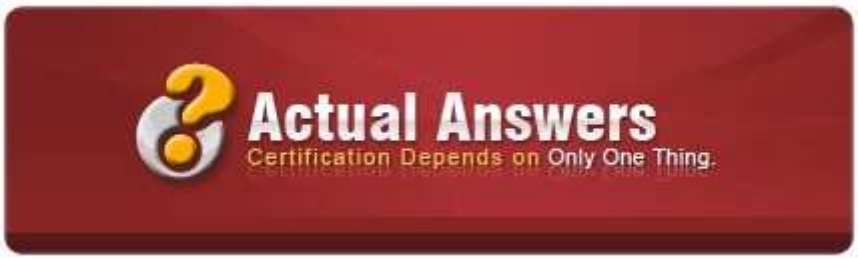
CAS-001_formatted

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

CompTIA CAS-001



CompTIA Advanced Security Practitioner

Version: 4.0
CompTIA CAS-001 Exam

Topic 1, Volume A

Exam A

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

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

Correct Answer: A
Section: (none)
Explanation

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

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

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

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

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

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

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

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

Correct Answer: BD
Section: (none)

Explanation

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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

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

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

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

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

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

Correct Answer: D
Section: (none)
Explanation

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

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

profile (administrative policy profile).

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

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

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

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

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

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

A. Apply remote access policies
B. Apply NTFS permissions
C. Apply group policies
D. Apply account policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to accomplish the task, you should apply group policy in the network. A group policy that is created by an administrator affects all users on a computer or all users on a domain. Group policies can be used for defining, customizing, and controlling the functioning of network resources, computers, and operating systems. They can be set for a single computer with multiple users, for users in workgroups, or for computers in a domain. Administrators can configure group policy settings for users as well as for computers in many ways. Group policies can be used to allow or restrict the access of a particular program by a particular user. It can also be used to configure the desktop, the Start menu, the taskbar. the Control Panel, security settings, among other things. In Windows XP, group policies can be configured by using the Group Policy Console dialog box, which can be opened by running the GPEDIT.MSC command from the Start menu.

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

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

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

QUESTION 6
Which of the following is the most secure authentication scheme and uses a public key cryptography and digital certificate to authenticate a user?

A. Form-based authentication
B. Basic authentication
C. Digest authentication
D. Certificate-based authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 6 CompTIA CAS-001 Exam

Explanation:
Certificate-based authentication is the most secure authentication scheme. A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. A digital certificate is an electronic document that includes identification information, public key, and the digital signature of a certification authority based on that certification authority's private key. When a user connects to the server, he presents his digital certificate containing the public key and the signature of the certification authority. The server verifies the validity of the signature and whether the certificate has been provided by a trusted certificate authority or not. The server then authenticates the user by using public key cryptography to prove that the user truly holds the private key associated with the certificate. Answer option B is incorrect. Basic authentication is a simple method of authentication that provides minimum security. It should be used only when security is not critical because basic authentication requests are not encrypted.
Answer option A is incorrect. Form-based authentication Form-based authentication allows users to create their own custom forms. It requires session tracking for the authentication, so that the container may use the login form. It is not a secure authentication scheme. Answer option C is incorrect. Digest authentication is a secure authentication method in which passwords are sent across a network as a hash value rather than as clear text.

It is a more secure authentication method as compared to Basic authentication. Digest authentication works across proxy servers and firewalls.

QUESTION 7
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 8
In which of the following activities an organization identifies and prioritizes technical, organizational, procedural, administrative, and physical security weaknesses?

A. Social engineering
"Certification Depends on Only One Thing" - www.actualanswers.com 8 CompTIA CAS-001 Exam
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 9 CompTIA CAS-001 Exam

QUESTION 9
SDLC phases include a minimum set of security tasks that are required to effectively incorporate security in the system development process. Which of the following are the key security activities for the development/ acquisition phase?

Each correct answer represents a complete solution. Choose two.

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

Correct Answer: AB
Section: (none)
Explanation

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

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

QUESTION 10
Which of the following is an XML-based framework developed by OASIS and used to exchange user, resource and service provisioning information between cooperating organizations?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Certification Depends on Only One Thing" - www.actualanswers.com 10 CompTIA CAS-001 Exam

Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used toexchange 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. Answer option A 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 D is incorrect. 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. Security Assertion Markup Language (SAML) 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 11

Which of the following terms is about communicating the user's need and ability to communicate, and the medium through which that communication may occur?

A. Data sharing
B. Presence
C. Instant messaging
D. Audio conferencing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 11 CompTIA CAS-001 Exam

Explanation:
Presence, in the world of telephony, is about communicating the user's need and ability to communicate, and the medium through which that communication may occur. If a user is connected to the Internet, presence may dictate that the user wants to be reached through the medium of IP telephony. The point of presence is to allow the user to be located and contacted wherever the user is physically using the preferred method of the user.

Answer option A is incorrect. Data sharing is one important element of collaboration. H.323 also offers data sharing as an optional capability. Data sharing is the practice of making data used for scholarly research available to other investigators.

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 C 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 user's 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.

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), whereas online chat also includes web-based applications that allow communication between users in a multi-user environment.

QUESTION 12
Which technology can be used to help ensure the efficient transport of VoIP traffic?

A. DNS
B. QoS
C. H.323
D. RSTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 12 CompTIA CAS-001 Exam

Explanation: Answer option B is correct.
Quality of Service (QoS) is a technology for prioritizing traffic on the network. VoIP requires optimization of

bandwidth to ensure users do not experience "call drops" created by lack of bandwidth due to congestion issues. QoS is a mechanism to provide this optimization.

QUESTION 13
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 14
Which of the following protocols is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web- based push to talk features?

A. SIP
B. MGCP
C. H.323

D. RTP

Correct Answer: D
Section: (none)
Explanation

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

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

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

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

addresses using NAT and PAT.

QUESTION 15
Collaboration platform offers a set of software components and services that enable users to communicate, share information, and work together for achieving common business goals. What are the core elements of a collaboration platform?

