**Lab Exercise 5- Create an Email Notification Alert in Splunk**

**Objective**

This exercise demonstrates how to configure Splunk to monitor failed login attempts and send an email notification using Gmail when the count exceeds a threshold.

**Prerequisites**

* Access to a Splunk instance.
* Gmail SMTP server details and credentials (with "Allow less secure apps" enabled or an app password for secure access).
* Sample auth.log file containing failed login attempts.

**Detailed Steps**

**1. Configure Gmail as the SMTP Server in Splunk**

1. **Log in to Splunk Web** with admin privileges.
2. Navigate to **Settings > Server Settings > Email Settings**.
3. Configure the following settings:
   * **Mail Host**: smtp.gmail.com:587
   * **Email Security**: Enable TLS
   * **Username**: Your Gmail address (e.g., your\_email@gmail.com)
   * **Password**: Gmail app password or account password if "Allow less secure apps" is enabled.
   * **Sender**: Your Gmail address (e.g., your\_email@gmail.com)
4. Click **Save** to apply the settings.

**2. Create a New Index**

1. Navigate to **Settings > Indexes**.
2. Click **New Index** and set the following details:
   * **Index Name**: login\_alerts
   * Leave other fields as default.
3. Save the index.

**3. Prepare and Upload the auth.log File**

1. Save the following sample log data as auth.log:

***auth.log***

Mar 23 12:01:45 server1 sshd[1234]: Failed password for invalid user root from 192.168.1.1 port 22 ssh2

Mar 23 12:05:12 server1 sshd[1256]: Failed password for user admin from 192.168.1.2 port 22 ssh2

Mar 23 12:10:03 server1 sshd[1278]: Failed password for invalid user guest from 192.168.1.3 port 22 ssh2

Mar 23 12:15:47 server1 sshd[1300]: Failed password for user john from 192.168.1.4 port 22 ssh2

Mar 23 12:20:29 server1 sshd[1322]: Failed password for user admin from 192.168.1.5 port 22 ssh2

1. Upload the file:
   * Go to **Settings > Add Data > Upload**.
   * Select auth.log and click **Next**.
   * Choose **Source Type** as **linux\_secure** or default.
   * Select the **login\_alerts** index as the destination.
   * Click **Review > Submit**.

**4. Create the Search Query**

1. Navigate to the **Search & Reporting** app.
2. Run the following query to search for failed login attempts:

index=login\_alerts "Failed password" | stats count as failed\_attempts

1. Verify that the search results display the count of failed attempts.

**5. Create an Alert for Email Notification**

1. Click **Save As > Alert** in the search bar.
2. Set the alert details:
   * **Title**: Failed Login Attempts Alert
   * **Alert Type**: Scheduled
   * **Time Range**: Run every 5 minutes.
   * **Trigger Condition**:
     + **Trigger alert when:** Number of results > 3.
3. Under **Alert Actions**, select **Send Email**:
   * **To**: Your email address (e.g., your\_email@gmail.com)
   * **Subject**: Alert: Too Many Failed Login Attempts
   * Customize the body if needed.
4. Save the alert.

**6. Validate the Alert**

1. Modify the log file to include additional failed login attempts.
2. Upload the updated auth.log file to the login\_alerts index.
3. Wait for the alert to trigger and check your Gmail inbox for the notification.

**Troubleshooting**

* **Email Not Received**:
  + Verify SMTP settings in **Email Settings**.
  + Ensure the email domain is not restricted in Splunk.
  + Check your Gmail account for blocked sign-in attempts.
* **No Alert Triggered**:
  + Confirm the search query returns results exceeding the threshold.
  + Check that the alert is enabled in **Settings > Searches, Reports, and Alerts**.