CompTIA Advanced Security Practitioner Certification Exam Objectives (CAS-002)

1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques.

Techniques

- Key stretching
- Hashing
- Code signing
- Pseudo random number generation
- Perfect forward secrecy
- Transport encryption
- Data at rest encryption
- Digital signature

Concepts

- Entropy
- Diffusion
- Confusion
- Non-repudiation
- Confidentiality
- Integrity
- Chain of trust, Root of trust
- Cryptographic applications and proper/improper implementations
- Advanced PKI concepts

Wild card

OCSP vs. CRL

Issuance to entities

Users

Systems

Applications

Key escrow

- Steganography
- Implications of cryptographic methods and design

Stream

Block

Modes

ECB

CBC

CFB

OFB

Known flaws/weaknesses

Strength vs. performance vs. feasibility to implement vs. interoperability

Implementations

- DRM
- Watermarking
- GPG
- SSL
- SSH
- S/MIME

1.2 Explain the security implications associated with enterprise storage

Storage types

- Virtual storage
- Cloud storage
- Data warehousing
- Data archiving
- NAS
- SAN
- vSAN

Storage protocols

- iSCSI
- FCoE
- NFS, CIFS

Secure storage management

- Multipath
- Snapshots
- Deduplication
- Dynamic disk pools
- LUN masking/mapping
- HBA allocation
- Offsite or multisite replication
- Encryption

Disk

Block

File

Record

Port

1.3 Given a scenario, analyze network and security components, concepts and architectures

Advanced network design (wired/wireless)

- Remote access

VPN

SSH

RDP

VNC

SSL

- IPv6 and associated transitional technologies
- Transport encryption
- Network authentication methods
- 802.1x
- Mesh networks

Security devices

- UTM
- NIPS
- NIDS
- INE
- SIEM
- HSM
- Placement of devices
- Application and protocol aware technologies

WAF

NextGen firewalls

IPS

Passive vulnerability scanners

DAM

Virtual networking and security components

- Switches
- Firewalls
- Wireless controllers
- Routers
- Proxies

Complex network security solutions for data flow

- SSL inspection
- Network flow data

Secure configuration and baselining of networking and security components

- ACLs
- Change monitoring
- Configuration lockdown
- Availability controls

Software defined networking

Cloud managed networks

Network management and monitoring tools

Advanced configuration of routers, switches and other network devices

- Transport security
- Trunking security
- Route protection

Security zones

- Data flow enforcement
- DMZ
- Separation of critical assets

Network access control

- Quarantine/remediation

Operational and consumer network enabled devices

- Building automation systems
- IP video
- HVAC controllers
- Sensors
- Physical access control systems
- A/V systems

- Scientific/industrial equipment

Critical infrastructure/Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)

1.4 Given a scenario, select and troubleshoot security controls for hosts

Trusted OS (e.g. how and when to use it)

End point security software

- Anti-malware
- Anti-virus
- Anti-spyware
- Spam filters
- Patch management
- HIPS/HIDS
- Data loss prevention
- Host-based firewalls
- Log monitoring

Host hardening

- Standard operating environment/configuration baselining

Application whitelisting and blacklisting

- Security/group policy implementation
- Command shell restrictions
- Patch management
- Configuring dedicated interfaces

Out-of-band NICs

ACLs

Management interface

Data interface

- Peripheral restrictions

USB

Bluetooth

Firewire

- Full disk encryption

Security advantages and disadvantages of virtualizing servers

- Type I

- Type II
- Container-based

Cloud augmented security services

- Hash matching

Anti-virus

Anti-spam

Vulnerability scanning

- Sandboxing
- Content filtering

Boot loader protections

- Secure boot
- Measured launch
- IMA - Integrity Measurement Architecture
- BIOS/UEFI

Vulnerabilities associated with co-mingling of hosts with different security requirements

- VMEscape
- Privilege elevation
- Live VM migration
- Data remnants

Virtual Desktop Infrastructure (VDI)

Terminal services/application delivery services

TPM

VTPM

HSM

1.5 Differentiate application vulnerabilities and select appropriate security controls

Web application security design considerations

- Secure: by design, by default, by deployment

Specific application issues

- Insecure direct object references
- XSS
- Cross-site Request Forgery (CSRF)
- Click-jacking

- Session management
- Input validation
- SQL injection
- Improper error and exception handling
- Privilege escalation
- Improper storage of sensitive data
- Fuzzing/fault injection
- Secure cookie storage and transmission
- Buffer overflow
- Memory leaks
- Integer overflows
- Race conditions

