

# Splunk Alert Project: Detecting Failed Logins on Windows Server

## 1. Project Overview

This project demonstrates the creation and testing of a **security alert in Splunk Enterprise** using Windows Security Event Logs collected from a Windows Server through the **Splunk Universal Forwarder**. The alert focuses on detecting **multiple failed authentication attempts (Event ID 4625)**, which may indicate brute-force attacks, credential misuse, or unauthorized access attempts.

---

## 2. Architecture & Setup

The environment was configured as follows:

- **Splunk Universal Forwarder** installed on the Windows Server
- **Splunk Enterprise** installed on the host machine
- Windows Security Event Logs forwarded to Splunk Enterprise
- Logs indexed in the **main** index
- Log source type configured as **WinEventLog:Security**

This setup ensures centralized log collection and real-time visibility into authentication-related events.

---

## 3. Objective

The primary objective of this project is to **trigger a security alert when more than five failed login attempts occur within a 10-minute time window**, enabling early detection of suspicious authentication behavior.

---

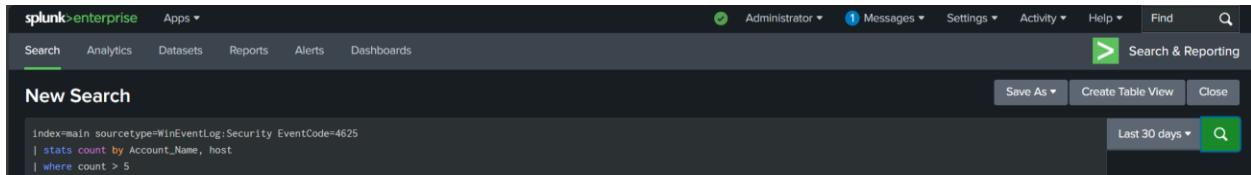
## 4. Splunk Search Query

The following SPL query was used to identify repeated failed login attempts:

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

This query aggregates failed login events by user account and host, triggering an alert when the defined threshold is exceeded.

**Note:** The alert time range in Splunk was configured to run over a **10-minute window** to meet the project objective.



The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise' and various dropdown menus like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a search bar with a green 'Search & Reporting' button. The main area is titled 'New Search' and contains the following search command:

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

Below the search command are buttons for 'Save As', 'Create Table View', and 'Close'. A time range selector shows 'Last 30 days' with a dropdown arrow, and a green search icon.

## 5. 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)

Save As Alert X

**Settings**

Title: failed login attempt

Description: Optional

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Expires: 24 hour(s) ▾

**Trigger Conditions**

Trigger alert when: Per-Result ▾

Throttle:

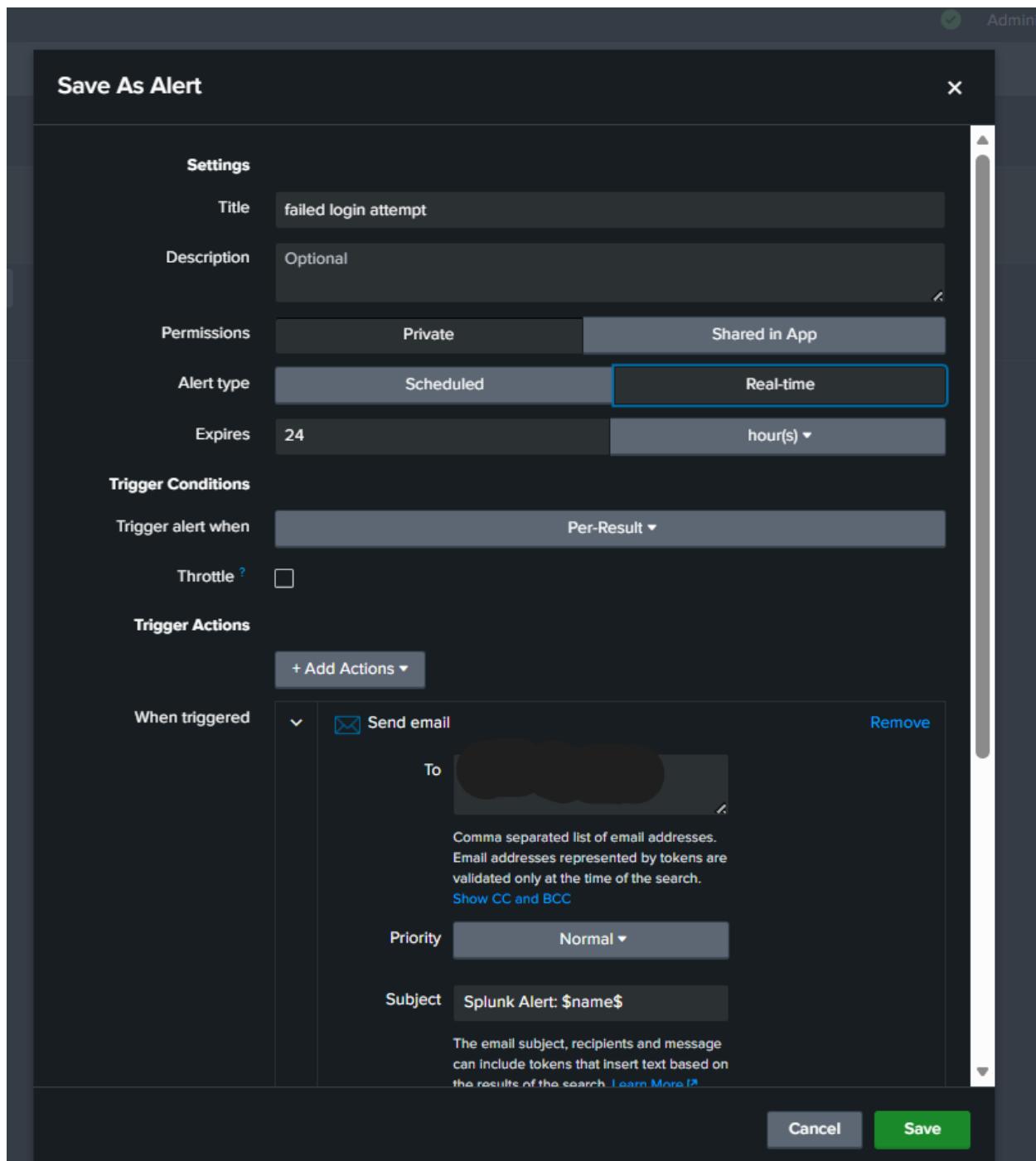
**Trigger Actions**

+ Add Actions ▾

When triggered:

<input type="button" value="Send email"/>	To: [REDACTED]	Remove
Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. <a href="#">Show CC and BCC</a>		
Priority: Normal ▾		
Subject: Splunk Alert: \$name\$ <small>The email subject, recipients and message can include tokens that insert text based on the results of the search. <a href="#">Learn More</a> ?</small>		

Cancel Save



## 6. 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.

## **7. 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.