Identifying Application Attack Indicators

(CompTIA Security + SY – 601)

Objectives:

- To use process Explorer and Performance monitor to display current resource utilization information
- To create a custom data collector
- To set in performance monitor to observe a simulated deviation from the baseline

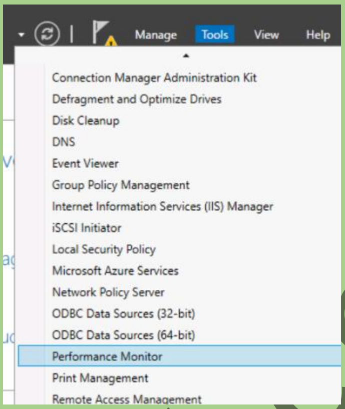
Resources:

- Windows Virtual Machine (DC1)

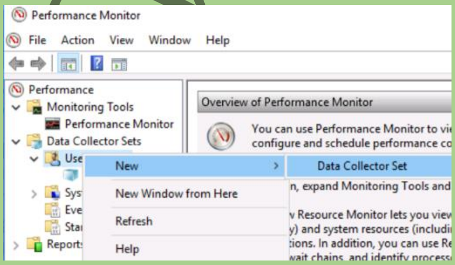
Instructions:

Display Process Explorer and Performance Monitor

- Log-in to DC1 VM
- In Server Manager, select **Tools > Performance Monitor**



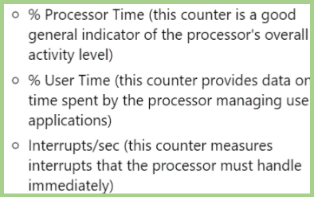
- Expand the **Data Collector Sets > User Defined** node and then select **New > Data collector set**



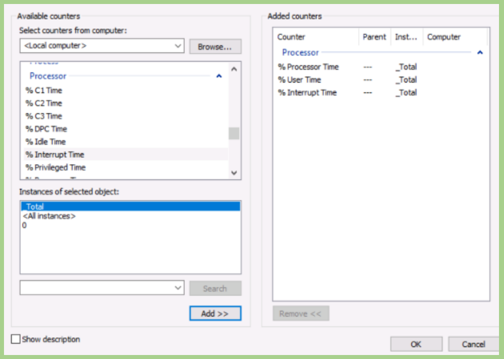
You can use Performance Monitor to vi
configure and schedule performance co
n, expand Monitoring Tools and
v Resource Monitor lets you view
y) and system resources (includi
tions. In addition, you can use Re
wait chains, and identify process

- Use **CPU baseline** as the name, select the radio button for **Create manually (advanced)** and then select **Next**

- With **create data** logs selected, check the box for **performance counter**, and then select **Next**
- On the which performance counters would you like to log? Page, select **Add**
- On the available counters page, expand the Processor node. Select the following three counters and **Add** them to the **Added Counters** column

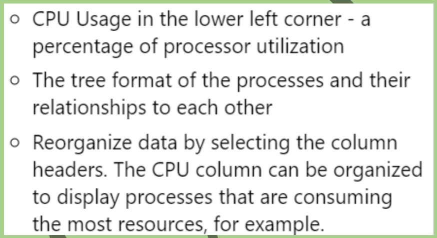


- % Processor Time (this counter is a good general indicator of the processor's overall activity level)
- % User Time (this counter provides data on time spent by the processor managing use applications)
- Interrupts/sec (this counter measures interrupts that the processor must handle immediately)

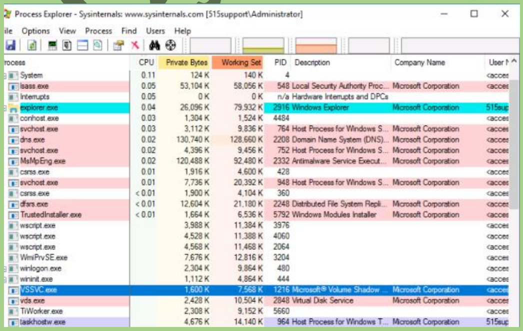


Counter	Parent	Inst...	Computer
Processor			
% Processor Time	---	_Total	
% User Time	---	_Total	
% Interrupt Time	---	_Total	

