



**DC3** Cyber  
Training  
Academy

## FY25 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 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:**

CF200-2508-OL (5-23 MAY)

CF200-2509-OL (27 MAY – 13 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:**

CY101-2508-OL (5-23 MAY)

CY101-2509-OL (27 MAY – 13 JUN)

---



**DC3** Cyber  
Training  
Academy

## FY25 May Offerings

### **Dark Web Activities (DWA)**

Dark Web Activities (DWA) introduces key concepts and tools for navigating and using the web, with a focus on identifying and tracking illegal activities and documenting findings. It distinguishes between the deep web and dark web, explaining their unique features and components. The course covers the essential technologies and tools used for accessing and navigating the dark web, as well as techniques for tracking illegal activities such as cyber crime, drug trafficking, and fraud.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**Prerequisite:** None

**Scheduled offering:**

[DWA-2508](#) (19-23 MAY)

---

### **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-2515-OL](#) (27 MAY – 19 JUN)

[INCH-2516-OL](#) (27 MAY – 19 JUN)

---



## FY25 May Offerings

### 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-2506](#) (19-23 MAY)

*Please note that INCH Test Out options are available.*

[INCH-TESTOUT-2503](#) (9 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

**Scheduled offerings:**

[LXE-2507-OL](#) (27 MAY – 19 JUN)

---



**DC3** Cyber  
Training  
Academy

## FY25 May Offerings

### Network + (NET+)

NET+ is a bootcamp-style course that builds on your existing user-level knowledge and experience with computer operating systems and networks so you can master the fundamental skills and concepts needed for success in any networking career. Students are taught to describe the major networking technologies and systems of modern networks and configure, manage, and troubleshoot modern networks. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included.

**Delivery:** In-residence

**Duration:** Approximately 40 hours over 1 week

**Prerequisite:** None

**Scheduled offering:**

[NET+-2504](#) (12-16 MAY)

---

### 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+-2505](#) (12-16 MAY)

---



**DC3** Cyber  
Training  
Academy

## FY25 May Offerings

### **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-2506](#) (5-16 MAY)

---