Advanced Scripting   
Script Security

Last Updated: 1/19/2023 12:41 PM Version 1  
Document Prepared for: CIT361 Student

# Name Daniel Harris ID 235868292

# Instructions

Save a copy of this document. Answer all questions directly in this document. You will save and upload this completed document as your homework submission.

# Overview

In this exercise you will learn how execution policies are used to help protect users from malicious code.

# Requirements

* Windows PowerShell
* Internet connectivity

# Task 1—Viewing the Execution Policy.

The local machine execution policy defines

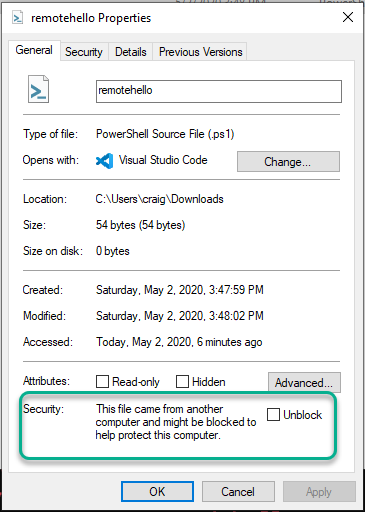
## Steps

1. Enter the command   
   Get-ExecutionPolicy
   1. What is was reported? Unrestricted
2. To get a complete list of the execution policies on your machine enter  
   Get-ExecutionPolicy -List
   1. Record each scope’s setting
      1. MachinePolicy Undefined
      2. UserPolicy Undefined
      3. Process Undefined
      4. CurrentUser Undefined
      5. LocalMachine Undefined
3. For a newly installed Windows Machine **Get-ExecutionPolicy** will return Restricted. **Get-ExecutionPolicy -List** will return *Undefined* for all scopes.
   1. What does this tell you about the default policy? It is strict by default. yes
   2. Is your computer using the default settings? yes
4. Were you able to run your script in the last exercise? yes
5. After viewing your Execution Policy settings explain your results. I need to change the policy to something more secure.

# Task 2—Modifying the Local Machine Scope

Now you will change the policy settings so that you can run scripts on your machine according to your desired preferences. You can set the *Process*, *CurrentUser*, and *LocalMachine* scope with PowerShell. To change the *MachinePolicy* or *UserPolicy*, you need to use a GroupPolicy which is beyond the scope of this class. To modify the LocalMachine policy you must run an elevated PowerShell

## Steps

1. Change the LocalMachine scope to **RemoteSigned**.
   1. Open an elevated PowerShell instance.
   2. Enter the command   
      Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
2. Close PowerShell and then start a new instance of PowerShell. These changes will only effect new instances of PowerShell.
3. To test the policy, you need to download a script from the internet. Using your web browser (either Edge or Chrome should work) download the file <http://lf.cit.byui.edu/as/rhello.ps1> and save it to your psfiles/scripts folder. (NOTE: you *must* save it to that location. If you didn’t, use the move command to move it.)
4. Make your psfiles/scripts folder your current directory
5. Run the rhello script by entering  
   ./rhello.ps1
   1. What was the result? Cannot be loaded, not digitally signed.
6. When you copy a file from a remote system the file gets flagged as coming from another system. PowerShell looks at the source of the file to help decide if it should be allowed to run. If you would like to run it anyway you can either change your Execution Policy or change the files blocking flag. Using file explorer navigate to your psfiles/scripts folder. Right-Click the rhello.ps1 file and look at its properties. You should see something like this.  
   
   1. You can check the **Unblock** checkbox to unblock the file but what is the fun in that when you can do it in PowerShell. You can use the Unblock-File cmdlet to do just that. We will unblock the file in a few steps. Leave it alone for now.

# Task 3—Modifying the Local User Scope

Now you will change the Execution Policy for just your user. Since this change only affects you, you do not need an elevated shell to perform this action.

## Steps

1. Set the LocalUser scope to Unrestricted. Enter the command:  
   Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
2. Test the policy by running it.  
   ./rhello.ps1
3. This time you should see a warning with the option to run the script or not. Press **R** then **Enter** to allow the script to run.
   1. Record the warning message here: No warning was displayed, unrestricted policy was preset

# Task 4—Modifying the Process Scope

You can change the Execution Policy for just the current PowerShell session using the Process Scope.

## Steps

1. Restrict this shells ability to run scripts. Enter the command  
   Set-ExecutionPolicy -ExecutionPolicy Restricted -Scope Process
2. Run the script  
   ./rhello.ps1
   1. Record your result. Unauthorized access
3. Now set the Process Scope to Bypass. Enter:  
   Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
   1. What was the result? The script ran
   2. How does this result differ from Unrestricted? No warning was given.

# Task 5—Removing Scopes.

## Steps

1. To get a complete list of the execution policies on your machine enter  
   Get-ExecutionPolicy -List
   1. Record each scope’s setting
      1. MachinePolicy Unefined
      2. UserPolicy Unefined
      3. Process Bypass
      4. CurrentUser Unrestricted
      5. LocalMachine Unefined
   2. Without closing your current PowerShell, open a new PowerShell instance and record the execution policy settings.
      1. MachinePolicy Undefined
      2. UserPolicy Undefined
      3. Process Undefined
      4. CurrentUser Unrestricted
      5. LocalMachine Undefined
2. What can you infer about Process settings from this information? Specific to one process only.
3. From the new shell, remove the Current User’s setting by entering  
   Set-ExecutionPolicy -ExecutionPolicy Undefined -Scope CurrentUser
4. Try to run the script. What is your result? Unauthorized access
5. Compare both shells settings, are they the same? No they are not

# Task 6—Unblocking a file

## Steps

1. To make sure we are still on the same page close all PowerShell instances. Next, open a new one.
2. Make **psfiles\scripts** your current folder.
3. Run the script again. It should be blocked. If not, go back through the exercises and see what you did wrong. Your settings should be LocalMachine is **RemotedSigned** with all others **Undefined**.
4. Now unblock the script. Enter the command:  
   Unblock-File .\rhello.ps1
5. Run the file again. What is the result? The script was able to un

# Wrap-up

Set your Execution-Policy scopes to values you feel comfortable with. Record your results here:

1. MachinePolicy undefined
2. UserPolicy undefined
3. Process undefined
4. CurrentUser undefined
5. LocalMachine remote signed

# Deliverable

Upload this document with completed answers to i-learn.