CompTIA Advanced Security Practitioner (CASP) (Exam CAS-002)

Course Outline

Course Introduction 4m
Course Introduction

Lesson 01 - The Enterprise Security Architecture 1h 29m
Topic A: The Basics of Enterprise Security
The Enterprise
Enterprise Security
Business Goals and Security
Common Enterprise Security Principles
Enterprise Threat Intelligence
What to Protect?
Defense in Depth
Common Components of an Enterprise Security Solutions
Policies, Standards, and Procedures
Enterprise Policy Types
Topic B: The Enterprise Structure
Organizational Structures
The Management Team
Network Administrator
The DBA
Programmers
Stakeholders
Finance
Human Resources
Physical Security and Facilities Roles
Discipline Collaboration
Topic C: Enterprise Security Requirements
Legal Compliance
PII
Privacy Requirements
Organizational Security Requirements
Lesson 01 Review

Lesson 02 - The Enterprise Security Technology 2h 45m
Topic A: Common Network Security Components and Technologies
Common Enterprise Security Components
VoIP Integration
IPv6 Migration and Integration
VLAN Integration
DNS Security Techniques
Secure Directory Services
NIDS
NIPS

The NIPS Process
ESB
The ESB Process
DAM
Topic B: Communications and Collaboration Security
UC Security
UC Attacks
UC Components
Traffic Prioritization (QoS)
Security Solutions for Data Flow
VoIP Security
The VoIP Implementation Process
VoIP Implementation Considerations
Remote Access Security
VPN Solutions
External Communications Security
Collaboration Platform Security Issues
Demo - Least Privilege
Common Mobile Devices
Enterprise Security Methods for Mobile Devices
Topic C: Cryptographic Tools and Techniques
Cryptography in the Enterprise
Considerations for Cryptography in the Enterprise
Demo - File Encryption
Cryptographic Methods and Design
Basic Approaches to Encryption
Transport Encryption Methods
Security Implications for Encryption
Digital Signature Techniques
Advanced PKI Components
Code Signing
Attestation
Entropy
PRNG
PFS
Confusion and Diffusion
Topic D: Advanced Authentication
Advanced Authentication Within the Enterprise
Certificate-Based Authentication
SAML
SPML
XACML
SOAP
WSS
Lesson 02 Review

Lesson 03 - Enterprise Resource Technology 1h 54m
Topic A: Enterprise Storage Security Issues
Common Enterprise Storage Technologies
NAS Security Implications

Lesson 04 - Security Design and Solutions 4h 37m

Topic A: Network Security Design
Network Design Types and Techniques
Network Design Considerations
Data Network Types
A Data Network Topology
Data Network Topology Types
A Network Diagram
Data Network Media Types
Network Transmission Methodologies
Physical Security
Building Layout
Facilities Management
Unified Threat Management
NIDS
NIPS
Inline Network Encryptor
Security Information and Event Management
SIEM Capabilities
Network-Attached HSM
Application and Protocol Aware Technologies
Virtual Networking and Security Components
Device Placement
Guidelines for Analyzing Network Security Components and Devices
Guidelines for Analyzing Network Security Components and Devices (Cont.)
Building Automation Systems
Hardware Attacks
Environmental Threats and Vulnerabilities
Sensors
Physical Access Control Systems
Scientific and Industrial Equipment
A/V Systems
IP Video
Network Attacks
SCADA
Secure Infrastructure Design
Storage Integration Considerations
Guidelines for Analyzing Network-Enabled Devices
Remote Access
IPv6 and Associated Transitional Technologies
Network Authentication
802.1X
Software-Defined Networking
Cloud-Managed Networks
Guidelines for Analyzing Advanced Network Design
Network Baselining
Configuration Lockdown
Change Monitoring
Availability Controls
ACLs

DMZ
Separation of Critical Assets
Data Flow Enforcement
Network Device Configuration
Network Access Control
Critical Infrastructure and Industrial Control Systems
Network Management and Monitoring Tools
Guidelines for Configuring Controls for Network Security
Topic B: Conduct a Security Assessment
Malware Sandboxing
Memory Dumping
Runtime Debugging
Vulnerability Assessment
Penetration Testing
Hacking Steps
Penetration Testing Techniques
Fingerprinting
Types of Social Engineering
Vulnerability Scanners
Port Scanners
Protocol Analyzers
Network Enumerators
Password Crackers
Fuzzers
HTTP Interceptors
Exploitation Tools and Frameworks
Passive Reconaissance and Intelligence Gathering Tools
Code Review Methods
A Social Engineering Test
Security Assessment Tools
How to Conduct a Security Assessment
Topic C: Host Security
Host-Based Security Controls
Host-Based Firewalls
Firewall Rules
Demo - Firewalls
TPM
Trusted OS
Endpoint Security
Endpoint Security Software
Guidelines for Selecting Host Hardware and Software
Security and Group Policy Implementations
Standard Operating Environment
Command Shell Restrictions
Patch Management
Out-of-Band Communication
Peripheral Restrictions
Communications Protocols Used by Peripherals
Full Disk Encryption
Trusted OS (Cont.)