- Select OK to complete the Available counters dialog box
- Select **Next**
- Select **Finish** to complete the Data Collector Set configuration
- Minimize Performance Monitor. You will use it in later tasks
- From the desktop, open the **LABFILES** folder, browse to the **Sysinternal** folder and then launch **procexp**
- Observe some of the key information reported by Process Explorer, including:



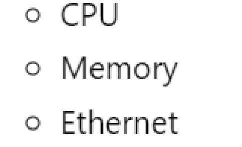
- CPU Usage in the lower left corner - a percentage of processor utilization
- The tree format of the processes and their relationships to each other
- Reorganize data by selecting the column headers. The CPU column can be organized to display processes that are consuming the most resources, for example.



Process Explorer - Sysinternals: www.sysinternals.com [515support\Administrator]
ile
Options
View
Process
Find
Users
Help

rocess	CPU	Private Bytes	Working Set	PID	Description	Company Name	User N
System	0.11	124 K	140 K	4			<acces
lsass.exe	0.05	53,104 K	58,056 K	548	Local Security Authority Proc...	Microsoft Corporation	<acces
Interrupts	0.05	0 K	0 K	n/a	Hardware Interrupts and DPCs		
explorer.exe	0.04	26,096 K	79,932 K	2916	Windows Explorer	Microsoft Corporation	515sup
conhost.exe	0.03	1,304 K	1,524 K	4484			<acces
svchost.exe	0.03	3,112 K	9,836 K	764	Host Process for Windows S...	Microsoft Corporation	<acces
dns.exe	0.02	130,740 K	128,660 K	2208	Domain Name System (DNS)...	Microsoft Corporation	<acces
svchost.exe	0.02	4,396 K	9,456 K	752	Host Process for Windows S...	Microsoft Corporation	<acces
MsMpEng.exe	0.02	120,488 K	92,480 K	2332	Antimalware Service Execut...	Microsoft Corporation	<acces
csrss.exe	0.01	1,916 K	4,600 K	428			<acces
svchost.exe	0.01	7,736 K	20,392 K	948	Host Process for Windows S...	Microsoft Corporation	<acces
csrss.exe	< 0.01	1,900 K	4,104 K	360			<acces
dfsrs.exe	< 0.01	12,604 K	21,180 K	2248	Distributed File System Repli...	Microsoft Corporation	<acces
TrustedInstaller.exe	< 0.01	1,664 K	6,536 K	5792	Windows Modules Installer	Microsoft Corporation	<acces
wscript.exe		3,988 K	11,384 K	3976			<acces
wscript.exe		4,528 K	11,388 K	4060			<acces
wscript.exe		4,568 K	11,468 K	2064			<acces
WmiPrvSE.exe		7,676 K	12,816 K	3204			<acces
winlogon.exe		2,304 K	9,864 K	480			<acces
wininit.exe		1,112 K	4,864 K	444			<acces
VSSVC.exe		1,600 K	7,568 K	1216	Microsoft® Volume Shadow ...	Microsoft Corporation	<acces
vds.exe		2,428 K	10,504 K	2848	Virtual Disk Service	Microsoft Corporation	<acces
TiWorker.exe		2,308 K	9,152 K	5660			<acces
taskhostw.exe		4,676 K	14,140 K	964	Host Process for Windows T...	Microsoft Corporation	515sup

- ➢ Leave Press Explorer open, you will use it in later tasks
- ➢ Right-click the **Taskbar** and then select **Task Manager**
- ➢ Select the **Performance** tab
- ➢ Select each of the following three categories to observe the relevant performance information

