



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:

CF100-2414-OL (15 JUL – 2 AUG)

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:

CF200-2414-OL (15 JUL – 2 AUG)



FY24 July Offerings

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:

CY101-2414-OL (15 JUL – 2 AUG)

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), Department of Defense (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 final, graded exam.

Delivery: In-residence

Duration: 80 hours of training over 2 weeks

Prerequisite: NIB and WFE-E

IACET CEU-eligible, ACE Recommendation

Scheduled Offering:

FIWE-2405 (8-19 JUL)



FY24 July 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-2407-OL (22 JUL – 22 AUG)

Introduction to Networks and Computer Hardware (INCH) OL/ILV

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 or Instructor-Led Virtual

Duration: Online is 40 hours of training over 4 weeks

Instructor-Led Virtual is 40 hours of training over 5 days

Prerequisite: None

IACET CEU-eligible, ACE Recommendation

Scheduled offerings:

INCH-2431-OL (8 JUL – 1 AUG)

INCH-2432-OL (8 JUL – 1 AUG)



FY24 July 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

Scheduled offering:

INCH-TESTOUT-2410 (19 JUL)

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

Scheduled offerings:

LXE-2409-OL (8 JUL – 1 AUG)



FY24 July Offerings

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-2405-OL (1-5 JUL)

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-2404-OL (8-12 JUL)



FY24 July Offerings

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+-2406 (15-19 JUL)

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+-2406 (29 JUL – 2 AUG)

Windows Forensic Examinations (WFE)

WFE provides training that enables professionals to conduct digital analysis of Windows systems in a forensically reliable manner. Building on the foundation of the Cyber Incident Response Course (CIRC), this course introduces best practices and relevant technical aspects of Windows forensic examinations. The course immerses students in mini-scenarios that escalate in difficulty, allowing them to practice and reinforce what they have learned while using trusted forensic tools, and provides a longform practice that prepares students for the Capstone Exam.

Delivery: In-residence

Duration: 80 hours of training over 2 weeks in-residence

Prerequisite: CIRC

Scheduled offering:

WFE-2406 (29 JUL – 9 AUG)
