☰ certstud .com
Search certifications Search

← Back to SSCP Overview

SSCP Study Notes

Download PDF

Comprehensive notes covering all 7 SSCP domains

Domain 1: Security Operations and Administration (16%)

Core Security Concepts

- **Confidentiality:** Protecting information from unauthorized disclosure
- **Integrity:** Ensuring data accuracy and preventing unauthorized modification
- **Availability:** Ensuring systems and data are accessible when needed
- **Authentication:** Verifying identity of users and systems
- **Authorization:** Granting appropriate access rights
- **Accountability:** Tracking actions to individual users

Asset Management

Asset classification, inventory management, labeling, handling procedures, secure disposal, media sanitization

Compliance and Audit

Regulatory requirements, internal policies, audit procedures, evidence collection, reporting mechanisms

Business Continuity and Disaster Recovery

- Business Impact Analysis (BIA)
- Recovery objectives: RTO, RPO, MTTR, MTBF

Analytics (⌘⇧A)
Feedback

- Backup strategies: Full, incremental, differential
- Disaster recovery planning and testing

Domain 2: Access Controls (15%)

Access Control Models

- **Discretionary Access Control (DAC):** Owner-controlled permissions
- **Mandatory Access Control (MAC):** System-enforced labels and clearances
- **Role-Based Access Control (RBAC):** Permissions based on job function
- **Rule-Based Access Control:** Policy-driven access decisions
- **Attribute-Based Access Control (ABAC):** Dynamic access based on attributes

Authentication Methods

- Something you know (passwords, PINs)
- Something you have (tokens, smart cards)
- Something you are (biometrics)
- Multi-factor authentication (MFA)
- Single Sign-On (SSO)

Identity Management

Provisioning, de-provisioning, identity lifecycle, federation, privileged access management

Domain 3: Risk Identification, Monitoring and Analysis (15%)

Risk Management Framework

- Risk identification and assessment

- Qualitative vs. quantitative analysis
- Risk treatment: Avoid, mitigate, transfer, accept
- Risk monitoring and review

Vulnerability Management

Vulnerability scanning, penetration testing, patch management, configuration management

Threat Intelligence

Threat actors, attack vectors, indicators of compromise (IOCs), threat modeling

Security Monitoring

- Log management and analysis
- Security Information and Event Management (SIEM)
- Intrusion detection and prevention
- Anomaly detection

Domain 4: Incident Response and Recovery (13%)

Incident Response Lifecycle

1. **Preparation:** Policies, procedures, tools, training
2. **Detection & Analysis:** Identifying and assessing incidents
3. **Containment:** Limiting damage and preventing spread
4. **Eradication:** Removing threat from environment
5. **Recovery:** Restoring systems to normal operations
6. **Post-Incident:** Lessons learned, documentation

Digital Forensics

Evidence collection, chain of custody, forensic analysis, legal considerations

Incident Classification

Severity levels, impact assessment, escalation procedures, communication protocols

Domain 5: Cryptography (10%)

Encryption

- **Symmetric:** AES, DES, 3DES - Same key for encryption/decryption
- **Asymmetric:** RSA, ECC - Public/private key pairs
- **Hybrid:** Combining symmetric and asymmetric

Hashing

MD5 (deprecated), SHA-1 (deprecated), SHA-256, SHA-3, HMAC

Public Key Infrastructure (PKI)

- Certificate Authorities (CA)
- Digital certificates
- Certificate lifecycle management
- Certificate revocation (CRL, OCSP)

Cryptographic Applications

TLS/SSL, VPN encryption, email encryption (S/MIME, PGP), disk encryption, digital signatures

Domain 6: Network and Communications Security (16%)

Network Architecture

- OSI and TCP/IP models
- Network segmentation and zoning
- DMZ, VLANs, subnetting
- Network devices: Routers, switches, firewalls

Network Security Controls

- **Firewalls:** Packet filtering, stateful inspection, next-gen
- **IDS/IPS:** Signature-based, anomaly-based
- **VPN:** Site-to-site, remote access, IPsec, SSL VPN
- **NAC:** Network Access Control

Wireless Security

WPA2, WPA3, EAP, RADIUS, wireless attacks and mitigations

Network Protocols

TCP/IP, UDP, ICMP, DNS, DHCP, HTTP/HTTPS, FTP/SFTP, SSH, SNMP

Domain 7: Systems and Application Security (15%)

System Hardening

- Removing unnecessary services and software
- Patch management
- Secure configurations and baselines
- Least privilege principle

Endpoint Security

Antivirus/antimalware, host-based firewalls, HIDS/HIPS, endpoint detection and response (EDR)

Secure Software Development

- Secure SDLC phases
- Code review and testing
- OWASP Top 10
- Application security testing

Virtualization and Cloud Security

- Hypervisor security
- Container security
- Cloud service models: IaaS, PaaS, SaaS
- Cloud deployment models: Public, private, hybrid
- Shared responsibility model

Mobile Security

MDM, MAM, BYOD policies, mobile threats, app security

SSCP Exam Tips

- ✓ Focus on practical implementation and operational security
- ✓ Understand the "how" not just the "what" - know how to apply concepts
- ✓ Pay attention to domain weights when allocating study time
- ✓ Practice with realistic exam questions to build confidence
- ✓ Master security best practices and industry standards
- ✓ Review ISC2's Code of Ethics - it's tested on the exam
- ✓ Manage your time: 125 questions in 180 minutes = ~1.4 min per question

- ✓ Read questions carefully - eliminate obviously wrong answers first