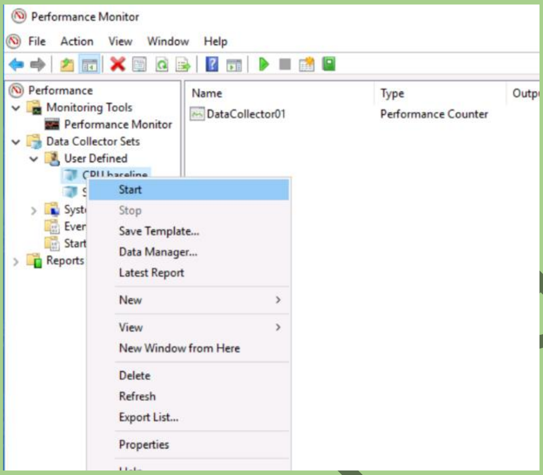


- ○ CPU
- ○ Memory
- ○ Ethernet

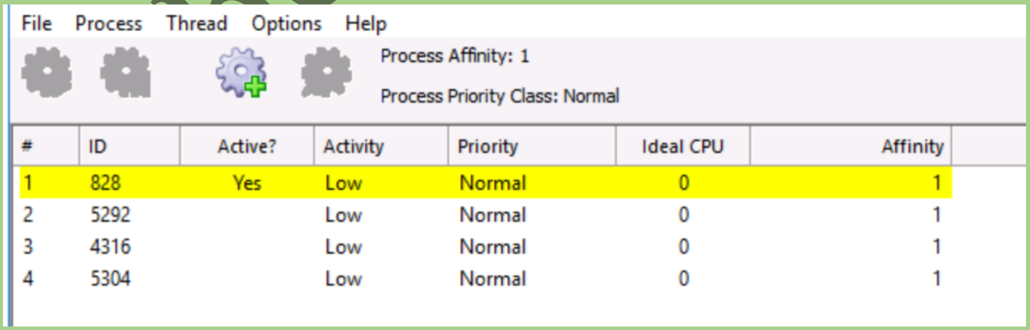
- ➢ Leave CPU selected
- ➢ Leave **Task Manager** open. You will use it in later tasks

Create Stress on the CPU

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



- ➢ From the **C:\LABFILES\Sysinternals** folder, open **cpustres 64**



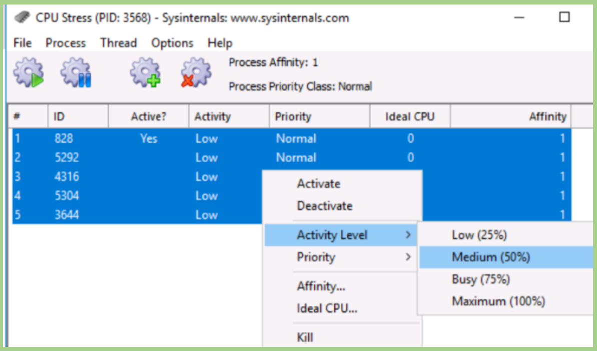
Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	828	Yes	Low	Normal	0	1
2	5292		Low	Normal	0	1
3	4316		Low	Normal	0	1
4	5304		Low	Normal	0	1

- ➢ Resize and reposition the Task Manager, Process Explorer, and CPU Stress window so that you can observe simultaneously

- In the CPU Stress console, select the **Create Threads** button. A thread is generated in the window
- Select all five threads, right-click them and then select Activity Level > Medium 50%



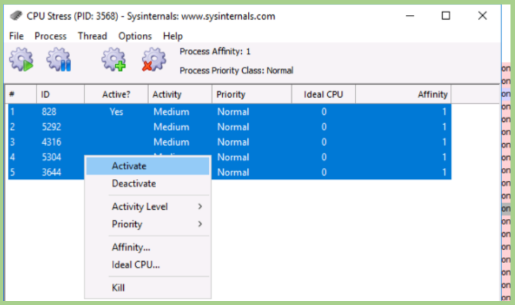
CPU Stress (PID: 3568) - Sysinternals: www.sysinternals.com

