Log_Analysis_Practice

Overview

Log analysis is the process of reviewing and interpreting logs to detect abnormal or malicious activity. It forms the backbone of SOC investigations.

By examining log entries systematically, analysts can identify security incidents, misconfigurations, or system errors that could escalate into threats.

Learning Approach

Students should practice reviewing common log sources such as authentication logs, web server logs, and firewall logs.

Understanding baseline log patterns is critical to distinguishing normal activity from anomalies.

Example / Use-Case

A series of failed login attempts followed by a successful login may indicate a brute-force attack. Analysts investigating logs can quickly detect such behavior.