|  |  |
| --- | --- |
| **Server & Cloud Security**  Diploma in CSF/IT  Oct 2022 | Week 5 |
| Practical |
| **Whitespace Week Activity: Server Stress Testing** | |

## Scenario

You are concerned about discovering application layer attacks against your Windows servers. You have decided to simulate some attacks that might consume processor or memory resources, making the server sluggish or unresponsive. First, you will use CPU Stress to simulate a heavy processor load on the server. Second, you will use test limit to simulate a similar heavy memory load. In both cases, you will monitor the output by using CPU Explorer, Task Manager, and Performance Monitor.

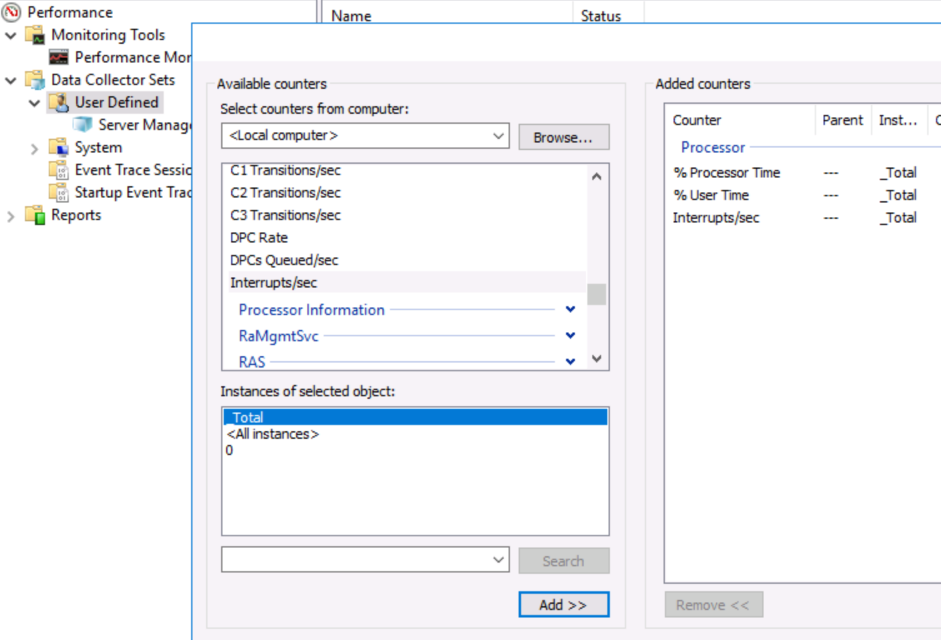
## Objectives

This activity is designed to test your understanding of and ability to analyze potential indicators associated with application attacks.

Task 1: Display Process Explorer and Performance Monitor

To prepare for application attack detection, you will use Process Explorer and Performance Monitor to display current resource utilization information. You will create a custom Data Collector Set in Performance Monitor to observe a simulated deviation from the baseline.

1. Sign in to DC1 VM.
2. In Server Manager, select **Tools > Performance Monitor**.
3. Expand the **Data Collector Sets > User Defined** node. Right-click the **User Defined** node and then select **New > Data Collector Set**.
4. Use CPU baseline as the Name, select the radio button for **Create manually (advanced)**, and then select **Next**.
5. With **Create data logs** selected, check the box for **Performance Counter**, and then select **Next**.
6. On the Which performance counters would you like to log? page, select **Add**.
7. On the Available counters page, expand the **Processor** node. Select the following three counters, and **Add** them to the **Added Counters** column:
   * % Processor Time (this counter is a good general indicator of the processor's overall activity level)
   * % User Time (this counter provides data on time spent by the processor managing user applications)
   * Interrupts/sec (this counter measures interrupts that the processor must handle immediately)



1. Select **OK** to complete the **Available counters** dialog box.
2. Select **Next**.
3. Which of the following is the path displayed for the Root directory, where the Performance Monitor Data Collector Set logs will be stored?

A. C:\Performance Monitor\Logs

B. %systemdrive%\Performance Monitor\Logs

C. %systemdrive%

D. %systemdrive%\PerfLogs\Admin\CPU baseline

Ans: D

1. Select **Finish** to complete the Data Collector Set configuration.

You will start the Data Collector Set in a later step.

1. Minimize Performance Monitor. You will use it in later tasks.
2. Download **Sysinternals.zip** from PoliteMall, put it into DC1 VM and unzip it. Browse to your **Sysinternals** folder, and then launch **procexp**.
3. Observe some of the key information reported by Process Explorer, including:
   * CPU Usage in the lower left corner - a percentage of processor utilization
   * The tree format of the processes and their relationships to each other
   * Reorganize data by selecting the column headers. The CPU column can be organized to display processes that are consuming the most resources, for example.
4. Leave Process Explorer open. You will use it in later tasks.
5. Right-click the **Taskbar**, and then select **Task Manager**.
6. Select the **Performance** tab.
7. Select each of the following three categories to observe the relevant performance information:
   * CPU
   * Memory
   * Ethernet
8. Leave **CPU** selected.
9. Leave Task Manager open. You will use it in later tasks.

