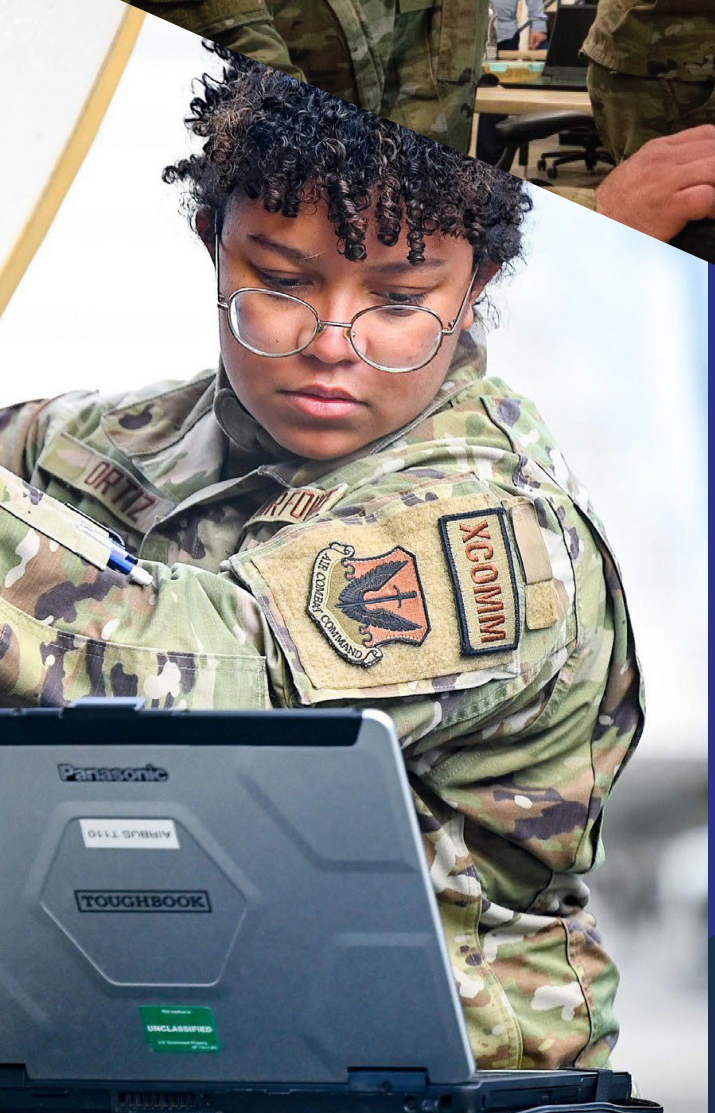


DC3 CYBER TRAINING ACADEMY

FY26

2026 Course Catalog

Mission

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

About

Established in 1998, the DC3 Cyber Training Academy has its headquarters and main in-residence training facility in Columbia, Maryland. A rigorous Academy curriculum provides DoW personnel with the relevant knowledge and cutting-edge skills they need to meet mission goals. Students can access courses four ways: in-residence, instructor-led virtual, on-demand, or through mobile training teams in a variety of locations in the United States and abroad. The Academy operates under the DoD Reform Initiative Directive 27.

What The Academy Offers

The DC3 Cyber Training Academy provides training in more than 30 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 six DoW certificates, widely recognized as validations of competency in digital forensic skills, malware analysis, and cyber activities to students who pass required combinations of courses.

For more information, please refer to DoW Certificates on page 6 of the course catalog.

Registrar Contact Information

Website: learn.dcita.edu
Phone: 443-545-3055
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: 833-844-7318

Accreditations

The DC3 Cyber Training 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 DC3 Cyber Training Academy in Columbia, Maryland.

Instructor-Led Virtual (ILV)
Classes are taught through interactive, instructor-led virtual sessions, with instructors available on-screen for the duration of the course.

On-Demand
Delivered in the DC3 Cyber Training Academy learning management system (LMS), on-demand classes are available for students to begin and complete at their convenience.

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.

[v. 2602]
Pub. Date 06 MAY 2026

Basic Offerings

Recommended Experience in the Field: 0-3 years

Designed for entry-level professionals, courses at the DC3 Cyber Training Academy's Basic level are best suited for those with a basic understanding of fundamental cybersecurity concepts and technologies, or more experienced learners looking to broaden their capabilities. Before attending any Basic level course, students are encouraged to have at least a basic proficiency in the following knowledge topics and practical skills:

- **Basic Networking:** Understanding of common network protocols such as TCP/IP, DNS, and DHCP.
- **Operating Systems:** Familiarity with Windows, Linux, and UNIX systems.
- **Security Fundamentals:** Awareness of basic cybersecurity concepts such as encryption, firewalls, antivirus, and intrusion detection systems.
- **Windows Administration:** Basic skills in managing Windows environments, including user account management, file permissions, and system configuration.
- **Linux/UNIX Basics:** Understanding of common Linux commands, file systems, and basic system administration tasks.
- **Command-line Interface Use:** Comfort with using the command line in both Windows (CMD/PowerShell) and Linux to execute commands and scripts.