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

A. Product and service integration
B. Real-time communication
C. Change management
D. Team collaboration
E. Messaging

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation: 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 a wiki, task management, full-text search)
· Real-time communication {presence, instant messaging, Web conferencing, application/desktop sharing, voice, audio and video conferencing)

QUESTION 16
Which of the following stages are involved in the successful implementation of a collaboration platform? Each correct answer represents a part of the solution. Choose two.

A. Ongoing collaboration solution design
B. Federated identity management
C. Platform implementation
D. Product and service integration
"Certification Depends on Only One Thing" - www.actualanswers.com 15 CompTIA CAS-001 Exam

Correct Answer: AC
Section: (none)
Explanation

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

QUESTION 17
You work as a Network Administrator for uCertify Inc. You want the clients and servers in your organization to be able to communicate in a way that prevents eavesdropping and tampering of data on the Internet. Which of the following will you use to accomplish the task?

A. EFS
B. WEP
C. SSL
D. MS-CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: In order to accomplish the task, you should use SSL in the organization's network. Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication.

Answer option B is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, i.e., authentication and encryption. It provides security for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream.

Answer option 0 is incorrect. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.

"Certification Depends on Only One Thing" - www.actualanswers.com 16 CompTIA CAS-001 Exam

Answer option A is incorrect. Encrypting File System (EFS) is used to encrypt sensitive data in files stored on disks using the NTFS file system. EFS is easy to manage, difficult to hack, andtransparent to the owner of a file and to applications because it runs as an integrated system service. Only the owner of a protected file can open the file and work on it. Using EFS involves a minimum of administrative effort.

QUESTION 18

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 19
Which of the following is frequently used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it?

A. Fuzzer
B. Port scanner
C. MegaPing
D. UDP scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A port scanner is a software application designed to probe a network host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. To portscan a host is to scan for listening ports on a single target host. To portsweep is to scan multiple hosts for a specificlistening port. The latter is typically used in searching for a specific service, for example, an SQL-based computer worm may portsweep looking for hosts listening on TCP/ UDP port 1433.

Answer option A is incorrect. 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 D 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.

Answer option C is incorrect. MegaPing is used to provide all essential network utilities for information system specialists, system administrators, or individuals. It also includes comprehensive security scanner, host and port monitor, and network utilities. All these scanners can scan individual computers, domains, any range of IP addresses, selected type of computers inside domains, and user specified host lists.

QUESTION 20
You work as a Network Administrator for uCertify Inc. You need to conduct network reconnaissance, which is carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized/allowed.

What will you do?

"Certification Depends on Only One Thing" - www.actualanswers.com 18 CompTIA CAS-001 Exam

A. Use a SuperScan
B. Use a netcat utility
C. Use a vulnerability scanner
D. Use an idle scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the given scenario, you will use a vulnerability scanner. The vulnerability scanner can be used to conduct network reconnaissance. Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

Answer option B is incorrect. Netcat is a freely available networking utility that reads and writes data across network connections by using the TCP/IP protocol. Netcat has the following features:
· It provides outbound and inbound connections for TCP and UDP ports. · It provides special tunneling such as UDP to TCP, with the possibility of specifying all network parameters.
· It is a good port scanner.
· It contains advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data. · It is an optional RFC854 telnet code parser and responder.

Answer option A is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the hostname of the remote system. It can also be used as an enumeration tool for the following:
· NetBIOS information
· User and Group Accounts information
· Network shares
· Trusted Domains
· Services probing

QUESTION 21
"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 22
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 23
Which of the following components are contained in Xsan?

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

A. Ethernet network
B. SAN volume
C. Xsan metadata controller
D. Server clients

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Xsan, introduced by Apple, is an enterprise-class SAN file system. It is a 64-bit duster file system specifically designed for small and large computing environments. It helps multiple Mac desktops and Xserve systems to share RAID storage volumes over a high-speed Fibre Channel network.
Xsan comprises the following components:
· SAN volume
· Fibre Channel network
· Xsan metadata controller
· Xsan clients

"Certification Depends on Only One Thing" - www.actualanswers.com 21 CompTIA CAS-001 Exam

· Ethernet network
· Network clients

QUESTION 24
Which of the following statements are true about network-attached storage (NAS)? Each correct answer represents a complete solution. Choose all that apply.

A. NAS systems do not contain hard disks.
B. NAS uses file-based protocols, such as NFS, SMB/CIFS, or AFP.
C. NAS is connected to a computer network providing data access to heterogeneous network clients.
D. NAS is file-level computer data storage.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network-attached storage (NAS) is file-level computer data storage connected to a computer network providing data access to heterogeneous network clients. NAS systems contain one or more hard disks, often arranged into logical, redundant storage containers or RAID arrays. It removes the responsibility of file serving from other servers on the network. NAS uses file-based protocols, such as NFS, SMB/CIFS, or AFP. NAS units rarely limit clients to a single protocol.

QUESTION 25
Which of the following is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program?

A. Gray box testing
B. White box testing
C. Black box testing
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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. Black box testing is also known as specification-based testing. It ignores the internal logic of an application. It refers to test activities using specification- basedtesting methods to discover errors in an application. The test activities are based on requirements and specifications of the application. It focuses on the following errors:
· Specification-based function errors
· Specification-based component/system behavior errors · Specification-based performance errors
· User-oriented usage errors
· Black box interface errors

Answer option B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods:

Control flow-based testing
o Create a graph from source code.
o Describe the flow of control through the control flow graph. o Design test cases to cover certain elements of the graph.

Data flow-based testing
o Test connections between variable definitions.
o Check variation of the control flow graph.
o Set DEF (n) contains variables that are defined at node n.
o Set USE (n) are variables that are read.

Answer option A is incorrect. Gray box testing is a combination of black box and white box testing. It is non-intrusive and impartial, as it does not require that a tester have access to the source code. It treats a system as a black box in the sense that it must be analyzed from the outside. Basically, it is used to find out defects related to bad design or bad implementation of the system. This type of testing is more commonly used with Web applications, as the Internet has a pretty stable interface.

QUESTION 26
Which of the following statements are true about OCSP and CRL?

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

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

Correct Answer: ABC
Section: (none)
Explanation

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

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

QUESTION 27
Which of the following is SAN management software and is designed for cross-platform workgroup collaboration?

