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

Examsoon

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.

"Certification Depends on Only One Thing" - www.actualanswers.com 2 CompTIA CAS-001 Exam

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 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 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.

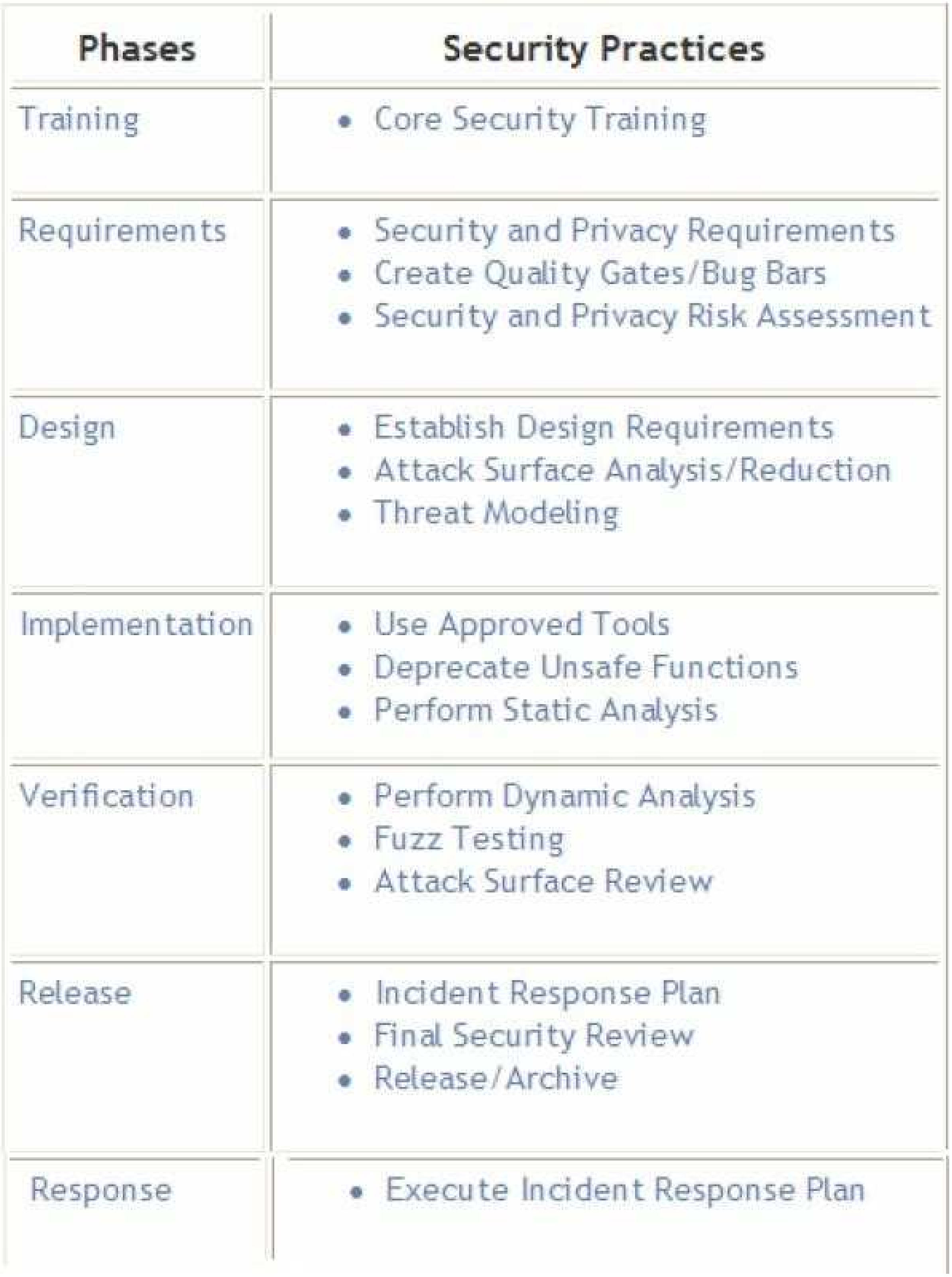
Answer option A is incorrect. Security Assertion Markup Language (SAMLJ is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION 4
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 5

In which of the following activities an organization identifies and prioritizes technical, organizational, procedural, administrative, and physical security weaknesses?

A. Social engineering

B. Vulnerability assessment

C. White box testing

D. Penetration testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed for include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.
Vulnerability is the most reliable weakness that any programming code faces.These programming codesmay be buffer overflow, xss, sql injection, etc. A piece of malware code that takes advantage of a newly announced vulnerability in a software application, usually the operating system or a Web server, is known as an exploit.
Answer option C is incorrect. White box is one of the three levels of penetration testing performed for an organization or network. This final level simulates an attacker with extensive knowledge of the organization and its infrastructure and security controls. The knowledge would come either from independent research and information gathering or from a trusted inside source with full knowledge of the network and its defenses.

Answer option A is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name. IP address, employee ID, or other information that can be misused.

Answer option D is incorrect. A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit.

QUESTION 6
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 7
Which of the following are the functions of a network security administrator? Each correct answer represents a complete solution. Choose three.

A. Backing up the files
B. Writing computer software
C. Maintaining and implementing a firewall
D. Developing, maintaining, and implementing IT security

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A network security administrator is a person who is responsible for providing security of any network. A network security administrator concentrates on network design and security. Following are the functions of a network administrator:
· Developing, maintaining, and implementing IT security · Maintaining and implementing a firewall
· Monitoring and securing the network and server
· Monitoring critical system files

QUESTION 8
"Certification Depends on Only One Thing" - www.actualanswers.com 19 CompTIA CAS-001 Exam
Which of the following arise every time an application takes a user-supplied data and sends it to a Web browser without first confirming or encoding the content?

