EDUSUM

#1 Online Certification Guide

ISC2 SSCP

ISC2 Systems Security Practitioner Certification Questions & Answers

Exam Summary – Syllabus –Questions

SSCP

ISC2 Systems Security Certified Practitioner (SSCP)

125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your SSCP Certification Well:

The SSCP is best suitable for candidates who want to gain knowledge in the ISC2 Cybersecurity. Before you start your SSCP preparation you may struggle to get all the crucial ISC2 Systems Security Practitioner materials like SSCP syllabus, sample questions, study guide.

But don't worry the SSCP PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the SSCP syllabus?
- How many questions are there in the SSCP exam?
- Which Practice test would help me to pass the SSCP exam at the first attempt?

Passing the SSCP exam makes you ISC2 Systems Security Certified Practitioner (SSCP). Having the ISC2 Systems Security Practitioner certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISC2 Systems Security Practitioner Certification Details:

Exam Name	ISC2 Systems Security Certified Practitioner (SSCP)
Exam Code	SSCP
Exam Price	$249 (USD)
Duration	180 mins
Number of Questions	125
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
Access Controls - 16%	
Implement and maintain authentication methods	- Single/multifactor authentication - Single sign-on - Device authentication - Federated access
Support internetwork trust architectures	- Trust relationships (e.g., 1-way, 2-way, transitive) - Extranet - Third party connections
Participate in the identity management lifecycle	- Authorization - Proofing - Provisioning/de-provisioning - Maintenance - Entitlement - Identity and Access Management (IAM) systems
Implement access controls	- Mandatory - Non-discretionary - Discretionary - Role-based - Attribute-based - Subject-based - Object-based
Security Operations and Administration - 15%	
Comply with codes of ethics	- (ISC)² Code of Ethics - Organizational code of ethics
Understand security concepts	- Confidentiality - Integrity - Availability - Accountability - Privacy - Non-repudiation - Least privilege - Separation of duties
Document, implement, and maintain functional security controls	- Deterrent controls - Preventative controls - Detective controls

Topic	Details
	- Corrective controls - Compensating controls
Participate in asset management	- Lifecycle (hardware, software, and data) - Hardware inventory - Software inventory and licensing - Data storage
Implement security controls and assess compliance	- Technical controls (e.g., session timeout, password aging) - Physical controls (e.g., mantrap, cameras, locks) - Administrative controls (e.g., security policies and standards, procedures, baselines) - Periodic audit and review
Participate in change management	- Execute change management process - Identify security impact - Testing /implementing patches, fixes, and updates (e.g., operating system, applications, SDLC)
Participate in security awareness and training	
Participate in physical security operations (e.g., data center assessment, badging)	
Risk Identification, Monitoring, and Analysis - 15%	
Understand the risk management process	- Risk visibility and reporting (e.g., risk register, sharing threat intelligence, Common Vulnerability Scoring System (CVSS)) - Risk management concepts (e.g., impact assessments, threat modelling, Business Impact Analysis (BIA)) - Risk management frameworks (e.g., ISO, NIST) - Risk treatment (e.g., accept, transfer, mitigate, avoid, recast)
Perform security assessment activities	- Participate in security testing - Interpretation and reporting of scanning and testing results - Remediation validation - Audit finding remediation
Operate and maintain monitoring systems (e.g., continuous monitoring)	- Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring) - Logging - Source systems

