CompTIA Advanced Security Practitioner (CASP) Certification Training Course

Description: The CompTIA Advanced Security Practitioner (CASP) Certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP exam will certify that the successful candidate has the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

Days: 5

Certifications: CompTIA CASP

# of Exams: 1 (CAS-001)

Prerequisites: The CompTIA Advanced Security Practitioner (CASP) Certification is aimed at an IT security professional who has a minimum of 10 years experience in IT administration including at least 5 years of hands-on technical security experience.

Enterprise Security

- Distinguish which cryptographic tools and techniques are appropriate for a given situation.
  - Cryptographic applications and proper implementation
  - Advanced PKI concepts
  - Implications of cryptographic methods and design
  - Transport encryption
  - Digital signature
  - Hashing
  - Code signing
  - Non-repudiation
  - Entropy
  - Pseudo random number generation
  - Perfect forward secrecy
  - Confusion
  - Diffusion

- Distinguish and select among different types of virtualized, distributed and shared computing
Advantages and disadvantages of virtualizing servers and minimizing physical space requirements
- VLAN
- Securing virtual environments, appliances and equipment
- Vulnerabilities associated with a single physical server hosting multiple companies’ virtual machines
- Vulnerabilities associated with a single platform hosting multiple companies’ virtual machines
- Secure use of on-demand / elastic cloud computing
- Vulnerabilities associated with co-mingling of hosts with different security requirements
- Virtual Desktop Infrastructure (VDI)
- Terminal services

- **Explain the security implications of enterprise storage**
  - Virtual storage
  - NAS
  - SAN
  - vSAN
  - iSCSI
  - FCoE
  - LUN masking
  - HBA allocation
  - Redundancy (location)
  - Secure storage management

- **Integrate hosts, networks, infrastructures, applications and storage into secure comprehensive solutions**
  - Advanced network design
  - Complex network security solutions for data flow
  - Secure data flows to meet changing business needs
  - Secure DNS
  - Secure directory services
  - Network design consideration
  - Multitier networking data design considerations
  - Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
  - Secure infrastructure design (e.g. decide where to place certain devices)
  - Storage integration (security considerations)
  - Advanced configuration of routers, switches and other network devices
  - ESB
  - SOA
  - SIEM
  - Database Access Monitor (DAM)
  - Service enabled
  - WS-security

- **Distinguish among security controls for hosts**
  - Host-based firewalls
  - Trusted OS (e.g. how and when to use it)
  - End point security software
  - Host hardening
  - Asset management (inventory control)
  - Data exfiltration
  - HIPS / HIDS
  - NIPS/NIDS
- **Explain the importance of application security**
  - Web application security design considerations
  - Specific application issues
  - Application sandboxing
  - Application security frameworks
  - Secure coding standards
  - Exploits resulting from improper error and exception handling
  - Privilege escalation
  - Improper storage of sensitive data
  - Fuzzing/fault injection
  - Secure cookie storage and transmission
  - Client-side processing vs. server-side processing
  - Buffer overflow
  - Memory leaks
  - Integer overflows
  - Race conditions
  - Resource exhaustion

- **Given a scenario, distinguish and select the method or tool that is appropriate to conduct an assessment**
  - Tool type
  - Methods

---

**Risk Management, Policy / Procedure and Legal**

- **Analyze the security risk implications associated with business decisions**
  - Risk management of new products, new technologies and user behaviors
  - New or changing business models/strategies
  - Internal and external influences
  - Impact of de-perimeterization (e.g. constantly changing network boundary)

- **Execute and implement risk mitigation strategies and controls**
  - Classify information types into levels of CIA based on organization/industry
  - Determine aggregate score of CIA
  - Determine minimum required security controls based on aggregate score
  - Conduct system specific risk analysis
  - Make risk determination
  - Decide which security controls should be applied based on minimum requirements
  - Implement controls
  - ESA frameworks
  - Continuous monitoring

- **Explain the importance of preparing for and supporting the incident response and recovery process**
  - E-Discovery
  - Data breach
  - System design to facilitate incident response taking into account types of violations
  - Incident and emergency response

- **Implement security and privacy policies and procedures based on organizational requirements.**
- Policy development and updates in light of new business, technology and environment changes
- Process/procedure development and updates in light of policy, environment and business changes
- Support legal compliance and advocacy by partnering with HR, legal, management and other entities
- Use common business documents to support security
- Use general privacy principles for PII / Sensitive PII
- Support the development of policies that contain

Research and Analysis

- **Analyze industry trends and outline potential impact to the enterprise**
  - Perform on-going research
  - Situational awareness
  - Research security implications of new business tools
  - Global IA industry/community
  - Research security requirements for contracts
- **Carry out relevant analysis for the purpose of securing the enterprise**
  - Benchmark
  - Prototype and test multiple solutions
  - Cost benefit analysis (ROI, TCO)
  - Analyze and interpret trend data to anticipate cyber defense aids
  - Review effectiveness of existing security
  - Reverse engineer / deconstruct existing solutions
  - Analyze security solutions to ensure they meet business needs
  - Conduct a lessons-learned / after-action review
  - Use judgment to solve difficult problems that do not have a best solution
  - Conduct network traffic analysis

Integration of Computing, Communications and Business Disciplines

- **Integrate enterprise disciplines to achieve secure solutions**
  - Interpreting security requirements and goals to communicate with other disciplines
  - Provide guidance and recommendations to staff and senior management on security processes and controls
  - Establish effective collaboration within teams to implement secure solutions
  - Disciplines
- **Explain the security impact of inter-organizational change**
  - Security concerns of interconnecting multiple industries
  - Design considerations during mergers, acquisitions and de-mergers
  - Assuring third party products - only introduce acceptable risk
  - Network secure segmentation and delegation
  - Integration of products and services
- **Select and distinguish the appropriate security controls with regard to communications and collaboration**
  - Unified communication security
  - VoIP security
- VoIP implementation
- Remote access
- Enterprise configuration management of mobile devices
- Secure external communications
- Secure implementation of collaboration platforms
- Prioritizing traffic (QoS)
- Mobile devices

- **Explain advanced authentication tools, techniques and concepts**
  - Federated identity management (SAML)
  - XACML
  - SOAP
  - Single sign on
  - SPML
  - Certificate based authentication
  - Attestation

- **Carry out security activities across the technology life cycle**
  - End to end solution ownership
  - Understanding results of solutions in advance
  - Systems Development Life Cycle
  - Adapt solutions to address emerging threats and security trends
  - Validate system designs