COMPTIA CAS-001 EXAM QUESTIONS & ANSWERS

Number: CAS-001
Passing Score: 800
Time Limit: 120 min
File Version: 31.1

COMPTIA CAS-001 EXAM QUESTIONS & ANSWERS

Exam Name: CompTIA Advanced Security Practitioner

Examsheets

QUESTION 1
You need to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future?

A. Perfect forward secrecy
B. Secure socket layer
C. Secure shell
D. Security token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Perfect forward secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

Forward secrecy has been used as a synonym for perfect forward secrecy, since the term perfect has been controversial in this context. However, at least one reference distinguishes perfect forward secrecy from forward secrecy with the additional property that an agreed key will not be compromised even if agreed keys derived from the same long-term keying material in a subsequent run are compromised.

Answer option C is incorrect. Secure Shell (SSH) is a program that is used for logging into a remote computer over a network. Secure Shell can be used to execute commands on a remote machine and to move files from one machine to another. SSH uses strong authentication and secure communications over insecure channels.

Answer option B is incorrect. Secure Sockets Layer (SSL) is a protocol that was developed by Netscape for transmitting private documents via the Internet. It uses a cryptographic system thatuses public and private keys to encrypt data. A public key is globally available and a private key is known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support the SSL protocol. Several web sites use this protocol to obtain confidential user information. When the SSL protocol is used to connect to a Web site, the URL must begin with https instead of http.

Answer option D is incorrect. Security token can be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access his bank account). The token is used in addition to or in place of a password to prove that the customer is who he claims to be. The token acts like an electronic key to access something.

QUESTION 2
The Security Development Lifecycle (SDL) consists of various security practices that are grouped under seven phases. Which of the following security practices are included in the Requirements phase?

Each correct answer represents a complete solution. Choose all that apply.

A. Incident Response Plan
B. Create Quality Gates/Bug Bars
C. Attack Surface Analysis/Reduction
D. Security and Privacy Risk Assessment

Correct Answer: BD
Section: (none)

Explanation

Explanation/Reference:
Explanation:
The Requirements phase of the Security Development Lifecycle (SDL) includes the following security practices:
· Security and Privacy Requirements
· Create Quality Gates/Bug Bars
· Security and Privacy Risk Assessment

Answer option C is incorrect. Attack Surface Analysis/Reduction is a security practice included in the Design phase of the Security Development Lifecycle (SDL).

Answer option A is incorrect. Incident Response Plan is a security practice included in the Release phase of the Security Development Lifecycle (SDL).

QUESTION 3
Which of the following components of a VoIP network is frequently used to bridge video conferencing connections?

A. MCU
B. Videoconference station
C. IP Phone
D. Call agent
"Certification Depends on Only One Thing" - www.actualanswers.com 3 CompTIA CAS-001 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Multipoint Control Unit (MCU) is a device frequently used to bridge video conferencing connections. The Multipoint Control Unit is an endpoint on the LAN that provides the ability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs). Answer option C is incorrect. IP Phones provide IP endpoints for voice communication. Answer option D is incorrect. A call agent provides call control for IP phones, CAC, bandwidth control and management, and address translation. Unlike a gatekeeper, which in a Cisco environment typically runs on a router, a call agent typically runs on a server platform. Cisco Unified Communications Manager is an example of a call agent.

The call agent controls switching logic and calls for all the sites under the central controller. A central gateway controller includes both centralized configuration and maintenance of call control functionality, when new functionality needs to be added, only the controller needs to be updated.

Answer option B is incorrect. A videoconference station provides access for end-user involvement in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. A user can view video streams and hear audio that originates at a remote user station.

QUESTION 4
Which of the following is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies?

A. SAML
B. SOAP
C. SPML
D. XACML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy delegation

"Certification Depends on Only One Thing" - www.actualanswers.com 4 CompTIA CAS-001 Exam

profile (administrative policy profile).

Answer option B is incorrect. SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks, it relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Answer option C is incorrect. Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.

Answer option A is incorrect. Security Assertion Markup Language (SAMLJ is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION 5
You work as a Network Administrator for uCertify Inc. You want to allow some users to access a particular program on the computers in the network. What will you do to accomplish this task?

A. Apply remote access policies
B. Apply NTFS permissions
C. Apply group policies
D. Apply account policies
"Certification Depends on Only One Thing" - www.actualanswers.com 5 CompTIA CAS-001 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to accomplish the task, you should apply group policy in the network. A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network resources, computers, and operating systems.

They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar. the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu.

Answer option D is incorrect. An account policy controls the password expiration policy, the lockout policy, and other password features.

Answer option B is incorrect. NTFS permissions are attributes of the folder or file for which they are configured. These include both standard and special levels of settings. The standard settings are combinations of the special permissions which make the configuration more efficient and easier to establish.

Answer option A is incorrect. A remote access policy specifies how remote users can connect to the network and the requirements for each of their systems before they are allowed to connect. It defines the methods users can use to connect remotely such as dial up or VPN. This policy is used to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

QUESTION 6
Which of the following security practices are included in the Implementation phase of the Security Development Lifecycle (SDL)? Each correct answer represents a complete solution. Choose two.

A. Establish Design Requirements
B. Perform Static Analysis
C. Use Approved Tools
D. Execute Incident Response Plan

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security practices performed during each phase of the Security Development Lifecycle (SDL) process are as follows:

Phases	Security Practices
Training	• Core Security Training
Requirements	• Security and Privacy Requirements • Create Quality Gates/Bug Bars • Security and Privacy Risk Assessment
Design	• Establish Design Requirements • Attack Surface Analysis/Reduction • Threat Modeling
Implementation	• Use Approved Tools • Deprecate Unsafe Functions • Perform Static Analysis
Verification	• Perform Dynamic Analysis • Fuzz Testing • Attack Surface Review
Release	• Incident Response Plan • Final Security Review • Release/Archive
Response	• Execute Incident Response Plan

C:\Documents and Settings\user-nwz\Desktop\1.JPG

QUESTION 7
SDLC phases include a minimum set of security tasks that are required to effectively incorporate security in the system development process. Which of the following are the key security activities for the development/

acquisition phase?

Each correct answer represents a complete solution. Choose two.

A. Prepare initial documents for system certification and accreditation
B. Conduct the risk assessment and use the results to supplement the baseline security controls
C. Determination of privacy requirements
D. Initial delineation of business requirements in terms of confidentiality, integrity, and availability

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Key security activities for the development/acquisition phase are as follows:
· Conduct the risk assessment and use the results to supplement the baseline security controls · Analyze security requirements
· Perform functional and security testing
· Prepare initial documents for system certification and accreditation · Design security architecture

Answer options D and C are incorrect. Key security activities for the initiation phase are as follows:
· Initial definition of business requirements in terms of confidentiality, integrity, and availability · Determination of information categorization and identification of known special handling requirements in transmitting, storing, or creating information · Determination of privacy requirements

QUESTION 8
In which of the following attacks does an attacker intercept call-signaling SIP message traffic and masquerade as the calling party to the called party and vice-versa?

A. Call tampering
B. Man-in-the-middle
C. Eavesdropping
D. Denial of Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: VoIP is more vulnerable to man-in-the-middle attacks. In the man-in-the-middle attack, the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, and vice-versa. The attacker can hijack calls via a redirection server after gaining this position.

Answer option A is incorrect. Call tampering involves tampering a phone call in progress. Answer option D is incorrect. DoS attacks occur by flooding a target with unnecessary SIP call- signaling messages. It degrades the service and causes calls to drop prematurely and halts call processing.

Answer option C is incorrect. In eavesdropping, hackers steal credentials and other information.

QUESTION 9
Which of the following protocols is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web- based push to talk features?

A. SIP
B. MGCP
C. H.323

D. RTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Real-time Transport Protocol (RTP), developed by the Audio-Video Transport Working Group of the IETF and first published in 1996, defines a standardized packet format for delivering audio and video over the Internet. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features. For these, it carries media streams controlled by H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols, making it one of the technical foundations of the Voice over IP industry. RTP is usually used in conjunction with the RTP Control Protocol (RTCP). When both protocols are used in conjunction, RTP is usually originated and received on even port numbers, whereas RTCP uses the next higher odd port number. RTP and RTCP typically use unprivileged UDP ports (1024 to 65535).

Answer option C is incorrect. H.323 is a group of protocols defined by the International Telecommunication Union for multimedia conferences over Local Area Networks. The H.323 collection of protocols collectively may use up to two TCP connections and four to six UDP connections. H.323 inspection is used for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 application inspecti

Answer option A is incorrect. Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP). Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. The protocol can be used for creating, modifying, and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc. The SIP protocol is a TCP/IP-based Application Layer protocol. Within the OSI model, it is sometimes placed in the session layer. SIP is designed to be independent of the underlying transport layer; it can run on TCP, UDP, or SCTP. It is a text-based protocol, sharing many elements of the Hypertext Transfer Protocol (HTTP) upon which it is based, allowing for easy inspection by administrators. SIP clients typically use TCP or UDP (typically on port 5060 and/ or 5061) to connect to SIP servers and other SIP endpoints.

Answer option B is incorrect. MGCP stands for Media Gateway Control Protocol. The Media Gateway Control Protocol is architecture for controlling media gateways on Internet Protocol (IP) networks and the public switched telephone network (PSTN). It is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet is called as media gateway. MGCP supports a large number of devices on an internal network with a limited set of external (global)

addresses using NAT and PAT.

QUESTION 10
Which of the following stages are involved in the successful implementation of a collaboration platform? Each correct answer represents a part of the solution. Choose two.

A. Ongoing collaboration solution design
B. Federated identity management
C. Platform implementation
D. Product and service integration

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following stages are involved in the successful implementation of a collaboration platform are as follows:
1. Platform implementation
2. Ongoing collaboration solution design

QUESTION 11
How many levels of threats are faced by the SAN?

A. 3
B. 7
C. 2
D. 5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Storage area network transfers and stores crucial data; often, this makes storage area network vulnerable to risks. There are three different levels of threats faced by the SAN:
· Level one: These types of threats are unintentional and may result in downtime and loss of revenue. However, administrators can prevent these threats. · Level two: These types of threats are simple malicious attacks that use existing equipments. · Level three: These types of threats are large scale attacks and are difficult to prevent. These threats come from skilled attackers using uncommon equipments.

