SSCP – Systems Security Certified Practitioner

Course Outline

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, 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., OS, apps, 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, threat intelligence, CVSS)
- Risk management concepts (e.g., impact assessments, threat modeling, 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

- Events of interest (e.g., anomalies, intrusions, unauthorized changes)
- Logging
- Source systems
- Legal and regulatory concerns (e.g., jurisdiction, privacy limitations)

4. Analyze Monitoring Results

- Security baselines and anomalies
- Visualizations, metrics, and trends (e.g., dashboards)
- 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/new countermeasures

2. Understand and Support Forensic Investigations

- Legal and ethical principles
- Evidence handling (e.g., triage, chain of custody, preservation)

3. Understand and Support BCP and DRP Activities

- Emergency response plans (e.g., contingency plans)
- Interim/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, ECC
- Non-repudiation (e.g., digital signatures, HMAC)
- Encryption algorithms (e.g., AES, RSA)
- Key strength (256–2048-bit)
- Cryptographic attacks and countermeasures

2. Understand Reasons and Requirements for Cryptography

- Confidentiality
- Integrity and authenticity
- Data sensitivity (e.g., PII, PHI, IP)
- Regulatory

3. Understand and Support Secure Protocols

- Services/protocols (e.g., IPSec, TLS, S/MIME, DKIM)
- Use cases
- Limitations and vulnerabilities

4. Understand Public Key Infrastructure (PKI) Systems

- Key management (e.g., rotation, creation, escrow)
- Web of Trust (e.g., PGP, GPG)

Domain 6: Network and Communications Security

1. Understand and Apply Networking Concepts

- OSI and TCP/IP models
- Network topographies (e.g., ring, star, mesh)
- Relationships (e.g., client-server, P2P)
- Transmission media (e.g., fiber, wireless)
- Common ports and protocols

2. Understand Network Attacks and Countermeasures

- e.g., DDoS, MITM, DNS poisoning

3. Manage Network Access Controls

- NAC and monitoring (e.g., quarantine)
- NAC standards/protocols (e.g., IEEE 802.1X, Radius, TACACS)
- Remote access (e.g., SSL VPN, IPSec, telework)

4. Manage Network Security
- Placement of devices (inline/passive)
- Segmentation (e.g., VLANs, ACLs)
- Secure device management

5. Operate and Configure Network-Based Security Devices
- Firewalls, proxies, IDS/IPS
- Routers and switches
- Traffic-shaping devices (e.g., WAN optimization)

6. Operate and Configure Wireless Technologies
- e.g., Bluetooth, NFC, WiFi
- Wireless security and devices (e.g., WIPS, WIDS)

Domain 7: Systems and Application Security

1. Identify and Analyze Malicious Code and Activity
- Malware types (e.g., ransomware, trojans, rootkits)
- Countermeasures (e.g., anti-malware, code signing, sandboxing)
- Malicious activities (e.g., insider threat, botnets)
- Activity countermeasures (e.g., awareness, patching, isolation)

2. Implement and Operate Endpoint Device Security
- HIDS, host firewalls
- Whitelisting
- Endpoint encryption
- TPM
- Mobile Device Management (e.g., BYOD, COPE)
- Secure browsing

3. Operate and Configure Cloud Security
- Deployment models (public, private, hybrid, community)
- Service models (IaaS, PaaS, SaaS)
- Virtualization (e.g., hypervisor)
- Legal concerns (privacy, data ownership, eDiscovery)
- Storage/transmission (archiving, recovery, resilience)
- Third-party/outsourcing (SLA, data destruction, auditing)
- Shared responsibility model

4. Operate and Secure Virtual Environments
- SDN, hypervisor
- Virtual appliances
- Continuity and resilience
- Attacks and countermeasures
- Shared storage