

Windows Event Log Generation and Analysis Activity.

1. Objective.

The objective of this activity was to generate and analyze windows event logs to understand how user actions are recorded by the Operating System. This exercise helps on developing log analysis skills that are essential for cybersecurity.

2. Actions performed.

The experiment was conducted on a Windows 11 machine to observe how user actions are captured within Windows event Logs.

1. An incorrect password was entered to simulate a failed login.
2. A correct password was used to sign in to the machine.
3. The command prompt was executed with administrative privileges.
4. A new file was created on Document folder.
5. The Local Security Policy was opened, and auditing was initiated to generate additional policy-related events.

3. Path to Event logs.

1. Win + R
2. type **eventvwr.msc**
3. Windows Logs

Or

1. Go to drive (C)
2. Windows.
3. system32.
4. winevt.
5. logs.

4. Logs Collected.

4.1. Security Logs.

These logs show login attempts, user actions and policy changes etc.

Event ID.	Description.	Explanation.
4625	Failed logon attempt.	User entered wrong password.
4624	Successful logon.	User logged in successfully.
4672	Special privileges assigned.	Administrator privileges granted.
4798	User's group membership calculated.	Accessed Local Security policy.
5061 ,5379 ,5058	Credential events.	System verified credentials or encryption operations.

4.2. Application Logs.

These logs show logs from software and applications.

Event ID.	Description.	Explanation.
16384	Program or service started.	Windows or an app started running as a background service.
8233	System backup .	Windows started a background process like a backup.
12288	Windows tool opened.	A system tool or a setting like Local Security Policy was used.
16394	App or service check.	Windows checked or verified a service or program.
256	Command Prompt started.	CMD was opened with administrator rights.

4.3. Security Logs.

These logs record what the Operating system and hardware are doing (drivers, services, startup, shutdown etc.)

Event ID	Description.	Explanation.
566	Object access event.	Windows tracked access to a system object .(This often linked to auditing.)
158	Disk or storage event.	Windows detected a storage volume ,normal during boot or a file creation.
10016	DCOM permission issue.	A windows component tried to use a service but didn't have full permission.
1	System or driver started.	Shows system startup , driver load, or a service beginning to run.
187	Disk or file system warning.	Windows noticed a temporary disk or file system problem but recovered.

4.3. Setup Logs.

No setup events were recorded during this activity because no software installation or updates were performed on the system. The setup log records events related to windows installation, updates or major configuration changes.

5. Why Log Analysis is Important?

Log analysis is one of the most important skills in cybersecurity. This helps security teams to detect, investigate and respond to attacks.

Event logs helps to keep in track of activities that happened in the system like logging in, running programs, or changing settings. These activities leave a record on event logs based on the category. By analyzing these logs professionals can spot unusual or suspicious behaviors.

6. What I learned.

Throughout this activity, I learned how to use the Windows Event viewer to observe and analyze system events. I understood that every action performed on the system such as logging in, running commands, creating or deleting a file, leaves a trace in event logs. By examining different log categories like security, application, system and setup, I learned how to identify which types of activities generate specific Event IDs. This helped me to understand the importance of event logs in detecting unauthorized access, troubleshooting system issues and maintaining overall security visibility.