DC3 Cyber Training Academy

FY25 September Offerings

Enroll Now

Click on the "Enroll Now" link to view the online catalog and to register for classes. Please contact the DC3 Cyber Training Academy Registrar with any questions.

Forensics and Intrusions in a Windows Environment (FIWE)

Forensics and Intrusions in a Windows Environment (FIWE) is an 80-hour scenario-based training course developing students' skills in conducting a full investigation of a network intrusion. FIWE is designed for Defense Criminal Investigative Organizations (DCIOs), DoD intrusion analysts, network operators, and investigators. Students conduct forensic examinations of victim devices, analyze log data and network traffic data, create an event timeline, perform malware analysis, and prepare narrative reports of their findings. These skills prepare students to perform a variety of network investigations. FIWE contains three modules and culminates with a graded Final Exam.

Delivery: Instructor-Led Virtual (ILV)
Duration: 80 hours of training over 2 weeks
Prerequisite: NIB and WFE
IACET CEU-eligible, ACE Recommendation
Scheduled Offering:
FIWE-2506-ILV (15-26 SEPT)

Intermediate Malware Analysis (IMA)

Intermediate Malware Analysis (IMA) is an 80-hour course that covers the methods used by attackers to gain unauthorized access to systems and malicious activities that they may perform while present there. Starting with a solid foundation, students will gain insights that will enable them to find patterns, recognize malicious behavior, and dissect complex code structures. Students will be provided with methods and strategies to investigate and analyze malicious software, including hands-on practical labs and instructor-led demonstrations. Upon course completion, students will be equipped with the knowledge, skills, and practical experience they need to perform a malware analysis during an attack investigation in the Linux environment.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: None
Scheduled Offering:
IMA-2503 (8-19 SEPT)

Managed Attribution (MA)

Managed Attribution (MA) will train students in the techniques, tactics, and procedures for developing deliberate, controlled, and misleading digital footprints to support law enforcement and counterintelligence operations. Students will learn about the methodologies used by adversaries and the necessary skills, techniques, and strategies to protect sensitive information, while performing law enforcement or counterintelligence operations. This course will also teach students to proactively defend against threats while maintaining operational security and preserving the integrity of their organizations.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
MA-2504 (8-12 SEPT)

Network Mapper (NMAP)

Network Mapper (NMAP) is an 8-hour course that provides instruction in using the Network Mapper tool to manage vulnerabilities, verify baseline configuration compliance, and identify risk among communication protocols, data services, and associated ports. NMAP is designed for work roles assigned to the specific task of exploring networks to isolate vulnerabilities and applying programs that protect exploitable ports from attacks. Students learn how to conduct reconnaissance on adversary networks. The course provides functional information and focuses on useful, real-life examples that students can immediately apply. NMAP contains five modules and culminates with a Final Exam.

Delivery: Online
Duration: 8 hours of training over 5 days
Prerequisite: INCH
Scheduled Offering:
NMAP-2505-OL (29 SEPT – 3 OCT)
