Systems Security Certified Practitioner (SSCP)

Content

Domain 1: Access Controls

1. **Implement and Maintain Authentication Methods**
   - Single/Multifactor authentication
   - Single sign-on
   - Device authentication
   - Federated access
2. **Support Internetwork Trust Architectures**
   - Trust relationships (e.g., 1-way, 2-way, transitive)
   - Extranet
   - Third-party connections
3. **Participate in the Identity Management Lifecycle**
   - Authorization
   - Proofing
   - Provisioning/De-provisioning
   - Maintenance
   - Entitlement
   - Identity and Access Management (IAM) systems
4. **Implement Access Controls**
   - Mandatory
   - Non-discretionary
   - Discretionary
   - Role-based
   - Attribute-based
   - Subject-based
   - Object-based

Domain 2: Security Operations and Administration

1. **Comply with Codes of Ethics**
   - (ISC)^2 Code of Ethics
   - Organizational code of ethics
2. **Understand Security Concepts**
   - Confidentiality
   - Integrity
   - Availability
   - Accountability
   - Privacy
   - Non-repudiation
   - Least privilege
   - Separation of duties
3. **Document, Implement, and Maintain Functional Security Controls**
   - Deterrent controls
   - Preventative controls
   - Detective controls

   - Corrective controls
   - Compensating controls
4. **Participate in Asset Management**
   - Lifecycle (hardware, software, and data)
   - Hardware inventory
   - Software inventory and licensing
   - Data storage
5. **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
6. **Participate in Change Management**
   - Execute change management process
   - Identify security impact
   - Testing/implementing patches, fixes, and updates (e.g., operating system, applications, SDLC)
7. **Participate in Security Awareness and Training**
8. **Participate in Physical Security Operations** (e.g., data center assessment, badging)

Domain 3: Risk Identification, Monitoring, and Analysis

1. **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 modeling, Business Impact Analysis (BIA))
   - Risk management frameworks (e.g., ISO, NIST)
   - Risk treatment (e.g., accept, transfer, mitigate, avoid, recast)
2. **Perform Security Assessment Activities**
   - Participate in security testing
   - Interpretation and reporting of scanning and testing results
   - Remediation validation
   - Audit finding remediation
3. **Operate and Maintain Monitoring Systems** (e.g., continuous monitoring)
   - Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring)
   - Logging
   - Source systems
   - Legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
4. **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)

Domain 4: Incident Response and Recovery

1. **Support Incident Lifecycle**

- Preparation
- Detection, analysis, and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/implementation of new countermeasure

2. **Understand and Support Forensic Investigations**
    - Legal and ethical principles
    - Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
3. **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

Domain 5: Cryptography

1. **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 countermeasures
2. **Understand Reasons and Requirements for Cryptography**
    - Confidentiality
    - Integrity and authenticity
    - Data sensitivity (e.g., PII, intellectual property, PHI)
    - Regulatory
3. **Understand and Support Secure Protocols**
    - Services and protocols (e.g., IPSec, TLS, S/MIME, DKIM)
    - Common use cases
    - Limitations and vulnerabilities
4. **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)

Domain 6: Network and Communications Security

1. **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
2. **Understand Network Attacks and Countermeasures** (e.g., DDoS, man-in-the-middle, DNS poisoning)
3. **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)
4. **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
5. **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)
6. **Operate and Configure Wireless Technologies** (e.g., Bluetooth, NFC, WiFi)
   - Transmission security
   - Wireless security devices (e.g., WIPS, WIDS)

Domain 7: Systems and Application Security

1. **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)
2. **Implement and Operate Endpoint Device Security**
   - HIDS
   - Host-based firewalls
   - Application whitelisting
   - Endpoint encryption
   - Trusted Platform Module (TPM)
   - Mobile Device Management (MDM) (e.g., COPE, BYOD)
   - Secure browsing (e.g., sandbox)
3. **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

4. **Operate and Secure Virtual Environments**
    - Software-defined networking
    - Hypervisor
    - Virtual appliances
    - Continuity and resilience
    - Attacks and countermeasures
    - Shared storage