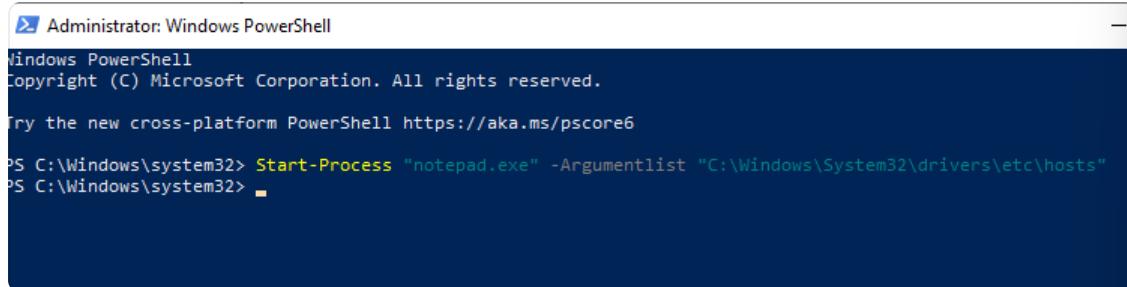


# Day 3: Log Analysis Basics: Windows PowerShell Logs

## Objective:

The objective of this lab is to explore and analyze Windows PowerShell logs to understand how PowerShell-related events are recorded and how they can be used to detect suspicious or malicious activity. It focuses on identifying, interpreting, and correlating PowerShell event IDs to recognize potential indicators of compromise or unauthorized script execution within a Windows environment.

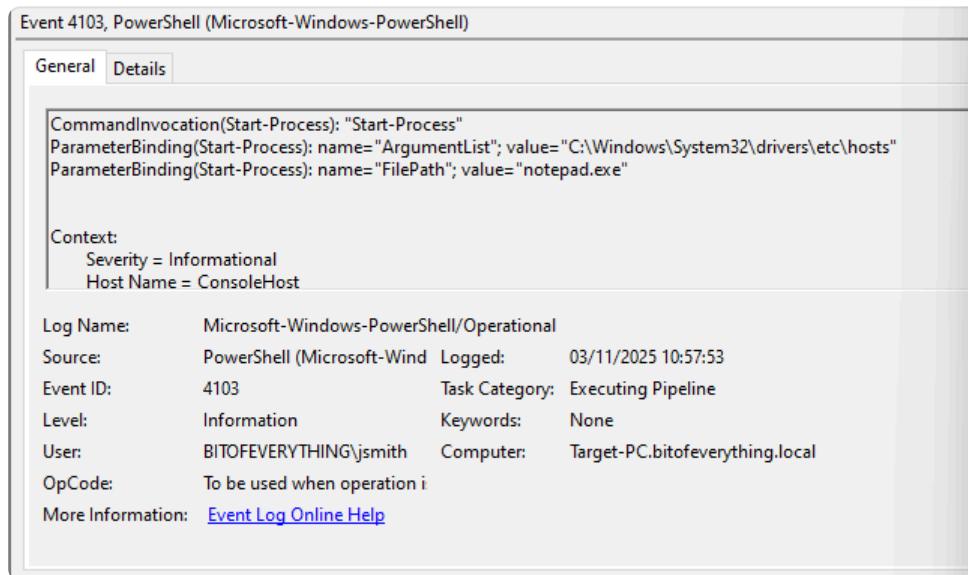


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Start-Process "notepad.exe" -ArgumentList "C:\Windows\System32\drivers\etc\hosts"
PS C:\Windows\system32>
```

Event ID **4103** records **detailed command execution information in PowerShell**. It captures each command that is run, including the parameters used, the process that invoked it, and the user account that executed it. This event is part of **script block logging** and is useful for monitoring what commands are actually being executed in the system, making it easier to detect suspicious or malicious activity, such as attempts to download files, execute payloads, or abuse legitimate tools (LOLBAS) for stealthy attacks.



Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General	Details		
CommandInvocation(Start-Process): "Start-Process" ParameterBinding(Start-Process): name="ArgumentList"; value="C:\Windows\System32\drivers\etc\hosts" ParameterBinding(Start-Process): name="FilePath"; value="notepad.exe"			
Context: Severity = Informational Host Name = ConsoleHost			
Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	03/11/2025 10:57:53
Event ID:	4103	Task Category:	Executing Pipeline
Level:	Information	Keywords:	None
User:	BITOFEVERYTHING\jsmith	Computer:	Target-PC.bitofeverything.local
OpCode:	To be used when operation i		
More Information:	<a href="#">Event Log Online Help</a>		

Event ID **4104**, on the other hand, captures the **contents of executed script blocks**. Whenever a PowerShell script block is executed, 4104 logs the actual code that ran, providing visibility into the script's logic and any potentially malicious instructions. This is especially valuable for detecting obfuscated or hidden commands that may be used in attacks, since it shows the full PowerShell commands and scripts in their executed form.

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):  
prompt

ScriptBlock ID: cf575864-492c-4e87-a8f2-25cd9c6c8ffc  
Path:

Log Name: Microsoft-Windows-PowerShell/Operational  
Source: PowerShell (Microsoft-Wind Logged: 03/11/2025 10:57:53  
Event ID: 4104 Task Category: Execute a Remote Command  
Level: Verbose Keywords: None  
User: BITOFEVERYTHING\jsmith Computer: Target-PC.bitofeverything.local  
OpCode: On create calls  
More Information: [Event Log Online Help](#)

### Conclusion:

In this lab, I learned how to enable and analyze Windows PowerShell logs to monitor command executions and detect potential security threats. I explored key event IDs such as 4103 and 4104, which record detailed information about PowerShell commands, users, and timestamps. Through this process, I gained practical skills in using Event Viewer to identify legitimate versus suspicious PowerShell activity, recognize signs of post-exploitation techniques, and understand the importance of PowerShell logging in threat detection and incident response.