



FedVTE
Training Catalog

SPRING 2015

advance.

If you need any assistance please contact the FedVTE Help Desk [here](#) or email the Help Desk at support@usalearning.net.

To speak with a Help Desk representative, call (202) 558-2203 or toll-free (888) 804-4510 Monday-Friday, 8:30 AM to 6:00 PM EST, except holidays.

Contents

Certified Ethical Hacker (CEHv7) 21 Hours.....	4
*Certified Ethical Hacker (CEHv8) 22 Hours.....	4
CompTIA A+ 220 - 801 Certification Prep 12 Hours.....	4
*CompTIA A+ 220 - 802 Certification Prep 11 Hours.....	4
CompTIA Advanced Security Practitioner Prep 20 Hours	4
CompTIA Network+ Certification Prep 17 Hours	5
CompTIA Security+ (SY0-301) Prep 32 Hours.....	5
CompTIA Security+ (SY0-401) Certification Prep 19 Hours	5
Cyber Risk Management for Managers 11 Hours	5
Cyber Risk Management for Technicians 11 Hours	5
Cyber Security Overview for Managers 6 Hours.....	6
Demilitarized Zone (DMZ) with IDS/IPS 9 Hours.....	6
*DISA ACAS Version 4.6 32 Hours.....	6
DISA HBSS Admin MR5 (2013 Version) 32 Hours.....	6
DISA HBSS Advanced MR5 (2013 Version) 32 Hours	6
DISA SIM (Security Information Manager) 3 Hours	6
DoD IA Boot Camp 12 Hours	7
*Einstein Silk Traffic Analysis 7 Hours.....	7
*Introduction to Investigation of Digital Assets 4 Hours	7
IPv6 Security 1 Hour.....	7
*ISACA Certified Information Security Auditor 21 Hours	7
ISACA Certified Information Security Manager 11 Hours	7
*(ISC)2™ CAP (R) Prep 10 Hours.....	7
*(ISC)2™ Certified Secure Software Lifecycle Professional 20 Hours	8
(ISC)2™ CISSP Certification Prep 20 Hours.....	8
(ISC)2™ CISSP Concentration: ISSAP 15 Hours	8
(ISC)2™ CISSP Concentration: ISSEP 12 Hours	8
*(ISC)2™ CISSP Concentration: ISSMP 13 Hours.....	9
(ISC)2™ Systems Security Certified Practitioner 16 Hours.....	9
Linux Operating System Security 9 Hours	9
Mobile Security 19 Hours.....	9
Network Monitoring with Open Source Tools 5 Hours.....	9

Penetration Testing <i>14 Hours</i>	9
*Software Assurance for Executives <i>10 Hours</i>	10
*Supply Chain Awareness <i>1 Hour</i>	10
*Supply Chain Risk Management Awareness <i>.5 Hours</i>	10
*Trustworthy Software Initiative (TSI) <i>1 Hour</i>	10
Windows Operating System Security <i>16 Hours</i>	10
Wi-Fi Communications and Security (WNS) <i>9 Hours</i>	10

**Indicates course is coming soon.*

Certified Ethical Hacker (CEHv7)

21 Hours

The CEHv7 certification prep course prepares students to sit for the EC-Council Certified Ethical Hacker certification exam. This course contains not only the lecture material to help the student broaden their knowledge of techniques such as enumeration, scanning and reconnaissance, but contains several demos and labs to improve skills and experience. Updates to v7 from v6 include several new tools and how to use them to perform various techniques. Topics include active and passive reconnaissance, hacking laws, Google hacking, social engineering, packet capture and scanning. The course then moves on to exploitation of several types and threats and how to cover your tracks. The course concludes with a 100-question practice exam.

Certified Ethical Hacker (CEHv8)

22 Hours

The CEHv8 certification prep course prepares students to sit for the EC-Council Certified Ethical Hacker version 8 certification exam. This course contains materials to aid the student in broadening their knowledge of advanced network assessment techniques including enumeration, scanning and reconnaissance. Updates to v8 from v7 include several new tools and how to use them to perform various techniques. Topics include active and passive reconnaissance, hacking laws, Google hacking, social engineering, packet capture and scanning. The course then moves on to exploitation of several types and threats and how to cover your tracks.