AO
Authorizing Official
OD

BMA
Basic Malware Analysis
MTT · RES

CCA
Cryptocurrency Activities
ILV · MTT · RES

CF200
Cyber Fundamentals 200
OD

CY101
Cyber 101
OD

DWA
Dark Web Activities
ILV · MTT · RES

ICI
Introduction to Cyber Investigations
ACE · OD

INCH
Introduction to Networks and Computer Hardware
ACE · IACET · MTT · OD · RES

NIB
Network Intrusions Basics
OD

NMAP
Network Mapper
OD

OPV
OpenVAS
OD

TEDA
Technology Evidence in Domestic Abuse
OD

Course Map Key

RES In-Residence
OD On-Demand
ILV Instructor-Led Virtual
MTT Mobile Training Team

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

Intermediate Offerings

Recommended Experience in the Field: 3-6 years

Building upon the Basic level, the DC3 Cyber Training Academy's Intermediate level aims to strengthen practical skills while also deepening knowledge for analysts, investigators, and network defenders. These courses teach students to identify cyberthreats, conduct insightful analysis, use advanced forensics tools, and engage in incident response activities. Intermediate courses are created for students who possess or are building a solid foundation in the following topics and skills:

- **Networking Fundamentals:** Understanding of how networks operate, including knowledge of the Open Systems Interconnection (OSI) model, IP addressing, subnetting, and basic routing concepts.
- **File Systems:** Understanding of basic file system structures, including how files are stored, accessed, and managed.
- **User and Permission Management:** Knowledge of how to manage users, groups, and permissions in both Windows and Linux environments.
- **Command-line Interface Use:** Strong ability with command-line utilities in both Windows and Linux/Unix
- **Basic Scripting:** Ability to write or modify simple scripts in scripting languages like PowerShell or Bash for automating tasks, analyzing data, and integrating multiple tools.
- **Programming:** Basic fundamentals.

CAC
Cyber Analyst Course
ILV · MTT · RES

CIRC
Cyber Incident Response Course
ACE · IACET · MTT · RES

CLOUD+
Cloud+ (CompTIA)
CT · ILV · MTT · RES

CySA+
Cybersecurity Analyst (CompTIA)
CT · ILV · MTT · RES

DataSys+
DataSys+ (CompTIA)
CT · ILV · MTT · RES

IMA
Intermediate Malware Analysis
MTT · RES

LA
Log Analysis
ACE · IACET · OD

LINUX+
Linux+ (CompTIA)
CT · ILV · MTT · RES

LXE
Linux Essentials
OD

MACF
Mac Forensics
ACE · ILV · MTT · RES

MA
Managed Attribution
MTT · RES

NET+
Network+ (CompTIA)
CT · ILV · MTT · RES

NTC
Network Traffic Collection
ACE · ILV · MTT · RES

PenTest+
Penetration Testing (CompTIA)
CT · ILV · MTT · RES

SEC+
Security+ (CompTIA)
CT · ILV · MTT · RES

WFE
Windows Forensic Examinations
ACE · IACET · ILV · MTT · RES

Course Map Key

RES In-Residence
OD On-Demand
ILV Instructor-Led Virtual
MTT Mobile Training Team

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

Advanced Offerings

Recommended Experience in the Field: 6+ years

The Advanced courses represent the pinnacle of the DC3 Cyber Training Academy's training pipelines. Incorporating a diverse range of tools and scenario-based challenges, these rigorous courses blend multiple disciplines and can be quite demanding at times. It is highly recommended that students build a strong skill set before attempting any of the Advanced level courses. Recommended skills include:

- **Forensic Process:** Deep understanding of digital forensics procedures as they relate to examination, analysis, and reporting.
- **Network Traffic Analysis:** Ability to analyze captured network traffic to identify suspicious activities, such as data exfiltration, C2 communications, and lateral movement.
- **Static Malware Analysis:** Skills in performing static analysis of malicious binaries using various tools to identify malware signatures without executing the code.
- **Forensic Suites:** Proficiency with forensic tools like Axiom, Forensic Toolkit, and EnCase to perform data carving, indexing, and case management.
- **Stand-alone Utilities:** Applying third-party information and diagnostic utilities, such as Sysinternals Suite and Zimmerman tools, to supplement forensic investigations.
- **Script Development:** Ability to write or modify scripts to parse data not handled by commercial tools.
- **Programming:** Understanding of basic programming concepts, formats, and various languages.

