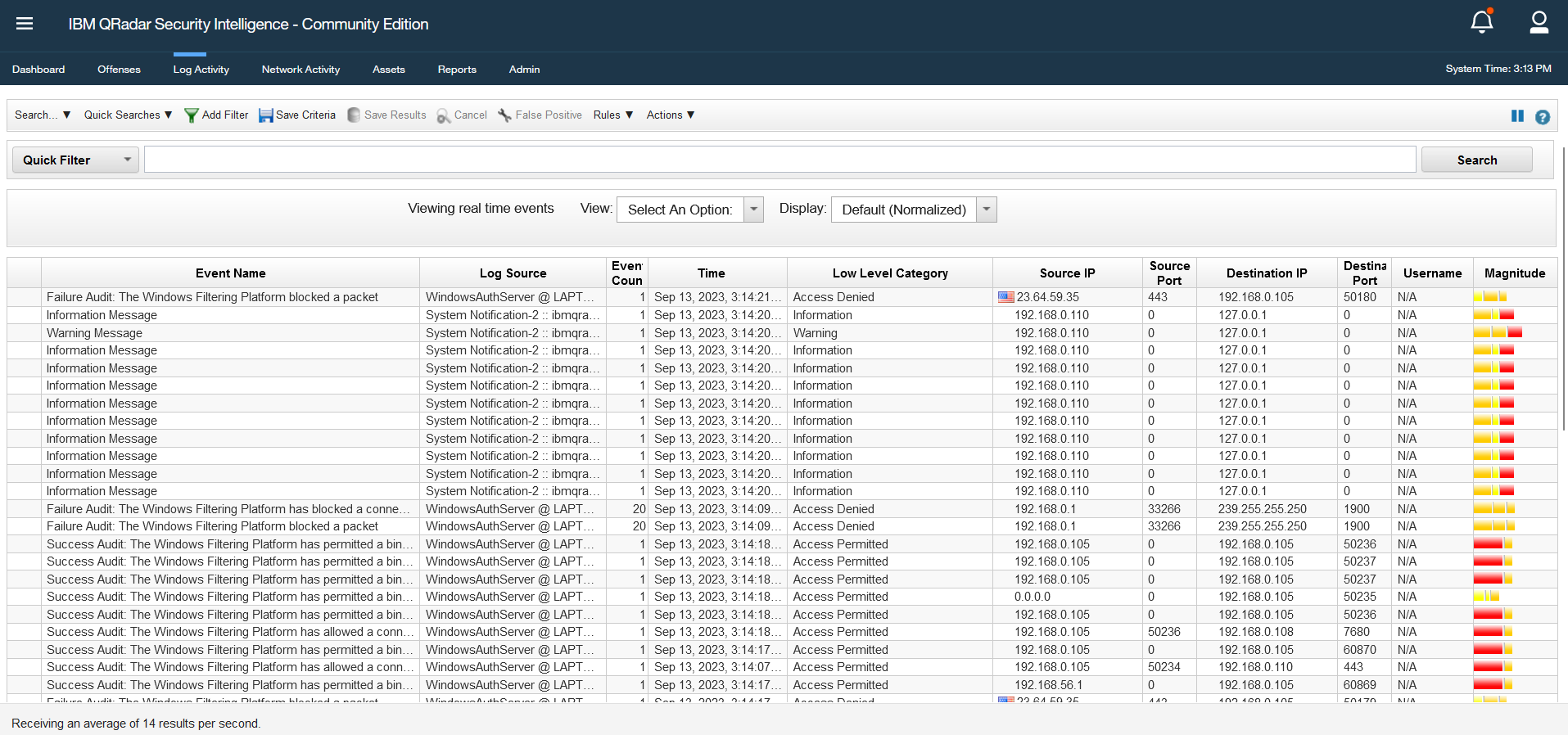
TASK-12

SAMEER CHAUHAN 21BCE0999 WEDNESDAY 13-09-23



**AIM-** We have to take any 4 logs from IBM Q Radar community edition



As in the above screenshot we can see logs of our computer generated by IBM Q Radar now we will select any 4 and discuss them in detail-

1. This is our first log which we have taken for research

**Description:** "The Windows Filtering Platform has permitted a bind to a local port" suggests that a program or process running on the system attempted to bind (associate) a network port with a local service, and this action was allowed by the Windows Filtering Platform.