QUESTION 12
Which of the following statements are true about OCSP and CRL?

Each correct answer represents a complete solution. Choose all that apply.

A. The OCSP checks certificate status in real time
B. The CRL is a list of subscribers paired with digital certificate status.
C. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current.
D. The CRL allows the authenticity of a certificate to be immediately verified.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Certificate Revocation List (CRL) is one of the two common methods when using a public key infrastructure for maintaining access to servers in a network. Online Certificate Status Protocol (OCSP), a newer method, has superseded CRL in some cases.

The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason for revocation. The dates of certificate issue, and the entities that issued them, are also included. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current OCSP overcomes this limitation by checking certificate status in real time. The OCSP allows the authenticity of a certificate to be immediately verified.

QUESTION 13
Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. What are the essential elements required for continuous monitoring?

Each correct answer represents a complete solution. Choose all that apply.

A. Ongoing assessment of system security controls
B. Security tools definition
C. Security status monitoring and reporting
D. Security impact analyses
E. Configuration management and change control

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

decisions. Following are the four essential elements required for continuous monitoring:
· Configuration management and change control
· Security impact analyses
· Ongoing assessment of system security controls
· Security status monitoring and reporting

QUESTION 14
Mike is trying to reduce the risks posed by end user activities. He is particularly concerned about how to deal with employees who take work home. Which of the following is the most likely risk posed by employees taking work home?

A. The employee selling confidential data
B. SQL Injection
C. Cost of transporting work data
D. Getting malware from home on the media used to transport work data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Employees who take work home, must take it on some sort of media. That media could pick up a virus or spyware from their home computer, which will then be brought back to the corporate network.

Answer option A is incorrect, Employees selling confidential data is always a possible risk, however it is less likely.

Answer option B is incorrect. SQL Injection is most likely accomplished by an external hacker.

Answer option C is incorrect. There is no significant cost associated.

QUESTION 15
Cloud computing is significantly impacting the definition of network perimeters. Which of the following is NOT a network perimeter issue with cloud computing?

A. Where is the data actually physically stored?
B. What is the viability of the cloud provider?
C. What regulatory requirements apply to the data given the data and the location of the servers?
D. What protections are in place on the cloud?

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While the viability of the provider is an important issue to consider, it is not a network perimeter issue.

"Certification Depends on Only One Thing" - www.actualanswers.com 30 CompTIA CAS-001 Exam

Answer options C, A, and D are incorrect. These are all significant network perimeter issues associated with cloud computing.

QUESTION 16
A partnership is a for profit business association of two or more persons. Which of the following statements are true about partnership? Each correct answer represents a complete solution.
Choose all that apply.

A. Each and every partner shares directly in the organization's profits and shares control of the business operation.
B. A partnership is an arrangement where parties agree to cooperate to advance their mutual interests.
C. The consequence of this profit sharing is that employees are jointly and independently liable for the partnership's debts.
D. Partnerships present the involved parties with special challenges that must be navigated unto agreement. "Certification Depends on Only One Thing" - www.actualanswers.com 31 CompTIA CAS-001 Exam

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A partnership is a for profit business association of two or more persons. Because the business component is defined broadly by state laws and because persons can include individuals, groups of individuals, companies, and corporations, partnerships are highly adaptable in form and vary in complexity.

A partnership is an arrangement where parties agree to cooperate to advance their mutual interests. Partnerships present the involved parties with special challenges that must be navigated unto agreement. Each and every partner shares directly in the organization's profits and shares control of the business operation. The consequence of this profit sharing is that partners are jointly and independently liable for the partnership's debts.

QUESTION 17
Resource exhaustion includes all of the following except_____

A. Opening too many connections

B. Allocating all system memory to a single application
C. Overflowing a buffer with too much data
D. Flooding a network with excessive packets

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Buffer overflow attacks is related to resource exhaustion but is not the same thing. The reason being that the buffer overflow is based on programmers not checking array bounds, rather than exhausting resources.

Answer options A, B, and D are incorrect. All of these are examples of resource exhaustion.

QUESTION 18
"Certification Depends on Only One Thing" - www.actualanswers.com 34 CompTIA CAS-001 Exam
Which of the following security measures would be most effective against a memory exhaustion DoS attack?

A. SPI Firewall
B. Secure programming
C. Checking user inputs
D. Truncating buffers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Memory exhaustion happens when a flaw in an application allows the application to keep consuming more memory leaving none available for other applications. Answer option C is incorrect. Checking user inputs is an effective defense against SQL injection attacks, but not memory exhaustion attacks.

Answer option D is incorrect. Truncating buffers is an effective defense against a buffer overflow attack, .but not against memory exhaustion attacks.

Answer option A is incorrect. An SPI firewall is effective in stopping a syn flood, but would not help against a memory exhaustion attack.

QUESTION 19
Denise works as a Security Administrator for a community college. She is assessing the various risks to her network. Which of the following is not a category of risk assessment?

A. Cost determination
B. Risk determination
C. Vulnerability assessment
D. Likelihood assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Of course the cost of addressing a risk must be computed, but that is not part of risk assessment. Answer option D is incorrect. Likelihood assessment is a key part of risk assessment. How likely is a given threat? What threats are the most likely to your network?

Answer option B is incorrect. Determining what risks your network has, is one of the first steps in risk assessment.

Answer option C is incorrect. Assessing your networks vulnerabilities is a key part of risk assessment.

Answer option C is incorrect. Assessing your networks vulnerabilities is a key part of risk assessment.

QUESTION 20
_____applies enterprise architecture concepts and practices in the information security domain.

A. ESA
B. OWASP
C. OVAL
D. AAR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enterprise Security Architecture (ESA) is a system for applying network architecture principles and guidelines to network security.

Answer option D is incorrect. An After Action Report (AAR) is conducted to assess what went wrong after a breach.

Answer option C is incorrect. Open Vulnerability and Assessment Language (OVAL) is a standard to assess vulnerabilities in a system.

Answer option B is incorrect. The Open Web Application Security Project (OWASP) is a set of standards for security web applications.

QUESTION 21
Which of the following is a written document and is used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement?

A. Patent law
B. Memorandum of understanding (MOU)
C. Memorandum of agreement (MOA)
D. Certification and Accreditation (COA or CnA)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A memorandum of understanding (MOU) is a document that defines a bilateral or multilateral agreement between two parties. This document specifies a convergence of will between the parties, representing a

proposed common line of action. A memorandum of understanding is generally used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement. It is a proper substitute of a gentlemen's agreement.

Answer option A is incorrect. Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time.

Answer option C is incorrect. A memorandum of agreement (MOU)is a document that is written between two parties to cooperatively work together on a project for meeting the pre-decided objectives. The principle of an MOA is to keep a written understanding of the agreement between two parties.

A memorandum of agreement is used in various heritage projects. It can also be used between agencies, the public and the federal or state governments, communities, and individuals. A memorandum of agreement (MOA) lays out the main principles of a positive cooperative effort. Answer option D is incorrect. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C8A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3.

"Certification Depends on Only One Thing" - www.actualanswers.com 39 CompTIA CAS-001 Exam

Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

QUESTION 22
Which of the following elements are essential elements of a privacy policy? Each correct answer represents a complete solution. Choose two.

"Certification Depends on Only One Thing" - www.actualanswers.com 41 CompTIA CAS-001 Exam

A. Opt-out provision
B. Reliability
C. Availability
D. Notification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The essential elements of a privacy policy, which provides a high-level management statement of direction, are notifications and opt-out provisions.

QUESTION 23
Which of the following is used to provide for the systematic review, retention and destruction of documents received or created in the course of business?

A. Document retention policy
B. Document research policy

C. Document entitled policy
D. Document compliance policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A document retention policy is used to provide for the systematic review, retention and destruction of documents received or created in the course of business. It will identify documents that need to be maintained and consist of guidelines for how long certain documents should be kept and how they should be destroyed.

Answer options B, D. and C are incorrect. These are not valid options.

QUESTION 24
Which of the following is a log that contains records of login/logout activity or other security-related events specified by the systems audit policy?

A. Process tracking
B. Logon event
C. Object Manager
D. Security Log
"Certification Depends on Only One Thing" - www.actualanswers.com 42 CompTIA CAS-001 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Security log records events related to security like valid and invalid logon attempts or events related to resource usage, such as creating, opening, or deleting files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer.

Answer option B is incorrect. In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authorizing the user referring to credentials presented by the user.

Answer option C is incorrect. Object Manager is a subsystem implemented as part of the Windows Executive which manages Windows resources.

QUESTION 25
Which of the following are the purposes of the Cost-benefit analysis process? Each correct answer represents a complete solution. Choose two.

A. To determine if an investment is sound
B. To describe the future value on the investment of the project
C. To see how it compares with alternate projects
D. To support benefit management, measurement, and reporting "Certification Depends on Only One Thing" - www.actualanswers.com 44 CompTIA CAS-001 Exam

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The Cost-benefit analysis (CBA) process is used to calculate and compare benefits and costs of a project for the following purposes:
· To determine if an investment is sound
· To see how it compares with alternate projects

Answer options D and B are incorrect. These are not the purposes of the Cost-benefit analysis process,

QUESTION 26
Which of the following is an approximate of the average or mean time until a component's first failure or disruption in the operation of the product, process, procedure, or design takes place?

A. MTBF
B. HMA
C. MSDS

D. MTF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mean TimetoFailure (MTTF) is an approximate of the average, or mean time until a components first failure, or disruption in the operation of the product, process, procedure, or design takes place. MTTF presumes that the product CANNOT be repaired and the product CANNOT continue any of its regular operations.

In many designs and components, MTTF is especially near to the MTBF, which is a bit longer than MTTF. This is due to the fact that MTBF adds the repair time of the designs or components. MTBF is the average time between failures to include the average repair time, or MTTR. Answer option A is incorrect. Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.

Answer option B is incorrect. Hash-based Message Authentication Code (HMAC) is a specific construction for calculating a Message Authentication Code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC. The resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

Answer option C is incorrect. A Material Safety Data Sheet (MSDS) is a document that specifies a set of guidelines regarding the proper handling, transporting, storage, and disposal of a hazardous substance or chemical. It also contains information on first-aid treatment, as it is helpful in case of accident or exposure to toxic material. This sheet is displayed in areas where such untoward incidents can be possible, so that in case of any emergency, proper actions, based on the information provided on the sheet, can be taken to handle the situation. The companies or organizations are required to create and paste MSDS in hazardous areas.

