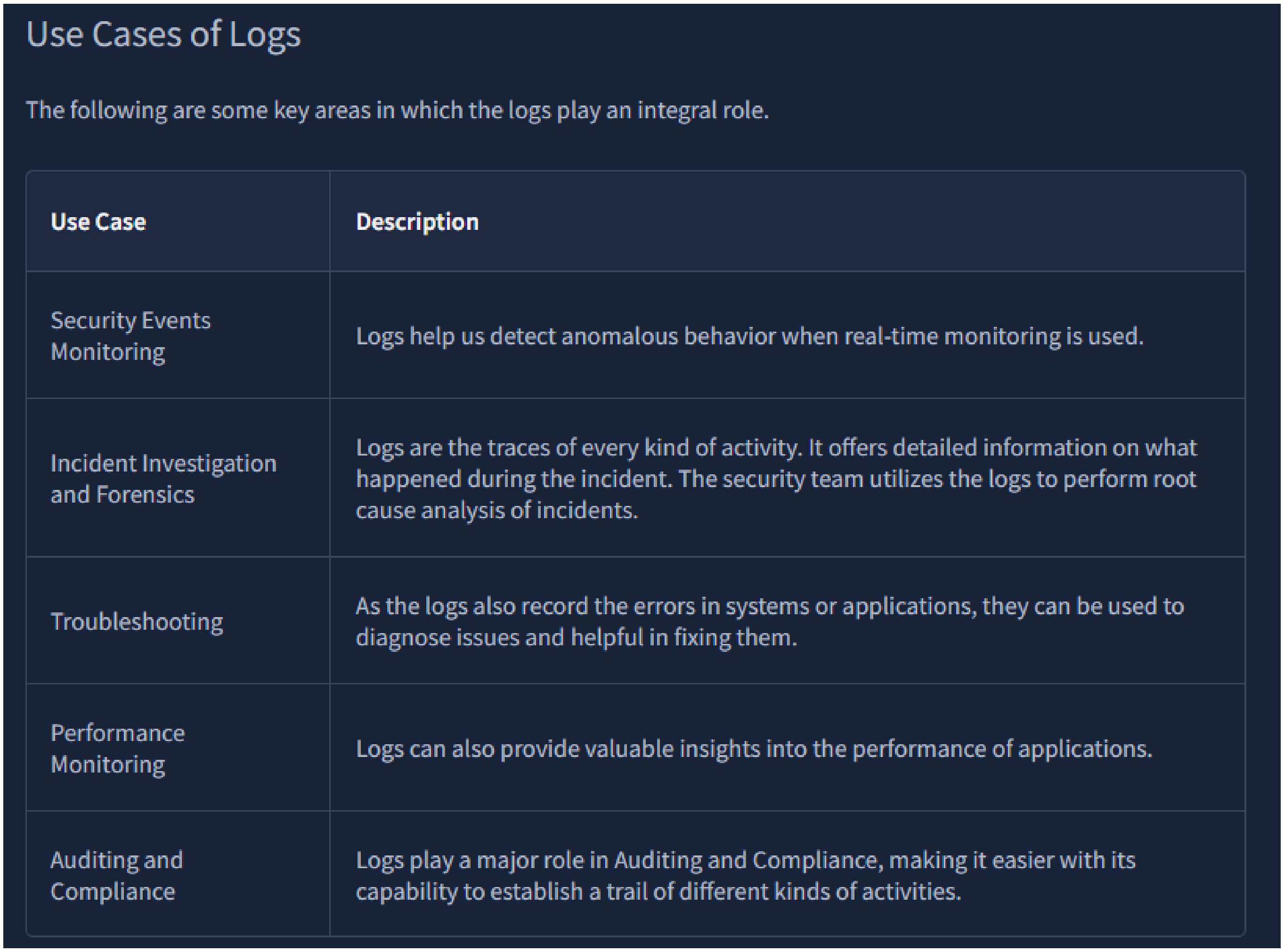
Logs Fundamentals

Logs are the digital footprints left behind by any activity. The activity could be a normal one or the one with malicious intent



Use Cases of Logs

The following are some key areas in which the logs play an integral role.

Use Case	Description
Security Events Monitoring	Logs help us detect anomalous behavior when real-time monitoring is used.
Incident Investigation and Forensics	Logs are the traces of every kind of activity. It offers detailed information on what happened during the incident. The security team utilizes the logs to perform root cause analysis of incidents.
Troubleshooting	As the logs also record the errors in systems or applications, they can be used to diagnose issues and helpful in fixing them.
Performance Monitoring	Logs can also provide valuable insights into the performance of applications.
Auditing and Compliance	Logs play a major role in Auditing and Compliance, making it easier with its capability to establish a trail of different kinds of activities.

