SQL Investigation Project

Mike Thomas

Cybersecurity Analyst

Date: July 1, 2025

Executive Summary

This investigation analyzed 50 user login records to identify suspicious activity. Key findings included multiple failed login attempts by several users, logins from unusual geographic locations, and irregular login times outside of standard working hours. These patterns indicate a potential risk of unauthorized access. Recommended actions include enabling multi-factor authentication, implementing account lockouts after repeated failures, and closely monitoring access from non-US IP addresses.

SQL Investigation Project

Scenario

A small organization suspected suspicious login activity. As the security analyst, you were tasked with investigating login records to detect potential security threats, including multiple failed logins, logins from unusual locations, and irregular login times.

Objectives

- Identify users with multiple failed login attempts.
- Detect logins from unusual (non-US) locations.
- Find users logging in at irregular hours.

Methodology

Using SQL, the login_records table was analyzed. Three key queries were executed to identify potential threats:

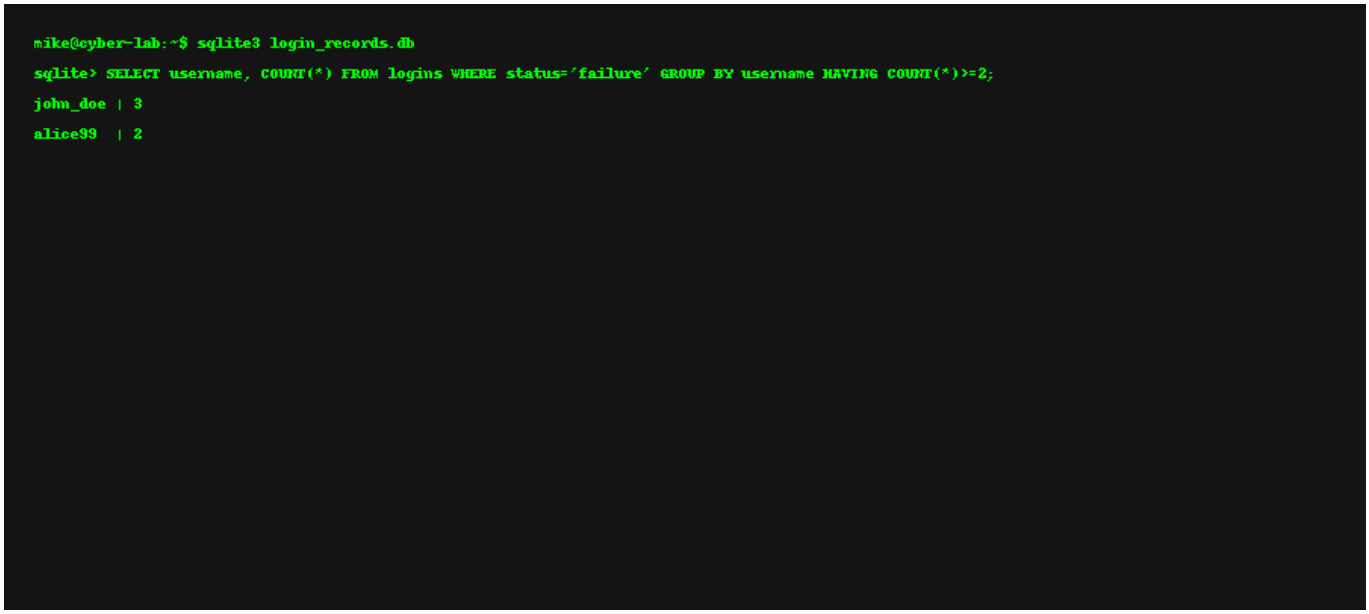
1. Failed login attempts by user.
2. Logins from unusual (non-US) locations.
3. Logins at irregular hours (before 6 AM or after 10 PM).

