Windows Event Logs

Types of Events

Windows event logging service can record five types of events

- Error
- Warning
- Information
- Success Audit
- Failure Audit

Primary Windows Logs

Application – information on installed applications

Security – Logon events, shared object access

System – operating system, device drivers, administration, trouble shooting, starting and stopping services

Setup – information on O.S. setup and installation

Forwarded Events – information received from other systems using log subscriptions. (Remote logging uses Windows Event Collector service, WinRM over port 5986, can also be set up using GPO’s)

Applications and Services – tends to store events for longer periods. Good for historical analysis.

Retention

Logs are overwritten when full.

Keep logs as long as possible

Certain regulations may require the retention of logs for a specific period on time.

Filter Current Log

Select type of event

Search based time, event level etc

create custom views

save the contents of custom views to file

`

Event Properties

Standard fields

- Log name – name of the event log where the log is stored.
- Source – service, component or application that created the event.
- Event id – specific code for specific type of event (learn these)
- Level –severity assigned to the event
- User – the user account involved or the user context of the Source (check event specific info)
- Opcode – assigned by the source. (investigate the source)
- Logged – Date & Time
- Task Category – assigned by the source. (investigate the source)
- Keywords – assigned by the source
- Computer – device that logged the event (remember remote access)
- Description **Event Specific info**

SEE eventlogedit from Shadow Brokers, https://www.securityweek.com/event-logs-manipulated-nsa-hacking-tool-recoverable

Log Records storage

Log records are stored in binary XML format with a .evtx extension (.evt in older versions) in System32\winevt\logs

To see XML representation click the details tab in the event specific information (useful for interaction through powershell)

Can be stored remotely using Log Subscriptions. Use a node running Windows Event Collector Service which subscribes to logs produced by other Systems.

HTTPS port 5986 using WinRM

Audit Policy

Audit policies dictate the creation of event records

Access Through:

gpedit -> computer configuration -> windows settings -> security settings -> advanced audit policy configuration (then expand tab in left menu) -> System Audit Policies

Microsoft Audit policy recommendations:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Powershell cmdlets

- Get-eventlog
- Get-winevent

In Class Exercise

Research, Search and examine samples for the following Events

Account Management events: can be found within the range of Id's 4720 ~4799. Examples: 4720 User account created, 4735, 4756,4799

Logon events: Examples: 4624. 4625, 4776. ***NOTE: There should be little or no locally logged logon events from User accounts***. These should be in the log of the DC. Aggregate local ***System*** logon events in centralized location. Result (Status) codes contain specific information.

Shared Objects (i.e. fileshares): Examples 5140,5142-45

Object Access – Scheduled tasks: Examples 4698-4701

File/Folder Access: Examples: 4656, 4657,4658

Access to External Storage Media: Example 4663

Audit Policy Changes: Example:4719

Security Event Log Cleared 1102

Question: Why not log everything?

Answer: The impact on resources.

So - Test in Your environment.