A. Injection flaws
B. Cookies
C. One-click attacks
D. XSS flaws

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cross Site Scripting vulnerabilities or XSS flaws arise every time an application takes a user- supplied data and

sends it to a Web browser without first confirming or encoding the content. A number of times attackers find these flaws in Web applications. XSS flaws allow an attacker to execute a script in the victim's browser, allowing him to take control of user sessions, disfigure Web sites, and possibly launch worms, viruses, malware, etc. to steal and access critical data from the user's database.

Answer option A is incorrect. Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of web applications. It is the most common technique of attacking a database. Injection occurs when user- supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

Answer option B is incorrect. Cookies are small collections of data stored on a client computer by a web server. By themselves, cookies are not a source of insecurity, but the way they are used can be. Programmers can foolishly store passwords or secret information in a cookie. A browser flaw could permit a site to read another site's cookies. Cookies containing session information could be stolen from a client computer and used by a hacker to hijack the user's logon session. Cookies are used to track a user's activities, and thus can leave a trail of sites users have visited. Users should block third-party cookies. Users should also use a secure browser and apply patches and updates as they become available.

Answer option C is incorrect. Cross-site request forgery, also known as one-click attack or session riding, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. The attack works by including a link or script in a page that accesses a site to which the user is known to have authenticated.

QUESTION 9
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 10
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 11
Which of the following statements are true about Continuous Monitoring? Each correct answer represents a complete solution. Choose all that apply.

A. 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.

B. Continuous monitoring process is used extensively in the U.S. Federal Government.

C. Continuous monitoring in any system takes place after initial system security accreditation.

D. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation.

Correct Answer: AC
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 of the 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.

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 C&A process is used extensively in the U.S. Federal Government.

QUESTION 12
New technologies can pose unique and new risks that must be managed. Which of the following new technologies poses the most risk due to regulatory compliance?

A. Tablets

B. Smart phones

C. Cloud computing

D. Virtualization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since cloud servers might be distributed anywhere in the world, the issue of complying with national regulations is a tricky one.
Answer option B is incorrect. While smart phones do pose risks, those risks are not due to regulatory issues.
Answer option D is incorrect. Virtualization, like smartphones, does pose its own security risks, but those risks are not primarily due to regulatory compliance. Answer option A is incorrect. Tablets are not an issue for regulatory compliance. Tablets may have their own security issues, but do not have specific regulatory issues.

QUESTION 13
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 14
Risk analysis provides the higher management the details necessary to determine the risks that should be mitigated, transferred, and accepted. What are the various stages in the risk analysis process?

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

A. Management
B. Threat assessment
C. Evaluation of control
D. Monitoring
E. Asset control
F. Inventory

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:
Answer: A,B,C,D,F
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

QUESTION 15
"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 16
Which of the following federal regulations requires federal agencies to be able to monitor activity in a "meaningful and actionable way"?

A. FISMA
B. HIPAA
C. Sarbanes-Oxley
D. CAN SPAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Federal Information Security Management Act requires continuous monitoring of affected federal systems.

Answer option B is incorrect. The Health Information Portability and Accountability Act Governs the privacy of health records.
Answer option C is incorrect. Sarbanes Oxley addresses the retention of documents and records in publically traded companies.

Answer option D is incorrect. CAN SPAN regulates unsolicited email, commonly called spam.

QUESTION 17
Which of the following is the best description of vulnerability assessment?

A. Determining what threats exist to your network.
B. Determining the impact to your network if a threat is exploited.
C. Determining the weaknesses in your network that would allow a threat to be exploited
D. Determining the likelihood of a given threat being exploited.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Weaknesses in your network due to inherent technology weaknesses, mis-configuration, or lapses in security are vulnerabilities.

Answer option A is incorrect. Determining the threats to your network is threat assessment not vulnerability assessment. In fact this phase is done before vulnerability assessment Answer option D is incorrect. Determining the likelihood of a given attack is likelihood assessment.
This would be done after vulnerability assessment.

Answer option B is incorrect. Impact analysis is certainly important, but this is done after vulnerability assessment.

QUESTION 18

Juan is trying to perform a risk analysis of his network. He has chosen to use OCTAVE. What is OCTAVE primarily used for?

A. A language for vulnerability assessment
B. A comprehensive risk assessment model
C. A threat assessment tool
D. An impact analysis tool

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
OCTAVE, or Operationally Critical, Threat, Asset and Vulnerability Evaluation is a comprehensive risk assessment model. Answer option A is incorrect. OVAL, or Open Vulnerability Assessment Language is the language for vulnerability assessment. Answer options C and D are incorrect. Threat assessment and impact analysis are both part of OVAL, but only a part

QUESTION 19
_____________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.

"Certification Depends on Only One Thing" - www.actualanswers.com 38 CompTIA CAS-001 Exam

QUESTION 20
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 21
Mark works as a Network Security Administrator for uCertify Inc. The organization is using an intranet to distribute information to its employees. A database residing on the network contains employees' information, such as employee name, designation, department, phone extension, date of birth, date of joining, etc. He is concerned about the security because the database has all information about employees, which can help an unauthorized person to recognize an individual.

Which Personally Identifiable Information should be removed from the database so that the unauthorized person cannot identify an individual?

A. Date of birth
B. Employee name
C. Employee code
D. Date of joining

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to the scenario, date of birth is uniquely identified information that can help the unauthorized person to recognize an individual. Therefore, Mark should remove date of birth of all employees from the database.

QUESTION 22
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 23
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 24
Risk assessment helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC. Which of the following steps covered by the risk assessment methodology?

Each correct answer represents a complete solution. Choose three.