A. SANmaestro
B. SANmelody
C. VisualSAN
D. MetaSAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
MetaSAN, developed by Tiger Technology Sari, is high-speed file sharing SAN management software. It is designed for cross-platform workgroup collaboration. This software allows users of Windows, Linux, and Mac OS X to share files with one another. MetaSAN enables sharing one (or

more) high speed RAID device with multiple computers using Fibre Channel, iSCSI, Ethernet, or InfiniBand interconnect.

Answer option C is incorrect. VisualSAN provides administrators with a single view of all devices across their storage networks. It delivers advanced network, performance, and configuration management capabilities. The VisualSAN management suite comprises three modules:
1.VisualSAN Network Manager
2.VisualSAN Configuration Manager
3.VisualSAN Performance Manager

Answer option B is incorrect. Standards Intel/AMD blades, servers, or virtual machines are converted by SANmelody into fully capable storage servers that perform virtualizing disks and serve them over existing networks to application servers. It enhances performance through built-in caching that minimizes delays from slow mechanical drives. SANmelody equitably distributes the available disk space into multiple applications spread across several machines.

Answer option A is incorrect. SANmaestro is an analysis and decision support tool. It monitors, reports, charts, gathers, and analyzes system performance and resource utilization information from multiple networked systems. This tool fits the organizations reporting and analysis needs, as it generates useful reports and charts.

This tool is used to collect system performance and utilization metrics. SANmaestro can analyze historical data accumulated over long periods {up to two years).

QUESTION 28
End point security is an information security concept that assumes that each device (end point) is responsible for its own security. Which of the following tools are examples of end point security software?

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

A. Grayware
B. Anti-malware
C. Anti-spyware
D. Anti-virus
E. Spam filters

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:
"Certification Depends on Only One Thing" - www.actualanswers.com 25 CompTIA CAS-001 Exam

Explanation:
End point security is an information security concept that assumes that each device (end point) is responsible for its own security. The examples of end point security software are:
· Anti-malware
· Anti-virus
· Anti-spyware
· Spam filters

Anti-malware programs can combat malware by providing real time protection against the installation of malware software on a computer. This type of protection works in the same way as that of antivirus protection. Anti-malware software scans all incoming network data for malware software and blocks any threats it comes across.

Anti-malware software programs can be used for detection and removal of malware software that has already been installed in a computer system. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found.

Anti-Virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

Anti-Virus software is a class of program that searches your hard drive, floppy drive, and pen drive for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets.

Popular Anti-Virus packages are as follows:
· Bit Defender Anti-Virus
· McAfee Virus Scan
· Kaspersky Anti-Virus
· F-Secure Anti-Virus
· Symantec Norton Anti-Virus
· Panda Titanium Anti-Virus

· Avira Anti-Virus
· Avast Anti-Virus
· Trend Micro Anti-Virus
· Grisoft AVG Anti-Virus
· ESET Nod32 Anti-Virus
· Webroot Anti-Virus
· Quick Heal Anti-Virus

· eTrust EZ Anti-Virus
· ZoneAlarm Anti-Virus

Anti-spyware is software that is designed to protect a computer against malware, adware, spyware, rogueware, etc. It is a quite different from antivirus software because it does not specialize in viruses. Protection against spyware helps to defend against bugs that can send outunauthorized information about victim, steal confidential information, slow down Internet connection, install unwanted programs on the computer, etc.

Spam filters are utilities that stop spam (unsolicited) mails from reaching users. Spam filters are available as modules or components for mail servers (both incoming and outgoing). Administrators can also install spam and matware-scanning modules on firewalls and proxy servers. Administrators should opt for tools that place suspect messages in a special folder or queue that enables users to double-check the automated filters.

Answer option A is incorrect. Grayware refers to applications or files that are not classified as viruses or trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization. Often grayware performs a variety of undesired actions such as irritating users with pop-up windows, tracking user habits and unnecessarily exposing computer vulnerabilities to attack.

QUESTION 29
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 30
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 31
Mary is a new security administrator. She wants to focus most of her efforts on the areas that have the greatest risk. Which of the following areas poses the greatest risk?

"Certification Depends on Only One Thing" - www.actualanswers.com 28 CompTIA CAS-001 Exam

A. Employees
B. Hackers
C. Cyber terrorism
D. Viruses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Employees pose the greatest risk. Even malware is often introduced to a network through lack of diligence on the part of employees.

Answer option B is incorrect. While hackers are a real problem, they pose less risk than internal employees.

Answer option D is incorrect. Viruses are a legitimate concern. However, they are often introduced due to employees failing to follow security polices.

Answer option C is incorrect. It is the case that cyber terrorism is a real threat. However, it is less of a threat than employees.

QUESTION 32

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

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

Correct Answer: D
Section: (none)
Explanation

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

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

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

"Certification Depends on Only One Thing" - www.actualanswers.com 29 CompTIA CAS-001 Exam

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

QUESTION 33
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 34
Cloud computing is significantly impacting the definition of network perimeters. Which of the following is NOT a network perimeter issue with cloud computing?

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

D. What protections are in place on the cloud?

Correct Answer: B
Section: (none)
Explanation

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

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

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

QUESTION 35
Network boundaries can be logical or physical. Which of the following are boundaries a network administrator cannot control?

A. Informational
B. Logical
C. External
D. Physical

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
External boundaries are those outside your network. This term does not refer to your network perimeter. A network administrator cannot control external boundaries. Answer options D and B are incorrect. Physical and logical boundaries are two broad classes of boundaries that are under your administrative control. Answer option A is incorrect. An information domain is a legitimate domain the administrator must address. Information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required.

QUESTION 36
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 37
Which of the following statements are true about audit findings?

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

A. Audit findings is described as dutifulness, obligingness, pliability, tolerance, and treatability.
B. Audit findings involve contracting out of a business function to an external provider/buyer.
C. The effective audit findings is designed to mitigate incomplete findings, as well as those that do not meet the intent of the process approach, have missing criteria or have incomplete objective evidence.
D. Audit findings are an effective method to facilitate the necessary improvements within a quality management system.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Audit findings are an effective method to facilitate the necessary improvements within a quality management system. The Effective Audit Findings is designed to mitigate incomplete findings, as well as those that do not meet the intent of the process approach, have missing criteria or have incomplete objective evidence. It helps organization in improving how it receives and interprets findings from second- and third-party auditors with the ultimate objective of quality management system improvement.

