**Services and Processes Exercise**

Please type your answers in **red** and submit this Word Document.

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

1. Display the properties for the Schedule service. What are the values for:

get-service schedule | select \*

RequiredServices: {RPCSS, SystemEventsBroker}

DependentServices: {NaturalAuthentication}

CanPauseAndContinue: False

CanStop: True

StartType: Automatic

2. Display the properties for the Spooler service. What are the values for:

get-service spooler | select \*

RequiredServices: {RPCSS, http}

DependentServices: {Fax}

CanPauseAndContinue: False

CanStop: False

StartType: Disabled

3. Display the properties for the Winmgmt service. What are the values for:

get-service winmgmt | select \*

RequiredServices: {RPCSS}

DependentServices: {VMUSBArbService, VMAuthdService, NcaSvc, iphlpsvc...}

CanPauseAndContinue: True

CanStop: True

StartType: Automatic

What is unique about the Winmgmt service?

It CanPauseAndContinue, it only has 1 RequiredService, it has many more DependentServices

4. Look up the CanShutdown property online. What is this property?

Boolean, default is False. If True the service will be notified when the system is shutting down

5. Run the following command: get-service | select name, status, starttype

a. What are the available start types?

Manual, Automatic, Disabled

b. Look up Windows Start Types online. What do each of these start types do

Automatic: starts automatically at during system start-up

Automatic (Delayed Start): start automatically after the system boot up completes; auto delayed start waits for critical or higher priority tasks to boot before loading

Manual: these services are not started by default and must be started manually when ready for use. Manual Services will stop on computer shutdown

Disabled: if a service is disabled it cannot be used by any application by default. Any

dependent applications will fail since the service can’t be started

6. For the command: get-service | where {$\_.status -eq "Running"}

a. What is the where command an alias to?

Where-Object

b. What is this command used for?

Selects objects that share particular property values from the collection of objects that are passed to it. Ie: you can select files created after a certain date, with particualar ID, or even computers based on their version of Windows

7. Display all active processes.

get-process

a. How many session ID's are currently present?

(get-process).si.count = 271

8. Open Notepad on your computer and find its associated process.

Start-process notepad

get-process notepad | select name, id, si, path

a. What are the following properties:

Name: notepad

Id: 16268

SI: 1

Path: C:\windows\system32\notepad.exe

b. What is the command to stop this process?

Stop-process -name notepad

or you can stop by ID: stop-process -id 16268 (the id will change though, so be aware)

9. Security Tip: Hackers can try to hide processes by giving them false names.

Display all of the processes named svchost.

Get-process svchost

a. Do we know if any of the processes are suspicious?

I do not, but we can check the ID and Path to help find out

b. Display all of the svchost processes and display the Id and Path. How can this output be used to identify a suspicious process?

A way to tell is to make certain there are no duplicate IDs and to make certain the path is familiar

10. What’s the command to get all services that begin with the string “wmi”?

Get-process wmi\*

11. What’s the command to search for all services that contains “svc”, but excludes “WlanSvc”?

Get-process \*svc\* -exclude “wlandsvc”

12. What’s the command to list all running services?

get-service | where {$\_.status -eq "running"}

13. What’s the command to find out services that have 2 dependent services?

get-service | where {$\_.dependentservices.count -eq “2”}

14. What’s the command to display all services and sort by DisplayName value?

Get-service | sort -displayname

15. List all the dependent services for the wudfsvc service?

Get-service “wudfsvc” -dependentservices – cannot find any services with the name “wudfsvc” on my system

I got the dependentservices for “server” instead:

get-service “server” -dependentservices or

get-service -name server -dependentservices

it returns status = running, name = com.docker.service, displayname = docker desktop services