Task 01 – Log Analysis, SIEM Dashboard Creation.

Author: B. Kartheek
Date: 03-10-25

1. Objective

- This report contains the details of the task includes Log analysis practice, Document Security Events, and setup Monitoring Dashboards. The goal of this task is to:
- Performing the log analysis using the windows event viewer tool.
- Documenting the security event that analyzed in the windows event viewer.
- Creation of dashboard in the SIEM tool like Kibana and also generating alerts.

2. Introduction

This task focused on log analysis, security event documentation, and monitoring dashboard setup using the Windows Event Viewer tool and SIEM tool. The goal Is to gain practical experience in identifying and responding to the security incidents by using the defensive tools.

3. Target & Attacker Description

- Target: Host A (Windows)
- Attacker: Host B (Linux machine)

4. Tools & Setup

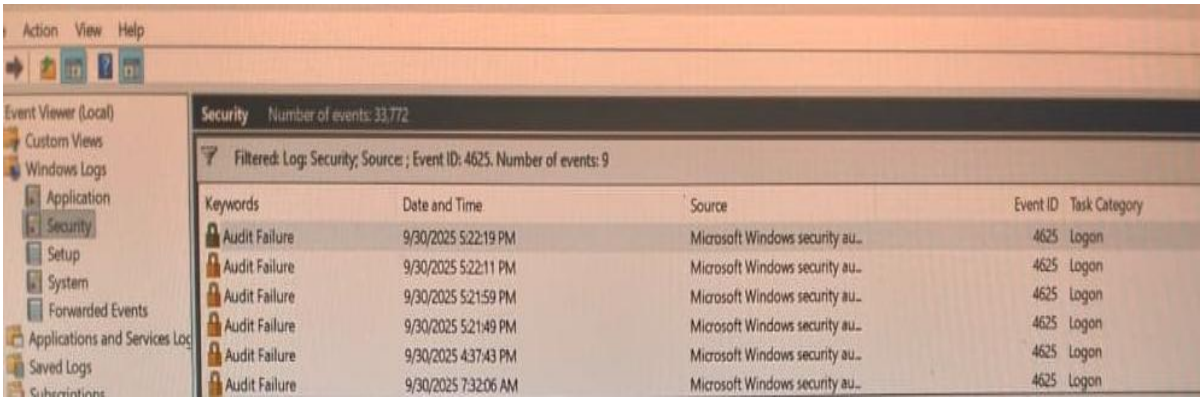
- Built-in: Windows Event Viewer, wevtutil CLI.
- Download LECmd tool in the Virtual Machine.

5. Log Analysis

Log analysis means the process of reviewing logs. Logs are nothing but record of events generated by software, hardware, and networks to gain the knowledge on system performance, its behavior, and its security, helps to identify errors, including security threats.

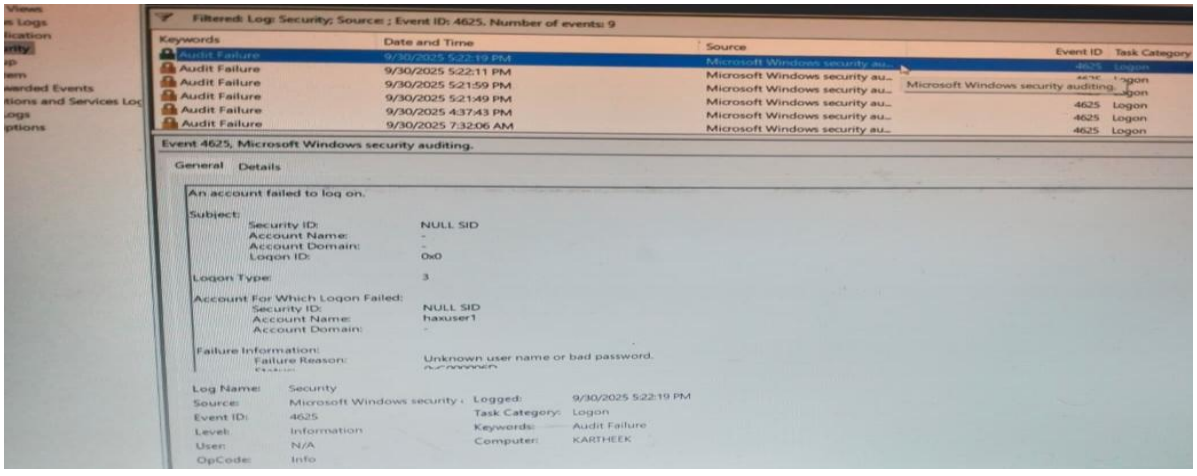
5.1 Windows Event Viewer

Windows event viewer is an windows tool that displays detailed system, security, and application logs, providing a record of what is happening in the computer.



