

Task #2: Identify Failed and Successful Logins from Windows Logs

Objective

The goal of this task is to help students analyze Windows login events and understand how to differentiate between successful and failed login attempts using Windows Event Viewer and PowerShell. By the end of this task, students will be able to detect suspicious login activities and identify possible brute-force attempts.

Attack Simulation & Detection Using PowerShell

We will now simulate both successful and failed login attempts and analyze them in Event Viewer.

Step 1: Simulate Login Events

Successful Login:

Lock your machine (Win + L) and log in with the correct password. This will generate a successful login event (Event ID 4624). Failed Login Attempt:

Lock your machine again and try logging in with the wrong password at least three times. This will generate failed login events (Event ID 4625).

Step 2: Detect Login Events using Windows Event Viewer

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

Windows Logs → Security

3. Click Filter Current Log and enter the following Event IDs:
 - 4624 → Successful login
 - 4625 → Failed login
4. Locate the logs corresponding to the login attempts and take a screenshot.

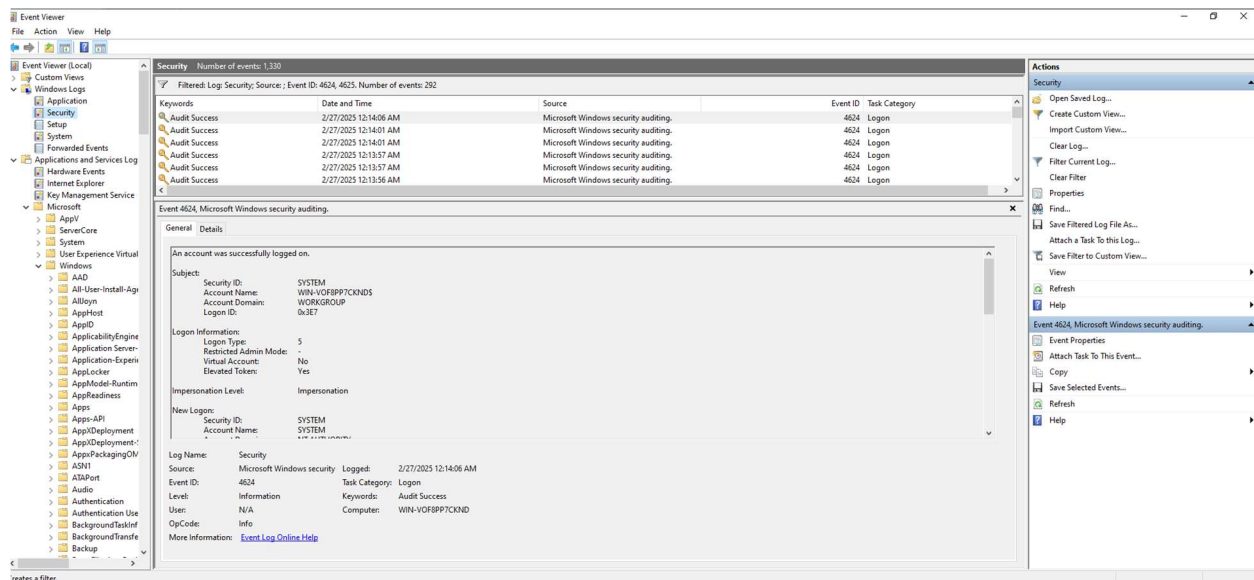


Figure 1 Successful Login EventID 4624

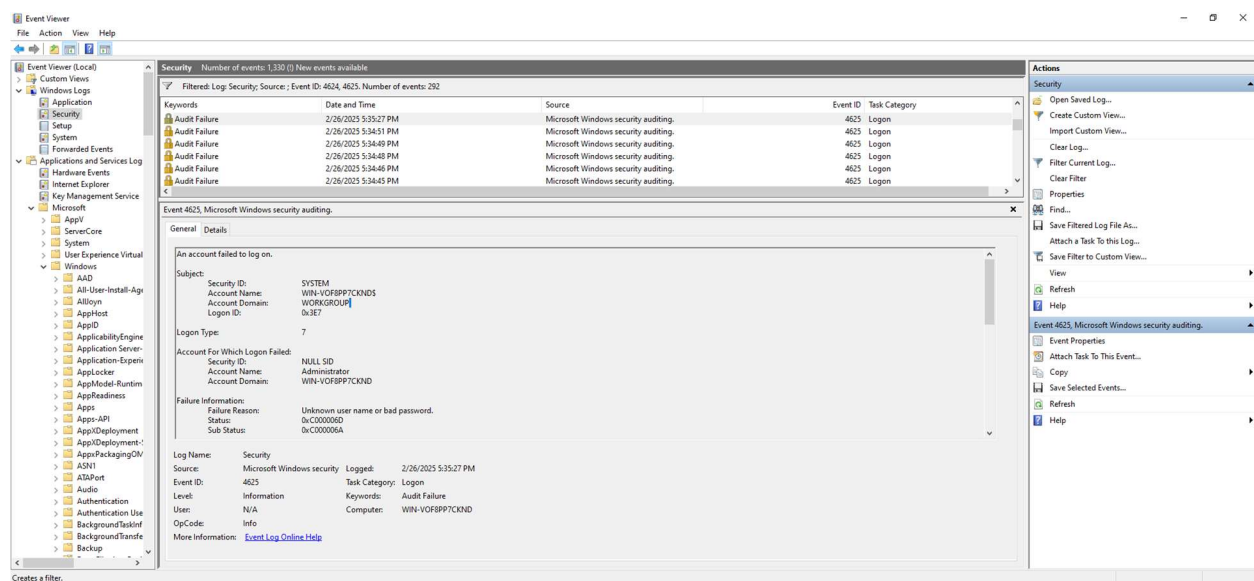


Figure 2 Failed Login EventID 4625

Step 3: Retrieve Login Events using PowerShell

Instead of using Event Viewer, use PowerShell to extract and analyze login attempts:

Check for Successful Logins

```
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624} | Select-Object TimeCreated, Message | Format-Table -AutoSize
```

- This command retrieves all successful login events from the Security log.

```
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-WinEvent -FilterHashtable @{LogName='Security'; ID=4624} | Select-Object TimeCreated, Message | Format-Table -AutoSize