QUESTION 27
Which is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality?

A. Agreement

B. Service Improvement Plan
C. Benchmarking
D. COBIT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance.

Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance.

Answer option A is incorrect. COBIT stands for Control Objectives for Information and Related Technology. COBIT is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

Answer options B and D are incorrect. These are not valid options.

QUESTION 28
Which of the following statements are true about prototypes?

Each correct answer represents a complete solution. Choose three.

A. It reduces initial project risks within a business organization.
B. It reduces the closeness between what a developer has defined for application architecture and what business management has understood.
C. It confirms technology recommendations for an application.
D. It helps verify some of the application requirements that are not dearly defined by a user.
"Certification Depends on Only One Thing" - www.actualanswers.com 48 CompTIA CAS-001 Exam

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following are the purposes of creating a prototype:
1.It reduces initial project risks within a business organization. 2.It helps verify some of the application requirements that are not clearly defined by a user. 3.It confirms technology recommendations for an application. 4.It reduces the gap between what a developer has defined for an application architecture and what business management has understood.
5.It also reduces the gap between what a user has defined for an application requirement or scenario and what a developer has defined in the application development.

Answer:

QUESTION 29
Which of the following statements are true about Fibre Channel over Ethernet (FCoE)?

Each correct answer represents a complete solution. Choose three.

A. It replaces the FCO and FC1 layers of the Fibre Channel stack with Ethernet.
B. It is an encapsulation of Fibre Channel frames over Ethernet networks.
C. It allows Fibre Channel to use 10 Gigabit Ethernet networks while preserving the Fibre Channel protocol.
D. It maps Fibre Channel over selected half duplex IEEE 802.3.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fibre Channel over Ethernet (FCoE) is an encapsulation of Fibre Channel frames over Ethernet networks. It allows Fibre Channel to use 10 Gigabit Ethernet networks while preserving theFibre Channel protocol. FCoE maps Fibre Channel over selected full duplex IEEE 802.3 networks for providing I/O consolidation over Ethernet and reducing network complexity in the datacenter. The

"Certification Depends on Only One Thing" - www.actualanswers.com 50 CompTIA CAS-001 Exam

FCoE protocol specification replaces the FCO and FC1 layers of the Fibre Channel stack with Ethernet.

Answer option D is incorrect. It is not a correct statement about Fibre Channel over Ethernet (FCoE).

QUESTION 30
Which of the following is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally?

A. File carving
B. Virtual backup appliance
C. Backup
D. Data recovery
"Certification Depends on Only One Thing" - www.actualanswers.com 51 CompTIA CAS-001 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often the data are being salvaged from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

Answer option C is incorrect. A backup or the process of backing up is making copies of data which may be used to restore the original after a data loss event.

Answer option A is incorrect. File carving is the process of reassembling computer files from fragments in the absence of filesystem metadata.

Answer option B is incorrect. A virtual backup appliance (VBA) is a small virtual machine that backs up and restores other virtual machines.

QUESTION 31
Which of the following refers to any system whereby things that are of value to an entity or group are monitored and maintained?

A. Asset management
B. Investment management
C. Service management
D. Product management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Asset management deals with the management of assets of an organization. An asset is defined as an item of value. It is essential for a company to identify, track, classify, and assign ownership for the most important assets. The main idea behind asset management is to ensure that the assets are protected.

Answer options B, D, and C are incorrect. These are not valid options.

"Certification Depends on Only One Thing" - www.actualanswers.com 52 CompTIA CAS-001 Exam

QUESTION 32
Allen is a network administrator for a hosting company. Multiple different companies store data on the same server. Which of the following is the best method to reduce security issues from co- mingling?

A. Install each data set on a separate drive
B. Install each data set on a separate partition
C. Install each data set on the same drive, but use EFS to encrypt each data set separately.
D. Install each data set on a separate VM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Visualization completely separates the data and prevents commingling. Visualization is a technology that enables customers to run multiple operating systems concurrently on a single physical server, where each of the operating systems runs as a self-contained computer, visualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device, or network resources. It is a computing technology that enables a single user to access multiple physical devices. The goal of visualization is usually a more effective use of resources. It simplifies provisioning, while adding flexibility at the same time.

"Certification Depends on Only One Thing" - www.actualanswers.com 53 CompTIA CAS-001 Exam

Answer options B and A are incorrect. An operating system can view partitions and drives just as if they were different folders/directories on the same drive.

Answer option C is incorrect. Encrypting the data sets with EFS will inhibit users' access for the data.

QUESTION 33
An organization s network uses public keys for message encryption. Which of the following manages security credentials in the network and issues certificates to confirm the identity and other attributes of a certificate in relation to other entities?

A. Certificate Authority
B. Certificate Revocation List
C. Public Key Infrastructure

D. Online Certificate Status Protocol

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Certification authority (CA) is an entity in a network, which manages security credentials and public keys for message encryption. It issues certificates that confirm the identity and other attributes of a certificate in relation to other entities. Depending on the public key infrastructure implementation, a certificate includes the owners name, the owner's public key, information about the public key owner, and the expiry date of the certificate.

Answer option B is incorrect. CRL stands for Certificate Revocation List. In CRL, the certificates that are revoked by the Certificate Authority (CA) are mentioned. It becomes necessary for NetScreen to check the status of certificates received against a CRL to ensure their validity in phase 1 negotiation. The firewall recovers the CRL that is defined in the CRL certificate if a CRL is not loaded into the NetScreens database. The firewall attempts to recover the CRL defined in the CA certificate by means of LDAP or HTTP. In case the CRL is not defined in the CA certificate it can use the URL defined by the user for the CRL.

Answer option D is incorrect. Online Certificate Status Protocol (OCSP) is used for obtaining the revocation status of an X.509 digital certificate. It is used to verify the status of a certificate. It was created as an alternative to certificate revocation lists (CRL). It provides more timely information about the revocation status of a certificate. It also eliminates the need for clients to retrieve the CRLs themselves. Therefore, it generates to less network traffic and provides better bandwidth

management. It is described in RFC 2560 and is on the Internet standards track.

Answer option C is incorrect. A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained andshared through a trusted authority. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

QUESTION 34
What is the goal of a black-box penetration testing?

A. To simulate a user to include customizable scripts, additional tools and configurable kernels in personalized distributions
B. To simulate an external hacking or cyber warfare attack
C. To simulate an attacker who has some knowledge of the organization and its infrastructure
D. To simulate a malicious insider who has some knowledge and possibly basic credentials to the target system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Black Box is a kind of Penetration testing, which assumes no prior knowledge of the infrastructure to be tested. The testers must first determine the location and extent of the systems before commencing their analysis. Black box testing simulates an attack from someone who is unfamiliar with the system.

Answer option D is incorrect. A white box penetration testing has a goal to simulate a malicious insider who has some knowledge and possibly basic credentials to the target system. Answer option A is incorrect. BackTrack

has a goal to simulate a user to include customizable scripts, additional tools and configurable kernels in personalized distributions.

Answer option C is incorrect. A grey box penetration testing has a goal to simulate an attacker who has some knowledge of the organization and its infrastructure.

QUESTION 35
A user has entered a user name and password at the beginning of the session, and accesses multiple applications. He does not need to re-authenticate for accessing each application. Which of the following authentication processes is he using?

A. File authentication
B. Mutual authentication
C. Biometric authentication
D. SSO authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user is using single sign-on (SSO) authentication process. In this process, he needs one-time authentication to access multiple resources. He is required to enter a user name and password

only at the beginning of the session. He does not need to re-authenticate or maintain separate usernames and passwords for accessing each application.

Answer option B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication.

Answer option A is incorrect. There is no such authentication process as File authentication. Answer option C is incorrect. Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment.

QUESTION 36
Which of the following helps an employee to access his corporation's network while traveling?

A. Remote access
B. Remote Assistance
C. Task Manager
D. Computer management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In most enterprises, networks secure remote access has become an important component. Remote access helps in accessing a computer or a network from a remote distance. In corporations, people working in branch offices, telecommuters, and people who are traveling may need to access the corporation s network. Home

users can access the Internet through remote access to an Internet service provider (ISP).

Answer option B is incorrect. Remote Assistance is a windows feature to enable support personnel (helper) to provide technical support to a remote user (host). Through Remote Assistance a helper can view Windows session of a host on his computer itself.
Remote Assistance works as follows:
· A remote user sends an invitation to an Administrator (or expert) through e-mail or Windows Messenger.
· The Administrator accepts the request and can then view the users desktop.

"Certification Depends on Only One Thing" - www.actualanswers.com 63 CompTIA CAS-001 Exam

To maintain privacy and security, all communication is encrypted. Remote Assistance can be used only with the permission of the person who requires the assistance.

Note: If the user has enabled the Allow this computer to be controlled remotely option in Remote control section of Remote Assistance Settings dialog box, an expert can even take control of the keyboard and mouse of a remote computer to guide the user.

Answer option D is incorrect. Computer Management is an administrative tool that allows administrators to manage the local computer in several ways, but it cannot be used to provide remote assistance to a user.

Answer option C is incorrect. The Task Manager utility provides information about programs and processes running on a computer. By using Task Manager, a user can end or run programs, end processes, and display a dynamic overview of his computers performance. Task Manager provides an immediate overview of system activity and performance.

QUESTION 37
You have considered the security of the mobile devices on your corporate network from viruses and malware. Now, you need to plan for remotely enforcing policies for device management and security, which of the following things are includes in the configuration management of mobile devices?

Each correct answer represents a part of the solution. Choose three.

A. Controlling the apps deployed on devices
B. Managing the OS version of devices
C. Supporting other preferred corporate policy
D. Managing application and security patches

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Configuration management is included in the remote device management policies. It involves deploying IT-approved software versions of supported mobile platforms. Configuration management includes the following things:
· Managing the OS version of devices
· Managing application and security patches
· Supporting other preferred corporate policy

"Certification Depends on Only One Thing" - www.actualanswers.com 64 CompTIA CAS-001 Exam

QUESTION 38
Which of the following teams has the responsibility of accounting for personnel and rendering aid?

"Certification Depends on Only One Thing" - www.actualanswers.com 67 CompTIA CAS-001 Exam

A. Physical security team

B. Emergency response team
C. Emergency management team
D. Damage assessment team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The emergency response team has the responsibility of accounting for personnel and rendering aid. The emergency response team includes fire wardens for each floor and those persons trained in administering first aid.

