

Lab #04a: Windows Event Viewer Exploration

Goal: Identify a failed login attempt and a system shutdown event using Event Viewer

Learning Objectives:

- Navigate Windows Event Viewer
- Analyze different types of logs (Application, Security, System)
- Locate and interpret a **failed login attempt**
- Locate and interpret a **system shutdown or reboot event**

Lab Environment Requirements:

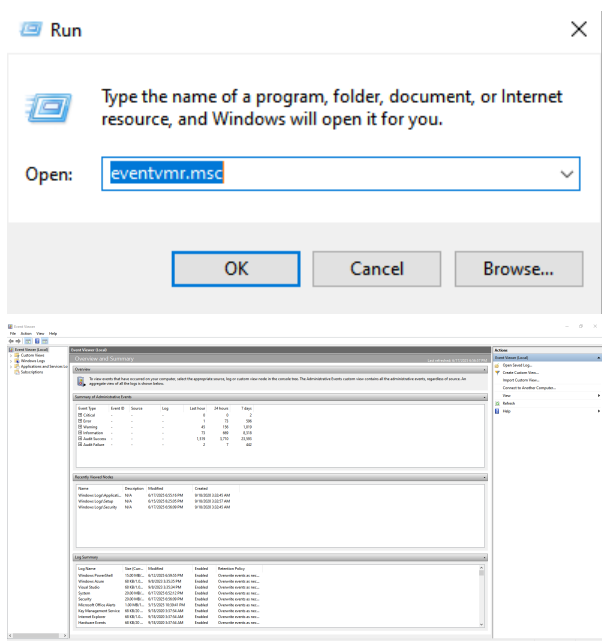
- A Windows system (Windows 10 or 11 recommended)
- Admin privileges

Step-by-Step Instructions / Summary

- Step 1: Open Event Viewer
- Step 2: Explore Log Types
- Step 3: Locate a Failed Login Attempt
- Step 4: Trigger a Failed Login
- Locate a Shutdown or Restart Event

1. Open Event Viewer

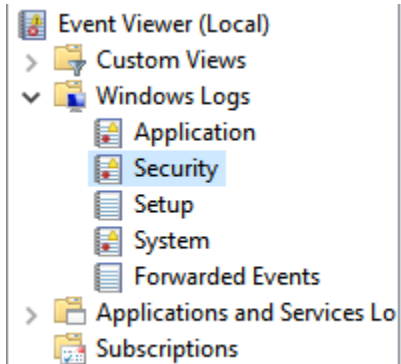
Press Windows + R
type eventvwr.msc
press Enter



2. Explore Log Types

a. Expand the following in the left panel

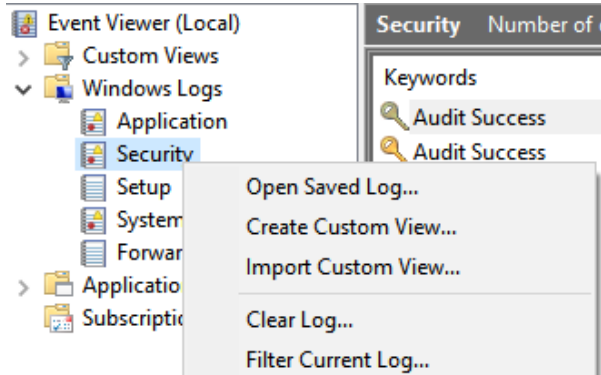
Press to expand the Windows Logs to show the following: Application, Security, and System.



Security Number of events: 32,675 (!) New events available	
Keywords	Date and Time
Audit Success	6/17/2025 7:02:15 PM
Audit Success	6/17/2025 7:02:15 PM
Audit Success	6/17/2025 7:02:15 PM
Audit Success	6/17/2025 7:02:15 PM
Audit Success	6/17/2025 7:02:15 PM
Audit Success	6/17/2025 7:00:59 PM
Audit Success	6/17/2025 7:00:59 PM

3. Locate a Failed Login Attempt

Right click security
Click Filter Current Log



Apply filter
Set Event IDs: 4625 (Failed login)

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

User:






<All Users>

Computer(s):

<All Computers>

Clear

After the filter

Keywords	Date and Time	Source	Event ID	Task Category
 Audit Failure	6/19/2025 8:29:19 AM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	6/18/2025 10:24:23 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	6/17/2025 5:28:51 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	6/17/2025 5:22:41 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	6/13/2025 12:25:03 PM	Microsoft Windows security auditing.	4625	Logon

Required questions:

What was the **username** attempted?

Administrator

What is the **Logon Type**?

2

What is the **Failure Reason**?

Audit Failure

Logon Type:

2

Account For Which Logon Failed:

Security ID:

NULL SID

Account Name:

Administrator

Logged:

6/19/2025 8:29:19 AM

Task Category: Logon

Keywords:

Audit Failure

4. Trigger a New Failed Login

- Log out and try to login with an incorrect password
- Repeat Step 3 to find new entry

After signing out, I used a guest account and then utilized the run command to open Event Viewer and next I applied the filter for id 4625.

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

User:

Computer(s):

The listed events:

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 14

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	6/19/2025 4:42:01 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:41:58 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:41:50 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:38:23 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:38:18 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:38:18 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/19/2025 4:05:21 PM	Microsoft Windows security auditing.	4625	Logon

Required questions with different user:

What was the **username** attempted?