Endpoint Security (Cont.)
Anti-Malware Software
Host Hardening
Guidelines for Hardening Hosts
Operating System Security
Host Hardening Action Steps
Asset Management
HIDS
HIPS
Host Monitoring
Virtualization Platforms
Hypervisors
Container-Based Virtualization
VDI
Security Implications of VDI
Terminal Services
Application Delivery Services
vTPM
VM Vulnerabilities
Guidelines for Virtualizing Servers and Desktops
Cloud Services
Cloud Security Services
Hash Matching
Content Filtering
Guidelines for Implementing Cloud Augmented Security Services
BIOS
UEFI
Secure Boot
Measured Launch
IMA
Lesson 04 Review

Lesson 05 - Managing Risk in Projects 1h 53m
Topic A: Create a Risk Management Plan
Risk
Risk Exposure
Risk Analysis Methods
Risks Facing an Enterprise
Project Buffer
Classification of Risks
Business Risk vs. Insurable Risk
Risk Tolerance
Probability Scale
Impact Scale
RBS
Enterprise Security Architecture Frameworks
ESA Framework Assessment Process
New Products and Technologies
New and Changing Business Models
Partnership Model

Probability Distribution
Quantitative Analysis Methods
Qualitative Analysis Methods
Risk Data Quality Assessment
Risk Urgency Assessment
Simulation
Monte Carlo Analysis
How to Analyze Risks
Topic D: Develop a Risk Response Plan
Negative Risks
Negative Risk Strategies
Positive Risks
Positive Risk Strategies
Contingency Plan
The BCP
DRP
Contingency Reserve
Risk-Related Contract Decisions
How to Develop a Risk Response Plan
Lesson 05 Review

Lesson 06 - Integrating Advanced Authentication and Authorization Techniques 27m
Topic A: Implement Authentication and Authorization Technologies
Authentication
Certificate-Based Authentication
SSO
Authorization
OAuth
The OAuth Process
XACML
SPML
Trust Models
RADIUS Configurations
LDAP
Active Directory
Kerberos
Guidelines for Implementing Authentication and Authorization
Topic B: Implement Advanced Identity Management
Attestation
Identity Propagation
Identity Federation
Identity Federation Methods
Guidelines for Implementing Advanced Identity Management
Lesson 06 Review

Lesson 07 - Implementing Cryptographic Techniques 57m

Topic A: Describe Cryptographic Concepts
Confidentiality
Integrity
Non-repudiation
Entropy
Confusion
Diffusion
Chain of Trust
Root of Trust
Steganography
Advanced PKI Concepts
Topic B: Choose Cryptographic Techniques
Cryptographic Applications
Cryptographic Methods
Block Cipher Modes
Cryptographic Design Considerations
Transport Encryption
Transport Encryption Protocols
Data at Rest Encryption
Hashing
Hash Functions
Key Stretching
Digital Signatures
Code Signing
Pseudorandom Number Generation
Perfect Forward Secrecy
Guidelines for Choosing Cryptographic Techniques
Topic C: Choose Cryptographic Implementations
DRM
Digital Watermarking
SSL/TLS
SSH
PGP and GPG
S/MIME
Guidelines for Choosing Cryptographic Implementations
Lesson 07 Review

Lesson 08 - Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture 1h 11m

Topic A: Implement Security Standards in the Enterprise
Standards
Categories of Standards
Interoperability Issues
Data Flow Security
Guidelines for Implementing Standards in the Enterprise
Topic B: Select Technical Deployment Models
Deployment Models
Cloud and Virtualization and Hosting Options
Elastic Cloud Computing

Data Remnants in the Cloud
Data Aggregation
Data Isolation
Resource Provisioning and De-provisioning
Virtual Machine Vulnerabilities
Virtual Environment Security
Virtual Environment Security (Cont.)
Network Segmentation
Network Delegation
Mergers and Acquisitions
Guidelines for Selecting Technical Deployment Models
Topic C: Secure the Design of the Enterprise Infrastructure
Infrastructure Design Security
Deployment Diagrams
Storage Integration
Guidelines for Securing the Design of the Enterprise Infrastructure
Topic D: Secure Enterprise Application Integration Enablers
Customer Relationship Management
Enterprise Resource Planning
Governance, Risk, and Compliance
Enterprise Service Bus
Service Oriented Architecture
Directory Services
Domain Name System
Configuration Management Database
Content Management System
Guidelines for Securing Enterprise Application Integration Enablers
Lesson 08 Review

