Powershell 3 Lab Review 2

**1. Display a list of running processes in a table that includes only the process names and ID numbers. Don’t let the table have a large blank area between the two columns.**

PS> Get-Process | Format-Table ProcessName, Id -AutoSize

ProcessName Id

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

conhost 3776

csrss 576

csrss 636

dllhost 2576

dwm 956

...

**2. Run this:**

Get-WmiObject -class Win32\_UserAccount

**Now run that same command again, but format the output into a table that has Domain and UserName columns. The UserName column should show the users’ Name property, like this:**

Domain UserName

======= ========

COMPANY DonJ

**Make sure the second column header says UserName, and not Name.**

PS> Get-WmiObject -Class Win32\_UserAccount | Format-Table Domain, @{l='UserName'; e={$\_.Name}}

Domain UserName

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

POLONIUS Administrator

POLONIUS DefaultAccount

POLONIUS Guest

POLONIUS stockal

ELSINORE Administrator

ELSINORE Guest

ELSINORE krbtgt

ELSINORE Polonius

**3. Have two computers (it’s OK to use localhost twice) run this command:**

Get-PSProvider

**Use Remoting to do this. Ensure that the output includes the computer names.**

PS> Invoke-Command -ComputerName Claudius -ScriptBlock {Get-PSProvider}

Name Capabilities Drives PSComputerName

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

Alias ShouldProcess {Alias} Claudius

Environment ShouldProcess {Env} Claudius

FileSystem Filter, ShouldProcess, Creden... {C, D} Claudius

Function ShouldProcess {Function} Claudius

Registry ShouldProcess, Transactions {HKLM, HKCU} Claudius

Variable ShouldProcess {Variable} Claudius

Certificate ShouldProcess {Cert} Claudius

WSMan Credentials {WSMan} Claudius

PS> Invoke-Command -ComputerName Polonius -ScriptBlock {Get-PSProvider}

Name Capabilities Drives PSComputerName

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

Registry ShouldProcess, Transactions {HKLM, HKCU} Polonius

Alias ShouldProcess {Alias} Polonius

Environment ShouldProcess {Env} Polonius

FileSystem Filter, ShouldProcess, Creden... {C, D} Polonius

Function ShouldProcess {Function} Polonius

Variable ShouldProcess {Variable} Polonius

**4. Use Notepad to create a file named C:\Computers.txt. In that file, put the following:**

Localhost

localhost

**You should have those two names on their own lines in the file—two lines total. Save the file and close Notepad. Then write a command that will list the running services on the computer names in C:\Computers.txt.**

PS> Get-Service -ComputerName (Get-Content C:\Computers.txt) | Where-Object {$\_.Status -eq "Running"}

Status Name DisplayName

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

Running Appinfo Application Information

Running Appinfo Application Information

Running AudioEndpointBu... Windows Audio Endpoint Builder

Running AudioEndpointBu... Windows Audio Endpoint Builder

Running Audiosrv Windows Audio

Running Audiosrv Windows Audio

Running BFE Base Filtering Engine

Running BFE Base Filtering Engine

...

**5. Query all instances of Win32\_LogicalDisk. Display only those instances that have a DriveType property containing 3 and that have 50 percent or more free disk space. Hint: to calculate free space percentage, it’s freespace/size \* 100.**

PS> Get-WMIObject -Class Win32\_LogicalDisk | Where-Object {($\_.DriveType -eq 3) -and ($\_.FreeSpace \* 2 -gt $\_.Size)}

DeviceID : C:

DriveType : 3

ProviderName :

FreeSpace : 45705965568

Size : 64422408192

VolumeName :

**6. Display a list of all WMI classes in the root\CIMv2 namespace.**

PS C:\Windows\system32> Get-WMIObject -Namespace root\CIMv2 -List

NameSpace: ROOT\CIMv2

Name Methods Properties

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

CIM\_Indication {} {CorrelatedIndications, IndicationFilterName, IndicationIde...

CIM\_ClassIndication {} {ClassDefinition, CorrelatedIndications, Ind...

CIM\_ClassDeletion {} {ClassDefinition, CorrelatedIndications, Ind...

CIM\_ClassCreation {} {ClassDefinition, CorrelatedIndications, Ind...

CIM\_ClassModification {} {ClassDefinition, CorrelatedIndications, Ind...

...

**7. Display a list of all Win32\_Service instances where the StartMode is Auto and the State is not Running.**

PS> Get-WMIObject Win32\_Service | Where-Object {($\_.StartMode -eq "Auto") -and ($\_.State -ne "Running")}

ExitCode : 0

Name : gpsvc

ProcessId : 0

StartMode : Auto

State : Stopped

Status : OK

ExitCode : 0

Name : MapsBroker

ProcessId : 0

StartMode : Auto

State : Stopped

Status : OK

ExitCode : 0

Name : WbioSrvc

ProcessId : 0

StartMode : Auto

State : Stopped

Status : OK

**8. Find a command that can send email messages. What are the mandatory parameters of this command?**

Send-MailMessage

The To, Subject and From parameters are mandatory.