CompTIA A+ 220 - 801 Certification Prep

12 Hours

The A+ 220-801 Certification Prep Self-Study is an introductory course presenting domain knowledge and objectives for the five domains featured in the A+ 220-801 portion of the A+ certification exam.

CompTIA A+ 220 - 802 Certification Prep

11 Hours

The A+ 220-802 Certification Prep Self-Study course is for entry-level IT professionals with at least 12 months experience in the field. Knowledge required for A+ candidates include installation, configuration, and maintenance of devices, PCs, and software for end users. This course contains materials for the four A+ 802 domains to aid the candidate in exam preparation.

CompTIA Advanced Security Practitioner Prep

20 Hours

This certification prep course helps to prepare students to sit for the CompTIA CASP CAS-001 certification exam by covering technical knowledge and skills required in designing and engineering secure solutions in enterprise environments. A broad spectrum of security disciplines are discussed to help with critical thinking when considering secure enterprise solutions and managing risk.

CompTIA Network+ Certification Prep

17 Hours

CompTIA's Network+ certification prep course was developed for the current Network+ exam code N10-005. Topics covered on the Network+ N10-005 exam as well as in this FedVTE prep course include network technologies, installation and configuration, media and topologies, management and security. This certification prep course includes video demonstrations, a practice exam, and hands-on labs.

CompTIA Security+ (SY0-301) Prep

32 Hours

This certification prep course prepares students to sit for the CompTIA Security+ (SY0-301) certification exam as well as teaches concepts and techniques that are valuable to the workplace. Topics covered in the course, and competencies tested on the exam include network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography. This certification prep course includes several reinforcing video demonstrations and hands-on labs as well as a practice quiz.

CompTIA Security+ (SY0-401) Certification Prep

19 Hours

This certification prep course prepares students to sit for the CompTIA Security+ (SY0-401) certification exam as well as teaches concepts and techniques that are valuable to the workplace. Topics covered in the course, and competencies tested on the exam include network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography. This certification prep course includes several reinforcing video demonstrations as well as a practice quiz.

Cyber Risk Management for Managers

11 Hours

Cyber Risk Management for Managers covers key concepts, issues, and considerations for managing risk from a manager's perspective. Discussions include identifying critical assets and operations, a primer on cyber threats and how to determine threats to your business function, mitigation strategies, and response and recovery.

Cyber Risk Management for Technicians

11 Hours

This course presents the concept of managing cyber risk from a technical perspective. An overview of cyber risk management opens the class, followed by foundational material on conducting a risk assessment of considerations such as threats, vulnerabilities, impacts, and likelihood. Various technical methods for conducting a risk assessment are presented, to include vulnerability assessments and penetration tests, with a focus on continuous monitoring of security controls and how to assess those security controls using the National Institute of Standards and Technology Special Publication 800-53 and 800-53a as a guide.

Cyber Security Overview for Managers

6 Hours

Cyber Security Overview for Managers is designed for managers and other stakeholders who may be involved in decision making regarding their cyber environment but do not have a strong technical background. Discussions will not focus on specific technologies or implementation techniques, but rather cyber security methodologies and the framework for providing a resilient cyber presence. The course aims to help managers better understand how people and devices work together to protect mission critical assets and more effectively evaluate their cyber posture.

Demilitarized Zone (DMZ) with IDS/IPS

9 Hours

This course introduces the concept of a network Demilitarized Zone (DMZ) and the security benefits it can provide. Best practices for designing and implementing a DMZ is followed with a section on IDS and IPS systems that includes an in-depth look at SNORT for network monitoring. The course concludes with log analysis and management best practices.

DISA ACAS Version 4.6

32 Hours

This course is intended for Operators and Supervisors of ACAS within the Department of Defense (DoD). The ACAS course contains 31 demonstrations, 10 hands-on labs, 74 lectures, and a quiz that users must pass to receive their certificate of completion.

DISA HBSS Admin MR5 (2013 Version)

32 Hours

In this course, students learn to use the Department of Defense's Host Based Security System (HBSS). Students will have access to 25 modules of lectures and 23 hands-on lab assignments. A course quiz is presented at the end and must be passed in order to receive the final course completion certificate. DoD HBSS Administrators are required to complete this course per DoD STIGs.

