Windows Event Logs

"Windows Event logs" or "Event Logs" are files in binary format (with .evtx extension) stored locally in the Windows directory of a computer with that operating system:

- **Windows 2000 to WinXP/Windows Server 2003:**
  `%WinDir%\system32\Config*.evt`
- **Windows Server 2008 to 2019, and Windows Vista to Win10:**
  `%WinDir%\system32\WinEVT\Logs*.evtx`

These logs keep a detailed record of the vast majority of events that have occurred on the system (hardware events, user logins, program execution and installation, etc.), allowing system administrators to keep track of everything that happens within a system during its execution and being able to diagnose and foresee potential issues.
Categories of registered events include:

- **Application:** Events logged by an application (Execution, Deployment error, etc.)
- **System:** Events logged by the Operating System (Device loading, startup errors, etc.)
- **Security:** Events that are relevant to the security of the system (Logins and logouts, file deletion, granting of administration permissions, etc.)
- **Directory Service:** This is a record available only to Domain Controllers, it stores Active Directory (AD) events.
- **DNS Server:** It is a record available only to DNS servers; logs of DNS service are stored.
- **File Replication Service:** Is a record available only for Domain Controllers, it stores Domain Controller Replication events.

If you are interested in learning more about these types of records, how they work and how to visualize them, visit the following links:
https://www.manageengine.eu/network-monitoring/Eventlog_Tutorial_Part_I.html
https://www.loggly.com/ultimate-guide/windows-logging-basics/#

SECURITY EVENT LOGS

Security Event Logs are events stored by the system that contain information related to the "Windows Security audit policies" (elements of systematic monitoring that helps with the evaluation of system security), which are used to allow precise control over any possible incident present in the system.
Some of these elements are:

- Account logon events (valid and invalid sign-ons and sign-offs)
- Account management (creation, modification, interaction and deletion of user accounts)
- Privilege use.
- Account management (creation, modification, interaction and deletion of user accounts)
- Resource usage (file creation, modification, interaction and deletion)

If you want to learn more about the Windows Security Audit, it's settings, and how to apply it, visit the following link: https://eventlogxp.com/essentials/securityauditing.html.

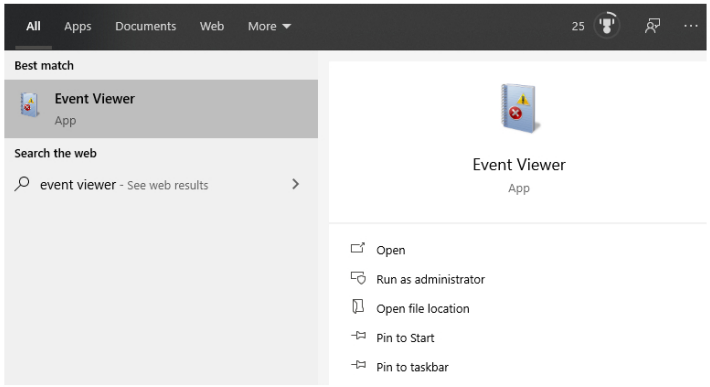
Event ID	Description
4624	An account was ***SUCCESSFULLY logged on***
4625	An account ***FAILED to log on***
4647	User initiated ***logoff***
4648	A ***logon*** was attempted ***USING EXPLICIT CREDENTIALS***
4649	A ***replay attack*** was ***DETECTED***
4659	A ***handle to an object*** was requested with ***INTENT TO DELETE***
4706	A ***new trust*** was ***CREATED*** to a domain
4720	A ***user account*** was ***CREATED***

4726	A ***user account*** was ***DELETED***
4732	A ***member was ADDED*** to a security-enabled local group

If you want to learn more about security events and get a more detailed list of these items, we recommend you visit the following links:
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx
https://www.andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/

EVENT VIEWER

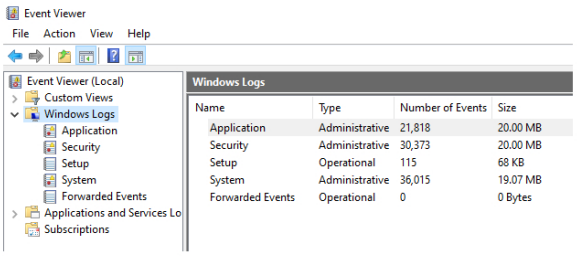
On Windows 10 we can view Windows Events using the Event Viewer. Search for it in the Windows search bar and run it.



