Hands-On Lab: Log Management & Security

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Log Management & Security

Table of Contents

[Introduction 2](#_Toc76729352)

[Objective 2](#_Toc76729353)

[Estimated Completion Time 2](#_Toc76729354)

[Materials Required 2](#_Toc76729355)

[Minimum System Configuration 2](#_Toc76729356)

[Log Security Issues with Event Viewer 3](#_Toc76729357)

[Opening Command Window (CMD) and Determine Local IP Address 3](#_Toc76729358)

[Using Event Viewer 4](#_Toc76729359)

[Assigning Tasks to Logs and Events 7](#_Toc76729360)

[Cleaning and Managing Event Viewer Logs 12](#_Toc76729361)

[Researching Events 15](#_Toc76729362)

[Self-Reflection and Response 17](#_Toc76729363)

[Instructor’s Response 17](#_Toc76729364)

[Resources 18](#_Toc76729365)

# Introduction

Computer systems do many things and accomplish many complex tasks very quickly. Sometimes things go wrong inside the system and sometime things happen that the system does not expect. When these things happen, the computer will record the event to a computer log – a record of events and activities that occur on a system. Some logs are routine, noting when users log in and access certain resources. Others are security-related, with unexpected activities and potential intrusions.

In this lab, students will examine the default logs present in a standard Windows operating system. Since the modern Microsoft Windows user OS, like Windows 10 is based on the same underlying architecture as Microsoft’s server systems, this knowledge can be scaled to understand the actions of commercial servers as well as end-user systems.

# Objective

Upon completion of this activity, the student will be able to:

* Access and review the various logs present in a Windows 10 computer.

# Estimated Completion Time

If you are prepared, you should be able to complete:

* The log management lab in 30 minutes to 1 hour.

# Materials Required

Completion of this lab requires a standard Windows 10 installation.

# Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

* Intel i5 or better CPU
* 8 GB RAM (minimum) - 16 GB RAM (recommended)
* 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
* Microsoft Windows 10 or latest version

# Log Security Issues with Event Viewer

To review the logs in a Windows OS-based computer, you will use the Event Viewer utility. While some specialized servers have their own log system, Event Viewer is used for most Windows platforms.

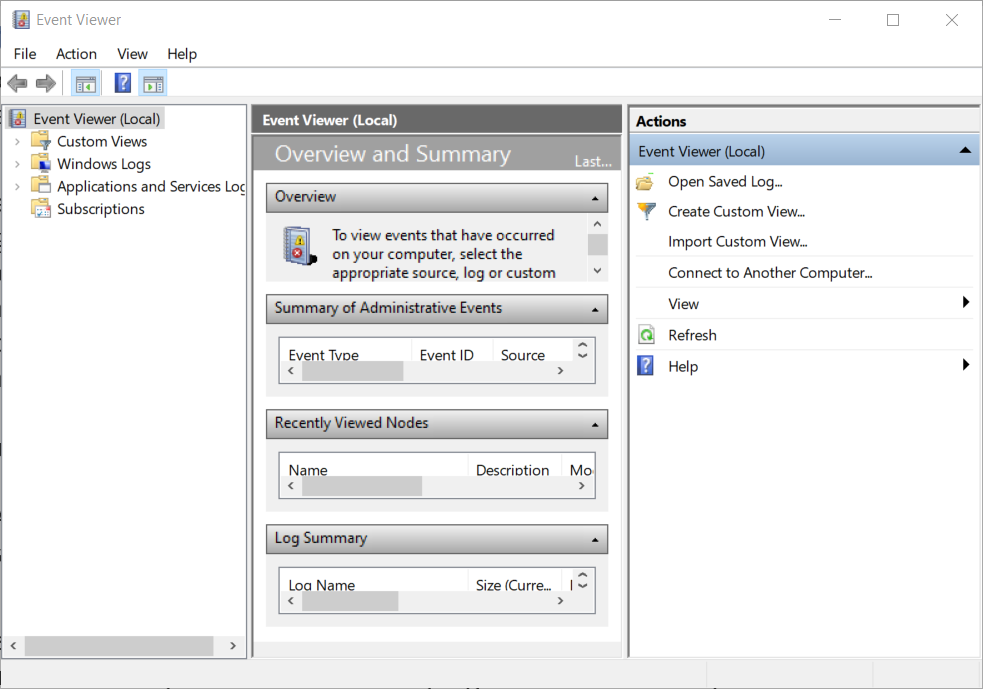
“Event Viewer displays these types of events:

* Error: A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.
* Warning: An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.
* Information: An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
* Success Audit: An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.
* Failure Audit: An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

The Event Log service starts automatically when you start Windows. Application and System logs can be viewed by all users, but Security logs are accessible only to administrators.”[[1]](#endnote-2)

## Opening Command Window (CMD) and Determine Local IP Address

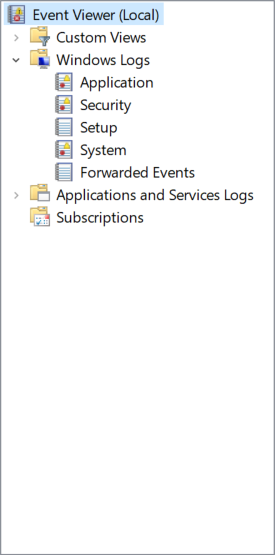
1. Open the Event Viewer using one of the following methods:
   1. Right click on the Windows **Start** button and select **Control Panel**. Next select **System & Security**, then double-click **Administrative tools**. Finally, double-click **Event Viewer**.
   2. Type *Event Viewer* in the Windows Task bar search field, and click on the app.
   3. Hold the **Windows** key, and press **R** to open the run field and type *eventvwr* (or **eventvwr.msc**) and select **OK**.
2. Once Event Viewer has started, you should see the default view shown in Figure L07-1.



