**Lab Exercise 3- Creating a Cron-Based Scheduled Alert in Splunk**

**Objective**

In this lab, you will learn how to create a **cron-based scheduled alert** in Splunk. Scheduled alerts in Splunk allow you to automate searches and notifications, making it easier to monitor data continuously.

**Objectives**

1. Create a search that will be run on a schedule.
2. Set up a cron expression to control when the search runs.
3. Set up an alert action (e.g., email notification) when the search results match specific conditions.

**Pre-requisites**

* Access to a Splunk instance with sufficient privileges to create alerts.
* A sample index or dataset to run the search on.

**Steps**

**Step 1: Access Splunk Web Interface**

1. Log in to the Splunk Web interface.
2. Navigate to the **Search & Reporting** app.

**Step 2: Create a Search for the Alert**

1. Go to the **Search & Reporting** app.
2. Create a search query that will be used to trigger the alert. For example, let's search for error logs in a custom index:

index=custom\_index log\_level="ERROR"

This search will return all events with a log\_level field set to ERROR.

1. You can customize this search based on your use case, for example, searching for logs exceeding a certain threshold, or matching specific keywords.

**Step 3: Save as a Scheduled Alert**

1. After testing the query and verifying it returns results, click on **Save As** at the top right of the search bar.
2. From the dropdown, select **Alert**.
3. Fill in the details for the alert:
   * **Title**: Name your alert (e.g., Error Logs Alert).
   * **Description**: Optionally, provide a description of the alert.
   * **Severity**: Choose the severity level (e.g., Critical).

**Step 4: Set the Schedule Using Cron Expression**

1. Under the **Schedule** section, configure the frequency of the search:
   * **Run alert every**: Select the frequency, e.g., every **5 minutes** or **Hourly**.
   * **Cron Expression**: You can define a custom cron expression to control when the search runs. For example:
     + To run every 5 minutes: \*/5 \* \* \* \*
     + To run every hour: 0 \* \* \* \*
     + To run every day at midnight: 0 0 \* \* \*

You can find more information about cron syntax [here](https://en.wikipedia.org/wiki/Cron#Overview).

**Step 5: Set Alert Conditions**

1. Under **Trigger Condition**, select when you want the alert to be triggered:
   * **If number of results**: Select the option to trigger the alert if there are more than 0 results. This will alert you every time an error log is found.
   * You can also use more advanced conditions, such as triggering based on thresholds or specific patterns.
2. Select **Trigger Alert** when conditions are met.

**Step 6: Set Alert Actions**

1. Choose an action for when the alert is triggered:
   * **Send Email**: Enter the recipient email address, subject, and message body for the alert notification. You can also include dynamic fields like the number of events or specific results from the search in the email.
   * **Webhook**: Optionally, you can configure a webhook to send the alert to another system.
   * **Run a Script**: Configure a script to run when the alert is triggered.
2. Click **Save** to create the scheduled alert.

**Step 7: Verify the Alert**

1. You can verify that the alert is scheduled by going to **Settings** > **Searches, Reports, and Alerts**.
2. Find your newly created alert in the list.
3. You can manually trigger the alert or wait for the cron schedule to run, depending on your chosen schedule.