**Assignment 3- : Loading Log Data, Creating an Index, and Running SPL Queries, Create Dashboard and Report**

**Objective**

The goal of this assignment is to upload a provided log data file into Splunk, create a new index for the data, and run specific SPL queries to analyze the data. This will help you understand data ingestion, indexing, and querying in Splunk.

**Steps for the Assignment**

**1. Prepare the Log Data**

Use the following log data for this assignment. Save it as auth\_access.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]: Accepted password for user john 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

Mar 23 12:25:40 server1 sshd[1344]: Accepted password for user alice from 192.168.1.6 port 22 ssh2

Mar 23 12:30:12 server1 sshd[1366]: Failed password for invalid user guest from 192.168.1.7 port 22 ssh2

Mar 23 12:35:55 server1 sshd[1388]: Accepted password for user alice from 192.168.1.8 port 22 ssh2

Mar 23 12:40:33 server1 sshd[1400]: Failed password for user root from 192.168.1.9 port 22 ssh2

**2. Create a New Index**

1. Log in to **Splunk Web**.
2. Navigate to **Settings > Indexes > New Index**.
3. Create an index with the following details:
   * **Index Name**: auth\_log\_index
   * **Data Type**: Events
   * Leave other settings as default and click **Save**.

**3. Upload Log Data to the New Index**

1. Navigate to **Settings > Add Data > Upload**.
2. Select the auth\_access.log file.
3. Assign the log data to the newly created index (auth\_log\_index).
4. Choose the **Source Type** as linux\_secure (or leave it to auto-detect).
5. Click **Review** and then **Submit**.
6. Verify the data upload by going to **Search & Reporting** and using the query:

index=auth\_log\_index

**4. Run SPL Queries**

Run the following queries in the **Search & Reporting** app and analyze the results:

**Query 1: Total Number of Failed Login Attempts**

index=auth\_log\_index "Failed password" | stats count as total\_failed\_logins

**Query 2: Failed Login Attempts by IP Address**

index=auth\_log\_index "Failed password" | stats count as failed\_attempts by src\_ip

**Query 3: Top 5 Users with Most Failed Login Attempts**

index=auth\_log\_index "Failed password" | stats count by user | sort - count | head 5

**Query 4: Trend of Failed Logins Over Time**

index=auth\_log\_index "Failed password" | timechart span=1m count as failed\_logins

**5. Save a Report**

1. After running Query 3 (Top 5 Users), click **Save As > Report**.
2. Name the report **Top Failed Users** and save it for future use.

**6. Create a Dashboard**

1. Navigate to **Dashboards** and click **Create New Dashboard**.
2. Name the dashboard **Auth Log Analysis**.
3. Add the following panels to the dashboard:
   * **Total Failed Logins** (Query 1).
   * **Failed Logins by IP Address** (Query 2).
   * **Top Failed Users** (Query 3).
   * **Trend of Failed Logins Over Time** (Query 4).
4. Save and view the dashboard.

**Deliverables**

1. **Search Queries**: Provide the SPL queries used for the analysis.
2. **Screenshots**: Include screenshots of:
   * The uploaded log data in the new index.
   * Query results for each of the provided SPL queries.
   * The final dashboard.
3. **Report**: Share the saved report for Query 3.

**Evaluation Criteria**

* Correct creation of the index and successful data upload.
* Accuracy of the SPL queries and their outputs.
* Proper design and content of the dashboard.