## Task 2: Create stress on the CPU

You will use CPU Stress to place a false load on the VM's processors. You'll use Performance Monitor, Task Manager, and Process Explorer to monitor the workload.

1. Select Performance Monitor. Under **Data Collector Sets > User Defined**, right-click the **CPU baseline** set, and then select **Start**.

You will leave the Data Collector Set running through the next several tasks. It gathers information as you accomplish activity steps.

1. Browse to your **Sysinternals** folder, and then launch **cpustres64**.

You will see a dashboard with four pre-created threads available. The menu allows you to start and stop threads, as well as to create new threads. Right-click threads to manage their priority level. You will create and execute threads in a later step.

[CPUStres](https://docs.microsoft.com/en-us/sysinternals/downloads/cpustres) is a performance management utility that applies a workload to the processor by creating one or more threads. Each thread can be given a priority level (low, medium, high, maximum). This tool is part of the Windows Sysinternals suite.

1. Resize and reposition the Task Manager, Process Explorer, and CPU Stress windows so that you can observe them simultaneously.

The goal is to view the effect of starting CPU Stress in Task Manager and Process Explorer.

1. In the CPU Stress console, select the **Create Threads** button. A thread is generated in the window.

The new thread is currently inactive. You can select additional values, such as workload, affinity, and priority.

There should now be five threads created. Four were created by default, and you created the fifth.

1. Select all five threads, right-click them, and then select **Activity Level** > **Medium (50%)**.
2. In CPU Stress, select the five threads, right-click the selection, and then select **Activate**.

The system will become very slow!

1. Switch to Task Manager. CPU Utilization should be nearly 100%.
2. Switch to Process Explorer. In the lower left corner, CPU Usage should also be nearly 100%.
3. In Process Explorer, open the **CPUSTRES64.exe** process to display detailed data. Select **Cancel** when you have browsed each tab.

Task 3: End the CPU Stress threads

You have now completed the stress test, so you will end the threads.

1. In the CPU Stress console, right-click each thread, and then select **Deactivate**.

You can select several or all of the threads by holding down the **SHIFT** or **CTRL** keys.

1. Display Process Explorer and Task Manager. CPU utlization should be well below 100%.
2. Close Process Explorer and CPU Stress.
3. Switch to Performance Monitor, right-click the **CPU baseline** data collector set, and select **Stop**.
4. Right-click **CPU baseline** and select **Latest Report**. Use this log to answer the following question:
5. Which of the following answers best describes the results of the CPU baseline data?

A. Processor utilization is high, then normal, then high again.

B. Processor utilization is unchanged throughout the activity.

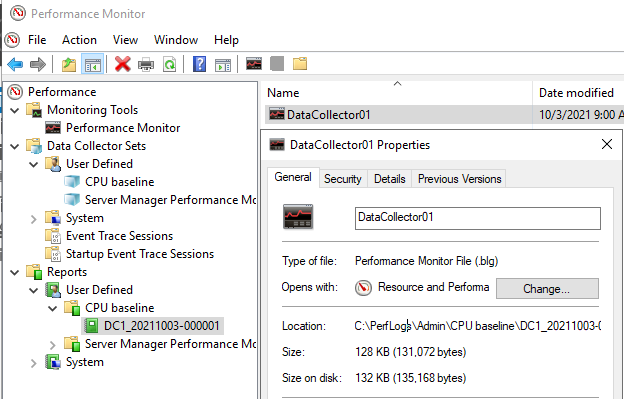
C. Processor utilization is high throughout the activity.

D. Processor utilization is normal, then high, then normal again.

Ans: D

1. Confirm that the CPU baseline report directory exists.

You can find the report you just generated, right click the “Data Collector” and select properties. Then you will notice the location of the report.



CPU utilization information Performance Monitor should record normal processor utilization until the CPU Stress utility is run. Processor utilization should be very high until you end the CPU Stress task. At that point, it should return to normal. If the report does not exist, you will need to repeat the entire Create stress on the CPU activity.

Task 4: Create stress on the Memory

You will use the testlimit utility to create a false workload that stresses the system's memory, simulating an application attack that attempts to consume RAM. You'll use Peformance Monitor and Task Manager to observe the results.

