

NETWORK INVESTIGATIONS TRACK

NIT470, Advanced Log Analysis (ALA)

Who Should Attend

DoD and federal agents who will be required to analyze network logs as part of an investigation.

Prerequisites

TT110 (INCH), RT120 (CIRC), NIT301 (NMC), FT210 (WFE-E) or FT215 (WFE-FTK), And one of the following: IT250 (FISE), IT260 (FIWE) or IT270 (FILE)

Duration

5 Days

Course Description

Teaches advanced techniques for processing log files from common operating systems and devices such as firewalls, intrusion detection systems, sniffers, etc. Students learn how to effectively filter and search through a variety of log formats and to extract data as required. Also includes instruction for recognizing the signs of unauthorized activity within log files and correlating any discovered events. Prospective students should know the elements of network traffic and network protocols. {Mobile}

Objectives

- Search and filter text and binary logs
- Format log data
- Extract data from log files, including data transfers found in captured network traffic
- Identify the artifacts associated with the different stages of a network intrusion

Topics Covered

Intrusion Analysis

- Intrusion Methods
- The Scientific Method and Intrusion Analysis
- Observation Intrusion Related Activities and Generating a Hypothesis
- Predicting the Nature and Location of Intrusion Artifacts
- Using Log Analysis to Evaluate an Intrusion Hypothesis
- Forming a Conclusion and Reporting Findings

Log Analysis

- Overview, Log File Types and Formats

Analyzing Text Logs

- Filtering, Searching and Extracting Data from Text Logs

Formatting and Searching Binary Logs

- Command Line Tools
- GUI Tools
- Searching Binary Logs with an IDS
- Formatting Binary Log Elements

Extracting Data from Binary Logs

- Basic Data Extraction and Carving

NETWORK INVESTIGATIONS TRACK

Preparation

To prepare for this course, we recommend the following review, reading, or research:

- Review the *Introduction to Networks and Computer Hardware* (INCH) course book, paying special attention to:
 - Operating Systems, specifically MS Windows Operating Systems Basics
 - Windows XP Command Line
 - Network Connectivity and Devices
 - IP Addresses, Subnets and Network Security (specifically Firewalls, IDS, Logs)

- Review the *Computer Incident Responders Course* (CIRC) course book, paying special attention to:
 - OSI Layer Functions and Physical Assessment
 - Witness Devices – Networks and Witness Devices, Switches, Firewalls, Routers, Sniffers and Intrusion Detection Systems, Remote Logging

- Review the *Forensics and Intrusions in a Windows Environment* (FIWE) course book, paying special attention to:
 - Network Architecture Basics, Wireshark, Network and Application Protocol Analysis
 - Fundamentals of Network Artifact Analysis, Network Device Artifact Analysis, Network Traffic Capture Analysis

- Review network security Web sites for log analysis topics

- Review log analysis sites that may have sample logs to view

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (<https://www.dcita.edu>), the internet, at Books 24/7, in your organization's technical library or at the public library. Instructions for D-Prep on the dcita.edu portal: log in. Under Online Courses (INCH/CIRC/FIWE), select DPrep Training; Course Name; Sort by Name Ascending.

ALA Grading Policy

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.