A. Vulnerability Identification

B. Cost Analysis

C. Threat Identification

D. System Characterization

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Risk assessment is the first process of risk management. It helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC.

The risk assessment methodology covers nine steps which are as follows:
· Step 1 - System Characterization
· Step 2 - Threat Identification
· Step 3 - Vulnerability Identification
· Step 4 - Control Analysis
· Step 5 - Likelihood Determination
· Step 6 - Impact Analysis

· Step 7 - Risk Determination
· Step 8 - Control Recommendations
· Step 9 - Results Documentation

QUESTION 25
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
"Certification Depends on Only One Thing" - www.actualanswers.com 45 CompTIA CAS-001 Exam
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 26
Which is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality?

A. Agreement
"Certification Depends on Only One Thing" - www.actualanswers.com 47 CompTIA CAS-001 Exam
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 27
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.

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 28
Which of the following statements are true about capability-based security?

A. It is a concept in the design of secure computing systems, one of the existing security models.

B. It is a computer security model based on the Actor model of computation.

C. It is a scheme used by some computers to control access to memory.

D. It is a concept in the design of secure computing systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Capability-based security is a concept in the design of secure computing systems. A capability (known in some systems as a key) is a communicable, unforgivable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure.

Although most operating systems implement a facility which resembles capabilities, they typically do not provide enough support to allow for the exchange of capabilities among possibly mutually untrusting entities to be the primary means of granting and distributing access rights throughout the system. A capability-based system, in contrast, is designed with that goal in mind. Answer options B, C, and A are incorrect. These are not correct statements about capability-based security.

QUESTION 29
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

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 30
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 31
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 32
Allen needs a program that injects automatically semi-random data into a program or stacks and detects bugs. What will he use?

A. Fuzzer
B. Happy path
C. Boundary value analysis
D. Agile testing

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
A fuzzer is a program that is used to inject automatically semi-random data into a program/stack and detect bugs. The programs and frameworks that are used to create fuzz tests or perform fuzz testing are called fuzzers. Fuzzing has evolved from a niche technique into a full testing discipline with support from both the security research and traditional QA testing communities. Fuzzing (Fuzz testing) is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Answer option C is incorrect. Boundary value analysis is a software testing technique in which tests are designed to include representatives of boundary values.

Answer option B is incorrect. A happy path is a default scenario that features no exception or error conditions, and contains the sequence of activities that will be executed if everything goes as anticipated.

Answer option D is incorrect. Agile testing is a software testing practice. It follows the principles of agile software development. This testing does not accentuate the testing procedures and focuses on ongoing testing against the newly developed code until quality software from an end customer's perspective results. It is built upon the philosophy that testers need to adapt to the rapid deployment cycles and changes in the testing patterns.

QUESTION 33
Which of the following is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously?

A. Electronic mail
B. Instant messaging
C. Video conferencing
D. Audio conferencing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Video conferencing is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously. Video conferencing differs from videophone calls in that it's designed to serve a conference rather than individuals.

It uses telecommunications of audio and video to bring people at different sites together for a meeting. This can be as simple as a conversation between two people in private offices (point-to- point) or involve several sites (multi-point) with more than one person in large rooms at different sites. Besides the audio and visual transmission of meeting activities, videoconferencing can be used to share documents, computer-displayed information, and whiteboards.

Answer option D is incorrect. Audio conferencing is a method of communication in which the calling party wishes to have more than one called party listens in to the audio portion of the call. The conference calls may be designed to allow the called party to participate during the call, or the call may be set up so that the called party merely listens into the call and cannot speak. It can be designed so that the calling party calls the other participants and adds them to the call. Answer option B is incorrect. Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The users text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.

"Certification Depends on Only One Thing" - www.actualanswers.com 56 CompTIA CAS-001 Exam

IM falls under the umbrella term online chat, as it is a real-time text-based networked communication system, but is distinct in that it is based on clients that facilitate connections between specified known users (often using Buddy List, Friend List or Contact List), whereasonline chat also includes web-based applications that allow communication between users in a multi-user environment.

Answer option A is incorrect. E-mail (electronic mail) is a method of exchanging of computer- stored messages by telecommunication. E-mail messages are usually encoded in ASCII text. However, a user can also send non-text files, such as graphic images and sound files, as attachments sent in binary streams. E-mail was one of the first applications being made available on the Internet and is still the most popular one. A large percentage of the total traffic over the Internet is of the e-mails. E-mails can also be exchanged between online service provider users and in networks other than the Internet, both public and private.

E-mails can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an e-mail reflector. Some mailing lists allow you to subscribe by sending a request to the mailing list administrator. A mailing list that is administered automatically is called a list server.

E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. A popular protocol for sending e-mails is Simple Mail Transfer Protocol and a popular protocol for receiving it is POP3. Both Netscape and Microsoft include an e-mail utility with their Web browsers.

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
"Certification Depends on Only One Thing" - www.actualanswers.com 59 CompTIA CAS-001 Exam
You work as a System Administrator for uCertify Inc. The company has a Windows-based network. A user requests you to provide him instructions regarding the installation of application software's on his computer. You want to show the user how to perform the configuration by taking control of his desktop. Which of the

following tools will you use to accomplish the task?

A. Remote desktop
B. Task Manager
C. Remote Assistance
D. Computer Management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to accomplish the task, you should use the Remote Assistance tool. By using Remote Assistance, you can take shared control of the users desktop, which will allow you to perform the necessary configurations on the shared desktop while the remote user is watching it straight away.

QUESTION 36
Which of the following is a flexible set of design principles used during tine phases of systems development and integration?

