Splunk Log Analysis Project – Auth Log Insights

lovish

Part A: **Analyzing Structured Log Files (CSV)**

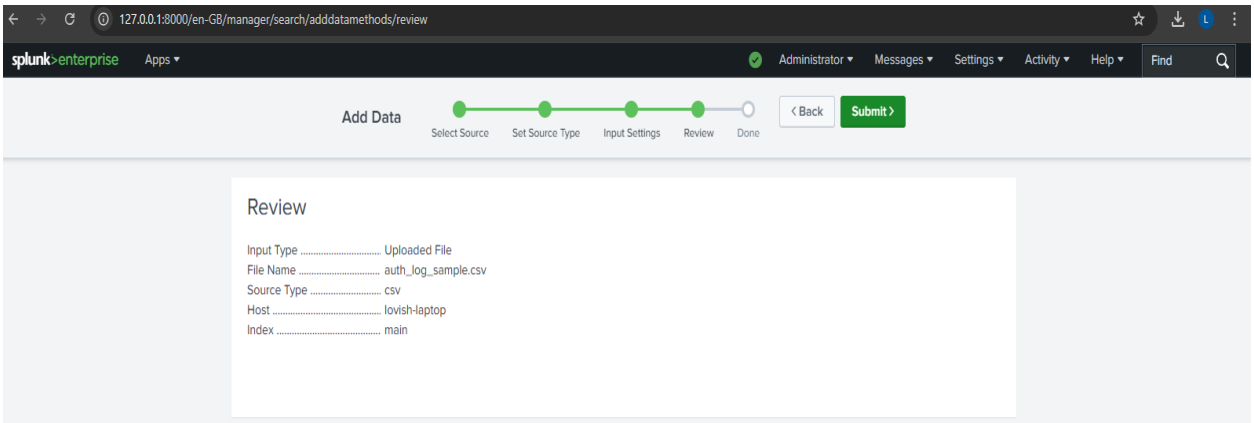
Dataset: auth_log_sample.csv
Sourcetype: csv_auth_logs

Overview:
This part focused on analyzing a structured dataset containing authentication logs in CSV format. Since fields were well-labeled, it allowed for straightforward log exploration using Splunk SPL queries.

Step 1: Uploading the Dataset into Splunk

To begin, I uploaded the structured log file auth_log_sample.csv into Splunk using the **Add Data** feature.

- **Sourcetype:** csv
- **Index:** main
- **Host:** lovish-laptop



Step 2: Querying the Log Data (Top 5 Use Cases)

Question 1: How many total login events are recorded in the log?

index=main sourcetype=csv | stats count as total_events

Total login events found in the dataset using stats count : 150

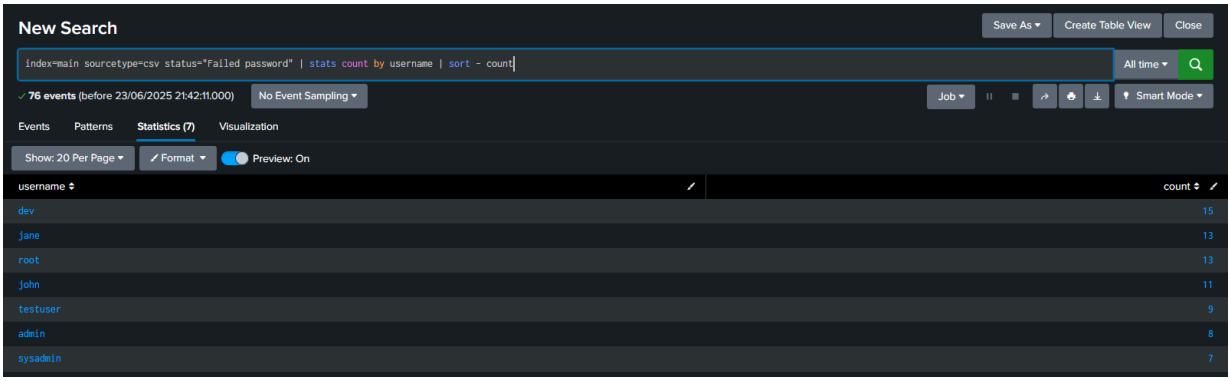
Question 2: What are the top 5 source IP addresses with the most login attempts?

index=main sourcetype=csv | stats count by src_ip | sort - count | head 5

Top 5 IPs with most login attempts detected using stats and sort.