**Figure L07-1** Windows Event Viewer

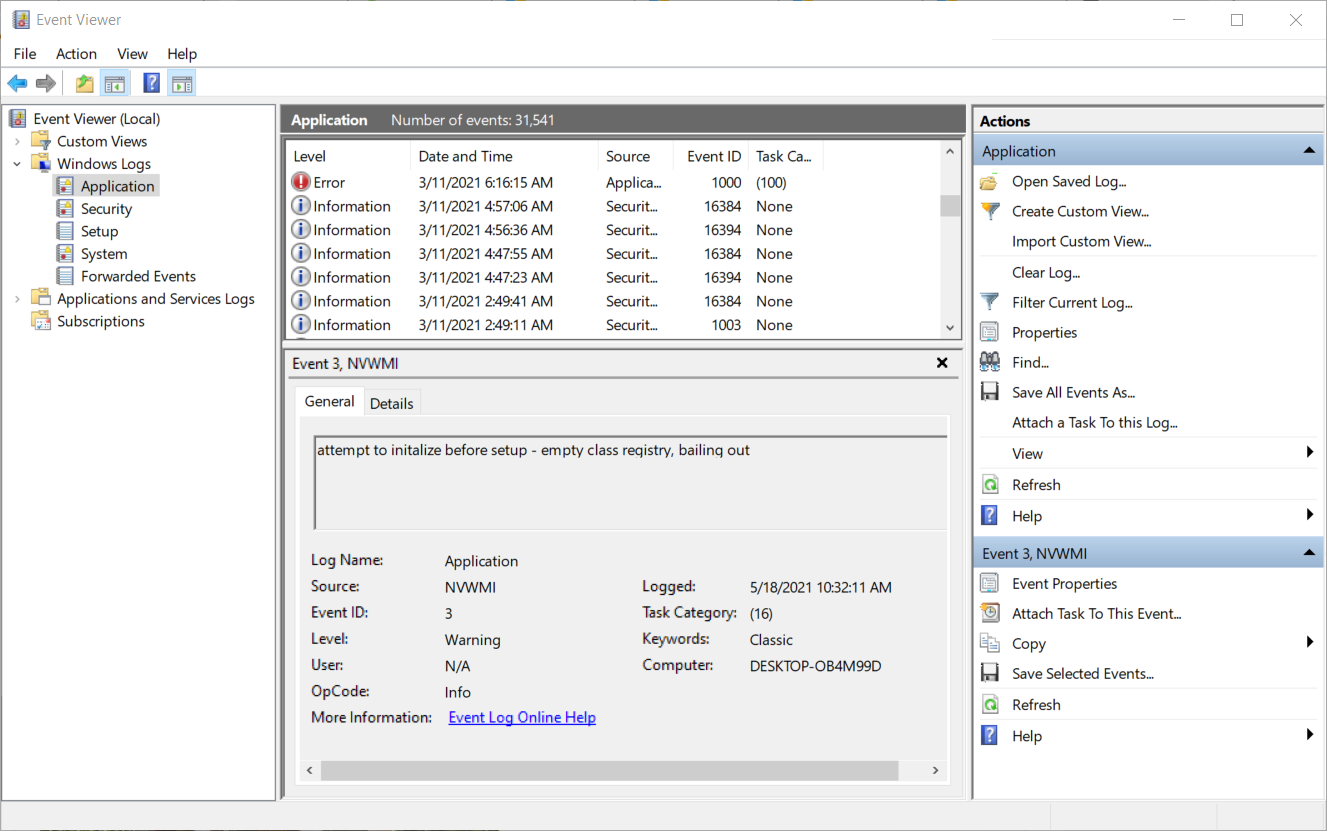
## Using Event Viewer

1. Once Event Viewer is running, select the **Windows Log** entry in the left pane. Here you will see the five default operating systems logs associated with most windows systems, shown in Figure L07-2. Specialized services like SQL servers and Domain controllers have additional logs.



