH. Finalmente, todas estas actividades contribuyeron a mejorar la perspectiva de seguridad que debe tenerse al analizar eventos de autenticación y control de acceso.

6. Reflexión final

Este laboratorio permitió comprender la importancia de monitorear, conocer e interpretar los eventos registrados en los procesos de autenticación y control de acceso, aplicando lógica y análisis para determinar si se trata de eventos potencialmente sospechosos o simples falsos positivos. Si bien un SIEM facilita la visualización de este tipo de eventos, la ausencia de esta herramienta obliga a conocer y utilizar comandos en Linux, así como a interpretar manualmente los registros, lo cual fortalece el criterio analítico y la seguridad del sistema.

Anexo A – Comandos Utilizados

ls /var/log/

sudo less /var/log/auth.log

sudo grep “authentication failure” /var/log/auth.log

sudo grep “invalid user” /var/log/auth.log

sudo tail -f /var/log/auth.log

su root

ssh usuariofalso@localhost

sudo grep “Failed password” /var/log/auth.log | awk ‘{print $(NF-3)}’ | sort | uniq -c | sort -nr