Práctica de laboratorio: Explorar procesos, subprocesos, controles y el registro de Windows

Objetivos

En esta práctica de laboratorio explorarán los procesos, subprocesos y controles con el Explorador de procesos en la suite SysInternals. También utilizarán el Registro de Windows para cambiar un ajuste.

Parte 1: Explorar procesos

Parte 2: Explorar subprocesos y controles

Parte 3: Explorar el Registro de Windows

Recursos necesarios

- 1 Una PC Windows con acceso a internet

Instrucciones

Parte 1: Explorar procesos

En esta parte explorarán procesos. Los procesos son programas o aplicaciones en ejecución. Estudiarán los procesos con el Explorador de procesos en la suite Sysinternals para Windows. También iniciarán y observarán un proceso nuevo.

Paso 1: Descargar la suite SysInternals para Windows.

a. Diríjanse al siguiente enlace para descargar la suite SysInternals para Windows:

   https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

b. Una vez finalizada la descarga, extraigan los archivos de la carpeta.

c. Dejen abierto el navegador web para los pasos siguientes.

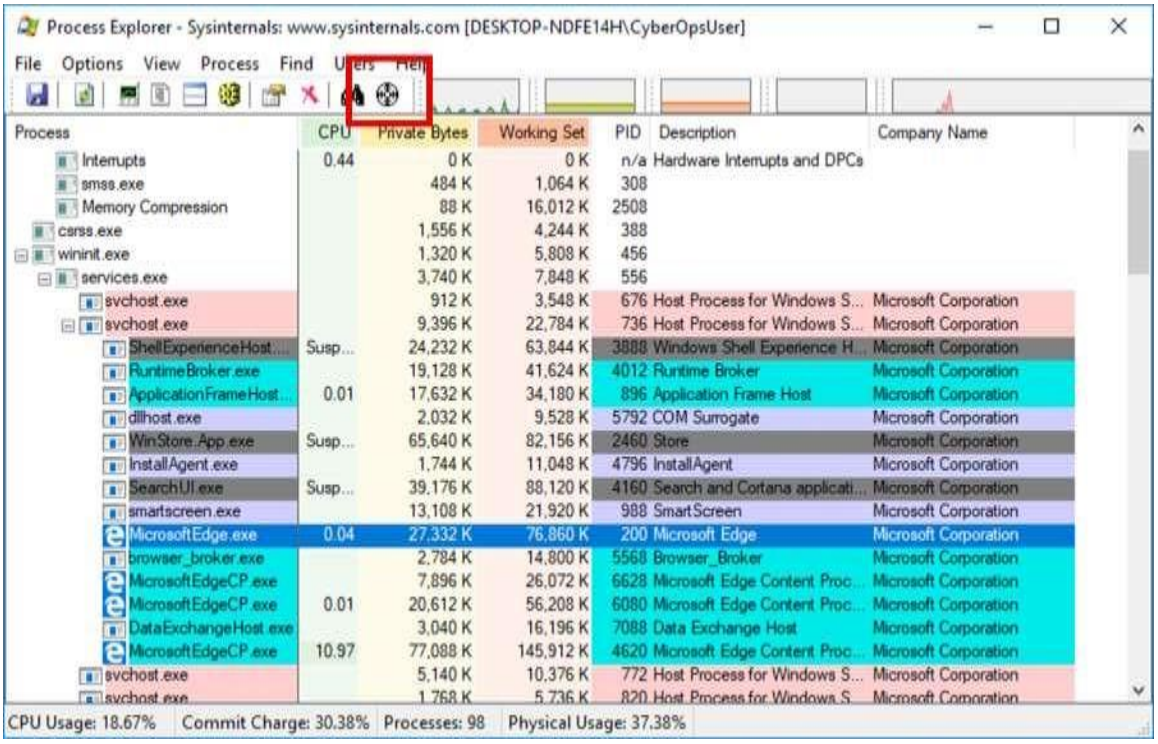
Paso 2: Explorar un proceso activo

a. Diríjanse a la carpeta SysinternalsSuite con todos los archivos extraídos.

