Class 15 - 13/09/2023

Task - Understanding QRadar logs

1st Event Log

1. **Event Type**: Success Audit
    - This indicates that the event being logged is a successful operation, typically referring to a positive outcome or action.
2. **Event Description**: A new process has been created
    - This describes the nature of the event. In this case, it suggests that a new process (a program or application) has been created on the system.
3. **Source**: WindowsAuthServer
    - This could be the name or identifier of the service or component responsible for generating this event. In this case, it appears to be related to Windows authentication.
4. **Source Hostname**: LAPTOP-25ALFK55
    - This is the hostname or name of the device or system where the event originated. In this case, it's "LAPTOP-25ALFK55," indicating the source machine.
5. **Event ID**: 1
    - The event ID is often a unique identifier associated with this specific event. It can be used for reference or to look up additional details related to this event.
6. **Event Timestamp**: Sep 14, 2023, 1:20:27 AM
    - This timestamp indicates when the event occurred. In this case, it occurred on September 14, 2023, at 1:20:27 AM.
7. **Category**: System Status
    - The category typically provides additional context about the type or classification of the event. In this case, it's related to "System Status,"

suggesting that it's an event related to the status of the system.

8. **Source IP Address**: 192.168.1.7
    - This is the IP address of the system or device where the event originated, which is 192.168.1.7 in this case.
9. **Source Port**: 0
    - The source port number, often used in network-related events. A port number of 0 might indicate that it's not relevant to this particular event.
10. **Destination IP Address**: 192.168.1.7
    - This is the IP address of the destination or target system where the event is directed or affecting. It's the same as the source IP address in this log entry, suggesting a local action.
11. **Destination Port**: 0
    - Similar to the source port, the destination port is often associated with network-related events. A port number of 0 might indicate that it's not relevant to this event.
12. **Username**: Akshay
    - This is the username associated with the event, suggesting that the user named "Akshay" was involved in or responsible for the creation of the new process.

In summary, this QRadar log entry indicates that a new process was successfully created on a system named "LAPTOP-25ALFK55" on September 14, 2023, at 1:20:27 AM. The event is related to system status, and the user "Akshay" appears to be associated with this action. It's important to note that further investigation may be needed to determine the nature and significance of this process creation and whether it was a legitimate or potentially suspicious activity.

2nd Event log:

1. **Event Type**: Failure Audit
    - This indicates that the event being logged is a failed operation or action. It suggests that something went wrong during the execution of a particular

operation.

2. **Event Description**: A privileged service was called
    - This describes the nature of the event. It indicates that a privileged or high-privileged service or operation was invoked but did not succeed.
3. **Source**: WindowsAuthServer
    - This could be the name or identifier of the service or component responsible for generating this event. In this case, it appears to be related to Windows authentication.
4. **Source Hostname**: LAPTOP-25ALFK55
    - This is the hostname or name of the device or system where the event originated. In this case, it's "LAPTOP-25ALFK55," indicating the source machine.
5. **Event ID**: 255
    - The event ID is often a unique identifier associated with this specific event. It can be used for reference or to look up additional details related to this event.
6. **Event Timestamp**: Sep 14, 2023, 1:33:12 AM
    - This timestamp indicates when the event occurred. In this case, it occurred on September 14, 2023, at 1:33:12 AM.
7. **Category**: Misc Authorization
    - The category typically provides additional context about the type or classification of the event. In this case, it's related to "Misc Authorization," suggesting that it's an event related to authorization actions.
8. **Source IP Address**: 192.168.1.7
    - This is the IP address of the system or device where the event originated, which is 192.168.1.7 in this case.
9. **Source Port**: 0
    - The source port number, often used in network-related events. A port number of 0 might indicate that it's not relevant to this particular event.
10. **Destination IP Address**: 192.168.1.7

- This is the IP address of the destination or target system where the event is directed or affecting. It's the same as the source IP address in this log entry, suggesting a local action.

11. **Destination Port**: 0
    - Similar to the source port, the destination port is often associated with network-related events. A port number of 0 might indicate that it's not relevant to this event.
12. **Username**: Akshay
    - This is the username associated with the event, suggesting that the user named "Akshay" was involved in or responsible for the privileged service call.

In summary, this QRadar log entry indicates that a privileged service call failed on a system named "LAPTOP-25ALFK55" on September 14, 2023, at 1:33:12 AM. The event is related to miscellaneous authorization, and the user "Akshay" appears to be associated with this action. The failure of a privileged service call can be a significant event that may warrant further investigation to understand the cause and potential security implications.