Types of Logs

Log Type	Usage	Example
System Logs	The system logs can be helpful in troubleshooting running issues in the OS. These logs provide information on various operating system activities.	- System Startup and shutdown events - Driver Loading events - System Error events - Hardware events
Security Logs	The security logs help detect and investigate incidents. These logs provide information on the security-related activities in the system.	-Authentication events - Authorization events - Security Policy changes events - User Account changes

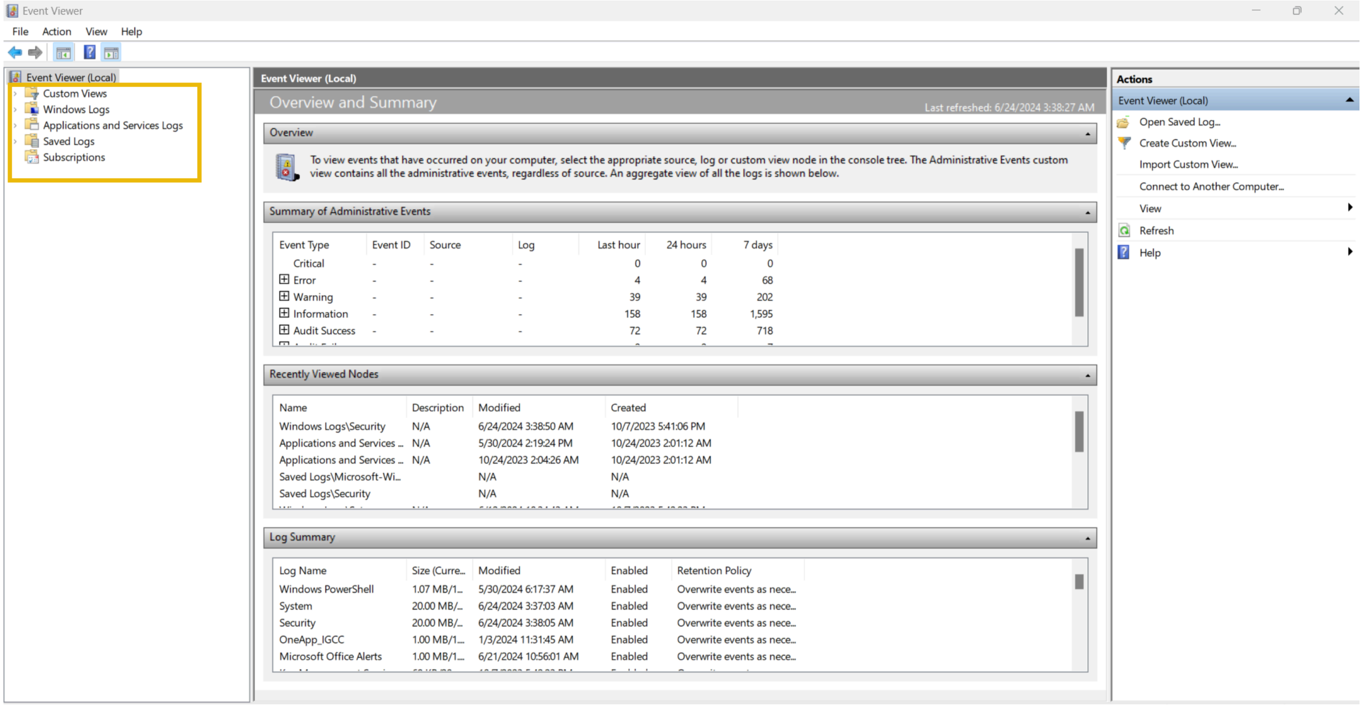
Log Type	Usage	Example
		events - Abnormal Activity events
Application Logs	The application logs contain specific events related to the application. Any interactive or non-interactive activity happening inside the application will be logged here.	- User Interaction events - Application Changes events - Application Update events - Application Error events
Audit Logs	The Audit logs provide detailed information on the system changes and user events. These logs are helpful for compliance requirements and can play a vital role in security monitoring as well.	- Data Access events - System Change events - User Activity events - Policy Enforcement events
Network Logs	Network logs provide information on the network's outgoing and incoming traffic. They play crucial roles in troubleshooting network issues and can also be handy during incident investigations.	- Incoming Network Traffic events - Outgoing Network Traffic events - Network Connection Logs - Network Firewall Logs
Access Logs	The Access logs provide detailed information about the access to different resources. These resources can be of different types, providing us with information on their access.	- Webserver Access Logs - Database Access Logs - Application Access Logs - API Access Logs

