

Task 12: Log Monitoring & Analysis Introduction

Log monitoring and analysis is an essential part of cybersecurity. Logs record system activities, user behavior, and security events. By reviewing logs, security teams can detect unauthorized access, suspicious behavior, and potential attacks. This task focuses on understanding log types, analyzing authentication logs, detecting failed logins, identifying anomalies, correlating events, learning SIEM basics, and documenting findings.

Understanding Log Types

Logs are generated by operating systems, applications, and security tools. Each log type provides different information:

- **System Logs** – Record operating system events such as startup, shutdown, and hardware errors.
- **Application Logs** – Store information about application activity, errors, and warnings.
- **Security Logs** – Track login attempts, account changes, and security-related events.
- **Audit Logs** – Record sensitive actions for accountability and compliance.
- **Network Logs** – Monitor traffic, firewall activity, and intrusion attempts.

Linux logs are usually stored in `/var/log`, while Windows logs are accessed through **Windows Event Viewer**.

Authentication Log Analysis

Authentication logs help identify who accessed a system and how.

Common authentication events include:

- Successful logins
- Failed login attempts
- Account lockouts
- Password changes
- Privilege escalation attempts

In Linux, authentication logs are found in `auth.log` or `secure`. In Windows, important Event IDs include:

- **4624** – Successful login
- **4625** – Failed login
- **4740** – Account lockout

Analyzing these logs helps detect unauthorized access and attack attempts.

Identifying Failed Login Attempts

Failed login attempts are a common indicator of attacks.

Signs of suspicious activity include:

- Multiple failed logins in a short time
- Repeated failures for the same user account
- Login attempts outside normal working hours
- Login attempts from unknown IP addresses

Such patterns may indicate brute-force attacks or compromised credentials.

Detecting Anomalies

Anomalies are activities that differ from normal behavior.

Examples include:

- Sudden increase in login attempts
- Unusual system restarts or service changes
- Access during late-night hours
- Unexpected data transfers

Establishing a baseline of normal behavior helps detect abnormal and potentially malicious activities.

Event Correlation

Event correlation involves linking related events across different logs.

Example:

- Multiple failed login attempts
- Followed by a successful login
- Followed by administrative actions

When correlated, these events may indicate a security incident. Correlation improves detection accuracy and reduces false positives.

SIEM Basics

SIEM (Security Information and Event Management) tools collect and analyze logs from multiple sources in one place.

Key SIEM features:

- Centralized log collection
- Real-time monitoring
- Event correlation
- Alert generation
- Security dashboards

Splunk Free is commonly used for learning log analysis and SIEM fundamentals.

Writing Alerts

Alerts notify security teams when suspicious activity occurs.

Effective alerts should include:

- Clear event description
- Severity level
- Time and source of the event
- Suggested action Examples:
 - Multiple failed logins within a short time
 - Login from an unknown location
 - Administrator login outside business hours

Good alerts help teams respond quickly to threats.

Documentation of Findings

Documenting findings is important for incident response and audits.

A log analysis report should include:

- Date and time of the event
- Log source and affected system
- Description of suspicious activity

- Analysis performed
 - Actions taken
 - Final outcome and recommendations
-

Final Outcome

After completing this task, the following skills were gained:

- Understanding log types
 - Analyzing authentication logs
 - Identifying failed login attempts
 - Detecting anomalies
 - Correlating events
 - Learning SIEM fundamentals
 - Writing alerts
 - Creating log analysis reports
-

Conclusion

Log monitoring and analysis play a vital role in cybersecurity. Regular log review, anomaly detection, and SIEM usage help identify threats early and strengthen incident response. These skills are essential for security operations and incident detection roles.

Prepared By:

Mohammed Javeeth .M