Brute Force Attack Detection using Splunk SIEM

Prepared By: Syed Bilal Faiz

Role: SOC Analyst Intern (Student) — Ubuntu / Splunk Enterprise

Date: 16 October 2025

Abstract

This project demonstrates detection and analysis of brute-force login attempts by monitoring Windows Security logs (Event ID 4625) using Splunk Enterprise on Ubuntu. The document is prepared as a professional project summary for presentation in interviews or academic review.

Objective

Detect and alert on multiple failed login attempts to identify potential brute-force attacks and demonstrate SOC analyst workflow using Splunk.

Component	Details
Operating System	Ubuntu 22.04 LTS
SIEM Platform	Splunk Enterprise
Log Source	Windows Security Logs (Event ID 4625) - Sample CSV included
Dataset	windows_failed_logins.csv
Role	SOC Analyst Intern (Student)

Implementation Procedure (Concise)

1. Install Splunk Enterprise on Ubuntu and start Splunk Web (http://localhost:8000).
2. Add Data → Upload 'windows_failed_logins.csv' → set Index = 'windows_logs'.
3. Run the detection query (see below) and verify results.
4. Save the search as an alert with trigger: Number of Results > 0 and configure notification.
5. Document findings and recommended remediation steps.

Detection Query (Splunk SPL)

Use the following SPL to detect accounts/IPs with more than 5 failed login attempts:

```
index=windows_logs EventCode=4625 | stats count by Account_Name, IpAddress | where count > 5
```

Alert Configuration (Concise)

Save the search as 'Brute Force Detection Alert'. Trigger when Number of Results > 0. Action: send email or webhook to SOC channel. Schedule: every 5 minutes (adjust per environment).

Example Results & Analysis

Sample output shows Account_Name and IpAddress with count. Example: admin from 192.168.1.15 (5 attempts) — indicates potential brute-force. Correlate with firewall and endpoint logs before blocking or taking containment actions.

Conclusion

This concise project demonstrates essential SOC tasks: log ingestion, detection, alerting, and basic analysis. It is suitable for inclusion in a professional portfolio or to present during interviews.

Prepared by: Syed Bilal Faiz

Date: 16 October 2025