Windows Event Logs Analysis

Some of the crucial types of logs stored in a Windows Operating System are:

- **Application:** There are many applications running on the operating system. Any information related to those applications is logged into this file. This information includes errors, warnings, compatibility issues, etc.
- **System:** The operating system itself has different running operations. Any information related to these operations is logged in the System log file. This information includes driver issues, hardware issues, system startup and shutdown information, services information, etc.
- **Security:** This is the most important log file in Windows OS in terms of security. It logs all security-related activities, including user authentication, changes in user accounts, security policy changes, etc.

Windows OS has a utility known as Event Viewer, which gives a nice graphical user interface to view and search for anything in these logs.



Event Viewer (Local)

Overview and Summary

Last refreshed: 6/24/2024 3:38:27 AM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Summary of Administrative Events

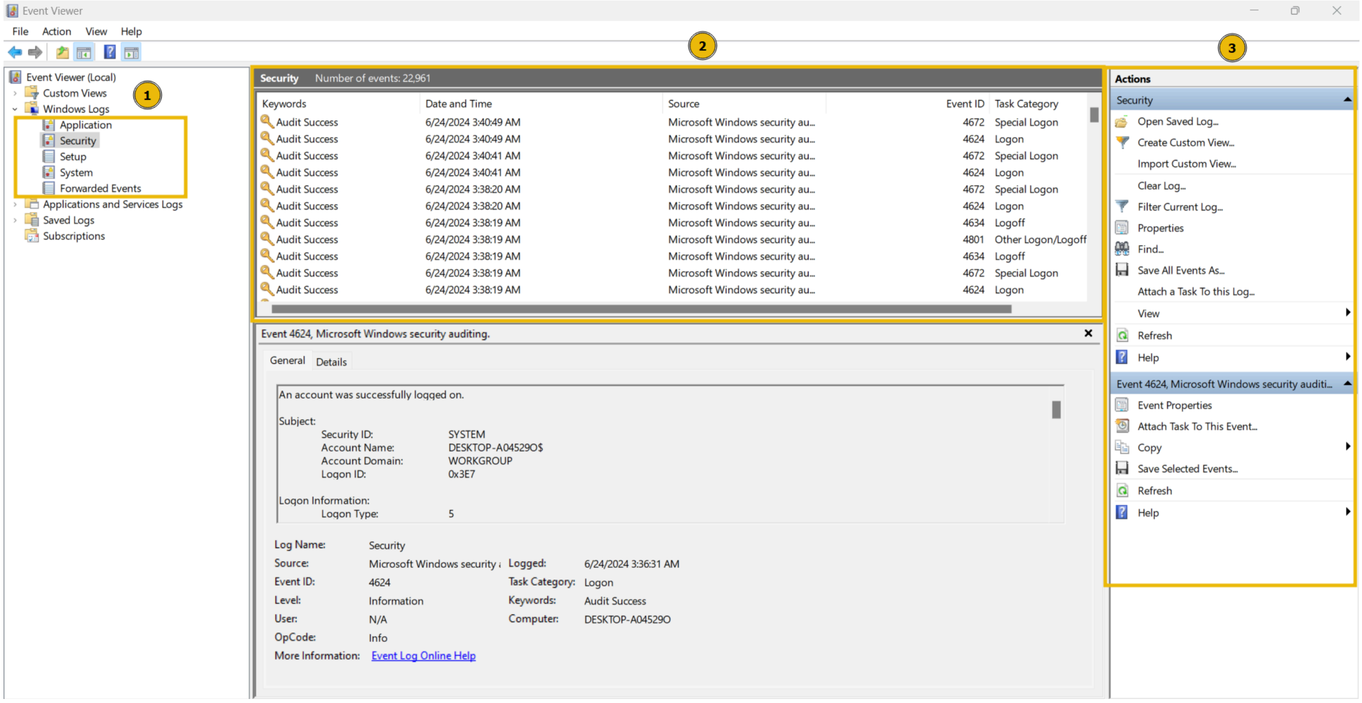
Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	4	4	68
⊞ Warning	-	-	-	39	39	202
⊞ Information	-	-	-	158	158	1,595
⊞ Audit Success	-	-	-	72	72	718

