Report 9

This week I worked on Windows Event Log Analysis. The contents included 1. Event Log Format, 2. Account Management Events, 3. Account Logon and Logon Events, 4. Access to Shared Objects, 5. Scheduled Task Logging, 6. Object Access Auditing, 7. Audit Policy Changes, 8. Auditing Windows Services, 9. Wireless LAN Auditing, 10. Process Tracking, 11. Additional Program Execution Logging. And 12. Auditing PowerShell Use. The first task to go over is the Event log format.

In Windows, the logs are stored in the **%SystemRoot%\System32\winevt\logs** directory by default. You can also save these logs remotely by subscribing to services made by other systems. They typically use WinRm and transporting them requires HTTPS on port 5986. These events can be recorded in Security, Forwarded, System, or Application event logs, or in modern Windows systems, in Event Viewer. Additionally, they may appear in a variety of other log files. The Setup event stores the logs data that occurred at the installation of Windows. Applications and Services Logs in Event Viewer record information on specific types of actions. The Forwarded Logs stores event from other systems. It is important to analyze different logs and determine which logs are vital to search for what you are looking for. These can include the Log Name, The Source content service that is running, and finding the Event ID to actually attribute an activity with a unique identifier. There is also other information that you may look for such as looking for the User involved in the Activity when an event occurred or the Description of the log which highlights additional information specific to the event. Often it is valuable for the analyst.

The second task to go over is the Account Management Events. This basically holds information related to account activities. These can include where an account was created or modified. Whether the account resides in a local account or a domain account.  Events are indicated by an ID and A description of the event.

The third task goes over Account Logon and Logon Events. Both of these events are logged in the Security event log. Account Login (Authentication) under domain accounts is executed by a domain controller inside a Windows Network. Accounts that reside locally are authenticated by the local system. As for Account Login, their events are logged in the system that is performing authentication. If you want to audit Account Logon and Logon events, you can set that in Group Policy. It should a priority for administrators to review their audit policies on a regular basis to ensure that all systems are operating as intended. That way systems such as your domain controller will be able to provide centralized accounting, which is where accounts are authenticated. Remember to pay attention in the working station are users performing unauthorized authentication on local user accounts as this is an indication that the system may be compromised.

The fourth task is Access to Shared Objects. Attackers will want to access credentials by remotely accessing the data by creating users or administrators. These events will be recorded in the Account Logon and Logon events as mentioned above. Attackers can also create additional logging by navigating **Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Object Access -> Audit File**

**Share**. These events are saved in the Security Log. They will contain an event ID. A description of the events such as, a network share having been accessed, a network share object being shared/modified, and A network share object was checked to see whether the client can be granted desired. All this information will be visible in the Security Log.

The fifth task involves Scheduled Task Logging. If you enable the history in the Task Scheduler, you will be able to keep a log record of activity related to the scheduled tasks that are occurring on the local system. Some of these task descriptions include Scheduled Task Created, Scheduled Task Updated, Scheduled Task Deleted, Scheduled Task Executed, and Scheduled Task Completed. To enable the history, you can use **wevtutil set-log Microsoft-Windows-TaskScheduler/Operational /enabled:true** command on Command Line as an Administrator. To check the status, use **wevtutil get-log Microsoft-Windows-TaskScheduler/Operational** command.

The sixth task is on Object Access Auditing. This is not typically enabled by default. To do this you can do this by navigating the **Local Security Policy to set Security Settings -> Local Policies -> Audit Policy -> Audit object**. Enabling object access auditing some activities need to be properly configured. That is because object access is constantly occurring, and logs need to be received extra auditing so that the system does overwhelm itself by recording every instance of object access events. You can access the events for Object Access in the Security Log. Some of the descriptions of the events are A scheduled task was created which can highlight the date, author, triggers, etc. A scheduled task was deleted, enabled, or disabled. Or when a scheduled task was updated. If you want to audit access to individual files or folders, need to configure manually by setting the auditing rules in the file or folder's Properties dialog box by selecting the Security tab, clicking Advanced, selecting the Auditing tab, and setting the appropriate audit you are looking for and then select the user account(s). Some events that are created when modifying objects are, A handle to an object was requested or A registry value was modified.

The seventh task is about Audit Policy Changes. Modifications that are made in the Audit Policy are important when identifying what was changed. The Event ID that is created when Audit Policies are changed is 4719. A description of the Event will highlight that a System audit policy was changed. You can access information in detail by using third-party tools. Event ID 1102 is when a Security event log is cleared. You are also able to see the account that cleared the log file.

The eighth task involves Auditing Windows Services. There are attacks that are dependent on Windows services that either execute commands remotely or maintain persistence on the system. So, to identify them, Windows records these events that are starting and stopping services in the System Event Log. Some of these events include Event ID 6005 – which indicated that an event log service was started. Event ID 7036 shows that service was stopped or started. Event ID 7045 signifies a service was installed by the system. These events are worth noting because they may indicate that your Auditing Windows Services may be compromised.