5.1.1 Identifying brute-force attacks

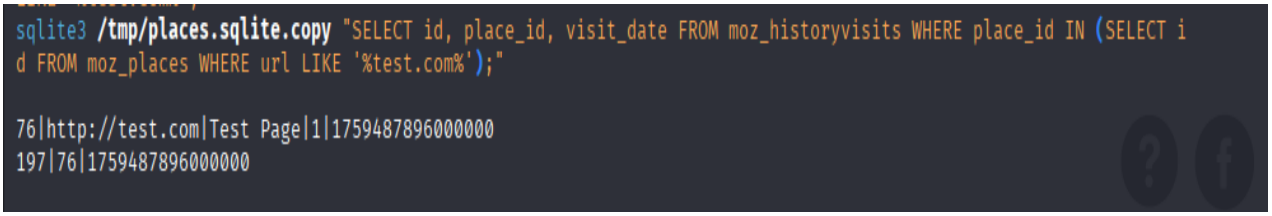
By analyzing the logs in the windows event viewer that continuous logs show the Brute-force attack and also there is a clear view of failed logins.



5.2 Browser History Analysis

For this browser history analysis in the Virtual Machine. I opened the test.com website For the detection of malicious URLs. I used SQLite tool to parse the Firefox history.

Firefox stores its browsing history, bookmarks, and other related data in SQLite database Called places.sqlite. This file is located within the user's Firefox profile directory.

