Failed Login Detection & SOC Log Analysis

Project Type: Authentication Monitoring / SOC Log Analysis

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this project was to analyze Windows authentication security logs to identify failed login attempts that could indicate unauthorized access, brute-force activity, or credential misuse. The assessment focused on reviewing failed authentication events to establish a baseline of normal login behavior and validate the absence of suspicious authentication patterns.

Tools & Technologies

- Windows Event Viewer
- Windows Security Event Logs
- Event ID filtering (Authentication failures)

Technical Steps Performed

1. Security Log Review

- Opened Event Viewer on the Windows endpoint.
- Navigated to:

Windows Logs → Security

2. Failed Login Event Filtering

- Applied a log filter for Event ID 4625 (failed logon attempts).
- Reviewed the filtered Security log to identify:
    - Frequency of failed login events ○ Timestamps and patterns
    - Repeated failures from the same source or account

3. Authentication Pattern Analysis

- Analyzed event metadata where available, including:
    - Logon type ○ Account name ○ Failure reason
- Assessed whether patterns aligned with:
    - Brute-force attempts ○ Unauthorized access attempts ○ Normal user behavior

---

Findings

- No failed login events (Event ID 4625) were observed during the review period.
- No repeated authentication failures or suspicious login patterns were identified.
- No evidence of brute-force attempts or unauthorized authentication activity was detected.
- Current authentication behavior aligns with a normal and secure baseline.

Outcome

- Established a baseline for failed authentication activity on the Windows endpoint.
- Confirmed the absence of suspicious or malicious login attempts.
- Verified that authentication logging is functional and suitable for SOC monitoring.
- Produced documented evidence supporting endpoint authentication security.

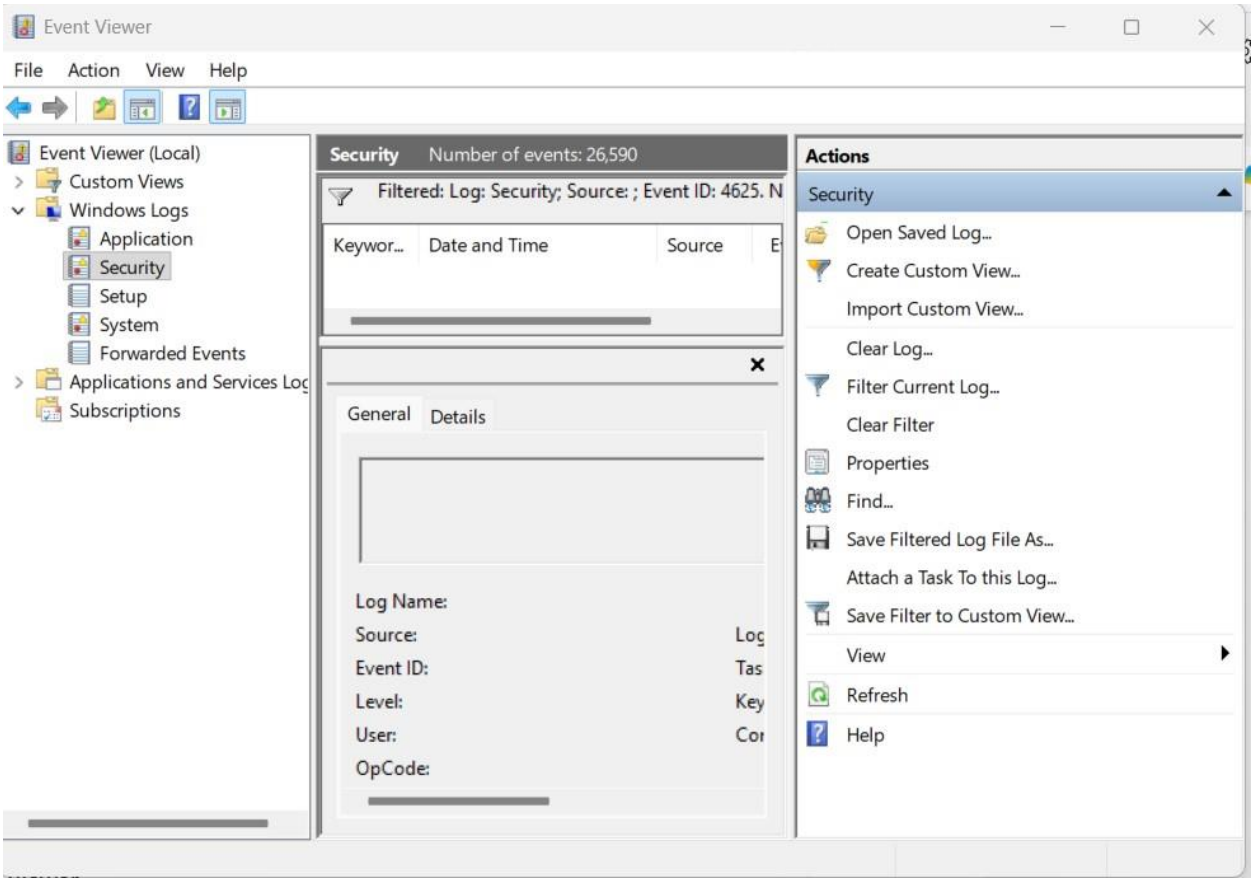
This project demonstrates hands-on experience performing SOC-style authentication log analysis, failed login detection, and baseline security validation using native Windows logging tools.