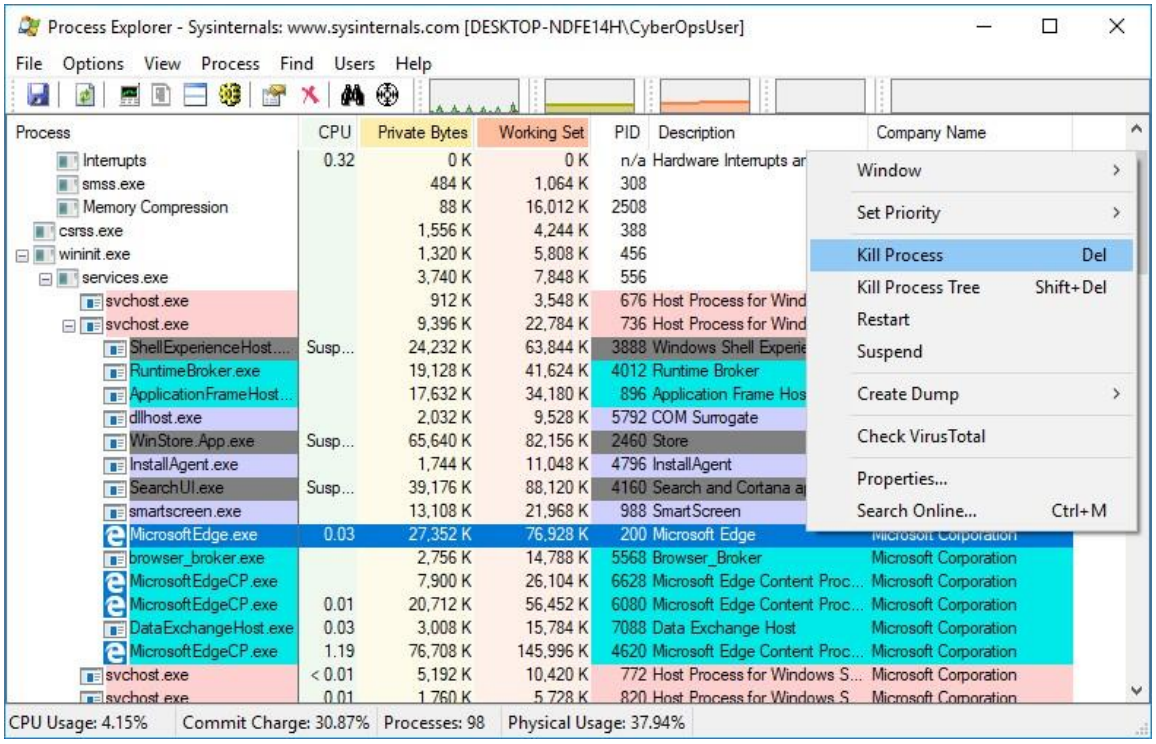
b. Abran **procexp.exe**. Acepten el Acuerdo de licencia de Process Wxplorer cuando el sistema se lo solicite.

c. El Explorador de procesos muestra una lista de los procesos activos actualmente.

d. Para localizar los procesos del navegador web, arrastre el icono **Encontrar proceso de Windows** en la ventana del navegador web. En este ejemplo se utiliza Microsoft Edge.



e. El proceso de Microsoft Edge se puede finalizar desde el Explorador de procesos. Hagan clic derecho sobre el proceso seleccionado y elijan **Kill Process** (Finalizar proceso). Haga clic en **Aceptar** para continuar.



¿Qué sucedió con la ventana del navegador web cuando se finalizó el proceso?

Paso 3: Iniciar otro proceso

a. Abran un símbolo del sistema (**Inicio** buscar **Símbolo del sistema** y seleccionar **Símbolo del sistema**)

b. Arrastre el icono **Encontrar proceso de Windows** en la ventana Command Prompt y localice el proceso resaltado en el explorador de procesos.

c. El proceso correspondiente al Símbolo del sistema es cmd.exe. Su proceso principal es explorer.exe. cmd.exe tiene un proceso secundario: conhost.exe.

d. Diríjanse a la ventana del Símbolo del sistema. Inicien un ping en el cursor y observen los cambios que se producen en el proceso cmd.exe.

¿Qué sucedió durante el proceso de ping?

e. Mientras observan la lista de procesos activos, descubren que el proceso secundario conhost.exe puede ser sospechoso. Para buscar contenido maliciosos, hagan clic derecho sobre **conhost.exe** y seleccionen **Check VirusTotal** (Revisar VirusTotal). Cuando el sistema se los solicite, hagan clic en **Yes** (Sí) para aceptar los Términos de servicio de VirusTotal. Luego hagan clic en **OK** (Aceptar) para ver el siguiente mensaje.

f. Expandan la ventana del Explorador de procesos o desplácense hacia la derecha hasta ver la colu mna de VirusTotal. Hagan clic en el enlace de la columna VirusTotal. Se abre el navegador web predeterminado con los resultados relacionados con el contenido maliciosos de conhost.exe.

g. Hagan clic derecho sobre el proceso cmd.exe y elijan **Kill Process** (Finalizar proceso).