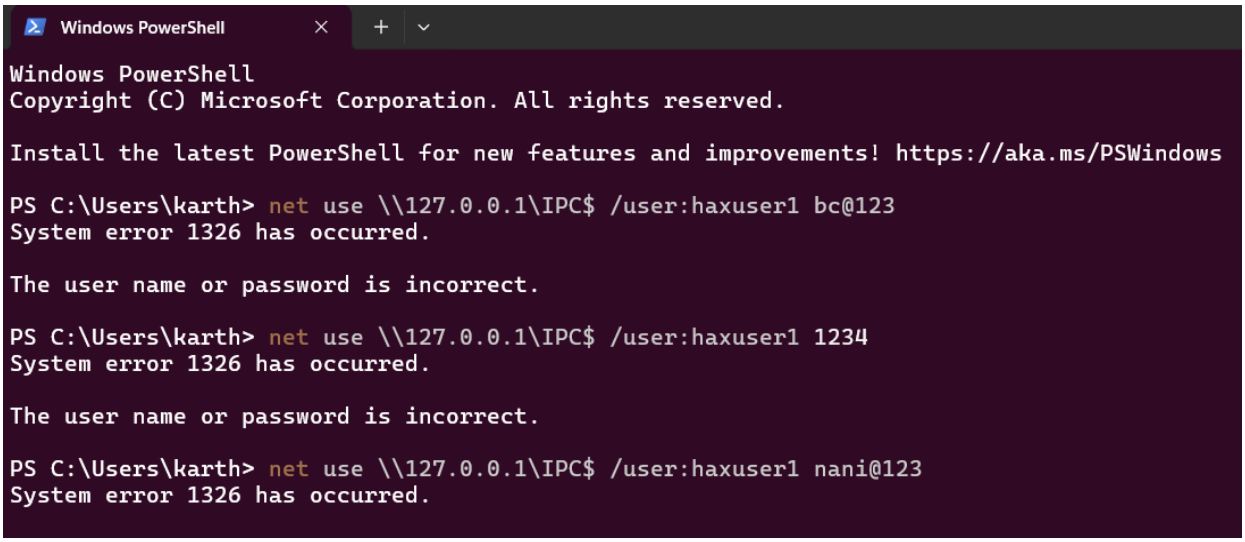


6. Creating template with fields

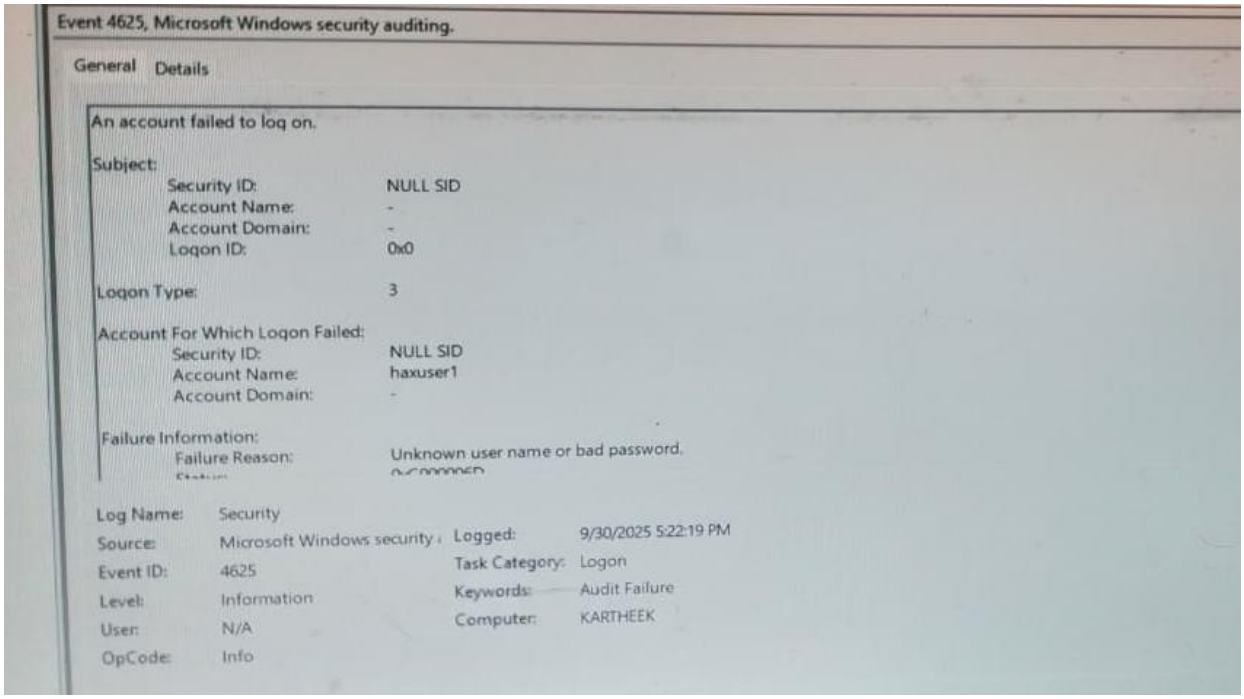
Date/Time	Source Ip	Event ID	Description	Action Taken
9/30/2025 5:22:59 PM	127.0.0.1	4625	Attacker tried to access the system with different passwords in the event viewer I detected it as a brute force attack	Account Temporarily locked

6.1 Mock Event

Practiced a mock event. I only used another account in my system and entered the wrong password for multiple times using windows power shell.



Analyzed the failed login attempts using the windows event viewer. I detected the audit failure continuously for more than five times. I analyzed the data like date and time, source IP, event ID, used port everything detailed.



6.1.1 Multiple failed logins mock event

Multiple failed logins documentation this is a practice of documenting the event of failed logins that it contains the details from the occurrence of event to mitigation of event and also the details of the attacker.

1. Incident Identification

Incident Number: 2025-09-30-001

Reported By: Tier 1 Analyst – Lab Environment

Date/Time Detected: 2025-09-30 17:22

Detection Method: Windows Event Viewer, Event ID 4625 (failed login)

2. Incident Description

Event Type: Brute-force login attempts

Systems Affected: Windows VM – Admin account

Source IP / Host: 127.0.0.1

Summary: Multiple failed login attempts (5+) detected on the administrator account within 5 minutes, indicating a potential brute-force attack.

3. Incident Classification

Category: Unauthorized Access Attempt

Severity: Medium

Impact: Minimal, but could lead to credential compromise in future.

4. Actions Taken

Immediate Response: Account temporarily locked.

Investigation: Verified failed login events in Event Viewer.

Mitigation: Tested account lockout policy; reviewed login attempts.

5. Timeline of Events

Time	Action / Observation	Analyst / Tool
17:22:11	First failed login attempt detected	Windows Event Viewer
17:22:19	Again failed login attempt detected	Windows Event Viewer
17:22:43	Continuous 4 failed login attempts	Windows Event Viewer
17:22:49	Account locked	
17:22:59	Blocked that using the Firewall	