TimeCreated      Message
-----
2/27/2025 12:15:46 AM An account was successfully logged on....
2/27/2025 12:15:46 AM An account was successfully logged on....
2/27/2025 12:15:42 AM An account was successfully logged on....
2/27/2025 12:15:42 AM An account was successfully logged on....
2/27/2025 12:15:41 AM An account was successfully logged on....
2/27/2025 12:14:06 AM An account was successfully logged on....
2/27/2025 12:14:01 AM An account was successfully logged on....
2/27/2025 12:14:01 AM An account was successfully logged on....
2/27/2025 12:13:57 AM An account was successfully logged on....
2/27/2025 12:13:57 AM An account was successfully logged on....
2/27/2025 12:13:56 AM An account was successfully logged on....
2/27/2025 12:13:42 AM An account was successfully logged on....
2/27/2025 12:13:40 AM An account was successfully logged on....
2/27/2025 12:13:40 AM An account was successfully logged on....
2/27/2025 12:13:40 AM An account was successfully logged on....
2/27/2025 12:13:39 AM An account was successfully logged on....
2/27/2025 12:13:39 AM An account was successfully logged on....
2/27/2025 12:13:39 AM An account was successfully logged on....
2/27/2025 12:13:39 AM An account was successfully logged on....
2/27/2025 12:13:39 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:38 AM An account was successfully logged on....
2/27/2025 12:13:37 AM An account was successfully logged on....
2/27/2025 12:13:37 AM An account was successfully logged on....
2/27/2025 12:13:37 AM An account was successfully logged on....
2/27/2025 12:13:36 AM An account was successfully logged on....
2/27/2025 12:13:36 AM An account was successfully logged on....
2/27/2025 12:13:36 AM An account was successfully logged on....
2/27/2025 12:13:36 AM An account was successfully logged on....
2/26/2025 7:02:33 PM An account was successfully logged on....
```