Recently Viewed Nodes

Name	Description	Modified	Created
Windows Logs\Security	N/A	6/24/2024 3:38:50 AM	10/7/2023 5:41:06 PM
Applications and Services ...	N/A	5/30/2024 2:19:24 PM	10/24/2023 2:01:12 AM
Applications and Services ...	N/A	10/24/2023 2:04:26 AM	10/24/2023 2:01:12 AM
Saved Logs\Microsoft-Wi...		N/A	N/A
Saved Logs\Security		N/A	N/A

Log Summary

Log Name	Size (Curre...	Modified	Enabled	Retention Policy
Windows PowerShell	1.07 MB/1...	5/30/2024 6:17:37 AM	Enabled	Overwrite events as nece...
System	20.00 MB/...	6/24/2024 3:37:03 AM	Enabled	Overwrite events as nece...
Security	20.00 MB/...	6/24/2024 3:38:05 AM	Enabled	Overwrite events as nece...
OneApp_IGCC	1.00 MB/1...	1/3/2024 11:31:45 AM	Enabled	Overwrite events as nece...
Microsoft Office Alerts	1.00 MB/1...	6/21/2024 10:56:01 AM	Enabled	Overwrite events as nece...



Security Number of events: 22,961

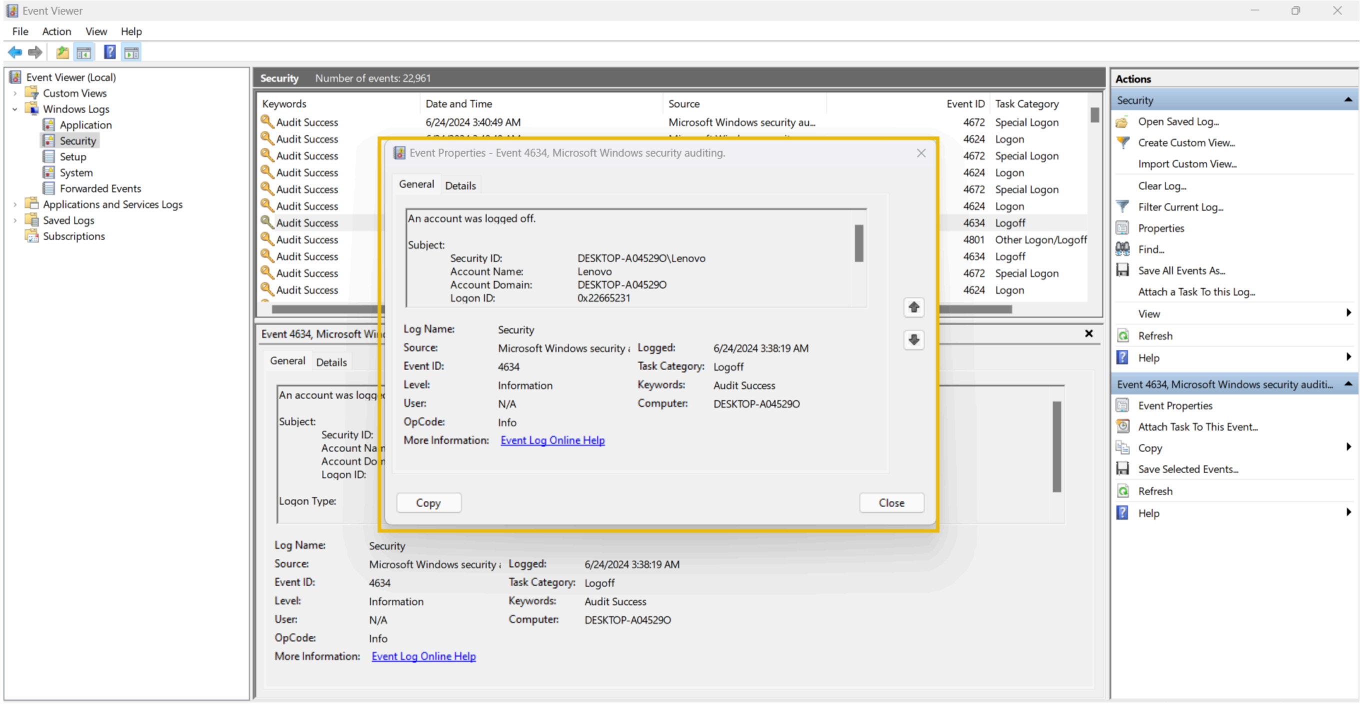
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	6/24/2024 3:40:49 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:40:49 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:40:41 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:40:41 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:38:20 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:38:20 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4634	Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4801	Other Logon/Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4634	Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-A04529O$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	6/24/2024 3:36:31 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-A04529O
OpCode:	Info		
More Information:	Event Log Online Help		



```
Security   Number of events: 22,961

Keywords        Date and Time            Source                              Event ID  Task Category
Audit Success   6/24/2024 3:40:49 AM     Microsoft Windows security au...    4672      Special Logon
Audit Success                                                                4624      Logon
Audit Success                                                                4672      Special Logon
Audit Success                                                                4624      Logon
Audit Success                                                                4672      Special Logon
Audit Success                                                                4624      Logon
Audit Success                                                                4634      Logoff
Audit Success                                                                4801      Other Logon/Logoff
Audit Success                                                                4634      Logoff
Audit Success                                                                4672      Special Logon
Audit Success                                                                4624      Logon
```

