

NETWORK INVESTIGATIONS TRACK

NIT315, Network Exploitation (NET)

Who Should Attend

DoD and federal law enforcement intrusion analysts.

Prerequisites

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

Duration

5 Days

Course Description

Students are exposed to the concepts and fundamentals of network and host exploitation techniques used by the targets of their investigations. This course also provides students with examples of data left behind by attacks and how to implement their own testing environment for use during investigations.

Objective

Given several scenarios, students will be able to:

- Explain high level network exploitation goals and processes
- Implement their own testing and evaluation environment
- Describe the most common exploitation techniques
- Execute network exploitation techniques to find, compromise and maintain control of a remote computer
- Describe the typical traces left by their actions

Topics Covered

Network exploitation strategies

- Introduction, Basic Definitions, Intrusion Goals and an Overview of the Intrusion Process
- Network Architecture and Attack Vectors
- Attack Platforms
- Documentation

Reconnaissance

- Methods, Indirect and Direct Reconnaissance

Attack Methods

- Excessive Input and Authentication Attacks
- Web Page Components
- Code and Command Injection

Entrenchment Methods

- Goals, Strategies and Tools, Control, Persistent Indicators, Memory Space
- Active Directory and Enterprise Network Entrenchment

Abuse Methods

- Goals, Strategies and Tools
- Data Theft
- Attack Pivots

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 and Linux Operating Systems
 - Windows XP Command Line
 - Windows 7, Internet Explorer 8
 - Basic networks (including 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 and Physical Assessment
- Review the *Forensics and Intrusions in a Windows Environment* (FIWE) course book, paying special attention to:
 - Computer Intrusions, Reconnaissance, Attacks, Entrenchment and Abuse
- 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 (INCH/CIRC/FIWE), select DPrep Training; Course Name; Sort by Name Ascending.

NET 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%.