Common Event ID's for Forensic & SOC Analysts

By,

Asif Khan

Sr. Cyber Forensics Expert

https://www.linkedin.com/in/asif-khan-b5379a126/

Common Event ID's

Certainly! Understanding common **Event IDs** and their meanings is crucial for interpreting Windows Event Logs effectively. Event IDs are numerical codes that uniquely identify specific events within the Windows operating system. They help **administrators** and **forensic analysts** to quickly recognize and respond to various system, security, and application events.

In this comprehensive guide, we'll cover common Event IDs across different logs, including their descriptions and significance in forensic analysis.

Table of Contents

---

1. Introduction to Event IDs

- **Definition:** An Event ID is a numerical code that identifies a specific event or type of event within Windows Event Logs.
- **Purpose:** Helps in filtering, searching, and interpreting events during system administration and forensic investigations.
- **Event Logs Categories:**
    - **System Log:** Records events logged by Windows system components.

- **Security Log:** Records security-related events, such as logon attempts and resource access.
- **Application Log:** Records events logged by applications.
- **Setup Log:** Records events related to application setup and installation.
- **Application and Service Logs:** Records events from individual applications and services.

---

2. System Log Event IDs

2.1 Service Control Manager Events

- **Event ID 7000:** *"The service failed to start due to the following error..."*
  - **Description:** A service failed to start.
  - **Significance:** Could indicate system instability or misconfigurations.
- **Event ID 7001:** *"The service depends on the service which failed to start..."*
  - **Description:** A dependent service failed to start.
  - **Significance:** Helps identify cascading failures.
- **Event ID 7034:** *"The service terminated unexpectedly..."*
  - **Description:** A service terminated unexpectedly.
  - **Significance:** May indicate software bugs or malicious activity.
- **Event ID 7040:** *"The start type of the service was changed from..."*
  - **Description:** Indicates a change in the startup type of a service.
  - **Significance:** Potentially unauthorized changes to services.
- **Event ID 7045:** *"A service was installed in the system."*
  - **Description:** A new service was installed.
  - **Fields to Examine:**
    - **Service Name**
    - **Service File Name**
    - **Service Type**
  - **Significance:** Important for detecting unauthorized or malicious services.

2.2 System Shutdown and Startup Events

- **Event ID 6005:** *"The Event Log service was started."*
    - **Description:** Indicates system startup.
    - **Significance:** Helps establish timelines.
- **Event ID 6006:** *"The Event Log service was stopped."*
    - **Description:** Indicates system shutdown.
    - **Significance:** Helps establish timelines.
- **Event ID 6008:** *"The previous system shutdown was unexpected."*
    - **Description:** Indicates an improper shutdown.
    - **Significance:** May result from system crashes or power loss.

2.3 Time Change Events

- **Event ID 1 (Kernel-General):** *"The system time has changed to..."*
    - **Description:** System time was changed.
    - **Fields to Examine:**
        - **Previous Time**
        - **New Time**
    - **Significance:** Time changes can affect log analysis and may indicate tampering.

2.4 Disk and Hardware Events

- **Event ID 7 (Disk):** *"The device, \Device\Harddisk0\DR0, has a bad block."*
    - **Description:** Indicates a bad sector on the hard disk.
    - **Significance:** May lead to data corruption or system instability.
- **Event ID 51 (Disk):** *"An error was detected on device \Device\Harddisk0\DR0 during a paging operation."*
    - **Description:** Disk I/O error.
    - **Significance:** Could indicate failing hardware.

---

3. Security Log Event IDs

3.1 Successful Logon Events

- **Event ID 4624:** *"An account was successfully logged on."*
    - **Description:** A user successfully logged on to the system.

- **Fields to Examine:**
  - **Logon Type**
  - **Account Name**
  - **Source Network Address**
- **Logon Types:**
  - **2:** Interactive (local console)
  - **3:** Network (e.g., accessing shared resources)
  - **10:** RemoteInteractive (Remote Desktop)
- **Significance:** Essential for tracking user activity.

3.2 Failed Logon Events

- **Event ID 4625:** *"An account failed to log on."*
  - **Description:** A failed logon attempt occurred.
  - **Fields to Examine:**
    - **Failure Reason**
    - **Account Name**
    - **Logon Type**
    - **Source Network Address**
  - **Significance:** May indicate password guessing or unauthorized access attempts.

