DC3 Cyber Training Academy

FY24

2024 Course Catalog

MISSION

To provide cyber training to individuals and Department of Defense (DoD) elements that must ensure Defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities.

About

Established in 1998, the Academy has its headquarters and main in-residence training facility in Hanover, Maryland. A rigorous Academy curriculum provides DoD personnel with the relevant knowledge and cutting-edge skills they need to meet mission goals. Students can access courses five ways: in-residence, instructor-led virtual, online scheduled, on-demand, or through mobile training units in a variety of locations in the United States and abroad. The Academy operates under the DoD Reform Initiative Directive 27.

What We Offer

The Academy provides training in more than a dozen courses—ranging from computer basics to network intrusions and cyber analysis—designed to meet the evolving needs of students. In addition, the Academy offers training in modern cybersecurity tools such as OpenVAS and Network Mapper.

Students who pass these courses receive course completion certificates. In addition, the Academy offers three DoD certifications, widely recognized as validations of competency in digital forensic skills, to students who pass required combinations of courses: Digital Media Collector (DMC), Digital Forensic Examiner (DFE), and Cyber Crime Investigator (CCI).

Registrar Contact Information

Website: learn.dcita.edu
Phone: 443-733-1990
Email: DC3.CTA.Registrar@us.af.mil
Office Hours: Monday-Friday, 8:00 am-4:30 pm ET

Help Desk Contact Information

Email: help@dcita.edu
Phone: 443-733-1910

Accreditations

The Academy has earned national recognition for its excellence in cyber training from these organizations:

American Council on Education (ACE)
ACE provides college credit recommendations for a select number of Academy courses.

Council on Occupational Education (COE)
COE is the Academy's main accreditor, assuring quality and integrity in career and technical education.

International Accreditors for Continuing Education and Training (IACET)
The Academy, which IACET has recognized for its excellence in institutional practices, is an authorized provider of IACET Continuing Education Units (CEUs).

Training Delivery Methods

In-Residence (RES)
Classes are taught on-site at the state-of-the-art Academy in Hanover, Maryland.

Instructor-Led Virtual (ILV)
This is synchronous, instructor-led learning, which offers the convenience of online delivery. Students log in each day, while instructors present course materials and exercises, communicate with students, and answer questions in real time.

Mobile Training Team (MTT)
These courses are taught in-residence at an off-site location. Instructors and equipment are mobilized within the U.S. or internationally for training delivery.

Online Scheduled
Delivered via DC3 CTA Cyber Learning Management Environment (LMS), classes are self-paced. Students log in and work when it is convenient within the scheduled course time frame.

On-Demand
Delivered in the DC3 CTA Cyber Learning Management Environment (LMS), on-demand classes are available for students to begin and complete at their convenience.

[v. 2401]

Core Offerings

A+
A+ (CompTIA)
CT · NP · RES

CF100
Cyber Fundamentals 100
NP · OL

CF200
Cyber Fundamentals 200
NP · OL

CY101
Cyber 101
NP · OL

ICI
Introduction to Cyber Investigations
ACE · NP · OL

INCH
Introduction to Networks and Computer Hardware
ACE · IACET · NP · ILV · OL · RES

NET+
Network+ (CompTIA)
CT · NP · RES

NIB
Network Intrusion Basics
NP · OL

NMAP
Network Mapper
OL

OPV
OpenVAS
NP · OL

Intermediate Offerings

AO
Authorizing Official
NP · OL

CAC
Cyber Analyst Course
ILV · RES

CIRC
Cyber Incident Response Course
ACE · IACET · RES

CySA+
Cybersecurity Analyst (CompTIA)
CT · RES

FIWE
Forensics and Intrusions in a Windows Environment
ACE · IACET · ILV · RES

LA
Log Analysis
ACE · IACET · OL · RES

LXE
Linux Essentials
NP · OL · RES

NTC
Network Traffic Collection
ILV · RES

PenTest+
Penetration Testing (CompTIA)
CT · RES

SEC+
Security+ (CompTIA)
CT · RES

TEDA
Technology Evidence in Domestic Abuse
NP · OL

WFE
Windows Forensic Examinations
IACET · RES

Digital Media Collector (DMC) — INCH > CIRC
Digital Forensic Examiner (DFE) — INCH > CIRC > WFE
Cyber Crime Investigator (CCI)* — INCH > CIRC > WFE > FIWE (with CI/LE badge)

NP No Prerequisites
RES In-Residence
ILV Instructor-Led Virtual
OL Online

ACE American Council on Education Credit Recommendation
CT Eligible for CompTIA CEUs
IACET Eligible for IACET CEUs

*ARMY MI/ARMY INSCOM students must have credentials verified by CDTI Training Program Manager before being eligible for certification.
*ARMY CID (USACIDC) students must have credentials verified by organizational POC before being eligible for certification.

