DC3 Cyber Training Academy

FY23 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.

Cyber Analyst Course (CAC)

The Cyber Analyst Course (CAC) is an 80-hour course that presents analytical methodologies and information sources applicable to a cyber environment. CAC is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Topics include interpreting analysis and forensic reports, internet research, computer system and network analysis, log analysis, data-hiding techniques, and intrusion identification. The course also covers using specialized analytical software and writing analysis reports. CAC contains six modules and culminates with a Final Knowledge Exam and a Final Performance Exam.
Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
Scheduled offering:
CAC-2304 (18-30 SEPT)

Cyber Fundamentals 200 (CF200)

CF200 is an 80-hour course that serves as the second installment of a two-part curriculum to provide foundational cyber knowledge to cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include the protection of DOD information systems from unauthorized and/or illegal access. The course comprises three units with multiple lessons; each unit culminates in a unit milestone exam and the 2 course ends with a Capstone Exam. There is a test-out option available to permit qualified personnel to bypass the course.
Delivery: Online asynchronous (Self-paced/no instructor)
Duration: 80 hours of training over 3 weeks
Prerequisite: None
Scheduled offering:
CF200-2315-OL (11-30 SEPT)

DC3 Cyber Training Academy

FY23 September Offerings

Cyber Incident Response Course (CIRC)

The Cyber Incident Response Course (CIRC) is an 80-hour course that prepares students in cyber incident response and evidence collection. In this course, students are provided various scenarios to understand and develop response protocols in a real-world environment. Using trusted forensic tools, students identify and extract digital evidence from various devices such as computers, cell phones and small form factor digital storage devices. Students are taught how to properly document evidence using lawful, professional techniques to ensure the legal admissibility of the seized evidence. CIRC contains three units with quizzes and a course Capstone Exercise.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
IACET CEU-eligible, ACE Recommendation
Scheduled Offering:
CIRC-2317 (5-16 SEPT)

Cyber 101 (CY101)

Cyber 101 (CY101) is a 40-hour course that is designed to provide fundamental cyber knowledge to students interested in developing cyber competency or who are in roles where they support cyber operations (such as CPTs, MDTs). CY101 is a requirement for any personnel identified in DoDD 8140 as a “cyber enabler.” The course consists of five units containing modules and lessons, unit Milestone Exams, and a final, graded Capstone Exam.

Delivery: Online asynchronous (Self-paced/no instructor)
Duration: 40 hours of training over 3 weeks
Prerequisite: None
Scheduled Offering:
CY101-2315-OL (11-30 SEPT)

Introduction to Networks and Computer Hardware Test Out (INCH-TO)

Introduction to Networks and Computer Hardware Test Out (INCH Test-Out) provides students with the opportunity to demonstrate mastery of both the content knowledge portion of the course material in addition to a hands-on desktop computer tear down and rebuild. The content knowledge portion covers computer basics, network theory, and input/output device identification and function. Students must also demonstrate mastery of common operating system functionality and the use of the command line in Microsoft Windows. Students have three hours to complete this portion of the Test -Out. An additional 30 minutes of the test out requires students to complete the physical disassembly and reassembly of a desktop computer. Students must achieve a 70% or greater on both sections of the Test-Out to be eligible to register for the Cyber Incident Response Course (CIRC). If the student fails to successfully complete the INCH Test-Out, they will have the opportunity to request registration in the one-week INCH-RES course offered at a later date.

Delivery: In-residence
Duration: 3 hours over 1 day
Prerequisite: None
Schedule offering:
INCH-TESTOUT-2312 (15 SEPT)

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 final, graded exam.

Delivery: Online
Duration: 40 hours of training over 4 weeks
Prerequisite: None
Schedule offering:
LXE-2310-OL (5-29 SEPT)

Network Intrusions Basics (NIB)

NIB is a 10-hour course that provides core knowledge needed to perform a network intrusion investigation. Students learn the language of intrusions and explore network fundamentals, including network architecture. The concepts presented in this course prepare students for additional network investigations courses. NIB contains two modules, each comprising two lessons, and a final, graded exam.

Delivery: Online asynchronous (Self-paced/no instructor)
Duration: Approximately 10 hours over 1 week
Prerequisite: None
Scheduled offerings:
NIB-2346-OL (5-11 SEPT)
NIB-2347-OL (11-18 SEPT)
NIB-2348-OL (18-25 SEPT)
NIB-2349-OL (25 SEPT – 2 OCT)

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-2304-OL (11-16 SEPT)

FY23 September 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-2304-OL (25-30 SEPT)

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+-2309 (11-16 SEPT)

Windows Forensic Examinations - EnCase (WFE-E)

WFE-E is a 40-hour course designed for students who wish to develop skills in conducting a computer forensic examination of digital devices and data including Defense Criminal Investigative Organizations (DCIOs). WFE-E instructs students in a comprehensive forensic examination process, including technical procedures and reporting. While students will use the EnCase forensic tool to conduct course examinations of Windows systems, the skills, processes, and techniques are applicable regardless of the tool a student will use in the field. WFE-E contains six modules and culminates with a final, graded exam.

Delivery: In-residence and Online
Duration: 40 hours of training over 1 week in-residence or over 4 weeks online
Prerequisite: CIRC
IACET CEU-eligible
Scheduled offering:
WFE-E-2312 (25-30 SEPT)