A. Service-oriented modeling framework (SOMF)
B. Sherwood Applied Business Security Architecture (SABSA)
C. Service-oriented modeling and architecture (SOMA)
D. Service-oriented architecture (SOA)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications- to be aware of available SOA-based services.

Answer option C is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer option A is incorrect. The service-oriented modeling framework (SOMF) has been proposed by author Michael 8ell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems.

The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme.

Answer option B is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

QUESTION 37

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 38
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.

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 39
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

QUESTION 40
Juan is working as a Security Administrator for a credit card processing company. He is concerned about PCI compliance and so, he uses network segmentation. How does segmentation help Juan?

A. Segmentation would help prevent viruses.
B. Segmentation reduces the scope of machines that need to be PCI compliant.
C. Segmentation is required by PCI regulations.
D. Segmentation would have no effect.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:
By segmenting the network, Juan reduces the number of machines that require PCI compliance, and thus makes PCI administration simpler.
Answer option C is incorrect, PCI regulations does not require network segmentation. Answer option D is incorrect. By reducing the scope of network that requires segmentation, it is easier to maintain compliance. Answer option A is incorrect. Segmentation may slow down the spread of a virus, but the impact of segmentation on viruses is based on what is done in each segment, not the segmentation itself.

QUESTION 41
You work as a Network Administrator for uCertify Inc. The company has a TCP/IP based network. You have segmented the network in multiple sub networks. Which of the following advantages will you get after segmentation?

Each correct answer represents a complete solution. Choose three.

A. Limited network problems
B. Improved security
C. Reduced congestion
D. Reduced performance

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 42
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 43
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

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 44
Which of the following concepts are included in the security of a SAN? Each correct answer represents a complete solution. Choose all that apply.

A. Host adapter-based security
B. Storage-controller mapping
C. Switch zoning
D. IDS implementation

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Storage area network (SAN) is a dedicated network that provides access to a consolidated, block level data storage. The security of SAN is completely dependent upon the users authentication or authorization. SAN security includes the following concepts:
· Host adapter-based security: Security measures for the Fibre Channel host bus adapter can be implemented at the driver level.
· Switch zoning: Switch zoning is used in a switch-based Fibre Channel SAN. It refers to the masking of all nodes connected to the switch.
· Storage-controller mapping: By mapping all host adapters against LUNs in the storage system, some storage sub-systems accomplish LUN masking in their storage.

Answer option D is incorrect, IDS is not implemented for the security of a SAN.

QUESTION 45
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 46
Which of the following features are provided by SAN for SQL servers? Each correct answer represents a complete solution. Choose all that apply.

A. Faster disaster recovery
B. Non-clustered environment
C. Storage efficiencies
D. Increased database size

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Storage area network (SAN) is a dedicated network that provides access to a consolidated, block level data storage.

SAN provides the following features for SQL servers:
· Increased database size
· Clustered environment
· Performance advantages
· Storage efficiencies
· Faster disaster recovery

QUESTION 47
Which of the following statements are true about distributed computing? Each correct answer represents a complete solution. Choose all that apply.

A. In distributed computing, the computers interact with each other in order to achieve a common goal
B. A distributed system consists of multiple autonomous computers that communicate through a computer network.

C. In distributed computing, a problem is divided into many tasks, each of which is solved by a programmer.

D. Distributed computing refers to the use of distributed systems to solve computational problems.
"Certification Depends on Only One Thing" - www.actualanswers.com 74 CompTIA CAS-001 Exam

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Distributed computing is a field of computer science that studies distributed systems. In distributed computing, a problem is divided into many tasks, each of which is solved by one computer. A distributed system consists of multiple autonomous computers that communicate through a computer network. It also refers to the use of distributed systems to solve computational problems. The computers interact with each other in order to achieve a common goal.

QUESTION 48
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 49
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 50
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:

· 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 51
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 52
_________ consists of very large-scale virtualized, distributed computing systems. They cover multiple administrative domains and enable virtual organizations.

A. Edge computing
B. Grid computing
C. Cloud computing
D. Virtualized computing
"Certification Depends on Only One Thing" - www.actualanswers.com 81 CompTIA CAS-001 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Grid computing is a system that is very large scaled, distributed, and virtualized. Answer option C is incorrect. Cloud computing is about delivering software or operating systems as a service, rather than installing them locally.

Answer option A is incorrect. Edge computing is about load balancing servers, literally on the edge of the network.

Answer option D is incorrect. Virtualized computing is about the way the system is hosted, not necessarily the servers distribution {as with cloud and grid computing).

QUESTION 53
What is this formula for SC information system = [(confidentiality, impact), (integrity, impact), (availability, impact)}?

A. Calculate firewall security
B. Calculate SLE
C. Calculate CIA aggregate score
D. Calculate ALE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is the formula for computing the aggregate CIA score.

Answer option D is incorrect. ALE or annualized loss expectancy is computed by multiplying the single loss expectancy by the annual rate of occurrence.

Answer option B is incorrect. SLE or single loss expectancy is the amount of loss expected from a single incident. It is calculated by multiplying the asset value times the exposure factor.

Answer option A is incorrect. There is no formula specific to calculating the security of a firewall.

QUESTION 54
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 55
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.

QUESTION 56
Software and systems as a service in the cloud provide flexibility for administrators. The administrator can create, shutdown, and restart virtual servers as needed. However this flexibility also leads to a problem. Which of the following problems is directly related to that?

A. Fragmented hard drives
B. User authentication
C. VM Sprawl
D. Virus spreading

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
VM sprawl refers to the situation where the multiple virtual machines become difficult to manage, and a consistent security policy is impossible to maintain.

Answer option D is incorrect. Viruses are actually less virulent in a virtualized environment. Answer option A is incorrect. Hard drive fragmentation is no more, or less likely in a virtualized environment.