Lesson 09 - Security Research and Analysis 1h 7m
Topic A: Perform an Industry Trends and Impact Analysis
Industry Best Practices
Demo - Security Research
Research Methods
Technology Evolution
New Technologies, Security Systems, and Services
New Security Technology Types
Global IA Industry and Community
Security Requirements for Contracts
Guidelines for Determining Industry Trends and Effects on the Enterprise
Situational Awareness
Situational Awareness Considerations
Emerging Business Tools
Social Media as an Emerging Business Tool
Mobile Devices as Emerging Business Tools
Emerging Security Issues
The Global Impact Analysis Industry
Security Requirements for Business Contracts
How to Perform an Industry Trends Impact Analysis
Topic B: Perform an Enterprise Security Analysis

Benchmarking
Network Traffic Analysis
Types of Network Traffic Analysis
Prototyping and Testing
Cost-Benefit Analysis
Security Analysis Strategies
Security Solution Analysis
Lessons Learned Review
How to Perform an Enterprise Security Analysis
Review Existing Security
Reverse Engineering
Solution Attributes
After-Action Report
Guidelines for Analyzing Scenarios to Secure the Enterprise
Lesson 09 Review

Lesson 10 - Disaster Recovery and Business Continuity 54m
Topic A: BCP Fundamentals
BCPs
BCP Development Phases
NIST Contingency Planning Steps
NFPA Business Planning Framework
Disruptive Events
BIA
BIA Organizational Goals
BIA Process
Critical Business Process
Vulnerability Assessments
MTD
RPO
RTO
RPO/RTO Optimization
Topic B: BCP Implementation
Program Coordinators
Advisory Committee-BCP Team
BCP Team Responsibilities
BCP Contents
Business Plan Evaluations
Business Plan Testing
Business Plan Maintenance
Business Continuity Process
Topic C: DRP Fundamentals
DRP
Disaster Recovery Strategy
Disaster Recovery Priority Levels
Disaster Recovery Response Approaches
Backup Strategies
Data Restoration Strategies
Alternate Sites
Topic D: DRP Implementation

Recovery Team
Salvage Team
Disaster Recovery Evaluation and Maintenance
Disaster Recovery Testing
Disaster Recovery Process
Lesson 10 Review

Lesson 11 - Responding to and Recovering from Incidents 35m
Topic A: Design Systems to Facilitate Incident Response
Internal and External Violations
Security Violations and System Design
System, Audit, and Security Logs
Guidelines for Designing Systems to Facilitate Incident Response
Topic B: Conduct Incident and Emergency Responses
E-Discovery
E-Discovery Policy
Data Breach
Data Breach Response
Chain of Custody
Forensic Analysis of Compromised Systems
COOP- Continuity of Operations
Order of Volatility
Guidelines for Conducting Incident and Emergency Responses
Lesson 11 Review

Lesson 12 - Legal Issues 35m
Topic A: Computer Crime Laws and Regulations
Common Law
Statutory Law
Types of Statutory Offenses
Administrative Law
Intellectual Property Law
Information Privacy Law
Computer Crime Law
Compliance
Liability
Internal and External Audits
Governmental Oversight Resources
Topic B: Computer Crime Incident Response
Computer Crime
The Computer Criminal Incident Response Process
The Evidence Life Cycle
Evidence Collection Techniques
Evidence Types
Chain of Evidence
Rules of Evidence
Surveillance Techniques
Search and Seizure
Computer Forensics
Lesson 12 Review

Lesson 13 - Judgment and Decision-Making 40m

Topic A: Develop Critical Thinking Skills
Intellectual Autonomy
Humility
Objectivity
Focus on the Argument
Clarity
Defining Your Argument
Intellectual Honesty
Logical Fallacies
Assessing Arguments Logically
How to Employ Critical Thinking Skills
Topic B: Determine the Root of a Problem
Obstacles to Analysis
Occam's Razor
Techniques for Applying Occam's Razor
Theme Analysis
The Four Guidelines Technique
How to Determine the Root of a Problem
Topic C: Use Judgment to Make Sound Decisions
Analyzing Problems
Analytical vs. Creative Thinking
Barriers to Creative Thinking
Brainstorming
Rules of Brainstorming
Evaluating Brainstorming Ideas
A Fishbone Diagram
A Pareto Chart
A Histogram
A Cost-Benefit Analysis
Phases in Cost-Benefit Analysis
A Prioritization Matrix
A Trade-Off Method
A Decision Tree
An Ease and Effect Matrix
A PMI Analysis Table
How to Use Judgment to Make Sound Decisions
Lesson 13 Review
Course Closure

Total Duration: 19h 9m