Project Title: Splunk Windows Security Monitoring
Author: Lokeshwar V
Date: July 2025

📑 Table of Contents

1️⃣ Introduction

This project demonstrates how to use Splunk Enterprise to monitor Windows Security logs for login activities. The goal is to visualize security events and set up automated alerts for suspicious failed login attempts.

2️⃣ Objectives

- Understand how Splunk collects and indexes Windows Security logs.
- Build a dashboard to monitor login activities.
- Identify failed login attempts, successful logins, and account lockouts.
- Configure email alerts to notify an administrator about failed logins.

3️⃣ Tools Used

- Splunk Enterprise (Free Trial)
- Windows Security Event Logs
- Gmail SMTP for email notifications

4️⃣ Dataset

This project uses the Windows Security Event Log:

- **EventCode 4625**: Failed Login Attempt
- **EventCode 4624**: Successful Login
- **EventCode 4740**: Account Lockout

5️⃣ SPL Queries Used

Failed Login Attempts:

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
| sort - count
```

Successful Login Attempts:

```
index=main sourcetype=WinEventLog:Security EventCode=4624
| stats count by Account_Name, host
| sort - count
```

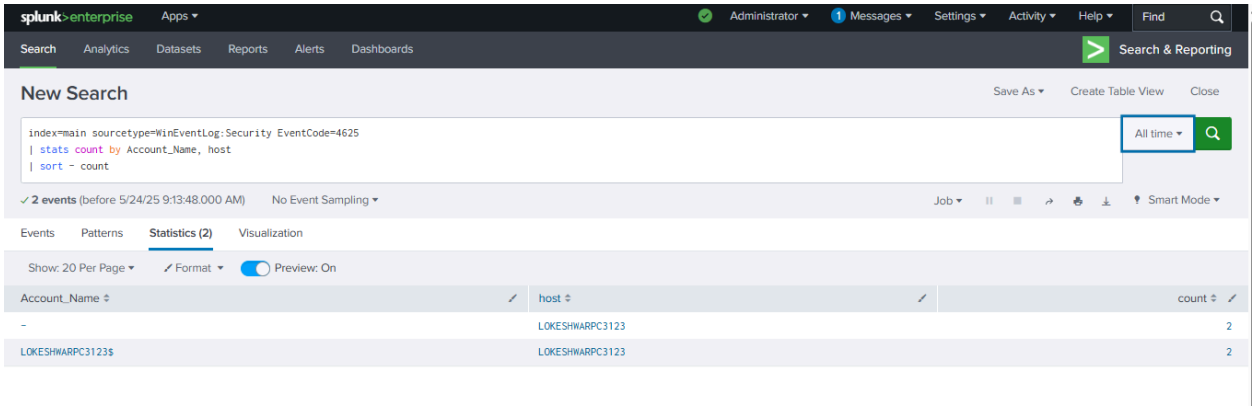
Account Lockouts:

```
index=main sourcetype=winEventlog:Security EventCode=4740
| stats count by Account_name, host
```

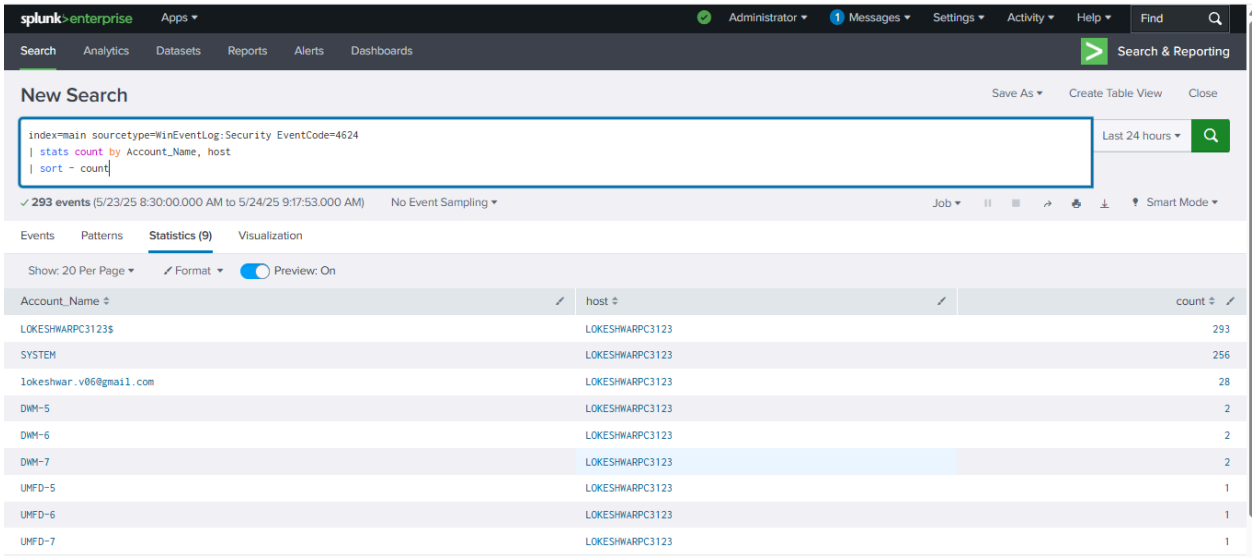
6️⃣ Dashboard Panels

The Splunk dashboard includes three panels:

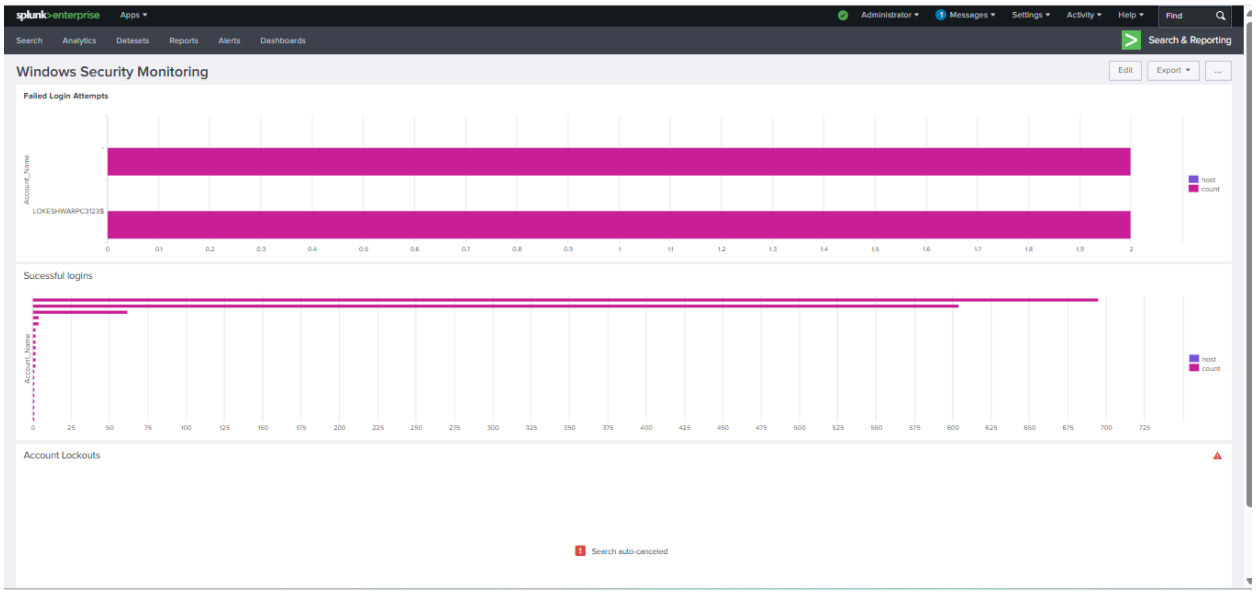
📊 1. Failed Login Attempts



📊 2. Successful Logins



3. Account Lockouts

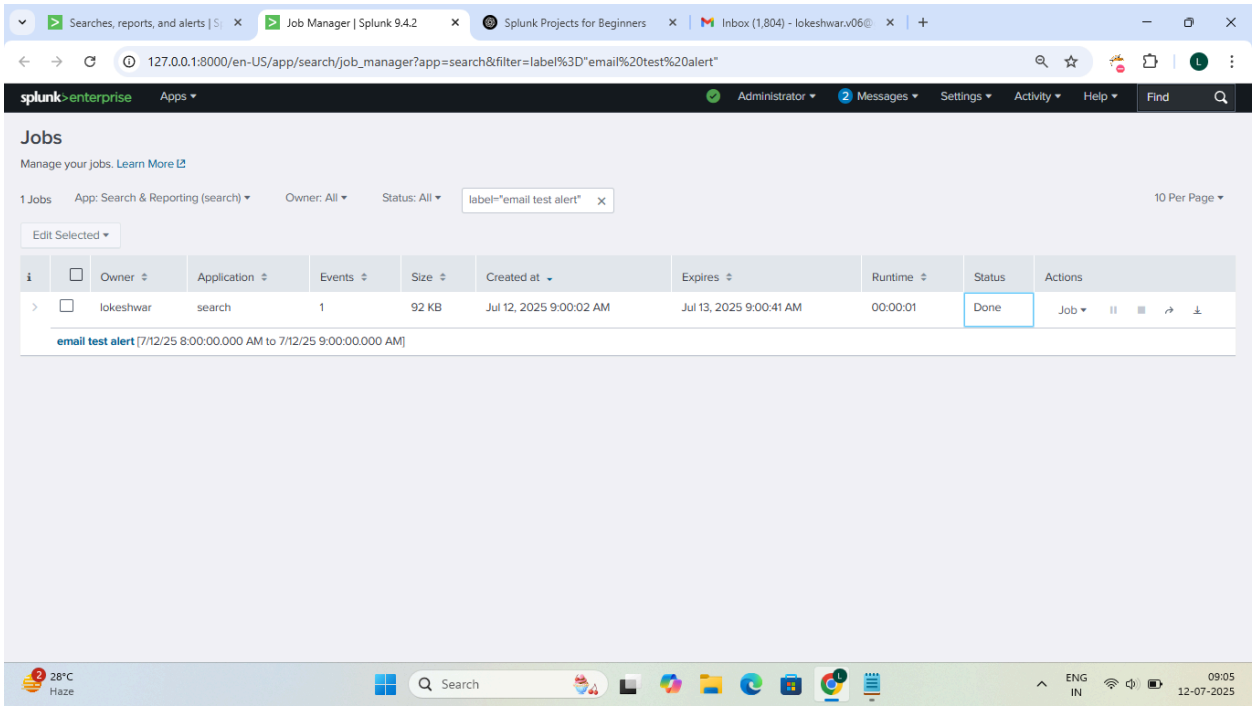


7 Alerts & Notifications

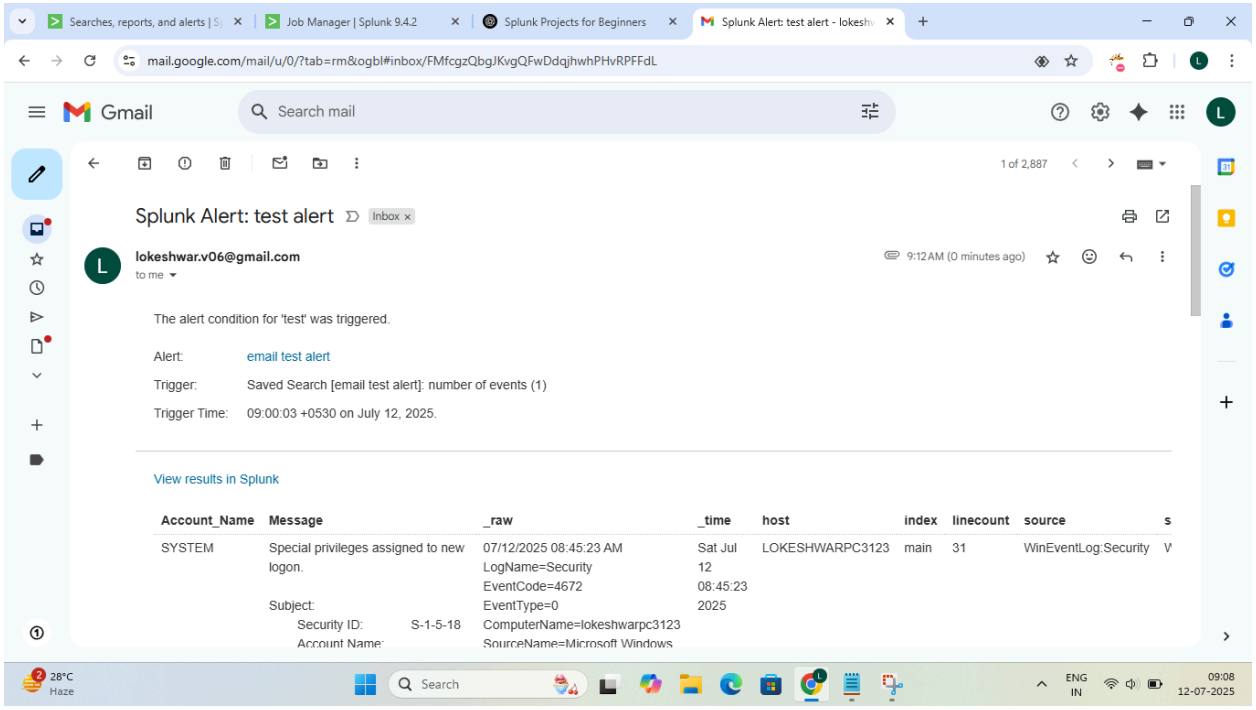
An alert was configured to detect failed login attempts and send an email notification when the condition is met.

- **Alert Type:** Scheduled Search
- **Trigger Condition:** Results greater than 0
- **Action:** Send Email
- **Email:** Configured via Gmail SMTP with App Password

Triggered Alert Example



Email Notification Example



8 Conclusion

This beginner-level Splunk project demonstrates how to:

- Set up SPL queries for Windows Security monitoring.
- Build a useful security dashboard.
- Configure alerts with automated email notifications.

The project can be improved further by adding more event types, advanced correlations, or integrating with other monitoring tools for real-world security monitoring.

End of Report