ISC2 SSCP

ISC2 IT/ICT Security Administration Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

SSCP

ISC2 Systems Security Certified Practitioner

150 Questions Exam – 700/1000 Cut Score – Duration of 240 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the SSCP Certification

Are you interested in passing the ISC2 SSCP exam? First discover, who benefits from the SSCP certification. The SSCP is suitable for a candidate if he wants to learn about Security Administrator. Passing the SSCP exam earns you the ISC2 Systems Security Certified Practitioner title.

While preparing for the SSCP exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SSCP PDF contains some of the most valuable preparation tips and the details and instant access to useful **SSCP study materials just at one click.**

ISC2 SSCP IT/ICT Security Administration Certification Details:

Exam Name	ISC2 Systems Security Certified Practitioner (SSCP)
Exam Code	SSCP
Exam Price	$249 (USD)
Duration	240 mins
Number of Questions	150
Passing Score	700/1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 SSCP Sample Questions**
Practice Exam	**ISC2 SSCP Certification Practice Exam**

SSCP Syllabus:

Topic	**Details**
Security Operations and Administration - 16%	
Comply with codes of ethics	- (ISC)² Code of Ethics - Organizational code of ethics
Understand security concepts	- Confidentiality - Integrity - Availability

Topic	Details
	- Accountability - Privacy - Non-repudiation - Least privilege - Segregation of duties (SoD)
Identify and implement security controls	- Technical controls (e.j., session timeout, password aging) - Physical controls (e.g., mantraps, cameras, locks) - Administrative controls (e.g., security policies, standards, procedures, baselines) - Assessing compliance - Periodic audit and review
Document and maintain functional security controls	- Deterrent controls - Preventative controls - Detective controls - Corrective controls - Compensating controls
Participate in asset management lifecycle (hardware, software and data)	- Process, planning, design and initiation - Development/Acquisition - Inventory and licensing - Implementation/Assessment - Operation/Maintenance - Archiving and retention requirements - Disposal and destruction
Participate in change management lifecycle	- Change management (e.g., roles, responsibilities, processes) - Security impact analysis - Configuration management (CM)
Participate in implementing security awareness and training (e.g., social engineering/phishing)	
Collaborate with physical security operations (e.g.,	

Topic	Details
data center assessment, badging)	
Access Controls - 15%	
Implement and maintain authentication methods	- Single/Multi-factor authentication (MFA) - Single sign-on (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID Connect) - Device authentication - Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))
Support internetwork trust architectures	- Trust relationships (e.g., 1-way, 2-way, transitive, zero) - Internet, intranet and extranet - Third-party connections
Participate in the identity management lifecycle	- Authorization - Proofing - Provisioning/De-provisioning - Maintenance - Entitlement - Identity and access management (IAM) systems
Understand and apply access controls	- Mandatory - Discretionary - Role-based (e.g., attribute-, subject-, object-based) - Rule-based
Risk Identification, Monitoring and Analysis - 15%	
Understand the risk management process	- Risk visibility and reporting (e.g., risk register, sharing threat intelligence/indicators of Compromise (IOC), Common Vulnerability Scoring (CVSS)) - Risk management concepts (e.g., impact assessments, threat modelling) - Risk management frameworks - Risk tolerance (e.g., appetite)

Topic	Details
	- Risk treatment (e.g., accept, transfer, mitigate, avoid)
Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)	
Participate in security assessment and vulnerability management activities	- Security testing - Risk review (e.g., internal, supplier, architecture) - Vulnerability management lifecycle
Operate and monitor security platforms (e.g., continuous monitoring)	- Source systems (e.g., applications, security appliances, network devices, and hosts) - Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring) - Log management - Event aggregation and correlation
Analyze monitoring results	- Security baselines and anomalies - Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines) - Event data analysis - Document and communicate findings (e.g., escalation)
Incident Response and Recovery - 14%	
Support incident lifecycle lifecycle e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO))	- Preparation - Detection, analysis and escalation - Containment - Eradication - Recovery - Lessons learned/implementation of new countermeasure
Understand and support forensic investigations	- Legal (e.g., civil, criminal, administrative) and ethical principles - Evidence handling (e.g., first responder, triage,

Topic	Details
	chain of custody, preservation of scene) - Reporting of analysis
Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	- Emergency response plans and procedures (e.g., information system contingency, pandemic, natural disaster, crisis management) - Interim or alternate processing strategies - Restoration planning - Backup and redundancy implementation - Testing and drills
Cryptography - 9%	
Understand cryptography	- Confidentiality - Integrity and authenticity - Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health information (PHI)) - Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))
Apply cryptography concepts	- Hashing - Salting - Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC) - Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails) - Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA), 256-, 512-, 1024-, 2048-bit keys) - Cryptographic attacks, cryptanalysis, and countermeasures (e.g., quantum computing)
Understand and implement secure protocols	- Services and protocols - Common use cases - Limitations and vulnerabilities