Event Properties - Event 4634, Microsoft Windows security auditing.

```
An account was logged off.

Subject:
        Security ID:        DESKTOP-A04529O\Lenovo
        Account Name:       Lenovo
        Account Domain:     DESKTOP-A04529O
        Logon ID:           0x22665231

Log Name:          Security
Source:            Microsoft Windows security a   Logged:          6/24/2024 3:38:19 AM
Event ID:          4634                           Task Category:   Logoff
Level:             Information                    Keywords:        Audit Success
User:              N/A                            Computer:        DESKTOP-A04529O
OpCode:            Info
More Information:  Event Log Online Help
```

Event 4634, Microsoft Wi

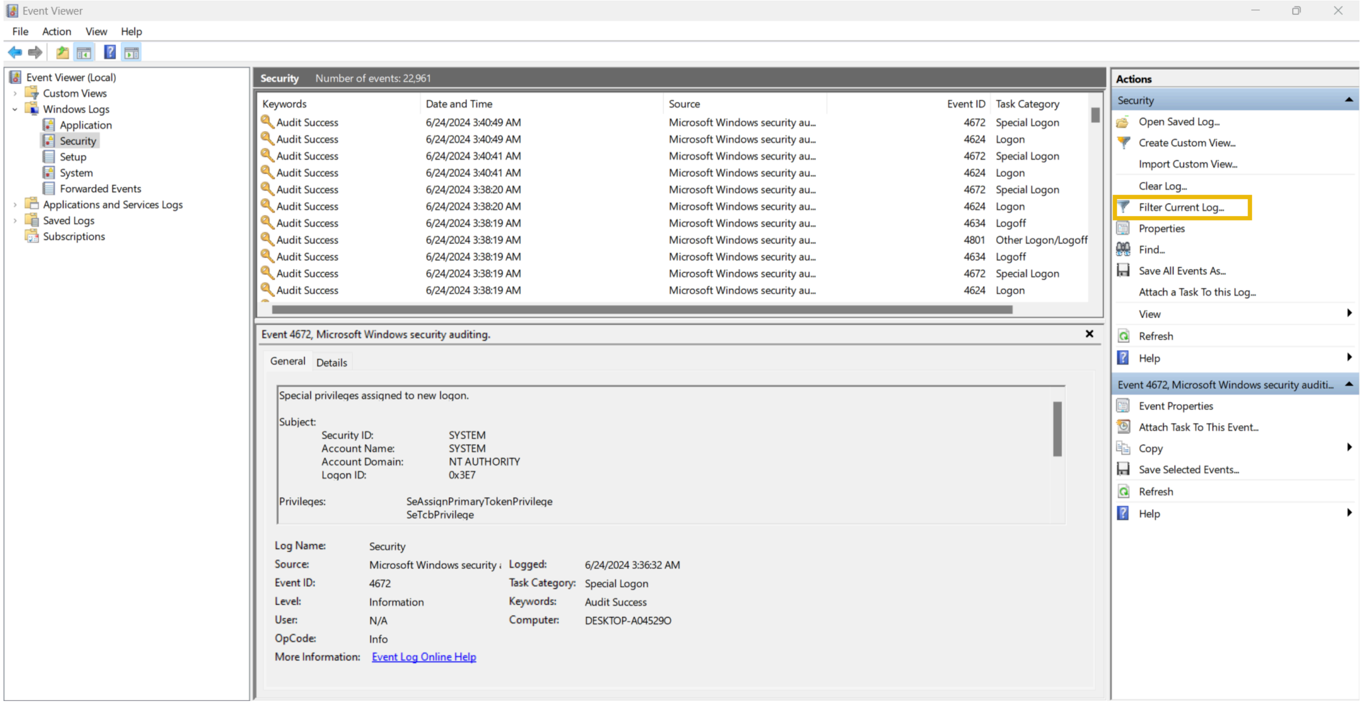
```
An account was logg

Subject:
        Security ID:
        Account Na
        Account Do
        Logon ID:

Logon Type:

Log Name:          Security
Source:            Microsoft Windows security a   Logged:          6/24/2024 3:38:19 AM
Event ID:          4634                           Task Category:   Logoff
Level:             Information                    Keywords:        Audit Success
User:              N/A                            Computer:        DESKTOP-A04529O
OpCode:            Info
More Information:  Event Log Online Help
```