Time of check

Time of use

- Resource exhaustion
- Geo-tagging
- Data remnants

Application sandboxing

Application security frameworks

- Standard libraries
- Industry accepted approaches
- Web services security (WS-security)

Secure coding standards

Database Activity Monitor (DAM)

Web Application Firewalls (WAF)

Client-side processing vs. server-side processing

- JSON/REST
- Browser extensions

ActiveX

Java Applets

Flash

- HTML5
- AJAX
- SOAP
- State management

- Javascript

2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks

Risk management of new products, new technologies and user behaviors

New or changing business models/strategies

- Partnerships
- Outsourcing
- Cloud
- Merger and demerger/divestiture

Security concerns of integrating diverse industries

- Rules
- Policies
- Regulations
- Geography

Ensuring third party providers have requisite levels of information security

Internal and external influences

- Competitors
- Auditors/audit findings
- Regulatory entities
- Internal and external client requirements
- Top level management

Impact of de-perimeterization (e.g. constantly changing network boundary)

- Telecommuting
- Cloud
- BYOD
- Outsourcing

2.2 Given a scenario, execute risk mitigation planning, strategies and controls

Classify information types into levels of CIA based on organization/industry

Incorporate stakeholder input into CIA decisions

Implement technical controls based on CIA requirements and policies of the organization

Determine aggregate score of CIA

Extreme scenario planning/worst case scenario

Determine minimum required security controls based on aggregate score

Conduct system specific risk analysis

Make risk determination

- Magnitude of impact

ALE

SLE

- Likelihood of threat

Motivation

Source

ARO

Trend analysis

- Return on investment (ROI)
- Total cost of ownership

Recommend which strategy should be applied based on risk appetite

- Avoid
- Transfer
- Mitigate
- Accept

Risk management processes

- Exemptions
- Deterrance
- Inherent
- Residual

Enterprise Security Architecture frameworks

Continuous improvement/monitoring

Business Continuity Planning

IT Governance

2.3 Compare and contrast security, privacy policies and procedures based on organizational requirements

Policy development and updates in light of new business, technology, risks 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

- Risk assessment (RA)/Statement of Applicability (SOA)
- Business Impact Analysis (BIA)
- Interoperability Agreement (IA)
- Interconnection Security Agreement (ISA)
- Memorandum of Understanding (MOU)
- Service Level Agreement (SLA)
- Operating Level Agreement (OLA)
- Non-Disclosure Agreement (NDA)
- Business Partnership Agreement (BPA)

Use general privacy principles for sensitive information (PII)

Support the development of policies that contain:

- Separation of duties
- Job rotation
- Mandatory vacation
- Least privilege
- Incident response
- Forensic tasks
- Employment and termination procedures
- Continuous monitoring
- Training and awareness for users
- Auditing requirements and frequency

2.4 Given a scenario, conduct incident response and recovery procedures

E-Discovery

- Electronic inventory and asset control
- Data retention policies
- Data recovery and storage
- Data ownership
- Data handling
- Legal holds

Data breach

- Detection and collection

Data analytics

- Mitigation

Minimize

Isolate

- Recovery/reconstitution
- Response
- Disclosure

Design systems to facilitate incident response

- Internal and external violations

Privacy policy violations

Criminal actions

Insider threat

Non-malicious threats/misconfigurations

- Establish and review system, audit and security logs

Incident and emergency response

- Chain of custody
- Forensic analysis of compromised system
- Continuity of Operation Plan (COOP)
- Order of volatility

3.0 Research, Analysis and Assessment

3.1 Apply research methods to determine industry trends and impact to the enterprise

Perform ongoing research

- Best practices
- New technologies
- New security systems and services
- Technology evolution (e.g. RFCs, ISO)

Situational awareness

- Latest client-side attacks
- Knowledge of current vulnerabilities and threats
- Zero day mitigating controls and remediation
- Emergent threats and issues

Research security implications of new business tools

- Social media/networking
- End user cloud storage
- Integration within the business

Global IA industry/community

- Computer Emergency Response Team (CERT)
- Conventions/conferences
- Threat actors
- Emerging threat sources/threat intelligence

Research security requirements for contracts

- Request for Proposal (RFP)
- Request for Quote (RFQ)
- Request for Information (RFI)
- Agreements