We can use this program to view all different types of logs, and we highly recommend that students check it out to view the logs on their own systems. For this purposes of this walkthrough, we're going to focus primarily on security-related events. When opening Event Viewer you should see a display similar to the below screenshot.

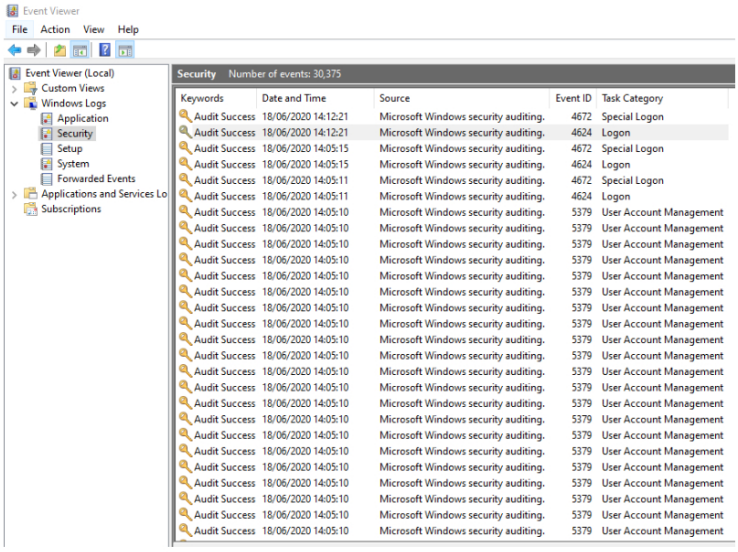
The Summary of Adminsitrative Events in the middle of the screen displays a high-level overview of all event types in the past 7 days. We can see that we have had 0 critical events in the past 7 days, 260 errors, and 223 warnings. On the right-hand side pane, we're going to expand the Windows Logs section. We can see this is split into 5 different sections;

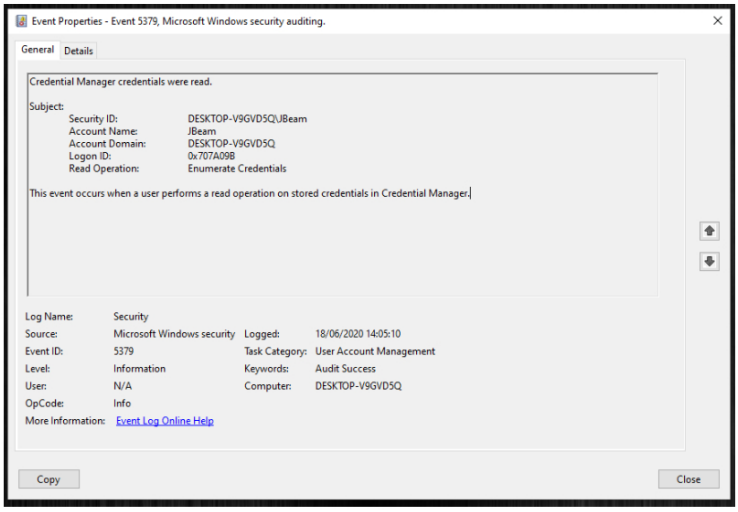
- Application
- Security
- Setup
- System
- Forwarded Events



If we click on Security, the middle pane will now show us Security Events. In the below screenshot we can see a lot of

events with the Event ID 5379 and the task category User Account Management. If we double click on one of these ID 5379 events, we can get some more information, which we'll cover below.



