Log Analysis

Duration: 1 day

- **Introduction to Log Files**
  - Importance of log analysis in cybersecurity
  - Overview of logging mechanisms
- **Common Log Formats**
  - Syslog structure and interpretation
  - Windows event log categories
  - Key fields and their meanings
- **Parsing and Analyzing Logs**
  - Techniques for log parsing
  - Identifying patterns and anomalies
  - Basic correlation and timeline reconstruction
- **Indicators of Compromise in Logs**
  - Recognizing signs of malicious activity
  - Mapping log entries to attack stages
- **Log Management & Compliance**
  - Retention policies and best practices
  - Compliance requirements and audit readiness