Tema3.3.2.11.EnriqueGomezTagle

lunes, 12 de febrero de 2024 23:22

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

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

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

Ventana cerrada

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?

   Ping generó un proceso hijo de CMD.

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 columna 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?

   Al finalizar CMD se detuvo tambien conhost.

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?

   Hora, info de seguridad, rendimiento, cadena

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?

   Archivos, claves de registro subprocesos

b. Cierre el Explorador de procesos cuando haya terminado.

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)?

   0x