Jeffrey Walley

Iterating Exercise

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

1. In the C:\Windows\System32 directory get all of the files with a .exe extension and a length greater than 1MB.

Use Foreach-object to display the Name and CreationTime for the files.

What is the command to perform this operation?

get-childitem | Where-Object {$\_.Name -Like "\*.exe" -and $\_.Length -gt 1MB} | foreach-object {$\_.Name; $\_.CreationTime}

2. Get all of the svchost processes.

Use Foreach-object to display the Id and Modules for each process.

a. What is the command to perform this operation?

Get-Process svchost | ForEach-Object {$\_.Id; $\_.Modules}

b. How can this output be used for system security scanning?

You can see the processID and associated modules running for each process; you can also see where the modules are stored. That way you can trace any suspect process back to it’s location

3. Use foreach-object to extract specific information from the registry.

Find all of the sub-keys of HKCU:\ used by Excel and display only the key names.

a. What is the command to perform this operation?

Get-childitem “HKCU:\Software\Microsoft\Office\Excel” -Recurse | select name

b. Find all of the sub-keys of HKCU:\ used by Excel and store them in a variable. Using this variable,for the command: $var | foreach-object { $\_.name; get-itemproperty $\_.PSPath }

What will the output be?

My output is ‘Cannot bind argument to parameter ‘Path’ because it is null

c. Perform the commands for b and review the output. What obvious problem do you see?

In the video they state there is no output, but I get results for 3 ‘Addins’ with an error stating the parameter ‘Path’ is null

d. What conclusion can be drawn from this?

In the video they state there are NO subkeys – I have 3 Subkeys. HKEY\_CURRENT\_USER\Software\Microsoft\Office\Excel\Addins; HKEY\_CURRENT\_USER\Software\Microsoft\Office\Excel\Addins\MicrosoftDataStreamerforExcel; HKEY\_CURRENT\_USER\Software\Microsoft\Office\Excel\Addins\PowerPivotExcelClientAddIn.NativeEntry.1