CompTIA Advanced Security Practitioner (CASP)

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. This course prepares students for the CAS-002 exam.

Length Days: 5

PREREQUISITES

- CompTIA Network+ Certification
- CompTIA Security+ Certification
- CompTIA A+ Certification

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

Although not required, we suggest that you either take the following courses or possess the equivalent knowledge in the areas of computer networking and computer maintenance:

- CompTIA® Network+® (N10-005) or CompTIA® Network+® (N10-006)
- CompTIA® A+®: A Comprehensive Approach (Exams 220-801 and 220-802)

TARGET AUDIENCE

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.

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.

COURSE OUTLINE

1 - MANAGING RISK

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

2 - INTEGRATING COMPUTING, COMMUNICATIONS, AND BUSINESS DISCIPLINES

- Facilitate Collaboration Across Business Units
- Secure Communications and Collaboration Solutions
- Implement Security Activities Throughout the Technology Life Cycle

3 - USING RESEARCH AND ANALYSIS TO SECURE THE ENTERPRISE

- Determine Industry Trends and Effects on the Enterprise
- Analyze Scenarios to Secure the Enterprise

4 - INTEGRATING ADVANCED AUTHENTICATION AND AUTHORIZATION TECHNIQUES

- Implement Authentication and Authorization Technologies
- Implement Advanced Identity Management

5 - IMPLEMENTING CRYPTOGRAPHIC TECHNIQUES

- Describe Cryptographic Concepts
- Choose Cryptographic Techniques
- Choose Cryptographic Implementations

6 - IMPLEMENTING SECURITY CONTROLS FOR HOSTS

- Select Host Hardware and Software
- Harden Hosts
- Virtualize Servers and Desktops
- Implement Cloud Augmented Security Services
- Protect Boot Loaders

7 - IMPLEMENTING SECURITY CONTROLS FOR ENTERPRISE STORAGE

- Identify Storage Types and Protocols
- Implement Secure Storage Controls

8 - ANALYZING AND IMPLEMENTING NETWORK SECURITY

- Analyze Network Security Components and Devices
- Analyze Network-Enabled Devices
- Analyze Advanced Network Design
- Configure Controls for Network Security

9 - IMPLEMENTING SECURITY CONTROLS FOR APPLICATIONS

- Identify General Application Vulnerabilities
- Identify Web Application Vulnerabilities
- Implement Application Security Controls

10 - INTEGRATING HOSTS, STORAGE, NETWORKS, AND APPLICATIONS IN A SECURE ENTERPRISE ARCHITECTURE

- Implement Security Standards in the Enterprise
- Select Technical Deployment Models
- Secure the Design of the Enterprise Infrastructure
- Secure Enterprise Application Integration Enablers

11 - CONDUCTING VULNERABILITY ASSESSMENTS

- Select Vulnerability Assessment Methods
- Select Vulnerability Assessment Tools

12 - RESPONDING TO AND RECOVERING FROM INCIDENTS

- Design Systems to Facilitate Incident Response
- Conduct Incident and Emergency Responses