

NETWORK INVESTIGATIONS TRACK

IT260, Forensics and Intrusions in a Windows Environment (FIWE)

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

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

Objective

Use tools and analysis techniques to analyze network traffic of an intruder and correlate the findings with forensic evidence found on a Windows victim machine.

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 Windows Operating System and fundamentals of Windows Artifact Analysis
- Forensic System Setup and Initial Case Processing
- Introduction to and installation of EnCase, Wireshark, jpcap, CoolMiner, Snort and Sawmill
- Analyzing First Responder Data
- File System Searching and Filtering
- Windows Registry, System Log, System Memory and Malicious Code Analysis

Network Device Analysis

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

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
 - Windows 7, Internet Explorer 8
 - Windows Registry
 - Basic networks, Network Connectivity, Configuration (including ports), Protocols and Devices
 - IP Addresses, Subnets and Network Security (specifically Anti-virus Software, Firewalls, IDS, Logs)
- 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
 - Windows 2003 Server Information Collection
- Review the *Windows Forensic Examinations* (WFE) course book, paying special attention to:
 - Getting Started - Lab Requests and Forensic Reporting
 - Beginning a New Case with EnCase - Beginning a Case, Digital Media Validation, the EnCase GUI and Bookmarking
 - Forensic Analysis Basics - Windows and the Windows Registry
 - Initial Forensic Analysis with EnCase - Malicious Code Scanning, File Signature and Hash Analysis, Keyword Searching
 - Using Automated Tools - Filters and Conditions, Data Carving, Advanced Keyword Searching, Date Searching
 - File Level Analysis - Web Related Evidence
- 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.

FIWE 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%.