**Práctica: Verificar Llamadas al Sistema de una Aplicación en Windows con Process Monitor**

En esta práctica, verificar

emos las llamadas al sistema de una aplicación común, como el **Bloc de Notas (Notepad.exe)**, para observar cómo interactúa con el sistema operativo.

**Paso 1: Descargar Process Monitor**

1. Ve a la página oficial de [Sysinternals Process Monitor](https://docs.microsoft.com/en-us/sysinternals/downloads/procmon) y descarga la herramienta.
2. Extrae el archivo ZIP y abre el programa ejecutando Procmon.exe como administrador.

**Paso 2: Configuración Inicial y Comienzo de la Captura**

1. Al abrir Process Monitor, comenzará a capturar todas las actividades del sistema automáticamente.
2. Verás que el panel principal de Process Monitor muestra todos los eventos en tiempo real, pero necesitamos centrarnos en la aplicación que queremos monitorear (Bloc de Notas).

**Paso 3: Aplicar Filtros para la Aplicación Específica**

1. Haz clic en **Filter** en el menú superior y selecciona **Filter…** para abrir la ventana de configuración de filtros.
2. En la ventana de filtro:
	* Configura el filtro para mostrar solo los eventos de Notepad:
		+ En el primer campo, selecciona **Process Name**.
		+ En el segundo campo, selecciona **is**.
		+ En el tercer campo, escribe notepad.exe.
		+ Haz clic en **Add** para añadir este filtro.
	* Confirma haciendo clic en **OK**.
3. Ahora, Process Monitor mostrará solo los eventos relacionados con notepad.exe.

**Paso 4: Ejecutar la Aplicación Bloc de Notas**

1. Abre el Bloc de Notas en tu computadora. Puedes hacer esto rápidamente presionando Win + R, escribiendo notepad y presionando Enter.
2. Realiza algunas acciones en el Bloc de Notas para generar actividad. Por ejemplo:
	* Escribe algo en el Bloc de Notas.
	* Guarda el archivo en una ubicación (esto generará llamadas al sistema relacionadas con el acceso al archivo).
	* Cierra el Bloc de Notas.

**Paso 5: Observación y Análisis de las Llamadas al Sistema**

1. Regresa a Process Monitor y observa los eventos que se generaron mientras usabas el Bloc de Notas.
2. Cada evento muestra:
	* **Operation**: El tipo de operación realizada, como CreateFile, ReadFile, WriteFile, que representan las llamadas al sistema realizadas por notepad.exe.
	* **Path**: La ruta del archivo o recurso accedido por Notepad.
	* **Result**: Indica si la operación fue exitosa (por ejemplo, SUCCESS) o falló (por ejemplo, ACCESS DENIED).
	* **Detail**: Muestra detalles adicionales sobre la llamada al sistema, como el tamaño de los datos leídos o escritos.

**Paso 6: Analizar un Evento Específico**

1. Para obtener más información sobre una llamada al sistema específica, haz doble clic en cualquier evento que te interese (por ejemplo, CreateFile para el archivo que guardaste).
2. En la ventana de detalles, puedes ver información detallada como:
	* **Nombre del proceso** que generó la llamada.
	* **Parámetros de la operación** (por ejemplo, la ruta completa del archivo, los permisos solicitados).
	* **Tiempo exacto** en que se realizó la llamada.

**Paso 7: Guardar o Exportar los Resultados (Opcional)**

1. Si deseas guardar los resultados para analizarlos más tarde, ve a **File > Save…** en el menú de Process Monitor.
2. Puedes guardar el registro en formato **PML** (formato nativo de Process Monitor) o exportarlo en formato **CSV** o **XML**.

**Ejemplo de Interpretación de Resultados**

Supongamos que observas un evento CreateFile para el archivo que guardaste con el Bloc de Notas. Aquí tienes cómo interpretar la información:

* **Operation**: CreateFile indica que notepad.exe intentó crear o abrir un archivo.
* **Path**: Muestra la ubicación completa del archivo, por ejemplo, C:\Users\Usuario\Documents\archivo.txt.
* **Result**: Si ves SUCCESS, significa que Notepad pudo acceder al archivo con éxito. Si el resultado es ACCESS DENIED, indica que hubo un problema de permisos.
* **Detail**: Puedes ver detalles sobre el tipo de acceso solicitado (lectura/escritura).