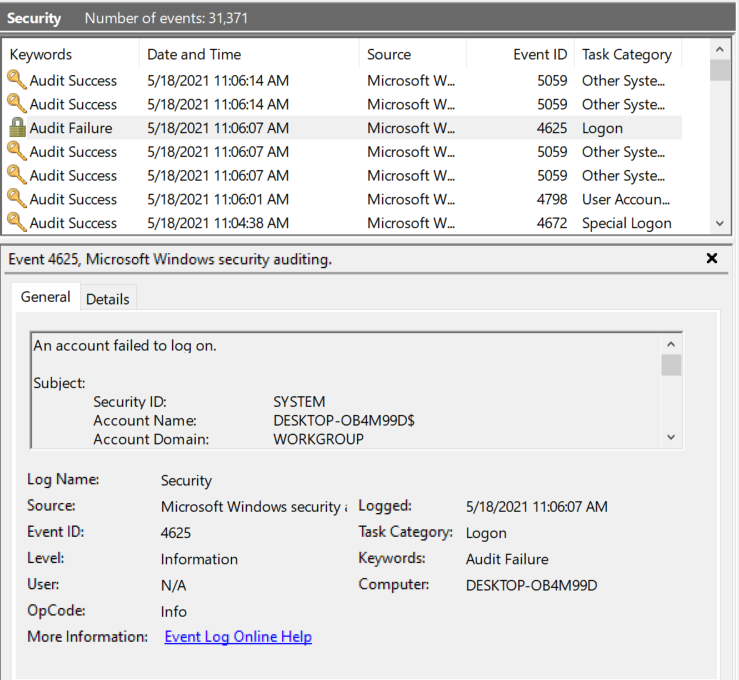
**Figure L07-2** Event Viewer Windows Logs

1. Select **Application** in the left pane. The center of Event Viewer will display the various entries the system has recorded. The Level of each entry was discussed in the Introduction to this lab. Scroll down your list and look for one entry of each type: *Information, Warning,* and *Error*. As shown in Figure L07-3, once you select an entry, the details are displayed in the bottom center box.



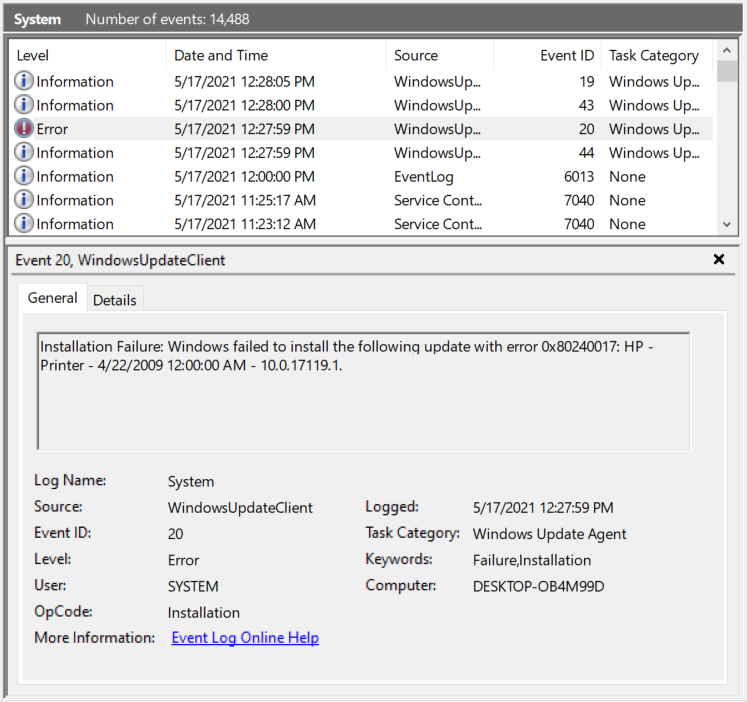
**Figure L07-3** Event Viewer Application Log

1. Select **Security** in the left pane. Again, the center of Event Viewer will display the various entries the system has recorded. You will most likely see many “Audit Success” entries, representing when a user or application accesses the system successfully. Scroll down your list and look for any Audit Failure entries, like the one shown in Figure L07-4. If you find multiple Audit failures, you may have detected someone trying to guess the password for the system, or it may just be a user that is not paying attention to their typing. Consistent failures should always be investigated.



**Figure L07-4** Event Viewer Security Log Audit Failure

1. Select **Setup** in the left pane. Again, the center of Event Viewer will display the various entries the system has recorded. If you’ve updated Windows and there were issues, they’ll be logged here.
2. Select **System** in the left pane. Here issues with the operating system are recorded. For example, the system in Figure L07-5 has an issue updating the drivers associated with an HP printer. Issues here are usually referred to the helpdesk unless you are the helpdesk. Scroll through this list and look for any *Errors*.

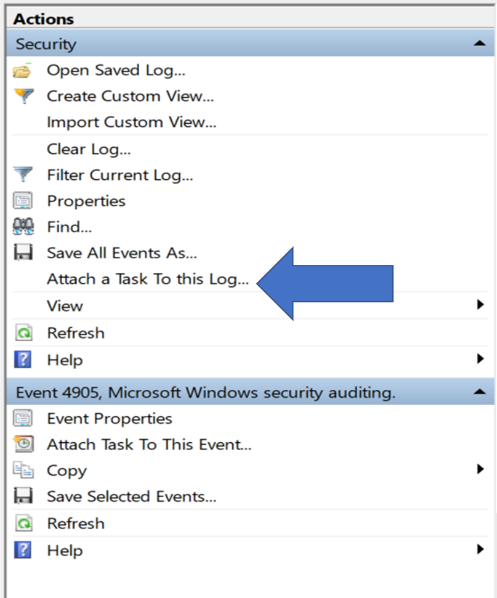


**Figure L07-5** Event Viewer System Log

1. The Forwarded Events log documents log entries that were forwarded to an outside resource, like a dedicated log server. Log servers can collect information from multiple systems and look for patterns that could indicate a systematic problem, or an attacker looking at multiple systems for a vulnerability that would allow them access.
2. In the left pane, click on **Applications and Services Logs**. While Windows Logs show operating system-focused events, here you see specialized logs for installed applications, and utilities like Internet Explorer, Microsoft Office applications and Windows PowerShell. Take a few minutes and scroll through the entries in these logs.

