

NETWORK INVESTIGATIONS TRACK

IT270, Forensics and Intrusions in a Linux Environment (FILE)

Who Should Attend

DoD and federal law enforcement intrusion analysts.

Prerequisites

TT110 (INCH), RT120 (CIRC) and FT210 (WFE-E) or FT215 (WFE-FTK) or Test Outs

Duration

10 Days

Course Description

FILE is a scenario-based course that teaches students how to conduct detailed Linux-based data analysis in a laboratory environment. Students conduct forensic media analysis and log file analysis to determine the specifics of a Linux-based intrusion. Topics also include hacking methodologies that are key to understanding an attack, case preparation and management.

Objectives

- Using tools and analysis techniques presented in class, analyze network traffic of an intruder and correlate the findings with forensic evidence found on a Linux victim machine.
- Prepare a forensic examination system running the Linux operating environment
- Analyze a compromised system running the Linux operating environment by analyzing both system and log files
- Complete a detailed intrusion analysis report

Topics Covered

Network Architecture and Information Assurance

- Network Architecture Basics, including LAN/WAN Topologies and Network Services
- Introduction to Wireshark and Creating Filters
- Network and Application Protocol Analysis

Identifying an Intrusion

- Computer Intrusions, Goals, Attacker Profiles and Intrusion Phases
- The Goals, Strategies and Techniques of Reconnaissance, Attack, Entrenchment and Abuse

Case Management and Investigative Methodology

- Investigating Using the Scientific Method
- Documentation

System Preparation and Forensic Analysis

- The Linux File System and fundamentals of Linux Artifact Analysis
- Forensic System Setup
- Analyzing First Responder Data
- Beginning a case with The Sleuth Kit and Autopsy
- Keyword Searching
- Malicious Code Analysis

NETWORK INVESTIGATIONS TRACK

Network Device Analysis

- Fundamentals of Network Artifact Analysis
- Network Device Artifact Analysis
- Network Traffic Capture Analysis

Preparation

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

- Review the *Introduction to Networks and Computer Hardware* (INCH) and the *Computer Incident Responders Course* (CIRC) course books, paying special attention to:
 - Operating Systems, specifically Linux
 - Windows XP Command Line
 - Basic networks, The OSI Model, Network Connectivity, Configuration (including ports), Protocols and Devices
 - IP Addresses, Subnets and Network Security (specifically Anti-virus Software, Firewalls, IDS, Logs)
 - Linux defined (including directories) and basic Linux commands
- Review the *Computer Incident Responders Course* (CIRC) course book, paying special attention to:
 - OSI Layer Functions, Logical and Physical Assessment
 - Witness Devices – Networks and Witness Devices, Switches, Firewalls, Routers, Sniffers and Intrusion Detection Systems, Remote Logging
 - Linux Incident Preparation and Information Collection
- Outside reading on hacking methodologies would also be beneficial

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, select DPrep Training; Course Name; Sort by Name Ascending.

FILE 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%.