Bash básico para SOC

1. Objetivo. – Crear un script para recopilar y mostrar información relevante del sistema, incluyendo intentos fallidos de autenticación, usuarios con privilegios elevados y servicios activos, con el fin de apoyar tareas básicas de monitoreo.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

3. Configuración

3.1 Preparación del entorno y creación de script

En primer lugar, se creó una carpeta destinada a almacenar el script de monitoreo. Posteriormente, se desarrolló el script utilizando el editor nano en Linux, dentro de este script se introdujeron distintos comandos orientados a tareas básicas de monitoreo, tales como intentos fallidos de login, identificación de usuarios con UID 0 (privilegios root) y la enumeración de servicios activos en el sistema. (ver Figura 1)

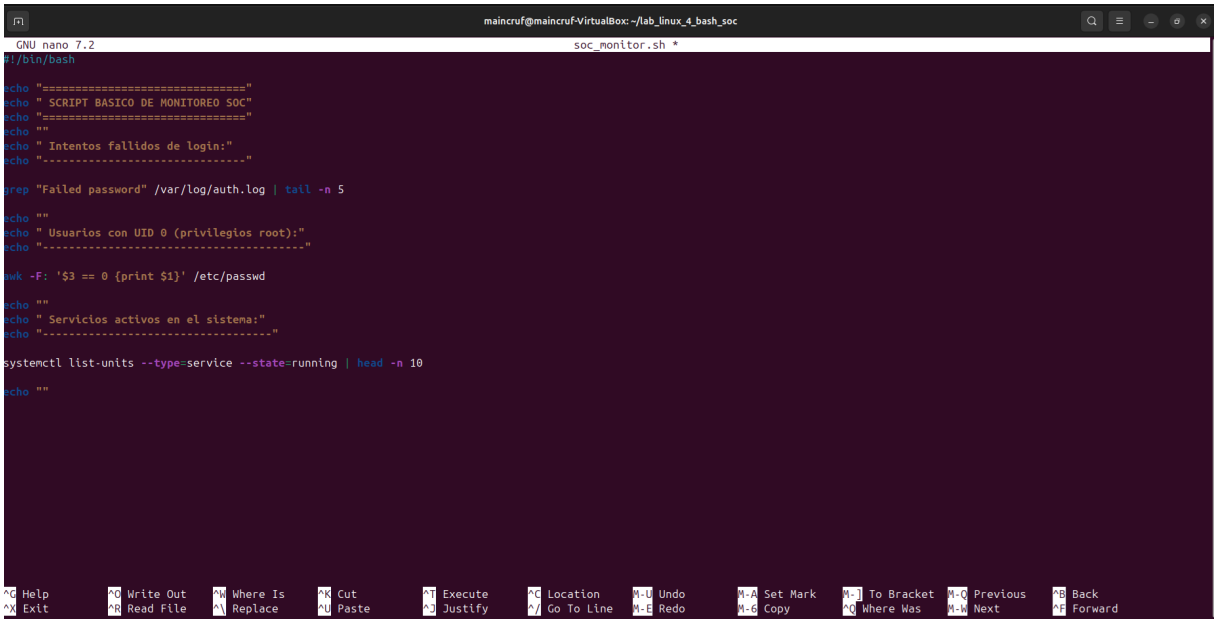

Figura 1. Creación de script de monitoreo.

4. Verificación Técnica

4.1 Permisos y ejecución de script de monitoreo

Se modificaron los permisos del script para permitir su correcta ejecución. Durante la ejecución, el script mostró los registros de autenticación y servicios activos del sistema. Además, no se identificaron usuarios con privilegios elevados como usuarios root. Con base en los resultados obtenidos, se concluyó que el script funcionó de manera correcta y cumplió con los objetivos. (Ver figura 2)

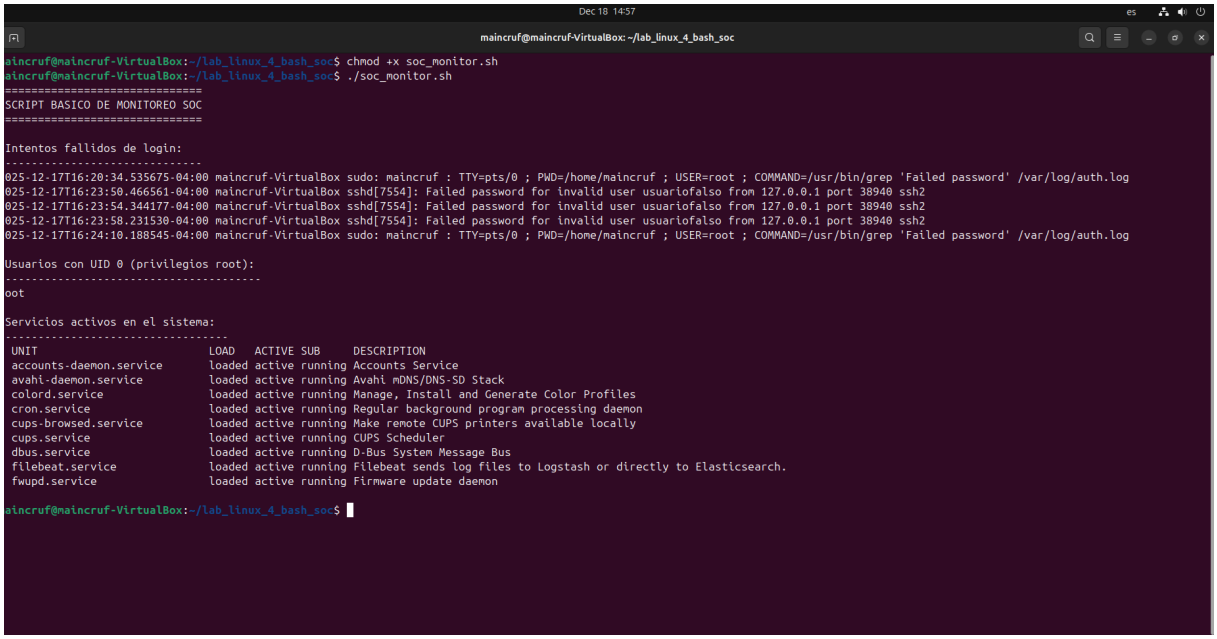

Figura 2. Resultado de la ejecución de scritp de monitoreo.