Question 3: Which usernames are most targeted in failed login attempts?

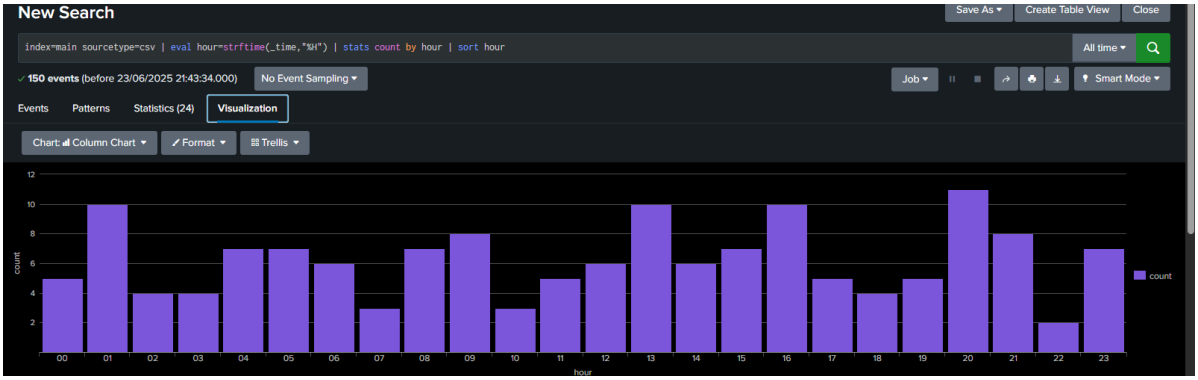
index=main sourcetype=csv status="Failed password" | stats count by username | sort - count



Failed login attempts per username showing possible brute force targets.

Question 4: During which hour were most login attempts made?

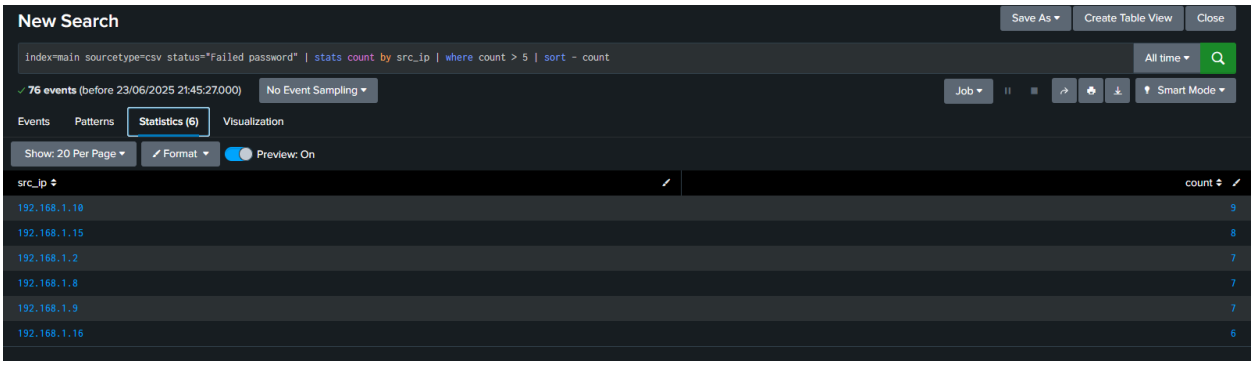
index=main sourcetype=csv | eval hour=strftime(_time,"%H") | stats count by hour | sort hour



Login activity visualized by hour to detect peak attack times.

Question 5: Find all IPs that had more than 5 failed login attempts.

index=main sourcetype=csv status="Failed password" | stats count by src_ip | where count > 5 | sort – count



IPs flagged for brute force behavior due to excessive failed attempts.

Lessons Learned

Working with structured logs made it easier to identify patterns and extract relevant insights. I learned how to use stats, dedup, eval, table, and where to query Splunk data efficiently.