The ninth task is about Wireless LAN Auditing. You can track wireless local area network (WLAN) activity in the Windows event log. Since rogue access points are common vectors of man-in-the-middle attacks and malware attacks, you should investigate foreign connections on devices that have Wi-Fi capability, especially those that can leave your environment, as well. This log file is stored in the **SystemRoot%\System32\winevt\Logs\Microsoft-Windows-WLANAutoConfig%4Operational.evtx.** These Event IDs associated with Wireless LAN Auditing are Event ID 8001 which indicates that a WLAN service has successfully connected to a wireless network. Event ID 8002 reveals that WLAN service failed to connect to a wireless network

The tenth task covers Process Tracking. Unlike Linux, Windows does not save the history of commands that were run by users. That has allowed attackers to use the "Living on the Land:" technique to rely on using Windows commands. It was a blind spot that attackers can use. This feature is not enabled by default, so to enable them requires accessing two separate Group Policy Settings. The first one, you navigate **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy -> Audit process tracking.** The second one you navigate to **Computer Configuration -> Administrative Templates -> System -> Audit Process Creation -> Include command line in process creation events.** With both of these enabled, you can effectively Track processes and log commands in the command line. Note that some command line arguments can contain confidential data such as passwords so make sure that you can access those logs securely and notify users of changes in the audit policy. The Event ID associated with Process Tracking is Event ID 4688. You can access it in the Security Log which provides an abundance of information on processes that were executed in the system. There are also Windows Filtering Platform (WFP) event IDs that can show as well. These include information that is related to local and remote IPs. The port numbers. Also, the Process ID and Names related to events. Some of the events involved with WFP are Event ID 5031 which signifies that The Windows Firewall Service blocked an application. Event ID 5156 indicates that The WFP has allowed a connection. The information about these events holds significant worth. This comes at the cost of storing a large amount of data. It t best to balance your security auditing to ensure that your environment is effective in managing information.

The eleventh task involved the Additional Program Execution Logging. AppLocker is a feature that helps in disadvantageous to attackers. To enable this, you need to access Event Viewer under Application and Services Logs\Microsoft\Windows\AppLocker. These event logs are stored in the **C:\Windows\System32\winevt\Log.** The name of these logs can include AppLocker%4EXE and DLL.evtx. There are two modes that AppLocker can set. They are audit-only mode or blocking mode. The Windows Defender also creates logs for scanned or blocked files. You can find this event log in the **C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx** and the **Microsoft-Windows-Windows Defender%4WHC.evtx.** These can contain information about malware or malicious scripts that were run. Here are some of the potential Event IDs and Descriptions of events. Examples such as Event ID 1006 inform you that the antimalware engine found malware or other potentially unwanted software. Event ID 5001 shows that Real-time protection is disabled. Event ID 5015 reveals that Scanning for viruses is disabled. Windows exploit protection is also another feature that provides a robust defense for your system. The key fact to note is that not all features are enabled by default since it can interfere with software that is recognized. To access the logs, they are located in **C:\Windows\System32\winevt\Logs\Microsoft-Windows Security-Mitigations%4KernelMode.evtx** and in the **Microsoft-Windows-Security Mitigations**

**%4UserMode.evtx.** There is also another option to increase the visibility of processes that are in your system. This is called **Sysmon**, a utility included in Sysinternals. Using this, a new system service is installed and a device driver to create event logs. They hold information on processes, network connections, and record the time when modifications to files were done. They are located in the Event Viewer under A**pplications and Services Logs\ Microsoft\Windows\ Sysmon\Operational.** The logs are located in the **C:\Windows\System32 \winevt\ Logs\ Microsoft-Windows-Sysmon%4Operational.evtx.** An example of information that is viewed is Event ID 255 describes a Sysmon error. Event ID 5 indicated that a process is terminated.

The last task covers Auditing PowerShell Use. Another great way to protect your system from attackers. Since this is not enabled by default, you need to enable this in Group Policy by navigating to **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell.** Three categories are included. There are Module, Script Block, and Transcript logging. Module logs pipeline execution events. Script Block collects de-obfuscated commands sent to PowerShell and Only records commands that were entered. Transcription logs the PowerShell input and output. Note that it will not log the output of programs outside that are running in PowerShell. Enabling this is crucial to providing the information if your system was compromised. The logs are located in the **%SystemRoot% \ System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx.** There are also two events that is created in the Event Viewer. Event ID 4103 which explains the pipeline execution from the module logging facility. Event ID 4104 describes script block logging entries. Event Id 400 shows that s the start of command execution or session. Keep in mind to check for accounts that are doing administrator activities related to log in.