CYBER SECURITY INTERNSHIP – TASK 12

Log Monitoring & Analysis

---

1. What is a Log?

A log is a record of events generated by operating systems, applications, or network devices. Logs store important information such as timestamps, event type, user actions, and system messages.

Logs are used for:

- Troubleshooting issues
- Monitoring user activity
- Detecting security incidents
- Forensic investigations

---

2. Types of Logs

System Logs

Record system-related events such as startup, shutdown, and errors.

Application Logs

Generated by applications to record application behavior and errors.

Security Logs

Record authentication events such as login attempts, access control, and policy violations.

Audit Logs

Track user actions for compliance and accountability.

---

3. Tools Used

- **Windows Event Viewer**
- **Linux Logs (Conceptual)**
- **SIEM Tools (Splunk – Conceptual)**

Windows Event Viewer was used to view and analyze security and system logs.

---

4. Authentication Log Analysis

Authentication logs record user login and logout activities. These logs help identify:

- Successful logins
- Failed login attempts
- Account lockouts

Monitoring authentication logs helps detect unauthorized access attempts.

---

5. Failed Login Attempt Analysis

Multiple failed login attempts within a short period may indicate:

- Brute-force attacks
- Unauthorized access attempts

Observation:
Repeated failed login attempts can indicate suspicious activity.

---

6. Anomaly Detection

Anomalies are unusual activities that deviate from normal behavior.

Examples:

- Login attempts at unusual times
- Multiple failed logins followed by a successful login
- Access from unknown systems

Anomaly detection helps identify potential intrusions early.

---

7. Event Correlation

Event correlation links multiple log events to understand security incidents.

Example sequence:

- Multiple failed logins
- Successful login
- Access to sensitive files

This pattern may indicate a compromised account.

---

8. Introduction to SIEM

SIEM (Security Information and Event Management) systems collect and analyze logs from multiple sources.

Functions of SIEM

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

Examples:

- Splunk
- IBM QRadar
- ArcSight

---

9. Alerting (Conceptual)

Alerts notify administrators when suspicious activities occur.

Examples:

- More than 5 failed login attempts
- Login from unknown device
- Access to critical files

Alerts help in quick incident response.

10. Importance of Log Monitoring

Log monitoring is important because it:

- Detects security threats
- Supports investigations
- Improves system security
- Ensures compliance