

# Splunk Log Analysis Project – Auth Log Insights

lovish

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

**Dataset:** auth\_log\_sample.csv

**Sourcetype:** csv\_auth\_logs

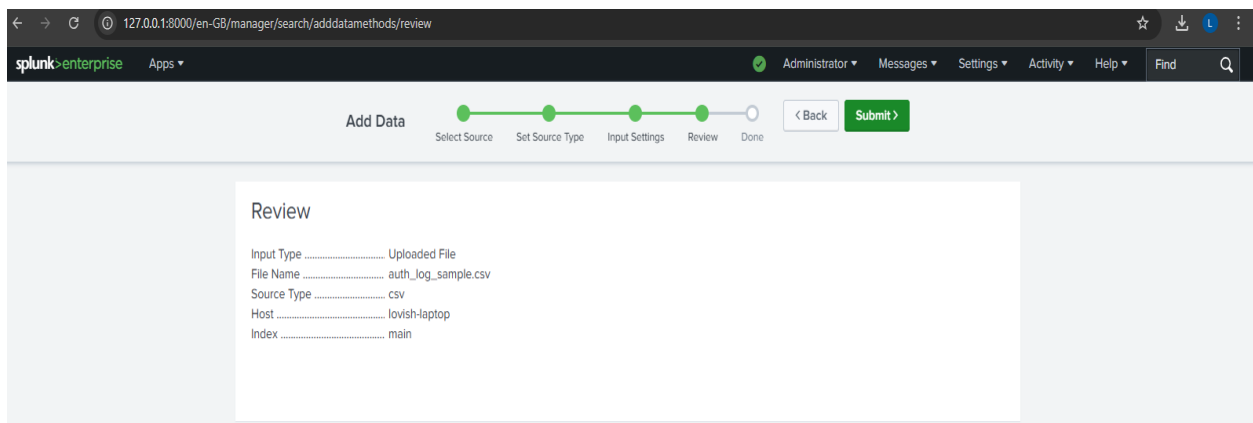
### Overview:

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.

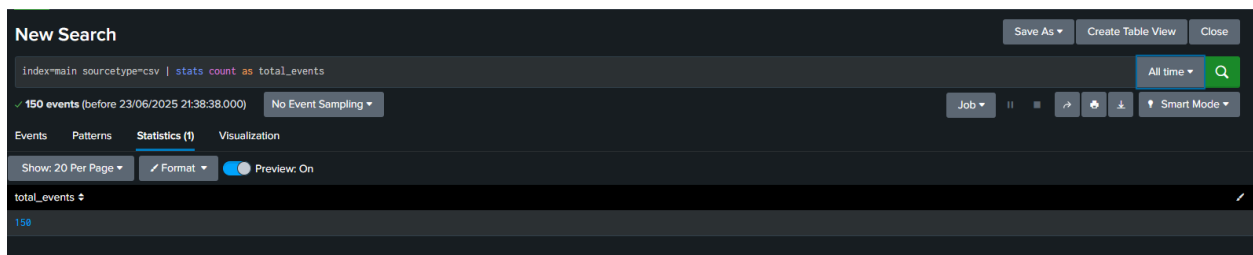
- **Sourcetype:** csv
- **Index:** main
- **Host:** lovish-laptop



### 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

The screenshot shows the Splunk Search interface with the query `index=main sourcetype=csv | stats count by src_ip | sort - count | head 5`. The search results are displayed in a table with 2 columns: `src_ip` and `count`. The results are sorted by count in descending order.

src_ip	count
192.168.1.10	15
192.168.1.2	12
192.168.1.15	11
192.168.1.18	11
192.168.1.6	11

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

The screenshot shows the Splunk Search interface with the query `index=main sourcetype=csv status="Failed password" | stats count by username | sort - count`. The search results are displayed in a table with 2 columns: `username` and `count`. The results are sorted by count in descending order.

username	count
dev	15
jane	13
root	13
john	11
testuser	9
admin	8
sysadmin	7

Failed login attempts per username showing possible brute force targets.

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

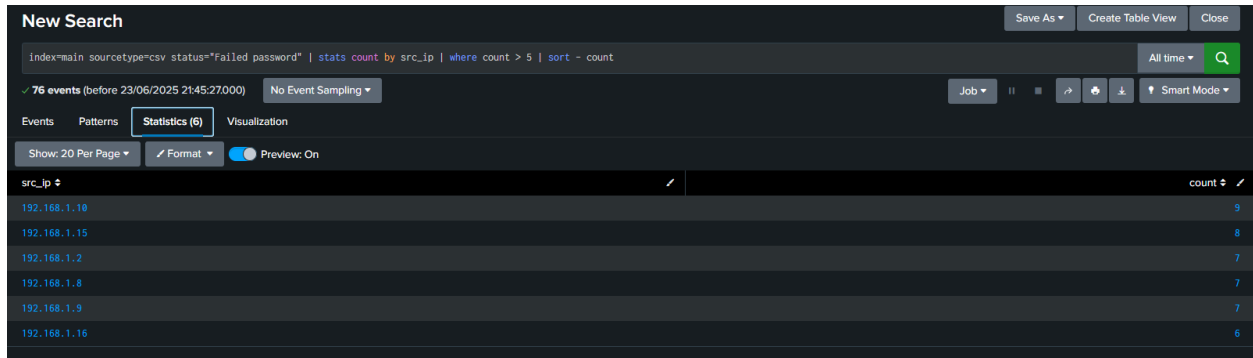
index=main sourcetype=csv | eval hour=strftime(\_time,"%H") | stats count by hour | sort hour



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



The screenshot shows the Splunk search interface with the following details:

- Search Bar:** index=main sourcetype=csv status="Failed password" | stats count by src\_ip | where count > 5 | sort - count
- Results:** 76 events (before 23/06/2025 21:45:27000). No Event Sampling.
- Table View:** Statistics (6) tab is active. The table shows the following data:

src_ip	count
192.168.1.10	9
192.168.1.15	8
192.168.1.2	7
192.168.1.8	7
192.168.1.9	7
192.168.1.16	6

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.