

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'.

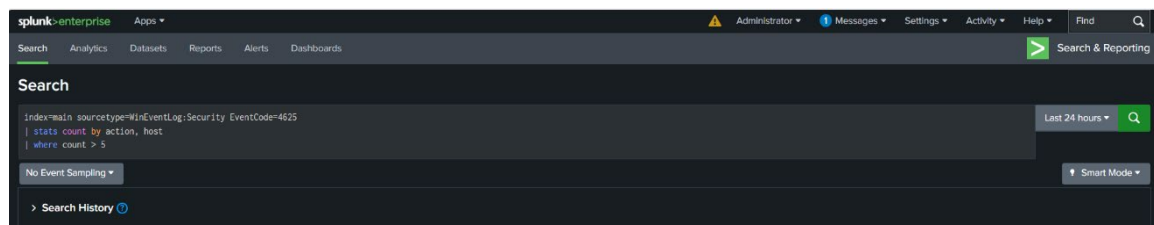
3. Objective

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 action, 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

AlertFailed Login

Description

Alert for failed login attempts on Windows Server

Alert type

ScheduledReal-time

Expires

24hour(s)

Trigger Conditions

Trigger alert when

Per-Result

Throttle

Trigger Actions

+ Add Actions

When triggered

Send email

Remove

To

dayosonibare@gmail.com

Comma separated list of email addresses. Email addresses represented by tokens are

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.

New Search

Save AsCreate Table ViewClose

Index:main

2,540 events (02/08/2025 06:00:00.000 to 03/08/2025 06:09:43.000)No Event Sampling

Job

Last 24 hours

Events (2,540)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDesired

1 hour per column

FormatShow: 20 Per PageView List

Hide Fields

All Fields

SELECTED FIELDS

host: 1

source: 5

sourcetype: 5

INTERESTING FIELDS

collection: 3

count: 5

host: 1

instance: 3

linecount: 4

object: 3

punct: 5

source_server: 1

Value: 100+

3D more fields

Extract New Fields

Time	Event
03/08/2025 06:09:35.000	<div>88/82/2825 28:89:35.862 -0700</div> <div>collection="CPU Load"</div> <div>object="processor"</div> <div>countern="User Time"</div> <div>instance="_total"</div> <div>Show all 6 lines</div> <div>host = WIN-PFL4HRESLIAH source = PerfromCPU Load sourcetype = PerfromCPU Load</div>
03/08/2025 06:09:35.000	<div>88/82/2825 28:89:35.862 -0700</div> <div>collection="CPU Load"</div> <div>object="processor"</div> <div>countern="Processor Time"</div> <div>instance="_total"</div> <div>Show all 6 lines</div> <div>host = WIN-PFL4HRESLIAH source = PerfromCPU Load sourcetype = PerfromCPU Load</div>
03/08/2025 06:09:35.000	<div>88/82/2825 28:89:35.861 -0700</div> <div>collection="Network Interface"</div> <div>object="Network Interface"</div> <div>countern="Bytes Sent/sec"</div> <div>instance="Intel(R) PRO 1000 MT Desktop Adapter"</div> <div>Show all 6 lines</div> <div>host = WIN-PFL4HRESLIAH source = PerfromNetwork Interface sourcetype = PerfromNetwork Interface</div>

8. Conclusion

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