DOD CERTIFICATES

To effectively counter ever-evolving cybersecurity threats, the Academy developed three learning paths to assist law enforcement personnel who are working toward a specific job role: Digital Media Collector (DMC), Digital Forensic Examiner (DFE) or Cyber Crime Investigator (CCI).

Digital Media Collector (DMC)

Duration*:
2-4 Months

INCH › CIRC ✓

Digital Forensic Examiner (DFE)

Duration:
3-4 Months

INCH › CIRC › WFE ✓

Cyber Crime Investigator (CCI)**

Duration:
4-6 Months

INCH › CIRC › WFE › FIWE ✓

*Duration is based on suggested time that includes completing a course, applying it at work, and returning to take the next course in the pipeline.
**ARMY MI/ARMY INSCOM students must have credentials verified by CDTI Training Program Manager before being eligible for certification.
**ARMY CID (USACIDC) students must have credentials verified by organizational POC before being eligible for certification.

INTERNATIONAL CYBER FORENSICS COURSE

The ICF course provides students with the solid working knowledge necessary to conduct incident response and digital forensics of digital media. This is a five-week course with 200 hours of instruction and more than 90 hours of hands-on training and activities. The component courses of Introduction to Networks and Computer Hardware (INCH), Cyber Incident Response Course (CIRC), Windows Forensic Examinations - EnCase (WFE-E), and Forensics and Intrusions in a Windows Environment (FIWE) are individually available to partner nations.

ICF Course Map

Duration:

5 weeks / 25 days, 200 hours of instruction

Delivery Methods:

In-Residence

Mobile Training Team (MTT)

Course Objectives

- Identify hardware components in a computer system
- Employ operating system tools to manage disks, partitions, and file systems
- Explain basic theory, technologies, and components that facilitate network data transmission
- Demonstrate how to handle digital media effectively when responding to an incident
- Generate a detailed and accurate account of a network intrusion
- Analyze network-based evidence
- Explain how to conduct a lawful network investigation

Table of Contents

A+

A+ (CompTIA)

COURSE DESCRIPTION

The Computing Technology Industry Association's (CompTIA) 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. The Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location. Please note that we do have a convenient Pearson VUE Mobile Testing Center on-site. For more details on how to use our testing center, please refer to page 29 of the course catalog.

COURSE DETAILS

Difficulty:
Core

Delivery:
In-Residence
40 hours over 5 days

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible

COURSE OBJECTIVES

- Install and configure PC system unit components and peripheral devices
- Install, configure, and troubleshoot display, multimedia devices, storage devices, print devices, and internal system components
- Install, configure, and maintain operating systems
- Maintain and troubleshoot Microsoft Windows
- Explain network infrastructure concepts
- Configure and troubleshoot network connections
- Manage users, workstations, and shared resources
- Implement client virtualization, cloud computing, physical security, and operational procedures
- Secure workstations, data, and troubleshoot security issues

AO

Authorizing Official

COURSE DESCRIPTION

This comprehensive program trains professionals before they assume Authorizing Official (AO) duties and provides Designated Representatives (AODRs) with a better understanding of the AO work role. Because AO work settings vary widely, this course concentrates on risk management and cybersecurity discipline areas that apply to all environments, rather than focusing on detailed technical content. The training emphasizes core concepts and principles, as well as best practices for technology risk management. The course uses an experiential learning model with realistic scenarios to support principle-based knowledge acquisition.

COURSE OBJECTIVES

- With the use of references, the student will evaluate and apply relevant laws, policies, and the evolving standards that inform the RMF process.
- Given an AO package, the student will analyze the degree to which an organization's mission and systems are aligned.
- Given an AO package, the student will evaluate security and risk assessments, mitigation strategies and controls, and other information needed to make a risk-based authorization decision.
- Given a specific part of an AO package, the student will evaluate mission need against risk to render an authorization decision.
- Given an entire AO package, the student will determine the acceptable level of risk to render an authorization decision.
- With the use of resources, the student will create and maintain an ongoing review of existing ATOs.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
On-Demand
8 hours

Prerequisites:
None

Accreditations:
None

CAC

Cyber Analyst Course

COURSE DESCRIPTION

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.