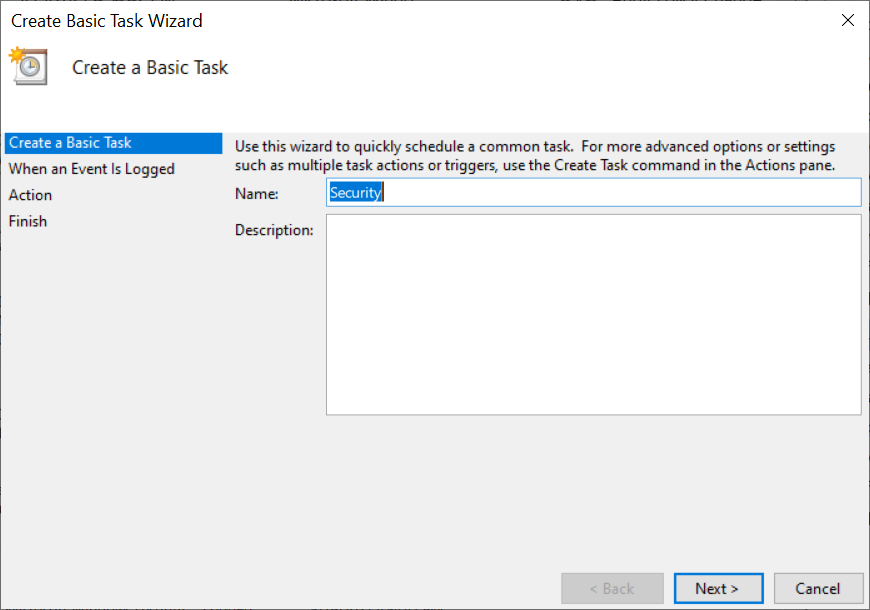
### Assigning Tasks to Logs and Events

1. An interesting feature of the Event Viewer is its ability to perform a special task if there is an entry to a particular log, or a recurrent of a particular message. Back in the Event Viewer, look in the bottom right corner. Here are several tools an administrator can use to improve their ability to manage the logs. Click on the Windows **Security** Log. Then In the upper right menu, select **Attach a Task to this Log…**, indicated by the arrow in Figure L07-6.



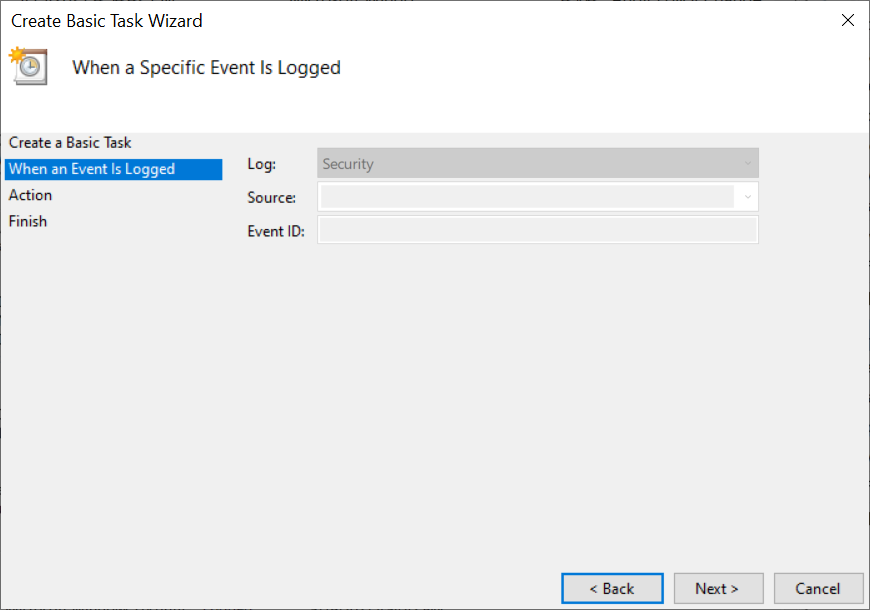
**Figure L07-6** Event Viewer Actions Menu

1. As shown in Figure L07-7, this brings up the Create Basic Task Wizard, where you can name this Task. You would normally start by naming this task. We won’t be saving this task, so the information you put in isn’t important. Click the **Next >** button.