AMA
Advanced Malware Analysis
MTT · RES

DF
Drone Forensics
MTT · RES

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

OUA
Online Undercover Activities
MTT · RES

SecurityX
CompTIA Advanced Security Practitioner (CompTIA)
CT · ILV · MTT · RES

Course Map Key

RES In-Residence
OD On-Demand
ILV Instructor-Led Virtual
MTT Mobile Training Team
ACE American Council on Education Credit Recommendation
CT Eligible for CompTIA CEUs
IACET Eligible for IACET CEUs

International Cyber Forensics Course (ICFC) MASL D179205

The ICFC provides students with the solid working knowledge necessary to conduct incident response and digital forensics of digital media. This is a seven-week course with 280 hours of instruction and more than 90 hours of hands-on training and activities.

ICFC Map

Duration:
7 weeks / 35 days, 280 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.

DoW Certificates

To effectively counter the ever-evolving cybersecurity threats, DC3 Cyber Training Academy developed six comprehensive learning paths designed to assist law enforcement and the DoW's cyber workforce in achieving specific job roles in digital forensics, malware analysis, and cyber activities. Our certificates are in compliance with DoD 8140 and are aligned with the DCWF work roles.

Digital Media Collector (DMC)

Duration*:
2–4 Months

INCH › CIRC ✓ → Digital Media Collector DMC

Digital Forensic Examiner (DFE)

Duration:
3–4 Months

INCH › CIRC › WFE ✓ → Digital Forensic Examiner DFE

Cyber Crime Investigator (CCI)**

Duration:
4–6 Months

INCH › CIRC › WFE › FIWE ✓ → Cyber Crime Investigator CCI

Cyber Activities Examiner (CAE)

Duration*:
4–6 Months

DWA › CCA › MA › OUA ✓ → Cyber Activities Examiner CAE

Malware Analysis and Reverse Engineering (MAR)

Duration*:
8–12 Months

BMA › IMA › AMA ✓ → Malware Analysis and Reverse Engineering MAR

Cyber Fundamentals Certificate (CFC)

Duration:
2–4 Months

CY101 › INCH › ICI › TEDA › DWA › CCA ✓ → Cyber Fundamentals Certificate CFC

*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 LE/CI credentials verified by CDTI Training Program Manager before being eligible for a certificate.
**ARMY CID (USACIDC) students must have LE/CI credentials verified by organizational POC before being eligible for a certificate.

Table of Contents

Table of Contents

AMA

Advanced Malware Analysis

COURSE DESCRIPTION

Advanced Malware Analysis (AMA) is designed to provide students with the fundamental principles of dissecting and reverse engineering complex malware. In this 80-hour course, students will inspect malware via disassembly tools and other static analysis methods to identify capabilities, indicators of compromise, and attacker infrastructure. Using both attacker and defender perspectives, students will learn to overcome the advanced techniques used to circumvent reverse engineering.

COURSE OBJECTIVES

- Apply knowledge of cyberattacks and malware detection to identify useful indicators of compromise in a malware sample.
- Demonstrate the disassembly of machine code and the reading of assembly language.
- Analyze advanced Windows malware samples, including those with packing, code injection, and anti-reversing techniques.
- Analyze malicious code in non-standard formats, including documents and mobile platforms.
- Perform an investigation using advanced forensic malware techniques.

RECOMMENDED COURSES

- Intermediate Malware Analysis (IMA)
- Linux Essentials (LXE)

RECOMMENDED CYBERCASTS

- Behavior Analysis of Malicious Portable Executables

COURSE DETAILS

Difficulty:
Advanced

Delivery:
In-Residence
Mobile Training Team
80 hours over 10 days

Accreditations:
None

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 8-hour 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

- Evaluate and apply relevant laws, policies, and the evolving standards that inform the RMF process.
- Analyze the degree to which an organization's mission and systems are aligned.
- Evaluate security and risk assessments, mitigation strategies and controls, and other information needed to make a risk-based authorization decision.
- Evaluate mission need against risk to render an authorization decision.
- Determine the acceptable level of risk to render an authorization decision.
- Create and maintain an ongoing review of existing ATOs.

COURSE DETAILS

Difficulty:
Basic

Delivery:
On-Demand
8 hours

Accreditations:
None

BMA

Basic Malware Analysis

COURSE DESCRIPTION

Basic Malware Analysis (BMA) is a 40-hour course designed to provide students with a foundational understanding of malicious software, including its forms, traits, motivations, and impacts. Students will learn how to interpret analytical reports resulting from static and dynamic analysis of malware and how to use these reports to develop mitigation strategies. Using common techniques and tools for both dynamic and static analysis, students will uncover the functionality of malware samples, including data exfiltration and stealthy operation. The results of this analysis will reveal tactics often deployed by malware authors. Upon completion of the course, students will be able to identify multiple malware samples using modern disassembly, debugging, and analysis tools.

