DC3 Cyber Training Academy

FY25 July 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.

Cyber Analyst Course (CAC)

The Cyber Analyst Course (CAC) is a 40-hour, one-week, in-residence course that fuels cyber professionals' critical thinking and provides analytical skills so they can interpret different types of reports, conduct internet research, identify intrusions, explore data-hiding techniques, and analyze computer systems, networks, and logs. Students explore real-world scenarios using specialized analytical tools that allow for skills practice, writing analysis reports, creating link diagrams, and completing performance exercises. The course includes 70 percent practical application and 30 percent knowledge-based learning, all preparing students for a final knowledge- and performance-based exam.
Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
CAC-2505 (21-25 JUL)

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-2506-OL (14 JUL – 14 AUG)

DC3 Cyber Training Academy

FY25 July Offerings

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-2502 (21 JUL – 1 AUG)

Introduction to Networks and Computer Hardware In-Residence (INCH-RES)

INCH-RES is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH-RES is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examination. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, security, and safety terminology and techniques, complete with the physical disassembly and reassembly of a computer. INCH-RES contains 10 modules and culminates in Capstone Exam. A test-out option is available to permit qualified personnel to bypass the course.
Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offering:
INCH-RES-2507B (14-18 JUL)

DC3 Cyber Training Academy

FY25 July Offerings

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-2519-OL (21 JUL – 14 AUG)
INCH-2520-OL (21 JUL – 14 AUG)

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-2507-OL (28 JUL – 28 AUG)

DC3 Cyber Training Academy

FY25 July Offerings

Linux Essentials (LXE)

Linux Essentials (LXE) is a 40-hour course that teaches core concepts and techniques of Linux system management and administration. LXE is designed for students who want to develop greater understanding of Linux or who conduct investigative and security activities associated with Linux environments. Students acquire intermediate Linux skills used in cyber investigation studies and real-world investigative and security tasks. The course prepares students to carry out functions and tasks relevant to any standard Linux environment. LXE contains nine lessons and culminates with a graded Final Exam.

Delivery: Online
Duration: 40 hours of training over 4 weeks
Prerequisite: None
Scheduled offerings:
LXE-2509-OL (21 JUL – 14 AUG)

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-2503 (28 JUL – 1 AUG)

DC3 Cyber Training Academy

FY25 July Offerings

OpenVAS (OPV)

OPV is an 8-hour course that provides instruction in using OpenVAS software to run vulnerability scans, generate reports, and analyze the results. This course is designed for vulnerability management analysts, information security analysts, cybersecurity specialists, and risk and vulnerability engineers. Students install OpenVAS using the command line and operate the Greenbone Security Assistant interface to navigate and customize the software. Practical exercises train students on OpenVAS terminology and techniques. OPV contains four modules and ends with a final, graded exam.
Delivery: Online
Duration: 8 hours of training over 1 week
Prerequisite: None
Scheduled offering:
OPV-2504-OL (28 JUL – 1 AUG)

Security + (SEC+)

Security+ (SEC+) is a bootcamp-style course that will be a significant part of your preparation to pass the CompTIA Security+ (Exam SY0-601) certification examination. The CompTIA SEC+ certification will help you build your cybersecurity skill set so you can confidently perform your duties in any entry-level security role. Vouchers are not included in this course and students must make their own arrangements to take the exam at any CompTIA testing center.
Delivery: In-Residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
SEC+-2507B (21-25 JUL)

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: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
PenTest+-2506B (28 JUL – 1 AUG)