**PRÁCTICA N°5**

**TEMA: “MONITOREO Y ANALISIS DE EVENTOS DE SEGURIDAD”**

**1. OBJETIVOS**

1.1 Familiarizar al estudiante en la navegación y filtración de registros en el visor de eventos.

1.2 Identificar patrones de actividades sospechosas o no autorizadas.

1.3 Introducir al estudiante en la propuesta de medidas correctivas y preventivas basadas en los hallazgos del análisis de logs.

**5.INFORME**

5.1 ¿Analizar los resultados de la práctica?

#### **Resultado Evento 4624 (Inicio de sesión exitoso)**

En la Figura 1 el evento 4624 se observa que el usuario logro autenticarse correctamente en el sistema, en varias ocasiones dependiendo el entorno de trabajo del usuario esto puede ser normal o puede indicar una vulnerabilidad.

El evento debe analizarse en conjunto con los datos del usuario, la hora y la IP de origen para confirmar si son accesos legítimos o existen un patrón sospechoso.

Interfaz de usuario gráfica, Tabla

Descripción generada automáticamente

Figura 1: Evento 4624

#### **Resultado Evento 4625 (Error de inicio de sesión)**

En la Figura 2 se observa el evento 4625, señalando que hubo un intento fallido de inicio de sesión del sistema, este intento puede deberse a contraseñas incorrectas o accesos no autorizados, analizando el intento fallido en un periodo corto se identifica que es el mismo usuario ingresando una contraseña errónea debido a un error de digitación.

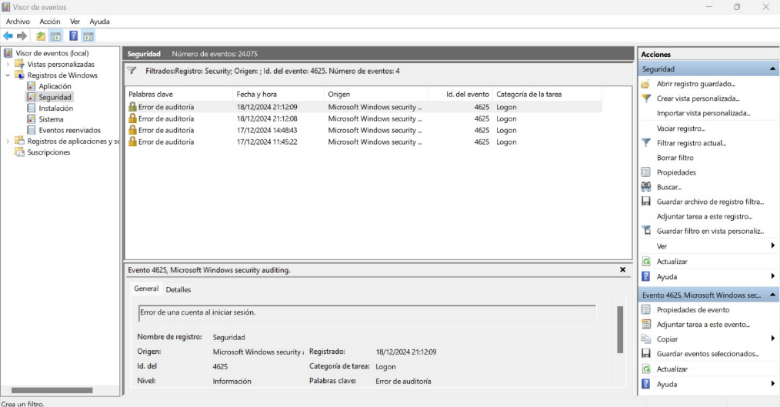


Figura 2:Evento 4625

#### **Resultado Evento 4672 (Privilegios especiales asignados durante el inicio de sesión)**

En la Figura 3 señala que al iniciar sesión el usuario a este se le asignado privilegios de administración, este tipo de acceso se debe monitorear cuidadosamente dado que los usuarios con privilegios administrativos pueden tener capacidad de modificar configuraciones críticas del sistema.

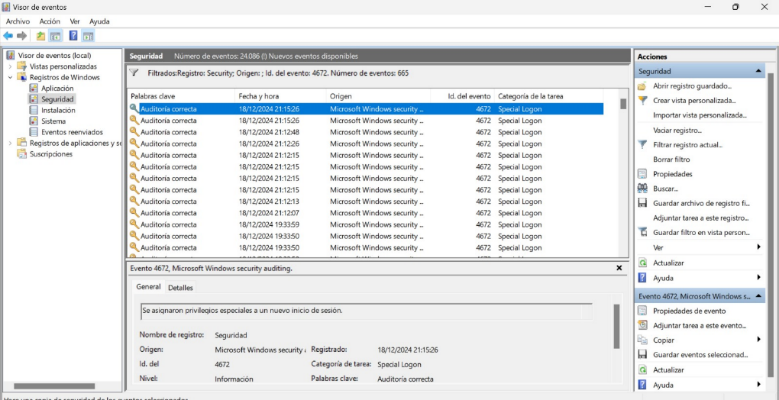


Figura 3:Evento 4672

En este caso el usuario cuanta con privilegios administrativos con el fin realizar esta práctica de laboratorio, los privilegios dependerán del área de trabajo y su rango.

5.2 Evaluar la importancia o criticidad de los eventos encontrados.

Los eventos encontrados nos indican el acceso del usuario al sistema el cual ha tenido algunos fallos por digitar de manera errónea la contraseña, muchos ingresos al sistema esto se da mas en empresas o corporativos dado que los usuarios no suelen estar siempre sen el dispositivo.

5.3 Que medidas preventivas o correctivas se recomienda basándose en los resultados.

Monitorear frecuente mente los eventos para encontrar anomalías o patrones repetitivos que no pertenezcan al usuario, de esta manera se reduce el riesgo de ataque a la organización.