GuestAccount

What is the **Logon Type**?

2

What is the **Failure Reason**?

Audit Failure

Logon Type: 2

Account For Which Logon Failed:

Security ID: NULL SID
Account Name: GuestAccount
Account Domain: LONGPC

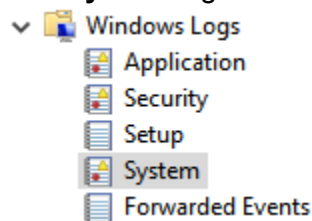
Logged: 6/19/2025 4:05:21 PM

Task Category: Logon

Keywords: Audit Failure

5. Locate a Shutdown or Restart Event

Click **System** log:



After clicking the System log:

Level	Date and Time	Source	Event ID	Task Category
Warning	6/19/2025 5:08:08 PM	DNS Client Events	1014	(1014)
Warning	6/19/2025 5:01:25 PM	DistributedCOM	10016	None
Warning	6/19/2025 4:55:29 PM	DistributedCOM	10016	None
Warning	6/19/2025 4:48:18 PM	DistributedCOM	10016	None
Information	6/19/2025 4:46:59 PM	Service Control Manager	7040	None

Filter by Event IDs:

1074 (Planned shutdown/restart)

Required questions:

Was it planned or unexpected?

It was planned

Who initiated it?

It was initiated by SYSTEM

What was the reason?

Operating System: **Upgrade** (Planned)

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

1074

The process C:\WINDOWS\servicing\TrustedInstaller.exe (LONGPC) has initiated the restart.

following reason: Operating System: Upgrade (Planned)

Shutdown Type: restart

Level	Date and Time
Information	6/12/2025 7:07:45 PM
Information	6/12/2025 6:57:02 PM
Information	6/9/2025 10:30:40 PM
Information	6/8/2025 11:44:19 PM
Information	6/6/2025 11:59:11 PM

Log Name: System

Source: User32

Event ID: 1074

Level: Information

User: SYSTEM

OpCode: Info

6006 (Event log service shutdown – system going down)

Required questions:

Was it planned or unexpected?

It was Planned (Clean shutdown)

Who initiated it?

Not specified or N/A

What was the reason?

Event log service stopped due to restart/shutdown

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

6006

The Event log service was stopped.

Level	Date and Time
Information	6/18/2025 11:16:41 PM
Information	6/17/2025 11:19:06 PM
Information	6/15/2025 8:25:03 PM
Information	6/13/2025 2:03:13 PM
Information	6/13/2025 3:20:31 AM

	<p>Log Name: System</p> <p>Source: EventLog</p> <p>Event ID: 6006</p> <p>Level: Information</p> <p>User: N/A</p> <p>OpCode: Info</p>
--	--

6008 (Unexpected shutdown)

<p>Required questions:</p> <p>Was it planned or unexpected? It was not planned</p> <p>Who initiated it? Not specified or N/A</p> <p>What was the reason? User initiated shutdown</p>	<p>Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">6008</div> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 60%;">Level</th> <th style="text-align: left; width: 40%;">Date and Time</th> </tr> </thead> <tbody> <tr><td>❗ Error</td><td>6/12/2025 4:14:55 PM</td></tr> <tr><td>❗ Error</td><td>4/13/2025 5:17:23 PM</td></tr> <tr><td>❗ Error</td><td>3/29/2025 7:46:37 PM</td></tr> <tr><td>❗ Error</td><td>3/20/2025 6:13:18 PM</td></tr> <tr><td>❗ Error</td><td>3/20/2025 10:47:19 AM</td></tr> </tbody> </table> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">The previous system shutdown at 11:08:07 PM on 6/10/2025 was unexpected.</div> <div style="background-color: #f0f0f0; padding: 10px;"> <p>Log Name: System</p> <p>Source: EventLog</p> <p>Event ID: 6008</p> <p>Level: Error</p> <p>User: N/A</p> <p>OpCode: Info</p> </div>	Level	Date and Time	❗ Error	6/12/2025 4:14:55 PM	❗ Error	4/13/2025 5:17:23 PM	❗ Error	3/29/2025 7:46:37 PM	❗ Error	3/20/2025 6:13:18 PM	❗ Error	3/20/2025 10:47:19 AM
Level	Date and Time												
❗ Error	6/12/2025 4:14:55 PM												
❗ Error	4/13/2025 5:17:23 PM												
❗ Error	3/29/2025 7:46:37 PM												
❗ Error	3/20/2025 6:13:18 PM												
❗ Error	3/20/2025 10:47:19 AM												



Tools & Skills Used

- Windows Event Viewer
- Security & System Log Analysis
- Event ID Filtering



Reflection & Takeaways

This lab helped me refresh my skills in navigating and analyzing logs using Windows Event Viewer. I found the **Security** logs to be the most helpful, especially in identifying any failed login attempts. As for the **System** logs, they provide me information about shutdowns and restarts.

Monitoring logs is an essential skill in cybersecurity because they can help detect suspicious activity, identify insider threats, and understand system events. My takeaway of this lab is the importance to distinguish false negatives and false positives providing critical to threat detection and response.