Answer option D is incorrect. The damage assessment team assesses the damage of the disaster in order to provide the estimate of time required to recover.

Answer option A is incorrect. The physical security team addresses crowd control and security and operates 24 hours a day to protect individuals and organizational assets.

Answer option C is incorrect. The Emergency management team consists of executives and line managers to make strong decisions at the Emergency Operations Center. This team coordinates with the managers still operating on undamaged areas of the business and makes decisions about the allocation of personnel necessary to support the response and recovery efforts. The leaders of each team report to the emergency management team.

QUESTION 39
Which scanning is one of the more unique scan types, as it does not exactly determine whether the port is open/closed, but whether the port is filtered/unfiltered?

A. UDP scanning
B. TCP SYN scanning
C. TCP FIN scanning
D. ACK scanning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ACK scanning is one of the more unique scan types. It determines whether the port is filtered or unfiltered instead of determining whether the port is open or closed. This is especially good when attempting to explore for the existence of a firewall and its rule-sets. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning.

Answer option B is incorrect. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:
1.The attacker sends a SYN packet to the target port.
2.If the port is open, the attacker receives the SYN/ACK message. 3.Now the attacker breaks the connection by sending an RST packet. 4.If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

Answer option A is incorrect. UDP scan is little difficult to run. UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. This method is also affected by ICMP rate limiting.

"Certification Depends on Only One Thing" - www.actualanswers.com 70 CompTIA CAS-001 Exam

Answer option C is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because Windows operating systems send only RST packets irrespective of whether the port is open or closed.

QUESTION 40
Consider the following scenario.

A user receive an email with a link to a video about a news item, but another valid page, for instance a product page on ebay.com, can be hidden on top underneath the 'Play' button of the news video. The user tries to play' the video but actually buys' the product from ebay.com.

Which malicious technique is used in the above scenario?

A. Malicious add-ons
B. Cross-Site Request Forgery
C. Click-jacking
D. Non-blind spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Click-jacking is a malicious technique that is used to trick Web users into revealing confidential information or sometimes taking control of their computer while clicking on apparently innocuous Web pages. Click-jacking is used to take the form of embedded code/script that can execute without the users' knowledge, such as clicking on a button appearing to execute another function. The term "click-jacking" was invented by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as UI redressing, Click-jacking can be understood as an instance of the confused deputy problem.

Answer option D is incorrect. Non-blind spoofing is a type of IP spoofing attack. This attack occurs when the attacker is on the same subnet as the destination computer, or along the path of the destination traffic. Being on the same subnet, it is easy for the attacker to determine the sequence number and acknowledgement number of the data frames. In a non-blind spoofing attack, the attacker can redirect packets to the destination computer using valid sequence numbers and acknowledge numbers. The result is that the computer's browser session is redirected to a malicious website or compromised legitimate sites that may infect computer with malicious code or

"Certification Depends on Only One Thing" - www.actualanswers.com 71 CompTIA CAS-001 Exam

allow the attacker to perform other malicious activities.

Answer option A is incorrect, Add-ons such as browser plug-ins, application add-ons. font packs, and other after-market components can be an attack vector for hackers. Such add-ons are malicious add-ons. These add-ons can be Trojan horses infecting computers. Antivirus software is an obvious form of defense. Security administrators should also establish a corporate security policy prohibiting the installation and use of

unapproved add-ons.

Answer option B is incorrect. CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding. CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution.

QUESTION 41
In which level of threats of the SAN are threats large scale attacks and difficult to prevent?

A. Level three
B. Level one
C. Level four
D. Level two

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Storage area network transfers and stores crucial data: often, this makes storage area network vulnerable to risks. There are three different levels of threats faced by the SAN:
· Level one: These types of threats are unintentional and may result in downtime and loss of revenue. However, administrators can prevent these threats. · Level two: These types of threats are simple malicious attacks that use existing equipments.

· Level three: These types of threats are large scale attacks and are difficult to prevent. These threats come from skilled attackers using uncommon equipments.

QUESTION 42
Interceptor is a pseudo proxy server that performs HTTP diagnostics, which of the following features are provided by HTTP Interceptor? Each correct answer represents a complete solution.
Choose all that apply.

A. It controls cookies being sent and received.
B. It allows to browse anonymously by withholding Referrer tag, and user agent.
C. It can view each entire HTTP header.
D. It debugs DOC, DOCX, and JPG file.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
HTTP diagnostics is performed by the HTTP Interceptor which is a pseudo proxy server and it also facilitates viewing the two way communication between the browser and the Internet.

Various features of HTTP Interceptor are as follows:
· View each entire HTTP header.
· Debug your PHP, ASP. CGI or JavaScript and htaccess file.
· Control Cookies being sent and received.
· Find out what sort of URL redirection the site may be using. · Browse anonymously by withholding Referrer tag, and user agent.

QUESTION 43
Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Which of the following are multitude of standards that a project must comply?

Each correct answer represents a complete solution. Choose all that apply.

A. Process compliance
B. Decision oversight
C. Control compliance
D. Standards compliance

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Compliance means that an organization must take care of organization's internal regulations, as well as follow the laws of the country and requirements of local legislation and regulations. It may result in conflicts.

Projects must comply with a multitude of standards. Those include the following:
· Standards compliance: Local, state, and federal government · Process compliance: Audit trails, retention, version control · Decision oversight: Change Control Board

QUESTION 44
In which of the following level of likelihood is the threat-source highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective?

A. Average
B. Low
C. High
D. Medium

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Answer option C is correct. Following are the three levels of likelihood:

"Certification Depends on Only One Thing" - www.actualanswers.com 78 CompTIA CAS-001 Exam

· High: In this level, the threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. · Medium: In this level the threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
· Low: In this level, the threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

QUESTION 45
John is concerned about internal security threats on the network he administers. He believes that he has taken every reasonable precaution against external threats, but is concerned that he may have gaps in his internal security. Which of the following is the most likely internal threat?

A. Employees not following security policy
B. Privilege Escalation
C. SQL Injection
D. Employees selling sensitive data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Employees may disregard policies, such as policies limiting the use of USB devices or the ability to download programs from the internet. This is the most pervasive internal security threat. Answer option D is incorrect. Employees selling sensitive data is, of course, possible. However, this scenario is less likely that option A.

Answer option C is incorrect. SQL Injection is most likely accomplished by an external hacker. Answer option B is incorrect. Privilege escalation can be done by internal or external attackers. However, even with internal attackers, it is far less likely than option B.

QUESTION 46
Juanita is a network administrator for a large insurance company. She is concerned about the security risks posed by the employees of the company. There are very thorough and comprehensive security policies at the company. Which of the following would be most effective action for Juanita to take?

A. Putting the company policies on the corporate intranet "Certification Depends on Only One Thing" - www.actualanswers.com 79 CompTIA CAS-001 Exam
B. Make all employees sign the company policy
C. Coordinate with HR to fire anyone who violates any policy
D. Improve employee security education

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Employees usually violate company polices because they are not aware of how significant the risks are. Educating employees is an excellent way to address this.

Answer option C is incorrect. Some employees may need to be terminated for their actions, but that cannot be a default policy.

Answer option E is incorrect. Employees may sign the policy and still not really read it, comprehend it. or follow it.

Answer option A is incorrect. While the company intranet is a good place to distribute company policies, it won't (by itself) improve compliance.

QUESTION 47
Derrick works as a Security Administrator for a police station. He wants to determine the minimum CIA levels for his organization. Which of the following best represents the minimum CIA levels for a police departments data systems?

A. Confidentiality = high, Integrity = high, Availability = high
B. Confidentiality = moderate. Integrity = moderate, Availability = high
C. Confidentiality = low. Integrity = low. Availability = low
D. Confidentiality = high, Integrity = moderate, Availability = moderate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Certification Depends on Only One Thing" - www.actualanswers.com 83 CompTIA CAS-001 Exam

For any law enforcement agency, confidentiality of data is absolutely critical. Breach of confidentiality could have catastrophic consequences. However, integrity and availability issues are standard/moderate.

Answer option A is incorrect. While a law enforcement agency needs high confidentiality, the integrity and availability needs are not high.

Answer option C is incorrect. Certainly all low is not appropriate. And the Confidentiality must be high.

Answer option B is incorrect. This setup is exactly the opposite of what is required.

QUESTION 48
John is establishing CIA levels required for a high schools grade server. This server only has grades. It does not have student or faculty private information (such as social security number, address, phone number, etc.). Which of the following CIA levels will be used by John?

A. Confidentiality = moderate, integrity = moderate. Availability = high
B. Confidentiality = low, Integrity = moderate, Availability = low
C. Confidentiality = high. Integrity = moderate, Availability = moderate
D. Confidentiality = high. Integrity = high, Availability = high

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Confidentiality is not critical here. If data is released, there is no significant negative consequences. Accidental or purposeful changes to grades are the most significant threat to this system. This means that integrity is critical. Finally the availability is not a major issue. If the system is down for a short time, there is no critical impact.

Answer option C is incorrect. There is no need for high confidentiality or for moderate availability.

Answer option D is incorrect. Certainly a grade server does not require all three CIA factors to be high. The data is not highly confidential and the availability is not critical.

Answer option A is incorrect. Moderate integrity is necessary, but moderate confidentiality is not. And it is absolutely unnecessary to have high availability.

"Certification Depends on Only One Thing" - www.actualanswers.com 84 CompTIA CAS-001 Exam

QUESTION 49
A memorandum of understanding (MOU) includes various aspects that are helpful in defining a bilateral or

multilateral agreement between two parties. which of the following are various aspects included in a memorandum of understanding (MOU)?

Each correct answer represents a complete solution. Choose three.

A. Compensation Details
B. Enforceable agreement
C. Communication Details
D. Terms of Agreement

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The various aspects included in a memorandum of understanding (MOU) are as follows:
Communication Details:
The names and contact information of each party
o Any probationary or trial period
o Any set date to review activity, performance, or satisfaction with the arrangement o What parts of this arrangement are open to change or negotiation and how? o What aspects of the arrangement should require formal notification and how? o How will disputes be settled?

Compensation Details:
o Who handles the money and how?
o How are people paid?

o When are people paid?
o How much are people paid?
o How long are people paid?