COURSE OBJECTIVES

- Review multiple reports containing relevant artifacts using basic cyber analysis techniques
- Analyze electronic artifacts in existing forensic and information reports
- Analyze basic data contained in text-based and binary logs
- Develop charts to visualize relevant data
- Develop information from internet-based resources while maintaining anonymity
- Classify network intrusions and malicious code types
- Investigate network traffic and explain network monitoring concepts

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
80 hours over 10 days

Instructor-Led Virtual
80 hours over 10 days

Prerequisites:
INCH

Accreditations:
None

CF100

Cyber Fundamentals 100

COURSE DESCRIPTION

Cyber Fundamentals 100 (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 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.

COURSE OBJECTIVES

- Disassemble a personal computer (PC) virtually and assemble it to an operational status to demonstrate both conceptual and procedural knowledge of physical computer components and architectures
- Differentiate between the basic features, functions, and requirements of commonoperating systems
- Select the type of data transmissions for the appropriate networking protocol to establish a computer network
- Summarize basic internet applications and potential vectors of intrusion

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
80 hours over 3 weeks

Prerequisites:
None

Accreditations:
None

CF200

Cyber Fundamentals 200

COURSE DESCRIPTION

Cyber Fundamentals 200 (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 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 course ends with a Capstone Exam. There is a test-out option available to permit qualified personnel to bypass the course.

COURSE OBJECTIVES

- Differentiate between the basic administrative concepts, structure, and internal processes of Windows and Linux operating systems
- Select the type of data transmissions for the appropriate networking protocol to manage an established network
- Determine the best cybersecurity defense practices to meet common security standards

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
80 hours over 3 weeks

Prerequisites:
None

Accreditations:
None

CIRC

Cyber Incident Response Course

COURSE DESCRIPTION

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 six module quizzes and a course Final Exam.

COURSE OBJECTIVES

- Deduce relevant information from an initial phone call and build a responder toolkit in preparation for an incident response
- Use best practices to respond to a forensic incident and assume control of the environment
- Collect forensic images from a live system
- Collect data during an active intrusion
- Create a bit-for-bit image of a digital media device
- Create a forensic image of various mobile devices
- Describe best practices used to package, track, transport, and store evidence

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
80 hours over 10 days

Prerequisites:
INCH

Accreditations:
ACE Recommended
Course 3 Semester Hours
Lower-Division

IACET CEU-eligible
4.0 CEUs

CY101

Cyber 101

COURSE DESCRIPTION

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.

COURSE OBJECTIVES

- Choose the correct location of the devices within a computer network
- Implement one layer (such as malware) of the appropriate operational security (OPSEC) policy
- Categorize types of attack methods, targets, and vulnerabilities
- Select the appropriate national and international laws, regulations, policies, and ethics that relate to cybersecurity
- Select risk management strategies that minimize risk, implement controls, and accept residual risk

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
40 hours over 3 weeks

Prerequisites:
None

Accreditations:
None

CySA+

Cybersecurity Analyst (CompTIA)

COURSE DESCRIPTION

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. The Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location. Please note that we do have a convenient Pearson VUE Mobile Testing Center on-site. For more details on how to use our testing center, please refer to page 29 of the course catalog.

COURSE OBJECTIVES

- Improve processes in security operations and differentiate between threat intelligence and threat hunting concepts; identify and analyze malicious activity using the appropriate tools and techniques
- Implement and analyze vulnerability assessments, prioritize vulnerabilities and make recommendations on mitigating attacks and vulnerability response
- Apply updated concepts of attack methodology frameworks, perform incident response activities and understand the incident management lifecycle
- Apply communication best practices in vulnerability management and incident response as it relates to stakeholders, action plans, escalation and metrics

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
40 hours over 5 days

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible

FIWE

Forensics and Intrusions in a Windows Environment

COURSE DESCRIPTION

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), 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.

COURSE OBJECTIVES

- Explain how to conduct a lawful network investigation
- Generate a detailed and accurate account of a network intrusion
- Analyze network-based evidence
- Analyze host-based evidence

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
80 hours over 10 days

Instructor-Led Virtual
80 hours over 10 days

Prerequisites:
NIB and WFE/WFE-E

Accreditations:
ACE Recommended
Course 5 Semester Hours
Upper-Division

IACET CEU-eligible
4.0 CEUs

*ARMY MI/ARMY INSCOM students must have credentials verified by CDTI Training Program Manager before being eligible for certification.
*ARMY CID (USACIDC) students must have credentials verified by organizational POC before being eligible for certification.