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	828	Yes	Low	Normal	0	1
2	5292		Low	Normal	0	1
3	4316		Low			1
4	5304		Low			1
5	3644		Low			1

- In CPU Stress, select the five threads, right click the section and then select **Activate**



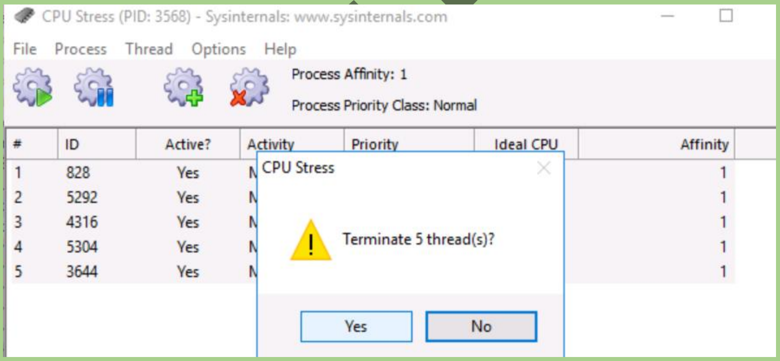
CPU Stress (PID: 3568) - Sysinternals: www.sysinternals.com

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	828	Yes	Medium	Normal	0	1
2	5292		Medium	Normal	0	1
3	4316		Medium	Normal	0	1
4	5304			Normal	0	1
5	3644			Normal	0	1

- Switch to Task Manager CPU, utilization should be nearly 100%
- Switch to Process Explorer. In the lower left corner, CPU usage should be nearly 100%
- In the process Explorer, open the CPUSTRES64.exe process to display detailed data, select **Cancel** when you have browsed each tab



CPU Stress (PID: 3568) - Sysinternals: www.sysinternals.com

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	828	Yes	N			1
2	5292	Yes	N			1
3	4316	Yes	N			1
4	5304	Yes	N			1
5	3644	Yes	N			1

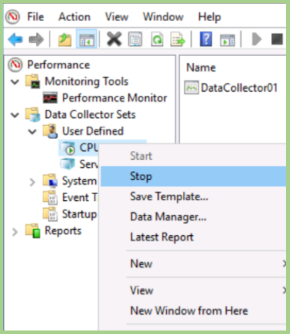
CPU Stress

Terminate 5 thread(s)?

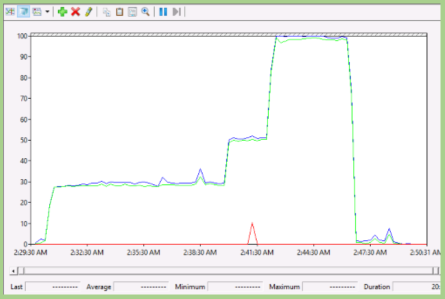
<u>End the CPU Stress threads</u>

- In the CPU Stress console, right-click each thread, and then select Deactivate
- Display Process Explorer and Task Manager, CPU utilization should be well below 100%
- Close Process Explorer and CPU Stress

- Switch to Performance Monitor, right-click the **CPU baseline** data collector set and select **Stop**