Topic	Details
Understand Public Key Infrastructure (PKI)	- Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow) - Web of Trust (WOT)
Network and Communications Security - 16%	
Understand and apply fundamental concepts of networking	- Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models - Network topologies - Network relationships (e.g., peer-to-peer (P2P), client server) - Transmission media types (e.g., wired, wireless) - Software-defined networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization, automation) - Commonly used ports and protocols
Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name System (DNS) poisoning) and countermeasures (e.g., content delivery networks (CDN))	
Manage network access controls	- Network access controls, standards and protocols (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+)) - Remote access operation and configuration (e.g., thin client, virtual private network (VPN))
Manage network security	- Logical and physical placement of network devices (e.g., inline, passive, virtual)

Topic	Details
	- Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL), firewall zones, micro-segmentation) - Secure device management
Operate and configure network-based security devices	- Firewalls and proxies (e.g., filtering methods, web application firewalls (WAF)) Intrusion detection systems (IDS) and intrusion prevention systems (IPS) - Network intrusion detection/prevention systems - Routers and switches - Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)
Secure wireless communications	- Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC)) - Authentication and encryption protocols (e.g., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP)) - Internet of Things (IoT)
Systems and Application Security - 15%	
Identify and analyze malicious code and activity	- Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless) - Malware countermeasures (e.g., scanners, anti-malware, code signing) - Malicious activity (e.g., insider threat, data theft, distributed denial of service (DDoS), botnet, zero-day exploits, web-based attacks, advanced persistent threat (APT)) - Malicious activity countermeasures (e.g., user awareness, system hardening, patching, sandboxing, isolation, data loss prevention (DLP))
Implement and operate endpoint device security	- Host-based intrusion prevention system (HIPS) - Host-based firewalls - Application white listing - Endpoint encryption (e.g., whole disk encryption)

Topic	Details
	- Trusted Platform Module (TPM) - Secure browsing - Endpoint Detection and Response (EDR)
Administer Mobile Device Management (MDM)	- Provisioning techniques (e.g., corporate owned, personally enabled (COPE), Bring Your Own Device (BYOD)) - Containerization - Encryption - Mobile application management (MAM)
Understand and configure cloud security	- Deployment models (e.g., public, private, hybrid, community) - Service models (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)) - Virtualization (e.g., hypervisor) - Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery) - Data storage, processing, and transmission (e.g., archiving, recovery, resilience) - Third-party/outsourcing requirements (e.g., service-level agreement (SLA), data portability, data destruction, auditing) - Shared responsibility model
Operate and maintain secure virtual environments	- Hypervisor - Virtual appliances - Containers - Continuity and resilience - Attacks and countermeasures - Shared storage

Broaden Your Knowledge with ISC2 SSCP Sample Questions:

Question: 1

Which of these statements about the benefits of VLANs is inaccurate?

a) Increased security
b) Excellent physical segmentation
c) Enhanced performance
d) No additional equipment required for configuration

Answer: b

Question: 2

How many primary types of authentication factors are there?

a) 2
b) 3
c) 7
d) 4

Answer: b

Question: 3

What is the primary purpose of SSO?

a) Authorization
b) Confidentiality
c) Availability
d) Authentication

Answer: d

Question: 4

Which of the following would you use to adequately secure the wireless network of a small office with ten employees, without any excessive administrative burden?

a) WEP (with AES)
b) WPA2 (with AES)
c) WEP-Enterprise
d) WPA2-Enterprise

Answer: b

Question: 5

In which of these control goal and class combinations does a motion sensor fall into?

a) Preventive, technical
b) Detective, technical
c) Preventive, physical
d) Detective, physical

Answer: d

Question: 6

Which of these statements about sharing threat intelligence is inaccurate?

a) The best method is to share as much internal information as possible.
b) It's recommended to set rules about what information can be shared.
c) One often-used standard for threat intelligence sharing is STIX.
d) Identify appropriate threat intelligence information sources.

Answer: a

Question: 7

Using a proprietary forensic tool for investigation relates to which of these reliability factors?

a) Clarity
b) Error rate
c) Credibility
d) Testability

Answer: d

Question: 8

You browse to a website and receive a pop-up message stating your computer is vulnerable and in immediate need of a missing patch. Which of the following might be present on that website?

a) PUA
b) Spyware
c) Virus
d) Scareware

Answer: d

Question: 9

An attacker is using a text file's spaces and tabs to store information. Which of the following is this an example of?

a) Encoding
b) Hashing
c) Steganography
d) Encryption

Answer: c

Question: 10

A company wants to select a dedicated alternative location for continuing its operations in the event of an incident, while minimizing operational downtime.

Which of the following would be most appropriate for that purpose?

a) Hot site
b) Warm site
c) Cold site
d) Mobile site

Answer: a

Avail the Study Guide to Pass ISC2 SSCP IT/ICT Security Administration Exam:

- Find out about the SSCP syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **SSCP syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the SSCP training. Joining the ISC2 provided training for SSCP exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **SSCP sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SSCP practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the SSCP exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the SSCP Certification

EduSum.Com is here with all the necessary details regarding the SSCP exam. We provide authentic practice tests for the SSCP exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **SSCP practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the ISC2 Systems Security Certified Practitioner.

Start Online Practice of SSCP Exam by visiting URL
https://www.edusum.com/isc2/sscp-isc2-systems-security-practitioner