ICI

Introduction to Cyber Investigations

COURSE DESCRIPTION

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.

COURSE OBJECTIVES

- Explain and define the scope and nature of cyber investigations
- Perform the collection and analysis of evidence in cyber investigations
- Prepare a subpoena and explain the legal fundamentals of cyber investigations
- Explain the role of cyber forensic laboratories in investigations
- Explain the different investigation methods among the military, civilians, corporate entities, and other countries and the available resources for each

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
40 hours over 5 weeks

Prerequisites:
None

Accreditations:
ACE Recommended
Course 3 Semester Hours
Lower-Division

INCH-RES

Introduction to Networks and Computer Hardware

COURSE DESCRIPTION

Introduction to Networks and Computer Hardware (INCH-RES) 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 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 contains 10 modules and culminates in a Capstone Exam. A test-out option is available to permit qualified personnel to bypass the course.

COURSE OBJECTIVES

- Disassemble and reassemble a computer system so that it is able to boot up to an operating system
- Establish a functional virtual machine that boots to an operating system
- Manipulate files and folders using the Windows command line to respond to a scenario with required actions
- Manipulate files and folders using Linux command-line tools to respond to a scenario with required actions
- Effect system changes using Linux command-line tools

NOTE

For LE/CI personnel to be eligible for certification, they must take and pass the in-residence version of the course.

COURSE DETAILS

Difficulty:
Core

Delivery:
In-Residence
40 hours over 5 days

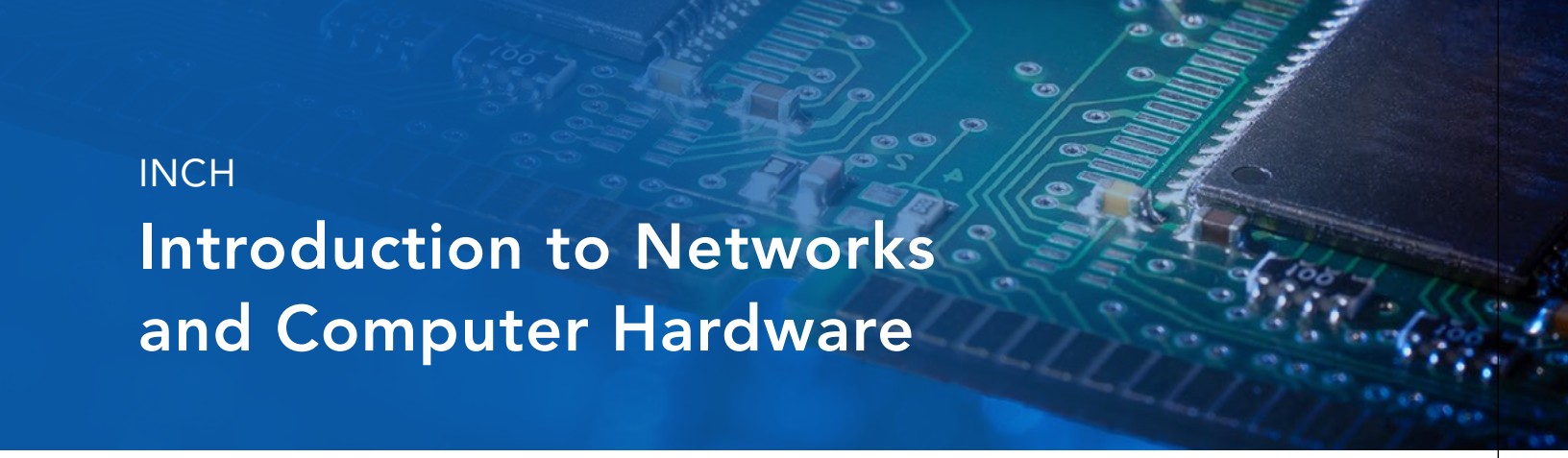
Prerequisites:
None

Accreditations:
None

INCH TEST OUT

INCH Test Out provides students with the opportunity to demonstrate mastery of both the content knowledge portion of the course material and a hands-on desktop computer disassembly and reassembly.