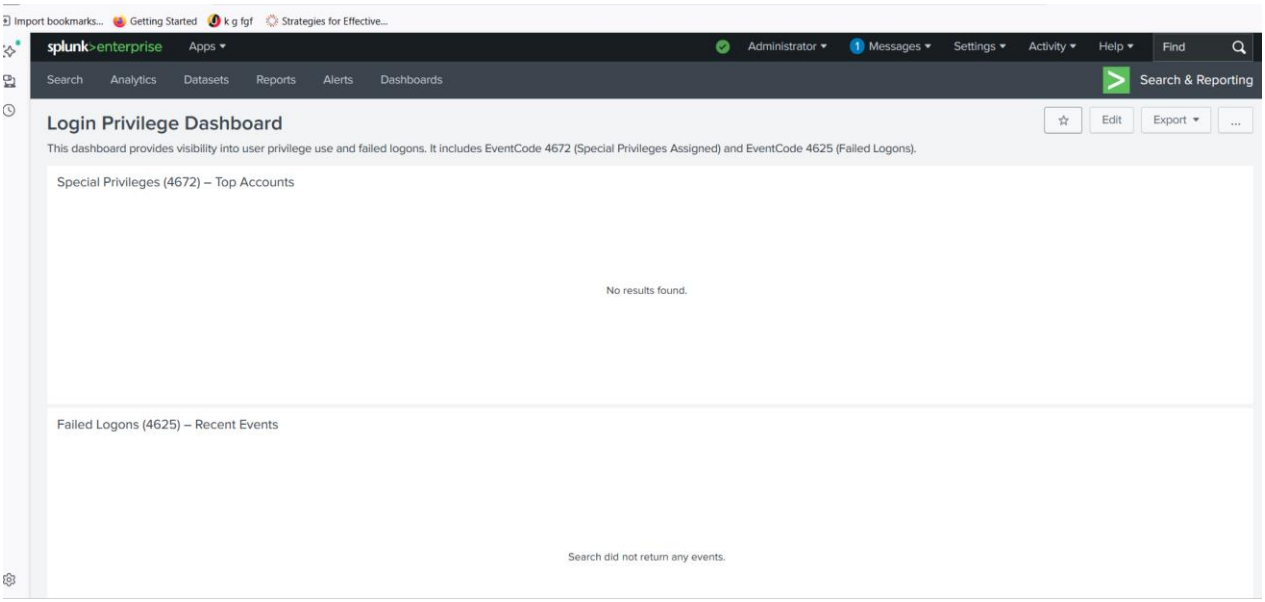
Portfolio Status

Project Status: Completed

Deliverable: SOC_Log_Analysis_Failed_Login_Assessment.pdf

Evidence: Event Viewer Security log filtered for Event ID 4625


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Security Number of events: 26,590
Filtered: Log: Security; Source: ; Event ID: 4625. N
Keywor...
Date and Time
Source
General Details
Log Name:
Source:
Event ID:
Level:
User:
OpCode:
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Login Privilege Dashboard
Edit
Export
This dashboard provides visibility into user privilege use and failed logons. It includes EventCode 4672 (Special Privileges Assigned) and EventCode 4625 (Failed Logons).
Special Privileges (4672) – Top Accounts
No results found.
Failed Logons (4625) – Recent Events
Search did not return any events.