Topic	Details
	- Legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
Analyze monitoring results	- Security baselines and anomalies - Visualizations, metrics, and trends (e.g., dashboards, timelines) - Event data analysis - Document and communicate findings (e.g., escalation)
Incident Response and Recovery - 13%	
Support incident lifecycle	- Preparation - Detection, analysis, and escalation - Containment - Eradication - Recovery - Lessons learned/implementation of new countermeasure
Understand and support forensic investigations	- Legal and ethical principles - Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) activities	- Emergency response plans and procedures (e.g., information system contingency plan) - Interim or alternate processing strategies - Restoration planning - Backup and redundancy implementation - Testing and drills
Cryptography - 10%	
Understand fundamental concepts of cryptography	- Hashing - Salting - Symmetric/asymmetric encryption/Elliptic Curve Cryptography (ECC) - Non-repudiation (e.g., digital signatures/certificates, HMAC, audit trail) - Encryption algorithms (e.g., AES, RSA) - Key strength (e.g., 256, 512, 1024, 2048 bit keys) - Cryptographic attacks, cryptanalysis, and counter measures
Understand reasons and requirements for cryptography	- Confidentiality - Integrity and authenticity

Topic	Details
	- Data sensitivity (e.g., PII, intellectual property, PHI) - Regulatory
Understand and support secure protocols	- Services and protocols (e.g., IPSec, TLS, S/MIME, DKIM) - Common use cases - Limitations and vulnerabilities
Understand Public Key Infrastructure (PKI) systems	Fundamental key management concepts (e.g., key rotation, key composition, key creation, exchange, revocation, escrow) - Web of Trust (WOT) (e.g., PGP, GPG)
Network and Communications Security - 16%	
Understand and apply fundamental concepts of networking	- OSI and TCP/IP models - Network topographies (e.g., ring, star, bus, mesh, tree) - Network relationships (e.g., peer to peer, client server) - Transmission media types (e.g., fiber, wired, wireless) - Commonly used ports and protocols
Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)	
Manage network access controls	- Network access control and monitoring (e.g., remediation, quarantine, admission) - Network access control standards and protocols (e.g., IEEE 802.1X, Radius, TACACS) - Remote access operation and configuration (e.g., thin client, SSL VPN, IPSec VPN, telework)
Manage network security	- Logical and physical placement of network devices (e.g., inline, passive) - Segmentation (e.g., physical/logical, data/control plane, VLAN, ACLs) - Secure device management
Operate and configure network-based security devices	- Firewalls and proxies (e.g., filtering methods) - Network intrusion detection/prevention systems - Routers and switches - Traffic-shaping devices (e.g., WAN optimization, load balancing)

Topic	Details
Operate and configure wireless technologies (e.g., bluetooth, NFC, WiFi)	- Transmission security - Wireless security devices (e.g.,WIPS, WIDS)
Systems and Application Security - 15%	
Identify and analyze malicious code and activity	- Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, and remote access trojans) - Malicious code countermeasures (e.g., scanners, anti-malware, code signing, sandboxing) - Malicious activity (e.g., insider threat, data theft, DDoS, botnet) - Malicious activity countermeasures (e.g., user awareness, system hardening, patching, sandboxing, isolation)
Implement and operate endpoint device security	- HIDS - Host-based firewalls - Application white listing - Endpoint encryption - Trusted Platform Module (TPM) - Mobile Device Management (MDM) (e.g., COPE, BYOD) - Secure browsing (e.g., sandbox)
Operate and configure cloud security	- Deployment models (e.g., public, private, hybrid, community) - Service models (e.g., IaaS, PaaS and SaaS) - Virtualization (e.g., hypervisor) - Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery) - Data storage and transmission (e.g., archiving, recovery, resilience) - Third party/outsourcing requirements (e.g., SLA, data portability, data destruction, auditing) - Shared responsibility model
Operate and secure virtual environments	- Software-defined networking - Hypervisor - Virtual appliances - Continuity and resilience - Attacks and countermeasures - Shared storage

ISC2 SSCP Sample Questions:

Question: 1

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: 2

How many primary types of authentication factors are there?

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

Answer: b

Question: 3

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: 4

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: 5

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: 6

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: 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

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

Question: 9

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: 10

What is the primary purpose of SSO?

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

Answer: d

Study Guide to Crack ISC2 Systems Security Practitioner SSCP Exam:

- Getting details of the SSCP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SSCP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISC2 provided training for SSCP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SSCP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SSCP practice tests is must. Continuous practice will make you an expert in all syllabus areas.