¿Qué sucedió con el proceso secundario conhost.exe?

Parte 2: Explorar subprocesos y controles

En esta parte explorarán subprocesos y controles. Los procesos pueden tener uno o más subprocesos. Un subproceso es una unidad de ejecución en un proceso. Un control es una referencia abstracta a bloques de memoria o a objetos administrados por un sistema operativo. Utilizarán el Explorador de procesos (procexp.exe) en la suite SysInternals para Windows para explorar los subprocesos y controles.

Paso 1: Explorar subprocesos

a. Abran un símbolo del sistema.

b. En la ventana del Explorador de procesos, hagan clic derecho sobre conhost.exe y seleccionen **Properties…** (Propiedades...). Hagan clic en la ficha **Threads** (Subprocesos) para ver los subprocesos activos correspondientes al proceso conhost.exe. Haga clic en **Aceptar** para continuar si se le solicita un cuadro de diálogo de advertencia.

c. Examinen los detalles del subproceso.

¿Qué tipo de información está disponible en la ventana de Propiedades?

d. Haga clic en **Aceptar** para continuar.

Paso 2: Explorar controles.

a. En el Explorador de procesos, hagan clic en **Vista** > seleccionar **Vista de panel inferior** > **Controles** para ver los controles asociados con el proceso conhost.exe.

Examinen los controles. ¿Hacia dónde apuntan los controles?

b. Cierre el Explorador de procesos cuando haya terminado.

Parte 3: Explorar el Registro de Windows

El Registro de Windows es una base de datos jerárquica que almacena la mayoría de los ajustes de configuración del sistema operativo y del entorno del escritorio.

a. Para acceder al Registro de Windows, hagan clic en **Inicio**, busquen **regedit** seleccionen el **Editor del registro**. Hagan clic en **Sí** cuando el sistema les solicite que permitan que esta aplicación efectúe cambios.

El Editor del registro tiene cinco secciones. Estas secciones se encuentran en el nivel superior del registro.

- HKEY_CLASSES_ROOT es en realidad la subclave de Clases de HKEY_LOCAL_MACHINE\Software\. Almacena información utilizada por aplicaciones registradas como la asociación de extensiones de archivos, al igual que datos de un identificador programático (ProgID), ID de clase (CLSID) e ID de interfaz (IID).
- HKEY_CURRENT_USER contiene los ajustes y las configuraciones correspondientes a los usuarios que tienen sesión iniciada.
- HKEY_LOCAL_MACHINE almacena información de configuración específica de la computadora local.
- HKEY_USERS contiene los ajustes y las configuraciones correspondientes a la computadora local. HKEY_CURRENT_USER es una subclave de HKEY_USERS.
- HKEY_CURRENT_CONFIG almacena la información de hardware que se utiliza la computadora local al momento del arranque.

b. En un paso anterior había aceptado el acuerdo EULA correspondiente al Explorador de procesos. Diríjanse a la clave del registro EulaAccepted correspondiente al Explorador de procesos.

Para seleccionar el Explorador de procesos, hagan clic en **HKEY_CURRENT_USER** > **Software** > **Sysinternals** > **Process Explorer**. Desplácese hacia abajo para ubicar la clave **EulaAccepted.** En este momento, el valor correspondiente a la clave de registro EulaAccepted es 0x00000001(1).

c. Hagan doble clic en la clave del registro **EulaAccepted**. En este momento, el dato del valor está definido en 1. El valor de 1 indica que el acuerdo EULA ha sido aceptado por el usuario.

d. Cambien el **1** por un **0** en el dato del Valor. El valor de 0 indica que no se aceptó el EULA. Hagan clic en **OK** (Aceptar) para continuar.

¿Cuál es el valor correspondiente a esta clave del registro en la columna Data (Datos)?

e. Abran el **Explorador de procesos**. Diríjanse a la carpeta en la que hayan descargado SysInternals. Abran la carpeta **SysInternalsSuite** y, luego, abran **procexp.exe**.

¿Qué vieron cuando abrieron el Explorador de procesos?