Lab - Exploring Processes, Threads, Handles, and Windows Registry

Objectives

In this lab, you will explore the processes, threads, and handles using Process Explorer in the SysInternals Suite. You will also use the Windows Registry to change a setting.

Part 1: Exploring Processes

Part 2: Exploring Threads and Handles

Part 3: Exploring Windows Registry

Required Resources

- 1 Windows PC with internet access

Instructions

Part 1: Exploring Processes

In this part, you will explore processes. Processes are programs or applications in execution. You will explore the processes using Process Explorer in the Windows SysInternals Suite. You will also start and observe a new process.

Step 1: Download Windows SysInternals Suite.

a. Navigate to the following link to download Windows SysInternals Suite:

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

b. After the download is completed, extract the files from the folder.

c. Leave the web browser open for the following steps.

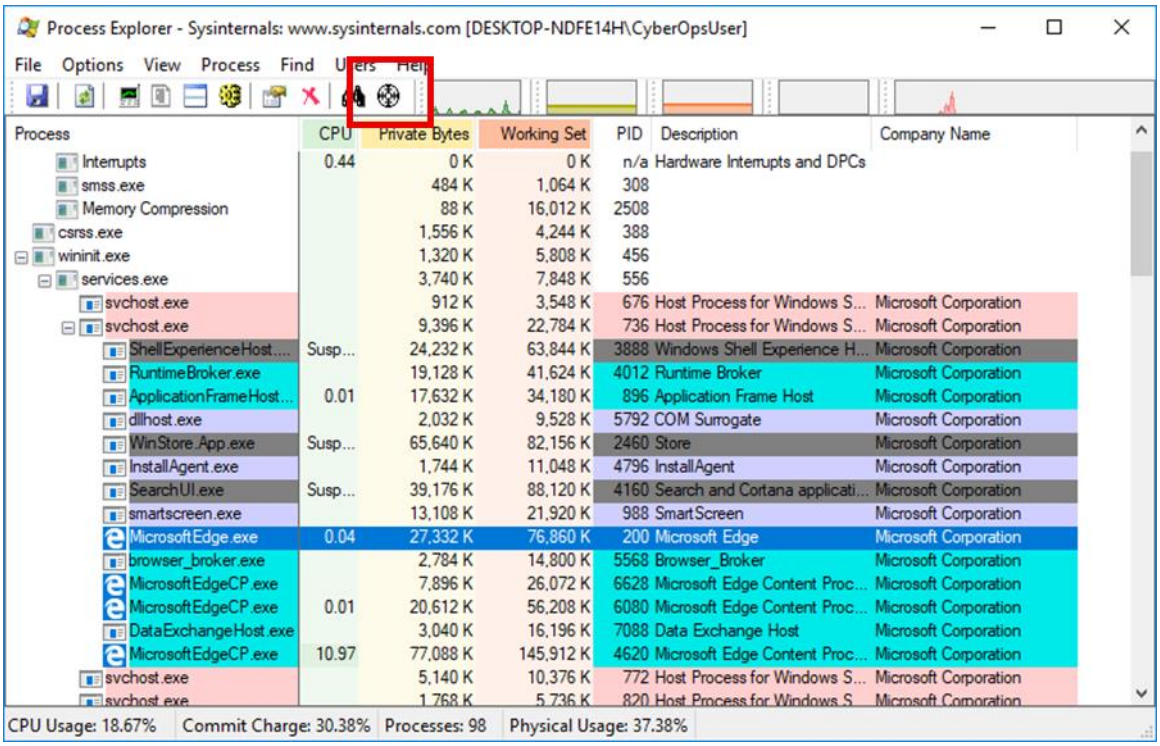
Step 2: Explore an active process.

a. Navigate to the SysinternalsSuite folder with all the extracted files.

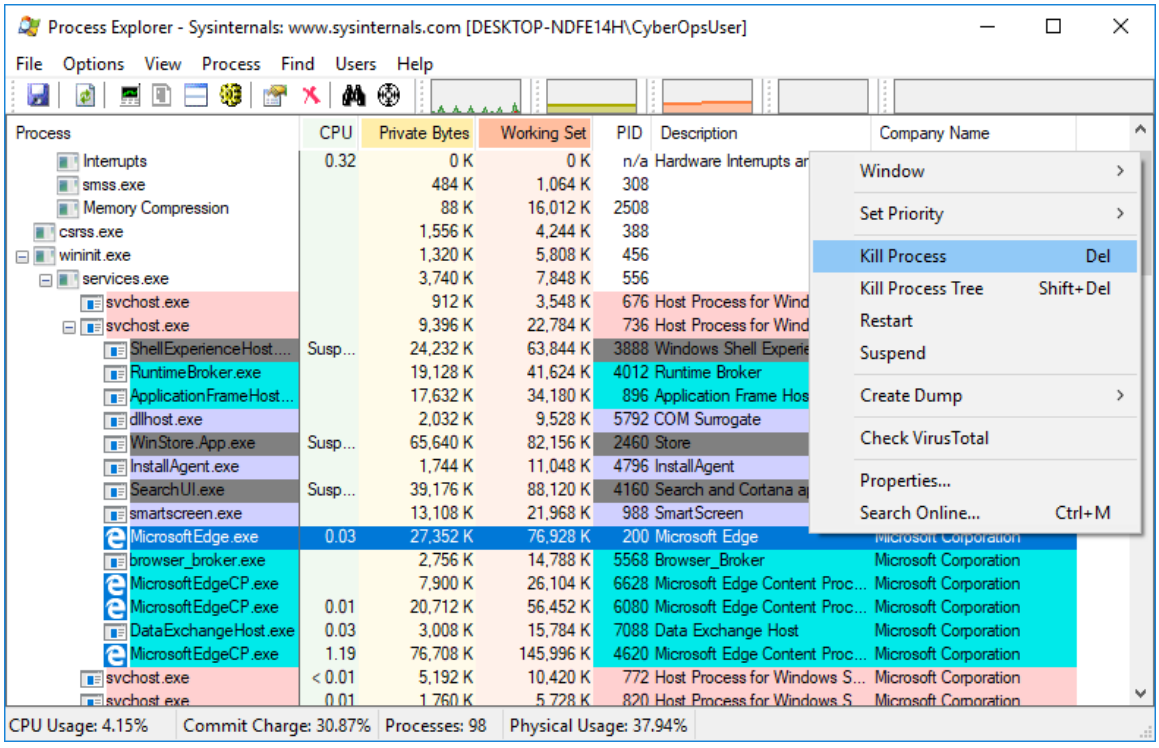
b. Open **procexp.exe**. Accept the Process Explorer License Agreement when prompted.