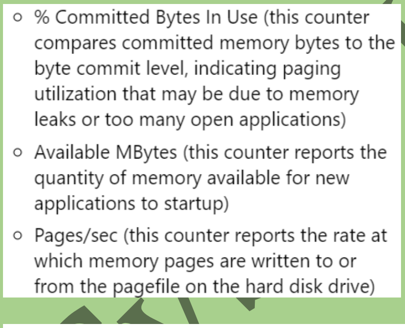


- Right-click CPU baseline and select latest report

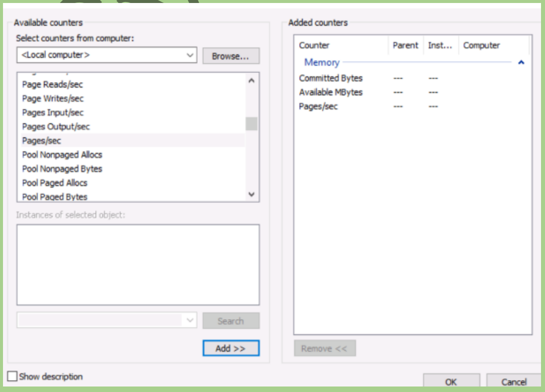


Create Stress on the Memory

- Select Performance Monitor, and then create a new Data Collector Set named **Memory baseline** with the following counters from the **Memory** category

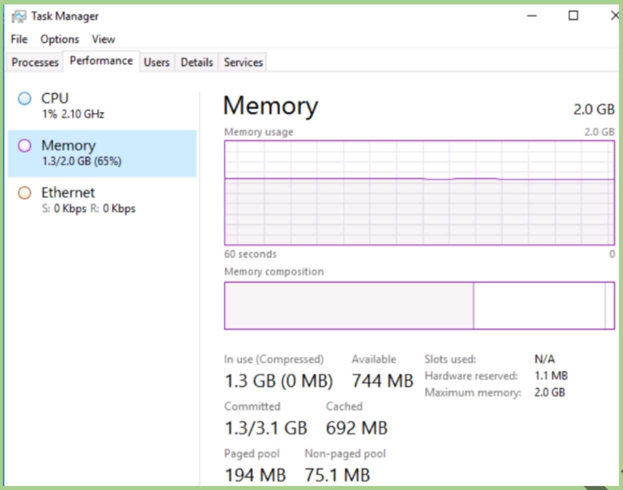


- % Committed Bytes In Use (this counter compares committed memory bytes to the byte commit level, indicating paging utilization that may be due to memory leaks or too many open applications)
- Available MBytes (this counter reports the quantity of memory available for new applications to startup)
- Pages/sec (this counter reports the rate at which memory pages are written to or from the pagefile on the hard disk drive)



Counter	Parent	Inst...	Computer
Memory			
Committed Bytes	---	---	
Available MBytes	---	---	
Pages/sec	---	---	

- Right-click the **Memory baseline** data collector
- From the desktop, select the Windows Start menu, right-click **Windows PowerShell** and then select **Run as Administrator**, select **Yes** to confirm the **UAC**
- In the Windows PowerShell console, enter **cd C:\LABFILES\Sysinternals**
- 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
- In the Windows PowerShell console, enter **cd C:\LABFILES\Sysinternals**
- In the Task Manager console, select the **Memory** node



CPU
1% 2.10 GHz

Memory
1.3/2.0 GB (65%)

Ethernet
S: 0 Kbps R: 0 Kbps

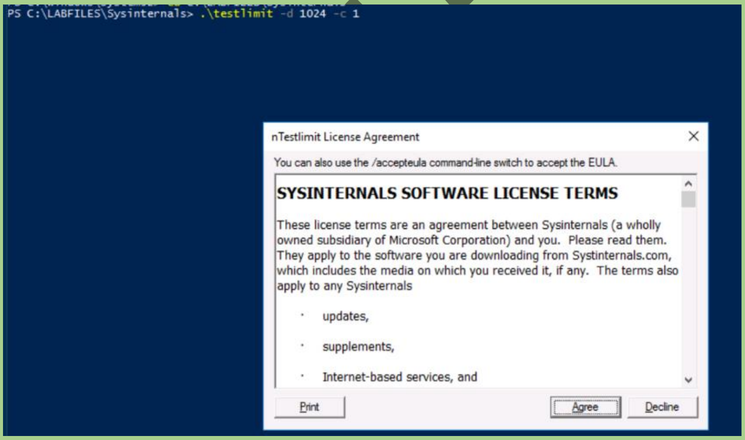
Memory 2.0 GB

Memory usage 2.0 GB

Memory composition

In use (Compressed): 1.3 GB (0 MB)
Available: 744 MB
Slots used: N/A
Hardware reserved: 1.1 MB
Maximum memory: 2.0 GB
Committed: 1.3/3.1 GB
Cached: 692 MB
Paged pool: 194 MB
Non-paged pool: 75.1 MB