Answer option A is incorrect. Compliance is described as dutifulness, obligingness, pliability, tolerance, and tractability. Compliance means that an organization must take care of the organization's internal regulations, as well as follow the laws of the country and requirements of

local legislation and regulations.

Answer option B is incorrect. Outsourcing is the term which is used to define the process of contracting a business function to someone else. It involves contracting out of a business function to an external provider/ buyer.

QUESTION 38
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 39
Denial of service attacks are quite common. Whether it is an ICMP flood, Syn Flood, or SMURF

attack, they all are based on the concept of_____.

A. Circumventing the firewall
B. Resource exhaustion
C. Exploiting OS vulnerabilities
D. Avoiding the IDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Resource exhaustion is the term for the situation wherein a target system has exhausted all of its resources and can no longer respond to legitimate requests. All denial of service attacks are based on this concept.
Answer option A is incorrect. While many DoS attacks to involve circumvention the firewall, this is not a necessary component of a DoS.
Answer option D is incorrect. Avoiding IDS detection is actually very difficult for a DoS attack. Answer option C is incorrect, Many DoS attacks do depend on exploiting OS vulnerabilities, However, this is not the basic concept of a DoS.

QUESTION 40
Resource exhaustion includes all of the following except_____

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

QUESTION 41
"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 42
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 35 CompTIA CAS-001 Exam

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

QUESTION 43

_____is defined as maintaining ongoing awareness of information.

A. Intrusion detection
B. Vulnerability assessment
C. Continuous Monitoring
D. Security Awareness

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is the definition of continuous monitoring. Ongoing is the keyword. Monitoring that is intermittent is very different than continuous monitoring.

Answer option B is incorrect. Vulnerability scanning can be part of continuous monitoring. And some vulnerability scanners have the option to monitor in real time, but a vulnerability scanner is only part of continuous monitoring.

Answer option A is incorrect. Intrusion detection should be real time and continuous, but does not involved risk management decisions or an awareness of information security.

Answer option D is incorrect. Security awareness is only one aspect of continuous monitoring.

QUESTION 44
Denise works as a Security Administrator for a community college. She is assessing the various risks to her network. Which of the following is not a category of risk assessment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Certification Depends on Only One Thing" - www.actualanswers.com 36 CompTIA CAS-001 Exam

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

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

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

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

QUESTION 45
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 46
"Certification Depends on Only One Thing" - www.actualanswers.com 37 CompTIA CAS-001 Exam
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 47
_____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 48
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 49
Mark works as a Human Resource Manager for uCertify Inc. He is responsible to hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. What will Mark do to accomplish the task?

A. Job rotation
B. Mandatory Vacations
C. Job responsibility
D. Separation of duties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Job rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breadth of exposure to the entire operation.

Job rotation is practiced to allow qualified employees to gain more insights into the processes of a company, and to reduce boredom and increase job satisfaction through job variation. This process helps an organization to improve its overall security by rotating employees among different job positions.

Answer option B is incorrect. Mandatory vacations are vacations that are forced on employees to avail them. These vacations can ensure that employees take the time off that they should. It is important that employees not get burned out.Whichwould make them less effective in carrying out their duties. Mandatory vacations ensure that employees are effective all the time when they are on duty.

Answer option C is incorrect. Job responsibility is the specific work task an employee is required to perform on a regular basis.

"Certification Depends on Only One Thing" - www.actualanswers.com 40 CompTIA CAS-001 Exam

Answer option D is incorrect. Separation of duties ensures that no one person is given the power to abuse the trust that others place in the information security. In any situation in which too much responsibility for a process falls to one person, there is the potential for abuse.

Another reason to separate duties is that if the person with all of the knowledge of a certain area or function suddenly leaves the company or dies in a tragic accident, then that knowledge is gone with the person. Someone else would have to quickly take over the position, possibly without adequate training, leaving the information vulnerable to attack while the new person learns the job. Separation of duties ensures that transition is smooth.

QUESTION 50
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 51
Which of the following elements are essential elements of a privacy policy? Each correct answer represents a complete solution. Choose two.

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

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 52
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 53
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 54
Which of the following types of Incident Response Teams (IRT) is responsible for a logical or physical segment of the infrastructure, usually of a large organization or one that is geographically dispersed?

A. Distributed IRT
B. Outsourced IRT
C. Coordinating IRT
D. Central IRT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The various types of Incident Response Team (IRT) are as follows:
· Central IRT: It handles all incidents for the organization, usually either a small organization or one that is centrally located.
· Distributed IRT: It is responsible for a logical or physical segment of the infrastructure, usually of a large organization or one that is geographically dispersed. · Coordinating IRT: It is a combination of central IRT and distributed IRT. Generally, the central team provides guidance to distributed IRTs, develops policies and standards, etc. The distributed team manages and implements incident response.
· Outsourced IRT: It states that the successful IRTs are comprised of the employees of the same organization, or may be fully or partially outsourced.

"Certification Depends on Only One Thing" - www.actualanswers.com 43 CompTIA CAS-001 Exam

QUESTION 55
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 56
Which of the following are the purposes of the Cost-benefit analysis process? Each correct answer represents a complete solution. Choose two.

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

Correct Answer: AC
Section: (none)
Explanation

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

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

QUESTION 57
Which of the following is the capability to correct flows in the existing functionality without affecting other components of the system?

A. Manageability
B. Reliability
C. Maintainability

D. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
· Availability: It is used to make certain that a service/resource is always accessible. · Manageability: It is the capability to manage the system for ensuring the constant health of the system with respect to scalability, reliability, availability, performance, and security. · Maintainability: It is the capability to correct flows in the existing functionality without affecting other components of the system.
· Answer option B is incorrect. It is not a valid option.

QUESTION 58
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 59
Which of the following standard organizations promulgates worldwide proprietary industrial and commercial standards?

