Maintain Efficient Process Utilization on Windows

1 hour Free

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.

Head's up: You'll experience a delay as the labs initially load (particularly for Windows labs). So, please **wait a couple of minutes for the labs to load**. The grade is calculated when the lab is complete, so be sure to hit "**End Lab**" when you're done!

You'll have 60 minutes to complete this lab.

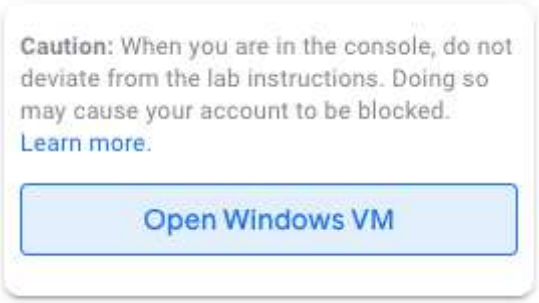
What you'll do

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

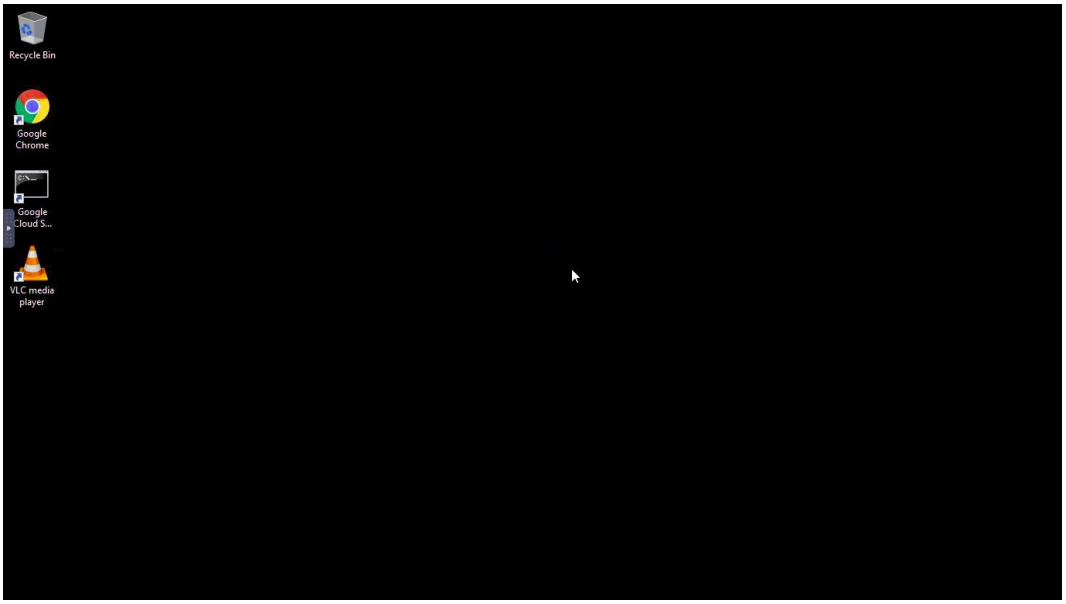
Start the lab

You'll need to start the lab before you can access the materials. To do this, click the green "Start Lab" button at the top of the screen.

After you click the "Start Lab" button, you will see a panel appear below where the start lab button was that has an **Open Windows VM** button.



Click the **Open Windows VM** button and a new tab will open with a visual interface for Windows OS, where you will be performing further steps in the lab. You should have a visual interface for Windows that looks like this:



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"
```

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

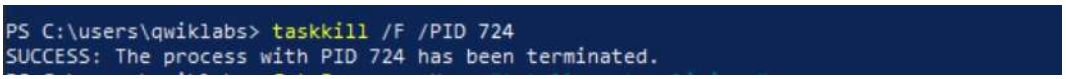
```
PS C:\users\qwiklabs> Get-Process -Name "totally_not_malicious"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    204      14     2696       7668      97.80    724   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]
```

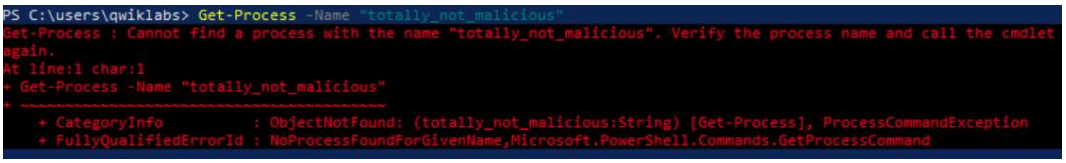
You should see this message after running taskkill with the PID for your process, which will likely be different than the ID specified here:



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

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

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



Click Check my progress to verify the objective.

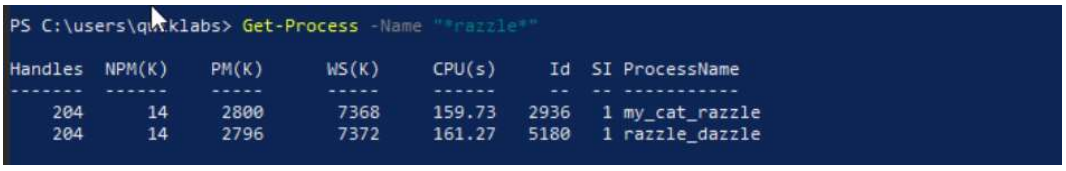
Malicious Process

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*"
```

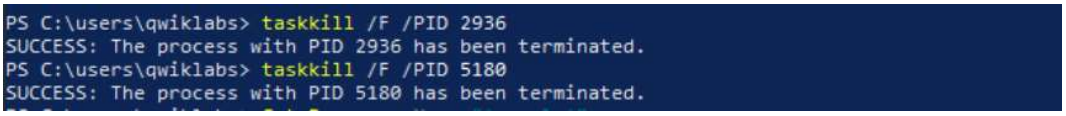
This will show two processes that contain "razzle" in their name:



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]
```



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

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

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):

Click Check my progress to verify the objective.

Razzle

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.

End your lab

When you have completed your lab, click **End Lab**. Qwiklabs removes the resources you've used and cleans the account for you.

You will be given an opportunity to rate the lab experience. Select the applicable number of stars, type a comment, and then click **Submit**.

The number of stars indicates the following:

- 1 star = Very dissatisfied
- 2 stars = Dissatisfied
- 3 stars = Neutral
- 4 stars = Satisfied

- 5 stars = Very satisfied

You can close the dialog box if you don't want to provide feedback.

For feedback, suggestions, or corrections, please use the **Support** tab.