Actividad Práctica: Análisis de Sucesos con el Visor de Eventos de Windows

Objetivo General: Capacitar al alumnado para utilizar el Visor de Eventos de Windows como herramienta fundamental para la detección, seguimiento y análisis de la actividad de un sistema, identificando sucesos relevantes para la administración y la seguridad informática.

Competencias Asociadas (del módulo MF0488_3):

- Detectar incidentes de seguridad de forma activa y preventiva.
- Aplicar procedimientos de análisis de la información ante una incidencia detectada.
- Realizar la recogida de evidencias para el análisis de un incidente.

Escenario: Formas parte del equipo técnico de TI. Una persona usuaria informa que ha notado "cosas raras" en su equipo últimamente: programas que se cierran solos y la sospecha de que alguien ha podido intentar acceder a su cuenta. Tu misión es utilizar el Visor de Eventos para investigar estas afirmaciones y crear un informe con tus hallazgos.

Recursos Necesarios:

- Un ordenador con sistema operativo Windows (10 u 11).
- Permisos de administración local para poder ver todos los registros y realizar acciones.

Desarrollo de la Actividad (Pasos Guiados)

Parte 1: Familiarización con la Herramienta (15 minutos)

1. **Abrir el Visor de Eventos:**
    - Pulsa la tecla de `Windows` + `R` para abrir el cuadro "Ejecutar".
    - Escribe `eventvwr.msc` y pulsa "Aceptar".
2. **Explorar la Interfaz:**
    - En el panel izquierdo, despliega la carpeta **"Registros de Windows"**.
    - Identifica los cinco registros principales y describe brevemente su propósito:
        - **Aplicación:** Eventos reportados por los programas instalados.
        - **Seguridad:** Eventos relacionados con la seguridad (inicios de sesión, acceso a recursos). *Nota: Requiere auditoría activada.*
        - **Instalación:** Eventos relacionados con la instalación de software y actualizaciones.
        - **Sistema:** Eventos reportados por los componentes del sistema operativo.
        - **Eventos reenviados:** (Vacío por defecto) Para eventos de otros equipos.

Parte 2: Generación y Detección de Eventos (30 minutos)

Quien realice la actividad deberá efectuar las siguientes acciones en su equipo y, a continuación, encontrar el evento correspondiente.

Acción 1: Intento de Inicio de Sesión Fallido

1. **Generar el evento:** Bloquea tu sesión de Windows (`Windows` + `L`). En la pantalla de inicio de sesión, intenta acceder introduciendo una contraseña incorrecta a propósito. Vuelve a iniciar sesión con tu contraseña correcta.
2. **Detectar el evento:**
    - Ve al registro de **Seguridad**.
    - Busca el evento con **ID de evento 4625**. Este ID corresponde a "No se pudo iniciar sesión en una cuenta".
    - Analiza los detalles del evento: fíjate en el nombre de la cuenta (`Nombre de cuenta`) y el origen del intento de inicio de sesión (`Nombre de la estación de trabajo`).

Acción 2: Cierre Inesperado de una Aplicación

1. **Generar el evento:** Abre una aplicación sencilla como la "Calculadora" o el "Bloc de notas". A continuación, abre el "Administrador de tareas" (`Ctrl` + `Shift` + `Esc`), busca el proceso de la aplicación, haz clic derecho sobre él y selecciona "Finalizar tarea".
2. **Detectar el evento:**
    - Ve al registro de **Aplicación**.
    - Busca un evento de nivel "Error" que se haya producido en el momento en que forzaste el cierre. Generalmente tendrá un **ID de evento 1000** (Error de aplicación) o **1002** (La aplicación dejó de responder).
    - Observa los detalles para ver el nombre de la aplicación que falló.

Acción 3: Cambio de la Hora del Sistema

1. **Generar el evento:** Haz clic derecho en el reloj de la barra de tareas y ve a "Ajustar fecha y hora". Desactiva la opción de "Establecer la hora automáticamente" y cambia la hora manualmente a cualquier otro valor. Vuelve a activar la hora automática.
2. **Detectar el evento:**
    - Ve al registro de **Sistema**.
    - Utiliza la opción "Filtrar registro actual..." del panel derecho. En "Orígenes del evento", selecciona `Kernel-General` o `Time-Service`.
    - Busca un evento que indique "La hora del sistema ha cambiado". El **ID de evento 1** de `Kernel-General` suele registrar este suceso.

Acción 4: Borrado de Registros (¡Una acción muy sospechosa!)

1. **Generar el evento:** En el Visor de Eventos, selecciona el registro de **Seguridad**. En el panel derecho, haz clic en **"Vaciar registro..."**. Te pedirá confirmación; puedes guardar una copia o simplemente "Borrar".
2. **Detectar el evento:**

- ¡El evento que registra el borrado no se guarda en el mismo log que se ha borrado! Ve al registro de **Sistema**.
- Busca el evento con **ID 1102**. El texto del evento será claro: "Se borró el registro de auditoría de seguridad".
- Este es un evento crítico en una investigación, ya que es una técnica común para ocultar las huellas de un ataque.

Entregable y Evaluación (15 minutos)

Se deberá crear un documento llamado **"Informe de Análisis de Sucesos"** que contenga una tabla como la siguiente, rellenada con la información de cada una de las 4 acciones realizadas:

Acción Realizada	Registro Afectado	ID del Evento	Captura de Pantalla (Detalles del evento)	Importancia del Evento (Breve explicación)
Inicio de sesión fallido	Seguridad	4625	*(Adjuntar captura)*	Indica un posible intento de acceso no autorizado o que alguien ha olvidado su contraseña. Múltiples eventos seguidos son una alerta de ataque de fuerza bruta.
Cierre forzado de App	Aplicación	1000 / 1002	*(Adjuntar captura)*	Ayuda a diagnosticar problemas de software. Podría indicar inestabilidad del programa o del sistema, o una acción de malware que cierra aplicaciones de seguridad.
Cambio de hora	Sistema	1	*(Adjuntar captura)*	Puede afectar a la autenticación (Kerberos) y a la correcta correlación de logs. Una acción atacante podría cambiar la hora para manipular las marcas de tiempo.

Borrado de logs	Sistema	1102	*(Adjuntar captura)*	Es una bandera roja de seguridad. Indica un intento deliberado de ocultar actividades en el sistema, lo que casi siempre se asocia a una acción maliciosa.

Exportar a Hojas de cálculo

Criterios de evaluación:

- Correcta identificación de los registros y los ID de evento para cada acción.
- Calidad y claridad de las capturas de pantalla.
- Coherencia y precisión en la explicación de la importancia de cada evento.
- Presentación y orden del informe final.
-