Annotated Query Example

```
-- This query finds users with 2 or more failed login attempts
SELECT username, COUNT(*) as failed_attempts
FROM logins
WHERE status = 'failure'
GROUP BY username
HAVING failed_attempts >= 2;
```

Terminal Screenshots

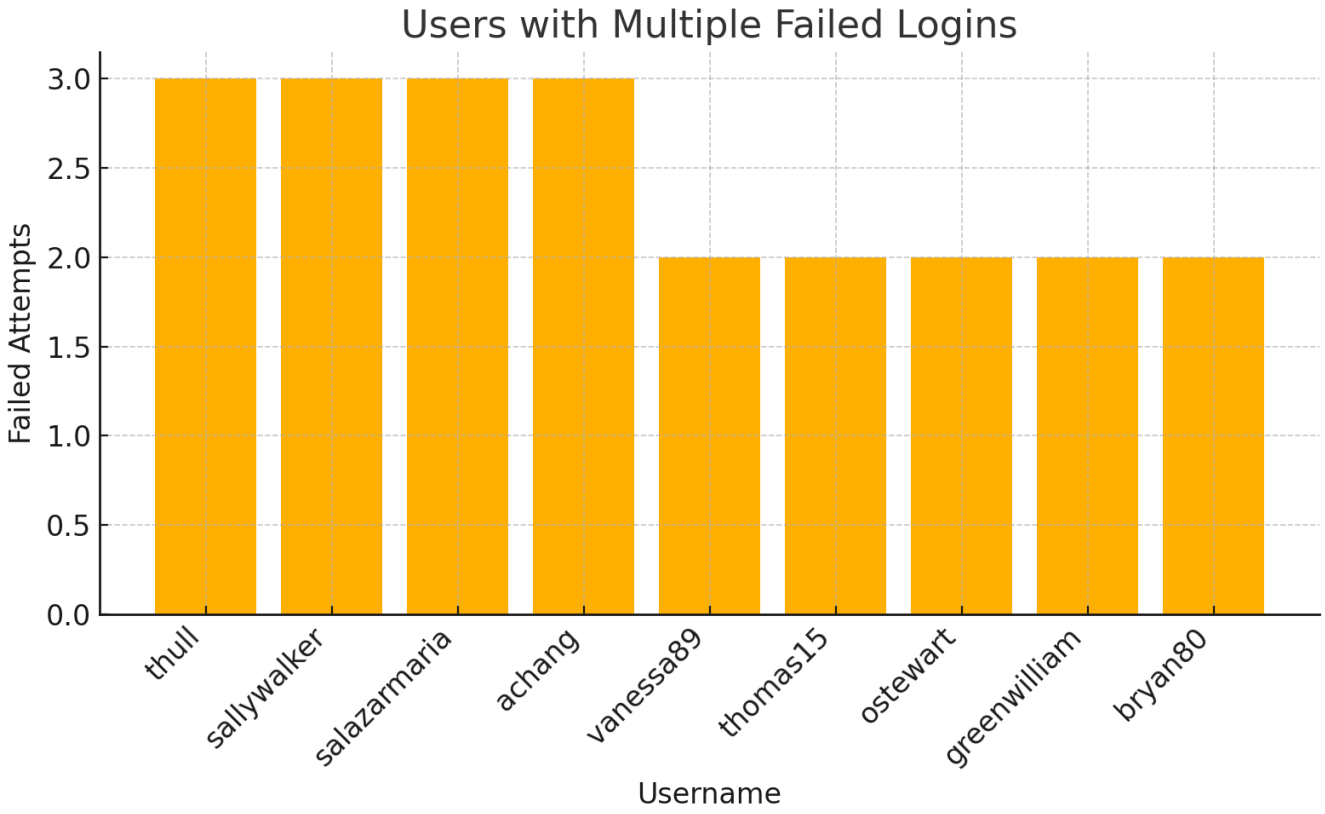
The following screenshots show the queries being executed in a Linux terminal to validate results.



