

Systems Security Certified Practitioner (SSCP) certification

Length: 5 Days

Summary: 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.

Certification: SSCP

SSCP certification requires passing the SSCP exam (administered separately). Successful applicants for SSCP certification must have at least one year of direct, full-time security experience in one or more of the seven domains of the (ISC)² CBK.

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
- IPsec

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

- Final Review and Test Prep
-