Event Logs

This research is supported by Award #1542465:
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)

What are event logs?

Windows keeps track of almost everything that happens in the operating system

Microsoft defines an event as "any significant occurrence in the system or in a program that requires users to be notified or an entry added to a log."

Examples of events are log ons, log offs, connections to wireless access points, improper shut downs of the computer, installations of programs, etc

Windows Event Logs

- What is actually recorded in the event log is dependent on the applications involved and the system settings
- Security event logging is disabled by default on most freshly installed windows sysstems.
- If they exists, event logs cad be incredibly useful, they would provided both local and network context that is difficult to replicate with other artifacts.

Event Log Analysis

- What Happened?: Event ID ->Event Category->Description
- Date/Time?: Time Stamp
- Users involved?: User Account->Description
- Systems Involved?:Hostname->IP Address
- Resources Accessed?: Files->Folders->Printers->Services

Event Analysis Cont.

- What Happened?
  - Even logs are designed to provide very specific information about activities that occurred on the system.
  - Items like Event IDs and Event Categories help to find relevant events
  - Event Description can provide more information of its nature
- Date/Time?
  - Timestamps are key in event logs.
  - The provide a temporal context of the events
  - Can also help narrow an investigators focus.

Event Log Analysis Cont.

- Users Involved?
  - Everything done within Windows is done using the context of an account
  - We can:
    - Identify references to specific users
    - Information about the Windows OS activities via special accounts like System and NetworkService.
- Systems Involved?
  - If the computer is in a network environment we can usually find references to systems other than the host as resources are accessed remotely
  - Originally only Netbios name was recored
  - After Windows 2000, IP address are now recorded in the event logs

Where to find Event Logs

- NT/Win2000/XP/Server 2003
  - .evt file type
  - %systemroot%\System32\config
  - Filename: SecEvent.evt, AppEvent.evt, SysEvent.evt
- Vista/Win7/Win8/Server 2008/Server2012
  - .evtx file type
  - %systemroot%\System32\winevt\logs
  - Remote log server
  - Filenames: Secutiy.evtx, Application.evtx, System.evtx, etc

Default location can be changed in the Registry

Where to find Event Logs

- Starting with Vista and Server 2008,
  - Significant changes to the event log structure
  - Log types and log locations were made
  - Historically a huge performance drain on the system, hence the new format, using the .evtx extension, was created to fix this and other problems
  - Good News: we are more likely to find Event Logs being used on the newest operating system
  - New format allows logs to be send to a remote log collector
  - Important to note that additional logs may be available on external servers

Where to find Event Logs

- Important to note the the file %systemroot%\System32\winevt\logs is only the default locations
- Administartors can designate other locations for individual logs utilizing the registry:
    - HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application
    - HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System
    - HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security

.evtx Log Format

- Memory Efficiencies
  - Less costly to log
- XML and filtering
- Improved messaging
  - IP addresses
  - EventIDs changed
- Expanded number of event logs
  - Increased the granularity of audit controls

.evtx Log Format Cont.

- Win2008 name changed from “Windows Event Log” to “Event Logging”
- Previously the entire log file had to be mapped into memory, meaning up to 300MB of memory might have to be allocated for just event logs
- Impacted performance and usually was enough justification for administrators to turn off logging
- From Vista on, log files now consist of a small header followed by self-contained 64KB chunks
- Now, only the current chunk is required to be in memory.

.evtx Log Format

- Stored in XML format, making log deconstruction much more intuitive and allows the use of industry standards, like X-Path filtering to create much more powerful searches and filters
- Logs are tokenized and stored in binary form, so raw string searches will miss much of the information in theses files
- Increased the readability of the log messaging.
  - Now include IP address in addition to hostnames
  - Added new event types
- Number of logs increased, allowing for specialized logs to be used
- New logs results in new events, giving a better view than before, into many of the runnign proccesses on the system like Task Scheduler and Plug and Play

Types of Event Logs

- Security
- System
- Application
- Custom

Security

Records events based on auditing criteria provided by local and global group policies

- Records access control and security settings information
- Events based on audit and group policies
- Example: Failed Logon; Folder access

System

Records events logged by the operating system or its components

- Contains events related to Windows services, system components, drivers, resources, etc.
- Example: Service stopped; System Rebooted

Application

Records events logged by applications

- Software events unrelated to Operating System
- Example: SQL Server fails to access a database

Custom Service

- Directory Service:Standard on Damian Controllers. Records events logged by Active Directory and its related Service
- File Replication Service: Standard on Domain Controllers. Records updates between the domain controller infrastructure
- DNS Server: Standard on servers running the DNS Service. Records DNS Administrative information such as zone management and the DNS Service starting and stopping.