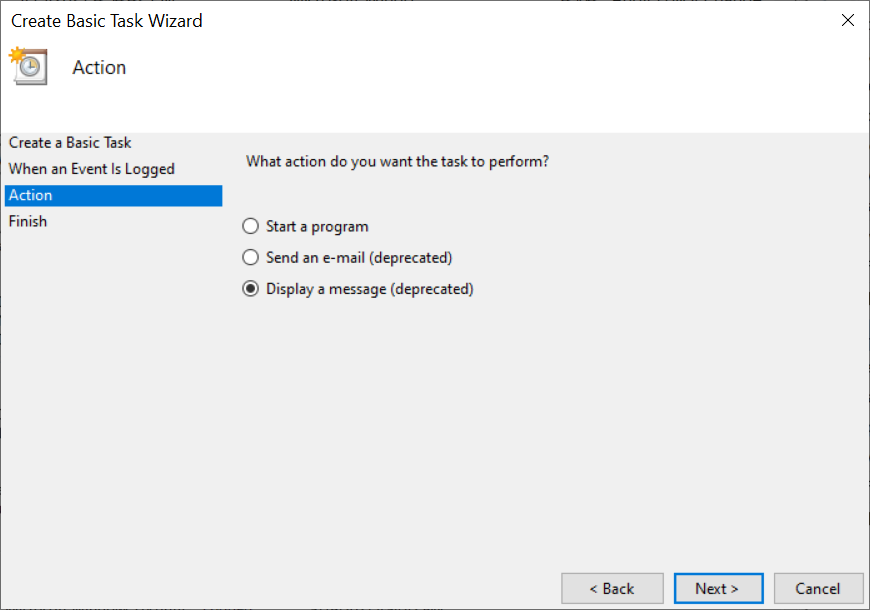
**Figure L07-7** Event Viewer Create Basic Task Wizard For Log, step 1

1. In the next window, you would accept the default settings, as this particular task does not allow additional information. If your system does, it may have a different configuration than the example computer.



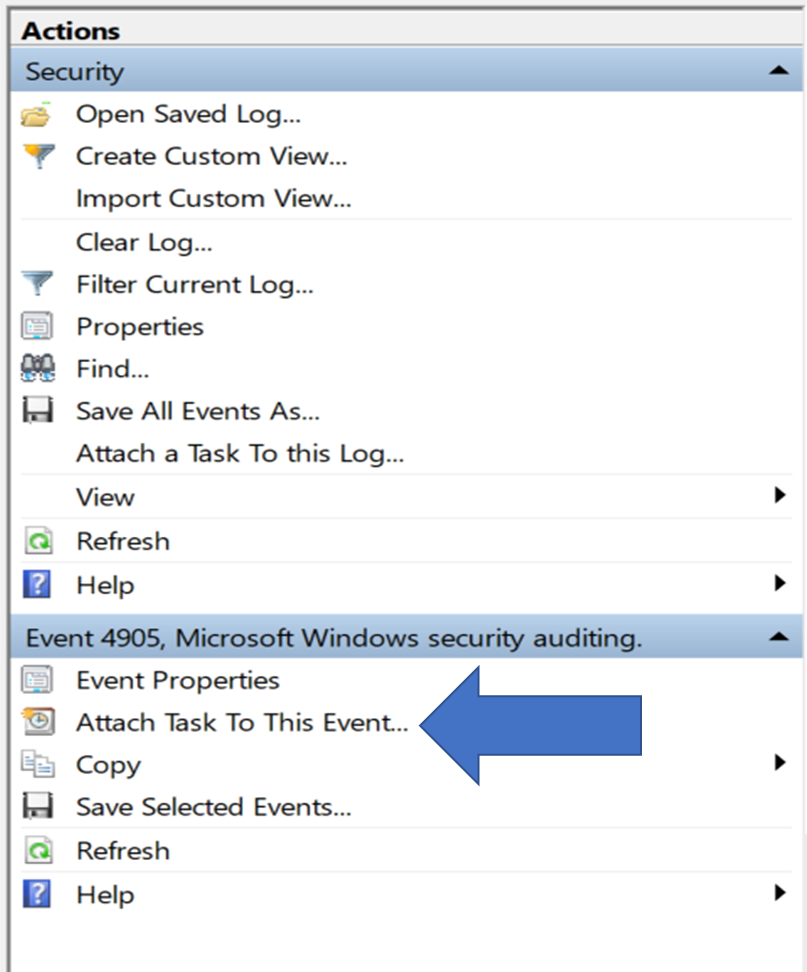
**Figure L07-8** Event Viewer Create Basic Task Wizard For Log, step two

1. Click the Next > button to go to the next step, where you will specify the action to be taken when this log has a new entry (See Figure L07-9). The system can Start a specific program, send you an e-mail, or display a pop-up message on the screen.



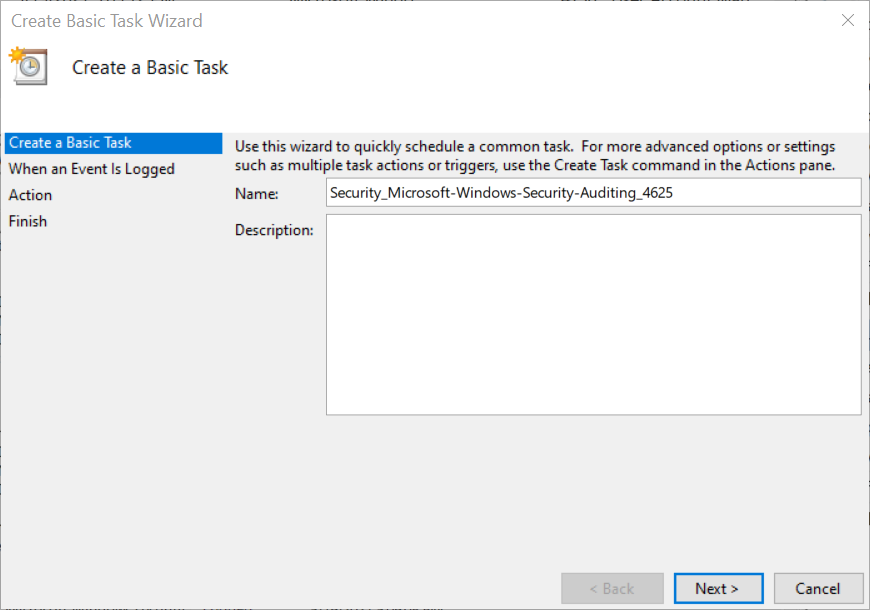
**Figure L07-9** Event Viewer Create Basic Task Wizard for Log, step three