Test Out Delivery:
In-Residence
3 hours over 1 day



INCH

Introduction to Networks and Computer Hardware

COURSE DESCRIPTION

Introduction to Networks and Computer Hardware (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. A test-out option is available to permit qualified personnel to bypass the course.

COURSE OBJECTIVES

- Identify hardware components in a computer system
- Explain the functions of computer hardware where data is stored, including hard drives, removable media, random-access memory, and the central processing unit
- Employ operating system tools to manage disks, partitions, and file systems
- Perform domain management and administrative tasks using Windows Server Active Directory and Group Policy tools
- Explain basic theory, technologies, and components that facilitate network data transmission
- Configure a system to be able to communicate on a network
- Perform basic computer troubleshooting
- Perform basic computer tasks using Windows
- Explain methods to implement basic computer and network security

NOTE

For LE/CI personnel to be eligible for certification, they must take and pass the in-residence version of the course.

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
40 hours over 4 weeks

Instructor-Led Virtual
40 hours over 5 days

Prerequisites:
None

Accreditations:
ACE Recommended
Course 3 Semester Hours
Lower-Division

IACET CEU-eligible
4.0 CEUs

LA

Log Analysis

COURSE DESCRIPTION

Log Analysis (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.

COURSE OBJECTIVES

- Explain log analysis methodology
- Explain the benefits of log analysis in an intrusion investigation
- Analyze and evaluate log files
- Perform the extraction of information from log files
- Arrange log file data

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
50 hours over 5 days

Online Scheduled
50 hours over 5 weeks

Prerequisites:
NIB

Accreditations:
ACE Recommended
Course 5 Semester Hours
Upper-Division

IACET CEU-eligible
4.0 CEUs

LXE

Linux Essentials

COURSE DESCRIPTION

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.

COURSE OBJECTIVES

- All course learning objectives are as defined by the Linux Professional Institute (LPI) for their Linux Essentials exam.

COURSE MATERIALS

- This course uses the textbook *Linux Essentials*, 2nd edition, by Christine Bresnahan and Richard Blum (ISBN-13: 978-1119092063)

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
40 hours over 5 days

Online Scheduled
40 hours over 4 weeks

Prerequisites:
None

Accreditations:
None

NET+

Network+ (CompTIA)

COURSE DESCRIPTION

Network+ (NET+, CompTIA) is a bootcamp-style course that builds on students' existing user-level knowledge and experience with computer operating systems and networks so they 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. The Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location. Please note that we do have a convenient Pearson VUE Mobile Testing Center on-site. For more details on how to use our testing center, please refer to page 29 of the course catalog.

COURSE DETAILS

Difficulty:
Core

Delivery:
In-Residence
40 hours over 5 days

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible

COURSE OBJECTIVES

- Explain the OSI and TCP/IP models
- Explain properties of network traffic
- Install and configure switched networks
- Configure IP networks, monitor ports and protocols
- Install and configure routed networks
- Explain network application and storage issues
- Monitor and troubleshoot networks
- Explain network attacks and mitigations
- Install and configure security devices
- Explain authentication and access controls
- Deploy and troubleshoot cabling solutions
- Implement and troubleshoot wireless technologies
- Compare and contrast WAN technologies
- Use remote access methods
- Identify site policies and best practices

NIB

Network Intrusions Basics

COURSE DESCRIPTION

Network Intrusions Basics (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.

COURSE OBJECTIVES

- Classify network intrusion elements
- Give examples of artifacts related to network intrusions
- Explain the basics of networking and network architecture

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
10 hours over 7 days

Prerequisites:
None

Accreditations:
None

NMAP

Network Mapper

COURSE DESCRIPTION

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.

COURSE OBJECTIVES

- Install Nmap in a Windows and Linux environment
- Determine what hosts, ports, and services are available on a network
- Determine what operating systems, applications, and devices are running on a network

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
8 hours over 5 days

Prerequisites:
INCH

Accreditations:
None

NTC

Network Traffic Collection

COURSE DESCRIPTION

Network Traffic Collection (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 DoD cyber-intrusions investigators, information assurance professionals, prospective lab examiners, and military intelligence and 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.