Terms of Agreement:
o When does the agreement start?
o How long does it last?
o How is the agreement terminated?
o What happens at the end of or after the agreement?

Miscellaneous:
o Any restriction to either party
o Any disclaimer statement
o Any privacy statement
o A place for all parties to sign the agreement

QUESTION 50
Which of the following is a security incident in which sensitive or confidential data is copied,

transmitted, viewed, or stolen by unauthorized person?

A. Security token
B. Data masking
C. Data breach
D. Data erasure

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
A data breach is the planned or unplanned release of secure information to an environment that is not trusted. Incidents range from concerted attack by black hats with the backing of organized crime or national governments to careless disposal of used computer equipment or data storage media.

A data breach is a security incident in which sensitive or confidential data is copied- transmitted, viewed, or stolen by unauthorized person. Financial information like credit card or bank details, personal health information (PHI), personally identifiable information (PII), and trade secrets of corporations or intellectual property can also be involved in a data breach. Answer options A, D, and B are incorrect. These are not valid options.

QUESTION 51
Which of the following statements are true about Risk analysis? Each correct answer represents a complete solution. Choose three.

A. It recognizes risks, quantifies the impact of threats, and supports budgeting for security.
B. It adjusts the requirements and objectives of the security policy with the business objectives and motives.
C. It provides the higher management the details necessary to determine the risks that should be mitigated, transferred, and accepted.
D. It uses public key cryptography to digitally sign records for a DNS lookup.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 90 CompTIA CAS-001 Exam

Explanation:
Risk analysis provides the higher management the details necessary to determine the risks that should be mitigated, transferred, and accepted. It recognizes risks, quantifies the impact of threats, and supports budgeting for security. It adjusts the requirements and objectives of the security policy with the business objectives and motives. The following are the stages in the risk analysis process.
1.Inventory
2.Threat assessment
3.Evaluation of control
4.Management
5.Monitoring

Answer option D is incorrect. It is not a valid statement about Risk analysis.

QUESTION 52
Which of the following steps are involved in a generic cost-benefit analysis process: Each correct answer represents a complete solution. Choose three.

A. Compile a list of key players
B. Assess potential risks that may impact the solution
C. Select measurement and collect all cost and benefits elements
D. Establish alternative projects/programs

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following steps are involved in a generic cost-benefit analysis process:
· Establish alternative projects /programs
· Compile a list of key players
· Select measurement and collect all cost and benefits elements · Predict outcome of cost and benefits over the duration of the project · Put all effects of costs and benefits in dollars
· Apply discount rate
· Calculate net present value of project options
· Sensitivity analysis
· Recommendation

Answer option B is incorrect. It is not a valid step.

"Certification Depends on Only One Thing" - www.actualanswers.com 91 CompTIA CAS-001 Exam

QUESTION 53
Which of the following is a document used to solicit proposals from prospective sellers which require a significant amount of negotiation?

A. RFQ
B. RFI
C. RFP
D. RPQ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Procurement planning involves preparing the documents required and determining the evaluation criteria for the contract award. Three common examples of procurement documents include:
· Requests for information (RFI)
· Requests for proposals (RFP)
· Requests for quotes (RFQ)

A request for information (RFI) is a document used to solicit information about prospective sellers well before a RFP or RFQ is issued. A buyer uses an RFI in order to survey the landscape of sellers that could potentially bid at a later point in time. An RFI typically precedes an RFP or RFQ by many months.

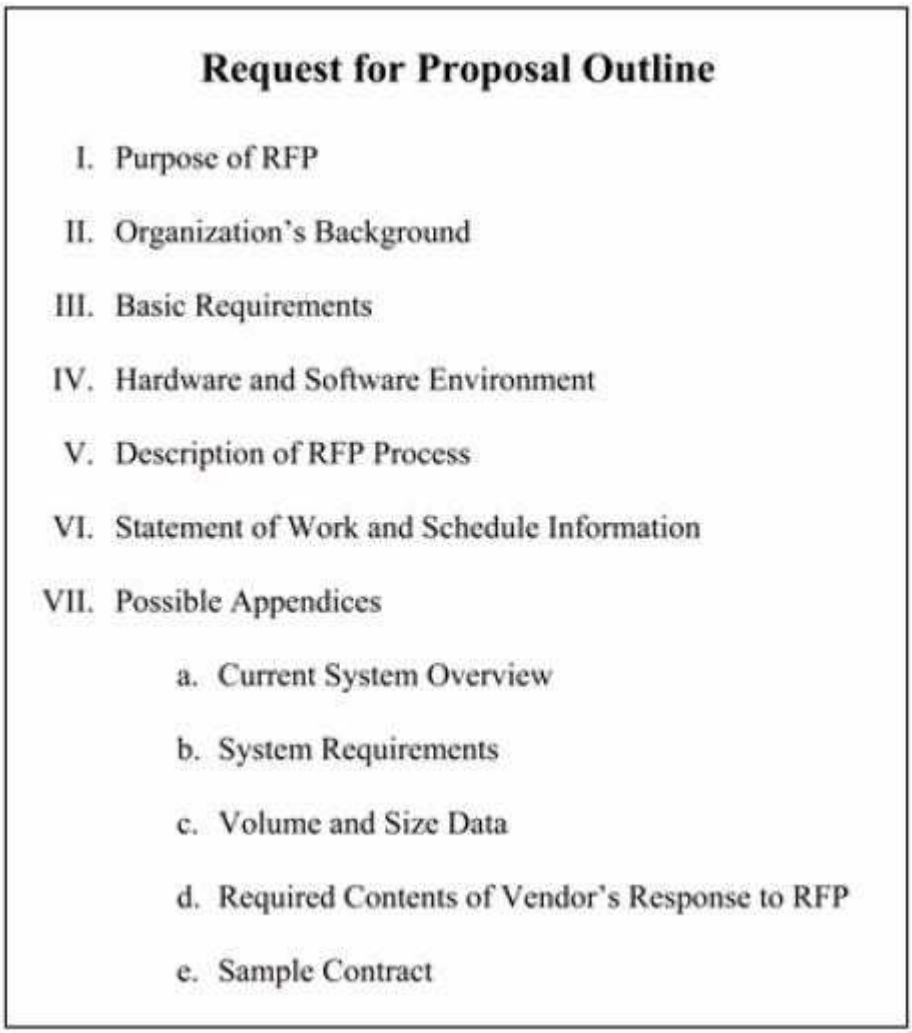
"Certification Depends on Only One Thing" - www.actualanswers.com 92 CompTIA CAS-001 Exam

Requests for Proposal
A request for proposal (RFP) is a document used to solicit proposals from prospective sellers which require a significant amount of negotiation. For example, if an agency wants to automate its work practices, it issues an RFP so sellers can respond with proposals. Sellers might propose various hardware, software, and networking solutions to meet the agency's needs.

Writing a good RFP is a critical part of procurement planning and, as with everything else, expertise is invaluable. Legal requirements are often involved in issuing RFPs and reviewing proposals, especially for government projects. It might be advantageous to consult experts familiar with procurement planning. To make sure the RFP contains the required information to provide the basis for a good proposal, the buying organization should ask the following questions:
· Can the seller develop a good proposal based on the information in the RFP? · Can the seller determine detailed pricing and schedule information based on the RFP?

Below diagram provides a basic outline for creating an RFP. Its main sections include a statement of the purpose, background information about the organization issuing the RFP, the basic requirements for the product or service being procured, the hardware and software environment, a description of the RFP process,

the statement of work and schedule information, and appendices, if required. A simple RFP might be three to five pages long, while an RFP for a larger, more complicated procurement might be hundreds of pages.



C:\Documents and Settings\user-nwz\Desktop\1.JPG

Outline For a Request for Proposal

Request for Quote
In contrast to a RFP, a request for quote (RFQ) is a document used to solicit quotes or bids, which require little negotiation, from prospective sellers for commodity items. For example, if the government wants to purchase 100 personal computers with specific features, it issues an RFQ to potential sellers. RFQs usually don't take as long to prepare as RFPs. nor do responses to them.

All procurement documents must be written to facilitate accurate and complete responses from prospective sellers. They should include background information about the organization and the project, the relevant statement of work, a schedule, a description of the desired form of response, evaluation criteria, pricing forms, and any required contractual provisions. They should also be comprehensive enough to ensure consistent, comparable responses, but flexible enough to allow consideration of seller suggestions for improved ways to meet the requirements.

Answer option D is incorrect. It is not a valid option.

QUESTION 54
Which of the following is a process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation?

A. Value engineering
B. Reverse engineering
C. Forensic engineering
D. Cost engineering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reverse engineering is a process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation. It often involves taking something

apart and analyzing its workings in detail to be used in maintenance or to try to make a new device or program that does the same thing without using or simply duplicating the original.

Answer options A, C, and D are incorrect. These are not valid options.

QUESTION 55
Which of the following is a method of providing an acknowledgement to the sender of the data and an assurance of the senders identity to the receiver, so that neither sender nor the receiver can later deny the data having processed by them?

A. Non-repudiation
B. Digital certificate
C. Digital signature

D. Information assurance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Non-repudiation is one of the security methods that is used to acknowledge the data delivery. It is a method of providing an acknowledgement to the sender of the data and an assurance of the sender's identity to the receiver, so that neither sender nor the receiver can later deny the data having processed by them. Nowadays, non-repudiation is achieved through digital signatures, as it ensures that the data or information, being transferred, has been electronically signed by thepurported person (receiver). It also ensures the furnishing of the signature by the sender since a digital signature can be created only by one person.

Answer options C, D. and B are incorrect. These are not valid options.

QUESTION 56
Which of the following is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations?

A. Incident response team
B. Incident investigation team
C. Incident command team
D. Incident management team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An Incident response team is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations. Incident response teams are common in corporations as well as in public service organizations. This team is generally composed of specific members designated before an incident occurs, although under certain circumstances the team may be an ad-hoc group of willing volunteers.

Incident response team members ideally are trained and prepared to fulfill the roles required by the specific situation (for example, to serve as incident commander in the event of a large-scale public emergency), as the size of an incident grows, and as more resources are drawn into the event, the command of the situation may shift through several phases. In a small-scale event, usually only a volunteer or Ad-hoc Team may respond. In small but growing, and large events, both specific member and ad-hoc teams may work jointly in a unified command system.