This is how a Windows event log looks. It has different fields. The major fields are discussed below:

- **Description:** This field has a detailed information of the activity.
- **Log Name:** The Log Name indicates the log file name.
- **Logged:** This field indicates the time of the activity.
- **Event ID:** Event IDs are unique identifiers for a specific activity.

Event ID	Description
4624	A user account successfully logged in
4625	A user account failed to login
4634	A user account successfully logged off
4720	A user account was created
4724	An attempt was made to reset an account’s password
4722	A user account was enabled
4725	A user account was disabled
4726	A user account was deleted

Event Viewer allows us to search for the logs related to a specific event ID with its ‘Filter Current Log’ feature. We can click on this feature to apply any filter.



Security Number of events: 22,961

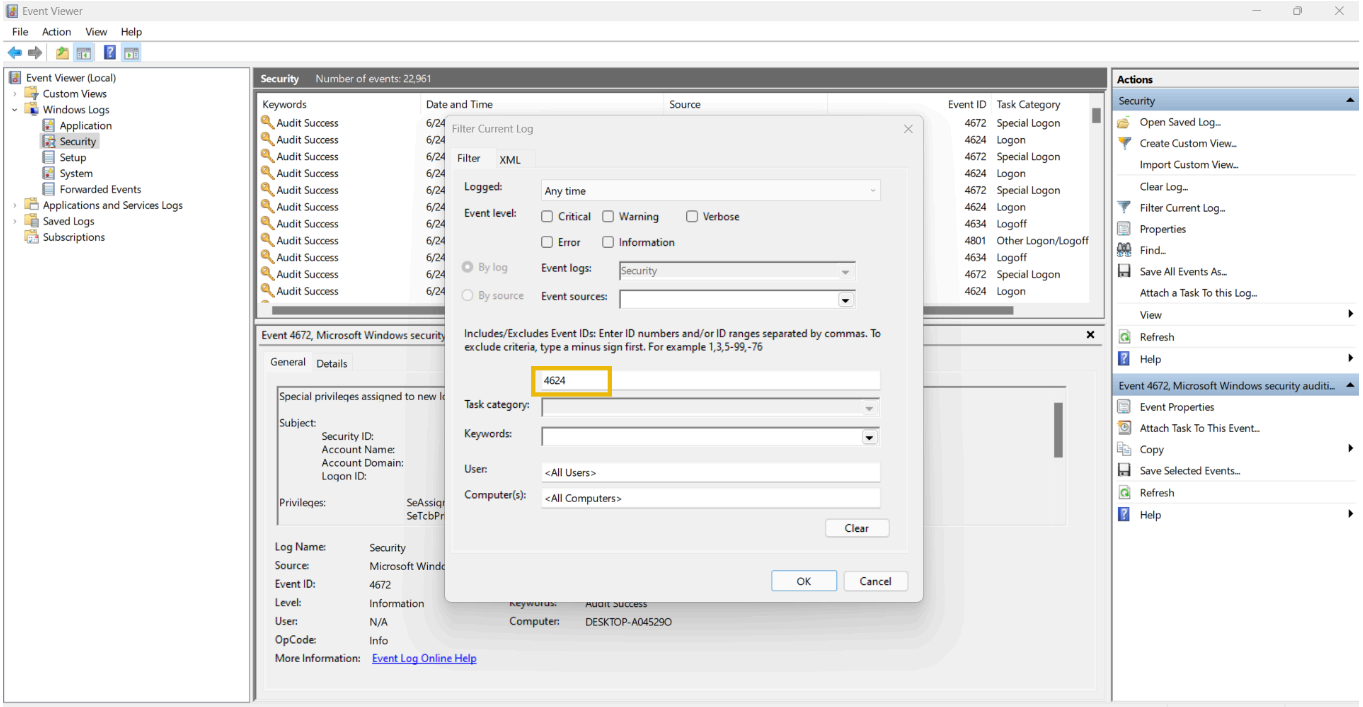
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	6/24/2024 3:40:49 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:40:49 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:40:41 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:40:41 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:38:20 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:38:20 AM	Microsoft Windows security au...	4624	Logon
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4634	Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4801	Other Logon/Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4634	Logoff
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4672	Special Logon
Audit Success	6/24/2024 3:38:19 AM	Microsoft Windows security au...	4624	Logon

