Systems Security Certified Practitioner (SSCP) Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 7 domains:

* Access Controls
* Security Operations and Administration
* Risk Identification, Monitoring, and Analysis
* Incident Response and Recovery
* Cryptography
* Network and Communications Security
* Systems and Application Security

Required Exams

Candidates earn their SSCP Certification by successfully completing one exam:

SSCP Certification exam

Audience Profile

The SSCP is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets, including those in the following positions:

* Network Security Engineer
* Security Consultant/Specialist

* Systems Administrator
* Security Administrator
* Security Analyst
* Systems/Network Analyst
* Systems Engineer
* Database Administrator
*

Course Objectives

Outline

Module 1: Access Controls * Implement and maintain authentication methods
* Support internetwork trust architectures
* Participate in the identity management lifecycle
* Implement access controls
Module 2: Security Operations and Administration * Comply with codes of ethics
* Understand security concepts
* Document, implement, and maintain functional security controls
* Participate in asset management
* Implement security controls and assess compliance
* Participate in change management
* Participate in security awareness and training
* Participate in physical security operations (e.g., data center assessment, badging)
Module 3: Risk Identification, Monitoring, and Analysis * Understand the risk management process
* Perform security assessment activities
* Operate and maintain monitoring systems (e.g., continuous monitoring)
* Analyze monitoring results
Module 4: Incident Response and Recovery * Support incident lifecycle
* Understand and support forensic investigations
* Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) activities
Module 5: Cryptography * Understand fundamental concepts of cryptography
* Understand reasons and requirements for cryptography
* Understand and support secure protocols
* Understand Public Key Infrastructure (PKI) systems
Module 6: Network and Communications Security * Understand and apply fundamental concepts of networking
* Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)
* Manage network access controls
* Manage network security
* Operate and configure network-based security devices
* Operate and configure wireless technologies
Module 7: Systems and Application Security * Identify and analyze malicious code and activity
* Implement and operate endpoint device security
* Operate and configure cloud security

* Operate and secure virtual environments