Answer option B is incorrect. User authentication is no more or less challenging in a virtualized environment.

QUESTION 57
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 58
Which of the following is a security incident in which sensitive or confidential data is copied,

"Certification Depends on Only One Thing" - www.actualanswers.com 88 CompTIA CAS-001 Exam
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 59
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. Data handling
B. Data recovery
C. Data Erasure
D. Data breach

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Data recovery is the process of recovering data from damaged, failed, corrupted, or inaccessible secondary storage device when it cannot be accessed normally. Often the data are being recovered from storage media like internal or external hard disk drives, solid-state drives (SSD).

USB drive, storage tapes, 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 options D, A, and C are incorrect. These are not valid op

QUESTION 60
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:

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 61
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.

QUESTION 62
Which of the following is the predicted elapsed time between inherent failures of a system during operation?

A. Mean time to recovery
B. Mean time to repair
C. Mean time between failures
D. Mean down time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.

QUESTION 63
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)

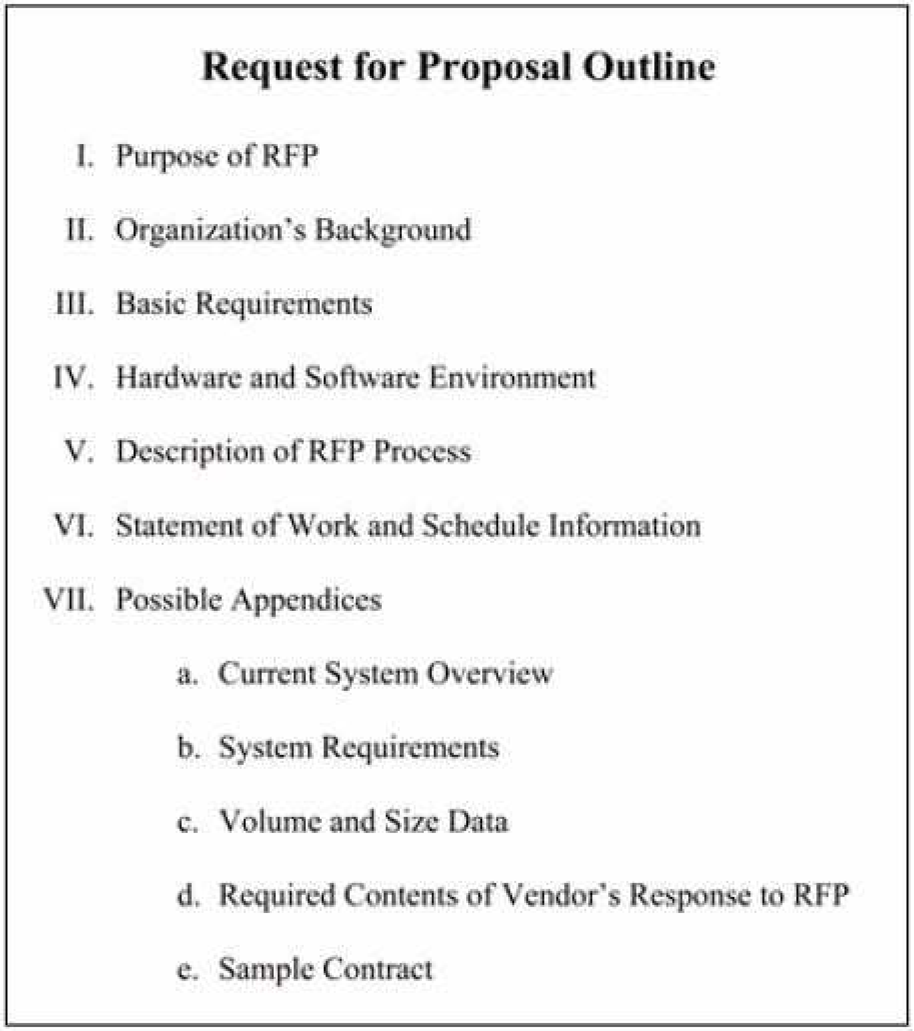
A request for information (RFI) is a document used to solicit information about prospective sellers well before a RFP or RFQ is issued. A buyer uses an RFI in order to survey the landscape of sellers that could potentially bid at a later point in time. An RFI typically precedes an RFP or RFQ by many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

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.



Request for Proposal Outline

I. Purpose of RFP

II. Organization's Background

III. Basic Requirements

IV. Hardware and Software Environment

V. Description of RFP Process

VI. Statement of Work and Schedule Information

VII. Possible Appendices

a. Current System Overview

b. System Requirements

c. Volume and Size Data

d. Required Contents of Vendor's Response to RFP

e. Sample Contract

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 64
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 65
A user can divide network traffic into which of the following classes of service? Each correct answer represents a complete solution. Choose three.

A. Video payload
B. Voice and video payload
C. Voice payload
D. Voice and video signal traffic

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can divide network traffic into the following three classes of service:

· Voice payload: Voice calls are a major part of network traffic, so a network traffic is mainly divided in this class.
· Video payload: Video traffic has variable packet rates and slightly variable bit rates, so this class is used to separate the video traffic.
· Voice and video signal traffic: This traffic is treated as a data application in QoS. In this class, protocols are used to tolerate jitter and delay.

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

QUESTION 66
Which of the following types of redundancy permits software to run simultaneously on multiple geographically distributed locations, with voting on results?

A. Process
B. Application
C. Hardware
D. Data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The various types of redundancy are as follows:
· Hardware redundancy: it includes the installation of multiple processors, mirrored disks, multiple server farms, and RAIDS.
· Process redundancy: It permits software to run simultaneously on multiple geographically distributed locations, with voting on results. It prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data. · Data redundancy: It allows the system to take backup on a permanent media at a regular time interval.
· Application redundancy: It needs at least two machines that can work on the same application. Application redundancy is the best way to make system infrastructure resilient against problems.

