SSCP (SSCP) — One-Page Study Guide

A) Exam Snapshot

- **Issuer:** ISC2
- **Exam:** Systems Security Certified Practitioner (SSCP); outline effective Oct 1, 2025
- **Delivery:** Computerized Adaptive Testing (CAT) at Pearson VUE
- **Time / items:** 2 hours; 100–125 items (variable)
- **Item types:** Multiple choice + advanced item types
- **Passing:** 700 out of 1000 (scaled score)

B) Domain Weights

Domain	Weight
1. Security Concepts and Practices	16%
2. Access Controls	15%
3. Risk Identification, Monitoring and Analysis	15%
4. Incident Response and Recovery	14%
5. Cryptography	9%
6. Network and Communications Security	16%
7. Systems and Application Security	15%

C) Core Workflow (How the exam “thinks”)

- Frame the scenario: identify the asset, owners, and what “bad” looks like (loss of confidentiality, integrity, availability).
- Map identities to access needs: user, service, admin; then pick authentication and authorization approach.
- Select the right control type first: administrative, technical, or physical; then confirm it matches the risk and constraints.
- Harden and baseline: compare the described state to secure configurations and approved change records.
- Monitor and interpret evidence: logs, alerts, and baselines; separate signal from noise and document findings.
- Triage incidents: detect, contain, preserve evidence, and support recovery while maintaining chain of custody.
- Use crypto with intent: choose hashing, encryption, signatures, or key exchange based on the protection goal.
- Close the loop: update risk records, lessons learned, and training based on results and compliance needs.

D) High-Yield Concepts

- CIA triad + related principles: accountability, non-repudiation, least privilege, segregation of duties (SoD).
- AuthN vs AuthZ vs accounting; identity lifecycle (provision, modify, de-provision) and auditability.
- Access control models: DAC, MAC, RBAC, ABAC; when privileged access management (PAM) changes the answer.
- Federation and SSO basics: SAML, OpenID Connect (OIDC), OAuth 2; trust boundaries and third-party risk.
- Risk language: threat, vulnerability, likelihood, impact; treatment options (mitigate, transfer, avoid, accept).
- Vulnerability management lifecycle: scan, validate, prioritize (CVSS/asset criticality), remediate, re-test.
- Incident response lifecycle: preparation through lessons learned; evidence handling and reporting integrity.
- Crypto intent: symmetric vs asymmetric, hashes, digital signatures, TLS, key management and rotation.
- Network fundamentals: OSI/TCP-IP, segmentation (VLAN/DMZ), VPN, common attacks (DDoS, MITM, DNS poisoning).
- Systems/app security: secure baselines, patching, logging, secure configurations, and change control evidence.

E) Common Traps

- Choosing a control without identifying the asset and required security property (confidentiality vs integrity vs availability).
- Mixing up authentication and authorization, or assuming “MFA” fixes weak privilege design.
- Treating logs as proof without checking integrity, time source, retention, and who can alter them.
- Picking encryption when the goal is integrity (hashing/signatures) or picking hashing when confidentiality is required.
- Ignoring scope boundaries: internal vs third-party, DMZ vs internal network, admin vs standard user paths.
- Skipping the first incident steps: containment and evidence preservation before deep analysis.
- Assuming “best practice” equals “required” when policy, baseline, or risk tolerance says otherwise.
- Failing to re-test after remediation or to document results for audit and tracking.

F) Cheat Sheet (Artifacts to recognize)

- Access control policy + role/entitlement matrix; evidence of least privilege reviews.
- Identity lifecycle records: joiner/mover/leaver tickets, approvals, and de-provision timestamps.
- Privileged access logs: PAM checkouts, admin session recordings, break-glass use evidence.
- Baseline configuration evidence: secure build standards, hardening check results, and change tickets.
- Vulnerability evidence: scan report, triage notes, remediation ticket, and re-scan proof.
- Incident evidence set: timeline, affected assets list, containment actions, and chain-of-custody form.
- Crypto evidence: key inventory/rotation record, certificate details, and encryption in-transit/in-rest proof.
- Network control evidence: firewall rules/ACLs, segmentation diagrams, VPN configuration summaries.

G) Exam-Day Tactics

- Read the last line first: decide what is being asked (best next step, best control, root cause, evidence).
- For CAT pacing: treat every item as important; avoid “throwaway” guesses and stay steady.
- Eliminate two options quickly using scope, control type, and intent; then choose the best remaining fit.
- Prefer answers that produce verifiable evidence and reduce risk, not answers that sound “most secure.”
- Watch absolutes (always, never) and vague terms (secure, robust) unless the scenario justifies them.
- If stuck, anchor on lifecycle order: identify -> implement -> monitor -> respond -> recover -> improve.
- Manage time: keep moving; mark mentally and move on when the marginal benefit of more thinking is low.

H) 30-Minute Final Review Plan

- 5 min: review domain weights; pick the top three weak areas and the top two “trap” patterns.
- 8 min: access controls sweep (AuthN/AuthZ, RBAC/ABAC, IAM lifecycle, PAM, federation/SSO).
- 5 min: incident response and forensics sweep (phases, containment first, chain of custody).
- 5 min: crypto sweep (hash vs encrypt vs sign; TLS intent; key handling).
- 5 min: network sweep (segmentation, DMZ/VPN, common attacks and countermeasures).
- 2 min: mindset reset (steady pace, choose evidence-based answers, avoid assumptions).

Source: official exam objectives & exam details. Quick review only; practice required.