Task 12: Log Monitoring & Analysis

By : NROUPSINH GOHIL

Objective

To understand how system logs help in **detecting security incidents**, identifying **failed login attempts**, spotting **anomalies**, and learning **basic SIEM concepts**.

Understanding Logs (Theory)

What are Logs?

Logs are **system-generated records** that capture events such as:

- User logins
- File access
- Errors
- Application activity
- Security events

Logs help in **monitoring**, **forensics**, and **incident response**.

Types of Logs

1. **Authentication Logs** – Login attempts (success/failure)
2. **System Logs** – OS-level events
3. **Application Logs** – App-specific events
4. **Security Logs** – Access violations, privilege use
5. **Network Logs** – Traffic and connection data

Practical Analysis (Windows)

Tool Used

Windows Event Viewer

Steps Performed

1. Opened **Event Viewer**
2. Navigated to:
   Windows Logs → Security
3. Observed:
   - **Event ID 4624** → Successful login

- **Event ID 4625** → Failed login

4. Filtered logs to view multiple failed login attempts
5. Identified:
    - Username
    - Source machine
    - Timestamp
6. Noted repeated failures → Possible brute-force attempt

Practical Analysis (Linux – Conceptual)

Important Log Files

- /var/log/auth.log
- /var/log/syslog

Commands Used

sudo cat /var/log/auth.log

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

Observations

- Multiple failed SSH login attempts
- Repeated IP addresses
- Login attempts outside normal working hours

Anomaly Detection

What is an Anomaly?

Any behavior that **deviates from normal patterns**, such as:

- Login attempts at odd hours
- Too many failures from one IP
- Sudden admin access

Detected Anomalies

- Repeated failed logins
- Same IP trying multiple usernames
- Access attempts during inactive hours

Log Correlation

Log correlation means **connecting multiple log events** to identify attacks.

Example:

- Firewall log shows incoming request
- Authentication log shows failed login
  Possible brute-force attack

SIEM Basics

What is SIEM?

Security Information and Event Management
It:

- Collects logs
- Correlates events
- Detects threats
- Generates alerts

Examples:

- Splunk
- ELK Stack
- IBM QRadar

Sample Alert Rule (Concept)

If failed login attempts > 5 from same IP within 10 minutes

→ Trigger security alert

Findings Summary

- Logs are critical for detecting attacks
- Failed login analysis helps identify brute-force attempts
- Correlating logs improves detection accuracy
- SIEM automates monitoring and alerting

DELIVERABLE :

Log Monitoring & Analysis Report

This task focused on analyzing system and security logs to detect suspicious activities. Windows Event Viewer was used to analyze authentication logs, identifying failed and successful login attempts. Multiple failed login attempts from the same source were detected, indicating potential brute-force activity. Linux authentication logs were also studied conceptually to understand SSH attack detection. Anomaly detection and log correlation techniques were explored, along with basic SIEM concepts. This task provided hands-on understanding of how logs play a crucial role in incident detection and response.