Event 4672, Microsoft Windows security auditing.

```
Special privileges assigned to new logon.

Subject:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
```

Log Name: Security
Source: Microsoft Windows security a Logged: 6/24/2024 3:36:32 AM
Event ID: 4672 Task Category: Special Logon
Level: Information Keywords: Audit Success
User: N/A Computer: DESKTOP-A045290
OpCode: Info
More Information: Event Log Online Help

When we click on the ‘Filter Current Log’ option, we will be prompted to enter the event IDs we want to filter. In the screenshot below, I filtered the event ID 4624.



Security Number of events: 22,961

Filter Current Log

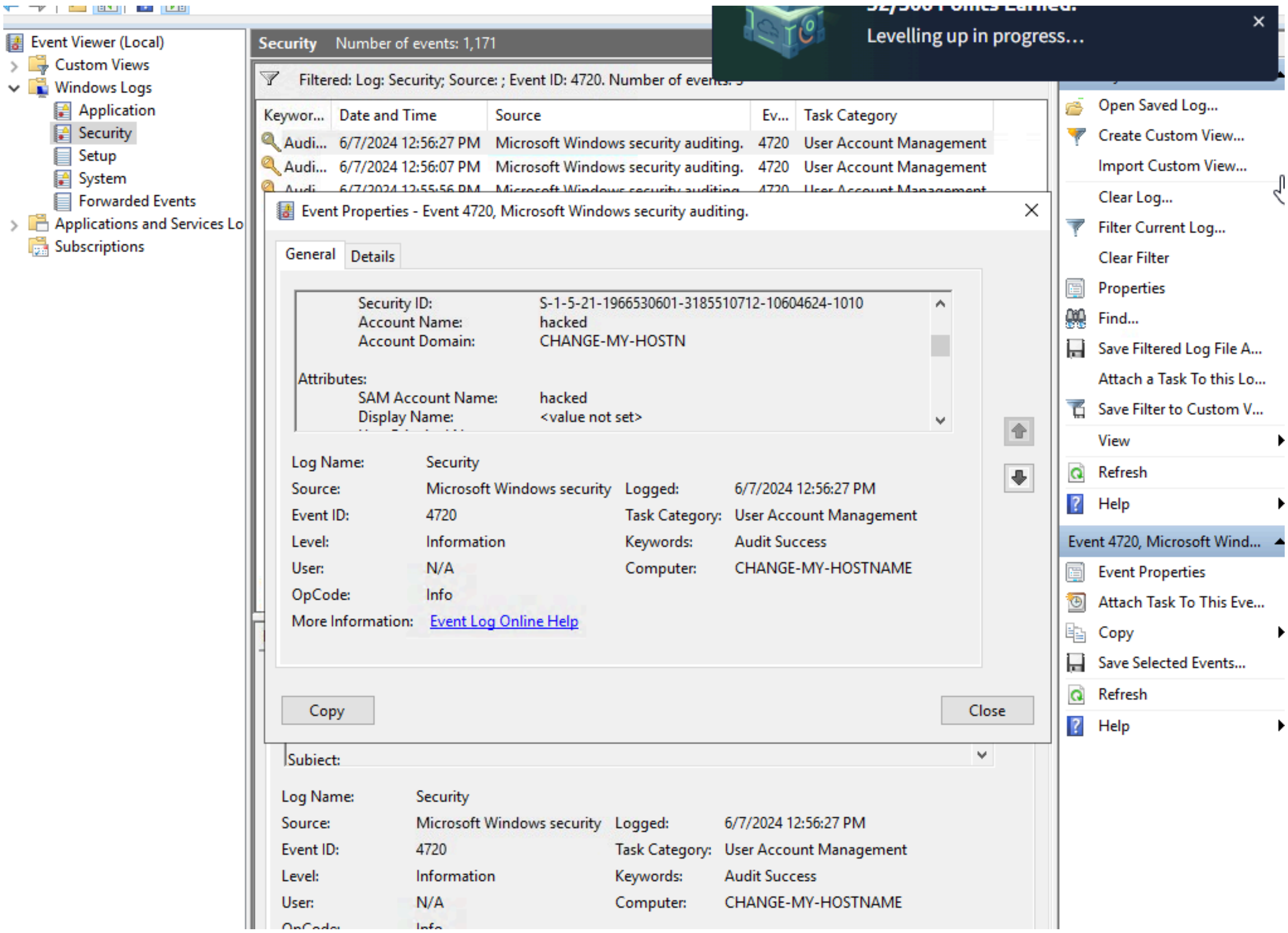
Logged: Any time
Event level: □ Critical □ Warning □ Verbose
□ Error □ Information
○ By log Event logs: Security
○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624