c. The Process Explorer displays a list of currently active processes.

d. To locate the web browser process, drag the **Find Window's Process** icon into the opened web browser window. Microsoft Edge was used in this example.



e. The Microsoft Edge process can be terminated in the Process Explorer. Right-click the selected process and select **Kill Process**. Click **OK** to continue.



What happened to the web browser window when the process is killed?

Step 3: Start another process.

a. Open a Command Prompt. (**Start** > search **Command Prompt** > select **Command Prompt**)

b. Drag the **Find Window's Process** icon into the Command Prompt window and locate the highlighted Command Prompt process in Process Explorer.

c. The process for the Command Prompt is cmd.exe. Its parent process is explorer.exe process. The cmd.exe has a child process, conhost.exe.

d. Navigate to the Command Prompt window. Start a ping at the prompt and observe the changes under the cmd.exe process.

What happened during the ping process?

e. As you review the list of active processes, you find that the child process conhost.exe may be suspicious. To check for malicious content, right-click **conhost.exe** and select **Check VirusTotal**. When prompted, click **Yes** to agree to VirusTotal Terms of Service. Then click **OK** for the next prompt.

f. Expand the Process Explorer window or scroll to the right until you see the VirusTotal column. Click the link under the VirusTotal column. The default web browser opens with the results regarding the malicious content of conhost.exe.

g. Right-click the cmd.exe process and select **Kill Process**.

What happened to the child process conhost.exe?

Part 2: Exploring Threads and Handles

In this part, you will explore threads and handles. Processes have one or more threads. A thread is a unit of execution in a process. A handle is an abstract reference to memory blocks or objects managed by an operating system. You will use Process Explorer (procexp.exe) in Windows SysInternals Suite to explore the threads and handles.

Step 1: Explore threads.

a. Open a command prompt.

b. In Process Explorer window, right-click conhost.exe and Select **Properties…**.. Click the **Threads** tab to view the active threads for the conhost.exe process. Click **OK** to continue if prompted by a warning dialog box.

c. Examine the details of the thread.

What type of information is available in the Properties window?

d. Click **OK** to continue.

Step 2: Explore handles.

a. In the Process Explorer, click **View** > select **Lower Pane View** > **Handles** to view the handles associated with the conhost.exe process.

Examine the handles. What are the handles pointing to?

b. Close the Process Explorer when finished.

Part 3: Exploring Windows Registry

The Windows Registry is a hierarchical database that stores most of the operating systems and desktop environment configuration settings.

a. To access the Windows Registry, click **Start** > Search for **regedit** and select **Registry Editor**. Click **Yes** when asked to allow this app to make changes.

The Registry Editor has five hives. These hives are at the top level of the registry.

- HKEY_CLASSES_ROOT is actually the Classes subkey of HKEY_LOCAL_MACHINE\Software\. It stores information used by registered applications like file extension association, as well as a programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data.
- HKEY_CURRENT_USER contains the settings and configurations for the users who are currently logged in.
- HKEY_LOCAL_MACHINE stores configuration information specific to the local computer.
- HKEY_USERS contains the settings and configurations for all the users on the local computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS.
- HKEY_CURRENT_CONFIG stores the hardware information that is used at bootup by the local computer.

b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the EulaAccepted registry key for Process Explorer.

Click to select Process Explorer in **HKEY_CURRENT_USER** > **Software** > **Sysinternals** > **Process Explorer**. Scroll down to locate the key **EulaAccepted**. Currently, the value for the registry key EulaAccepted is 0x00000001(1).

c. Double-click **EulaAccepted** registry key. Currently the value data is set to 1. The value of 1 indicates that the EULA has been accepted by the user.

d. Change the **1** to **0** for Value data. The value of 0 indicates that the EULA was not accepted. Click **OK** to continue.

What is value for this registry key in the Data column?

e. Open the **Process Explorer**. Navigate to the folder where you have downloaded SysInternals. Open the folder **SysInternalsSuite** > Open **procexp.exe**.

When you open the Process Explorer, what did you see?