# INCIDENT REPORT

(SOC Analyst Mini Project – Incident Report)

Date: 2025-08-01
Analyst Name: Ajay Ibrahim
Alert Title: Brute Force Login Attempt Detected
Alert Source: Splunk SIEM

## Incident Summary

On August 1st, 2025, Splunk triggered a scheduled alert for multiple failed login attempts from a single IP address (192.168.1.200). The alert was based on a brute-force detection rule: More than 5 failed logins within a short time window.

## Log Evidence

Here are the relevant entries:

| Timestamp | IP Address | Username | Status |
|---|---|---|---|
| 10:15:00 | 192.168.1.200 | user1 | Failed |
| 10:15:01 | 192.168.1.200 | user1 | Failed |
| 10:15:02 | 192.168.1.200 | user1 | Failed |
| 10:15:03 | 192.168.1.200 | user1 | Failed |
| 10:15:04 | 192.168.1.200 | user1 | Failed |
| 10:16:10 | 192.168.1.200 | user2 | Failed |

These logs were detected from the Splunk lookup file brute_force_log.csv.

## Analysis

Repeated failed login attempts from the same IP

Attempted with two different usernames

Typical pattern of automated brute-force attack

## Action Taken

Alert triggered in Splunk (stored under “Triggered Alerts”)

IP address 192.168.1.200 flagged for investigation

Recommendation: Block IP and escalate if seen again

## Tools Used

| Tool | Purpose |
|---|---|
| Splunk | Log monitoring, alerting, dashboard |
| Lookup CSV | Simulated log source |

## Conclusion

This incident demonstrates the ability to detect brute-force attacks using Splunk SIEM. By building a custom alert, the system can automatically identify high-risk behavior based on failed login patterns.