National White Collar Crime Center

To register, visit our training site at:

www.nw3c.org

Questions? Call 877-528-7674

CS 235 Basic Network Intrusion Investigations (BNII)

Cybersecurity

Classroom Course

4 days

Prerequisite: CS 100

This course covers the skills and techniques involved in responding to a network security incident. The course focuses on the identification, extraction, and detailed examination of artifacts associated with network and intrusions. Memory analysis, host machine forensics, network traffic and log analysis, malware analysis, and virtual machine sandboxing are covered through lecture, discussion, and hands-on exercises. Additional topics include key cybersecurity concepts and issues, as well as the various classifications and types of network attacks.

Introduction to cybersecurity

The cybersecurity threatscape. The CIA Triad. Case studies.

Network traffic analysis

The OSI and TCP/IP models. Monitoring, capturing, and parsing artifacts from PCAP files.

Network attacks

Attack types (insider threat, opportunistic, targeted, advanced persistent threats, blended attacks). Examination of artifacts from keystroke logger, brute force attack, privilege escalation, remote access, data tampering, data exfiltration, botnet, and DDoS attacks.

Investigative techniques

Live machine triage and the order of volatility. Capturing volatile data. Best practices for data analysis.

Hands-on experience

Host machine triage, memory analysis, network traffic and log analysis, malware analysis, and virtual machine sandboxing.

Version 3.1, updated April 2018

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.