Individual team members can be trained in various aspects of the response, be it Medical Assistance/First Aid, hazardous materials spills, hostage situations or disaster relief. Ideally the team has already defined a protocol or set of actions to perform to mitigate the negative effects of the incident.

Answer option D is incorrect. To manage the logistical, fiscal, planning, operational, safety and community issues related to the incident/emergency, an Incident management team will provide the command and control infrastructure that is required. Answer options B and C are incorrect. These are not valid options.

QUESTION 57
Todd is a security administrator, who is responsible for responding to incidents. There has been a

virus outbreak. Which of the following is the final step Todd should take?

A. Eradication
B. Recovery
C. AAR
D. Containment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An after action review is the last phase. At this point it is important to evaluate how the breach occurred and learn from those mistakes.

Answer option A is incorrect. Eradication is actually an early stage, immediately after containment.

Answer option D is incorrect. Containment is the first thing you do once you are aware of the attack.

Answer option B is incorrect. Recovery is actually the next to the last thing to do. That step occurs once the virus is eradicated, but before you do the after action review.

QUESTION 58
John has been granted standard user access to an ecommerce portal. After logging in. he has access to administrative privileges. What is this called?

A. Privilege Escalation
B. Hacking
C. SQL Injection
D. A rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Whenever a user has (accidentally or on purpose) more privileges than assigned, that is called privilege escalation. Privilege escalation is the act of exploiting a bug or design flaw in a software application to gain access to resources, which normally would have been protected, from an application or user. The result is that the application performs actions with more privileges than intended by the application developer or system administrator.

Answer option D is incorrect. A rootkit is software that takes control of the systems root.

Answer option C is incorrect. SQL injection is a method of getting into a website by using SQL commands injected into the website.

Answer option B is incorrect. In this case, this was accidental. The user did not purposefully hack into the system.

QUESTION 59
Which of the following elements of security means that the only authorized users are able to modify data?

A. Authenticity
B. Availability
C. Confidentiality
D. Integrity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are four elements of security, which are as follows:
· Confidentiality: It means that data should only be accessible by authorized users. This access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.
· Integrity: it means that the only authorized users are able to modify data. Modification admits writing, changing, changing status, deleting, and creating. · Availability: It means that data should only be available to authorized users. · Authenticity: it means that a host or service should be able to verify the identity of a user.

QUESTION 60
Which of the following statements are true about Security Requirements Traceability Matrix (SRTM)? Each correct answer represents a complete solution. Choose two.

A. It consists of various security practices that are grouped under seven phases.
B. It is a software development security assurance process proposed by Microsoft.
C. It allows requirements and tests to be easily traced back to one another.
D. It provides documentation and easy presentation of what is necessary for the security of a system.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security Requirements Traceability Matrix (SRTM) is a grid that provides documentation and easy presentation of what is necessary for the security of a system. SRTM is essential in those technical projects that call for security to be incorporated. SRTM can be used for any type of project. It allows requirements and tests to be easily traced back to one another. SRTM ensures that there is accountability for all processes. It also ensures that all work is being completed.

Answer options B and A are incorrect. The Security Development Lifecycle (SDL) is a software development security assurance process proposed by Microsoft. It reduces software maintenance costs and increases reliability of software concerning software security related bugs. The Security Development Lifecycle (SDL) includes the following seven phases:
1.Training

2.Requirements
3.Design
4.Implementation
5.Verification
6.Release
7.Response

QUESTION 61
Which of the following phases of the System Development Life Cycle (SDLC) describes that the system should be modified on a regular basis through the addition of hardware and software?

A. Operation/Maintenance

B. Development/Acquisition
C. Initiation
D. Implementation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are five phases in the SDLC. The characteristics of each of these phases are enumerated below:
· Phase 1: Phase i of the SDLC is known as initiation. In this phase, the need for an IT system is expressed and the purpose and scope of the IT system is documented. · Phase 2: Phase 2 of the SDLC is known as development or acquisition. In this phase, the IT system is designed, purchased, and programmed.
· Phase 3: Phase 3 of the SDLC is known as implementation. This phase involves the system security features. The system security features should be configured, enabled, tested, and verified.
· Phase 4: Phase 4 of the SDLC is known as operation or maintenance. This phase describes that the system should be modified on a regular basis through the addition of hardware and software. · Phase 5: Phase 5 of the SDLC is known as disposal. This phase involves disposition of information, hardware, and software.

QUESTION 62
Which of the following provides cryptographic security services for electronic messaging applications?

A. POP3
B. EFS
C. S/MIME
D. SMTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security {using encryption). Answer option A is incorrect. Post Office Protocol version 3 (POP3) is a protocol used to retrieve e-mails from a mail server. It is designed to work with other applications that provide theability to send e-mails. POP3 is mostly supported by the commercially available mail servers. It does not support retrieval of encrypted e-mails. POP3 uses port 110.

Answer option D is incorrect. Simple Mail Transfer Protocol (SMTP) is a protocol for sending e- mail messages between servers. E-mailing systems use this protocol to send mails over the Internet. SMTP works on the application layer of the TCP/IP or OSI reference model. The SMTP client typically initiates a Transmission Control Protocol (TCP) connection to the SMTP server on the well-known port designated for SMTP, port number 25. However, e-mail clients require POP or IMAP to retrieve mails from e-mail servers.

Answer option B is incorrect. The Encrypting File System (EFS) is a component of the NTFS file system that is used to encrypt files stored in the file system of Windows 2000, Windows XP Professional, and Windows Server 2003 computers. EFS uses advanced and standard cryptographic algorithms to enable transparent encryption and decryption of files. The encrypted data cannot be read by an individual or program without the appropriate cryptographic key.

Encrypted files can be protected even from those who have physical possession of the computer where the encrypted files are stored. Even authorized persons who are able to access the computer and its file system cannot view the data. EFS is the built-in file encryption tool for

windows file systems.

QUESTION 63
Jane works as an administrator for a cloud computing company. Her company supports virtual servers from many organizations, in different industries. What is the most significant security concern when integrating systems from different industries?

A. Different industries have the same security concerns
B. Different industries have different regulatory requirements
C. Different industries have different virus vulnerabilities
D. Different industries have different firewall requirements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Different industries can have radically different regulatory and legal requirements. For example the credit card industry and health care industry have very specific, and different requirements. Answer option C is incorrect. In most cases, viruses are not industry specific. The same virus can affect multiple different systems in diverse industries.

Answer option D is incorrect. Firewall requirements are not different for different industries. Answer option A is incorrect. Different industries do not have the same security concerns.

QUESTION 64
Which of the following are the security issues with COTS products?

Each correct answer represents a complete solution. Choose all that apply.

A. Threats of failures
B. Failure to meet individual requirements
C. High cost of product
D. Dependency on third-party vendors
E. Integration

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
COTS products speed up and reduce the cost of system construction, but they often introduce the following issues:
· Integration: COTS products must be integrated with the existing systems. However, they may contain incompatibilities with the existing programs and services. · Dependency on third-party vendors: All COTS products are provided by third-party vendors. It implies becoming increasingly dependent on third-party vendors and can cause risks if the vendor goes out of business.
· Failure to meet individual requirements: These products may not meet all of the organization's specific requirements as they are designed for general use. · Threats of failures: If COTS products do not give the desired results, a project may end up performing badly or might be a complete failure altogether.

QUESTION 65
What of the following statements is true about voice VLAN?

A. It is used to separate VPN traffic from voice traffic.
B. It is used to separate common user data traffic from TCP traffic.
C. It is used to separate common user data traffic from HTTP traffic.
D. It is used to separate common user data traffic from voice traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The voice VLAN is used to separate common user data traffic from the voice traffic. It enables a single access port to accept untagged data traffic. Users can access tagged voice traffic and associate each type of traffic with distinct and separate VLANs. It gives a higher priority to voice traffic than common user data traffic.

Answer options B, C, and A are incorrect. These statements are not true about voice VLAN.

QUESTION 66
Which of the following is a version of netcat with integrated transport encryption capabilities?

A. Nikto
B. Cryptcat
C. Encat
D. Socat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cryptcat is a version of netcat with integrated transport encryption capabilities. It is a simple Unix utility that reads and writes data across the network while encrypting the data being transmitted. Cryptcat uses both TCP and UDP. Cryptcat is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.

Answer option A is incorrect. Nikto is not a version of Netcat. Nikto is an open-source Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems, it performs generic and server-type specific checks. It also captures and prints any cookies received. It can work in both Linux and Windows environments. Nikto performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs.

Answer option D is incorrect. Socat is a more complex cousin of netcat. It is larger and more flexible and also has more options that must be configured for a given task. Answer option C is incorrect. Encat is not a version of Netcat.

QUESTION 67
Mark wants to compress spreadsheets and PNG image files by using lossless data compression so that he can successfully recover original data whenever required. Which of the following compression techniques will Mark use?

Each correct answer represents a complete solution. Choose two.

A. Vector quantization
B. Deflation
C. Adaptive dictionary algorithm
D. Color reduction

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to accomplish the task, Mark should use the following compression techniques:
· Adaptive dictionary algorithm
· Deflation
· Run-length encoding
· Entropy encoding

These techniques perform lossless data compression.

QUESTION 68
SCADA stands for supervisory control and data acquisition. Which of the following statements are true about SCADA? Each correct answer represents a complete solution. Choose all that apply.

A. SCADA systems also records and logs all events into a file stored on a hard disk.
B. SCADA systems include only software components.
C. SCADA is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions.
D. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Certification Depends on Only One Thing" - www.actualanswers.com 116 CompTIA CAS-001 Exam

SCADA stands for supervisory control and data acquisition. It refers to industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes. It is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control.

SCADA systems include hardware and software components. Hardware gathers and feeds data into a computer system that has SCADA software installed. The computer then processes this data and presents it in a timely manner. This system also records and logs all events into a file stored on a hard disk or sends them to a printer. It warns when conditions become hazardous by sounding alarms.

QUESTION 69
Cloud computing is best described as which of the following?

A. Distributed load balanced servers
B. Delivering software as a service
C. Large scale distributed computing
D. Distributed virtualized servers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The main focus of cloud computing is about delivering software as a service or operating systems as a service. They may or may not be on distributed computing systems. Answer option C is incorrect. Large scale distributed computing is called grid computing. Answer option A is incorrect. Load balancing is what edge computing is about. It may be that cloud computing also accomplishes load balancing, but that is not the primary purpose.