COURSE OBJECTIVES

- Explain basic theory, technologies, and components that facilitate network data transmission
- Examine network traffic and previously captured data
- Perform a logical and physical assessment of a network to identify potential witness devices and the data they contain
- Assess a network and configure and place a network monitoring sensor
- Configure network data acquisition tools
- Use common internet research utilities
- Explain a network monitoring system in a wireless environment
- Analyze network traffic and system artifacts to identify probing and intrusion techniques

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
40 hours over 5 days

Instructor-Led Virtual
40 hours over 5 days

Prerequisites:
CIRC

Accreditations:
None

OPV

OpenVAS

COURSE DESCRIPTION

OpenVAS (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.

COURSE OBJECTIVES

- Install OpenVAS software successfully in a Linux environment
- Run an OpenVAS "quick start" vulnerability scan utilizing the Greenbone Security Assistant interface
- Configure the target, parameters, and breadth of an OpenVAS custom vulnerability scan based on a scenario
- Assess the vulnerability risks to a system and possible remediation based on the results of an OpenVAS report generated from a custom vulnerability scan

COURSE DETAILS

Difficulty:
Core

Delivery:
Online Scheduled
8 hours over 5 days

Prerequisites:
None

Accreditations:
None

PenTest+

Penetration Testing (CompTIA)

COURSE DESCRIPTION

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. The Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location. Please note that we do have a convenient Pearson VUE Mobile Testing Center on-site. For more details on how to use our testing center, please refer to page 29 of the course catalog.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
40 hours over 5 days

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible

COURSE OBJECTIVES

- Includes updated techniques emphasizing governance, risk and compliance concepts, scoping and organizational/customer requirements, and demonstrating an ethical hacking mindset
- Includes updated skills on performing vulnerability scanning and passive/active reconnaissance, vulnerability management, as well as analyzing the results of the reconnaissance exercise
- Includes updated approaches to expanded attack surfaces, researching social engineering techniques, performing network attacks, wireless attacks, application-based attacks and attacks on cloud technologies, and performing post-exploitation techniques

SEC+

Security+ (CompTIA)

COURSE DESCRIPTION

Security+ (SEC+, CompTIA) is a bootcamp-style course that will be a significant part of a student's preparation to pass the CompTIA Security+ (Exam SY0-601) certification examination. The CompTIA SEC+ certification will help build a student's cybersecurity skill set to confidently perform duties in any entry-level security role. The Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location. Please note that we do have a convenient Pearson VUE Mobile Testing Center on-site. For more details on how to use our testing center, please refer to page 29 of the course catalog.

COURSE OBJECTIVES

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls, and identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions
- Explain data privacy and protection concepts
- Perform incident response and digital forensics

COURSE DETAILS

Difficulty:
Core

Delivery:
In-Residence
40 hours over 5 days

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible

TEDA

Technology Evidence in Domestic Abuse

COURSE DESCRIPTION

Technology Evidence in Domestic Abuse (TEDA) is a 90-minute course that provides first responders an overview of the role that technology can play in domestic abuse and violence cases. TEDA introduces critical concepts on the intersection of technology and domestic abuse and violence, including how abuse manifests, underlying dynamics of abuse, signs of escalation, relevant UCMJ articles, DoD policies, and industry best practices for the collection of digital evidence.

COURSE OBJECTIVES

- Describe the fundamentals of domestic abuse and provide examples of abuse tactics through technology (for example, a threatening text; spoofing; hacking into IoT devices or victim email, social media accounts)
- Categorize abuser behaviors, including with technology, that indicate increased risk of escalation and violence (for example, cyberstalking)
- Select the applicable military law and DoD policy concerning abuse
- Evaluate a situation and perform necessary actions in accordance with best practices

COURSE DETAILS

Difficulty:
Core

Delivery:
On-Demand
90 minutes over 3 days

Prerequisites:
None

Accreditations:
None

WFE

Windows Forensic Examinations

COURSE DESCRIPTION

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 long-form practice that prepares students for the Capstone Exam.

COURSE OBJECTIVES

- Conduct a forensic examination of an image of the Windows operating system in a forensically sound (repeatable, documented, and non-destructive) manner
- Choose the basic functions, configurations, outputs, tools and settings that need to be adjusted when conducting a forensic examination of a Windows operating system
- Examine a forensic image from a Windows computer using basic forensic processes and automated tools
- Use tools and a repeatable, documented process to gain access to protected files
- Produce documentation that completely and accurately summarizes all forensic actions taken on the machine

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
80 hours over 10 days

Prerequisites:
CIRC

Accreditations:
IACET CEU-eligible
4.0 CEUs

PVTC

Pearson VUE Testing Center

DESCRIPTION

The DC3 Cyber Training Academy is equipped with a state-of-the-art Pearson VUE Testing Center, which is available for students to use after one of the CompTIA Bootcamps. Students who have taken the equivalent CompTIA Certification Exam after one of the bootcamps have seen an impressive 80% certification pass rate. This is because our bootcamps are taught by instructors who are certified in all the CompTIA courses we offer and they can provide specific knowledge to help students successfully pass the certification exam(s). Please continue to check the course calendar for upcoming and new CompTIA courses and certifications. Students who have taken a bootcamp elsewhere and need to take a certification exam may utilize our center as long as they have a paid voucher.