A. IEEE
B. ANSI
"Certification Depends on Only One Thing" - www.actualanswers.com 46 CompTIA CAS-001 Exam
C. ISO
D. W3C

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The International Organization for Standardization, widely known as ISO, is an international- standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments.

Answer option B is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

Answer option A is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro- technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

Answer option D is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated, with support from DARPA and the European Commission.

QUESTION 60
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 61
Which of the following statements are true about prototypes?

Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: (none)
Explanation

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

Answer:

QUESTION 62
Which of the following is a structured review process to analyze what happened, why it happened, and how it can be done better, by the participants and those responsible for the project or event?

A. After action report
B. After action analysis
C. After action summary
D. After action review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An after action review (AAR) is a structured review process to analyze what happened, why it happened, and

how it can be done better, by the participants and those responsible for the project or event. It occurs within a cycle of establishing the leader's intent, planning, preparation, action and review.

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

QUESTION 63
Which of the following statements are true about capability-based security?

"Certification Depends on Only One Thing" - www.actualanswers.com 49 CompTIA CAS-001 Exam

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 64
Which of the following statements are true about Fibre Channel over Ethernet (FCoE)?

Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

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

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

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

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

QUESTION 65
which of the following is the randomness collected by an operating system or application for use in cryptography or other uses that require random data?

A. Confusion
B. Diffusion
C. Digital signature
D. Entropy

Correct Answer: D
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 the purported 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 B, A, and A are incorrect. These are not valid options.

QUESTION 66
Which of the following is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally?

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

Correct Answer: D
Section: (none)
Explanation

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

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

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

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

QUESTION 67
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 68
Which of the following are examples of privilege escalation? Each correct answer represents a complete solution. Choose two.

A. John uses SQL commands to login to a website hedoes not have authorization to
B. Juan logs in with his account, then takes over Anita's privileges
C. John logs in as a standard user but uses a flaw in the system to get admin privilege
D. Fred uses Ophcrack to get a Windows XP password

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In both cases the user had some authentic access, but then got additional privileges they had not been authorized.

Answer option C is incorrect. This is an example of SQL injection.

Answer option D is incorrect. This is an example of password cracking.

QUESTION 69
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 70
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

"Certification Depends on Only One Thing" - www.actualanswers.com 54 CompTIA CAS-001 Exam

deployment cycles and changes in the testing patterns.

QUESTION 71
Allen is using a security feature that ensures that if hackers want to compromise a private key, they will only be

able to access data in transit protected by that key and not any future data because future data will not be associated with that compromised key?

Which security feature is he using?

A. IPSec
B. PGP
C. SPKI
D. PFS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PFS (Perfect Forward Secrecy) will ensure that the same key will not be generated again, so forcing a new diffie-hellman key exchange. 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. Simple public key infrastructure (SPKI) does not deal with public authentication of public key information, that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, since the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an 'authorization loop" in SPKI terminology, where authorization is integral to its design.

Answer option B is incorrect. Pretty Good Privacy (PGP) is an encryption method that uses public- key encryption to encrypt and digitally sign e-mail messages during communication between e- mail clients. PGP is effective, easy to use. and free. Therefore, it is one of the most common ways to protect messages on the Internet.

"Certification Depends on Only One Thing" - www.actualanswers.com 55 CompTIA CAS-001 Exam

Answer option A is incorrect. Internet Protocol Security (IPSec) is an Internet Protocol security standard. It is used to provide a general, policy-based IP layer security mechanism that is usedfor providing host-by-host authentication. IPSec policies can be defined as having security rules and settings that control the flow of inbound data,

QUESTION 72
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 73
Which of the following statements best describe the advantages of Simple Object Access Protocol (SOAP): Each correct answer represents a complete solution. Choose three.

A. It is versatile enough to allow for the use of different transport protocols.
B. It is simple and extensible.
C. It allows easier communication through proxies and firewalls than previous remote execution technology.
D. It is language and platform dependent.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The advantages of SOAP are as follows:
· It allows easier communication through proxies and firewalls than previous remote execution

technology.
· It is versatile enough to allow for the use of different transport protocols. The standard stacks use HTTP as a transport protocol, but other protocols are also usable.
· It is platform independent.
· It is language independent.
· It is simple and extensible.

QUESTION 74
An organization s network uses public keys for message encryption. Which of the following manages security credentials in the network and issues certificates to confirm the identity and other attributes of a certificate in relation to other entities?

A. Certificate Authority
B. Certificate Revocation List
C. Public Key Infrastructure
D. Online Certificate Status Protocol

Correct Answer: A
Section: (none)
Explanation

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

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

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

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

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

QUESTION 75
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 76
"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 77
Which of the following is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems?

A. System Development Life Cycle
B. Security Requirements Traceability Matrix
C. Security Development Life Cycle
D. Product lifecycle management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle:
1.Initiation
2.Development/acquisition
3.Implementation
4.Operation/maintenance
5.Disposal

Answer option C is 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

Answer option B is incorrect. 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 option D is incorrect. Product lifecycle management (PLM) is the process of managing the entire lifecycle of a product from its conception, through design and manufacture, to service and disposal. PLM integrates people, data, processes and business systems and provides a product information backbone for companies and their extended enterprise. Product lifecycle management is very important for a corporation s information technology structure. The core of PLM is in the creations and central management of all product data and the technology used to access this information and knowledge.

QUESTION 78
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 79
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 80

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

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

Correct Answer: A
Section: (none)
Explanation

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

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

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

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

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

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

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

QUESTION 81
You have considered the security of the mobile devices on your corporate network from viruses and malware. Now, you need to plan for remotely enforcing policies for device management and security, which of the following things are includes in the configuration management of mobile devices?

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

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

Correct Answer: BD
Section: (none)
Explanation

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

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

QUESTION 82
Which of the following devices allows telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system?

A. IP phone
B. Laptop
C. IP camera
D. Smartphone

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

"Certification Depends on Only One Thing" - www.actualanswers.com 65 CompTIA CAS-001 Exam

Answer option D is incorrect. 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.