COURSE OBJECTIVES

- Identify and describe common traits of malware.
- Explain the process and acceptable procedures to reduce risk when handling malware.
- Explain the main components of the Windows operating systems affected by malware.
- Explain the procedures for creating an isolated and forensically sound malware analysis lab ("sandbox").
- Examine and analyze a variety of malware using static analysis techniques.
- Demonstrate the use of a sandbox environment to monitor a piece of malware as it executes.

RECOMMENDED COURSES

- Network Intrusions Basics (NIB)
- Network Traffic Collection (NTC)

COURSE DETAILS

Difficulty:
Basic

Delivery:
In-Residence
Mobile Training Team
40 hours over 5 days

Accreditations:
None

CAC

Cyber Analyst Course

COURSE DESCRIPTION

The Cyber Analyst Course (CAC) is a 40-hour, one-week, in-residence course that fuels cyber professionals' critical thinking and provides analytical skills so they can interpret different types of reports, conduct internet research, identify intrusions, explore data-hiding techniques, and analyze computer systems, networks, and logs. Students explore real-world scenarios using specialized analytical tools that allow for skills practice, writing analysis reports, creating link diagrams, and completing performance exercises. The course includes 70 percent practical application and 30 percent knowledge-based learning, all preparing students for a final knowledge- and performance-based exam.

COURSE OBJECTIVES

- Apply analytical methodologies to the cyber domain.
- Analyze evidence of a network intrusion.
- Analyze forensic data collected from a device.
- Analyze network devices and traffic associated with a cyber incident.
- Examine device logs for relevant cyber incident-related data.
- Evaluate public information available online to support cyber analysis.
- Develop various analytical products that depict a cyber incident, using provided artifacts and online repositories.

RECOMMENDED COURSES

- Introduction to Networks and Computer Hardware (INCH)

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
None

SecurityX

CompTIA Advanced Security Practitioner (CompTIA)

COURSE DESCRIPTION

The CompTIA SecurityX bootcamp runs for 40 hours over 5 days and covers technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. The DC3 Cyber Training 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.

COURSE OBJECTIVES

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise.
- Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment.
- Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques.
- Consider the impact of governance, risk, and compliance requirements throughout the enterprise.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Advanced

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

CCA

Cryptocurrency Activities

COURSE DESCRIPTION

Cryptocurrency Activities (CCA) is a 40-hour training course designed for law enforcement and counterintelligence professionals and provides students with an understanding of cryptocurrency fundamentals and the skills necessary to conduct investigations into cryptocurrency transactions. The course immerses students in scenario-based exercises that allow them to practice and reinforce what they have learned while using trusted resources. CCA culminates with a graded Final Exam.

COURSE OBJECTIVES

- Understand the basic technical principles that apply to the functionality and utilization of cryptocurrency.
- Understand the scope of the cryptocurrency economy, including both legal and illicit typologies.
- Examine cryptocurrency transactions using publicly available resources to trace the movement of assets.
- Examine cryptocurrency transactions using knowledge of common cryptocurrency laundering techniques to trace the movement of assets.

COURSE DETAILS

Difficulty:
Basic

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
None

CF200

Cyber Fundamentals 200

COURSE DESCRIPTION

Cyber Fundamentals 200 (CF200) is an 80-hour course that provides foundational cyber knowledge to cyberspace workforce elements and DoW personnel, whose duties include the protection of DoW 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.

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:
Basic

Delivery:
On-Demand
80 hours over 3 weeks

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.

RECOMMENDED COURSES

- Introduction to Networks and Computer Hardware (INCH)

RECOMMENDED CYBERCASTS

- Introduction to Axiom
- Collecting BitLocker-encrypted Data
- Collecting System Information and Searching Data with PowerShell
- Imaging Memory in Linux
- Incident Response: Actions and Reactions

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Mobile Training Team
80 hours over 10 days

Accreditations:
ACE Recommended Course
3 Semester Hours
Lower-Division

IACET CEU-eligible
4.0 CEUs

CLOUD+

Cloud+ (CompTIA)

COURSE DESCRIPTION

The CompTIA Cloud+ bootcamp is 40 hours over 5 days, and it helps validate essential skills necessary to implement, maintain, optimize and troubleshoot cloud-based infrastructure services. Cloud+ prepares the student for the work roles of Network Operations Specialist, Systems Administrator, Enterprise Architect and Security Architect. The DC3 Cyber Training 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.

