

#90-Days-SOC-Challenge #Hex Security

#Challenge 1

Task #1: Explore and Collect Logs from Windows Event Viewer using PowerShell

Objective:

The goal of this task is to introduce PowerShell-based attack detection using Windows Event Viewer. Students will simulate a suspicious PowerShell command execution, retrieve logs using PowerShell, and analyze the security events that get recorded in the system.

Preparation:

By default, Powershell logs are not enabled. We need to enable both script blok logging and module execution logs.

Enable Logging for PowerShell Execution

- Press Win + R to open the Run dialog.
- Type gpedit.msc and press Enter to open the Group Policy Editor.
- Navigate to the following path: Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell
- Turn on Module Logging
- Turn on Powershell Script Block Logging
- Turn on Script Execution
- Turn on Powershell Transcription
- Apply

Attack Simulation & Detection Using PowerShell

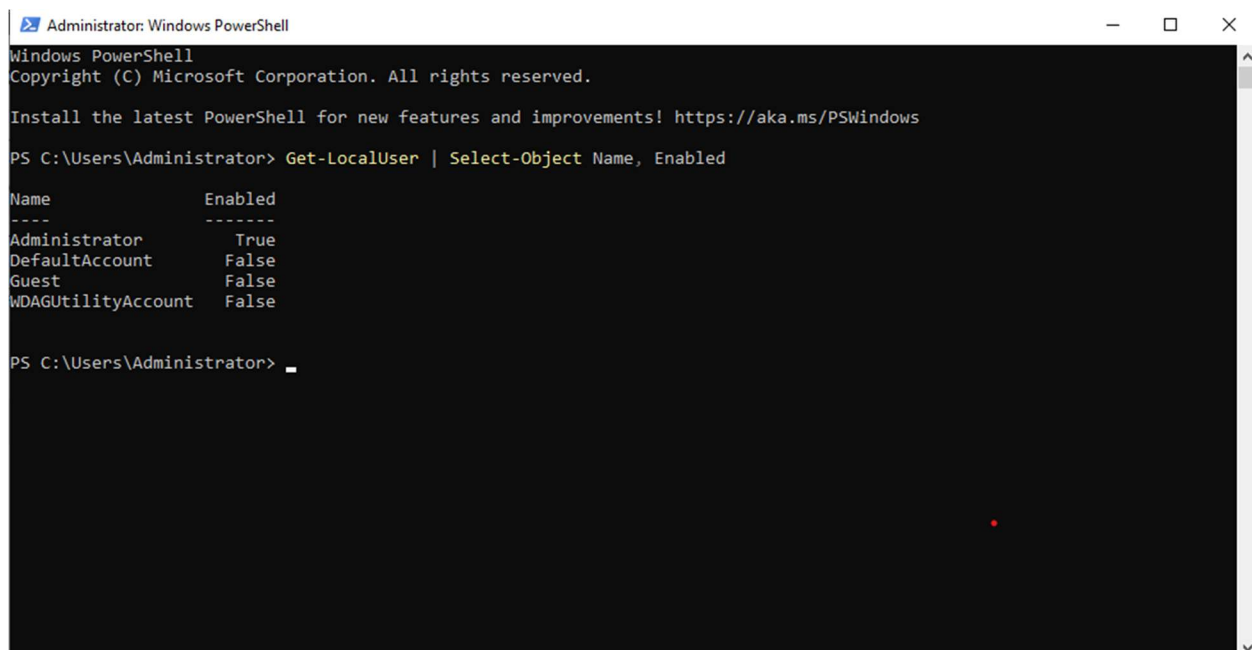
We will now simulate an attacker's reconnaissance technique by executing a PowerShell command that retrieves local user accounts.

Step 1: Execute a Suspicious PowerShell Command

Run the following command in an elevated PowerShell session:

Get-LocalUser | Select-Object Name, Enabled

This command lists all local user accounts on the system along with their status (enabled/disabled). Attackers use similar commands post-exploitation to enumerate users before escalating privileges.