**9. Run a command that will display the folder permissions on C:\.**

PS> Get-ChildItem C:\ | Where-Object {$\_.PSIsContainer} | Select-Object Name, Mode

Name Mode

---- ----

PerfLogs d-----

Program Files d-r---

Program Files (x86) d-r---

Review d-----

Users d-r---

Windows d-----

**10. Run a command that will display the permissions on every subfolder of C:\Users. Just the direct subfolders; you don’t need to recurse all files and folders. You’ll need to pipe one command to another command to achieve this.**

PS> Get-ChildItem C:\Users | Where-Object {$\_.PSIsContainer} | Get-ChildItem | Where-Object {$\_.PSIsContainer} | Select-Object Parent, Name, Mode

Parent Name Mode

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

Administrator Desktop d-r---

Administrator Documents d-r---

Administrator Downloads d-r---

Administrator Favorites d-r---

Administrator Links d-r---

Administrator Music d-r---

Administrator Pictures d-r---

Administrator Saved Games d-----

Administrator Videos d-r---

Polonius Contacts d-r---

Polonius Desktop d-r---

Polonius Documents d-r---

Polonius Downloads d-r---

Polonius Favorites d-r---

Polonius Links d-r---

Polonius Music d-r---

Polonius OneDrive d-r---

Polonius Pictures d-r---

Polonius Saved Games d-r---

Polonius Searches d-r---

Polonius Videos d-r---

Public Documents d-r---

Public Downloads d-r---

Public Music d-r---

Public Pictures d-r---

Public Videos d-r---

stockal Contacts d-r---

stockal Desktop d-r---

stockal Documents d-r---

stockal Downloads d-r---

stockal Favorites d-r---

stockal Links d-r---

stockal Music d-r---

stockal OneDrive d-r---

stockal Pictures d-r---

stockal Saved Games d-r---

stockal Searches d-r---

stockal Videos d-r---

**11. Find a command that will start Notepad under a credential other than the one you’ve used to log into the shell.**

PS> Start-Job -ScriptBlock {Notepad} -Credential 'Elsinore\Polonius'

Id Name PSJobTypeName State HasMoreData Location Command

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

2 Job2 BackgroundJob Running True localhost Notepad

**12. Run a command that makes the shell pause, or idle, for 10 seconds.**

Start-Sleep 10

**13. Can you find a help file (or files) that explains the shell’s various operators?**

about\_Arithmetic\_Operators

about\_Assignment\_Operators

about\_Comparison\_Operators

about\_Join

about\_Logical\_Operators

about\_Operators

about\_Operator\_Precedence

about\_Redirection

about\_Split

about\_Type\_Operators

**14. Write an informational message to the Application event log. Use a category of 1 and raw data of 100,100.**

PS> New-EventLog -LogName Application -Source Me

PS> Write-EventLog -LogName Application -Source Me" -EventID 1 -EntryType Information -Message "Information Event" -Category 1 -RawData 100,100

PS> Get-EventLog -LogName Application

Index Time EntryType Source InstanceID Message

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

1611 Nov 23 11:16 Information Me 1 Information Event

1610 Nov 23 10:55 Information Micro... 4111 Successful automatic...

1609 Nov 23 10:54 Information VSS 8224 The VSS service is s...

1608 Nov 23 10:44 Information VSS 8224 The VSS service is s...

...

**15. Run this command:**

Get-WmiObject -Class Win32\_Processor

**Study the default output of this command. Now, modify the command so that it displays in a table. The table should include each processor’s number of cores, manufacturer, and name. Also include a column called “MaxSpeed” that contains the processor’s maximum clock speed.**

PS C:\Windows\system32> Get-WmiObject -Class Win32\_Processor | Format-Table -Property NumberOfCores, Manufacturer, Name,

@{l='MaxSpeed'; e={$\_.MaxClockSpeed}}

NumberOfCores Manufacturer Name MaxSpeed

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

1 AuthenticAMD AMD A10 PRO-7350B R6, 10 Compute Cores... 2100

**16. Run this command:**

Get-WmiObject -Class Win32\_Process

**Study the default output of this command, and pipe it to Get-Member if you want. Now, modify the command so that only processes with a peak working set size greater than 5,000 are displayed.**

PS> Get-WmiObject -Class Win32\_Process | Where-Object {$\_.PeakWorkingSize -gt 5000}