1. Unless this is your personal computer and you want to activate this task, click **Cancel**.
2. You can also assign a task to a specific event. Back in the *Security* log, scroll down to an *Audit Failure* event. If you were the administrator for this computer and wanted to be notified if another Audit Failure associated with this, you would click **Attach Task To This Event** option indicated by the arrow in Figure L07-10 below.



**Figure L07-10** Event Viewer Attach Task to This Event

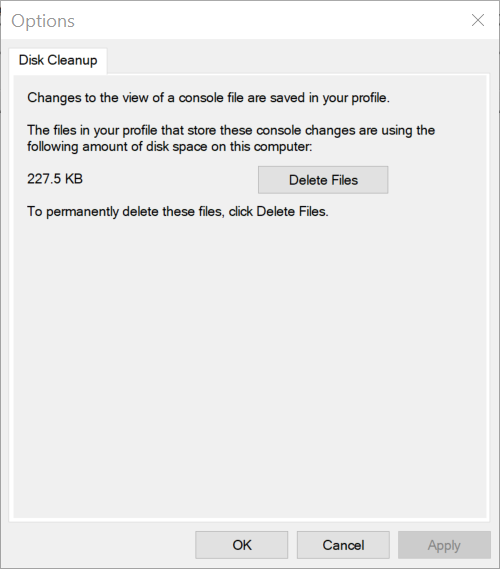
1. The process from here forward, as shown in Figure L07-11 is the same as the previous “Attach a Task”. You would name it, assign an action, then save it. Click Cancel when you’ve reviewed these steps.



**Figure L07-11** Event Viewer Create Basic Task Wizard for Entry

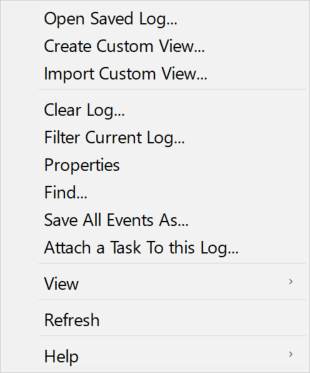
### Cleaning and Managing Event Viewer Logs

1. If you find your system has tens of thousands of entries like the example system, you may want to periodically delete the archived log files. While they’re typically small – this system’s Event Viewer logs were only 227.5 KB, it’s not a bad idea to keep the file small if you want to review it later. To clean up ALL Log files, select **File** then **Options** from the Event Viewer menu at the top of the window.
2. As shown In Figure L07-12, here you can simply click the **Delete** **Files** button to empty out the log.



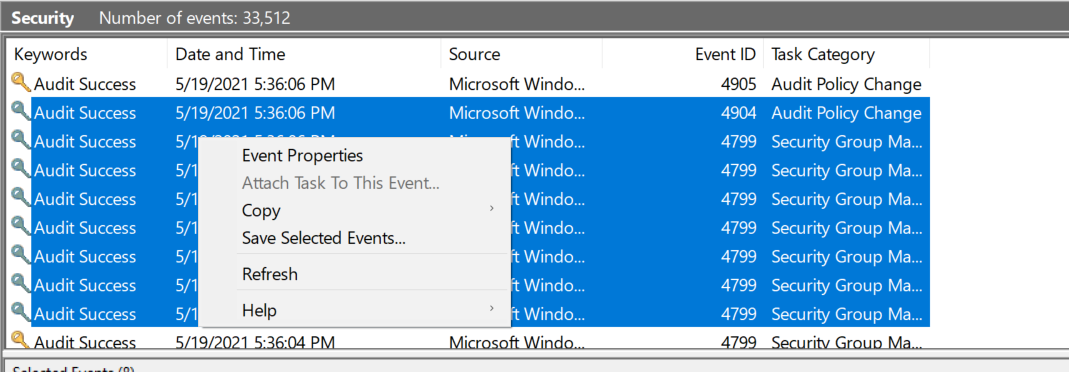
**Figure L07-12** Event Viewer Disk Cleanup

1. To clean up a specific log, right click the name of the log in the left view and select **Clear Log**, as shown in Figure L07-13.



**Figure L07-13** Selected Log Menu Options

1. If you’d rather save the entries in your logs, there are two ways to do this. If you want to save an entire log, you would use the menu from Figure L07-13 above, and select Save All Events As… which will open a Save File window and prompt you for a name. The default option saves the logs in a proprietary format (Event Files .evtx), although you can change this to XML (.xml), Text (.txt) or CSV (Comma Separated)(.csv) to allow review in a more user-friendly format.
2. If you just want to save a subset of a log’s entries, you can select those files by clicking on the first entry, holding the **shift** (to select sequential entries) or **Control** (to select individual entries) key, right clicking, and selecting **Save Selected Events…** from the menu, as shown in Figure L07-14.