- Resize the Windows PowerShell console and the Task Manager console so that you can observe
- Run the following command in Windows PowerShell to stimulate the consumption of memory, selecting Agree when prompted to accept the license agreement**: .\testlimit -d 1024 -c I**



```
PS C:\LABFILES\Sysinternals> .\testlimit -d 1024 -c 1
```

nTestlimit License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

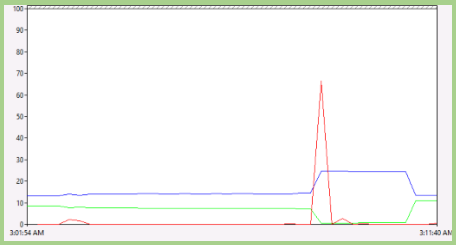
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

- Switch to Task Manager, and the view the **Memory** Category
- In the Task Manager, select **Processes** tab
- Scroll down to the Background Processes section, right-click Test Windows Limits, and then select **End Task**

- Select Performance Monitor, and then Stop the **Memory baseline** Data collector Set.
- Right-click Memory baseline and then select Latest Report



Observations:

- **Use of Tools**: The lab involved using Process Explorer and Performance Monitor to monitor and analyze CPU and memory usage in a Windows environment.
- **Creating Data Collectors**: Custom data collectors were created for both CPU and memory, focusing on logging performance counters.
- **Simulating Resource Stress**: The lab simulated CPU and memory stress using specific tools (CPUSTRES64.exe and testlimit).
- **Monitoring Resource Utilization**: Key resource utilization metrics were observed through Task Manager, Process Explorer, and Performance Monitor.
- **Report Generation**: After the tests, performance data was reviewed by generating reports from the data collectors.

Results:

- **CPU Stress Simulation**: The CPU usage was successfully driven close to 100% by creating multiple threads in CPUSTRES64.exe, confirming the effectiveness of the stress simulation.
- **Memory Stress Simulation**: Memory usage increased significantly as simulated by the testlimit command in PowerShell, effectively demonstrating memory stress.
- **Performance Metrics Captured**: The custom data collectors captured performance metrics accurately, reflecting the stress applied to both CPU and memory.
- **System Response**: The system's response to stress was observable through increased resource utilization in both CPU and memory, providing clear indicators of the system's behavior under load.
- **Reports Generated**: Reports generated from the data collectors provided a clear summary of the resource utilization during the stress tests.

Conclusion:

The lab successfully demonstrated how to identify application attack indicators by monitoring and analyzing system resource utilization under simulated stress conditions. By utilizing tools such as Process Explorer and Performance Monitor, the lab provided a comprehensive approach to understanding how applications impact system resources. The generated reports confirmed the effectiveness of the data collectors in capturing critical performance metrics, which are essential in diagnosing potential application-level attacks or resource misuse.

Future Work:

- **Automation of Monitoring Processes**: Explore the automation of the data collection and reporting process to enhance efficiency in real-time monitoring scenarios.
- **Extended Stress Testing**: Conduct prolonged stress tests to observe long-term effects on system performance and stability.
- **Diverse Resource Monitoring**: Expand the monitoring to include additional system resources such as disk I/O, network activity, and GPU usage.
- **Integration with Security Tools**: Integrate these monitoring tools with security solutions to automatically flag potential attack indicators based on abnormal resource utilization.
- **Real-World Application Testing**: Apply the same monitoring and stress-testing methodology to real-world applications to assess their robustness against potential attack vectors.