3rd Event log:

1. **Event Type**: Failure Audit
    - This indicates that the event being logged is a failed operation or action. It suggests that something went wrong during the execution of a particular operation.
2. **Event Description**: A privileged service was called
    - This describes the nature of the event. It indicates that a privileged or high-privileged service or operation was invoked but did not succeed.
3. **Source**: WindowsAuthServer
    - This could be the name or identifier of the service or component responsible for generating this event. In this case, it appears to be related to Windows authentication.

4. **Source Hostname**: LAPTOP-25ALFK55
    - This is the hostname or name of the device or system where the event originated. In this case, it's "LAPTOP-25ALFK55," indicating the source machine.
5. **Event ID**: 51
    - The event ID is often a unique identifier associated with this specific event. It can be used for reference or to look up additional details related to this event.
6. **Event Timestamp**: Sep 14, 2023, 1:35:06 AM
    - This timestamp indicates when the event occurred. In this case, it occurred on September 14, 2023, at 1:35:06 AM.
7. **Category**: Misc Authorization
    - The category typically provides additional context about the type or classification of the event. In this case, it's related to "Misc Authorization," suggesting that it's an event related to authorization actions.
8. **Source IP Address**: 192.168.1.7
    - This is the IP address of the system or device where the event originated, which is 192.168.1.7 in this case.
9. **Source Port**: 0
    - The source port number, often used in network-related events. A port number of 0 might indicate that it's not relevant to this particular event.
10. **Destination IP Address**: 192.168.1.7
    - This is the IP address of the destination or target system where the event is directed or affecting. It's the same as the source IP address in this log entry, suggesting a local action.
11. **Destination Port**: 0
    - Similar to the source port, the destination port is often associated with network-related events. A port number of 0 might indicate that it's not relevant to this event.
12. **Username**: Akshay

- This is the username associated with the event, suggesting that the user named "Akshay" was involved in or responsible for the privileged service call.

In summary, this QRadar log entry indicates that a privileged service call failed on a system named "LAPTOP-25ALFK55" on September 14, 2023, at 1:35:06 AM. The event is related to miscellaneous authorization, and the user "Akshay" appears to be associated with this action. The failure of a privileged service call can be a significant event that may warrant further investigation to understand the cause and potential security implications.

4th Event log:

1. **Event Type**: Success Audit
    - This indicates that the event being logged is a successful operation, typically referring to a positive outcome or action.
2. **Event Description**: The Windows Filtering Platform has allowed a connection
    - This describes the nature of the event. It suggests that the Windows Filtering Platform (a component in Windows used for filtering and processing network traffic) allowed a connection, meaning that a network connection was permitted without any issues.
3. **Source**: WindowsAuthServer
    - This could be the name or identifier of the service or component responsible for generating this event. In this case, it appears to be related to Windows authentication.
4. **Source Hostname**: LAPTOP-25ALFK55
    - This is the hostname or name of the device or system where the event originated. In this case, it's "LAPTOP-25ALFK55," indicating the source machine.
5. **Event ID**: 1
    - The event ID is often a unique identifier associated with this specific event. It can be used for reference or to look up additional details related to this event.

6. **Event Timestamp**: Sep 14, 2023, 1:35:07 AM
    - This timestamp indicates when the event occurred. In this case, it occurred on September 14, 2023, at 1:35:07 AM.
7. **Category**: Access Permitted
    - The category typically provides additional context about the type or classification of the event. In this case, it's related to "Access Permitted," indicating that a network connection was successfully allowed.
8. **Source IP Address**: 192.168.1.7
    - This is the IP address of the system or device where the event originated, which is 192.168.1.7 in this case.
9. **Source Port**: 50686
    - The source port number is often used in network-related events and represents the port from which the connection originated.
10. **Destination IP Address**: 50.112.199.176
    - This is the IP address of the destination or target system with which the successful network connection was established.
11. **Destination Port**: 443
    - The destination port number is the port on the destination system to which the successful connection was made. Port 443 is commonly associated with HTTPS (secure web browsing).
12. **Username**: N/A

In summary, this QRadar log entry indicates that the Windows Filtering Platform on the system named "LAPTOP-25ALFK55" allowed a successful network connection from the source IP address 192.168.1.7 (port 50686) to the destination IP address 50.112.199.176 (port 443) on September 14, 2023, at 1:35:07 AM. The event is categorized as "Access Permitted," signifying that the network connection was successfully allowed without any issues.