SYSTEMS SECURITY CERTIFIED PRACTITIONER

DURATION: 5 DAYS

COURSE OVERVIEW

Looking to move up in the information security field? If you have at least one year of security experience, you qualify for the Systems Security Certified Practitioner (SSCP) certification, which offers junior security professionals a way to validate their experience and demonstrate competence with (ISC)²®'s seven domains. A free copy of the Official (ISC)² Guide to The SSCP® CBK® from (ISC)² Press and a SSCP certification practice exam from Self-Test Software are included with the course. Interested in group training toward 8570.1 compliancy? This course can be a component of our 8570.1 Training Solution that can also include assessments, certification preparation and program management, post training and testing, 8570 compliancy tracking and reporting, and continuing education. Learn more about our 8570 Training Solution by contacting us at 1-888-DOD-8570

TARGET AUDIENCE

This course has proven to be very valuable to personnel in an organization that are fairly new to the field of information security or that do not have security as their primary job responsibility. Many of the attendees have been Information Systems Auditors, System and Network Administrators, Application Programmers and Project Managers.

COURSE OBJECTIVES

In-depth coverage of the seven domains-required to pass the SSCP Exam:

1. Access Controls
2. Security Operations and Administration
3. Analysis and Monitoring
4. Cryptography
5. Networks and Telecommunications
6. Malicious Code/Malware
7. Risk, Response, and Recovery

COURSE CONTENT

1. Testing-Taking Tips and Study Techniques

    Preparation for the SSCP Exam

- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam the First Time

2. Security Operations and Administration

- Change Control/Configuration Management
- Dual Control, Separation of Duties, Rotation of Duties
- Vulnerability Assessment and Pen-Testing

3. Access Controls

- AAA
- Authentication Methods (Types 1, 2, & 3)
- Authorization - DAC, RBAC, MAC
- Accounting - Logging, Monitoring, Auditing
- Central/Decentralized and Hybrid Management
- Single Sign-On - Kerberos, Radius, Diameter, TACACS
- Vulnerabilities - Emanations, Impersonation, Rouge Infrastructure, Social Engineering

4. Cryptography

- Intro/History
- Symmetric
- Asymmetric
- Hashing
- Cryptosystems - SSL, S/MIME, PGP
- PKI
- Cryptanalysis

5. Malicious Code and Malware

- Layering, Data Hiding, and Abstraction
- Database Security
- AI
- OOD
- Mobil Code
- Malware Architecture Problems - Covert Channels + TOC/TOU, Object Reuse
- Network Vulnerabilities

6. Networks and Telecommunications

OSI/DoD TCP/IP Models
TCP/UDP/ICMP/IP
Ethernet
Devices - Routers/Switches/Hubs
Firewalls
Wireless
WAN Technologies - X.25/Frame Relay/PPP/ISDN/DSL/Cable
Voice - PBX/Cell Phones/VOIP
IP Sec

7. Risk, Response, and Recovery

CIA
Roles and Responsibilities - RACI
Asset Management
Taxonomy - Information Classification
Risk Management
Policies, Procedures, Standards, Guidelines, Baselines
Knowledge Transfer - Awareness, Training, Education
BIA Policy
BIA Roles and Teams
Data Backups, Vaulting, Journaling, Shadowing
Alternate Sites
Emergency Response
Required notifications
BIA Tests

8. Analysis and Monitoring

Ethics - Due Care/Due diligence
Intellectual Property
Incident Response
Forensics
Evidence
Laws - HIPAA, GLB, SOX

9. Review and Q&A Session

al Review and Test Prep

COURSE PREREQUISITES

Systems administration experience, familiarity with TCP/IP, and an understanding of UNIX, Linux, and Windows. This advanced course also requires intermediate-level knowledge of the security concepts covered in our Security+ Prep Course