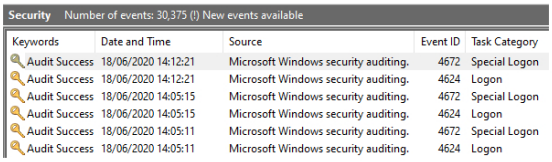


Event 5379 is related to users logging in to a Windows system. Let's explain the information in this event log:

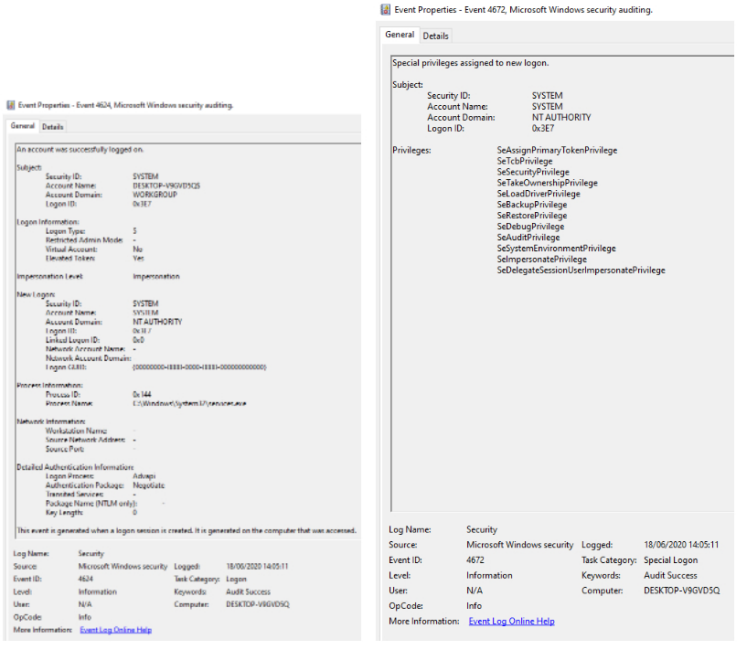
- **Credential Manager credentials were read –** When a user submits credentials when logging into Windows, the system will read the stored credentials in the Credential Manager to ensure that the user-provided credentials exist, and if they're valid, allowing the users to successfully login.
- **Security ID –** The Security Identification value of the account attempt to sign in.
- **Account Name –** The name of the account.
- **Account Domain –** The domain the account is trying to log in to. As this is just a personal PC on a home network, the default domain is WORKGROUP.
- **Logon ID –** This is a semi-unique (unique between reboots) number that identifies the logon session.
- **Read Operation –** Enumerate credentials is the action taken by the system, as covered under the first bullet-point.

In the bottom section of the window we can also see the time that the event was logged (18/06/2020 14:05:10), the computer that the event was generated on (DESTKOP-V9GVD5Q), and that the audit was successful, based on the Keyword value.

In the first screenshot above showing a list of Security Events, at the top we can see there are some Logon events and Special Logon events, let's take a deeper look at them.



In the above screenshot, we can see events with the IDs 4672 Special Logon and 4624 Logon. This pane displays the events with the newest at the top, so the actual sequence is: Logon > Special Logon. But what does this actually mean? The logon event is whenever a user logs into the system, and the Special Logon is when an administrator logs in. We can see these are paired up, because when a user account with administrator privileges logs into Windows it requires the Logon event, then the Special Logon event. Below are screenshots of both of these event types expanded within Event Viewer.

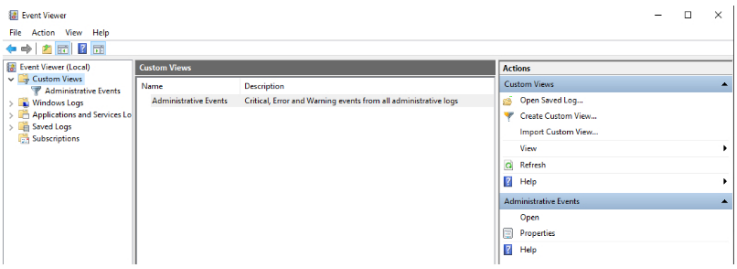


Why do you think it's a good idea for security teams to monitor user logons and special logons? (Really think about it for a minute before you carry on reading!).