Task category:
Keywords:
User: <All Users>
Computer(s): <All Computers>

practical



Security Number of events: 1,171

Filtered: Log: Security; Source: ; Event ID: 4720. Number of events: 3

Keywor...	Date and Time	Source	Ev...	Task Category
Audi...	6/7/2024 12:56:27 PM	Microsoft Windows security auditing.	4720	User Account Management
Audi...	6/7/2024 12:56:07 PM	Microsoft Windows security auditing.	4720	User Account Management
Audi...	6/7/2024 12:55:56 PM	Microsoft Windows security auditing.	4720	User Account Management

Event Properties - Event 4720, Microsoft Windows security auditing.

```
        Security ID:            S-1-5-21-1966530601-3185510712-10604624-1010
        Account Name:           hacked
        Account Domain:         CHANGE-MY-HOSTN

Attributes:
        SAM Account Name:       hacked
        Display Name:           <value not set>
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:          6/7/2024 12:56:27 PM
Event ID:         4720                         Task Category:   User Account Management
Level:            Information                  Keywords:        Audit Success
User:             N/A                          Computer:        CHANGE-MY-HOSTNAME
OpCode:           Info
More Information: Event Log Online Help
```

Subject:

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:          6/7/2024 12:56:27 PM
Event ID:         4720                         Task Category:   User Account Management
Level:            Information                  Keywords:        Audit Success
User:             N/A                          Computer:        CHANGE-MY-HOSTNAME
OpCode:           Info
```

Here i am viewing an event of an account creation and found that the name is called hacked and found out other information like there was a password reset and who made this account

Web Server Access Logs Analysis

All these requests are logged by the website and stored in a log file on the web server running that website.

his log file contains all the requests made to the website along with the information on the timeframe, the IP requested, the request type, and the URL.

example from apache web server access log:

- **IP Address:** “172.16.0.1” - The IP address of the user who made the request.
- **Timestamp:** “[06/Jun/2024:13:58:44]” - The time when the request was made to the website.
- **Request:** The request details.
  - **HTTP Method:** “GET” - Tells the website what action to be performed on the request.
  - **URL:** “/” - The requested resource.
- **Status Code:** “200” - The response from the server. Different numbers indicate different response results.

- **User-Agent:** “Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36” - Information about the user’s Operating System, browser, etc. when making the request.

We can perform manual log analysis by using some command line utilities in the Linux operating system. The following are some commands that can be useful during manual log analysis.

`cat` [log name]

```
root@kali$ cat access.log
172.16.0.1 - - [06/Jun/2024:13:58:44] "GET /products HTTP/1.1" 404 "-" "Mozilla/5.0 (W
10.0.0.1 - - [06/Jun/2024:13:57:44] "GET / HTTP/1.1" 404 "-" "Mozilla/5.0 (Macintosh;
192.168.1.1 - - [06/Jun/2024:13:56:44] "GET /about HTTP/1.1" 500 "-" "Mozilla/5.0 (Win
```

`grep` is a very useful command line utility that allows you to search for strings and patterns inside a log file. For example, you may need to search if a specific IP address is present in your log file

```
root@kali$ grep "192.168.1.1" access.log
192.168.1.1 - - [06/Jun/2024:13:56:44] "GET /about HTTP/1.1" 500 "-" "Mozilla/5.0 (Wind
192.168.1.1 - - [06/Jun/2024:13:53:44] "GET /products HTTP/1.1" 404 "-" "Mozilla/5.0 (W
192.168.1.1 - - [06/Jun/2024:13:46:44] "GET /about HTTP/1.1" 200 "-" "Mozilla/5.0 (Wind
```

The `less` command is helpful for handling multiple log files. You may need to analyze specific chunks one by one. For this, you can use the less command-line utility, which helps you view one page at a time.

```
root@kali$ less access.log
172.16.0.1 - - [06/Jun/2024:13:52:44] "GET /products HTTP/1.1" 404 "-" "Mozilla/5.0 (Wi
10.0.0.1 - - [06/Jun/2024:13:48:44] "GET /about HTTP/1.1" 404 "-" "Mozilla/5.0 (Windows
192.168.1.1 - - [06/Jun/2024:13:46:44] "GET /about HTTP/1.1" 200 "-" "Mozilla/5.0 (Wind
:
```