Cyber Security Project:

GitHub Repository: https://github.com/AdarshVL/Cyber\_Security\_Project

# 🔎 Abstract

This project explores the application of Splunk for cybersecurity log analysis, focusing on login events to detect anomalies and suspicious behavior. By ingesting a structured dataset into Splunk, learners gain practical experience in writing Search Processing Language (SPL) queries, visualizing authentication patterns, and interpreting results for security monitoring. The project demonstrates a systematic approach to threat detection through dashboards and data-driven insights.

# 📖 Project Description

This project demonstrates how to ingest, analyze, and visualize log data using Splunk’s Search & Reporting capabilities. We focus on login event data (success/failure) to detect suspicious authentication patterns that could indicate brute-force attempts or targeted attacks.

Objectives:

• Gain hands-on experience with Splunk log ingestion

• Learn SPL (Search Processing Language) queries for event analysis

• Create dashboards for cybersecurity monitoring and insights

• Detect and report anomalies in authentication activity

# 📌 What is this Project About?

This project provides practical exposure to cybersecurity log analysis with Splunk. Students will:   
• Understand how to ingest and structure log data within Splunk  
• Write SPL queries to analyze login events (success/failure)  
• Develop interactive dashboards to visualize authentication trends  
• Detect anomalies and suspicious login behavior  
• Gain insights into the role of log analytics in incident response and SOC workflows

# 🛠️ Methodology

The methodology followed in this project consists of multiple stages:  
  
1. \*\*Data Preparation\*\*: A synthetic dataset (sample.csv) was created containing timestamp, username, IP address, and status.  
2. \*\*Data Ingestion\*\*: Uploaded into Splunk index (bootcamp\_logs) for analysis.  
3. \*\*Exploratory Analysis\*\*: SPL queries applied to understand success/failure distribution, user behavior, and IP activity.  
4. \*\*Visualization\*\*: Queries saved as dashboard panels using Splunk visualizations (pie charts, bar graphs, timecharts).  
5. \*\*Interpretation\*\*: Findings interpreted to highlight potential brute-force attempts and suspicious account activity.  
6. \*\*Documentation\*\*: Queries, screenshots, and analysis recorded in the repository.

# ⚙️ Steps Performed

## 1. Prepare the Dataset

A structured log file (sample.csv) was created with fields:  
- timestamp  
- username  
- ip\_address  
- status (success/failure)  
  
👉 Dataset available in the repository under /dataset folder.

## 2. Upload the Data to Splunk

Steps:  
• Open Splunk Search & Reporting app  
• Navigate: Settings → Add Data → Upload  
• Upload sample.csv  
• Choose source type: CSV  
• Assign to index: bootcamp\_logs

## 3. Run SPL Queries

Queries executed to analyze login patterns.

|  |  |
| --- | --- |
| SPL Query | Purpose / Insight |
| index=bootcamp\_logs | stats count by status | Counts login successes and failures, showing overall authentication trends. |
| index=bootcamp\_logs status=failure | stats count by username | Identifies usernames with repeated failed logins, useful for detecting targeted attacks. |
| index=bootcamp\_logs | stats count by ip\_address, status | Highlights suspicious IP addresses generating multiple failures, indicating brute-force attempts. |
| index=bootcamp\_logs | timechart count by status | Visualizes login trends over time to detect anomalies in authentication patterns. |

👉 All queries are documented in /queries/spl\_queries.txt

## 4. Build Dashboard Panels

Dashboard titled “Login Analysis” created with panels:  
- Pie Chart: Success vs Failure distribution  
- Bar Graph: Failed logins by username  
- Timechart: Login attempts over time  
  
👉 Screenshots available in /screenshots folder.

## 5. Interpret & Present Findings

Findings from the dashboard:  
• High number of failed logins from a single IP → Possible brute-force attack  
• Certain usernames showed repeated failures → Targeted attacks suspected  
• Login success/failure patterns over time revealed anomalies compared to baseline activity  
• Normal login activity helped distinguish false positives from true incidents

# 🌐 Significance & Applications

This project mirrors real-world SOC operations where log analysis is critical for detecting cyber threats. It provides a foundation for:  
• Security Monitoring & Threat Detection  
• Incident Response (detecting compromised accounts)  
• Compliance & Audit Reporting  
• Building hands-on skills in SIEM tools (Splunk)

# 📑 Final Report

A detailed report with dataset, queries, analysis, and dashboard screenshots is included in /report folder.

# 💡 Tips for Learners

• Start with clean, structured data

• Explore your fields before writing queries

• Begin with simple SPL queries, then move to advanced

• Focus on security insights, not just visuals

• Document queries and findings properly

# 🚀 Tech Stack & Tools

• Splunk Enterprise / Splunk Cloud

• SPL (Search Processing Language)

• Dataset: Structured CSV logs

# 📂 Repository Contents

• dataset/ → Sample log dataset

• queries/ → All SPL queries with explanations

• screenshots/ → Dashboard & panel images

• report/ → Final project report (PDF)

# 🔮 Conclusion & Future Scope

This project successfully applied Splunk to analyze login event data for cybersecurity monitoring. Dashboards provided real-time insights into authentication patterns, anomalies, and potential threats. The knowledge gained can be extended to:  
• Monitoring larger, real-world datasets from enterprise environments  
• Incorporating machine learning for anomaly detection  
• Expanding log sources (firewalls, servers, applications)  
• Automating alerts and incident response workflows  
Overall, the project bridges theoretical cybersecurity concepts with hands-on SIEM practice.