**Malicious PowerShell Execution**

Step 1: Install Sysmon

1. Download Sysmon:
   * From Microsoft Sysinternals: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
2. Download a good config file:
   * Use [SwiftOnSecurity's Sysmon config](https://github.com/SwiftOnSecurity/sysmon-config)
3. Install Sysmon with config:

Open cmd as Administrator:

sysmon64.exe -accepteula -i sysmonconfig-export.xml

You should now see logs under:

Event Viewer → Applications and Services Logs → Microsoft → Windows → Sysmon → Operational

Step 2: Enable PowerShell Script Block Logging (for Event ID 4104)

To get PowerShell script content (important!), enable script block logging:

1. Open PowerShell as Administrator:
2. Set-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging" -Value 1
3. Restart PowerShell or reboot the machine.

Step 3: Simulate a Malicious PowerShell Command

This is only for learning/testing, not real attack use.

In PowerShell:

$cmd = 'Start-Sleep -Seconds 5'

$bytes = [System.Text.Encoding]::Unicode.GetBytes($cmd)

$encoded = [Convert]::ToBase64String($bytes)

powershell.exe -EncodedCommand $encoded

This simulates an encoded PowerShell command (malicious behavior).

Step 4: Check Sysmon Logs in Event Viewer

Go to:

Event Viewer → Applications and Services Logs → Microsoft → Windows → Sysmon → Operational

Look for:

🔍 Event ID 1 – Process Creation

* Image: powershell.exe
* CommandLine: Contains -EncodedCommand
* ParentImage: Could be winword.exe (if run via macro)

🔍 Event ID 4104 – PowerShell Script Block Logging

* Shows decoded PowerShell content (Start-Sleep -Seconds 5)
* Helps understand what the encoded command was doing

Correct Path to View Event ID 4104:

1. Open Event Viewer.
2. Navigate to:
3. Applications and Services Logs
4. → Microsoft
5. → Windows
6. → PowerShell
7. → Operational
8. Now you'll see Event ID 4104 when PowerShell scripts run.