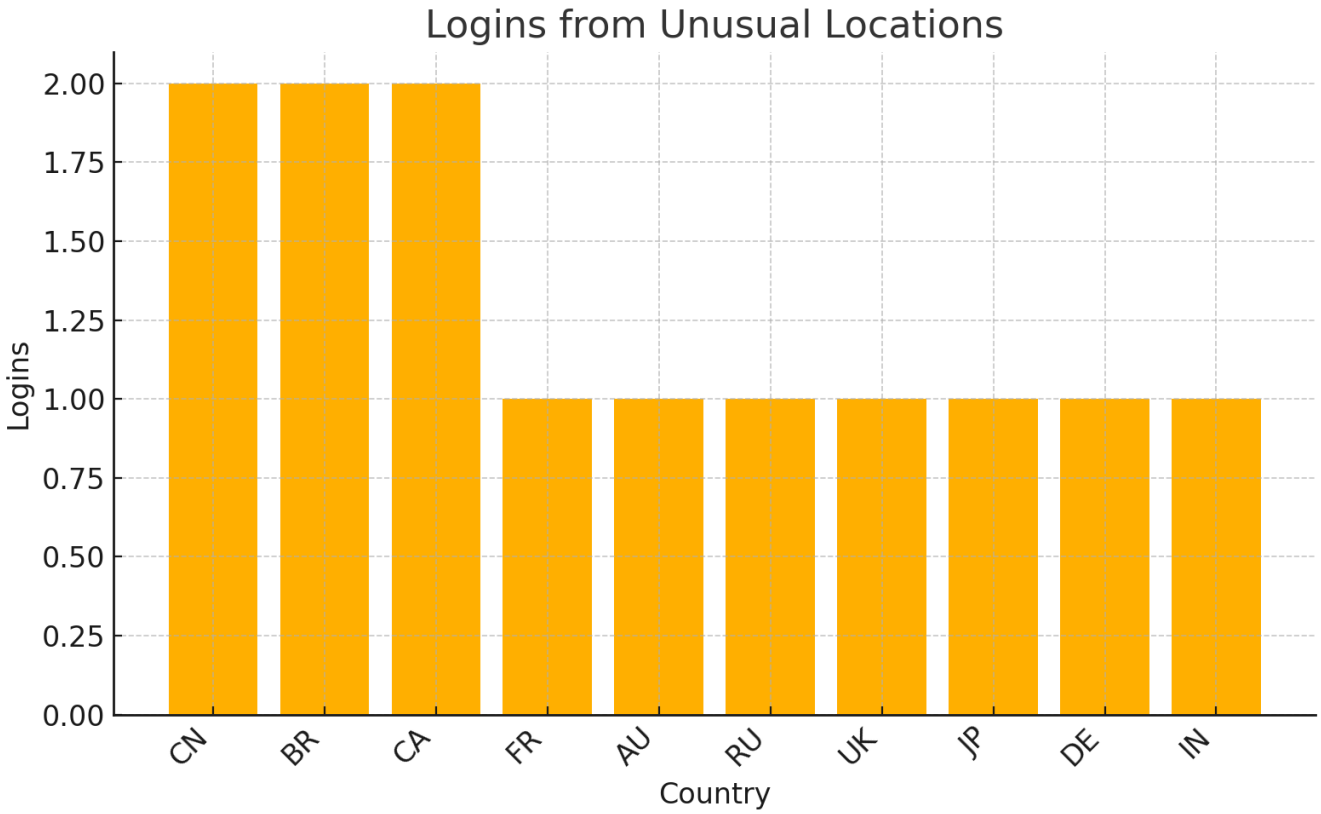
Findings

The following charts summarize the investigation results:

