Name: Syeda Maryam Raza **Roll # 261910689**

Course: CSCS 462 (A) **Assignment: 2**

Assignment Report

In this Splunk project, the primary goal was to **ingest sample log data**, analyze it using search queries, visualize trends through dashboards, and set up alerts for suspicious activities, such as failed login attempts.

- The process began by navigating to the **"Add Data"** section in Splunk and choosing the **"Upload"** option.
- A sample log file **(currency.csv)** was uploaded, and the source type was set to **“csv”** to match the format of standard web access logs.
- The data was then assigned to an index named **“summary”**, and the indexing was confirmed, making the data available for search and analysis.

Once the data was indexed, the **Search & Reporting app** in Splunk was used to explore and analyze it.

- To view all the log entries, the query **index=summary** was used.
- To identify unauthorized access attempts, the search was refined to **index=summary status=401**, which returned all HTTP 401 error entries.
- Additionally, login attempts from a specific IP address were examined using **index=summary clientip="192.168.1.20".** To better understand user activity, a statistical summary was created with the query **index=summary | stats count by clientip**, which showed the number of requests per client IP.

To visually represent these findings, a new **dashboard** was created in Splunk.

- The dashboard included three key panels: **"Failed Logins Over Time", "Most Active IPs",** and **"Access Trends Per Hour".**
- These visualizations were created using time-based and statistical search queries, helping to uncover patterns and trends in the access logs.
- After building the **dashboard**, it was **saved**, shared with stakeholders, and **exported as a PDF** for reporting and documentation purposes.

Finally, a basic **alert was configured** to enhance monitoring.

- The alert was based on the query **index=summary | stats count by clientip**, designed to identify IP addresses with repeated failed login attempts.
- The alert was set to trigger when the count of HTTP 401 errors exceeded 5 within a 5-minute window.

- For response actions, the alert was configured to send an email notification and to be added to the **“Alert Dashboard”** for real-time visibility.

This end-to-end implementation demonstrates how Splunk can be used to effectively manage log data—from ingestion to actionable insights. With dashboards and alerts in place, it becomes easier to detect anomalies and respond promptly to potential security threats.