

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'.

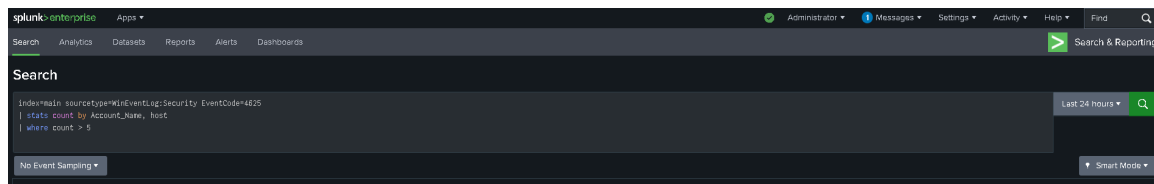
3. Objective

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

✕

✉ 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.

New Search

Save AsCreate Table ViewClose

Index=main

Last 24 hours

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

JobPauseRefreshShareSmart Mode

Events (2,540)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect

1 hour per column

FormatShow: 20 Per PageView List

TimeEvent

>03/08/202506:09:35.00003/08/2025 20:49:35.862 -0700collection=CPU Loadobject=Processorcounter=% User Timeinstance=TotalShow all 6 lineshost = WIN-PFL4HR3L6AH | source = Perfmon-CPU Load | sourcetype = Perfmon-CPU Load

>03/08/202506:09:35.00003/08/2025 20:49:35.862 -0700collection=CPU Loadobject=Processorcounter=% Processor Timeinstance=TotalShow all 6 lineshost = WIN-PFL4HR3L6AH | source = Perfmon-CPU Load | sourcetype = Perfmon-CPU Load

>03/08/202506:09:35.00003/08/2025 20:49:35.861 -0700collection=Network Interfaceobject=Network Interfacecounter=Bytes Sent/secinstance="Intel(R) PRO,1000 MT Desktop Adapter"Show all 6 lineshost = WIN-PFL4HR3L6AH | source = Perfmon-Network Interface | sourcetype = Perfmon-Network Interface

SELECTED FIELDS

host 1source 5sourcetype 3

INTERESTING FIELDS

collection 3counter 5index 1instance 3inaccount 4object 2pcount 5splunk_server 1value 100+

30 more fieldsExtract New Fields

8. Conclusion

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