EJERCICIO RESUELTO
Módulo: Sistemas Informáticos

Uso del comando Eventcreate.

Descripción:

Es usted el Administrador de un sistema con Windows.

Imagine que necesita registrar un evento en cualquiera de los archivos de registro de eventos. Esto se puede hacer usando el comando **eventcreate**.

Registrar un evento ayuda a los administradores del sistema a rastrear cosas si algo no ha funcionado de la manera esperada. Con este comando, podemos crear un evento personalizado con identificación y descripción personalizadas. Y podemos registrar el evento en cualquiera de los archivos de registro de eventos (Sistema, Aplicación, Seguridad, etc.).

Investiguemos el uso básico de este comando, de forma que podamos generar un evento desde la línea de comandos de Windows.

Objetivos:

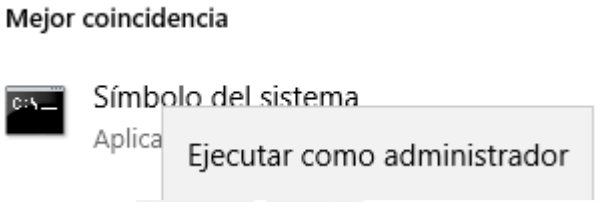
- Generar un evento en un archivo de registro del registro de eventos del sistema operativo.

Recursos:

- Sistema operativo Windows 10 o Windows Server

Resolución:

1. Como un usuario con privilegios de administración, abrimos el símbolo de sistema.



2. Observamos la ayuda del comando **eventcreate**, tecleando **evencreate /?**

```
C:\Users\Administrador.WIN-H93PL3JR9QS>eventcreate /?

EVENTCREATE [/S sistema [/U nombre_usuario [/P [contraseña]]]] /ID IdEvento
            [/L nombre_registro] [/SO nombre_origen] /T tipo /D descripción

Descripción:
    Esta herramienta de línea de comandos permite a un administrador
    crear un id. y mensaje de evento personalizados en el registro
    de eventos especificado.

Lista de parámetros:
    /S    sistema           Especifica el sistema remoto al que conectarse.

    /U    [dominio\]usuario  Especifica el contexto de usuario en el que
                             el comando debe ejecutarse.

    /P    [contraseña]       Especifica la contraseña para el contexto
```

Entre todos los parámetros que podemos usar, vamos a buscar necesarios para generar un evento básico, estos son:

a. **Descripción**, un texto
b. **Identificación**, número de identificador.
c. **Tipo** de evento.
d. Nombre del **archivo de registro** de eventos.

3. Con el parámetro /t, especificamos el tipo de evento, que puede ser un evento de éxito, error, advertencia o información.

```
/T    tipo              Especifica tipo de evento para crear.
                        Los tipos válidos: SUCCESS, ERROR, WARNING,
                        INFORMATION.
```

4. Con el parámetro /id, se especifica el número identificador del evento.

```
/ID   IdEvento          Especifica el id. del  evento. Un id. de
                        mensaje personalizado válido es un valor
                        en el intervalo entre 1 - 1000.
```

5. Con el parámetro /l, se especifica el nombre del registro donde se va a crear el evento, estos registros son los de aplicación (application), seguridad (security), instalación (setup) y sistema (system).

```
/L    nombre_registro   Especifica el registro de evento en
                        el que se creará un evento.
```

6. Con el parámetro /d, especificamos un texto descriptivo que servirá para detallar en que consiste el evento o que finalidad tiene.

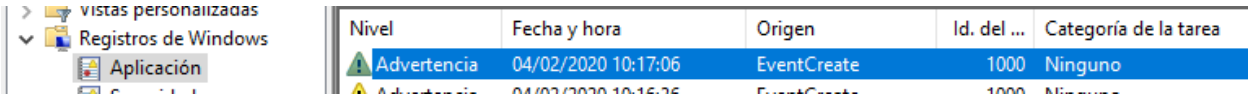
```
/D    descripción       Especifica el texto de la descripción para el
                        nuevo evento.
```

7. Un ejemplo de creación de evento puede ser:

```
C:\Users\Administrador.WIN-H93PL3JR9QS>eventcreate /t warning /id 1000 /l application /d "Evento generado por Administrador"

CORRECTO: se ha creado un evento de tipo 'warning' en el registro 'application'
con 'EventCreate' como origen.
```

8. Este evento se almacenará en el registro de aplicación del visor de eventos:



9. Si abrimos el evento podemos observar sus propiedades y que se ha generado correctamente: