**Splunk Alert Project: Detecting Failed Logins on Windows Server**

1. **Project Overview**

This project demonstrates how to create and trigger a security alert in Splunk Enterprise using data collected from a Windows Server via the Splunk Universal Forwarder. The alert identifies multiple failed login attempts (Event ID 4625), which can be indicative of brute-force attacks or unauthorized access attempts.

1. **Architecture & Setup**

• Splunk Universal Forwarder installed on Windows Server.  
• Splunk Enterprise installed on Host PC.  
• Forwarder configured to send Windows Security logs to Splunk Enterprise.  
• Data indexed under 'main' index with sourcetype 'WinEventLog:Security'.

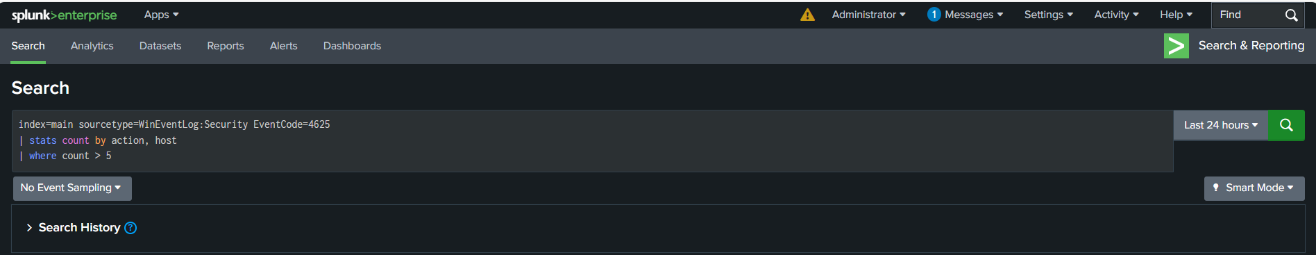
1. **Objective**

Trigger an alert when more than 5 failed login attempts (EventCode 4625) occur within a 10-minute window.

1. **Splunk Search Query**

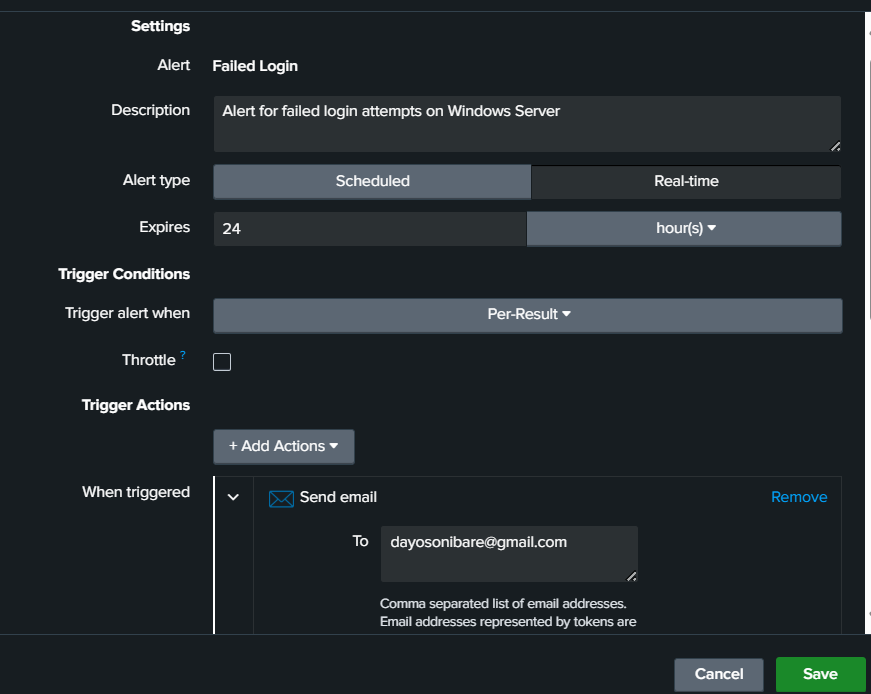
The following SPL query was used to detect failed login attempts:

***index=main sourcetype=WinEventLog:Security EventCode=4625  
| stats count by action, host  
| where count > 5***

******

1. **Alert Configuration**

• Title: Failed Logins Alert  
• Type: Scheduled Alert (Every 10 minutes)  
• Time Range: Last 10 minutes  
• Trigger Condition: Number of results > 0  
• Trigger Actions: Send Email (Configured via SMTP in Splunk Settings)

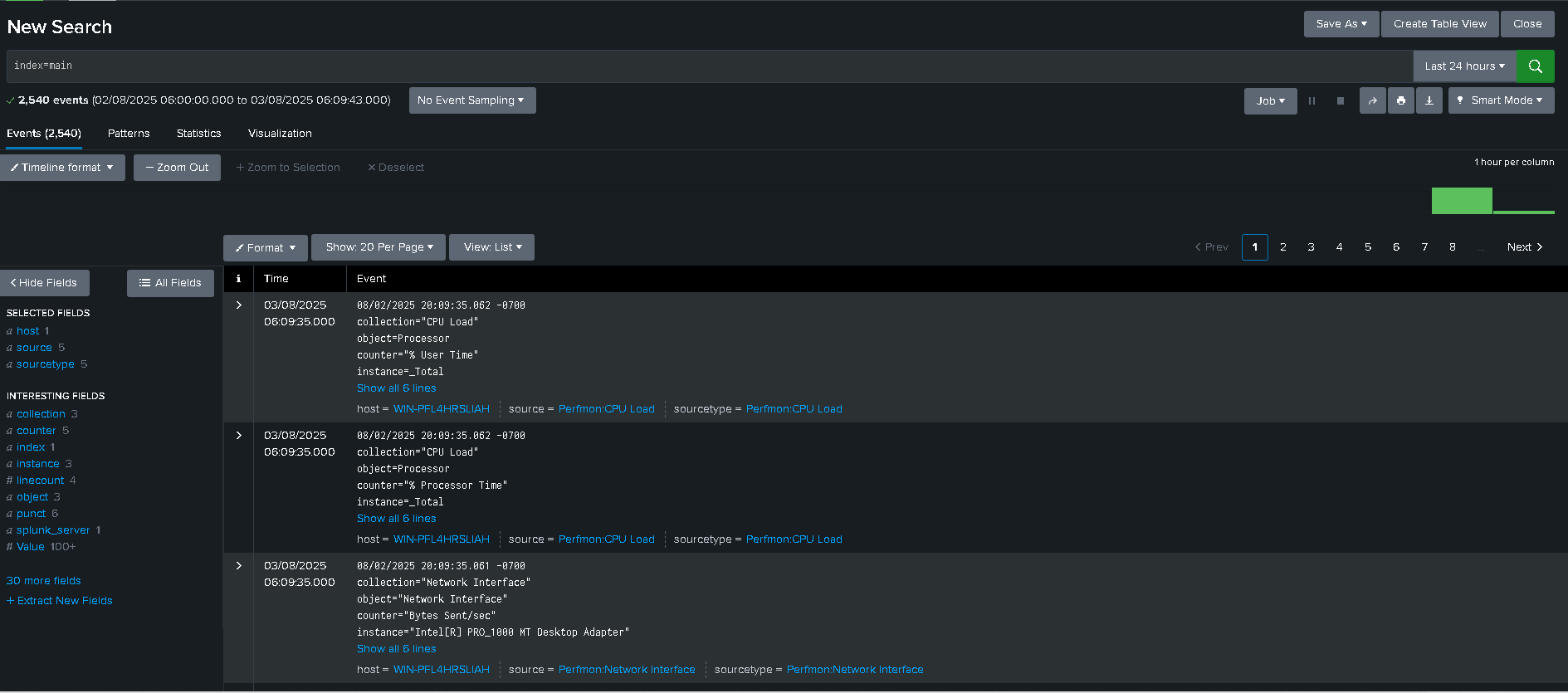


1. **Simulating the Alert**

To simulate real-world conditions, failed login attempts were manually triggered on the Windows Server using the `runas` command with incorrect credentials. This ensured multiple Event ID 4625 logs were generated and forwarded to Splunk for processing.

1. **Validation & Output**

The alert was successfully triggered after 6 failed login attempts. It appeared in the 'Triggered Alerts' section of Splunk, and an email notification was received, confirming successful detection and response.



1. **Conclusion**

This project demonstrates the practical use of Splunk for real-time log monitoring and alerting.