Splunk Bank Monitoring Project, Final Report

Author: Winnie Mango
Date: 23/11/2025
Project Type: Banking Log Analysis & Security Dashboard

---

1. Objective

This project aims to analyze simulated banking logs to identify security-related activities, including:

- Failed login attempts
- High-value transactions
- Suspicious IP activity
- Most active users

This shows practical skills in Splunk, SPL queries, dashboard creation, and monitoring banking cybersecurity.

---

2. Dataset

File: bank_logs.csv

Format: CSV

Columns: timestamp, user, action, amount, IP, status, account_number

Total Events: 21

Users: 8

> All events were ingested into Splunk successfully, as confirmed by the search query: source="bank_logs.csv"

---

3. SPL Queries Used

All queries used in the project:

```
index=main action="login_failed" | timechart count
index=main action="login" | stats count by user | sort -count
index=main action="transaction" amount>10000 | timechart sum(amount)
index=main action="login" | stats count by user, ip_address | where count>5
source="bank_logs.csv"
index=main OR index=default | head 20
```

> These queries capture failed logins, active users, high-value transactions, suspicious IP activity, and data verification.

---

4. Dashboard Overview

The project includes a Splunk dashboard to visualize the following panels:

1. Full Dashboard Overview
2. Failed Login Trend
3. Most Active Users
4. High-Value Transactions
5. Suspicious IP Activity
6. Search Tab — SPL Queries
7. Data Verification

> Screenshots of all panels are available in the GitHub repository:
Winnie cyber portfolio/splunk-bank-monitoring-project/dashboard-screenshots/

---

5. Analysis / Observations

Failed Logins: Four users attempted logins that failed, totaling eight failed attempts.

Most Active Users: Activity is spread across eight users.

High-Value Transactions: No transactions were over 10,000 during the dataset period.

Suspicious IP Activity: No users hit the suspicious IP threshold (more than five logins per IP).

Data Verification: All events were correctly ingested from bank_logs.csv.

> The dataset shows no fraudulent activity, but the dashboard and queries are ready to monitor live banking logs.

---

6. Conclusion

This project shows the ability to:

- Ingest banking logs into Splunk
- Run SPL queries for security monitoring
- Build dashboards to visualize key activities
- Detect anomalies or suspicious activity (even if none occurred)
- Document findings clearly for banking environments

> The setup can be extended to support real-time monitoring and larger datasets for complete SOC operations.