COURSE OBJECTIVES

- Understand cloud architecture and design concepts.
- Implement and maintain a secure cloud environment.
- Successfully provision and configure cloud resources.
- Demonstrate the ability to manage operations throughout the cloud environment life cycle using observability, scaling, and automation.
- Understand fundamental DevOps concepts related to deployment and integration.
- Troubleshoot common issues related to cloud management.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

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 Cyber Protection Teams (CPTs) or Mission Defense Teams (MDTs). In accordance with DoDM 8140.03 (15 Feb 2023), CY101 satisfies DoD 8140 foundational qualification requirements for all DoW Cyber Workforce Framework (DCWF) Cyber Enabler work roles. 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:
Basic

Delivery:
On-Demand
40 hours over 6 weeks

Accreditations:
None

CySA+

Cybersecurity Analyst (CompTIA)

COURSE DESCRIPTION

Cybersecurity Analyst (CySA+) is a 40-hour 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 DC3 Cyber Training 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.

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.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

DataSys+

DataSys+ (CompTIA)

COURSE DESCRIPTION

The CompTIA DataSys+ bootcamp is a 40-hour course that provides the knowledge and skills required to deploy, manage, and maintain databases, including employing the fundamentals of scripting and programming in a database environment while using security and business continuity best practices. The DC3 Cyber Training 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.

COURSE OBJECTIVES

- Design and model databases to meet a specific organizational need.
- Execute database tasks, including processing and structuring data files, and running routines.
- Install, configure and maintain database software and tools for optimal performance.
- Establish and maintain sound security, backup and recovery policies and procedures.
- Work with key stakeholders to translate data into actionable intelligence.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

DWA

Dark Web Activities

COURSE DESCRIPTION

Dark Web Activities (DWA) is a 40-hour introductory course that describes the basic tools and mechanics of the dark web. Students need no technical background for this course. They learn what the dark web is, what tools and technologies exist within and on it, and what activities are most prevalent on the dark web. This course will distinguish between the surface web, deep web and dark web, explaining the unique features and components of each. Tailored to investigators, the course discusses the concepts of identifying and tracking illegal activities, such as cyber crime, drug trafficking, and fraud, and how to document findings. It serves as the introductory course for the Cyber Activities Examiner (CAE) Certification, followed by Cryptocurrency Activities, Managed Attribution and Online Undercover Activities.

COURSE OBJECTIVES

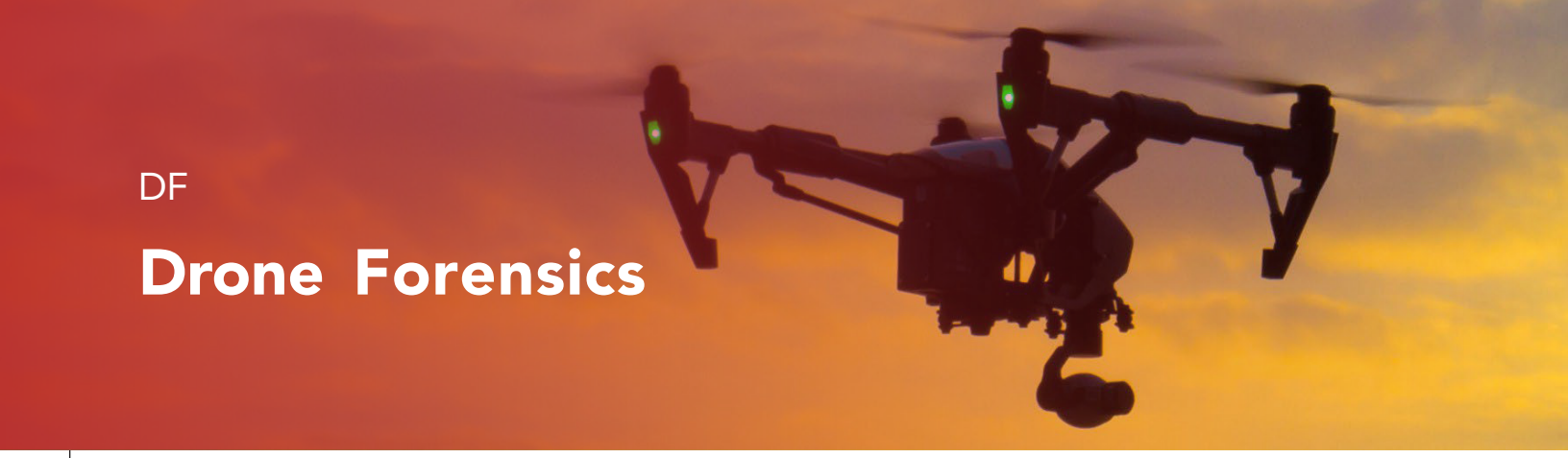
- Define the dark web, describe its distinguishing features, and recognize its various components.
- Describe the key information collected and technologies and tools commonly used to access and navigate the dark web.
- Identify techniques to discover and track illegal activities on the dark web, including cybercrime, drug trafficking, and fraud.
- Determine the appropriate steps of an investigation given a case study based on dark web illicit activities.