Answer option C is incorrect. An IP camera is a digital camera used for surveillance. It is unlike analog closed circuit television cameras can send and receive data through a computer network and the Internet. There are two types of IP cameras:

Centralized IP camera: It needs a central Network Video Recorder (NVR) to handle the recording, video and alarm management.
Decentralized IP camera: It does not need a central Network Video Recorder (NVR). Decentralized IP camera has built-in recording functionality and so. it can record directly to digital storage media.

Answer option B is incorrect. A laptop is a type of portable computer. It is designed for mobile use and small and light enough to sit on a person's lap while in use. It integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device (touchpad or trackpad, pointing stick), speakers, and often including a battery, into a single small and light unit.

Laptops are usually notebook-shaped with thicknesses between 0,7*1.5 inches (18-38 mm) and dimensions ranging from 10x8 inches (27x22cm, 13" display) to 15x11 inches (39x28cm, 17" display) and up. Modern laptops weigh 3 to 12 pounds (1.4 to 5.4 kg): older laptops were usually heavier. Most laptops are designed in the flip form factor to protect the screen and the keyboard when closed.

QUESTION 83
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.
"Certification Depends on Only One Thing" - www.actualanswers.com 66 CompTIA CAS-001 Exam

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 84
Dipen is looking for a method to effectively get security policies read by staff and management, which of the following is the best solution?

A. Printed policies
B. Intranet Website
C. Routine informational meetings
D. Email blast

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Dipen should use the Intranet Website. This method puts the security policies in a location that is easy for staff to access, and it is also easy to update. It also does not interfere unnecessarily with employees work processes.

Answer option D is incorrect. An email blast is inconvenient, and must be repeated any time updates to the policies are made. It is also inconvenient for staff members to refer back to. Answer option A is incorrect. Printed policies are difficult to store and access, generate unnecessary paper, and are difficult to update.

Answer option C is incorrect. Routine meetings are very intrusive and interrupt the normal work flow. They can also be difficult to schedule all the staff at a specific time.

QUESTION 85
Which of the following teams has the responsibility of accounting for personnel and rendering aid?

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

A. Physical security team
B. Emergency response team
C. Emergency management team
D. Damage assessment team

Correct Answer: B
Section: (none)
Explanation

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

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

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

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

QUESTION 86
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 87
Which of the following is a computer program that is designed to assess computers, computer systems, networks, or applications for weaknesses?

A. Vulnerability scanner
B. Paros
C. Port scanner
D. SYN scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Vulnerability scanners work on the concept of port scanners. In addition to identifying hosts and open ports, a vulnerability scanner also provides information on the associated vulnerabilities. Vulnerability scanners are very useful to identify out-of-date software versions, applicable patches, system upgrades, etc. The weakness of these scanners is that they can only identify surface vulnerabilities. These scanners are unable to address the overall risk level of a scanned network.

Answer option B is incorrect. Paros is a Web application vulnerability scanner that supports editing /viewing HTTP/HTTPS messages on-the-fly to change items such as cookies and form fields. It also includes various features, such as Web traffic recorder, Web spider, hash calculator, and a scanner for testing common Web application attacks such as SQL injection and cross-site scripting. A SYN scan is a type of TCP scanning. This scan type is also known as 'half-open scanning' because it does not open a full TCP connection. The port scanner generates a SYN packet. If the target port is open, it responds with a SYN-ACK packet. The scanner host responds with an RST packet that causes the connector before the handshake is completed.

Answer option C is incorrect. A port scanner is a software tool that is designed to search a network host for open ports. This tool is often used by administrators to check the security of their networks. It is also used by hackers to compromise the network and systems.

QUESTION 88
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.

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 89
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 90
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 91
Which of the following are the reasons to use SAN?

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

A. Faster backup of large amounts of data
B. Fast and extensive disaster recovery
C. Better disk utilization
D. Cost effectiveness
E. Better availability for applications

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reasons to use SAN are as follows:
· Better disk utilization
· Fast and extensive disaster recovery
· Better availability for applications
· Faster backup of large amounts of data

Answer option D is incorrect. Installing SAN is expensive and it is not a reason to use SAN.

QUESTION 92
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 93
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 94
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.

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 95
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 96
CORRECT TEXT

Fill in the blank with the appropriate word.

_____encryption protects a file as it travels over protocols, such as FTPS (SSL), SFTP (SSH), and HTTPS.

"Certification Depends on Only One Thing" - www.actualanswers.com 75 CompTIA CAS-001 Exam

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: Transport
Explanation: Transport encryption protects a file as it travels over protocols, such as FTPS (SSL). SFTP (SSH), and HTTPS. Leading solutions use encryption strengths up to 256-bit. File encryption encrypts an individual file so that if it ever ends up in someone else's possession, they will not be able to open it or see the contents. Pretty Good Privacy (PGP) is commonly used to encrypt files. PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.
Transport

QUESTION 97
Which of the following refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements?

A. Trusted OS
B. Distributed operating system
C. Network operating system

D. Real time operating system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Trusted Operating System (TOS) refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements.

The Common Criteria, combined with the Security Functional Requirements (SFRs) for Labeled Security Protection Profile (LSPP) and Mandatory Access Control(MAC) is the most common set of criteria for trusted operating system design. The Common Criteria is the outcome of a multi-year effort by the governments of the U.S., Canada. United Kingdom, France, Germany- the Netherlands and other countries with an aim to develop a harmonized security criteria for IT products.

Answer option D is incorrect. A real-time operating system (RTOS) is an operating system used to serve real-time application requests. It is an operating system that guarantees a certain capability within a specified time constraint. A key characteristic of an RTOS is the level of its consistency concerning the amount of time it takes to accept and complete an application s task. A real-time OS has an advanced algorithm for scheduling and is more frequently dedicated to a narrow set of applications.

"Certification Depends on Only One Thing" - www.actualanswers.com 76 CompTIA CAS-001 Exam

Answer option C is incorrect. The network operating system (NOS) manages resources on a network, offers services to one or more clients, and enables clients to access remote drives as if the drives where on clients own computer. The functions provided by a network operating system are as follows:
· File and print sharing
· Account administration for users
· Security

Answer option B is incorrect. A distributed operating system is the logical aggregation of operating system software over a collection of independent, networked, communicating, and spatially disseminated computational nodes.

