Event Logging in Windows and Linux

**Introduction**

Event logs are like the black boxes of our computers. They quietly record everything happening under the hood—good, bad, and suspicious. Whether it's a user logging in, a failed service, or someone trying to access files they shouldn't—logs catch it all.

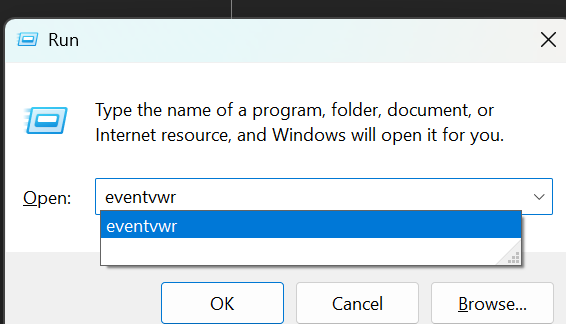
In this report, I explored how logging works on both **Windows** and **Linux**, how to view logs, what commands are useful, and how we can spot real activity (or even threats) using those logs.

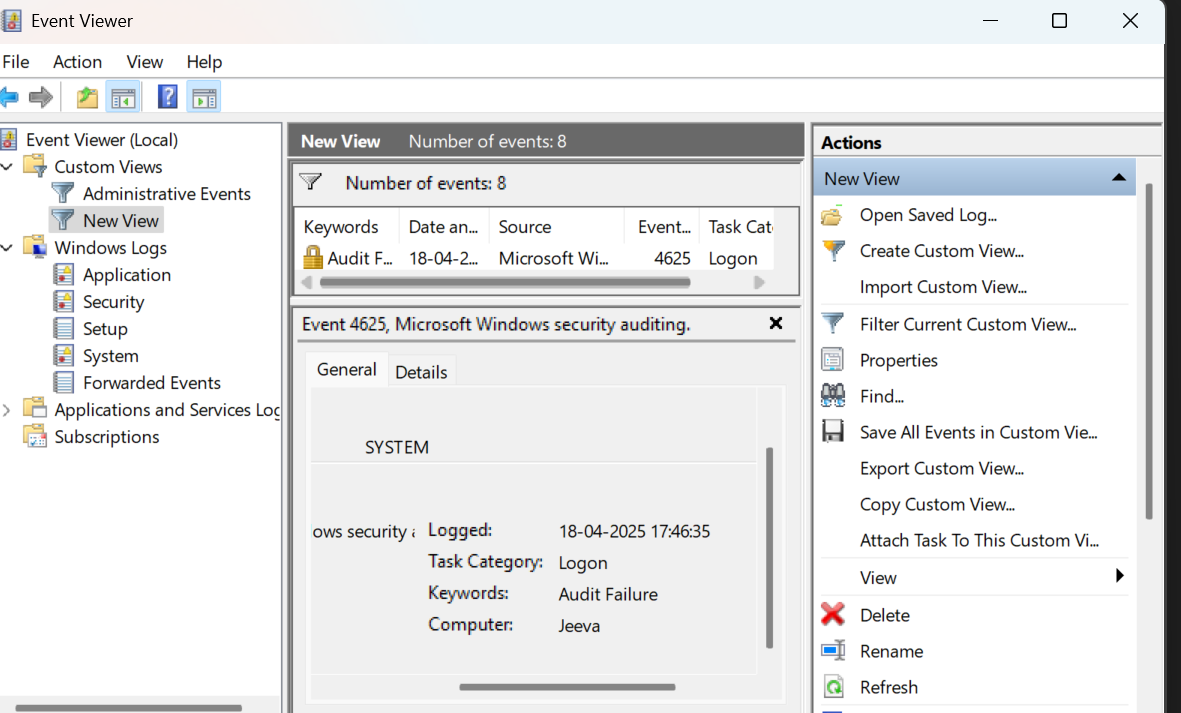
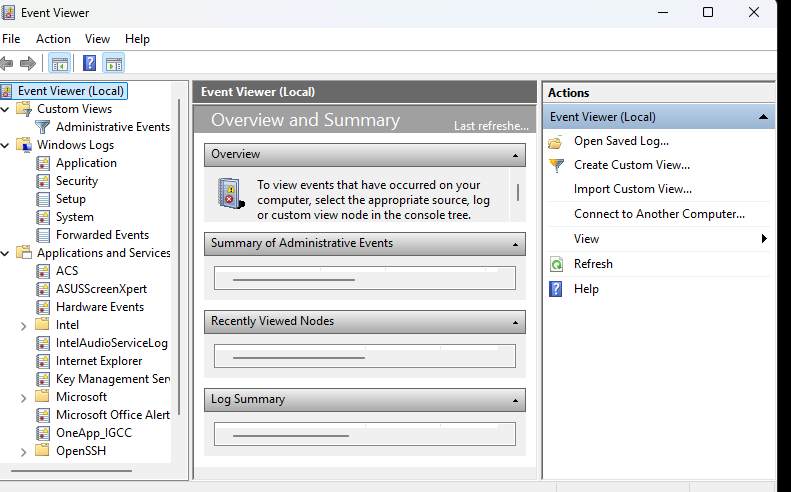
**Why Event Logging is Important**

* It helps **troubleshoot system problems**.
* Logs record **security events** like logins or file access.
* We can use logs to **detect suspicious activity** (e.g., brute force attempts).
* For companies, logs are vital for **compliance** and **audits**.

**Checking Logs Using Event Viewer**

To open:





This filter is for login failure even ID which is 4625.

**Useful PowerShell Commands**

These are more practical when you're on multiple systems or want to automate.

**View Latest System Logs:**

Get-EventLog -LogName System -Newest 10

**Get Failed Login Attempts (Security ID: 4625):**

Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625}

**Export Logs to File:**

wevtutil epl System "C:\logs\systemlog.evtx"

**Linux Logging Basics**

Linux systems rely heavily on text-based logs stored in /var/log. Depending on the distro, you might see files like syslog, auth.log, or messages.

📝 Example Log Files:

* /var/log/syslog – General system events (Ubuntu)
* /var/log/auth.log – SSH logins, sudo use
* /var/log/messages – General events (CentOS)

**Commands to View Linux Logs**

Here are commands I tested:

cat /var/log/syslog # View entire log

tail -f /var/log/auth.log # Monitor auth in real-time

grep "Failed password" auth.log # Find failed SSH logins

less /var/log/dmesg # View boot/kernel logs

**Real Linux Example – SSH Login Check**

grep "Accepted password" /var/log/auth.log

*Use case:* You can find who successfully logged in, from which IP, and when

grep "Failed password" /var/log/auth.log

*Use case:* Spot failed login attempts, possibly from bots or hackers.

**Using journalctl (Systemd Systems)**

This command helps you navigate newer logs more smoothly.

**View Everything:**

journalctl

View SSH logs:

journalctl -u ssh

View logs since yesterday:

journalctl --since "yesterday"

