DC3 Cyber Training Academy

FY24 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-2406 (23 SEPT – 4 OCT)

---

### 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:**
CF100-2417-OL (30 SEPT – 18 OCT)

---

### 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:**
CF200-2417-OL (30 SEPT – 18 OCT)

---

### 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:**
CY101-2417-OL (30 SEPT – 18 OCT)

---

DC3 Cyber Training Academy

# FY24 September 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-2408-OL (23 SEPT – 24 OCT)

---

## 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-2435-OL (23 SEPT – 17 OCT)
INCH-2436-OL (23 SEPT – 17 OCT)

---

DC3 Cyber Training Academy

# FY24 September 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-2414 (30 SEPT – 4 OCT)

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

---

## 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-2407-OL (23 SEPT – 24 OCT)

---

DC3 Cyber Training Academy

# FY24 September 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 final, graded exam.

**Delivery:** Online
**Duration:** 40 hours of training over 4 weeks
**Prerequisite:** None
**Scheduled offerings:**
LXE-2411-OL (23 SEPT – 17 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-2406-OL (9-13 SEPT)

---

### 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-2407 (16-20 SEPT)

---

### 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-2405-OL (3-6 SEPT)

---

### 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-2412 (30 SEPT – 11 OCT)