Chapter 27 Lab

Create a new, local user named TestMan on your computer. Be sure to assign a password to the account. Do not place the user in any user groups other than the default Users group.

Then, create a constrained endpoint on your computer. Name the endpoint ConstrainTest. Design it to only include the SmbShare module, and to only make the Get-SmbShare command is visible (in addition to a small core set of cmdlets like Exit-PSSession, Select-Object, and so forth). After creating the session configuration, register the endpoint. Configure the endpoint to only permit TestMan to connect (with Read and Execute permissions), and configure it to run all commands as your local Administrator account. Be sure to provide the correct password for Administrator when you are prompted.

Use Enter-PSSession to connect to the constrained endpoint. When doing so, use the –Credential parameter to specify the TestMan account, and provide the proper password when prompted. Ensure that you can run Get-SmbShare, but not any other command (such as Get-SmbShareAccess).

Here is one possible solution:

First, create the session configuration file.

New-PSSessionConfigurationFile -Path C:\Scripts\ConstrainTest.pssc `

-Description 'Chapter 27 lab' `

-ExecutionPolicy Restricted `

-ModulesToImport SMBShare `

-PowerShellVersion 3.0 `

-VisibleFunctions 'Get-SMBShare'`

-SessionType RestrictedRemoteServer

Next we need to register it.

Register-PSSessionConfiguration -Path C:\Scripts\ConstrainTest.pssc `

-Name ConstrainTest `

-ShowSecurityDescriptorUI `

-AccessMode Remote `

-RunAsCredential Administrator

To test, we’ll enter the session using alternate credentials.

PS C:\> enter-pssession -ComputerName localhost -ConfigurationName ConstrainTest -Credential testman

We can see what commands are available to us:

[quark]: PS>get-command

CommandType Name ModuleName

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

Function Exit-PSSession

Function Get-Command

Function Get-FormatData

Function Get-Help

Function Get-SmbShare SMBShare

Function Measure-Object

Function Out-Default

Function Select-Object

And try to run an authorized command

[quark]: PS>get-process

The term 'get-process' is not recognized as the name of a cmdlet, function, script file, or

operable program. Check the spelling of the name, or if a path was included, verify that the path

is correct and try again.

+ CategoryInfo : ObjectNotFound: (get-process:String) [], CommandNotFoundException

+ FullyQualifiedErrorId : CommandNotFoundException