



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.

A+ (A+)

A+ course is the industry standard for launching IT careers. In this bootcamp-style course, students install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. A+ is designed for individuals with basic computer user skills who are interested in obtaining a job as an entry-level IT technician. It is also designed for students seeking the CompTIA A+ certification who want to prepare for the CompTIA's A+ Core 1 (220-1001) and Core 2 (220-1002) certification exams. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included with this course.

Delivery: In-residence

Duration: 40 hours of training over 1 week

CompTIA CEU-eligible

Prerequisite: None

Scheduled offering:

A+-2501 (9-13 DEC)

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:

CF200-2502-OL (2-20 DEC)



DC3 Cyber
Training
Academy

FY25 December 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:

CY101-2503B-OL (16 DEC – 3 JAN)

Cybersecurity Analyst (CySA+)

Cybersecurity Analyst (CySA+) is a bootcamp-style course that teaches incident detection, prevention, and response through continuous security monitoring for success in a high-stakes analysis. Students learn processes in security operations, vulnerability management, incident response and management, and how to apply best practices for reporting and communication. Vouchers are not included.

Delivery: In-residence

Duration: 40 hours of training over 1 week

Prerequisite: None

Scheduled Offering:

CySA+-2503 (16-20 DEC)



FY25 December 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-2502 (2-6 DEC)

Please note that INCH Test Out options are available.

INCH-TESTOUT-2501 (20 DEC)

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-2502-OL (9 DEC – 9 JAN)



FY25 December Offerings

Linux+ (Linux+)

The Computing Technology Industry Association's (CompTIA) Linux+ proves you have the skills administrators need to secure the enterprise, power the cloud, and keep systems running. This bootcamp-style course covers an evolving job role that focuses more on how Linux powers the cloud. Students will review cutting edge technologies that help automate and orchestrate business processes, including infrastructure as code and containers. Vouchers are not included.

Delivery: In-residence

Duration: 40 hours of training over 1 week

Prerequisite: None

Scheduled Offering:

[Linux+-2502 \(2-6 DEC\)](#)

Mac Forensics (MACF)

The Mac Forensics (MACF) course focuses on conducting digital investigations of Macintosh operating systems (macOS) and iPhone operating systems (iOS) in a forensically sound manner. It builds on the foundation of the Forensics Intrusions in a Windows Environment course and introduces best practices and relevant technical aspects of macOS forensic examinations and incident response. It includes scenarios that build upon each other so students can practice what they learn using trusted forensic tools

Delivery: In-residence

Duration: 40 hours of training over 1 week

Prerequisite: None

Scheduled offerings:

[MACF-2502 \(16-20 DEC\)](#)



FY25 December 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-2501-OL (9-13 DEC)

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-2502 (2-6 DEC)



FY25 December 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-2501-OL \(2-6 DEC\)](#)

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-2502 \(2-13 DEC\)](#)
