VANTAGEPOINT
I.T. TRAINING & CONSULTING

Technology Innovation Centre (UTECH), 237 Old Hope Road, Kingston 6, Jamaica W.I.
Tel: 876-970-0197, Fax: 927-1925, Email: info@vantagepointitc.com Website: www.vantagepointitc.com

CompTIA® Advanced Security Practitioner (CASP) (Exam CAS-002)

Course Specifications

Course Number:

093023

Course Length:

5 days

Course Description

Overview:

You have experience in the increasingly crucial field of information security, and now you're ready to take that experience to the next level. *CompTIA® Advanced Security Practitioner (CASP) (Exam CAS-002)* is the course you will need to take if your job responsibilities include securing complex enterprise environments. In this course, you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened. Today's IT climate demands individuals with demonstrable skills, and the information and activities in this course can help you develop the skill set you need to confidently perform your duties as an advanced security professional.

This course can also benefit you if you intend to pass the CompTIA Advanced Security Practitioner (CAS-002) certification examination. What you learn and practice in this course can be a significant part of your preparation.

Course Objectives:

In this course, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security.

You will:

- Manage risk in the enterprise.

- Integrate computing, communications, and business disciplines in the enterprise.
- Use research and analysis to secure the enterprise.
- Integrate advanced authentication and authorization techniques.
- Implement cryptographic techniques.
- Implement security controls for hosts.
- Implement security controls for storage.
- Analyze network security concepts, components, and architectures, and implement controls.
- Implement security controls for applications.
- Integrate hosts, storage, networks, and applications in a secure enterprise architecture.
- Conduct vulnerability assessments.
- Conduct incident and emergency responses.

Target Student:

This course is designed for IT professionals who want to acquire the technical knowledge and skills needed to conceptualize, engineer, integrate, and implement secure solutions across complex enterprise environments. The target student should aspire to apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies; translate business needs into security requirements; analyze risk impact; and respond to security incidents.

This course is also designed for students who are seeking the CompTIA Advanced Security Practitioner (CASP) certification and who want to prepare for Exam CAS-002. Students seeking CASP certification should have at least 10 years of experience in IT management, with at least 5 years of hands-on technical security experience.

Prerequisites:

To be fit for this advanced course, you should have at least a foundational knowledge of information security. You may also demonstrate this level of knowledge by passing the Security+ (SY0-401) exam.

Course Content

Lesson 1: Managing Risk

Topic A: Identify the Importance of Risk Management

Topic B: Assess Risk

Topic C: Mitigate Risk

Topic D: Integrate Documentation into Risk Management

Lesson 2: Integrating Computing, Communications, and Business Disciplines

Topic A: Facilitate Collaboration Across Business Units

Topic B: Secure Communications and Collaboration Solutions

Topic C: Implement Security Activities Throughout the Technology Life Cycle

Lesson 3: Using Research and Analysis to Secure the Enterprise

Topic A: Determine Industry Trends and Effects on the Enterprise

Topic B: Analyze Scenarios to Secure the Enterprise

Lesson 4: Integrating Advanced Authentication and Authorization Techniques

Topic A: Implement Authentication and Authorization Technologies

Topic B: Implement Advanced Identity Management

Lesson 5: Implementing Cryptographic Techniques

Topic A: Describe Cryptographic Concepts

Topic B: Choose Cryptographic Techniques

Topic C: Choose Cryptographic Implementations

Lesson 6: Implementing Security Controls for Hosts

Topic A: Select Host Hardware and Software

Topic B: Harden Hosts

Topic C: Virtualize Servers and Desktops

Topic D: Implement Cloud Augmented Security Services

Topic E: Protect Boot Loaders

Lesson 7: Implementing Security Controls for Enterprise Storage

Topic A: Identify Storage Types and Protocols

Topic B: Implement Secure Storage Controls

Lesson 8: Analyzing and Implementing Network Security

Topic A: Analyze Network Security Components and Devices

Topic B: Analyze Network-Enabled Devices

Topic C: Analyze Advanced Network Design

Topic D: Configure Controls for Network Security

Lesson 9: Implementing Security Controls for Applications

Topic A: Identify General Application Vulnerabilities

Topic B: Identify Web Application Vulnerabilities

Topic C: Implement Application Security Controls

Lesson 10: Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture

Topic A: Implement Security Standards in the Enterprise

Topic B: Select Technical Deployment Models

Topic C: Secure the Design of the Enterprise Infrastructure

Topic D: Secure Enterprise Application Integration Enablers

Lesson 11: Conducting Vulnerability Assessments

Topic A: Select Vulnerability Assessment Methods

Topic B: Select Vulnerability Assessment Tools

Lesson 12: Responding to and Recovering from Incidents

Topic A: Design Systems to Facilitate Incident Response

Topic B: Conduct Incident and Emergency Responses