



DC3 Cyber
Training
Academy

FY23 May 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 Fundamentals 100 (CF100)

CF100 is an 80-hour course that introduces students to hardware and software basics, operating systems, network architecture, and internet applications. It is the first installment of a two-part curriculum providing foundational cyber knowledge to cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include protecting DOD information systems from unauthorized and/or illegal access. The course contains three units comprising multiple lessons; each unit culminates in a unit Milestone Exam and the course ends with a Capstone Exam. A test-out option is available at the start of each unit so that qualified personnel may bypass portions of the course.

Delivery: Online asynchronous (Self-paced/no instructor)

Duration: 80 hours of training over 3 weeks

Prerequisite: None

Scheduled offering:

CF100-2310-OL (30 MAY – 16 JUN)

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 offerings:

CF200-2309-OL (8-26 MAY)

CF200-2310-OL (30 MAY – 16 JUN)



DC3 Cyber
Training
Academy

FY23 May 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-2312 (22 MAY – 2 JUN)

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:

CY101-2310-OL (30 MAY – 16 JUN)



FY23 May Offerings

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-2303-OL (22 MAY – 22 JUN)

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 offerings:

INCH-RES-2310 (8-12 MAY)

INCH-RES-2311 (22-26 MAY)

Please note that INCH Test Out options are available.



FY23 May Offerings

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-2308](#) (5 MAY)

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-2306-OL](#) (8 MAY – 1 JUN)



FY23 May Offerings

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-2328-OL (1-5 MAY)

NIB-2329-OL (8-12 MAY)

NIB-2330-OL (15-19 MAY)

NIB-2331-OL (22-26 MAY)

NIB-2332-OL (30 MAY – 2 JUN)

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-2302-OL (15-19 MAY)



DC3 Cyber
Training
Academy

FY23 May Offerings

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: In-residence

Duration: Approximately 40 hours over 1 week

Prerequisite: None

Scheduled offering:

[NTC-2304](#) (1-5 MAY)

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-2302-OL](#) (8-12 MAY)
