Answers: 11.4.4.2 Lab – Task and System CLI Commands

Introduction

In this lab, you will work with task and system CLI commands.

Required Resources

- 1 PC with Windows installed

Instructions

Part 1: Task CLI Commands

The tasklist command shows the running processes on a computer while the taskkill command terminates running processes. These two commands can be used on a remote computer. These commands can be filtered and targeted using the available options for the commands. In this lab, the username ITEUser is used in the examples.

Step 1: The tasklist command

a. Open notepad. Open Internet Explorer. If Internet Explorer is not available, use Microsoft Edge instead.

b. Open a command prompt. At the prompt, enter the **tasklist** command.

```
C:\Users\ITEUser> tasklist
```

Question:

What command would you use to display the results of tasklist one page at a time?

Type your answers here.

c. Enter the tasklist help command to review the syntax and options for the tasklist command.

```
C:\Users\ITEUser> tasklist /?
```

Or

```
C:\Users\ITEUser> help tasklist
```

Questions:

What is the option to list the modules that are associated with a task?

Type your answers here.

What command would you use if you want to find all the tasks that use the module oleaut32.dll? List a few tasks that uses oleaut32.dll.

Type your answers here.

Using the options available with tasklist, you can filter the tasklist results for specific image name, such as notepad.exe for notepad. Record the PID for the next step.

```
C:\Users\ITEUser> tasklist /FI "imagename eq notepad.exe"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
notepad.exe                   3128 Console                    1     14,016 K
```

Questions:

What command would you use to find out all the tasks that are associated with your username?

Type your answers here.

What command would you use to find out all the processes that have been running for more than 1 hour and 40 minutes?

Type your answers here.

Step 2: The taskkill command

The Task Manager can be used to terminate a process. However, sometimes a rogue process may need to be terminated manually using the CLI command taskkill. The taskkill command may save you from having to force an unscheduled reboot of the system. F

a. Use the taskkill help command to review the command syntax and the available options.

```
C:\Users\ITEUser> taskkill /?
```

Question:

What command would you use if you wanted to terminate all process owned by a particular user?

Type your answers here.

Note: If you ran the command from the previous step, reopen Notepad and Internet Explorer. Use the tasklist command to list the PID for notepad.exe.

b. Use the PID for notepad.exe that you have recorded in the previous step. The PID 3128 is used in this example.

```
C:\Users\ITEUser> taskkill /PID 3128
SUCCESS: Sent termination signal to the process with PID 3128.
```

c. The Notepad application should be closed. Also, use the tasklist command to verify that the process has been terminated.

d. Use the /IM option to use the name of the process with the taskkill command to end the process. Internet Explorer (iexplore.exe)

```
C:\Users\ITEUser> taskkill /IM iexplore.exe
SUCCESS: Sent termination signal to the process "iexplore.exe" with PID 3916.
SUCCESS: Sent termination signal to the process "iexplore.exe" with PID 6740.
```

e. Depending on the Windows version, Internet Explorer may not be closed. You may need to add **/T** to terminate the associated child process.

```
C:\Users\ITEUser> taskkill /IM iexplore.exe /T
SUCCESS: Sent termination signal to process with PID 6740, child of PID 3916.
SUCCESS: Sent termination signal to process with PID 3916, child of PID 2828.
```

f. Sometimes, you may have to forcefully terminate a process. To forcibly terminate a process, add the **/F** option to the taskkill command.

```
C:\Users\ITEUser> taskkill /IM iexplore.exe /T /F
SUCCESS: The process with PID 6740 (child process of PID 3916) has been terminated.
SUCCESS: The process with PID 3916 (child process of PID 2828) has been terminated.
```

g. Verify that Internet Explorer is closed.

Part 2: System CLI Commands

Step 1: The sfc command

When you encounter random errors, issues during boot, or some of the Windows components are not working properly, the System File Checker (sfc) can scan the integrity of the system and replace any corrupted or missing system files with a known good version.

a. Open a command prompt with administrative privileges.

b. Review the syntax and options of the sfc command.

```
C:\Windows\system32> sfc /?
```

Question:

What option would you use if you only wanted to scan the integrity of all the protected system files?

Type your answers here.

c. Use the **/scannow** option when you want to scan and repair all the protected system files.

```
C:\Windows\system32> sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 2% complete.
<output omitted>
```

Step 2: The dism command

Deployment Image Servicing and Management (DISM) is a Windows command line utility that is used to service and prepare Windows images. For example, you can use DISM to manage the information included within the Windows image or service the image itself, for example adding or removing drivers or upgrading to a higher Windows edition.

In this step, you will be reviewing the options with this command and list all the available drivers without making changes to the operating system.

a. To see the available options for the dism command, enter **dism** at a command prompt with administrative privileges. The available options are different depending on your Windows version.

```
C:\Windows\system32> dism

Deployment Image Servicing and Management tool
Version: 10.0.17763.1

DISM.exe [dism_options] {Imaging_command} [<Imaging_arguments>]
DISM.exe {/Image:<path_to_offline_image> | /Online} [dism_options]
         {servicing_command} [<servicing_arguments>]
<output omitted>
```

b. To learn more information about the running operating system, enter **dism /online /?** to see the available options.

```
C:\Windows\system32> dism /online /?
```

c. While using dism, you can learn more information about the 3rd party drivers in the running operating system, enter **dism /online /get-drivers** at the prompt.

```
C:\Windows\system32> dism /online /get-drivers
```

d. To see all the drivers, the **/all** options can be added to the command.

```
C:\Windows\system32> dism /online /get-drivers /all
```

e. To make easier to read, you can format the output into a table by adding **/format:table** option.

```
C:\Windows\system32> dism /online /get-drivers /all /format:table
```

Question:

What would you add to the command so you can view the output one page at a time?

Type your answers here.

f. The driver results can be saved to a text file if necessary. Using the **>**, a new file C:\Users\ITEUser\Drivers_Results.txt is created and the results are written into this new file. If you want to append more results to this file, you will replace **>** with **>>** so the file is not overwritten with new information.

```
C:\Windows\system32> dism /online /get-drivers /all /format:table >
C:\Users\ITEUser\Drivers_Results.txt
```

g. Use the **more** or **type** command to verify the creation of the text file.

```
C:\Windows\system32> more C:\Users\ITEUser\Drivers_Results.txt

Deployment Image Servicing and Management tool
Version: 10.0.17763.1

Image Version: 10.0.17763.475
<some output omitted>
```

Step 3: The shutdown command

If your computer becomes unable to shutdown via the Start menu, the command line **shutdown** command can come in handy.

a. In a command prompt, enter **shutdown** at the prompt. Review the syntax and available options for shutting down the computer via the command line.

```
C:\Windows\systme32> shutdown
Usage: shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o]
[/hybrid] [/soft] [/fw] [/f]
    [/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]
<output omitted>
```

Notice the options to shut down or restart a remote computer, add comments regarding the reason for restart or shutdown, and the ability to set a time-out period before the shutdown.

Question:

Enter the command to log off your computer. Record the command below.

Type your answers here.

b. Log back into the computer and shut it down in 120 seconds using the command line.

Questions:

Record the command below. What warning message did you see?

Type your answers here.

What command would you use to abort the shutdown?

Type your answers here.