3.3 Account Management Events

- **Event ID 4720:** *"A user account was created."*
  - **Description:** A new user account was created.
  - **Significance:** Important for detecting unauthorized account creations.
- **Event ID 4722:** *"A user account was enabled."*
  - **Description:** An account was re-enabled after being disabled.
  - **Significance:** May be used to regain access to a disabled account.
- **Event ID 4725:** *"A user account was disabled."*
  - **Description:** An account was disabled.
  - **Significance:** Could be part of normal operations or indicate malicious activity.

- **Event ID 4726:** *"A user account was deleted."*
    - **Description:** An account was deleted.
    - **Significance:** Important for auditing account deletions.

3.4 Privilege Use Events

- **Event ID 4672:** *"Special privileges assigned to new logon."*
    - **Description:** A user logged on with administrative privileges.
    - **Significance:** Critical for detecting privileged account usage.

3.5 Audit Log Clearing

- **Event ID 1102:** *"The audit log was cleared."*
    - **Description:** Security log was cleared.
    - **Significance:** Potential indicator of malicious activity attempting to cover tracks.

3.6 System Integrity Events

- **Event ID 4616:** *"The system time was changed."*
    - **Description:** Indicates a change in system time.
    - **Significance:** May affect log analysis and indicate tampering.

---

4. Application Log Event IDs

4.1 Application Errors

- **Event ID 1000 (Application Error):** *"Faulting application name..."*
    - **Description:** Indicates that an application crashed.
    - **Fields to Examine:**
        - **Faulting Application Name**
        - **Faulting Module Name**
        - **Exception Code**
    - **Significance:** Useful for diagnosing application crashes.

4.2 Application Hang

- **Event ID 1002 (Application Hang):** *"The program [application name] version [version] stopped interacting with Windows..."*
    - **Description:** An application became unresponsive.

- **Significance:** May indicate performance issues or resource exhaustion.

4.3 MsiInstaller Events

- **Event ID 11707:** *"Installation of [product name] succeeded."*
  - **Description:** An application was installed successfully.
  - **Significance:** Helps track software installations.
- **Event ID 11708:** *"Installation of [product name] failed."*
  - **Description:** An application installation failed.
  - **Significance:** May indicate issues with software deployment.

---

5. Setup Log Event IDs

5.1 Windows Update Events

- **Event ID 19 (WindowsUpdateClient):** *"Installation Successful: Windows successfully installed the following update..."*
  - **Description:** A Windows Update was installed successfully.
  - **Significance:** Important for ensuring systems are up to date.
- **Event ID 20 (WindowsUpdateClient):** *"Installation Failure: Windows failed to install the following update..."*
  - **Description:** A Windows Update installation failed.
  - **Significance:** May leave the system vulnerable.
- **Event ID 21 (WindowsUpdateClient):** *"Installation Pending: Windows is waiting to install the following update..."*
  - **Description:** A Windows Update is pending installation.
  - **Significance:** Indicates updates that require action.

5.2 System Installation Events

- **Event ID 300 (Setup):** *"The Windows installer has initiated a system restart to complete the installation or update..."*
  - **Description:** Indicates a restart initiated by an installer.
  - **Significance:** Helps track system changes.

---

6. Application and Service Logs Event IDs

6.1 PowerShell Logs

- **Event ID 4103 (Microsoft-Windows-PowerShell):** *"PowerShell Pipeline Execution Details."*
    - **Description:** Logs details about executed PowerShell commands.
    - **Significance:** Useful for detecting malicious scripts.
- **Event ID 4104 (Microsoft-Windows-PowerShell):** *"PowerShell Script Block Logging."*
    - **Description:** Captures the content of PowerShell scripts executed.
    - **Significance:** Critical for detecting and analyzing malicious PowerShell activity.

6.2 Sysmon Logs

- **Event ID 1 (Sysmon):** *"Process creation detected."*
    - **Description:** Logs when a process is created.
    - **Significance:** Provides detailed process information for threat hunting.
- **Event ID 3 (Sysmon):** *"Network connection detected."*
    - **Description:** Logs network connections initiated by processes.
    - **Significance:** Helps identify suspicious network activity.

6.3 Windows Defender Logs

- **Event ID 1000 (Windows Defender):** *"Malware Detection."*
    - **Description:** Malware was detected on the system.
    - **Significance:** Indicates potential compromise.
- **Event ID 1116 (Windows Defender):** *"Antivirus scan started."*
    - **Description:** An antivirus scan was initiated.
    - **Significance:** Helps track security operations.

