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'.

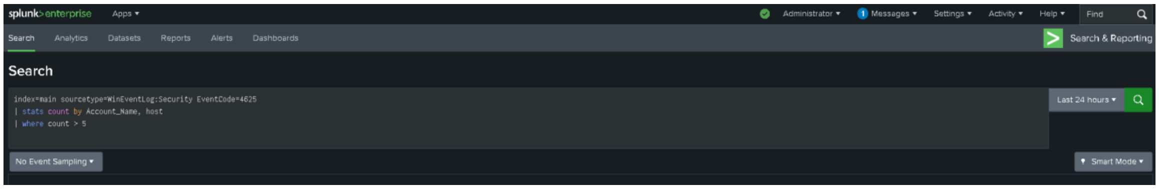
3. Objective

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:

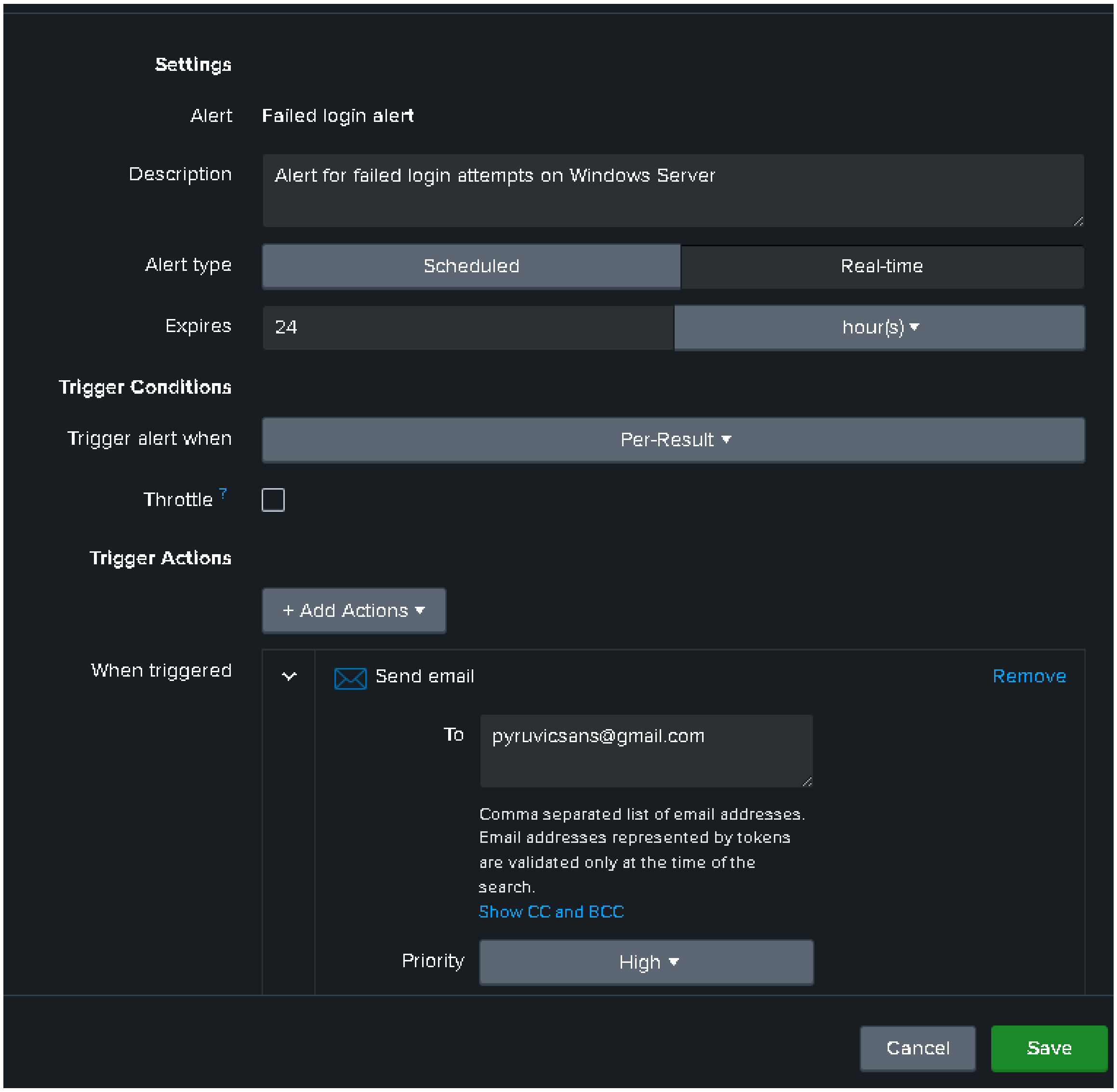
index=main sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
| where count > 5



```
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: Send email — Remove

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

Priority: High ▾

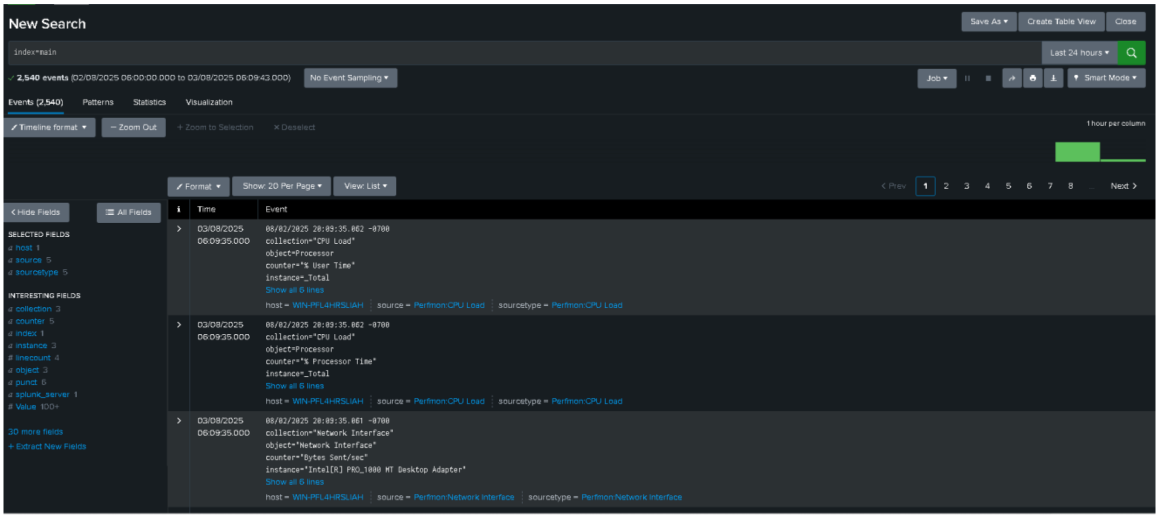
Cancel Save

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.