- Most employees will work from 9 AM to 5 PM in office-based organizations. We could monitor for logon activity at unusual times, such as generating an alert for an account that logs in at 3 AM, when the user is only supposed to work from 9-5. This could be a sign of account compromise or insider threat.
- Accounts with administrative privileges have the ability to perform many more tasks than standard users. We need to closely monitor these accounts, because if they are compromised, the attackers are going to have a great time. Monitoring this can also alert the security team to insider threats that want to abuse their admin accounts to cause damage or perform other malicious actions.

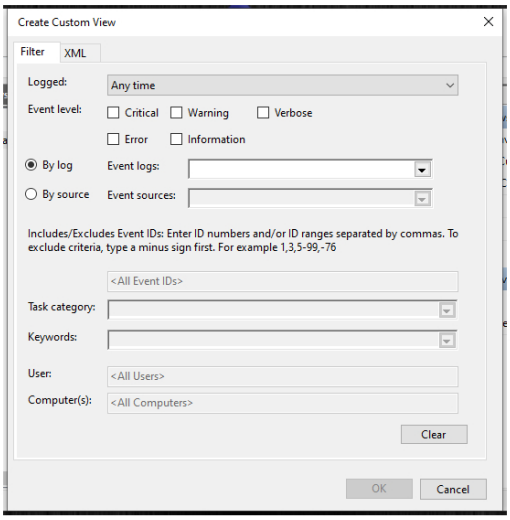
CUSTOM VIEWS

Event Viewer allows us to create custom search profiles, called "Custom Views". We can easily use these to retrieve the event IDs we want from a system, removing all of the extra noise that we're not interested in. Below we will walk you through creating a Custom View to look only for logon and logoff activity. Firstly, open Event Viewer and click on Custom Views on the left-hand side.

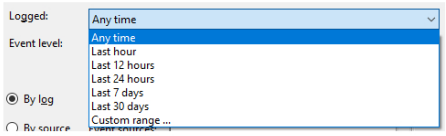


We can see in the above screenshot that by default there is already one Custom View, named "Administrative Events". On the right-hand side we can click "Create Custom View" to make our own filter. The below window will

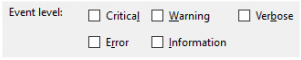
popup, allowing us to create the View. Below we will cover all of the properties we can set.



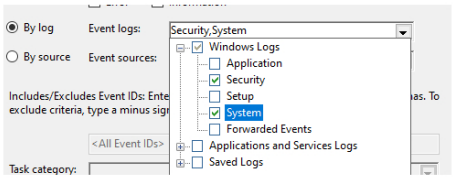
- **Logged:** Allows us to set a date range to retrieve logs from. We can set a custom range, or use the presets including "Any Time", "Last Hour", "Last 12 Hours", "Last 24 Hours", and "Last 7 Days". This can be useful if a system is not connected to a SIEM, allowing us to retrieve specific event logs after a malware infection or security incident.



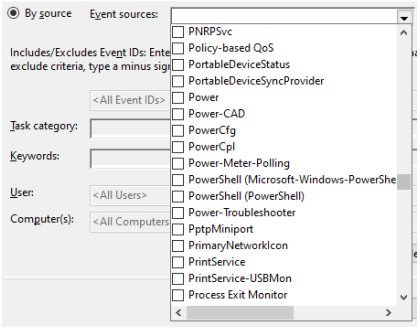
- **Event Level:** Allows us to select which event levels we want to filter on, which will provide us with different events based on the selected levels.



- **By Log:** We can choose what logs we want to filter on. The below screenshot shows a hierarchy structure, where we can select logs at any level. In the below screenshot example, we're only looking for Security and Systems event logs from Windows.