COURSE DETAILS

Difficulty:
Basic

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
None



DF

Drone Forensics

COURSE DESCRIPTION

Drone Forensics (DF) is a 40-hour scenario-based training course. The course provides training that enables professionals to gather forensic artifacts from and conduct digital analysis on Unmanned Aerial Systems (UAS) in a forensically reliable manner. DF introduces best practices and relevant technical aspects of interacting with unmanned aerial systems and their associated peripherals. The course not only introduces students to the forensic artifacts found on these systems and how to recover and analyze them but also provides participants the opportunity to get direct experience with the systems. The course will contain 4-days of hands-on, in-class exercises with a conclusion on the final day with a cumulative exam.

COURSE OBJECTIVES

- Understand the fundamentals of Unmanned Aerial Systems (UAS).
- Safely seize drones in a forensically sound, repeatable process so that data can be reliably extracted.
- Retrieve and deconstruct data from the operational UAS using forensically sound, repeatable processes.
- Reassemble a disassembled drone into a fully operational state.
- Demonstrate the safe operation of a UAS.

COURSE DETAILS

Difficulty:
Advanced

Delivery:
In-Residence
Mobile Training Team
40 hours over 5 days

Accreditations:
None

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), DoW 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 graded Final 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:
Advanced

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
80 hours over 10 days

Accreditations:
ACE Recommended Course
6 Semester Hours
Upper-Division

IACET CEU-eligible
4.0 CEUs

RECOMMENDED COURSES

- Cyber Analyst Course (CAC)
- Cybersecurity Analyst (CySA+)
- Log Analysis (LA)
- Network Intrusions Basics (NIB)
- Penetration Testing (PenTest+)
- Windows Forensics Examinations (WFE)

RECOMMENDED CYBERCASTS

- Introduction to Axiom
- Introduction to PowerShell
- Windows Management Instrumentation Command-line
- Indicator Analysis With MITRE's ATT&CK Model
- Network Monitoring - Traffic Analysis
- Packet Analysis With Wireshark
- Phases of Intrusion
- Sysinternals Tools

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 graded Final 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:
Basic

Delivery:
On-Demand Scheduled
40 hours over 5 weeks

Accreditations:
ACE Recommended Course
3 Semester Hours
Lower-Division

IMA

Intermediate Malware Analysis

COURSE DESCRIPTION

Intermediate Malware (IMA) is an 80-hour course that covers some of the methods used by attackers to gain unauthorized access to systems, and some malicious activities that they may perform while present there. Starting with a solid foundation, students will learn to find patterns, recognize malicious behavior, and dissect complex code structures. Students will be provided with methods and strategies to investigate and analyze malicious software, including hands-on practical labs and instructor-led demonstrations. Upon course completion, students will be equipped with the knowledge, skills, and practical experience they need to perform a malware analysis in the Linux environment.

COURSE OBJECTIVES

- Categorize different types of malware based on their features.
- Compare and contrast system architecture and operating systems (OSs) by how malware impacts them.
- Prepare a malware analysis environment.
- Use malware analysis tools.
- Inspect malware using static analysis methods.
- Inspect malware using dynamic analysis methods.
- Produce a report on a malware incident.

RECOMMENDED COURSES

- Basic Malware Analysis (BMA)

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Mobile Training Team
80 hours over 10 days

Accreditations:
None

INCH

Introduction to Networks and Computer Hardware

COURSE DESCRIPTION

Introduction to Networks and Computer Hardware (INCH) is a 40-hour course teaching computer basics, network theory, and input/output device identification and function. INCH is tailored for professionals currently working in or aspiring to careers in 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 ten 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.

COURSE DETAILS

Difficulty:
Basic

Delivery:
In-Residence
Mobile Training Team
40 hours over 5 days

On-Demand
40 hours over 4 weeks

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 graded Final 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.

RECOMMENDED COURSES

- Network Intrusions Basics (NIB)

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
On-Demand
50 hours over 5 weeks

Accreditations:
ACE Recommended Course
6 Semester Hours
Upper-Division

IACET CEU-eligible
4.0 CEUs

LINUX+

Linux+ (CompTIA)

COURSE DESCRIPTION

Linux+ (CompTIA) is a bootcamp-style course that gives students the skills administrators need to secure the enterprise, power the cloud, and keep systems running. The 40-hour course explores an evolving work role that focuses 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. The DC3 Cyber Training 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.

COURSE OBJECTIVES

- System Management: Configure and manage software, storage, processes, and services.
- Security: Understand best practices for permission and authentication, firewalls, and fire management.
- Scripting, Containers, and Automation: Create simple shell scripts and execute basic BASH scripts, version control using Git, and orchestration processes.
- Troubleshooting: Analyze system properties and processes and troubleshoot user, application, and hardware issues.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

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 graded Final Exam.