3.2 Analyze scenarios to secure the enterprise

Create benchmarks and compare to baselines

Prototype and test multiple solutions

Cost benefit analysis

- ROI
- TCO

Metrics collection and analysis

Analyze and interpret trend data to anticipate cyber defense needs

Review effectiveness of existing security controls

Reverse engineer/deconstruct existing solutions

Analyze security solution attributes to ensure they meet business needs:

- Performance
- Latency
- Scalability
- Capability
- Usability
- Maintainability
- Availability
- Recoverability

Conduct a lessons-learned/after-action report

Use judgment to solve difficult problems that do not have a best solution

3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results

Tool type

- Port scanners
- Vulnerability scanners
- Protocol analyzer
- Network enumerator
- Password cracker
- Fuzzer
- HTTP interceptor
- Exploitation tools/frameworks
- Passive reconnaissance and intelligence gathering tools

Social media

Whois

Routing tables

Methods

- Vulnerability assessment
- Malware sandboxing
- Memory dumping, runtime debugging
- Penetration testing
- Black box
- White box
- Grey box
- Reconnaissance
- Fingerprinting
- Code review
- Social engineering

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Given a scenario, facilitate collaboration across diverse business units to achieve security goals

Interpreting security requirements and goals to communicate with stakeholders from other disciplines

- Sales staff
- Programmer
- Database administrator
- Network administrator
- Management/executive management
- Financial
- Human resources
- Emergency response team
- Facilities manager
- Physical security manager

Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls

Establish effective collaboration within teams to implement secure solutions

IT governance

4.2 Given a scenario, select the appropriate control to secure communications and collaboration solutions

Security of unified collaboration tools

- Web conferencing
- Video conferencing
- Instant messaging
- Desktop sharing
- Remote assistance
- Presence
- Email
- Telephony

VoIP

- Collaboration sites

Social media

Cloud-based

Remote access

Mobile device management

- BYOD

Over-the-air technologies concerns

4.3 Implement security activities across the technology life cycle

End-to-end solution ownership

- Operational activities
- Maintenance
- Commissioning/decommissioning
- Asset disposal
- Asset/object reuse
- General change management

Systems Development Life Cycle

- Security System Development Life Cycle (SSDLC)/Security Development Lifecycle (SDL)
- Security Requirements Traceability Matrix (SRTM)

- Validation and acceptance testing
- Security implications of agile, waterfall and spiral software development methodologies

Adapt solutions to address emerging threats and security trends

Asset management (inventory control)

- Device tracking technologies

Geo-location/GPS location

- Object tracking and containment technologies

Geo-tagging/geo-fencing

RFID

5.0 Technical Integration of Enterprise Components

5.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture

Secure data flows to meet changing business needs

Standards

- Open standards
- Adherence to standards
- Competing standards
- Lack of standards
- Defacto standards

Interoperability issues

- Legacy systems/current systems
- Application requirements
- In-house developed vs. commercial vs. commercial customized

Technical deployment models (Outsourcing/insourcing/managed services/partnership)

- Cloud and virtualization considerations and hosting options

Public

Private

Hybrid

Community

Multi-tenancy

Single tenancy

- 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
- Data remnants
- Data aggregation
- Data isolation
- Resources provisioning and de-provisioning

Users

Servers

Virtual devices

Applications

- Securing virtual environments, services, applications, appliances and equipment
- Design considerations during mergers, acquisitions and demergers/divestitures
- Network secure segmentation and delegation

Logical deployment diagram and corresponding physical deployment diagram of all relevant devices

Secure infrastructure design (e.g. decide where to place certain devices/applications)

Storage integration (security considerations)

