**Assignment 2- Create an Alert for Monitoring Unauthorized Access Attempts on a Web Server**

**Objective**

**Scenario: Monitoring Unauthorized Access Attempts on a Web Server**

You are tasked with creating a Splunk alert that monitors unauthorized access attempts on a web server. The log data contains HTTP request information, including status codes indicating access issues (e.g., 401 for unauthorized and 403 for forbidden access). The alert should trigger when more than **10 unauthorized access attempts** occur from the same IP address within 10 minutes.

**Alternative Log Data**

Save the following as webserver\_access.log:

***webserver\_access.log***

192.168.1.10 - - [23/Mar/2024:12:01:45 +0000] "GET /admin HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.11 - - [23/Mar/2024:12:03:12 +0000] "POST /login HTTP/1.1" 403 256 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:05:33 +0000] "GET /dashboard HTTP/1.1" 200 512 "-" "Mozilla/5.0"

192.168.1.12 - - [23/Mar/2024:12:06:45 +0000] "GET /admin HTTP/1.1" 403 128 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:08:15 +0000] "GET /admin HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.11 - - [23/Mar/2024:12:10:20 +0000] "POST /login HTTP/1.1" 403 256 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:12:45 +0000] "GET /settings HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:14:50 +0000] "GET /admin HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:16:33 +0000] "GET /admin HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:18:15 +0000] "GET /dashboard HTTP/1.1" 200 512 "-" "Mozilla/5.0"

192.168.1.10 - - [23/Mar/2024:12:20:00 +0000] "GET /admin HTTP/1.1" 401 128 "-" "Mozilla/5.0"

192.168.1.11 - - [23/Mar/2024:12:21:50 +0000] "POST /login HTTP/1.1" 403 256 "-" "Mozilla/5.0"

**Steps for the Lab Exercise**

**1. Upload Log Data to Splunk**

1. Navigate to **Settings > Add Data > Upload**.
2. Select webserver\_access.log and upload it.
3. Choose the **Source Type** as access\_combined (or default).
4. Assign the data to an index (e.g., web\_alerts).
5. Verify the data upload by clicking **Start Searching**.

**2. Write the Search Query**

1. Go to the **Search & Reporting** app.
2. Write the query to detect unauthorized access attempts:

index=web\_alerts status IN (401, 403) | stats count by clientip | where count > 10

1. Run the query to verify it returns IP addresses with more than 10 unauthorized attempts.

**3. Create an Alert**

1. Click **Save As > Alert**.
2. Fill in the following details:
   * **Title**: Unauthorized Access Alert
   * **Alert Type**: Scheduled
   * **Time Range**: Run every 10 minutes.
   * **Trigger Condition**: Number of results > 0.
3. **Alert Actions**:
   * Select **Send Email**.
   * Configure the email settings:
     + **To**: Your email address (**hiteshupes@gmail.com**).
     + **Subject**: Alert: Unauthorized Access Attempts Detected.
     + Customize the body message as required.
4. Save the alert.

**4. Validate the Alert**

1. Modify the webserver\_access.log file to add additional unauthorized access attempts.
2. Re-upload the updated log file.
3. Wait for the alert to trigger and verify you receive an email notification.

**Deliverables**

1. **Search Query**: Submit the query used to detect unauthorized access attempts.
2. **Alert Configuration**: Provide a screenshot or description of the alert settings.
3. **Validation Output**: Share a screenshot of the triggered alert or email notification.

**Evaluation Criteria**

* Correctness of the search query.
* Proper configuration of the alert trigger and notification.
* Successful validation of the alert.