Task 12: Log Monitoring & Analysis

Objective: Analyze system logs to detect security incidents such as failed logins, brute-force attempts, and anomalous behavior.

Tools: Linux logs (/var/log/auth.log), Windows Event Viewer, Splunk Free (SIEM basics).

Key Findings:

Source	Observation
Linux SSH Logs	Multiple failed login attempts from same IP
Windows Security Logs	Event ID 4625 followed by 4624
Correlation	Possible brute-force leading to successful login

Mitigation: Enable account lockout, enforce strong passwords, deploy SIEM alerts, enable MFA.

Conclusion: Log monitoring enables early incident detection and is essential for SOC operations.