Enterprise application integration enablers

- CRM
- ERP
- GRC
- ESB
- SOA
- Directory Services
- DNS
- CMDB
- CMS

5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives

Authentication

- Certificate-based authentication
- Single sign-on

Authorization

- OAUTH
- XACML
- SPML

Attestation

Identity propagation

Federation

- SAML
- OpenID
- Shibboleth
- WAYF

Advanced trust models

- RADIUS configurations
- LDAP
- AD

CASP ACRONYMS

3DES – Triple Digital Encryption Standard

AAA – Authentication, Authorization, and Accounting

AAR – After Action Report

ACL – Access Control List

AD – Active Directory

AES – Advanced Encryption Standard

AH – Authentication Header

AJAX – Asynchronous JAVA and XML

ALE – Annualized Loss Expectancy

AP – Access Point

APT – Advanced Persistent Threats

ARO – Annualized Rate of Occurrence

ARP – Address Resolution Protocol

AUP – Acceptable Use Policy

BCP – Business Continuity Planning

BIOS – Basic Input/Output System

BPA – Business Partnership Agreement

BPM – Business Process Management

CA – Certificate Authority

CAAS – Communication as a Service

CAC – Common Access Card

CBC – Cipher Block Chaining

CCMP – Counter-Mode/CBC-Mac Protocol

CCTV – Closed-Circuit Television

CERT – Computer Emergency Response Team

CFB – Cipher Feedback

CHAP – Challenge Handshake Authentication Protocol

CIA – Confidentiality, Integrity and Availability

CIFS – Common Internet File System

CIRT – Computer Incident Response Team

CISO – Chief Information Security Officer

CMDB – Configuration Management Database

COOP – Continuity of Operations

COTS – Commercial Off-the-Shelf

CRC – Cyclical Redundancy Check

CredSSP – Credential Security Support Provider

CRL – Certification Revocation List

CRM – Customer Resource Management

CSRF – Cross-Site Request Forgery

DAC – Discretionary Access Control

DAM – Database Activity Monitoring

DDOS – Distributed Denial of Service

DEP – Data Execution Prevention

DES – Digital Encryption Standard

DHCP – Dynamic Host Configuration Protocol

DLL – Dynamic Link Library

DLP – Data Loss Prevention

DMZ – Demilitarized Zone

DNS – Domain Name Service (Server)

DOM – Document Object Model

DOS – Denial of Service

DRP – Disaster Recovery Plan

DSA – Digital Signature Algorithm

EAP – Extensible Authentication Protocol

ECB – Event Control Block

ECC – Elliptic Curve Cryptography

EFS – Encrypted File System

ELA – Enterprise License Agreement

EMI – Electromagnetic Interference

ESA – Enterprise Security Architecture

ESB – Enterprise Service Bus

ESP – Encapsulated Security Payload

EV – Extended Validation (Certificate)

