Google IT Support Certificate: Course 3: Operating Systems and You

Week 5: Process Management

Quiz: Maintain Efficient Process Utilization on Windows

Introduction

In this lab, you'll use the new commands you learned to do some process maintenance on a Windows virtual machine. As an IT Support Specialist, it's super important that you maintain efficient process utilization on your machines.

What you'll do

- Collect process information using the Task Viewer.
- Terminate a specific process using Windows PowerShell.
- Terminate multiple processes using Windows PowerShell.

Terminating a specific process

On Windows, you can view running processes in the Task Viewer, or use Windows PowerShell (this is what you'll be using for this lab). For these operations, you'll need to be running a Windows PowerShell terminal in ***Administrative*** mode. So, search the Start Menu for Windows PowerShell, right-click it, and select "**Run as Administrator**".

From Windows PowerShell, you can use `Get-Process` to search for a process by name. The "totally_not_malicious" process is running on this machine, too. Search for it, using this command:

```
Get-Process -Name "totally_not_malicious"
```

Copied!

content_copy

Each row represents a process, and one of the columns shows the process ID:

```
Handles  NPM(K)  PM(K)   WS(K)  CPU(s)   Id   SI ProcessName

-------  ------  -----   -----  ------   --   -- -----------

    209      14   2724   10996  271.06   7164   1 totally_not_malicious
```

To end a process, you can use taskkill and specify the Process ID, or PID, of the process:

Note: Make sure you **replace/substitute** the "[PROCESS ID]" with id of the process you got from the previous command.

```
taskkill /F /PID [PROCESS ID]
```

Copied!

content_copy

You should see this message after running taskkill with the PID for your process, which will likely be different than the ID specified here:

```
SUCCESS: The process with PID 7164 has been terminated.
```

To verify that the process is no longer running, you can search for it again:

```
Get-Process -Name "totally_not_malicious"
```

Copied!

content_copy

This should throw an error because no process by that name exists anymore, indicating that you've successfully ended it:

```
Get-Process : Cannot find a process with the name "totally_not_malicious".
Verify the process name and call the cmdlet

again.

At line:1 char:1

+ Get-Process -Name "totally_not_malicious"

+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
    + CategoryInfo          : ObjectNotFound:
(totally_not_malicious:String) [Get-Process], ProcessCommandException

    + FullyQualifiedErrorId :
NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand
```

Click Check my progress to verify the objective.

Malicious Process

Check my progress

Terminating multiple processes

There are processes containing the word "razzle" also running on this VM. `Get-Process` doesn't handle processes with partially-matching names, like grep does, and running `Get-Process -Name "razzle"` would result in no matches. However, you can use "wildcards" (asterisks) to look for processes that contain "razzle" in their name:

```
Get-Process -Name "*razzle*"
```

Copied!

content_copy

This will show two processes that contain "razzle" in their name:

```
Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName

-------  ------    -----      -----     ------     --  -- -----------

    209      14     2784      11028     572.89   2120   1 my_cat_razzle

    209      14     2824      11036     572.83   7052   1 razzle_dazzle
```

You can use taskkill, like before, once for each of the "razzle" processes:

Note: Make sure you **replace/substitute** the "[PROCESS ID]" with id of the process you got from the previous command.

```
taskkill /F /PID [PROCESS ID]
```

Copied!

content_copy

```
PS C:\users\qwiklabs> taskkill /F /PID 2120

SUCCESS: The process with PID 2120 has been terminated.

PS C:\users\qwiklabs> taskkill /F /PID 7052

SUCCESS: The process with PID 7052 has been terminated.
```

You can use `Get-Process` again to verify that the processes have been ended:

```
Get-Process -Name "*razzle*"
```

Copied!

content_copy

You shouldn't see any processes in the output. When you ran this before to verify that the malicious process had been terminated, it printed an error message because the specifically-named process was not present. When you use a wildcard (*) in the search, you aren't looking for an exact match. So, rather than an error message, the command outputs nothing at all (because there are no matches):

```
PS C:\users\qwiklabs> Get-Process -Name "*razzle*"
```

```
PS C:\users\qwiklabs>
```

Click Check my progress to verify the objective.

Razzle

Check my progress

Conclusion

Congrats! You've successfully used the Windows PowerShell commands `Get-Process` to find Windows processes, and taskkill to end them. As an IT Support Specialist, it's important for you to monitor system processes and maintain them using the Task Viewer and Windows PowerShell.