Information Systems Security – C845
Course Feedback

Overview

IT security professionals must be prepared for the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection and prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures. This course provides a comprehensive, up-to-date global body of knowledge that ensures students have the right information security knowledge and skills to be successful in IT operational roles to mitigate security concerns and guard against the impact of malicious activity. Students demonstrate how to manage and restrict access control systems; administer policies, procedures, and guidelines that are ethical and compliant with laws and regulations; implement risk management and incident handling processes; execute cryptographic systems to protect data; manage network security; and analyze common attack vectors and countermeasures to assure information integrity and confidentiality in various systems. This course prepares students for the Systems Security Certified Practitioner (ISC2 SSCP) certification exam.

Competencies

- **Manage Control Access**
  The graduate manages control access to privileged, confidential, or proprietary resources.

- **Security Operations Concepts and Policies**
  The graduate evaluates security operations concepts, and policies to ensure the confidentiality, integrity, and availability of information assets is applied.

- **Processes and Security Threats**
  The graduate proposes security risks mitigations processes to identify, evaluate, prioritize, and prevent potential security threats.

- **Cyber Operations Effectiveness**
  The graduate evaluates security incident handling plans to protect and preserve organization assets and data.

- **Cryptographic Systems and Operations Execution**
  The graduate evaluates cryptographic systems and operations to protect data security.
The graduate defends the security of a network by maintaining the confidentiality, integrity, and availability (CIA) of the information transmitted over communication networks.

Security Countermeasures
The graduate evaluates security concerns with countermeasures to guard against the impact of malicious activity to end-point device security, virtualization, cloud, and large-scale distributed systems.

Learning

Getting Started
Welcome to Information Systems Security. This course employs uCertify learning resources that contain all of the necessary reading materials, knowledge checks, and videos needed to prepare you for the (ISC)² SSCP certification exam.

For the best understanding of the course content, complete each lesson. To help you track your progress, we suggest you follow the pacing guide identified at the beginning of the course.

Competency will be demonstrated by the successful completion of the (ISC)² SSCP certification exam, scheduled at a professional test center. Those who pass the exam will earn an Associate of (ISC)² designation. See the (ISC)² SSCP Certification Process link within the Course Information section below for a complete explanation.

Assessments

Objective Assessment: ISC² - Systems Security Certified Practitioner, Associate of (ISC)²

STATUS: Not Attempted
# OF ITEMS:
TIME ALLOTTED: minutes
CODE: IOV1
A score of **Competent** or **Exemplary** is required to pass all assessments. Passing a preassessment does not guarantee you will pass the high stakes assessment.

On objective assessments, you will be charged a retake fee for the third attempt and every attempt thereafter. For more information click here.