QUESTION 67
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 68
Which of the following contains the complete terms and conditions which both the partners agree to be bound by as a participant in the partner program?

A. Business Partner Agreement

B. Document automation

C. Indenture

D. Implicit contract

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business Partner Agreement (BPA) contains the complete terms and conditions which both the partners agree to be bound by as a participant in the partner program. This program comes into action once the application to participate in the Program is accepted by both the partners. Answer option B is incorrect. Document automation is the design of systems and workflow that assist in the creation of electronic documents.

Answer option D is incorrect. Implicit contract refers to voluntary and self-enforcing long term agreements made between two parties regarding the future exchange of goods or services.

Answer option C is incorrect. An indenture is a legal contract reflecting a debt or purchase obligation, specifically referring to two types of practices: in historical usage, an indentured servant status, and in modern usage, an instrument used for commercial debt or real estate transaction.

QUESTION 69
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 70
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 71
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 72
Darryl is an administrator for a visualization company. He is concerned about security vulnerabilities associated with visualization. Which of the following are the most significant issues?

A. Privilege escalation from one VM to another
B. The server drive crashing and bringing down all VMs
"Certification Depends on Only One Thing" - www.actualanswers.com 102 CompTIA CAS-001 Exam
C. Viruses moving from one VM to another
D. Data from one VM being copied to another VM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a virtualized environment, any issues with the underlying drive affect all the VMs hosted on that drive.

Answer option C is incorrect. Viruses cannot move from one VM to another. This is one strength of a VM.

Answer option A is incorrect. Each VM behaves like a separate server. Privilege escalation between VMs is impossible.

Answer option D is incorrect. Data cannot be inadvertently copied from one VM to another with a properly configured VM.

QUESTION 73
John is a security administrator for a large retail company. He wishes to address new threats, what is the most important step for him to take in addressing new threats?

"Certification Depends on Only One Thing" - www.actualanswers.com 103 CompTIA CAS-001 Exam

A. Performing a proper risk assessment
B. Performing a vulnerability assessment
C. Ensuring the firewall is properly configured
D. Creating security policies for the new threat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A risk assessment is the most important first step. Without a proper risk assessment, it is impossible to properly perform any other security steps.

QUESTION 74
What routine security measure is most effective in protecting against emerging threats?

A. System patches

B. Properly configuring the firewall

C. Updating the disaster recovery plan

D. Vulnerability assessments

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Many new threats depend on exploiting system flaws. By routinely patching your system, you will achieve a significant level of protection against emerging threats.

Answer option C is incorrect. Updating a disaster recovery plan will not be effective against emerging threats.

Answer option B is incorrect. Obviously the firewall should be properly configured, but that is less effective against emerging threats.

Answer option D is incorrect. A vulnerability assessment is usually only useful against known threats, not emerging threats.

QUESTION 75
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 76
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 77
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 78
Which of the following statements are true about a smartphone? Each correct answer represents a complete solution. Choose two.

A. It allows the user to install and run more advanced applications based on a specific platform.
B. It can be simple software-based Softphones or purpose-built hardware devices that appear much like an ordinary telephone or a cordless phone.
C. It allows telephone calls to be made over an IP network.
D. It is a mobile phone with advanced PC like capabilities.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. A smartphone is a mobile phone with advanced PC like capabilities. Blackberry and iPhone are the two most popular brands of smartphones. It allows the user to install and run more advanced applications based on a specific platform.

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

Answer options C and B are incorrect. An IP phone uses Voice over IP technologies, allowing telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system. Calls can traverse the Internet, or a private IP Network such as that of a company. The phones use control protocols such as Session Initiation Protocol, Skinny Client Control Protocol, or one of the various proprietary protocols such as Skype. IP phones can be simple software-based Softphones or purpose-built hardware devices that appear much like an ordinary telephone or a cordless phone. Ordinary PSTN phones are used as IP phones with analog telephony adapters (ATA). Following is an image of an IP phone:

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

QUESTION 79
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 80
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 81
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 112 CompTIA CAS-001 Exam

QUESTION 82
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:

"Certification Depends on Only One Thing" - www.actualanswers.com 113 CompTIA CAS-001 Exam

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 83
Which of the following are the advantages of the Virtual Desktop Infrastructure (VDI)? Each correct answer represents a complete solution. Choose three.

A. Cost Efficiency
B. Green Solution
C. Improved Manageability
D. Server-Hosted

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Virtual Desktop Infrastructure (VOI) is used to virtualize the desktop environment delivering enterprise-class control, and to increase the manageability. It maintains the familiar end-user environment. It virtualizes the desktop images that are deployed from a centralized hosting server. It provides the end user with a virtual PC that works same as their current PC. It is used to consolidate the number of servers that support desktops. It has the following advantages:
1.Green Solution
2.Cost Efficiency
3.Improved Manageability
4.Central management of files and user's profile.

QUESTION 84
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 85
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 86
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:

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 87
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 88
ESA stands for Enterprise Security Architecture. What is the purpose of ESA?

A. To provide a framework for securing web applications.
B. To provide a framework for evaluating vulnerabilities.
C. To apply financial security concepts to network security.
D. To apply network architecture paradigms to network security.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enterprise Security Architecture is about applying network architecture principles to network security.

Answer option B is incorrect. Open Vulnerability and Assessment Language is a standard to assess vulnerabilities in a system.

Answer option A is incorrect. The Open Web Application Security Project is a set of standards for security web applications.