COURSE OBJECTIVES

- Describe the features of Linux that differentiate it from Microsoft Windows-based operating systems.
- Manipulate Linux files and directories using common Linux commands.
- Manipulate user and group accounts using common Linux commands.
- Change Linux file system permissions using common Linux commands.
- Create multiple file systems using common Linux commands.
- Demonstrate how to mount file systems using common Linux commands.
- Describe the characteristics of common Linux file systems.

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:
On-Demand
40 hours over 4 weeks

Accreditations:
None

MACF

Mac Forensics

COURSE DESCRIPTION

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 in a Windows environment. 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. This 40-hour course includes scenarios that build upon each other so students can practice what they learn using trusted forensic tools.

COURSE OBJECTIVES

- Apply forensic investigative tactics, techniques, and procedures to a macOS and iOS system.
- Review forensic images and other data sources to recover potentially relevant information.
- Structure a framework to identify and analyze macOS and iOS malware.
- Generate a detailed and accurate summary of potential security compromises of a macOS and iOS device.

RECOMMENDED CYBERCASTS

- Mac OS X Basics for First Responders

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
ACE Recommended Course
3 Semester Hours
Lower-Division

MA

Managed Attribution

COURSE DESCRIPTION

Managed Attribution (MA) trains students in the techniques, tactics, and procedures for developing deliberate, controlled, and misleading digital footprints to support law enforcement and counterintelligence operations. Students learn about the methodologies used by adversaries and the necessary skills, techniques, and strategies to protect sensitive information, while performing law enforcement or counterintelligence operations. This 40-hour course also teaches students to proactively defend against threats while maintaining operational security and preserving the integrity of their organizations.

COURSE OBJECTIVES

- Demonstrate knowledge of digital footprints.
- Perform a risk analysis to support a mission requiring managed attribution.
- Use tools (such as VPN), tunneling (pivots/jump points or forward and reverse tunneling), and methodologies (spoofing, proxy servers, encryption, and others) to obfuscate their identity.
- Analyze and discuss scenarios.
- Use methods and tools to spoof, hide, or manipulate identifying information or data.
- Analyze logs to discover information related to compromise or attack.
- Maintain operational security.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Mobile Training Team
40 hours over 5 days

Accreditations:
None

NET+

Network+ (CompTIA)

COURSE DESCRIPTION

Network+ (NET+) (CompTIA) is a 40-hour 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 DC3 Cyber Training 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.

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.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

NIB

Network Intrusions Basics

COURSE DESCRIPTION

Network Intrusions Basics (NIB) is a 15-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 graded Final 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:
Basic

Delivery:
On-Demand
15 hours over 7 days

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.

RECOMMENDED COURSES

- Introduction to Networks and Computer Hardware (INCH)

COURSE DETAILS

Difficulty:
Basic

Delivery:
On-Demand
8 hours over 5 days

Accreditations:
None

NTC

Network Traffic Collection

COURSE DESCRIPTION

Network Traffic Collection (NTC) is an introduction to the practice of capturing and analyzing network traffic for surveillance purposes in accordance with wiretap authorities. In this 40-hour course, students will practice evaluating networks to determine the best strategic placement for network monitoring devices to ensure the capture of targeted host traffic while remaining undetected on a network. Upon completion of this course, students will be able to identify anomalies in network traffic by analyzing communication patterns and captured data packets, as well as implement effective strategies for filtering network traffic to ensure relevant data is captured in compliance with wiretap authorities.

COURSE OBJECTIVES

- Explain basic theory, technologies, and components that facilitate network data transmission.
- Examine network traffic as well as 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 identify the proper placement of a network-monitoring sensor.
- Configure network data acquisition tools.
- Collect and analyze network traffic and system artifacts to identify intrusion techniques.

RECOMMENDED COURSES

- Cyber Incident Response Course (CIRC)

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
ACE Recommended Course
3 Semester Hours
Lower-Division

OUA

Online Undercover Activities

COURSE DESCRIPTION

Online Undercover Activities (OUA) is a 40-hour scenario-based training course that develops professionals' skills in conducting a full online undercover operation. The course provides both theory and practical training, enabling students to develop and plan an online undercover operation, access the dark web, create personas, manage digital footprints, navigate dark web marketplaces and forums, and report their findings and activities. OUA contains six modules and culminates in a graded Final Exam.

COURSE OBJECTIVES

- Apply the key concepts related to online undercover activities.
- Develop and deploy undercover personas for online activities.
- Use anonymity and encryption tools for the purpose of achieving secure and untraceable online communication.
- Demonstrate proficiency in a variety of online intelligence gathering methods, including open-source intelligence (OSINT), deep web and dark web exploration, and the use of advanced intelligence tools.
- Execute monitoring and surveillance operations while deploying effective counter-surveillance measures.
- Collect and preserve digital evidence.
- Analyze and report on gathered data effectively.
- Understand strategies for psychological resilience in undercover activities.