DETAILS

Difficulty:
Core - Intermediate

Delivery:
In-Residence

Duration:
Exams range from 90 to 165 minutes, depending on the certification

Prerequisites:
None

HOW TO USE THE CENTER

- Attend one of the scheduled CompTIA "bootcamp" courses and test the last day of class (normally Friday mornings)
- Purchase a valid voucher in advance; **CTA does not provide any testing vouchers**
- Email the Registrar at DC3.CTA.Registrar@us.af.mil and ask to test on a week when there is a CompTIA course in session (you do not have to attend the scheduled "bootcamp" to test that Friday)

CURRENT COMPTIA OFFERINGS

- A+
- Cybersecurity Analyst (CySA+)
- Network+ (NET+)
- Penetration Testing (PenTest+)
- Security+ (SEC+)

CYB

CyberCasts

DESCRIPTION

CyberCasts are on-demand, streaming-video, microlearning modules created by Academy subject matter experts (SMEs) and instructors. They are designed to enhance a student's learning experience at the Academy and to give an opportunity to earn Continuing Education Units (CEUs). Most Academy CyberCasts are between 1 and 2 hours in length and can be viewed at any time. The Academy offers a catalog of over 200 CyberCasts on a wide range of topics.

QUICK STATS

200+
CYBERCASTS

167,101
TOTAL VIEWS

118,541
CREDIT HOURS

TOPICS COVERED

Networking | Hardware | IoT | Vulnerabilities | Security | Risk Mitigation | Log Analysis | Emerging Threats | Tool Tutorials | System Administration | Digital Forensics

To view a full list of available CyberCasts, visit learn.dcita.edu.

DETAILS

Difficulty:
Basic - Advanced

Delivery:
On-Demand Video
1 to 2 hours

Prerequisites:
None

Accreditations:
CompTIA CEU-eligible for

- A+
- CASP+
- Cloud+
- CySA+
- DataSys+
- Linux+
- Network+
- PenTest+
- Security+

DC3 Cyber Training Academy Policies And Process

FOR ALL NON-SCHOOL-RELATED ISSUES

Students should use their military chain of command through their service's detachment leadership.

FOR ALL SCHOOLHOUSE-RELATED ISSUES

Students should follow the process described below: Most student complaints/grievances can be resolved informally by discussing the matter with the instructor. If a student's complaint cannot be resolved informally by working with the instructor, the student may submit a written description of the issue, along with supporting documentation (if applicable) to the CTA Registrar (DC3.CTA.Registrar@us.af.mil).

DC3 Cyber Training Academy will examine the submission, consult with the DC3 CTA Student Engagement government representative, and provide an appropriate response and a written description of the resolution.

If the response is not satisfactory to the student, the student may petition the DC3 Cyber Training Academy Director for review and/or possible investigation.

The DC3 Cyber Training Academy Director would then examine the submission and provide an appropriate response and a written description of the resolution. All decisions by the DC3 Cyber Training Academy Director are final.

While the appeals and grievance decisions of the Academy are final, students may inform our accrediting agency, the Council on Occupational Education (COE), if they feel their issues are not satisfactorily resolved.

For information on the Academy's behavior and conduct standards, please review the Standards of Behavior and Conduct Standard Operating Procedure.

CONTACT

CTA Registrar
Monday-Friday,
8:00 am-4:30 pm ET
DC3.CTA.Registrar@us.af.mil
443-733-1990

Council on Occupational Education (COE)
7840 Roswell Road
Building 300, Suite 325
Atlanta, GA 30350
800-917-2081

DC3 Cyber Training Academy

CONTACT

learn.dcita.edu
443-733-1990
DC3.CTA.Registrar@us.af.mil

ADDRESS

DC3 Cyber Training Academy
7740 Milestone Parkway, Suite 400
Hanover, MD 21076