QUESTION 98
The Top Level Management contains the Board of Directors (BOD) and the Chief Executive Officer (CEO) or General Manager (GM) or Managing Director (MO) or President. What are the roles of the top level management?

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

A. The Top Level Management decides the objectives, policies, and plans of the organization.
B. The Top Level Management prepares long-term plans of the organization.
C. The Top Level Management has minimum authority and responsibility to take few decisions.
D. The Top Level Management assembles the available resources.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Top Level Management contains the Board of Directors (BOD) and the Chief Executive Officer (CEO) or General Manager (GM) or Managing Director (MD) or President. The Board of Directors is the representatives of the Shareholders, i.e. they are selected by the Shareholders of the company. Similarly, the CEO is selected by the Board of Directors of an organization.

Following are the main roles of the top level management:
· The top level management decides the objectives, policies, and plans of the organization. · The top level management assembles the available resources. · The top level management does mostly the work of decision making. · The top level management spends more time in planning and organizing. · The top level management prepares long-term plans of the organization. · The top level management has maximum authority and responsibility to take any decision.

QUESTION 99
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 100
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 101
John is concerned about internal security threats on the network he administers. He believes that he has taken every reasonable precaution against external threats, but is concerned that he may have gaps in his internal security. Which of the following is the most likely internal threat?

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

Correct Answer: A
Section: (none)
Explanation

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

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

QUESTION 102
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 103
Juan realizes that more and more employees at his company are using smart phones. He wants to assess the risk posed by these devices. Which of the following best describes the most significant risk from smart phones?

A. Smart phones extend the network and introduce new attack vectors
B. Smart phones can be a way for employees to steal data
C. Smart phones pose no real additional risks
D. Smart phones can be a distraction to employees

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Smart phones extend your network perimeter and introduce a new vector for malware to be introduced to your network.

Answer option D is incorrect. While smart phones may be a distraction, that is not the primary risk from them.

Answer option B is incorrect. While smart phones could be used to steal data, that is a less significant and less common risk.

"Certification Depends on Only One Thing" - www.actualanswers.com 80 CompTIA CAS-001 Exam

Answer option C is incorrect. Smart phones do indeed pose new risks.

QUESTION 104
David works as a Network Administrator for a large company. The company recently decided to extend their intranet access, to allow trusted third party vendors access to the corporate intranet, what is the best approach for David to take in securing intranet?

A. Tighten user access controls on the intranet servers
B. Patch the OS on the intranet servers
C. Place intranet servers in a DMZ so both corporate users and trusted vendors can access it
D. Install an IDS on the intranet servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By placing the intranet servers in a DMZ, external vendors accessing those servers would be separated from the corporate network. The most significant threat from allowing outside vendors access to internal resources, is that an attack could originate from their network.

Answer option D is incorrect. An IDS is always a good idea, however it will only warn you that an attack is occurring, not make the attack less likely.

Answer option A is incorrect. Managing user controls is always a good idea. However, in this case the real problem is segmenting the external users from the internal network.

Answer option B is incorrect. One should always be patching the OS regardless of the situation.

Topic 2, Volume B

QUESTION 105
_____ 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 106
Which of the following statements are true about mergers?

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

A. Mergers occur when the merging companies have their different consent.
B. Mergers present the involved parties with special challenges that must be navigated unto agreement.
C. Mergers refer to the aspect of corporate strategy, corporate finance and management dealing with the buying, selling, dividing, and combining of different companies,
D. Mergers can be vertical, horizontal, congeneric or conglomerate, depending or the nature of the merging companies.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mergers refer to the aspect of corporate strategy, corporate finance and management dealing with the buying, selling, dividing, and combining of different companies and similar entities that can help an enterprise grow rapidly in its domain or location of origin, or a new field or new location, without creating a subsidiary, other child entity or using a joint venture.

Mergers occur when the merging companies have their mutual consent as different from acquisitions, which can take the form of a hostile takeover. Mergers can be vertical, horizontal, congeneric or conglomerate, depending or the nature of the merging companies.

Answer option 8 is incorrect. A partnership is an arrangement where parties agree to cooperate to advance their mutual interests. Partnerships present the involved parties with special challenges

"Certification Depends on Only One Thing" - www.actualanswers.com 82 CompTIA CAS-001 Exam

that must be navigated unto agreement.

QUESTION 107

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 108
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 109
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 110
Denish is the administrator for a cloud computing vendor. He is evaluating the security benefits and threats of cloud computing. Cloud computing has a number of challenges, which of the following is a cloud less susceptible to, than a traditionally hosted server?

A. Internal Data Theft
B. Privilege Escalation
C. DDoS attacks
D. Hard drive failure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Because the cloud is a distributed network, with distributed servers, it is more resilient against distributed denial of service attacks. It takes a great more resources to successfully launch a denial of service attack against a cloud.

Answer option B is incorrect There is no difference in privilege escalation between a cloud and a traditionally hosted server.

Answer option A is incorrect. There is no difference in internal data threat between a cloud and a traditionally hosted server.

Answer option D is incorrect. Actually a hard drive failure is no more or less likely in a cloud than a traditionally hosted server. However, if the server holds multiple virtualized systems, the impact could actually be greater in the cloud.

QUESTION 111

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
"Certification Depends on Only One Thing" - www.actualanswers.com 85 CompTIA CAS-001 Exam

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 112
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?

"Certification Depends on Only One Thing" - www.actualanswers.com 86 CompTIA CAS-001 Exam

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 113
Which of the following are the examples of the biometric identifiers? Each correct answer represents a complete solution, Choose three.

A. Iris scan
B. Voiceprint
C. Fingerprint
D. Subdermal chip

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sensitive PII means personally identifiable information, if it is lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. In Sensitive PII, complete social security numbers {SSN). alienregistration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint. or iris scan) can be considered.

Following are few additional examples include any grouping of information that consists of the individuals name or other unique identifier plus:
1.License number, passport number, or truncated SSN
2.Date of birth {for example, 4-March, 1960)
3.Citizenship or immigration status

"Certification Depends on Only One Thing" - www.actualanswers.com 87 CompTIA CAS-001 Exam

4.Financial information like account numbers or Electronic Funds Transfer information 5.Medical information 6.System authentication information like mother's maiden name, account passwords, or personal identification numbers (PINs)

QUESTION 114
You work as a security administrator for uCertify Inc. You are conducting a security awareness campaign for the employees of the organization. What information will you provide to the employees about the security awareness program?