DISA HBSS Advanced MR5 (2013 Version)

32 Hours

In this course, students learn to use the Department of Defense's Host Based Security System beyond what they have already learned in the administrator version of the course. Students will have access to 25 modules of lectures and 15 hands-on lab assignments. A course quiz is presented at the end and must be passed in order to receive the final course completion certificate. Course topics include McAfee's Solidcore Application and Change Control, Policy Auditor, and Data Loss Prevention products.

DISA SIM (Security Information Manager)

3 Hours

This 3-hour course is intended to provide students with an overview of DISA's SIM program and its primary tool – ArcSight ESM. It will describe how to gain access, log in, analyze events, create dashboards and reports, and create content. The course contains a lab that allows students to interact with the system and a quiz that must be passed before the student can obtain a completion certificate.

DoD IA Boot Camp

12 Hours

The DoD IA Boot Camp is an in-depth study program designed so students may successfully perform their duties as IA professionals, to include Information Assurance Managers, Information Assurance Officers, or System Administrators with IA duties. This course will provide the student with DoD policy guidance as related to law, policy, technical implementation guidance, documentation requirements, and references necessary to support a successful DoD IA program.

Einstein Silk Traffic Analysis

7 Hours

This course is designed for analysts involved in daily response to potential cyber security incidents, and who have access to the Einstein environment. The course begins with an overview of network flow and how the SiLK tools collect and store data. The next session focuses specifically on the Einstein environment. The basic SiLK tools are covered next, giving the analyst the ability to create simple analyses of network flow. Advanced SiLK tools follow, and cover how to create efficient and complex queries. The course culminates with a lab where students use their new skills to profile a network.

Introduction to Investigation of Digital Assets

4 Hours

This course is designed for technical staff who are new to the area of Digital Media Analysis and Investigations. It provides an overview of the digital investigation process and key activities performed throughout the process and various tools that can be used to perform each activity.

IPv6 Security

1 Hour

This presentation addresses IPv6 security. Topics include concepts, threats, network reconnaissance, network recon mitigation strategies, network mapping, network mapping mitigation strategies, neighbor discovery, attacks, attack mitigation strategies, tunneling, and tunneling mitigation strategies and best practices. The presentation has several reinforcing video demonstrations.

ISACA Certified Information Security Auditor

21 Hours

The ISACA Certified Information Security Auditor (CISA) certification prep course prepares students to sit for the CISA certification exam as well as provides the students with training assets to strengthen their audit, control, and monitoring skills to apply to their information technology and business systems. Topics include introduction to the IS audit process, introduction to IT governance, project management, IS operations and service management, introduction to information security management, introduction to business continuity and disaster recovery planning. Video demonstrations and an exam are part of the training.

ISACA Certified Information Security Manager

11 Hours

The ISACA Certified Information Security Manager (CISM) 2013 certification prep course self study prepares students to sit for the management-focused CISM exam as well as strengthens their information security management expertise through the in-depth courseware, reinforcing

demonstrations, and final quiz. The course covers topics from the four domains featured in the CISM certification: Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, and Information Security Incident Management.

(ISC)2™ CAP (R) Prep

10 Hours

This certification prep course, complete with a 100-question practice exam, is designed to help prepare students for the (ISC)2 CAP – Certified Authorization Professional certification exam as well as strengthen their knowledge and skills in the process of authorizing and maintaining information systems. Topics include understanding security and authorization of information, categorizing information systems, selecting security controls, implementing security controls, assessing security controls, authorizing information systems and monitoring security controls.

(ISC)2™ Certified Secure Software Lifecycle Professional

20 Hours

This certification prep course helps prepare students to sit for the (ISC)2 CSSLP certification exam by covering application security concepts and the software development lifecycle (SDLC). This course is for individuals with at least 4 years of experience in secure software concepts, software requirements, software design, and software implementation.

(ISC)2™ CISSP Certification Prep

20 Hours

The (ISC)2 Certified Information Systems Security Professional (CISSP) certification prep course confirms an individual's knowledge in the information security field. The objectives for the CISSP certification exam were updated in the first quarter of 2012, so the FedVTE course update reflects the new CISSP objectives and the ten domains upon which the exam is based. This course also includes hands-on labs.

(ISC)2™ CISSP Concentration: ISSAP

15 Hours

The Information Systems Security Architecture Professional (ISSAP) concentration of the CISSP certification prep course prepares students with security architect and analyst experience to sit for the (ISC)2 ISSAP certification exam. This course includes a practice exam and reinforcing video demonstrations for many of the topics included in the six domains of the ISSAP.

