

FedVTE Course Library

Advanced PCAP Analysis and Signature Dev	1 Hour	3
Basic Network Traffic Analysis	5 Hours	3
CCNA Security	34 Hours	3
Certified Ethical Hacker (CEHv6)	45 Hours	3
Certified Ethical Hacker (CEHv7)	21 Hours	3
Cisco Network Security 1	9 Hours	4
Cisco Network Security 2	9 Hours	4
CompTIA A+ Prep	20 Hours	4
*CompTIA Network+ Certification Prep	17 Hours	4
CompTIA Security+ (SY0-301) Prep	32 Hours	4
*Cyber Risk Management for Managers	11 Hours	5
Cyber Security Compliance Validation (CCV)	8 Hours	5
*Cyber Security Overview for Managers	6 Hours	5
*DISA Assured Compliance Assessment Solution (ACAS)	32 Hours	5
DISA HBSS Admin 4.5 (2011 Version)	32 Hours	5
DISA HBSS Admin MR4 (2012 Version)	32 Hours	5
DISA HBSS Advanced 4.5 (2011 Version)	32 Hours	6
DISA HBSS Advanced MR4 (2012 Version)	32 Hours	6
DISA HBSS Management Roles	1 Hour	6
DISA HBSS Supplemental Content	1 Hour	6
DNSSEC Training Workshop	2 Hours	6
DoD NetOps 100 and 200	4 Hours	7
Email Authentication Workshop	4 Hours	7
Emerging Cyber Security Threats (2010)	13 Hours	7
Inside Botnets	3 Hours	7
Internet Security Fundamentals	3 Hours	7
Introduction to HTTP/HTTPS Analysis	5 Hours	8
Introduction to Insider Threat	5 Hours	8
Introduction to IPv6	5 Hours	8

Introductory Control Systems Security (ICSST)	6 Hours	8
IPv6 Security	1 Hour	8
ISACA Certified Information Security Auditor	21 Hours	9
ISACA Certified Information Security Manager	18 Hours	9
(ISC)2™ CAP (R) Prep	10 Hours	9
*(ISC)2™ CISSP Certification Prep	20 Hours	9
(ISC)2™ CISSP (R) Certification Prep Version 2	27 Hours	9
(ISC)2™ CISSP Concentration: ISSAP	15 Hours	10
(ISC)2™ CISSP Concentration: ISSEP	12 Hours	10
(ISC)2™ CISSP Concentration: ISSMP	13 Hours	10
(ISC)2™ Systems Security Certified Practitioner	16 Hours	10
Malware Analysis	12 Hours	10
Mobile Security	19 Hours	10
Monitoring for Insider Threat	6 Hours	11
NCSD TDP Information Security Fundamentals	13 Hours	11
NCSD TDP Intro to Digital Investigations	1 Hours	11
*Network Monitoring with Open Source Tools	5 Hours	11
Networking Fundamentals	3 Hours	11
*Penetration Testing	14 Hours	12
Python Scripting for SiLK	3 Hours	12
Reverse Engineering 101	8 Hours	12
Supply Chain Awareness	1 Hour	12
*Technical Mentoring – Technical Writing	3 Hours	12
US-CERT TM Incident Handler	40 Hours	13
US-CERT TM Malware Analysis	7 Hours	13
US-CERT TM Malware Analyst	8 Hours	13
US-CERT TM Network Analyst	30 Hours	13
Using Linux for Analysis (ULA)	4 Hours	13

*Course added January 2013

Advanced PCAP Analysis and Signature Dev **1 Hour**

The Advanced PCAP Analysis and Signature Development (APA) course takes users through an introduction to rules, goes over example syntax, protocols and expressions. This course contains several supporting video demonstrations as well as lab exercises writing and testing basic rules.

Basic Network Traffic Analysis **5 Hours**

This course addresses network security from the traffic analysis perspective. Topics include What is Network Security, Why Should You Care About Network Security, Implementing Network Security, and several topics on protocols and DNS. This course includes several supporting video demonstrations, lab exercises, and a final quiz.

CCNA Security **34 Hours**

The CCNA Security course is aimed at those who already have experience with routers and basic level networking skills, and those who may be interested in taking the CCNA Security exam. Content covered in the CCNA Security course include protocol sniffers, analyzers, TCP/IP, desktop utilities, Cisco IOS, the Cisco VPN, a Cisco simulation program called Packet Tracer, and some web-based resources. Students will get an in-depth theoretical understanding of network security, knowledge and skills designed to implement it.

Certified Ethical Hacker (CEHv6) **45 Hours**

The CEHv6 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. 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 (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.