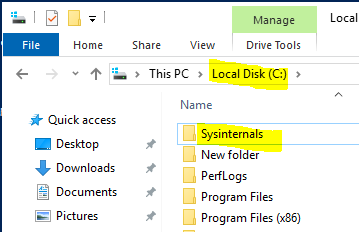
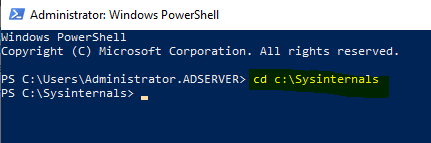
1. Select Performance Monitor, and then create a new Data Collector Set named Memory baseline with the following counters from the **Memory** category:
   * % Committed Bytes In Use (this counter compares committed memory bytes to the byte commit level, indicating paging utilization that may be due to memory leaks or too many open applications)
   * Available MBytes (this counter reports the quantity of memory available for new applications to startup)
   * Pages/sec (this counter reports the rate at which memory pages are written to or from the pagefile on the hard disk drive)
2. Right-click the **Memory baseline** data collector set, and then select **Start**.

You will leave the Data Collector Set running through the next several tasks. It gathers information as you accomplish activity steps.

1. From the desktop, select the Windows **Start** menu, right-click **Windows PowerShell**, and then select **Run as Administrator**. Select **Yes** to confirm the UAC prompt.
2. In the Windows PowerShell console, enter into your Sysinternals folder.

For example, if your Sysinternals is located directly in your C: drive, you can type the following command in PowerShell:

cd c:\Sysinternals

1. In the Task Manager console, select the **Memory** node.
2. Resize the Windows PowerShell console and the Task Manager console so that you can observe them simultaneously.

The goal is to view the effect of starting the testlimit utility in Task Manager.

1. Run the following command in Windows PowerShell to simulate the consumption of memory, selecting **Agree** when prompted to accept the license agreement:

.\testlimit -d 1024 -c 1

*(-d 🡺 Leak and touch memory in specified MBs)*

*(-c 🡺 Count of number of objects to allocate)*

1. Which of the following answers best describes the purpose of the .\ characters in this command?

A. The .\ characters inform Windows PowerShell that this is a script.

B. The .\ characters inform Windows PowerShell to look in the current folder for the executable.

C. The .\ characters inform Windows PowerShell that this is not a script.

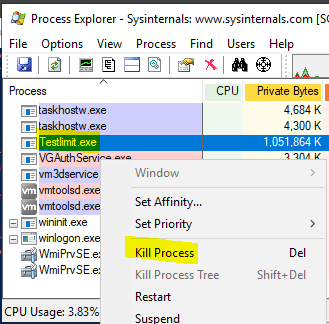
D. All Windows PowerShell cmdlets require .\ as the first two characters.

Ans: B

1. Switch to Task Manager, and then view the **Memory** category.

Memory utilization should be very high.

1. In  **Process Explorer** , right-click **Testlimit**, and then select **Kill Process**.



1. Select Performance Monitor, and then *stop* the **Memory baseline** Data Collector Set.
2. Right-click **Memory baseline** and then select **Latest Report**. Use this log to answer the following question:
3. Which of the following answers best describes the results of the Memory baseline data?

A. Memory utilization is normal, then high, and then normal again through the activity.

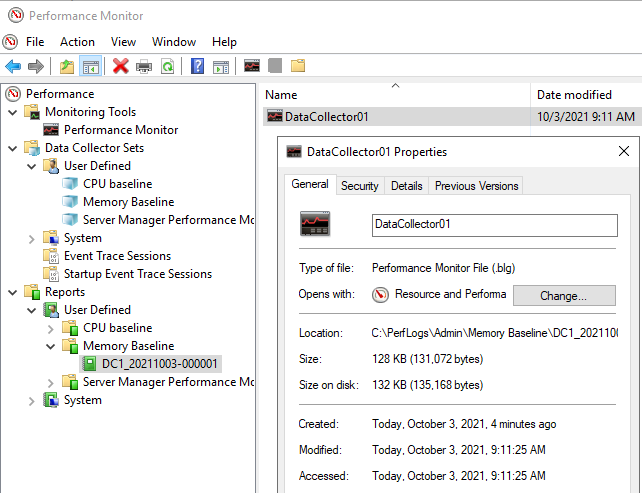
B. Memory utilization is high, then normal, and then high again through the activity.

C. Memory utilization is high through the activity.

D. Memory utilization is unchanged through the activity.

Ans: A

1. Confirm that the Memory baseline report directory exists.



Memory utilization information Performance Monitor should record normal memory utilization until the testlimit command is run. Memory utilization should be very high until you end the testlimit task. At that point, it should return to normal. If the report does not exist, you will need to repeat the entire Create stress on the Memory activity.

1. What is the purpose behind baselining a server's performance?

A. Baselining limits the server's performance, based on an application's utilization requirements.

B. Baselining is a required step during the configuration of the server.

C. Baselining documents the server's current performance so that the results can be compared against future performance data.

D. To maintain the manufacturer's warranty.

Ans: C

---End of Practical---