Threat Detection Lab – Phase 3: Failed Login Detection

Generated on: 2025-05-08 21:00:49

# Objective

Detect failed login attempts on the system using audit logs, simulating brute-force or unauthorized access activity.

# Trigger Action

A fake SSH login was attempted using a non-existent user:

ssh fakeuser@localhost

# Detection Command

sudo grep -a "Failed password" /var/log/auth.log

# Sample Log Output

May 08 16:48:12 zakiya-vm-VirtualBox sshd[1278]: Failed password for invalid user fakeuser from 127.0.0.1 port 45678 ssh2

# Screenshot Evidence

- Failed\_Login\_Log.png: Captures the filtered result of failed login attempts.

- auth.log.live.png: Shows real-time monitoring using:

sudo tail -f /var/log/auth.log

This demonstrates live detection and correlation of SSH login events.

# Control Mapping

|  |  |  |
| --- | --- | --- |
| Control ID | Control Name | Justification |
| AC-7 | Unsuccessful Login Attempts | Detects and logs repeated failed authentication attempts |
| SI-4 | System Monitoring | Enables monitoring and correlation of suspicious behavior |