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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-LocalUser | Select-Object Name, Enabled

Name                Enabled
----                -
Administrator       True
DefaultAccount       False
Guest                False
WDAGUtilityAccount   False

PS C:\Users\Administrator> _
```

Step 2: Detect the Attack using Windows Event Viewer

1. Open Event Viewer (Win + R, type eventvwr.msc, press Enter).
2. Navigate to:

Applications and Services Logs → Microsoft → Windows → PowerShell → Operational

3. Click Filter Current Log and enter Event ID 4104 (Execute a Remote Command).
4. Locate the entry showing the execution of the Get-LocalUser command.
5. Take a screenshot of the event details.

Security
Number of events: 963 (1) New events available

Filtered: Log: Security; Source: ; Event ID: 4624, 4625. Number of events: 187

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/26/2025 3:53:32 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/26/2025 3:53:17 PM	Microsoft Windows security auditing.	4624	Logon
Audit Failure	2/26/2025 3:53:04 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	2/26/2025 3:53:00 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	2/26/2025 3:52:56 PM	Microsoft Windows security auditing.	4625	Logon
Audit Success	2/26/2025 3:52:17 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/26/2025 3:50:58 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/26/2025 3:50:58 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/26/2025 3:49:05 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/26/2025 3:44:53 PM	Microsoft Windows security auditing.	4624	Logon

Event 4625, Microsoft Windows security auditing.

General Details

Logon ID: 0x3E7
Logon Type: 7
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: Administrator
Account Domain: WIN-VOF8PP7CKND
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Log Name: Security
Source: Microsoft Windows security Logged: 2/26/2025 3:53:04 PM
Event ID: 4625 Task Category: Logon
Level: Information Keywords: Audit Failure
User: N/A Computer: WIN-VOF8PP7CKND
OpCode: Info
More Information: [Event Log Online Help](#)

Operational
Number of events: 134 (1) New events available

Filtered: Log: Microsoft-Windows-PowerShell/Operational; Source: ; Event ID: 4104. Number of events: 5

Level	Date and Time	Source	Event ID	Task Category
Verbose	2/26/2025 3:24:01 PM	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remote Command
Verbose	2/26/2025 3:24:02 PM	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remote Command
Verbose	2/26/2025 3:24:58 PM	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remote Command
Verbose	2/26/2025 3:24:58 PM	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remote Command
Verbose	2/26/2025 3:24:58 PM	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

☒ Friendly View ☐ XML View

[ActivityID] {a26bcde4-88a4-0002-a5de-6ba2a488db01}
- Execution
[ProcessID] 2464
[ThreadID] 3432
Channel Microsoft-Windows-PowerShell/Operational
Computer WIN-VOF8PP7CKND
- Security
[UserID] S-1-5-21-2475926541-1254565493-1524966021-500
- EventData
MessageNumber 1
MessageTotal 1
ScriptBlockText Get-LocalUser | Select-Object Name, Enabled
ScriptBlockId b32228a3-5ff3-4602-bb85-ed4156f8a7d7
Path

Step 3: Retrieve Logs using PowerShell (Alternative Detection Method)

Instead of using Event Viewer, use PowerShell to directly extract the event:

Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" | Where-Object {\$_.Id -eq 4104} | Select-Object TimeCreated, Message

- This command fetches all script block executions from PowerShell logs and filters them by Event ID 4104.
- Look for the command Get-LocalUser in the output.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" | Where-Object {$_.Id -eq 4104} | Select-Object TimeCreated, Message

TimeCreated      Message
-----
2/26/2025 6:53:34 PM Creating Scriptblock text (1 of 1):...
2/26/2025 6:53:34 PM Creating Scriptblock text (1 of 1):...
2/26/2025 6:50:43 PM Creating Scriptblock text (1 of 1):...
2/26/2025 6:50:43 PM Creating Scriptblock text (1 of 1):...
2/26/2025 6:50:38 PM Creating Scriptblock text (1 of 1):...
2/26/2025 6:50:38 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:24:21 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:24:21 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:24:06 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:24:06 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:24:06 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:23:47 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:23:47 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:23:47 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:21:32 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:21:32 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:21:09 PM Creating Scriptblock text (1 of 1):...
2/26/2025 4:21:09 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:56:50 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:56:50 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:56:44 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:56:44 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:41 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:41 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:39 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:34 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:34 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:31 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:25 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:25 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:02 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:55:01 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:54:59 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:54:59 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:32:29 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:32:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:32:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:30 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:29 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
2/26/2025 3:29:28 PM Creating Scriptblock text (1 of 1):...
```

Lesson Learn:

- I have learnt PowerShell is a very powerful tool for not just automating and managing, but also for monitoring and security auditing.
- By enabling features like module logging, script block logging, and transcription, I can track what is happening on a system in a detailed way which is very useful for incident detection.