Answer option C is incorrect. There is not a model for applying financial security paradigms to network security.

"Certification Depends on Only One Thing" - www.actualanswers.com 118 CompTIA CAS-001 Exam

QUESTION 89
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 90
Mark is responsible for secure programming at his company. He wants to implement steps to validate the security of software design. At what phase in the SDLC should he implement design validation for security?

A. After the design phase

B. This is not a part of SDLC

C. During the testing phase

D. At every phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Every phase of the SDLC could potentially change the design, even slightly. Therefore the security of the design must be validated.

Answer option A is incorrect. Yes you would validate the design after the design phase, but this is not the only time you would validate it.

Answer option C is incorrect. Validation would occur during testing, but also during other phases.

Answer option B is incorrect. Design validation should be a part of every phase of the SDLC.

QUESTION 91
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 92
Minimum security controls can only be determined after___________.

A. A penetration test.
B. The aggregate CIA score has been computed.
C. System securitypoliciesare put in place.
D. A vulnerability assessment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You must compute the CIA (Confidentiality. Integrity, and Availability) requirements of the system before you can determine the required minimum controls.

Answer option D is incorrect. A vulnerability assessment is a good practice, but is not necessary to determine minimal security controls.

Answer option A is incorrect. A penetration test is a good practice, but is not necessary to determine minimal security controls.

Answer option C is incorrect. The system securitypoliciesshould be developed after the CIA score has been computed.

"Certification Depends on Only One Thing" - www.actualanswers.com 121 CompTIA CAS-001 Exam

QUESTION 93
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 94
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 95
PFS depends on which type of following encryption?

A. Symmetric
B. Classic
C. Secret
D. Asymmetric

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Perfect Forward Secrecy depends on asymmetric or public key cryptography and cannot be achieved with symmetric cryptography.

Answer option A is incorrect. Perfect Forward Secrecy cannot be accomplished via symmetric cryptography

Answer option C is incorrect. Remember that the security of any algorithm is not dependent on it being secret, merely upon the key being kept secret.

Answer option B is incorrect. Classic cryptography (such as the Caesar cipher, Vigenere cipher, etc.) is no longer used for secure communications.

QUESTION 96
John is setting up a public web server. He has decided to place it in the DMZ. Which firewall should have the tightest restrictions?

A. On the web server itself
B. Inner end of the DMZ
C. Outer end of the DMZ
D. The restrictions should be consistent

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The inner firewall is the one that protects the actual network from the outside world. Also it is usually necessary to allow far more users to connect to the web server than you allow into your actual network.

Answer option C is incorrect. The outer end of the DMZ must have less restrictions in order to

"Certification Depends on Only One Thing" - www.actualanswers.com 124 CompTIA CAS-001 Exam

allow a variety of outside users to connect to the web server.

Answer option A is incorrect. If you have a firewall on the web server itself, it should be consistent with the outer end of the DMZ.

Answer option D is incorrect. The inner end of the DMZ should be the most secure.

QUESTION 97
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 98
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?

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 99
As a network administrator, if you are experiencing intermittent security issues what is the first thing you should do?

A. Try obvious fixes
B. Define a solution
C. Isolate the problem
D. Consider alternative solutions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Intermittent problems require isolation before any solution can be found. It is important to limit possible causes. This is done by isolating the network segment. By slowly removing each possible culprit you eventually will have isolated the actual problem.

Answer option B is incorrect. You cannot define a solution if you have not isolated the problem. Answer option A is incorrect. Once you have isolated the problem, you can then attempt obvious fixes.

Answer option D is incorrect. Alternative solutions should be considered after you have isolated the problem and tried obvious fixes.

QUESTION 100
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 101
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

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 102
Which of the following types of scalability is for distributed systems to expand and contract its

resource pool to hold heavier loads?

A. Functional
B. Load
C. Administrative
D. Geographic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Scalability is the ability of a system, network, or process, which handles growing amount of work in a capable regular method or its ability to be enlarged to hold that growth. Scalability can be deliberated in various dimensions/ways:
· Administrative scalability: This type of scalability is used for increasing the number of organizations to share and enlarge a single distributed system. · Functional scalability: This type of scalability is used to improve the system by inserting new functionality at least effort.
· Geographic scalability: This type of scalability is used to maintain the performance, usability. · Load scalability: This type of scalability is for distributed systems to expand and contract its resource pool to hold heavier loads.

QUESTION 103
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 104

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 105

Which of the following Web sites provides a virtual community where people with a shared interest can communicate and also can post their thoughts, ideas, and anything else and share it with their friends?

A. E-commerce site

B. Blog

C. Social networking site

D. Internet forum

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation: Answer option C is correct.
Social networking web sites provide a virtual community in which people with a shared interest may communicate. These sites provide users the ability to create their profile page. The users can post their thoughts, ideas, and anything else and can share it with their friends. Some popular social networking sites are MySpace, Twitter, and Facebook.

Answer option A is incorrect. Electronic commerce, commonly known as e-commerce or eCommerce, or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. E-commerce sites can be used by users to browse various products and to make purchases. Amazon.com is an example of an e-commerce site.

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

QUESTION 106
Which of the following is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to?

A. NDA
B. SLA
C. OLA
D. SA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A non-discloser agreement is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to.

QUESTION 107
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

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 108
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 109
Which of the following department in an organization is responsible for documenting and the controlling the incoming and outgoing cash flows as well as the actual handling of the cash flows?

A. Human Resource
B. Financial
C. Stakeholder
D. Management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Roles and responsibilities of the finance department are important for the smooth operation of the business. The most common function of this department is the documentation and controlling of incoming and outgoing cash flows as well as the actual handling of the cash flows. The responsibilities of the finance department are as follows:
· Budget management

· Grants management
· Salary administration
· Property management
· Purchasing
· Handling cash

Answer option D is incorrect. It is the responsibility of management to ensure that employees are provided for in terms of finances, health care, and other related economic issues as well as making certain that more ethereal social issues, such as community viability and emotional stability are positive.

