

Project Title: Splunk Windows Security Monitoring

Author: Lokeshwar V

Date: July 2025



Table of Contents

1. Introduction
 2. Objectives
 3. Tools Used
 4. Dataset
 5. SPL Queries Used
 6. Dashboard Panels
 7. Alerts & Notifications
 8. Conclusion
-

1 Introduction

This project demonstrates how to use Splunk Enterprise to monitor Windows Security logs for login activities. The goal is to visualize security events and set up automated alerts for suspicious failed login attempts.

2 Objectives

- Understand how Splunk collects and indexes Windows Security logs.
- Build a dashboard to monitor login activities.
- Identify failed login attempts, successful logins, and account lockouts.
- Configure email alerts to notify an administrator about failed logins.

3 Tools Used

- Splunk Enterprise (Free Trial)
- Windows Security Event Logs
- Gmail SMTP for email notifications

4 Dataset

This project uses the Windows Security Event Log:

- **EventCode 4625:** Failed Login Attempt
- **EventCode 4624:** Successful Login
- **EventCode 4740:** Account Lockout

5 SPL Queries Used

Failed Login Attempts:

```
index=main sourcetype=WinEventLog:Security EventCode=4625  
| stats count by Account_Name, host  
| sort - count
```

Successful Login Attempts:

```
index=main sourcetype=WinEventLog:Security EventCode=4624  
| stats count by Account_Name, host  
| sort - count
```

Account Lockouts:

```
index=main sourcetype=winEventlog:Security EventCode=4740  
| stats count by Account_name, host
```

6 Dashboard Panels

The Splunk dashboard includes three panels:



1. Failed Login Attempts

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
| sort - count
```

All time

✓ 2 events (before 5/24/25 9:13:48.000 AM) No Event Sampling Job II III ↗ ⚙ ⬇ Smart Mode

Events Patterns **Statistics (2)** Visualization

Show: 20 Per Page Format Preview: On

Account_Name	host	count
-	LOKESHWARPC3123	2
LOKESHWARPC3123	LOKESHWARPC3123	2

2. Successful Logins

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

```
index=main sourcetype=WinEventLog:Security EventCode=4624
| stats count by Account_Name, host
| sort - count
```

Last 24 hours

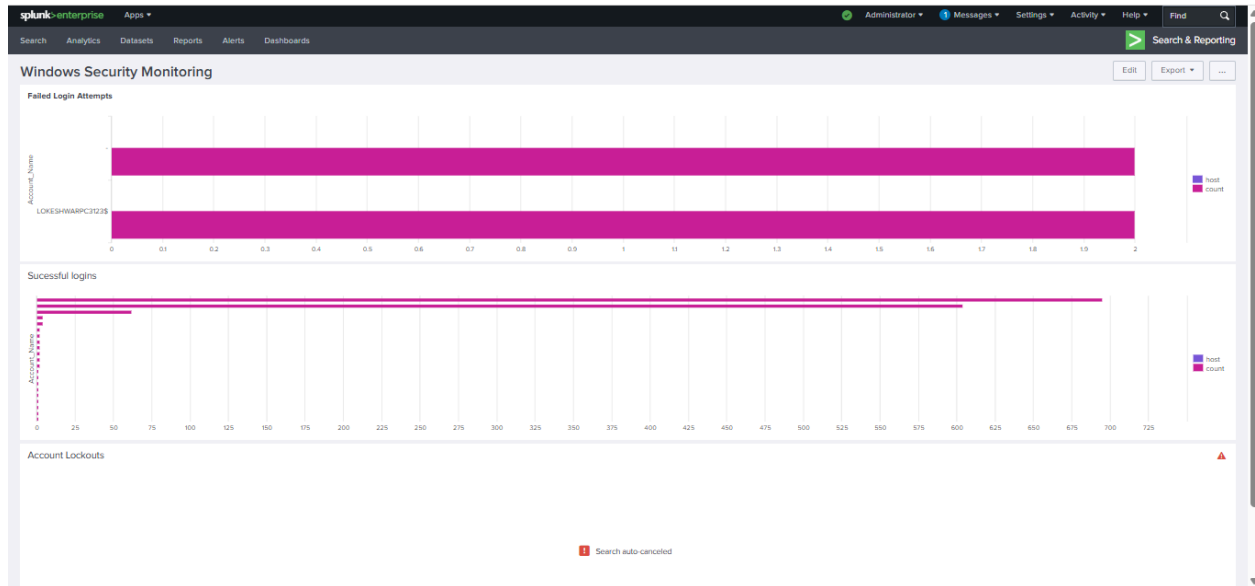
✓ 293 events (5/23/25 8:30:00.000 AM to 5/24/25 9:17:53.000 AM) No Event Sampling Job II III ↗ ⚙ ⬇ Smart Mode

Events Patterns **Statistics (9)** Visualization

Show: 20 Per Page Format Preview: On

Account_Name	host	count
LOKESHWARPC3123	LOKESHWARPC3123	293
SYSTEM	LOKESHWARPC3123	256
lokeshwar.v06@gmail.com	LOKESHWARPC3123	28
DWM-5	LOKESHWARPC3123	2
DWM-6	LOKESHWARPC3123	2
DWM-7	LOKESHWARPC3123	2
UNFD-5	LOKESHWARPC3123	1
UNFD-6	LOKESHWARPC3123	1
UNFD-7	LOKESHWARPC3123	1

3. Account Lockouts



7 Alerts & Notifications

An alert was configured to detect failed login attempts and send an email notification when the condition is met.

- **Alert Type:** Scheduled Search
- **Trigger Condition:** Results greater than 0
- **Action:** Send Email
- **Email:** Configured via Gmail SMTP with App Password

Triggered Alert Example

Splunk Enterprise interface showing the Job Manager. The URL is `127.0.0.1:8000/en-US/app/search/job_manager?app=search&filter=label%3D"email%20test%20alert"`. The page displays a table of jobs with the following columns: Owner, Application, Events, Size, Created at, Expires, Runtime, Status, and Actions. A single job is listed with the status "Done".

Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
lokeshwar	search	1	92 KB	Jul 12, 2025 9:00:02 AM	Jul 13, 2025 9:00:41 AM	00:00:01	Done	Job ▾ ▮ ↗ ⬇

email test alert [7/12/25 8:00:00.000 AM to 7/12/25 9:00:00.000 AM]

Email Notification Example

Gmail interface showing an email notification from Splunk. The subject is "Splunk Alert: test alert". The email body contains the following information:

The alert condition for 'test' was triggered.

Alert: [email test alert](#)

Trigger: Saved Search [email test alert]: number of events (1)

Trigger Time: 09:00:03 +0530 on July 12, 2025.

[View results in Splunk](#)

Account Name	Message	_raw	_time	host	index	linecount	source	s
SYSTEM	Special privileges assigned to new logon.	07/12/2025 08:45:23 AM LogName=Security EventCode=4672 EventType=0	Sat Jul 12 08:45:23 2025	LOKESHWARPC3123	main	31	WinEventLog:Security	V
	Subject: Security ID: S-1-5-18	ComputerName=lokeshwarpc3123						
	Account Name:	SourceName=Microsoft Windows						

8 Conclusion

This beginner-level Splunk project demonstrates how to:

- Set up SPL queries for Windows Security monitoring.
- Build a useful security dashboard.
- Configure alerts with automated email notifications.

The project can be improved further by adding more event types, advanced correlations, or integrating with other monitoring tools for real-world security monitoring.

End of Report