**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.

**2. PREPARATORIO**

***2.1 Consultar que es un log o registro de eventos en un sistema operativo?***

Un log es un archivo o una base de datos del sistema operativo en la cual se almacena secuencias cronológicas de eventos que ocurren en el sistema, estos eventos puede ser el inicio de sesión errores de hardware o software o actualizaciones del sistema [1].

Estos eventos ayudan a verificar el rendimiento del estado del sistema como si la seguridad fue alterada [1].

***2.2 Investigar que es un visor de eventos en Windows y cómo se accede a él?***

El visor de eventos es una herramienta que permite a los administradores monitorear los eventos registrados en el sistema operativo [2].

Acceso al Visor de Eventos:

1. Desde el menú de inicio: Escribe "Visor de eventos" en la barra de búsqueda y selecciónalo [2].
2. Combinación de teclas: Presiona Win + X, selecciona "Administrador de dispositivos" y luego "Visor de eventos" [2].
3. Ejecutando un comando: Abre la ventana de ejecución (Win + R), escribe eventvwr y presiona Enter [2].

***2.4 Enumerar ejemplos de eventos que pueden auditarse y su importancia? (mínimo 3)***

1. Inicio y Cierre de sesión de un usuario: Se rastrea el acceso del usuario al sistema [3].

2. modificación de archivos: Cambios o modificaciones en archivos críticos y sensibles [3].

3. Cambios en la configuración de seguridad: Se monitorea cambios en las políticas de seguridad de la compañía u organización [3].

Bibliografía

[1] C. Prosise, *Incident response & computer forensics*, 2nd ed. New York: McGraw-Hill/Osborne, 2003.

[2] M. Burnett, G. Giuseppini, y J. Faircloth, *Microsoft Log Parser Toolkit: A Complete Toolkit for Microsoft’s Undocumented Log Analysis Tool*, 1 st. 2005.

[3] Karl-Bridge-Microsoft, «Event Types - Win32 apps». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://learn.microsoft.com/en-us/windows/win32/eventlog/event-types