

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.

2. 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'.

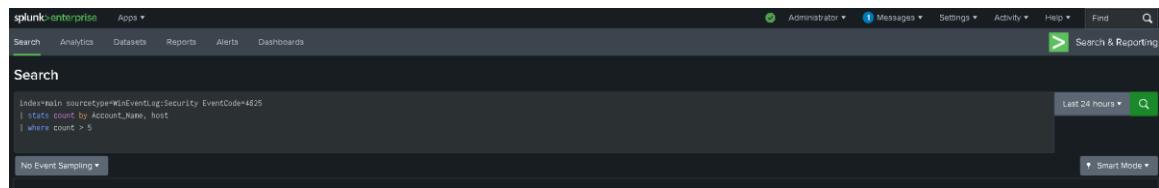
3. Objective

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

4. Splunk Search Query

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

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



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)

Settings

Alert Failed login alert

Description Alert for failed login attempts on Windows Server

Alert type Scheduled Real-time

Expires 24 hour(s) ▾

Trigger Conditions

Trigger alert when Per-Result ▾

Throttle ?

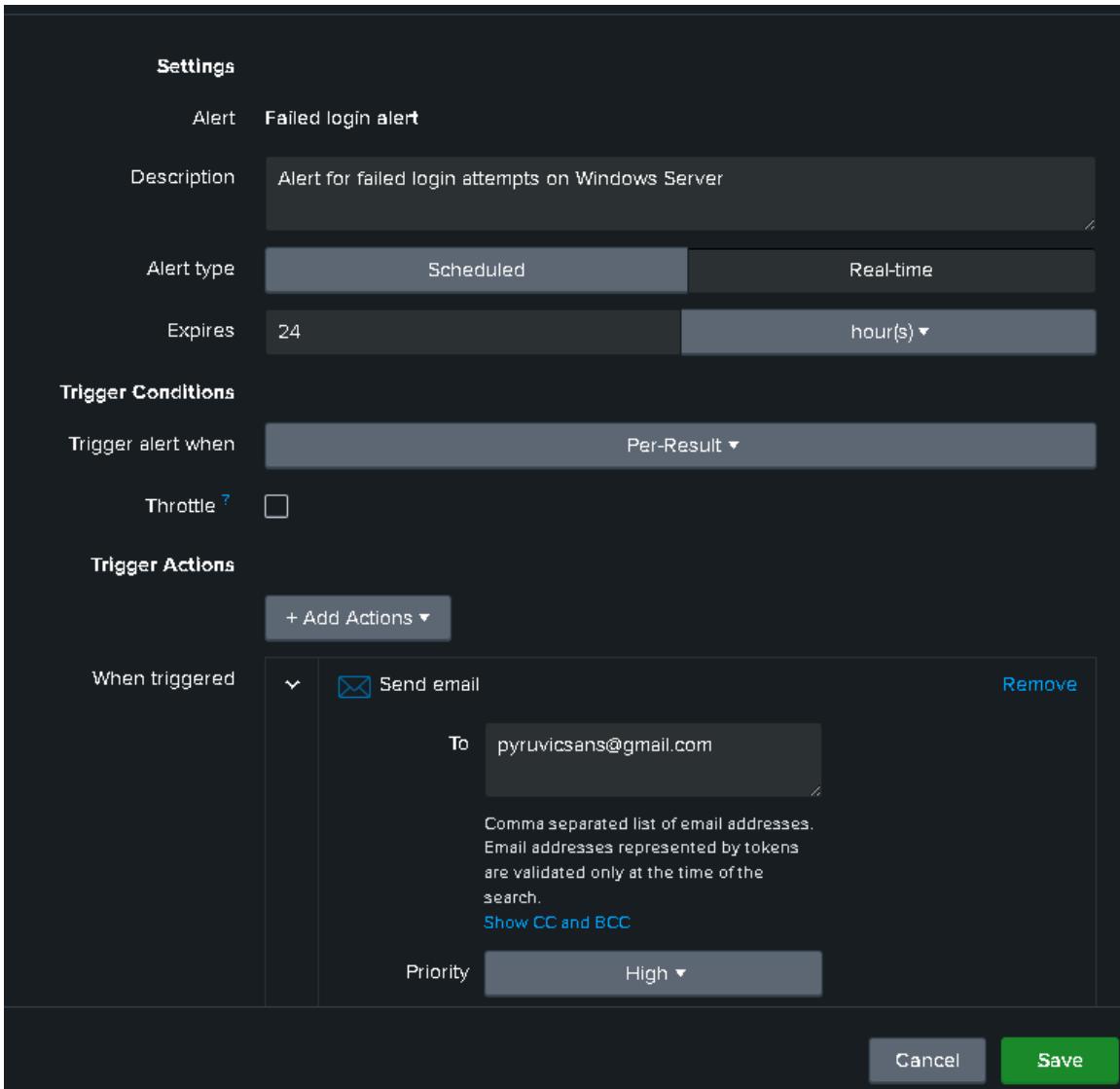
Trigger Actions

+ Add Actions ▾

When triggered	Action	Details	Remove
	Send email	To pyruvicsans@gmail.com Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. Show CC and BCC	Remove

Priority High ▾

Cancel **Save**



The screenshot shows the 'Settings' page for a Splunk alert named 'Failed login alert'. The alert is described as 'Alert for failed login attempts on Windows Server'. It is set to 'Scheduled' mode and expires after 24 hours. The trigger condition is set to 'Per-Result'. There is an unchecked checkbox for 'Throttle'. Under 'Trigger Actions', there is one entry: 'Send email' to the address 'pyruvicsans@gmail.com'. A note below the 'To' field specifies that commas separate email addresses and that validation occurs at search time. The priority is set to 'High'. At the bottom, there are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** Shows "New Search" and a date range from "02/08/2025 06:00:00.000" to "03/09/2025 06:09:43.000".
- Toolbar:** Includes "Save As", "Create Table View", "Close", "Last 24 hours", "Job", "Smart Mode", and a search icon.
- Event List:**
 - Event 1:** Time: 03/09/2025 06:09:35.000, Event: collection="CPU Load" object="Processor" counter="User Time" instance="Total" host = WIN-PRUERSUAH | source = Perfmon\CPU Load | sourcetype = Perfmon\CPU Load
 - Event 2:** Time: 03/09/2025 06:09:35.000, Event: collection="CPU Load" object="Processor" counter="Processor Time" instance="Total" host = WIN-PRUERSUAH | source = Perfmon\CPU Load | sourcetype = Perfmon\CPU Load
 - Event 3:** Time: 03/09/2025 06:09:35.000, Event: collection="Network Interface" object="NtwinN Interface" counter="Bytes Sent/sec" instance="Intel[R] PRO_1000 MT Desktop Adapter" host = WIN-PRUERSUAH | source = Perfmon\Network Interface | sourcetype = Perfmon\Network Interface
- Left Panel:** Shows "SELECTED FIELDS" (host, collection, object, counter, instance) and "INTERESTING FIELDS" (collection, object, counter, instance, punct, value, splunk_server).
- Bottom:** Navigation buttons for "Format", "Show 20 Per Page", "View List", and page numbers 1 through 8.

8. Conclusion

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