

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'.

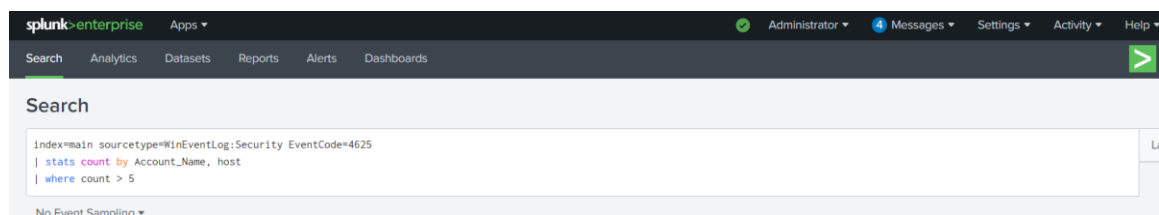
3. Objective

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

Title

Failed Login Alert

Description

Alert for failed login attempts on windows Server.

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week ▾

On

Monday ▾

 at

18:00 ▾

Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

1

Trigger

Once

For each result

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

index=main

✓ 4,750 events (12/6/25 12:00:00.000 AM to 1/5/26 3:12:35.000 PM)

No Event Sampling ▼

Job ▼

Events (4,750)

Patterns

Statistics

Visualization

✓ Timeline format ▼

– Zoom Out

+ Zoom to Selection

× Deselect

Format ▼

Show: 20 Per Page ▼

View: List ▼

< Prev

1

2

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 5

a sourcetype 5

INTERESTING FIELDS

a Account_Domain 8

a Account_Name 22

a collection 2

a ComputerName 1

a counter 3

EventCode 100+

EventType 5

a index 1

a instance 2

a Keywords 8

linecount 29

a LogName 3

i	Time	Event
>	12/29/25 1:07:30.000 PM	<div>12/29/2025 13:07:30.896 -0800</div> <div>collection="Available Memory"</div> <div>object=Memory</div> <div>counter="Available Bytes"</div> <div>instance=0</div> <div>Show all 6 lines</div> <div>host = WIN-OM0DH70VTT5 source = Perfmon:Available Memory sourcetype = Perfmon:Available Memory</div>
>	12/29/25 1:07:22.000 PM	<div>12/29/2025 13:07:22.001 -0800</div> <div>collection="CPU Load"</div> <div>object=Processor</div> <div>counter="% Processor Time"</div> <div>instance=_Total</div> <div>Show all 6 lines</div> <div>host = WIN-OM0DH70VTT5 source = Perfmon:CPU Load sourcetype = Perfmon:CPU Load</div>
>	12/29/25 1:07:21.000 PM	<div>12/29/2025 13:07:21.771 -0800</div> <div>collection="Available Memory"</div> <div>object=Memory</div>

8. Conclusion

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