Answer option D is incorrect. Cloud computing may be accomplished via virtualization. but it need not be. Virtualized computing is about the way the systemis hosted, not necessarily theservers distribution (as with cloud and grid computing).

QUESTION 70
Juan is responsible for IT security at an insurance firm. He has several severs that are going to be retired. Which of the following is NOT one of the steps in decommissioning equipment?

A. Plan
B. Communicate
C. Review
D. Follow through

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reviews are not part of the decommissioning process. Unlike security breaches, decommissioning is planned, and relatively limited in scope, so after action reviews are unnecessary.

Answer options A. B, and D are incorrect. The three steps of de-commissioning are plan, communicate, and follow through.

QUESTION 71
Denish works as a Security Administrator for a United States defense contractor. He wants to ensure that all systems have appropriate security precautions, based on their total score. Which of the following standards should he refer to?

A. OVAL

B. OWASP
C. CIA
D. DIACAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Defense IA Certification and Accreditation Process (DIACAP) is the process for accrediting defense related information systems.

Answer option B is incorrect. The Open Web Application Security Process (OWASP) is a process for ensuring web applications are written securely.

Answer option A is incorrect. The Open Vulnerability Assessment Language (OVAL) is used to assess vulnerabilities.

Answer option C is incorrect. Confidentiality, Integrity, and Availability (CIA) are the three areas of security that are scored, not a standard.

QUESTION 72
Mark works as a Network Security Administrator for a public school. He has decided that a hot site is appropriate for the schools grade servers, so they can have 1005= uptime, even in the event of a major disaster. Was this appropriate?

A. No, a hot site is usually not required by most organizations.
B. Yes, a hot site is required for the school

C. Yes, a hot site is always a good idea.
D. No, a school needs do not require a hot site.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A hot site provides 100% uptime, but is quite expensive. In the case of a school, short downtime would not be detrimental to the business.

Answer option C is incorrect. Hot sites are only necessarily when 100% uptime must absolutely be achieved, and the excessive cost is justified.

Answer option A is incorrect. Each organization is different. Some will require a hot site, some won't

Answer option B is incorrect. A school does not require a hot site. The cost is excessive and it is not needed for business continuity.

QUESTION 73
Angela is trying to ascertain the types of security hardware and software her client should implement. What should she do before deciding?

A. Assess that businesses specific risks and threats.
B. Assess the technical skill of management.
C. Assess that businesses specific opportunities.
D. Assess the technical skill of that businesses employees.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 122 CompTIA CAS-001 Exam

Explanation:
Security measures must be aligned to business needs, and that can only be done after a businesses, specific threats and risks are analyzed.

Answer option C is incorrect. Opportunities are part of a business analysis, not a security analysis.

Answer options D and B are incorrect. The skill level of the businesses employees is irrelevant to this issue.

QUESTION 74
_____ is the concept that disclosure of the long-term secret keying material that is used to derive an agreed key does not compromise the secrecy of agreed keys that had previously been generated.

A. Authentication protocol
B. Diffie-Hellman
C. Perfect forward secrecy
D. Key exchange protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Perfect forward secrecy means that if an attacker discovers the material used to derive a key, that does not compromise previously generated keys. This is important as it prevents those keys from having to be replaced.

Answer option A is incorrect. An authentication protocol is any protocol used to verify the identity of a user or machine in network communications.

Answer option B is incorrect. Diffie-Hellman is a protocol for exchanging keys over an insecure medium.

Answer option D is incorrect. Key exchange protocols are only concerned with exchanging a symmetric key, not with the situation that might arise should the key derivation process become compromised.

"Certification Depends on Only One Thing" - www.actualanswers.com 123 CompTIA CAS-001 Exam

QUESTION 75
Maria is concerned about outside parties attempting to access her companies network via the wireless connection. Where should she place the WAP?

A. Centrally in the building
B. WAPs should be placed at each corner
C. In the server room
D. Inside a secure room

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: The more centrally located the WAP is the less of its range can extend beyond the building, making it more difficult for intruders to attempt to access the wireless network.

Answer option C is incorrect. The server room is not a good place for WAP. It will probably be less accessible to users, and if the server room is near the perimeter of the building, will not address the problem described.

Answer option B is incorrect. Placing a WAP near a building corner will guarantee that a lot of its coverage area extends beyond the building making it easier for attackers to access the wireless network.

Answer option D is incorrect. The locating of the WAP inside a room, of any kind, is irrelevant to this question.

QUESTION 76
Fred is a network administrator for an insurance company. Lately there has been an issue with the antivirus software not updating. What is the first thing Fred should do to solve the problem?

"Certification Depends on Only One Thing" - www.actualanswers.com 125 CompTIA CAS-001 Exam

A. Devise a plan to solve the problem
B. Clearly define the problem
C. Try reasonable alternatives
D. Consider probable causes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The first step in problem solving is always to clearly define the problem. You have to fist be able to clearly define the problem before any other problem solving steps can be taken.

Answer option C is incorrect. You cannot try reasonable alternatives until you define the problem.

Answer option D is incorrect. Considering probable causes is an excellent idea, once you have defined the problem.

Answer option A is incorrect. You must first define the problem, then devise a plan before you have any chance of solving the problem.

QUESTION 77
Which of the following governing factors should be considered to derive an overall likelihood rating that is used to specify the probability that a potential vulnerability may be exercised within the construct of the associated threat environment?

Each correct answer represents a complete solution. Choose three.

A. Threat-source motivation and capability
B. Detect a problem and determine its cause
C. Nature of the vulnerability
D. Existence and effectiveness of current controls

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To derive an overall likelihood rating that is used to specify the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors should be considered:
· Threat-source motivation and capability
· Nature of the vulnerability
· Existence and effectiveness of current controls

Answer option B is incorrect. It is not a valid option.

QUESTION 78
Continuous Monitoring is the fourth phase of the Security Certification and Accreditation process, which of the following activities can be involved in the Continuous Monitoring process?

Each correct answer represents a complete solution. Choose three.

A. Security control monitoring
B. Status reporting and documentation
C. Configuration Management and Control
D. Network impact analysis
"Certification Depends on Only One Thing" - www.actualanswers.com 127 CompTIA CAS-001 Exam

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Continuous monitoring in any system takes place after initial system security accreditation. It involves tracking changes to the information system that occur during its lifetime, and then determines the impact of those

changes on the system security. Due to the necessary changes in hardware, software, and firmware during the lifetime of an information system, an evaluation ofthe results of these modifications has to be conducted to determine whether corresponding changes necessarily have to be made to security controls, to bring the system to the desired security state.

Continuous Monitoring is the fourth phase of the Security Certification and Accreditation process.

The Continuous Monitoring process involves the following three activities:

1. Configuration Management and Control
2. Security control monitoring and impact analysis of changes to the information system.
3. Status reporting and documentation

1. Configuration management and control: This activity involves the following functions:
o Documentation of information system changes
o Security impact analysis

2. Security control monitoring: This activity involves the following functions:
o Security control selection
o Selected security control assessment

3. Status reporting and documentation: This activity involves the following functions:
o System security plan update
o Plan of action and milestones update
o Status reporting

The objective of these tasks is to observe and evaluate the information system security controls during the system life cycle. These tasks determine whether the changes that have occurred will negatively impact the system security.

Answer option D is incorrect. It is not a valid activity.

QUESTION 79
You are completing the requirements for vendor selection and need to create a procurement form that will ask the vendor to provide only a price for commercial-off-the-shelf solution. What type of procurement form will you need to provide to the vendor?

A. Purchase order
B. Request for proposal
C. Request for information
D. Request for quote

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A request for quote (RFQJ is a procurement document that you, the buyer in this instance, will provide to the vendor. The RFQ asks the vendor to provide just a price for the identified work, product, or service.

Answer option B is incorrect. Request for proposal is a type of procurement document used to request proposals from prospective sellers of products or services. It invites the vendors to create a proposal, which can include ideas, suggestions, and more for the project. In some application

areas, it may have a narrower or more specific meaning.

Answer option C is incorrect. A request for information is a query from the buyer to the seller asking for additional information such as brochures, references, samples of their work, or whitepapers. It's not a promise or intent to purchase from the vendor, but it asks the vendor to provide more information about their business.

Answer option A is incorrect. A purchase is a pre-determined agreement on price where you may ask the vendor to provide the goods or service.

QUESTION 80
Mark, a malicious hacker, submits Cross-Site Scripting (XSS) exploit code to the Website of the Internet forum for online discussion. When a user visits the infected Web page, the code gets automatically executed and Mark can easily perform acts such as account hijacking, history theft, etc. Which of the following types of cross-site scripting attacks does Mark intend to perform?

A. Non-persistent
B. Persistent
C. Document Object Model (DOMJ
D. SAX

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mark intends to perform a persistent type of cross-site scripting attack. A persistent type of Cross- Site Scripting (XSS) exists when data provided to a Web application by a user is first stored persistently on the server (in a database, or other location), and later displayed to users in a Web page without being encoded using HTML entities. An example of this is online message boards or Internet forums where users are allowed to post HTML-formatted messages for other users to read.

Answer option A is incorrect. A non-persistent type of Cross-Site Scripting (XSS) occurs when data provided by a Web client is used immediately by server-side scripts to generate a page of results for that user. If invalidated user-supplied data are included in the resulting page without HTML encoding, this will allow client-side code to be injected into the dynamic page. One of the most common examples of this is a search engine.

Answer option C is incorrect. With a DOM-based cross-site scripting attack, the problem exists within the pages of a client-side script, if a piece of JavaScript accesses a URL request parameter

and uses this information to write some HTML to its own page. However, this information is not encoded using HTML entities; a Cross-Site Scripting (XSS) hole will likely be present. This written data will be re-interpreted by browsers as HTML, which could include additional client-side scripts.

Answer option D is incorrect. SAX is not a type of cross-site scripting attack. SAX is a parsing mechanism for XML.

QUESTION 81
Mark works as a Network Security Administrator for uCertify Inc. Mark has been assigned to a task to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Mark successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. Security was not compromised as the webpage was hosted internally.
B. The attack was social engineering and the firewall did not detect it.
C. The attack was Cross Site Scripting and the firewall blocked it.

D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to the scenario, the attack was social engineering and the firewall did not detect it.

