PRÁCTICA 3: SYSMON

En equipos servidor y en estaciones de trabajo donde se guarde información confidencial importante se hace necesario monitorizar adecuadamente el sistema y guardar registros de todo lo que pasa, o al menos de lo más importante.

En los sistemas Windows existe una herramienta creada por Microsoft llamada **sysmon**. System Monitor (Sysmon) es un servicio que una vez instalado permanece activo siempre para supervisar y registrar la actividad del sistema en el registro de sucesos de Windows. Sysmon puede registrar sucesos de:

- Procesos que se crean.
- Conexiones de red.
- Cambios en el registro.
- Comandos que se ejecutan.

En una investigación forense estudiaremos los LOGs en general, en particular los que aporta sysmon son de mucho interés dado que se pueden personalizar y generan mucha información sobre lo que acontece en el sistema informático.

Objetivos principales de la práctica:

- **Instalar, configurar, monitorizar y analizar los LOGs generados por sysmon.**

Software a utilizar:

1. Windows 7,8,10 (32 o 64 bits)
2. Sysinternals suite (https://docs.microsoft.com/en-us/sysinternals/downloads/)
3. Fichero de configuración (https://github.com/SwiftOnSecurity/sysmon-config)
4. Sysmon Tools (https://github.com/nshalabi/SysmonTools)

Se pide:

- Instala o utiliza una máquina virtual con Windows (1)
- Descargate la utilidad **sysmon** (2)
- Descargate el fichero de configuración (3)
    - Investiga un poco el contenido del fichero de configuración. Es interesante que veas cómo está estructurado y los ID de los eventos que registra a qué se refiere.
    - Sigue las instrucciones para instalar el servicio en la máquina virtual anterior.
- Una vez habilitado el servicio sysmon, instala algún tipo de software en la máquina virtual como por ejemplo **notepad++.**
- La última parte de sysmon sería el análisis de la información que recoge.
    - Por defecto sysmon guarda los registros en el fichero de eventos en la siguiente ruta: **C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx**

- Abre el fichero con el “**Visor de eventos**”
- Exporta el contenido del fichero a formato **XML** (Menú contextual -> guardar todos los eventos como XML)
- Abre el fichero XML con la utilidad **SysmonViewer** y explora su funcionalidad.