6.4 Task Scheduler Logs

- **Event ID 106 (TaskScheduler):** *"Task registered or updated."*
    - **Description:** A scheduled task was created or modified.
    - **Significance:** Attackers may use scheduled tasks for persistence.

6.5 Remote Desktop Services Logs

- **Event ID 1149 (TerminalServices-RemoteConnectionManager):** *"Remote Desktop Services: User authentication succeeded."*

- **Description:** A user successfully authenticated via RDP.
- **Significance:** Important for monitoring remote access.

---

7. Event IDs Related to Account Management

- **Event ID 4727:** *"A security-enabled global group was created."*
- **Event ID 4728:** *"A member was added to a security-enabled global group."*
- **Event ID 4732:** *"A member was added to a security-enabled local group."*
- **Event ID 4756:** *"A member was added to a security-enabled universal group."*
- **Event ID 4767:** *"A user account was unlocked."*

Significance: Changes to group memberships and account statuses can indicate privilege escalation or account misuse.

---

8. Event IDs Related to Logon and Logoff

- **Event ID 4634:** *"An account was logged off."*
  - **Description:** A user logged off from the system.
  - **Significance:** Helps track session durations.
- **Event ID 4647:** *"User initiated logoff."*
  - **Description:** The user initiated a logoff.
  - **Significance:** Differentiates between user-initiated and system-initiated logoffs.
- **Event ID 4648:** *"A logon was attempted using explicit credentials."*
  - **Description:** Credentials were used to log on on behalf of another user.
  - **Significance:** May indicate lateral movement or credential theft.

---

9. Event IDs Related to System Integrity

- **Event ID 5038 (System Integrity):** *"Code integrity determined that the image hash of a file is not valid."*
  - **Description:** Indicates potential tampering with system files.
  - **Significance:** May suggest malware infection or system compromise.

- **Event ID 6281 (Audit Failure):** *"Code Integrity determined that the page hashes of an image file are not valid."*
    - **Description:** Failed code integrity checks.
    - **Significance:** Potential unauthorized modifications to code.

---

10. Event IDs Related to Policy Changes

- **Event ID 4719:** *"System audit policy was changed."*
    - **Description:** Changes were made to audit policies.
    - **Significance:** May indicate attempts to hide malicious activities.
- **Event ID 4739:** *"Domain Policy was changed."*
    - **Description:** Modifications to domain policies.
    - **Significance:** Critical in domain environments for detecting unauthorized changes.

---

11. Event IDs Related to Object Access

- **Event ID 4663:** *"An attempt was made to access an object."*
    - **Description:** Logs access to objects (files, folders, registry keys) when auditing is enabled.
    - **Significance:** Helps detect unauthorized access to sensitive data.
- **Event ID 5140:** *"A network share object was accessed."*
    - **Description:** Indicates access to shared folders over the network.
    - **Significance:** Useful for monitoring file sharing activities.

---

12. Additional Resources

Books and Guides

- **"Windows Security Monitoring"** by Andrei Miroshnikov.
- **"Windows Forensic Analysis Toolkit"** by Harlan Carvey.
- **"Incident Response & Computer Forensics"** by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia.

Online References

- **Microsoft Docs:**
  - Security Audit Events for Windows
- **Ultimate Windows Security:**
  - Security Log Encyclopedia

Tools

- **Event Log Explorer:** Advanced event log viewer and analyzer.
- **Log Parser Studio:** GUI for Microsoft's Log Parser.
- **Sysinternals Suite:** Collection of advanced system utilities.

Communities

- **SANS Digital Forensics and Incident Response:**
  - Training, articles, and community discussions.
- **Forensic Focus Forums:**
  - Discussions on forensic methodologies and tool usage.
- **Reddit r/DFIR:**
  - Community of professionals discussing digital forensics and incident response.

---

13. Summary

Understanding **Common Event IDs and Their Meanings** is essential for:

- **System Administrators:**
  - Quickly identifying and responding to system events.
- **Forensic Analysts:**
  - Interpreting logs accurately during investigations.
- **Security Professionals:**
  - Detecting and responding to security incidents.
- **Compliance Officers:**
  - Ensuring adherence to audit and compliance requirements.

By familiarizing yourself with these common Event IDs, you can effectively monitor system activities, detect anomalies, and support incident response efforts. Remember that context is

crucial; always correlate events with other logs and system behaviors for comprehensive analysis.