Cisco Network Security 1 9 Hours

This is the first of two courses focusing on network security in Cisco products such as routers, switches, and firewalls. The course introduces network security, vulnerabilities, threats, attacks, attack examples and vulnerability analysis. The course includes several reinforcing video demonstrations.

Cisco Network Security 2 9 Hours

This is the second of two courses focusing on network security in Cisco products such as routers, switches, and firewalls. Topics in this course include intrusion detection and prevention, encryption and VPN technology, configuring VPNs, secure network architecture, and PIX contexts, failover and management. Several reinforcing video demonstrations are included with this course.

CompTIA A+ Prep 20 Hours

This certification prep course prepares students to sit for the CompTIA A+ certification exam as well teaches valuable lessons to the student that can be used in the workplace. The A+ certification is described as being the starting point for a career in IT. The exam covers maintenance of PCs, mobile devices, laptops, operating systems and printers. This certification prep course includes several reinforcing video demonstrations and hands-on labs.

***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, 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.

***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 concluding with response and recovery. An administrator's focused cyber risk management course will be available in FedVTE during summer 2013.

Cyber Security Compliance Validation (CCV) 8 Hours

This course introduces the Cybersecurity Compliance Validation (CCV) assessment processes, team roles and responsibilities, and the technical criteria that is used as the basis for assessing US Federal Departments/Agencies. The course contains supplemental demonstrations and a senior management briefing.

***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.

***DISA Assured Compliance Assessment Solution (ACAS) 32 Hours**

This course is intended for Operators and Supervisors of ACAS within the 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 4.5 (2011 Version) 32 Hours

This 32 hour DISA Host Based Security System Course is mandatory for all administrators of the HBSS 4.5 MR1 baseline within the DOD. The HBSS course contains 29 demonstrations, 18 hands-on labs, 63 lectures, and a quiz that users must pass to receive their certificate of completion.

DISA HBSS Admin MR4 (2012 Version) 32 Hours

This 32 hour DISA Host Based Security System Course is mandatory for all administrators of the HBSS MR4 baseline within the DOD. The HBSS course contains 29 demonstrations, 18 hands-on labs, 63 lectures, and a quiz that users must pass to receive their certificate of completion.

DISA HBSS Advanced 4.5 (2011 Version)

32 Hours

This 32 hour DISA Host Based Security System Course is a follow-on from the Admin version of the course and introduces new products and advanced topics. It is intended for administrators of the HBSS 4.5 MR1 baseline within the DOD. The HBSS course contains 20 demonstrations, 18 hands-on labs, 49 lectures, and a quiz that users must pass to receive their certificate of completion.

DISA HBSS Advanced MR4 (2012 Version)

32 Hours

This 32 hour DISA Host Based Security System Course is a follow-on from the Admin version of the course and introduces new products and advanced topics. It is intended for administrators of the HBSS MR4 baseline within the DOD. The HBSS course contains 20 demonstrations, 18 hands-on labs, 49 lectures, and a quiz that users must pass to receive their certificate of completion.

DISA HBSS Management Roles

1 Hour

This 1 hour DISA Host Based Security System Course includes an introductory module designed to familiarize those without previous knowledge of HBSS to the components of the system and how the DOD is using it. It also includes a module that will instruct those in management roles how to maintain compliance with HBSS directives, as well as, support some of their other responsibilities using components of the system.

DISA HBSS Supplemental Content

1 Hour

This 1 hour DISA Host Based Security System Course includes a quick introduction to provide HBSS administrators' senior leaders with the information necessary to champion HBSS within their organization. It also provides administrators with multiple modules that provide scenario-based training covering topics that did not make it into the admin or advanced courses.

DNSSEC Training Workshop

2 Hours

This course covers the basics of DNSSEC, how it integrates into the existing global DNS and provides a step-by-step process to deploying DNSSEC on existing DNS zones. Topics include DNSSEC introduction, DNSSEC mechanisms, signing a zone, delegation signer (DS) RRs, setting up a secure resolver, server operational considerations and DNSSEC conclusions. Video demonstrations supplement this training.

DoD NetOps 100 and 200 **4 Hours**

The DoD NetOps 100 (NetOps Overview) course is designed to give students an understanding of where DoD is driving and why it is important to have a joint perspective. NetOps 200 (NetOps Applied to GIG Operations) provides an overview on some of the tools, technologies, and architectures. Topics include evolution of NetOps, Net-Centric Operations & Warfare (NCOW), Global Information Grid (GIG), elements of NetOps and GIG command and control requirements.