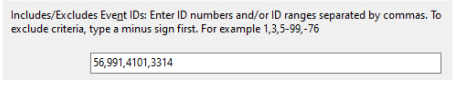


- By Source: If we don't want to select log groups, we can instead choose sources. These are specific areas of the operating system and applications. See the below screenshot for some examples of the source we can choose from.



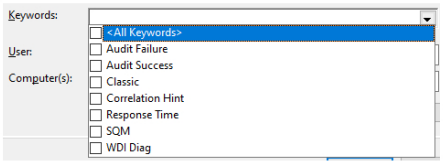
- **Includes/Excludes Event IDs:** This section allows us to define exactly what event IDs we want to capture. We can enter in any Event IDs we want to retrieve by listing them, using a comma as a separator, for example:

```
56,991,4101,3314
```

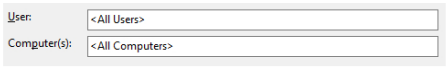


- **Keywords:** We can look for specific keywords within Events. See the below screenshot for the options we can

choose.



- User and Computers: This section lets us focus on specific users or systems, if other Windows systems are pushing their event logs to the system we're viewing Event Viewer on. If there was a user named "KellyP" and we only wanted to investigate events related to them, we would use their user account name in the User field.

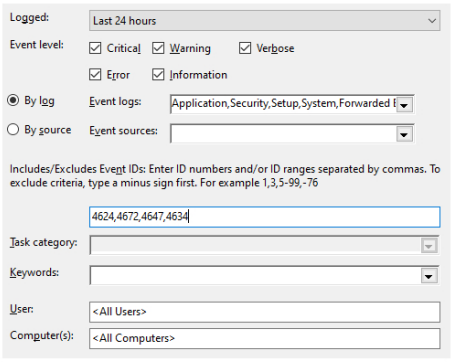


Custom Views Example: Login Monitoring

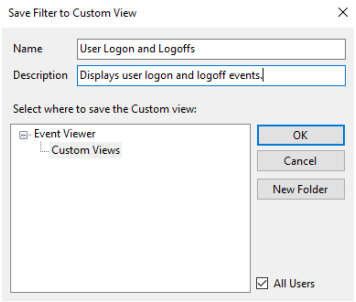
Just so that you fully understand how Custom Views can be used, let's go through an example where we want to monitor employee login and logoff times. The following are events we need to consider for our View:

- **User Logon Successful** – 4624
- **Special Logon** – 4672
- **User Initiated Logoff** – 4647
- **User Logoff** – 4634

In the below screenshot you can see the settings we have set. We want to view all events associated with users logging in and out, over the past 24 hours.

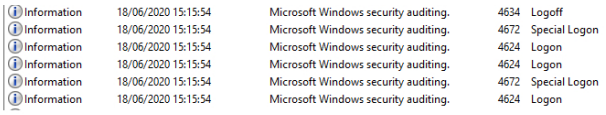


Next we'll be prompted to provide a name, description, and where we want to save the View.



Now the filter will show us only the event IDs we have defined. It's worked! We can now see events related to user accounts logging in and out!

Level	Date and Time	Source	Event ID	Task Category
Information	18/06/2020 15:30:59	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:24:57	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:24:57	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:16:34	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:16:34	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:16:15	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:16:15	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:16:14	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:16:14	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:16:01	Microsoft Windows security auditing.	4634	Logoff
Information	18/06/2020 15:16:01	Microsoft Windows security auditing.	4634	Logoff
Information	18/06/2020 15:16:01	Microsoft Windows security auditing.	4634	Logoff
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4634	Logoff



Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4634	Logoff
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4624	Logon
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4672	Special Logon
Information	18/06/2020 15:15:54	Microsoft Windows security auditing.	4624	Logon

Try looking at the Event Viewer on your host system (or a virtual machine if you're running another host operating system) and see what you can find! In the next lesson, you will have the chance to analyze some Windows event logs to see if you can make sense of a chain of events, and retrieve important information from them.

Quizzes

Lab) Event Log Analysis

Previous Topic

Back to Lesson

Next Topic