**Assignment 1- Creating an Index and Running SPL Queries**

**Objective**

Learn to create a Splunk index, upload log data into the index, and run basic SPL queries to analyze the data.

**Log Data**

Save the following log data as simple\_auth.log:

Mar 23 10:01:45 server1 sshd[1234]: Failed password for user root from 192.168.0.1 port 22 ssh2

Mar 23 10:03:12 server1 sshd[1256]: Accepted password for user admin from 192.168.0.2 port 22 ssh2

Mar 23 10:05:33 server1 sshd[1278]: Failed password for invalid user guest from 192.168.0.3 port 22 ssh2

Mar 23 10:07:45 server1 sshd[1300]: Failed password for user alice from 192.168.0.4 port 22 ssh2

Mar 23 10:09:15 server1 sshd[1322]: Accepted password for user bob from 192.168.0.5 port 22 ssh2

**Steps for the Assignment**

**1. Create an Index**

1. Log in to **Splunk Web**.
2. Navigate to **Settings > Indexes > New Index**.
3. Create an index with the following details:
   * **Index Name**: simple\_auth\_index
   * **Data Type**: Events
4. Save the index.

**2. Upload Log Data**

1. Navigate to **Settings > Add Data > Upload**.
2. Select the simple\_auth.log file.
3. Assign the data to the newly created index (simple\_auth\_index).
4. Review and submit the data upload.
5. Verify the data upload by running the following query in the **Search & Reporting** app:

index=simple\_auth\_index

**3. Run Basic SPL Queries**

Run the following queries in the **Search & Reporting** app:

**Query 1: Total Events in the Index**

index=simple\_auth\_index | stats count as total\_events

**Query 2: Count of Successful and Failed Logins**

index=simple\_auth\_index | eval status=if(match(\_raw, "Accepted password"), "Success", "Failure") | stats count by status

**Query 3: List of Unique IP Addresses**

index=simple\_auth\_index | stats dc(src\_ip) as unique\_ips values(src\_ip) as ip\_list

**Query 4: Failed Login Attempts by User**

index=simple\_auth\_index "Failed password" | stats count by user

**4. Save the Results**

1. **Save as Report**: After running Query 2, save the query results as a report named **Login Status Summary**.
2. **Save as Dashboard Panel**:
   * Create a new dashboard named **Auth Log Dashboard**.
   * Add panels for Queries 1, 2, and 4.

**Deliverables**

1. **SPL Queries**: Submit the queries used in the exercise.
2. **Screenshots**:
   * Query results for each SPL query.
   * The dashboard with panels for Queries 1, 2, and 4.

**Evaluation Criteria**

* Successful creation of the index.
* Accuracy of the SPL queries and their results.
* Proper configuration of the dashboard.

This assignment is simple and helps you get started with Splunk's core functionalities.