Email Authentication Workshop **4 Hours**

This curriculum provided by Online Trust Alliance (OTA) includes an overview of the issues and standards of email with detailed discussion focusing on implementing and testing Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM). Topics include an email authentication workshop introduction, securing the email channel, OTA recommendations – email authentication and deployment guide, case studies and context and resources.

Emerging Cyber Security Threats (2010) **13 Hours**

This course covers a broad range of cyber security elements that pose threats to your information security posture. The various threats are covered in detail followed by mitigation strategies and best practices. Topics include cyber security policy, knowing your enemy, mobile device security, cloud computing security, Radio Frequency Identification (RFID) security, LAN security using switch features, securing the network perimeter, securing infrastructure devices, security and DNS and IPv6 security. Video demonstrations are included throughout to reinforce concepts.

Inside Botnets **3 Hours**

This course is an introduction to botnet technologies and motives. The course begins with an introduction and works into the architecture, coordination, and how botnets are operated. Also covered are current trends in botnet technology and how to defend against botnets. Besides several chapter review quizzes, a lab exercise is included that walks students through the process of building and controlling a botnet, and executing attacks against other hosts.

Internet Security Fundamentals **3 Hours**

The Internet Security Fundamentals course begins with an overview of how the Internet works and an introduction to security. Students also receive an overview of the OSI Reference Model, network routing, IPv4, and DNS concluding with a “How the Internet Works” quiz.

Introduction to HTTP/HTTPS Analysis **5 Hours**

The purpose of this module is to explain the HTTP and HTTPS protocols, to demonstrate attacks using these protocols, and to provide experience in analyzing these attacks. Topics include an introduction to HTTP-HTTPS analysis, purpose of HTTP, HTTP protocol, examples of HTTP request and response, state in HTTP, HTTPS protocol, detecting and analyzing attacks, using packets, Wireshark: SiLK Analysis Start Rfilter, types of attacks, information gathering, server behavioral analysis, packet-based detecting gathering, flow-based detecting gather, log-based detecting gathering, cross-site scripting, packet-and-flow-based detecting XSS, Cross-Site Request Forgery (CSRF), scope of CSRF attacks, detecting and preventing CSRF, SQL injection definition and scope, blind SQL injection, fingerprinting SQL database, detecting SQL inject, CGI BIN attacks, HTTP response splitting and HTTP request smuggling. Video demonstrations, a lab, and a quiz are part of the training.

Introduction to Insider Threat **5 Hours**

The insider threat course introduces what insider threat is, types of threats posed, who the malicious insiders are, and insider threat mitigation. There are several exercises reviewing insider IT sabotage as well as several insider threat case studies.

Introduction to IPv6 **5 Hours**

This class provides a brief primer on IPv6. It covers the features of IPv6, compares it to IPv4, and describes security features in detail. It covers transition strategies and finishes with demos of the suite on various operating systems and includes a hands-on lab.

Introductory Control Systems Security (ICSST) **6 Hours**

The Introduction to Control Systems Security is a DHS course that discusses the vulnerabilities of SCADA systems, the impact if those vulnerabilities were exploited, how to recognize and report a cyber-incident, and mitigation approaches. Reinforcing demos are included in this course as well as a Control System Security Program Overview and FAQ.

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, 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 18 Hours

The ISACA Certified Information Security Manager (CISM) certification prep course prepares students to sit for the management-focused CISM exam as well as strengthens their information security management expertise through the in-depth courseware and reinforcing demonstrations. Topics include CISM introduction, information security governance, information risk management, information security program development, information security program management, incident management and response. Video demonstrations and a quiz are included in the training.

(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™ 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 (R) Certification Prep Version 2 27 Hours

This certification prep course, complete with practice quizzes for each domain as well as a 100-question final quiz is designed to prepare the student to sit for the (ISC)2 Certified Information Systems Security Professional (CISSP) certification exam, as well as apply knowledge from the vast breadth of information security content in their everyday duties. The course was developed based on the 10 (ISC)2 CISSP domains.

(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 100-question practice exam and includes video demonstrations reinforcing 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 towards 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.

Malware Analysis 12 Hours

This course is for technical staff responsible for handling, storing, and analyzing malicious code. It provides a basic introduction to malware analysis, best practices, trends and intruder techniques, and analyzing and characterizing malicious code.

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 and investigations. The course contains video demonstrations, exercises, and a final quiz.