(ISC)2™ CISSP Concentration: ISSEP

12 Hours

The Information Systems Security Engineering Professional (ISSEP) concentration of the CISSP certification prep course prepares students with systems security engineering experience to sit for the (ISC)2 ISSEP certification exam. This course includes a 100-question practice exam and was developed following the four domains of the ISSEP.

(ISC)2™ CISSP Concentration: ISSMP

13 Hours

The Information Systems Security Management Professional (ISSMP) concentration of the CISSP certification prep course prepares students with management experience to sit for the (ISC)2 ISSMP certification exam. This course includes a 100-question practice exam and includes video demonstrations reinforcing many of the topics included in the five domains of the ISSMP.

(ISC)2™ Systems Security Certified Practitioner

16 Hours

The Systems Security Certified Practitioner (SSCP) certification prep course is a self-study resource for those preparing to take the (ISC)2 SSCP certification exam as well as those looking to increase their understanding of information security concepts and techniques. The certification is described as being ideal for those working toward positions such as network security engineers, security systems analysts, or security administrators. This course, complete with a 100-question practice exam and video demonstrations, was developed based on the seven SSCP domains.

Linux Operating System Security

9 Hours

This course introduces students to the security features and tools available in Linux as well as the considerations, advantages, and disadvantages of using those features. The class will be based on Red Hat Linux and is designed for IT and security managers, and system administrators who want to increase their knowledge on configuring and hardening Linux from a security perspective.

Mobile Security

19 Hours

The purpose of the Mobile Security course is to learn about mobile devices and how to secure them. The course begins with an introduction to cellular and wireless technologies and moves into threats to mobile devices, how to secure them, and mobile forensics.

Network Monitoring with Open Source Tools

5 Hours

The Network Monitoring with Open Source Tools course was designed to give the learner a general awareness of network security and monitoring concepts. Discussions and demonstrations focus on network threats, and the capabilities of tools. After completion of the course, students should be able to detect attacks using network monitoring tools.

Penetration Testing

14 Hours

The Penetration Testing course discusses concepts, tools, and techniques for conducting a penetration test. The course lays the groundwork with familiar ethical hacking concepts, moves into penetration testing methods, and determines the most effective penetration tool for the desired goal.

Software Assurance for Executives

10 Hours

This course is designed for executives and managers who wish to learn more about software assurance as it relates to acquisition and development. The purpose of this course is to expose participants to concepts and resources available now for their use to address software security assurance across the acquisition and development life cycles.

Supply Chain Awareness

1 Hour

This 60-minute presentation addresses supply chain awareness for hardware and software. A lecture and set of optional slides (Supply Chain Awareness – Hardware, and Supply Chain Awareness – Software) are available. A quiz is part of this training.

Supply Chain Risk Management Awareness

.5 Hours

Supply Chain Risk Management Awareness is a 20-minute course providing students with knowledge about the growing sophistication of supply chain exploitation facing government and private industry on Information and Communication Technology (ICT) systems. Additionally, the course will help students understand how supply chain risk management can affect requirements, acquisition practices, and operational requirements.

Trustworthy Software Initiative (TSI)

1 Hour

The Trustworthy Software Assurance presentation is an overview of the history and current trends in software trustworthiness, delivered by the technical director of the UK's Trustworthy Software Initiative (TSI). The discussion includes the trustworthy software framework as well as the current focus and future direction of UK TSI.

Windows Operating System Security

16 Hours

This course introduces students to the security aspects of Microsoft Windows. The class begins with an overview of the Microsoft Windows security model and some key components such as processes, drivers, the Windows registry, and Windows kernel. An overview of the users and group permission structure used in Windows is presented along with a survey of the attacks commonly seen in Windows environments. Patching, networking, and the built-in security features of Windows such as the firewall, anti-malware, and BitLocker are all covered in light detail.

Wi-Fi Communications and Security (WNS)

9 Hours

The purpose of the Wi-Fi Communications and Security course is to teach the technologies of the 802.11 family of wireless networking, including the principles of network connectivity and network security. The course is designed to provide a relevant, high-level overview of many elements that are critical components in Wi-Fi networking and security.