**Log Source:** Windows Auth Server @ LAPTOP-0UCJ730O" means that the log entry originates from a computer or server named "LAPTOP-0UCJ730O," and it's associated with a service or application named "Windows Auth Server."

**Timestamp:** "Sep 13, 2023, 3:18:05 PM" indicates when this event occurred. It provides the date and time in a standardized format.

**Event Type:** "Access Permitted" suggests that whatever action is being logged was allowed or permitted by the system's security settings.

**Source IP Address:** "224.0.0.251" is the IP address of the system or device that initiated the action being logged.

**Source Port:** "5353" is the port number on which the source system sent the network traffic. Port 5353 is commonly associated with the m DNS (Multicast DNS) protocol, which is used for device discovery and service resolution on local networks.

**Destination IP Address:** "192.168.0.100" is the IP address of the local system or service to which the connection was made. In this case, it's the same as the source IP, indicating that the connection is local.

**Destination Port:** "5353" is the port number on which the local system received the incoming network traffic. In this case, it matches the source port, which is common for UDP multicast traffic.

**User/Account:** "N/A" means that the log entry doesn't specify a specific user or account associated with this event. This could be because it's a system-level event or because the logging system didn't capture user information.

**Event id-** "14" is an identifier used to categorize and differentiate different types of events in a log system. In this case, it represents a specific type of event related to network communication.

1. Now we will discuss our second log



**Description**: "A privileged service was called" means that an operation was attempted that required privileged or elevated access rights. Privileged services often have higher levels of system access and control.

**Log Source**: "Windows Auth Server @ LAPTOP-0UCJ730O" means that this log entry is associated with a service or application named "Windows Auth Server" running on a computer called "LAPTOP-0UCJ730O."

**Event ID**: 358 is typically used to categorize and identify specific types of events in a log system. In this case, it represents a failure audit event related to a privileged service call.

**Timestamp**: "Sep 13, 2023, 3:34:09 PM" provides us the date and time when this event occurred, allowing you to track when the event took place.

**Event Type**: "Failure Audit" indicates that the action described in this log entry was not successful and was audited for security purposes.

**Source IP Address**: "192.168.0.105" is the IP address of the system or device that initiated the privileged service call.

**Source Port**: "0" represents an dynamically assigned source port. It's used by the operating system to establish connections.

**Destination IP Address**: "192.168.0.105" is the local system's IP address to which the privileged service call was made. In this case, it appears to be a local operation within the same device.

**Destination Port**: "0" is also listed as the destination port. Port "0" is typically used to represent an unspecified or reserved port.

3-Now we will discuss our third log-



**Event Type:** "Information Message" indicates that this log entry is informational in nature. It is not an error or security-related event but rather serves to convey a message or notification.

**Log source:** "System Notification-2" suggests that this log entry is related to a system notification, and the number "2" may represent a specific notification or message identifier.

**Source IP Address:** "192.168.0.110" is the IP address of the system or device from which this log entry originated.

**Source Port:** "0" typically represents an ephemeral or dynamically assigned source port. It's used by the operating system to establish connections.

**Destination IP Address:** "127.0.0.1" is the loopback IP address, commonly used to refer to the local machine itself. In this context, it indicates that the system notification is being generated and logged on the local system.

**Destination Port:** "0" is also listed as the destination port. Port "0" is typically used to represent an unspecified or reserved port.

**User/Account:** "N/A" suggests that the log entry doesn't specify a specific user or account associated with this notification. This is common for system-level notifications.

**4-**Now we will see our 4th log :



**Event Type:** "Health Metric" indicates that this log entry pertains to the monitoring of health metrics or system health status.

**Log source:** "Health Metrics-2" suggests that this log entry is related to health metrics, and the number "2" may represent a specific health metric identifier or category.

**Timestamp:** "Sep 13, 2023, 3:45:54 PM" provides the date and time when this health metric was recorded, allowing you to track when the metric was collected.

**Source IP Address:** "192.168.0.110" is the IP address of the system or device from which this log entry originated.

**Source Port:** "0" typically represents an ephemeral or dynamically assigned source port, which is used by the operating system to establish connections.

**Destination IP Address:** "127.0.0.1" is the loopback IP address, commonly used to refer to the local machine itself. In this context, it indicates that the health metric data was collected and logged on the local system.

**Destination Port:** "0" is also listed as the destination port. Port "0" is typically used to represent an unspecified or reserved port.

**User/Account:** "N/A" suggests that the log entry doesn't specify a specific user or account associated with this health metric. This is common for system-level health monitoring.