Answer option A is incorrect. The responsibilities of HR (Human Resource) depend on the size of the organization. HR directors and HR managers head up several different departments thatare led by functional or specialized HR staff, such as the training manager, the compensation manager, or the recruiting manager.

Answer option C is incorrect. Stakeholder has direct or indirect stake in an organization. Key stakeholders in a business organization include creditors, customers, directors, employees, government, owners, suppliers, unions, and the community from which the business draws its resources.

QUESTION 110
You are responsible for evaluating, recommending, and directing changes to the Corporate Security Manager in order to ensure the security of assets, facilities, and employees of the organization. What is your designation?

A. Facility manager
B. HR manager
C. Physical security manager
D. Network administrator

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A physical security manager is responsible for evaluating, recommending, and directing changes to the Corporate Security Manager in order to ensure the security of assets, facilities, and employees of the organization. He should have a strong knowledge of security principles and security elements.

The duties and responsibilities of a physical security manager are as follows:
· Coordinate all physical security issues throughout the organization. · Develop and implement policies, standards, guidelines and procedures related to physical security operations.
· Manage physical security and BSOC supervisors.
· Responsible for design of Security features.
· Responsible for development of written physical security plans for critical infrastructures. · Manage the purchasing, installation, upgrading and maintenance of all existing physical security equipments.

Answer option A is incorrect. A network administrator is responsible for the maintenance of computer hardware and software that comprises a computer network. He normally deploys, configures, maintains, and monitors active network equipment.

Answer option B is incorrect. An HR manager heads up several different departments that are led by functional or specialized HR staffs.

Answer option D is incorrect. A facility manager is responsible for best utilization of company resources and in making of a strategy for maximum allocation of space used in new contract.

QUESTION 111
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 112
In which of the following phases of the system development life cycle (SDLC) is the primary implementation of the configuration management process performed?

A. Implementation
B. Operation/maintenance
C. Initiation
D. Acquisition/development

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 146 CompTIA CAS-001 Exam

Explanation:
The primary implementation of the configuration management process is performed during the operation/ maintenance phase of the SDLC. The operation/maintenance phase describes that the system should be modified on a regular basis through the addition of hardware and software. Answer options C, D, and A are incorrect. The other phases are too early for this process to take place.

QUESTION 113
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 114
Which of the following terms suggests that the supplier of an application program or system provides all the hardware and software components and resources to meet the customers requirement and no other supplier is required to be involved?

A. End-to-end solution
B. COTS product
C. Change Management
D. Collaboration platform
"Certification Depends on Only One Thing" - www.actualanswers.com 152 CompTIA CAS-001 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An end-to-end solution (E2ES) suggests that the supplier of an application program or system provides all the hardware and software components and resources to meet the customer's requirement and no other supplier is required to be involved.

Answer option B is incorrect. COTS stands for Commercial Off-The-Shelf products. These products save time and efforts of creating own programs and services by purchasing these products from a third-party vendor. COTS products speed up and reduce the cost of system construction.

Answer option D is incorrect. Collaboration platform is an unified electronic platform that supports both synchronous and asynchronous communication using a variety of devices and channels. It offers a set of software components and services. These components and services enable users to communicate- share information, and work together for achieving common business goals.

A collaboration platform consists of the following core elements:
· Messaging (email, calendaring and scheduling, contacts). · Team collaboration (file synchronization, ideas and notes in awiki, task management, full-text search)
· Real-time communication (presence, instant messaging. Web conferencing, application/desktop sharing, voice, audio and video conferencing)

Answer option C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure.

The main aims of Change Management are as follows:
· Minimal disruption of services
· Reduction in back-out activities
· Economic utilization of resources involved in the change

QUESTION 115
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.

QUESTION 116
Which of the following protocols will you use to query and modify information stored within directory services?

A. TFTP
B. LDAP

C. SSL
D. TLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services. The Lightweight Directory Access Protocol (LDAP) is a standard protocol, which provides access to the directory. It also provides a common language for LDAP clients and servers to communicate with each other. The LDAP is commonly used as standard in the industry. By using a directory service such as LDAP, information existing in multiple systems and formats can be brought at one place.
Answer options C and D are incorrect. The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to provide transport level security for Web services applications.

Answer option A is incorrect. Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). TFTP can be implemented in a very small amount of memory. It is useful for booting computers such as routers which did not have any data storage devices. It is used to transfer small amounts of databetween hosts on a network, such as IP phone firmware or operating system images when a remote X Window System terminal or any other thin client boots from a network host or server.

The initial stages of some network based installation systems (such as Solaris Jumpstart, Red Hat Kickstart and Windows NTs Remote Installation Services) use TFTP to load a basic kernel that performs the actual installation. TFTP uses UDP port 69 for communication.

QUESTION 117
Security Information and Event Management (SIEM) solution provides real-time analysis of security alerts generated by network hardware and applications, which of the following capabilities does this solution have?

Each correct answer represents a complete solution. Choose three.

A. Retention
B. Dashboard
C. Data aggregation
D. Remanence
E. Data redundancy

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Security Information and Event Management (SIEM) solution is a combination of the formerly different product categories of SIM (security information management) and SEM (security event management). It provides real-time analysis of security alerts generated by network hardware and applications. SIEM solution is also used to log security data and generate reports for compliance purposes.

The SIEM capabilities are as follows:

· Data aggregation
· Correlation
· Alerting

- Dashboard
- Compliance
- Retention