Access Control, Authentication, and Public Key Infrastructure

Code: 3426

5 days

Course Overview

This course defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides learners a professional resource detailing how to put access control systems to work in addition to how to test and manage them.

In addition to premium instructional content from Jones & Bartlett Learning's comprehensive Information Systems Security and Assurance (ISSA) curriculum, this course provides access to a customized 'virtual sandbox' learning environment that aggregates an unparalleled spectrum of cybersecurity applications. Providing instant, unscheduled access to labs from the convenience of a web-browser, this course allows you to practice 'white hat' hacking on a real IT infrastructure—these are not simulations. Winner of the 'Security Training and Educational Programs' top prize at the prestigious 2013 Global Excellence Awards by Info Security Products Guide, the industry's leading information security research and advisory guide, these labs provide valuable exposure to complex, real world challenges and over 200 hours of training exercises on how hackers and perpetrators use these applications and tools.

Certification:

This course covers content within the following industry certification exams:

- System Security Certified Practitioner (SSCP) - two content domains covered
- Certified Information Systems Security Professional (CISSP) - four content domains covered
- Security + - one content domain covered
- National Institute of Standards and Technology (NIST) - five content domains covered
- 8570.01 - two content domains covered

Who Needs To Attend

Information security analysts

Course Details
Topics Include

- Define authorization and access to an IT infrastructure based on an access control policy framework
- Mitigate risk to an IT infrastructure's confidentiality, integrity, and availability with sound access controls
- Analyze how a data classification standard impacts an IT infrastructure's access control requirements and implementation
- Develop an access control policy framework consisting of best practices for policies, standards, procedures, and guidelines to mitigate unauthorized access
- Define proper security controls within the user domain to mitigate risks and threats caused by human behavior
- Implement appropriate access controls for information systems within IT infrastructures
- Design appropriate authentication solutions throughout an IT infrastructure based on user types and data classification standards
- Implement a secure remote access solution
- Implement PKI and encryption solutions to ensure the confidentiality of business communications
- Mitigate risk from unauthorized access to IT systems through proper testing and reporting

Course Outline

1. The Need for Access Control Systems
   - Access Control Framework
   - Assessing Risk and Its Impact on Access Control
   - Business Drivers for Access Controls
   - Access Controls Law, Policies, and Standards
   - Security Breaches and the Law

   - Mapping Business Challenges to Access Control Types
   - Human Nature and Organizational Behavior
   - Access Control for Information Systems
   - Physical Security and Access Control
   - Access Control in the Enterprise

3. Implementing, Testing, and Managing Access Control Systems
   - Access Control System Implementations
   - Access Control Solutions for Remote Workers
   - Public Key Infrastructure and Encryption
   - Testing Access Control Systems
   - Access Control Assurance
Prerequisites

General knowledge of networking and management information systems