DC3 Cyber Training Academy

FY25 June 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.

Basic Malware Analysis (BMA)

Basic Malware Analysis (BMA) is a 40-hour course designed to provide students with a foundational understanding of malicious software and its forms, traits, author motivations, and impacts. Students will be introduced to common techniques and tools for both dynamic and static analysis and will develop a basic understanding of the process for uncovering the functionality of malware samples. Students also learn how to establish a network-isolated malware analysis lab, and how to interpret analytical reports resulting from static and dynamic analysis of malware. The BMA course contains six modules with corresponding module exams and culminates in a graded Final Exam.
Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
BMA-2502 (23-27 JUN)

Cryptocurrency Activities (CCA)

Cryptocurrency Activities (CCA) is a 40-hour in-residence training course designed for law enforcement and counterintelligence professionals and provides students with an understanding of cryptocurrency fundamentals and the skills necessary to conduct investigations into cryptocurrency transactions. The course immerses students in scenario-based exercises that allow them to practice and reinforce what they have learned while using trusted resources. CCA culminates with a graded Final Exam.
Delivery: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
CCA-2506-ILV (2-6 JUN)

Drone Forensics (DF)

Drone Forensics (DF) is a 40-hour scenario-based training course. The course provides training that enables professionals to gather forensic artifacts from and conduct digital analysis on Unmanned Aerial Systems (UAS) in a forensically reliable manner. DF introduces best practices and relevant technical aspects of interacting with unmanned aerial systems and their associated peripherals. The course not only introduces students to the forensic artifacts found on these systems and how to recover and analyze them but also provides participants the opportunity to get direct experience with the systems. The course will contain 4-days of hands-on, in-class exercises with a conclusion on the final day with a cumulative exam.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
DF-2501 (23-27 JUN)

Introduction to Cyber Investigations (ICI)

Introduction to Cyber Investigations (ICI) is a 40-hour course that prepares students to perform or support the role of a case agent responsible for a basic cyber investigation. ICI is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Students learn basic technical concepts and the legal framework that guides the conduct of cyber investigations. Students also study special aspects of cyber case management (including online evidence collection) and subjects of cyber investigations. ICI contains five modules with module assignments and exercises and culminates with a final, graded exam.

Delivery: Online
Duration: 40 hours of training over 5 weeks
Prerequisite: None
ACE Recommendation
Scheduled Offering:
ICI-2505-OL (9 JUN – 10 JUL)

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: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
IMA-2501 (2-13 JUN)

Introduction to Networks and Computer Hardware (INCH)

INCH is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examinations. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, as well as security and safety terminology and techniques. INCH contains 10 modules and culminates with a Capstone Exam.
Delivery: Online
Duration: 40 hours of training over 4 weeks
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offerings:
INCH-2517-OL (23 JUN – 17 JUL)
INCH-2518-OL (23 JUN – 17 JUL)

Log Analysis (LA)

LA is a 50-hour course that provides a comprehensive understanding of log analysis techniques. LA is designed for cyber investigators or analysts interested in furthering their skills in determining the how, when, and where of a network intrusion through log file analysis and investigation. Students learn how to process logs from Windows and Linux operating systems, firewalls, intrusion detection systems, and web and email servers. Students learn how to assemble evidence found in logs to assist in tasks ranging from building a case to recognizing an intrusion. LA contains three modules comprising multiple lessons and culminates with a final, graded exam.
Delivery: Online
Duration: 50 hours of training over 5 weeks
Prerequisite: None
Scheduled offering:
LA-2506-OL (23 JUN – 24 JUL)

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 (16-20 JUN)

Network Traffic Collection (NTC)

NTC is a 40-hour course that prepares students to strategically place monitoring sensors in a network to capture traffic to and from a specific host. NTC is designed for Department of Defense (DOD), cyber-intrusions investigators, information assurance professionals, prospective lab examiners, and military intelligence and 5 counterintelligence personnel. Students examine how to evaluate a network, both physically and logically, to determine proper sensor placement. Students also study how to filter network traffic to comply with wiretap authority, hide the presence of the monitoring workstation on the network, and evaluate captured traffic for the proper content. NTC contains five modules and culminates with a final, graded exam.

Delivery: Instructor-Led Virtual (ILV)

Duration: 40 hours of training over 1 week

Prerequisite: None

Scheduled offering:

NTC-2505-ILV (23-27 JUN)

Online Undercover Activities (OUA)

Online Undercover Activities (OUA) is a 40-hour scenario-based training course that will develop professionals' skills in conducting a full online undercover operation. The course provides both theory and practical training, enabling students to develop and plan an online undercover operation, create personas, manage digital footprints, engage in simulated dark web marketplaces and forums, and report their findings and activities. OUA contains six modules and culminates in a final, graded exam.

Delivery: In-residence

Duration: 40 hours of training over 1 week

Prerequisite: None

Scheduled Offering:

OUA-2502 (23-27 JUN)

Penetration Testing (PenTest+)

Penetration Testing (PenTest+) is a bootcamp-style course that covers all penetration testing stages and teaches vulnerability management. Students learn planning and scoping, information gathering and vulnerability scanning, how to apply best practices for reporting and communication, updated approaches to attacks and exploits, code analysis, and uses of various tools. Vouchers are not included.

Delivery: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
PenTest+-2506-ILV (23-27 JUN)