```
index=main
```

✓ 2,540 events (02/08/2025 06:00:00.000 to 03/08/2025 06:09:43.000)

SELECTED FIELDS
a host 1
a source 5
a sourcetype 5

INTERESTING FIELDS
a collection 3
a counter 5
a index 1
a instance 3
# linecount 4
a object 3
a punct 6
a splunk_server 1
Value 100+

30 more fields
+ Extract New Fields

```
i  Time         Event
>  03/08/2025   08/02/2025 20:09:35.062 -0700
   06:09:35.000 collection="CPU Load"
                object=Processor
                counter="% User Time"
                instance=_Total
                Show all 6 lines
                host = WIN-PFL4HRSLIAH | source = Perfmon:CPU Load | sourcetype = Perfmon:CPU Load
>  03/08/2025   08/02/2025 20:09:35.062 -0700
   06:09:35.000 collection="CPU Load"
                object=Processor
                counter="% Processor Time"
                instance=_Total
                Show all 6 lines
                host = WIN-PFL4HRSLIAH | source = Perfmon:CPU Load | sourcetype = Perfmon:CPU Load
>  03/08/2025   08/02/2025 20:09:35.061 -0700
   06:09:35.000 collection="Network Interface"
                object="Network Interface"
                counter="Bytes Sent/sec"
                instance="Intel[R] PRO_1000 MT Desktop Adapter"
                Show all 6 lines
                host = WIN-PFL4HRSLIAH | source = Perfmon:Network Interface | sourcetype = Perfmon:Network Interface
```

8. Conclusion

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