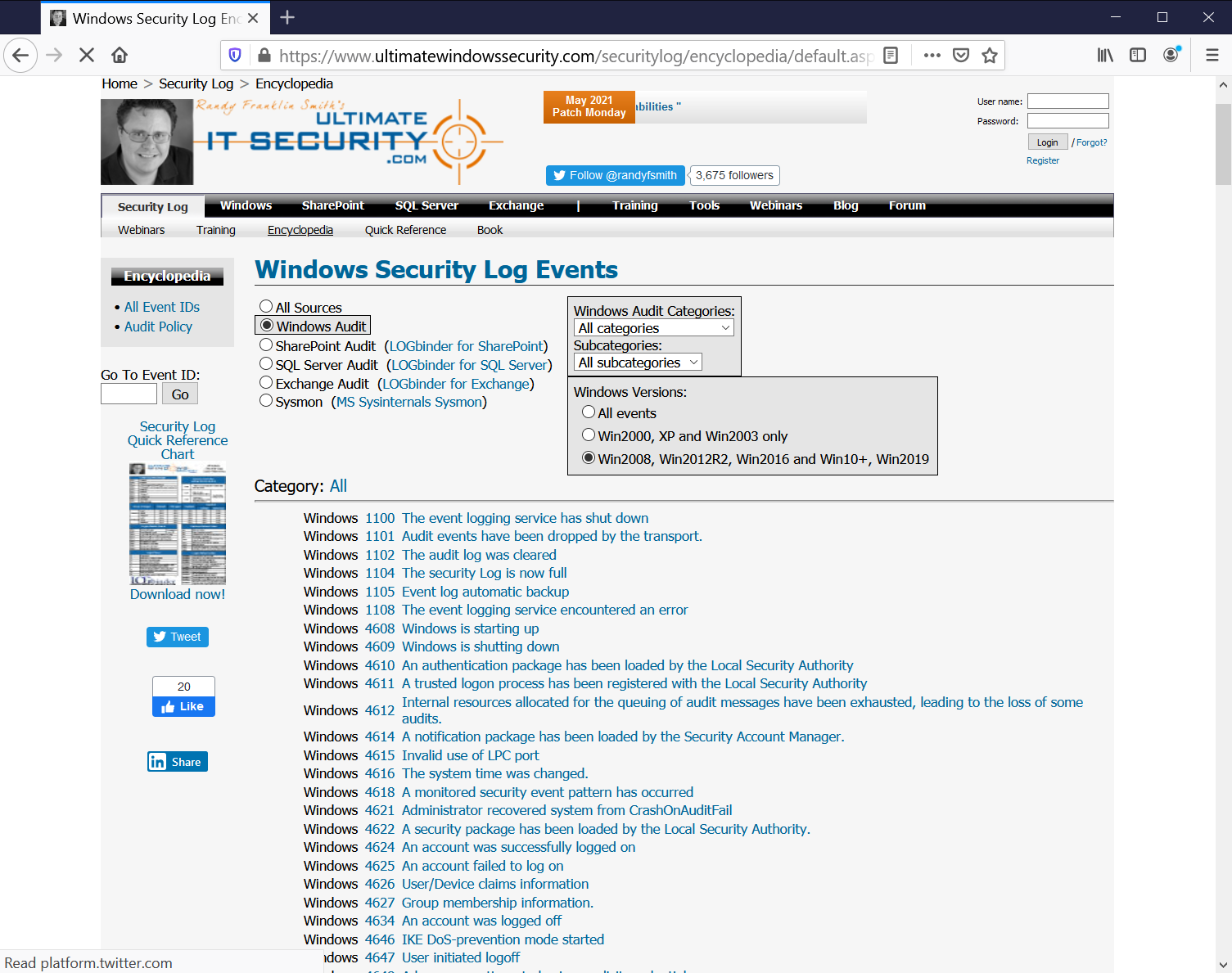


**Figure L07-14** Selected Events Menu Options

# Researching Events

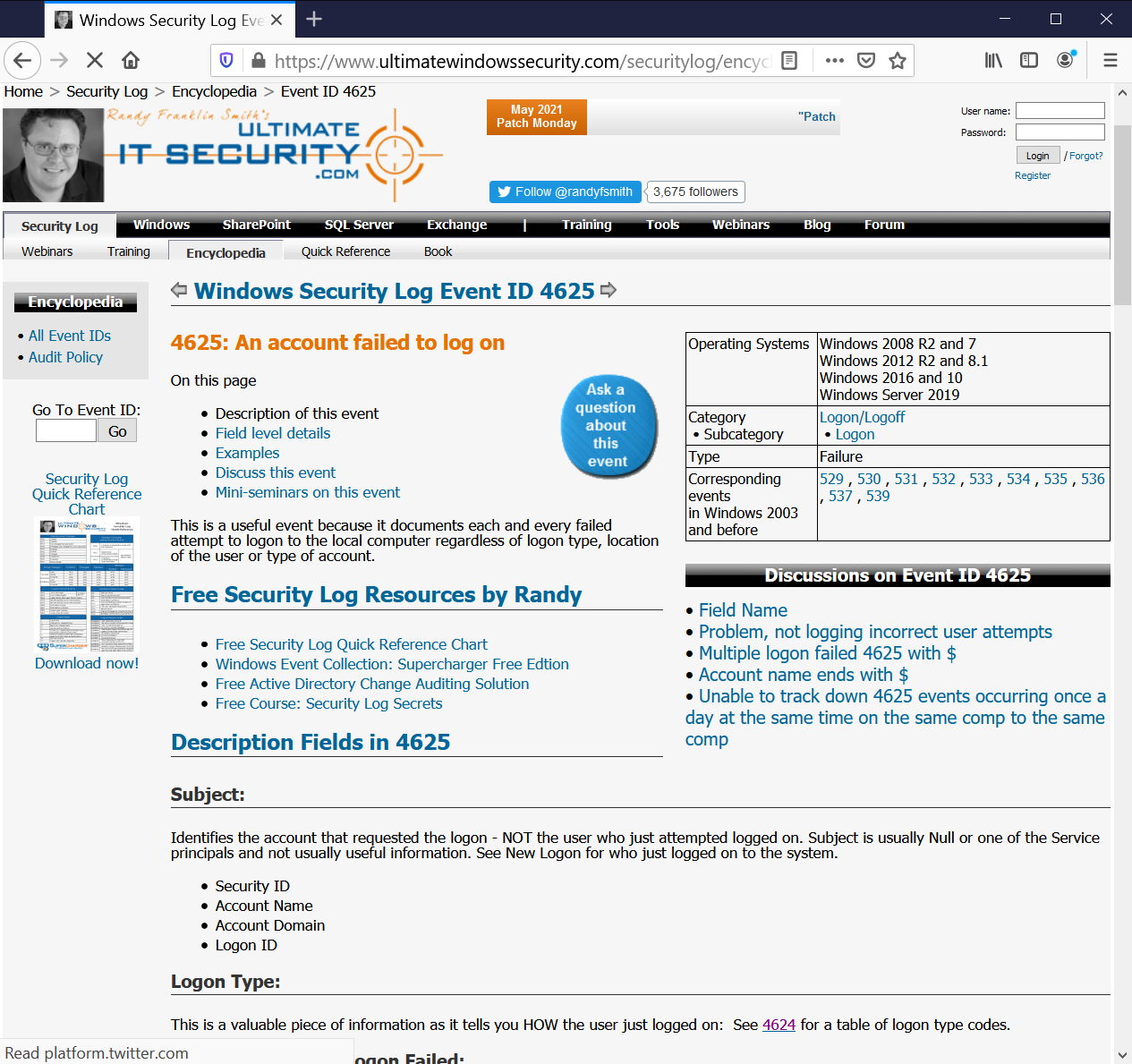
The last task you would perform should you find an anomaly in a log is to research it. This essentially involves web searches, looking at reputable sites for more information on a particular error.

1. Scroll back through the Windows logs and identify a number of Audit Failures, Warnings, and Errors. Then open a web browser and type the name of the error, and any Event ID that is associated with it.
2. At first you may have difficulty finding a reputable resource to help you. There are some support sites like <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>, that have searchable encyclopediad of Windows Event Viewer ID codes, as shown in Figure L07-12 below. Go to this site now.



**Figure L07-15** Ultimate Windows Security from Ultimate IT Security

1. Here you can scroll down the list and find the Windows Security Log Event ID from our example system (4625) and learn more about it. While this entry was rather obvious, and performed just for this lab, there are probably entries in your system that aren’t so obvious. Scroll down and select one of the Event IDs.
2. As shown in Figure L07-13, you can now find out more about the error, and even browser related links. Feel free to review several other log entries, and familiarize yourself with the process of researching these events. One day you’ll have a system issue and need to perform these steps to determine if the entry is malicious or a system or user error.