QUESTION 82
Which of the following counters measures the rate at which the bytes are sent through or received by a network?

A. Network Interface: Bytes Received/sec
B. Network Interface: Output Queue Length
C. Network Interface: Bytes Sent/sec
D. Network Interface: Bytes/sec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The values of Network Interface counters measure the number of bytes sent or received over a TCP/IP connection. No pre-defined values have been set for these counters. A sudden increase in the network traffic indicates an external attack. The counters used to measure the network traffic are as follows:
Network Interface: Bytes Received/sec: This counter shows the rate at which bytes are received by a network. A sudden and unexpected increase in the value of this counter indicates an external attack on the network.
Network Interface: Bytes Sent/sec: This counter shows the rate at which the bytes are sent through the network. A sudden increase in the value of this counter indicates that a large volume of data is being accessed. It also indicates an external attack on the network. Network Interface: Bytes/sec: This counter measures the rate at which the bytes are sent through or received by a network. A sudden increase in the value of this counter indicates an external attack on the network.
Network Interface: Output Queue Length: This counter is maintained by TCP/IP. It is used to measure the number of output packets in a queue. An increase in the value of this counter indicates that the server is experiencing periods of unresponsiveness. Its value can also increase if the server contains faulty network hardware.

QUESTION 83
Which of the following statements are true about Mean Time to Repair (MTTR)? Each correct answer represents a complete solution. Choose three.

A. It is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.
B. It is the average time taken to repair a Configuration Item or IT Service after a failure.
C. It represents the average time required to repair a failed component or device.
D. It includes lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Mean Time to Repair (MTTR) is the average time taken to repair a Configuration Item or IT Service after a failure. It represents the average time required to repair a failed component or device. Expressed mathematically, it is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time. It generally does not include lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).

MTTR is often part of a maintenance contract, where a system whose MTTR is 24 hours is generally more valuable than for one of 7 days if mean time between failures is equal, because its Operational Availability is higher. MTTR is every now and then incorrectly used to mean Mean Time to Restore Service.

QUESTION 84
Which of the following can monitor any application input, output, and/or system service calls made from, to, or by an application?

A. Network-based firewall
B. Dynamic firewall
C. Host-based firewall
D. Application firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A host-based application firewall can monitor any application input, output, and/or system service calls made from, to, or by an application. This is done by examining information passed through system calls instead of. or in addition to, a network stack. A host-based application firewall can only provide protection to the applications running on the same host.

"Certification Depends on Only One Thing" - www.actualanswers.com 137 CompTIA CAS-001 Exam

An example of a host-based application firewall that controls system service calls by an application is AppArmor or the Mac OS X application firewall. Host-based application firewalls may also provide network-based application firewalling.

Answer option A is incorrect. A network-based application layer firewall, also known as a proxy- based or reverse-proxy firewall, is a computer networking firewall that operates at the application layer of a protocol stack. Application firewalls specific to a particular kind of network traffic may be titled with the service name, such as a Web application firewall. They may be implemented through software running on a host or a stand-alone piece of network hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it on to the client or server. Because it acts on the application layer, it may inspect the contents ofthe traffic, blocking specified content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software.

Answer option D is incorrect. An application firewall is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. The application firewall is typically built to monitor one or more specific applications or services (such as a web or database service), unlike a stateful network firewall, which can provide some access controls for nearly any kind of network traffic. There are two primary categories of application firewalls:
· Network-based application firewalls
· Host-based application firewalls

Answer option B is incorrect. A dynamic packet-filtering firewall is a fourth generation firewall technology. It is also known as a stateful firewall. The dynamic packet-filtering firewall tracks the state of active connections, and then determines which network packets are allowed to enter through the firewall. It records session information, such as IP addresses and port numbers to implement a more secure network. The dynamic

packet-filtering firewall operates at Layer3, Layer4, and Layers.

QUESTION 85
Which of the following security principles would be most helpful in preventing privilege escalation?

A. Single point of failure
B. Least privileges
C. Implicit deny
D. Job rotation
"Certification Depends on Only One Thing" - www.actualanswers.com 138 CompTIA CAS-001 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By assigning the least privileges needed for each user, the odds of privilege escalation are reduced. The principle of least privilege gives a user only those privileges that are essential to do his/her work. In information security, computer science, and other fields, the principle of least privilege is also known as the principle of minimal privilege or least privilege. It defines that in a particular abstraction layer of a computing environment, every module must be able to access only the information and resources that are essential for its legitimate purpose, it requires that each subject in a system be granted the most restrictive set of privileges required for authorized tasks.

Answer option D is incorrect. Job rotation, while a good security concept, will have no effect on privilege escalation.

Answer option C is incorrect. Implicitly denying any user any access until authorized, won't affect privilege escalation.

Answer option A is incorrect. A single point of failure is actually a negative, and does not improve security.

QUESTION 86
What security objectives does cryptography meet:

Each correct answer represents a complete solution. Choose all that apply.

A. Authentication
B. Confidentiality
C. Data integrity
D. Authorization

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cryptography is used to meet the following security objectives:

Confidentiality is used to restrict access to the sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals/processes.

Data integrity is used to address the unauthorized/accidental modification of data. This includes data insertion, deletion, and modification. In order to ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Authentication is used to establish the validity of a transmission, message, or an originator. It also

verifies an individual's authorization to receive specific categories of information, but it is not specific to cryptography. Therefore, authentication applies to both individuals and the information itself. The goal is for the receiver of the data to determine its origin.

Non-repudiation is used to prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

QUESTION 87
Which of the following is a deterministic algorithm to generate a sequence of numbers with little or no discernible pattern in the numbers, apart from broad statistical properties?

A. Java Cryptographic Extension
B. Simple and Protected GSSAPI Negotiation Mechanism
C. Pseudorandom number generator
D. Twofish

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Pseudorandom number generator is a deterministic algorithm to generate a sequence of numbers with little or no discernible pattern in the numbers, apart from broad statistical properties. A pseudorandom number generator (PRNG) also called a deterministic random bit generator (DRBG). It is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values called the PRNG s state, which contains a truly random seed. Even though, sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom numbers are important in practice for their speed in number generation and their reproducibility, and they are thus vital in applications such as simulations, in cryptography, and in procedural generation.

Good statistical properties are a vital requirement for the output of a PRNG and common classes of suitable algorithms include linear congruential generators, lagged Fibonacci generators, and linear feedback shift registers.

Cryptographic applications require the output to be unpredictable and more intricate designs are required. More recent examples of PRNGs with strong randomness guarantees are based on computational hardness assumptions, and comprise the Blum Blum Shub, Fortuna. and Mersenne Twister algorithms.

Answer option E is incorrect. The Simple and Protected GSSAPINegotiation Mechanism (SPNEGO) is a GSSAPI"pseudo mechanism' that is used to negotiate one of a number of possible real mechanisms. It is often pronounced as "spengo".
It is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports.

The pseudo-mechanism uses a protocol to determine what common GSSAPImechanisms are available, selects one and then dispatches all further security operations to it. This can help organizations to deploy new security mechanisms in a phased manner.

Answer option D is incorrect. Twofish is a symmetric key block cipher. It operates on 128-bits block size and uses key sizes up to 256 bits. It uses pre-computed key-dependent S-boxes and a relatively complex key

schedule. One half of an n-bit key is used as the actual encryption key,and the other half of the key is used to modify the encryption algorithm. It borrows some elements from the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers.

Answer option A is incorrect. JCE (Java Cryptographic Extension) is used to provide a framework and implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. It was developed as an extension package to include APIs and implementations for cryptographic services that were subject to U.S. export control regulations.

QUESTION 88
You are working in an organization, which has a TCP/IP based network. Each employee reports you whenever he finds a problem in the network and asks you to debug the problem, what is your designation in the organization?

A. Database administrator
B. Stakeholder
C. Network administrator
D. Facility manager

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You are working as a network administrator in the organization and responsible for the operation and configuration of the network. You have to resolve the problems related with the network whenever any employee reports you.

QUESTION 89
Which of the following statements best describe delegation in a network? Each correct answer represents a complete solution. Choose two.

A. It improves security by limiting broadcasts to the local network.
B. It is an act or profession of splitting a computer network into subnetworks.
C. Its usability depends on used authentication method and appropriate account configuration.
D. It allows a user to use an impersonation token to access network resources.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Delegation is the assignment of authority and responsibility to another person to carry out specific activities. It allows a user to use an impersonation token to access network resources.

The ability to use delegation depends on used authentication method and appropriate account configuration. User should be careful while using impersonation and delegation because of the additional security and scalability issues caused by it. There are two types of delegation in a network:
· Delegation at Authentication/Identity Level
· Delegation at Authorization/Access Control Level

Answer options B and A are incorrect. Network segmentation in computer networking is the act or profession of splitting a computer network into subnetworks, each being a network segment or network layer. The advantages of such splitting are primarily for boosting performance and improving security.
Advantages:
Reduced congestion: improved performance is achieved because on a segmented network, there are fewer

hosts per subnetwork, thus minimizing local traffic.

Improved security: Broadcasts will be contained to the local network. Internal network structure will not be visible from outside.

Containing network problems: It limits the effect of local failures on other parts of the network.

"Certification Depends on Only One Thing" - www.actualanswers.com 149 CompTIA CAS-001 Exam

QUESTION 90
In which of the following phases of the System Development Life Cycle (SDLC) is the IT system designed, purchased, and programmed?

A. Operation/Maintenance
"Certification Depends on Only One Thing" - www.actualanswers.com 153 CompTIA CAS-001 Exam
B. Development/Acquisition
C. Disposal
D. Initiation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Answer optionBis correct.

There are five phases in the SDLC, The characteristics of each of these phases are enumerated below:

Phase 1: Phase 1 of the SDLC is known as initiation. In this phase, the need for an IT system is expressed and the purpose and scope of the IT system is documented.

Phase 2: Phase 2 of the SDLC is known as development or acquisition. In this phase, the IT system is designed, purchased, and programmed.

Phase 3: Phase 3 of the SDLC is known as implementation. This phase involves the system security features. The system security features should be configured, enabled, tested, and verified.

Phase 4: Phase 4 of the SDLC is known as operation or maintenance. This phase describes that the system should be modified on a regular basis through the addition of hardware and software.

Phase 5: Phase 5 of the SDLC is known as disposal. This phase involves disposition of information, hardware, and software.