6. Lessons Learned / Recommendations

Ensure account lockout policies are enforced

Monitor for multiple failed login attempts proactively

Test alert rules in lab environments regularly

7. Report Prepared By

Analyst Name: B. Kartheek

Date: 2025-09-30

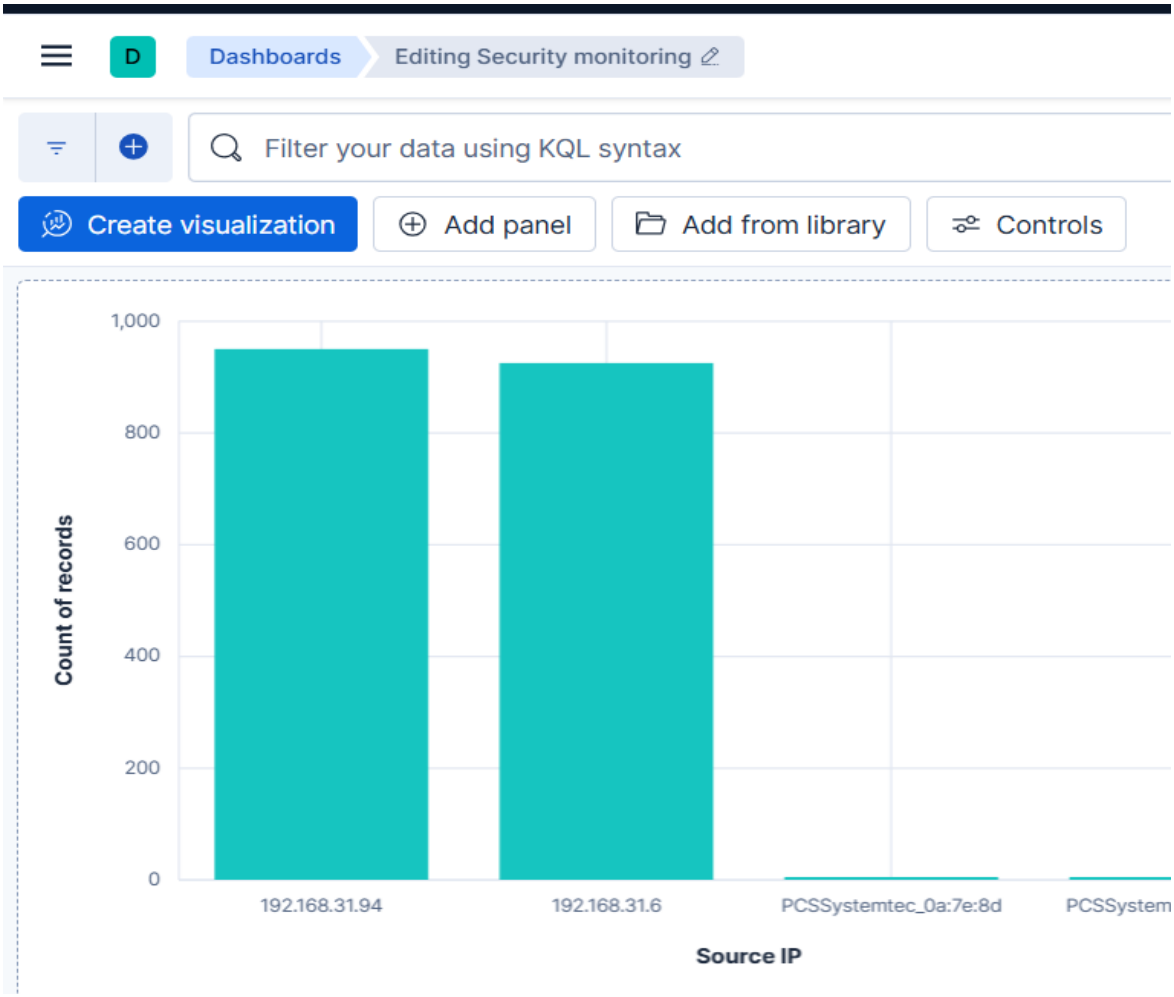
7.Monitoring Dashboard

Monitoring dashboard in the Kibana created the dashboard with the visualizations for the Top 10 source IPs generating alerts, Frequency of critical Event IDs.

For this dashboard creation the logs should be uploaded to the Kibana then these logs visualization should be done by creating the index fields and analyze them.

7.1 Source IPs generating alerts

This below graphical visualization shows the top10 source IPs generating alerts that x-axis shows the source IPs and y-axis shows the count of records that means how many times that particular IP address used for the attack and after the visualization then the alerts should be created.



8. Key Learnings

- Gained a knowledge on Log Forensics that means I learnt how to analyze the logs when the attack happened like the type of attack and it happened time.
- Learned how to make a documentation of occurred event and also understood the importance of the documented event.
- Understood how to translate the logs to the SIEM tool and also learned how to create the visualization along with alerts generation.

8.1 Challenges

At starting I faced difficulty in analyzing the logs and creating the visualization along with the generation of alerts.

I overcame these, by studying the documentation of the SIEM tool then I performed according to the documentation and finally performed the task.