Systems Security Certified Practitioner
SSCP
Course Syllabus
10 Hours

Course Description
The Systems Security Certified Practitioner (SSCP) certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. It provides industry-leading 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 SSCP indicates a practitioner's technical ability to tackle the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more. This course covers the objectives for the certification exam:

- **Systems Security Certified Practitioner (SSCP)**

Learning Objectives
Upon completion of the course, students will understand:

- Authentication mechanisms including single and multifactor authentication
- Function of trust architectures, including one-way, two-way, and transitive trust relationships
- Management life cycle and specific access controls such as mandatory, non-discretionary, role-based, and attitude based-controls
- Management of hardware, software, and data asset best practices
- Best practices for implementing compliance, participating in change management activities, and conducting security awareness and training in the enterprise
- Identifying, evaluating, and prioritizing potential threats to the organization's network and systems are critical for proper IT systems security
- Risk management process, including risk assessment, treatment, and assessment activities
- Outlines of best practices for operating and maintaining monitoring systems, and analyzing monitoring results using security analytics, metrics, and trends
- Cryptography best practices including hashing, salting, encryption, and digital signature usage
- Network security best practices for OSI and TCP/IP models, as well as common ports and protocols
- Secure practices for managing LAN-based, network-based, and wireless platforms technologies
- Analysis of malicious activity, including malicious code and countermeasures
- Best practices for endpoint device and cloud security, including host-based firewalls, HIDS, virtualization, and service models
- Securing big data systems and operating and securing virtual environments, including appliance and attack countermeasures

Course Format
SSCP is a self-paced, online course delivered through the learning management system Skillsoft. The site to access the coursework is su.skillport.com. Login credentials will be provided to you on the cohort launch date. If you do not receive them by the launch date, please check your Spam/Junk folder of your email and/or contact your advisor or O2O program coordinator. Once you have logged into your account, you can locate the coursework by selecting "View My Learning Plan."

Coursework is delivered through videos, tutorials, and tests. No textbooks are required for the course; however, students are encouraged to utilize additional resources to assist with certification preparation. Resource Guides with

lists of supplemental study materials for each certification are available at http://libguide.get-vet.syr.edu/curriculum/.

Course Completion Requirements

SSCP coursework is due within 90 days from the assignment date. The course hours listed at the top of the syllabus reflect the time it would take to click through the slides and do not account for taking notes or the end of module tests. You must complete all eight modules listed within Topic 1. Successful completion of a module is marked after you review the lesson videos and score 80% or higher on the end of module tests.

At the beginning of a module, you will be asked to take a pre-test. Scoring 80% or higher on the pre-test signifies competence in the information that will be covered; you will therefore be waived from completing the module. A non-credit certificate of completion will be awarded for successful completion of the coursework.

Industry Certification Requirements

In order for the program to fund your SSCP certification exam you will need to meet the SSCP practice exam requirements. Your advisor or O2O program coordinator will provide you with access to the practice exam as well as completion instructions once you have finished the coursework.

Support

- For technical support, please contact Skillsoft Support at support.skillsoft.com
- For course content support, please utilize Skillsoft's "Ask My Mentor" tool, located in the left-hand Menu within the module course player
- For program support or questions, please contact your advisor or O2O program coordinator

Course Outline

Topic 1: Security Foundations for SSCP Certification

1.1 SSCP Domain: Access Controls

1.2 SSCP Domain: Security Operations

1.3 SSCP Domain: Security Administration

1.4 SSCP Domain: Risk Management

1.5 SSCP Domain: Incident Response and Recovery

1.6 SSCP Domain: Cryptography

1.7 SSCP Domain: Network and Communications Security

1.8 SSCP Domain: Systems and Application Security