Check for Failed Logins

Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625} | Select-Object TimeCreated, Message | Format-Table -AutoSize

- This command retrieves all failed login attempts from the Security log.

```
Administrator Windows PowerShell

PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625} | Select-Object TimeCreated, Message | Format-Table -AutoSize

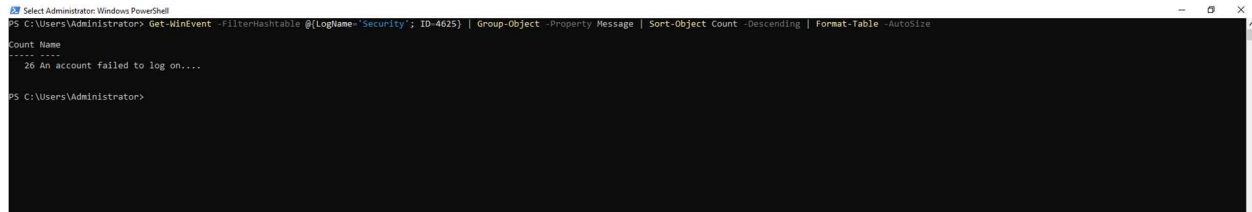
TimeCreated      Message
-----
2/26/2025 5:36:20 PM An account failed to log on....
2/26/2025 5:35:27 PM An account failed to log on....
2/26/2025 5:34:51 PM An account failed to log on....
2/26/2025 5:34:49 PM An account failed to log on....
2/26/2025 5:34:48 PM An account failed to log on....
2/26/2025 5:34:46 PM An account failed to log on....
2/26/2025 5:34:45 PM An account failed to log on....
2/26/2025 5:34:44 PM An account failed to log on....
2/26/2025 5:33:14 PM An account failed to log on....
2/26/2025 5:33:13 PM An account failed to log on....
2/26/2025 5:33:12 PM An account failed to log on....
2/26/2025 5:33:12 PM An account failed to log on....
2/26/2025 5:33:10 PM An account failed to log on....
2/26/2025 5:33:10 PM An account failed to log on....
2/26/2025 5:33:09 PM An account failed to log on....
2/26/2025 5:29:54 PM An account failed to log on....
2/26/2025 5:29:52 PM An account failed to log on....
2/26/2025 5:29:51 PM An account failed to log on....
2/26/2025 5:29:50 PM An account failed to log on....
2/26/2025 5:29:48 PM An account failed to log on....
2/26/2025 5:28:38 PM An account failed to log on....
2/26/2025 5:28:36 PM An account failed to log on....
2/26/2025 5:28:34 PM An account failed to log on....
2/26/2025 5:28:32 PM An account failed to log on....
2/26/2025 3:53:04 PM An account failed to log on....
2/26/2025 3:53:00 PM An account failed to log on....
2/26/2025 3:52:56 PM An account failed to log on....

PS C:\Users\Administrator>
```

Analyze Login Attempts for Possible Brute-Force Activity To check for multiple failed login attempts from the same user or IP:

Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625} | Group-Object -Property Message | Sort-Object Count -Descending | Format-Table -AutoSize

- If you see multiple failed attempts for the same account within a short time, it might indicate brute-force activity.



```
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @(LogName= Security ; ID=4625) | Group-Object -Property Message | Sort-Object Count -Descending | Format-Table -AutoSize

Count Name
-----
26 An account failed to log on...
```

Learning Outcomes

- Understanding of Windows Security Logs.
- Ability to detect brute-force attacks.
- Practical use of PowerShell for log analysis.