FCoE – Fiber Channel over Ethernet

FTP – File Transfer Protocol

GPG – GNU Privacy Guard

GPU – Graphic Processing Unit

GRC – Governance, Risk and Compliance

GRE – Generic Routing Encapsulation

HBA – Host Bus Adapter

HDD – Hard Disk Drive

HIDS – Host-based Intrusion Detection System

HIPS – Host-based Intrusion Prevention System

HMAC – Hashed Message Authentication Code

HOTP – HMAC-based One-time Password

HSM – Hardware Security Module

HSTS – HTTP Strict Transport Security

HVAC – Heating, Ventilation Air Conditioning

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

ICS – Industrial Control System

IDF – Intermediate Distribution Frame

IdM – Identity Management

IdP – Identity Provider

IDS – Intrusion Detection System

IETF – Internet Engineering Task Force

IKE – Internet Key Exchange

IM – Instant Messaging

IMAP – Internet Message Access Protocol

INE – Inline Network Encryptor

IP – Internet Protocol

IPS – Intrusion Prevention Systems

IPSec – Internet Protocol Security

IRC – Internet Relay Chat

ISA – Interconnection Security Agreement

ISMS – Information Security Management System

ISP – Internet Service Provider

IV – Initialization Vector

KDC – Key Distribution Center

KVM – Keyboard, Video, Mouse

L2TP – Layer 2 Tunneling Protocol

LDAP – Lightweight Directory Access Protocol

LEAP – Lightweight Extensible Authentication Protocol

LOB – Line of Business

LUN – Logical Unit Number

MaaS – Monitoring as a Service

MAC – Mandatory Access Control

MAC – Media Access Control

MAC – Message Authentication Code

MAN – Metropolitan Area Network

MBR – Master Boot Record

MD5 – Message Digest 5

MDF – Main Distribution Frame

MDM – Mobile Device Management

MEAP – Mobile Enterprise Application Platform

MFD – Multifunction Device

MITM – Man in the Middle

MOA – Memorandum of Agreement

MOU – Memorandum of Understanding

MPLS – Multiprotocol Label Switching

MSCHAP – Microsoft Challenge Handshake Authentication Protocol

MSS – Managed Security Service

MTBF – Mean Time Between Failure

MTD – Maximum Tolerable Downtime

MTTR – Mean Time to Recovery

MTU – Maximum Transmission Unit

NAC – Network Access Control

NAS – Network Attached Storage

NAT – Network Address Translation

NDA – Non-Disclosure Agreement

NIDS – Network Intrusion Detection System

NIPS – Network Intrusion Prevention System

NIST – National Institute of Standards and Technology

NLA – Network Level Authentication

NOS – Network Operating System

NSP – Network Service Provider

NTFS – New Technology File System

NTLM – New Technology LANMAN

NTP – Network Time Protocol

OCSP – Online Certificate Status Protocol

OFB – Output Feedback

OLA – Operating Level Agreement

OS – Operating System

OTP – One-Time Password

OVAL – Open Vulnerability Assessment Language

PaaS – Platform as a Service

PACS – Physical Access Control Server

PAP – Password Authentication Protocol

PAT – Port Address Translation

PBX – Private Branch Exchange

PCI-DSS – Payment Card Industry Data Security Standard

PDP – Policy Distribution Point

PEAP – Protected Extensible Authentication Protocol

PEP – Policy Enforcement Point

PFS – Perfect Forward Secrecy

PGP – Pretty Good Privacy

PII – Personal Identifiable Information

PIP – Policy Information Point

PKI – Public Key Infrastructure

POTS – Plain Old Telephone Service

PPP – Point-to-Point Protocol

PPTP – Point-to-Point Tunneling Protocol

PSK – Pre-Shared Key

QoS – Quality of Service

RA – Recovery Agent

RA – Registration Authority

RAD – Rapid Application Development

RADIUS – Remote Authentication Dial-in User Server

RAID – Redundant Array of Inexpensive/Independant Disks

RAS – Remote Access Server

RBAC – Role-Based Access Control

RBAC – Rule-Based Access Control

REST – Representational State Transfer

RFI – Request for Information

RFP – Request for Proposal

RFQ – Request for Quote

RPO – Recovery Point Objective

RSA – Rivest, Shamir and Adleman

RTO – Recovery Time Objective

RTP – Real-Time Transport Protocol

S/MIME – Secure/Multipurpose Internet Mail Extensions

SaaS – Software as a Service

SAML – Security Assertions Markup Language

SAN – Subject Alternative Name

SAN – Storage Area Network

SCADA – Supervisory Control and Data Acquisition

SCAP – Security Content Automation Protocol

SCP – Secure Copy

SCSI – Small Computer System Interface

SDL – Security Development Life Cycle

SDLC – Software Development Life Cycle

SDLM – Software Development Life Cycle Methodology

SHA – Secure Hashing Algorithm

SIEM – Security Information Event Management

SIM – Subscriber Identity Module

SIP – Session Initiation Protocol

SLA – Service Level Agreement

SLE – Single Loss Expectancy

SMS – Short Message Service

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOA – Service Oriented Architecture

SOAP – Simple Object Access Protocol

SOA – Start of Authority

SOC – Security Operations Center

SOE – Standard Operating Environment

SOW – Statement of Work

SOX – Sarbanes-Oxley Act

SP – Service Provider

SPIM – Spam over Internet Messaging

SPIT – Spam over Internet Telephony

SPML – Service Provisioning Markup Language

SRTM – Security Requirements Traceability Matrix

SRTP – Secure Real-Time Protocol

SSD – Solid State Drive

SSDLC – Security System Development Life Cycle

SSH – Secure Shell

SSL – Secure Sockets Layer

SSO – Single Sign-On

SSP – Storage Service Provider

TACACS – Terminal Access Controller Access Control System

TCO – Total Cost of Ownership

TCP/IP – Transmission Control Protocol/Internet Protocol

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

TOS – Type of Service

TOTP – Time-based One-time Password

TPM – Trusted Platform Module

TSIG – Transaction Signature Interoperability Group

UAC – User Access Control

UAT – User Acceptance Testing

UDDI – Universal Description Discovery and Integration

UDP – User Datagram Protocol

UPS – Uninterruptable Power Supply

URL – Universal Resource Locator

USB – Universal Serial Bus

UTM – Unified Threat Management

VaaS – Voice as a Service

VDI – Virtual Desktop Infrastructure

VLAN – Virtual Local Area Network

VoIP – Voice over IP

VPN – Virtual Private Network

vSAN – Virtual Storage Area Network

VTC – Video Teleconferencing

VTPM – Virtual TPM

WAF – Web Application Firewall

WAP – Wireless Access Point

WAYF – Where Are You From

WEP – Wired Equivalent Privacy

WIDS – Wireless Intrusion Detection System

WIPS – Wireless Intrusion Prevention System

WPA – Wireless Protected Access

WRT – Work Recovery Time

WSDL – Web Services Description Language

WWN – World Wide Name

XACML – eXtensible Access Control Markup Language

XSS – Cross-Site Scripting