Applications and Service Logs

- Primary reason for providing event logs with their own directory is that instead of just three logs, you will find over 60 logs in a standard install
- Can be daunting, but is also a good thing for a forensic analyst.
- More logs means greater likelihood that important information will be stored
- Example: addition to Plug and Play logging
- Logs are increasingly dedicated to a specific purpose
- Many of the 60+ logs are unused on a typical system

Logs

- Setup
  - New log intended to be a close companion to Application, System, and Security Log
  - Identifies what Windows security updates, patches, and hotfixes have been added to the system
- Forwarded Events
  - Ability to consolidate logs from multiple machines on a ‘’collector’’ system.
  - If reviewing on such a system, you will see logs sent from other systems present in the forwarded events lgo
- Applications and Services
  - Comprises all the new ‘’custom’’ logs introduced in Win2008. A majority of the logs are found in the Microsoft folder within the event viewer.

Security Log

- Most commonly reviewed log in forensic
    - User authentication and logon
    - User behaviour and actions
    - File / Folder/ Share access
    - Security settings modifications
    -
- Failure and Success can be audited
    - Detailed logging can be enabled on specific users accounts
- Only updated by the LSASS process
    - Third-party applications cannot insert events.

What is Recorded?

- Account Logon
  - Events stored on system who authorized logon(i.e. Domain Controller or local system for non-Domain accounts)
- Account Mgmt
  - Account Maintenance and modifications
- Directory Service
  - Attempted access of Active Directory objects
- Logon Events
  - Each instance of logon / logoff on local system

What is Recorded?

- Object Access
  - Access to objects identified in system access control list
- Policy Change
  - Change of user rights, audit policies or trust policies
- Privilege Use
  - Each case of an account exercising a user right
- Process Tracking
  - Process start, exit, handles, object access, etc
- System Events
  - System start and shutdown; actions affecting security log

Event Types

- Error
  - Significant problem; Loss of data or functionality
  - Example: Service fails to load
- Warning
  - Not significant, but could indicate a future problem
  - Example: Disk space is log
- Information
  - Successful operation of application, driver or service
  - Example: Event Log Service was started

Event Types

- Success Audit
  - Audited Security event completed successfully
  - Example: Successful user logon
- Failure Audit
  - Audited security event did not complete successfully
  - Example: Failed access to a network drive

Logon Type Codes

- 2: Logon via console
- 3: Network Logon
- 4: Batch Logon-often used by scheduled tasks
- 5: Windows service logon
- 7: Credentials used to lock or unlock screen
- 8: Network logon sending credentials in cleartext
- 9: Different credentials used than logged on users
- 10: Remote interactive logon
- 11: Cached credentials used to logon - System likely offline from DC
- 12: Cached remote interactive
- 13 Cahced unlock

How do you look at the event logs?

Event viewer- a program included with windows that lets you parse the logs

It has many different options and filters to organize and sort the event logs

Logs tend to include thousands and thousands of entries, so the ability to effectively parse is important

Check which users have logged in to this computer

On the left, click on Windows logs, then in the drop down menu, click on Security

What event ID corresponds with a regular logon? Which one corresponds with a Special Logon?

It may look like many different accounts are logged in. Do they look like regular user accounts?

How to see previously connected wi-fi access points

On the left pane, go to Applications and Services logs, Microsoft, Windows, WLAN AutoConfig, and open the log inside.

What actions do these event logs seem to describe? Name three actions and their corresponding event log ID.

This research is supported by Award #1542465:
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)