COURSE DETAILS

Difficulty:
Advanced

Delivery:
In-Residence
Mobile Training Team
40 hours over 5 days

Accreditations:
None

OPV

OpenVAS

COURSE DESCRIPTION

OpenVAS (OPV) is an eight-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 graded Final 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:
Basic

Delivery:
On-Demand
8 hours over 5 days

Accreditations:
None

PenTest+

Penetration Testing (CompTIA)

COURSE DESCRIPTION

Penetration Testing (PenTest+) (CompTIA) is a 40-hour 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 DC3 Cyber Training 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.

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.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

SEC+

Security+ (CompTIA)

COURSE DESCRIPTION

Security+ (SEC+) (CompTIA) is a 40-hour 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 DC3 Cyber Training 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.

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 (IoT), and mobile security solutions.
- Implement secure cloud solutions.
- Explain data privacy and protection concepts.
- Perform incident response and digital forensics.

Authorized Audience: This course is for government civilian and military personnel only. Contractors are not permitted to take this course.

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
40 hours over 5 days

Accreditations:
CompTIA CEU-eligible

TEDA

Technology Evidence in Domestic Abuse

COURSE DESCRIPTION

Technology Evidence in Domestic Abuse (TEDA) is a 2-hour, self-paced online course and teaches students the fundamentals of using technology evidence in domestic abuse cases. Intended primarily for law enforcement personnel and first responders, the course content familiarizes students with causes and types of domestic abuse and presents real-life domestic abuse scenarios to emphasize that abuse through technology is not always distinct from physical violence. Students learn to recognize, collect, preserve, and analyze digital evidence, and increase their understanding of applicable laws.

COURSE OBJECTIVES

- Describe the fundamentals of domestic abuse and provide examples of abuse tactics through technology (for example, a threatening text; spoofing; hacking into Internet of Things (IoT) devices or victim email or 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 DoW policy concerning abuse.
- Evaluate a situation and perform necessary actions in accordance with best practices.

COURSE DETAILS

Difficulty:
Basic

Delivery:
On-Demand
2 hours

Accreditations:
None

WFE

Windows Forensic Examinations

COURSE DESCRIPTION

Windows Forensic Examinations (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 80-hour 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.

RECOMMENDED COURSES

- Cyber Incident Response Course (CIRC)
- Introduction to Networks and Computer Hardware (INCH)

RECOMMENDED CYBERCASTS

- Introduction to Axiom
- File Carving in EnCase

COURSE DETAILS

Difficulty:
Intermediate

Delivery:
In-Residence
Instructor-Led Virtual
Mobile Training Team
80 hours over 10 days

Accreditations:
ACE Recommended Course
3 Semester Hours
Lower-Division
3 Semester Hours
Upper-Division

IACET CEU-eligible
4.0 CEUs

CYB

CyberCasts

DESCRIPTION

CyberCasts are on-demand, streaming-video, microlearning modules created by DC3 Cyber Training 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 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

178,913
TOTAL VIEWS

127,343
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

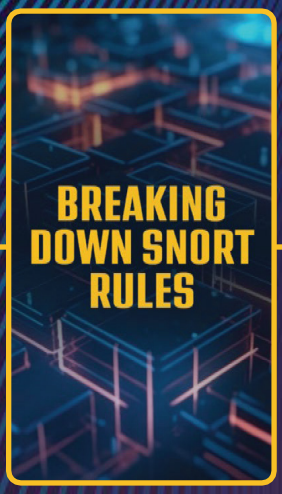
Delivery:
On-Demand Video
1 to 2 hours

Recommended Courses:
None

Accreditations:
CompTIA CEU-eligible for

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

DC3 CYBER TRAINING ACADEMY



DC3 QuickBytes

DC3 QuickBytes are short microlearning videos that provide students with quick tutorials on how to perform specific actions using a variety of different tools and techniques. QuickBytes are developed by DC3 Cyber Training Academy instructors and subject matter experts.

Learn more and view QuickByte videos at learn.dcita.edu.

DC3 Cyber Training Academy Policies and Procedures

FOR ALL NON-SCHOOL-RELATED ISSUES

Students should use their chain of command through their service or organizational leadership.

FOR ALL ACADEMY-RELATED ISSUES

Students should follow the procedures 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 DC3 Cyber Training Academy Registrar at (DC3.CTA.Registrar@us.af.mil).

Staff will examine the submission, consult with the DC3 Cyber Training Academy Student Engagement government representative, and provide an appropriate response with 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 will then examine the submission and provide an appropriate response with 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 (SOP).

CONTACT

DC3 CTA Registrar
Monday-Friday,
8:00 am-4:30 pm ET
DC3.CTA.Registrar@us.af.mil
443-545-3055

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
443-545-3055
DC3.CTA.Registrar@us.af.mil

ADDRESS

DC3 Cyber Training Academy
7021 Columbia Gateway, Suite 100
Columbia, MD 21046