**Figure L07-16** Ultimate Windows Security Entry for Event ID 4625.

# Self-Reflection and Response

What are some of the reasons you would need to look at the Windows System Log?

|  |
| --- |
| It is good to review the logs every now and again to see if there are any issues with the system or applications that you need to be aware of. If you suspect there is any unauthorized activity, then Logs would be a source to gather information from. If you see errors or warnings in the logs then you can check suspicious entries online to see if there is any malicious activity. |

Briefly describe how you might manage the growth in the size of system log files. Why would you need to keep copies of log files?

|  |
| --- |
| You can choose to delete old log files that are no longer needed to help free up any space, but many choose to save the log files to refer to in the future. Logs are often saved in .csv or .xml formats to be able to more easily parse data from. |

How long do you think system logs should be retained?

|  |
| --- |
| I would base that information on what the policy is in place at the business that I work for / with. If I were to set a policy I would try to keep monthly logs and back them up into compressed yearly logs, and keep a backup of those for multiple years until space became an issue. From the log files I see on my personal system the logs are not large in size, so if space is available, I would keep log backups indefinitely. |

## Instructor’s Response

|  |
| --- |
|  |

# Resources

1. How to use Event Viewer in Windows, https://kb.blackbaud.com/knowledgebase/articles/Article/75433 [↑](#endnote-ref-2)