Monitoring for Insider Threat **6 Hours**

The purpose of this module is to raise awareness of insider threat risks, identify the indicators and precursors of malicious acts, demonstrate tools to detect malicious behavior, and review actual cases to show how countermeasures can be effective. Topics include monitoring strategies for insider threat detection, malicious insider overview, problem areas on defense, desired and current state, 2009 E-Crime Watch Survey, overview of prior research, insider threat portfolio, types of insider crime, insider IT sabotage, unknown access paths, monitoring strategies, perimeter controls problem and solution strategies, sabotage exfiltrating credentials of the IRC, types of fraud, fraud considerations, theft of intellectual property (IP), top observed theft of IP exploits and vulnerabilities, data leakage problem, rogue devices problem, remote access attempts problem, case studies of IP theft, deriving candidate controls, deriving controls and indicators and deriving controls. Video demonstrations, a lab, and a quiz are part of the training.

NCS D TDP Information Security Fundamentals **13 Hours**

This competency area provides NCS D staff with an overview of basic concepts in information security. It builds upon and extends the general IT security awareness training required of all federal employees. Topics include an introduction and overview, history and development of the Internet, common threats, vulnerabilities and attacks, risk management, resilience management, incident management, incident response, overview of US-CERT, overview of control systems security and overview of critical infrastructure cyber security.

NCS D TDP Intro to Digital Investigations **1 Hours**

This presentation covers computer forensics (including an introduction) and topics such as the process, following on-site process for encryption, memory and verification, following the process for analysis, report findings and data preservation, and computer forensic laws. A quiz is part of the training.

***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, tools and their capabilities. After completion of the course, students should be able to detect attacks using network monitoring tools.

Networking Fundamentals **3 Hours**

This course covers the OSI model, media, routing, and the TCP/IP stack. The material is extracted from the introduction to the Cisco CCNA training course.

***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.

Python Scripting for SiLK **3 Hours**

The purpose of this course is to provide analysts with an introduction to the ways Python scripting can extend and automate different analysis tasks with a specific focus on scripting with SiLK tool suite. Video demonstrations, hands-on exercises, and a final quiz are part of this course.

Reverse Engineering 101 **8 Hours**

This course provides an introduction to x86 assembly code, discusses several reverse engineering tools, explores the fundamentals of the Microsoft Windows operating system and API, and the basics of performing static analysis of Windows malware. Topics include reverse engineering in context of malware engineering, MS Windows: An interface to a computer, MS Windows data types, Windows API exercise: writing code, reverse engineering tools: IDA Pro and OllyDbg the Debugger, computer mechanics and assembly code, Intel X86 architecture, register and arithmetic, how stack memory works, control flow and test instructions, common constructs/structure, call address/function, crypto algorithms and a “Where to Go from Here” summary. Video demonstrations, labs, and a quiz are part of the training.

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.

***Technical Mentoring – Technical Writing** **3 Hours**

The Technical Writing course is designed for staff who are not professionally trained writers but who must write as part of their jobs. The documents they write most often include emails, reports, leadership alerts and senior leadership dailies. Several writing examples and activities compliment the course lecture.

US-CERT TM Incident Handler **40 Hours**

The purpose of this course is to learn about fundamental concepts for performing incident handling. Along with supporting labs, video demonstrations, and document resources, topics include CSIRT management issues, code of conduct, incident handling methodology, coordinating response, handling major events, working with law enforcement, malware handling and storage, vulnerability remediation, analysis and reporting. The course includes a quiz as well.

US-CERT TM Malware Analysis **7 Hours**

This course is geared to handling, storing, and analyzing of malicious code. Topics include malware handling and storage, malware obfuscation and content from inside botnets, building a runtime analysis environment, introduction to malware analysis, malware runtime analysis (US-CERT TM), reverse engineering 101 (US-CERT TM) and malicious code courses. Video demonstrations, labs, and quizzes are part of the training.

US-CERT TM Malware Analyst **8 Hours**

The purpose of this course is to learn about fundamental concepts for handling, storing and analyzing malicious code. Topics in this course include basic log file analysis, data hiding and encryption, working with law enforcement and introduction to malware analysis. This course contains several supporting labs, video demonstrations, and a final quiz.

US-CERT TM Network Analyst **30 Hours**

The purpose of this course is to learn how to perform surface analysis on network traffic. Topics include intro to PCAP analysis and Sig development, malware handling and storage, malware obfuscation, network security from traffic analysis perspective, Python scripting for SiLK, inside botnets and IPv6. This course contains several supporting video demonstrations and hands-on exercises.

Using Linux for Analysis (ULA) **4 Hours**

This course describes the basic architecture of a Linux system, explains how to use common command line utilities on a Linux system for analysis purposes, and how to perform analysis work such as malware and incident response analysis. This course includes several reinforcing video demonstrations.