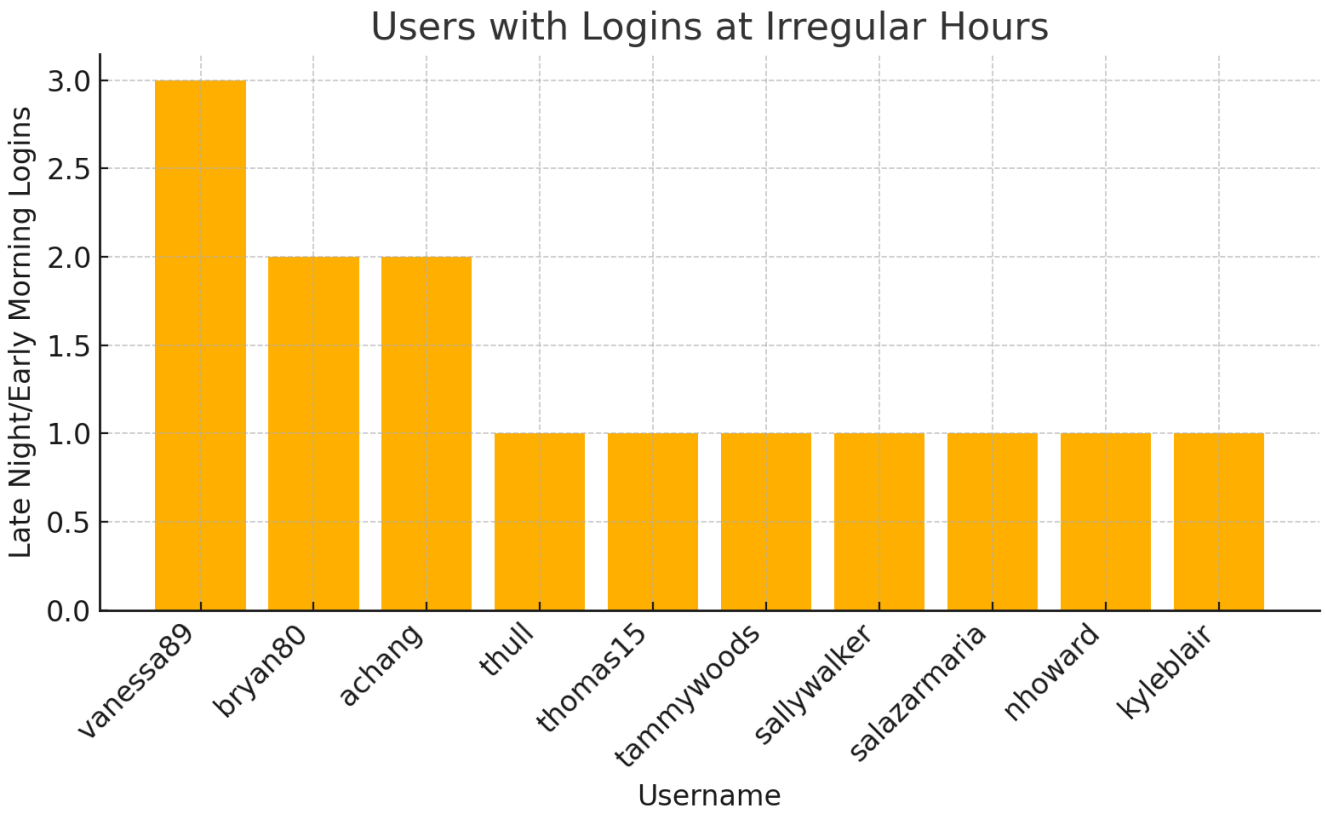
1. Users with Multiple Failed Logins



2. Logins from Unusual Locations



3. Users with Logins at Irregular Hours



Recommendations

- Implement account lockout after multiple failed login attempts.

- Enable multi-factor authentication for all users.

- Review and restrict access from foreign or unusual IP addresses.

- Monitor and alert on logins during non-business hours.

All findings are based on the analysis of 50 login records from the organization's authentication system.

Project files (dataset, SQL scripts, and visuals) are available in the GitHub repository:

https://github.com/mikexthomas/sql-investigation-project