Each correct answer represents a complete solution. Choose three.

A. It improves awareness of the need to protect system resources.
B. It improves the possibility for career advancement of the IT staff.
C. It enhances the skills and knowledge so that the computer users can perform their jobs more securely.
D. It constructs in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The purpose of security awareness, training, and education is to increase security by:
· Improving awareness of the need to protect system resources. · Enhancing the skills and knowledge so that the computer users can perform their jobs more securely.
· Constructing in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.
· Making computer system users aware of their security responsibilities and teaching them correct practices, which helps users change their behavior.

It also supports individual accountability because without the knowledge of the necessary security measures and how to use them, users cannot be truly accountable for their actions.

QUESTION 115
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 116
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 89 CompTIA CAS-001 Exam

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

QUESTION 117
You work as a Desktop Support Technician for uCertify Inc. A user reports that the security log on his Windows 7 computer is full. After analyzing, you observe that the security log is full of logon events, access, and other security events. The user does not want these events to be stored in the security log, what should you do to resolve the issue?

A. Clear the security log and assign some more space to it.
B. Add the user to the Power Users group
C. Upgrade the hard drive of the users computer.
D. Disable all auditing on the user's computer.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As the security log is full of the events occurring on the computer, it is clear that auditing is enabled on the system. You must disable all auditing on the users computer to resolve the issue. Answer options A and C are incorrect. By upgrading the hard drive of the computer, you can assign some more space to the security log but this will be a temporary solution. The security log will be filled up again because auditing is enabled.

Answer option B is incorrect. Adding the user to the Power user group will not solve the problem because auditing is enabled on the system and events continue to be stored in the security log.

QUESTION 118
Which of the following statements are true about Risk analysis? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

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

Explanation:

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

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

QUESTION 119
Which of the following steps are involved in a generic cost-benefit analysis process: Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: (none)
Explanation

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

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

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

QUESTION 120
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 121
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

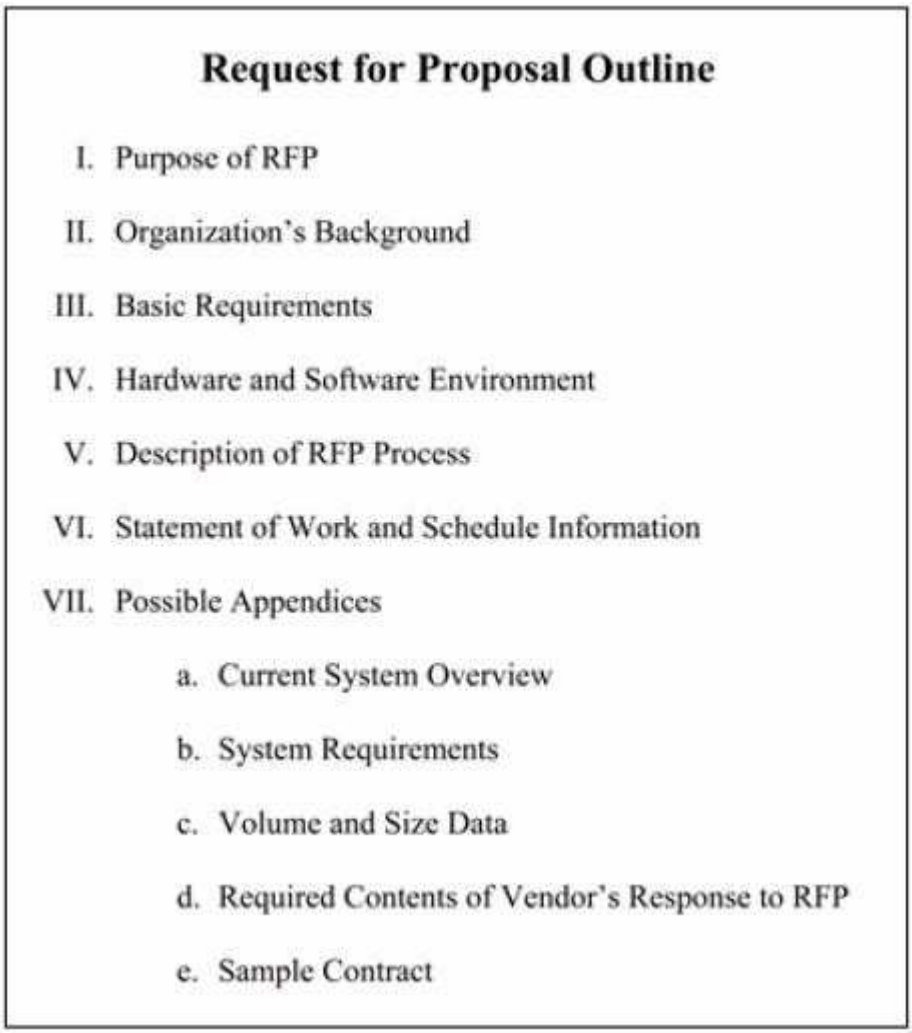
Explanation/Reference:
Explanation: Procurement planning involves preparing the documents required and determining the evaluation criteria for the contract award. Three common examples of procurement documents include:
· Requests for information (RFI)
· Requests for proposals (RFP)
· Requests for quotes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



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.

"Certification Depends on Only One Thing" - www.actualanswers.com 94 CompTIA CAS-001 Exam

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

QUESTION 122
Your manager has approached you regarding her desire to outsource certain functions to an external firm. The manager would like for you to create a document for sending to three vendors asking them for solutions for

these functions that your organization is to outsource. Which type of a procurement document will you create and send to the vendors to accomplish the task?

A. Request for Information
B. Invitation for Bid
C. Request for Proposal
D. Request for Quote

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to the scenario, you will create and send the Request for Proposal procurement document.

QUESTION 123
Which of the following is a meeting of minds between two or more legally competent parties, about their relative duties and rights regarding current or future performance?

A. Scope
B. Service Improvement Plan
C. Contract negotiation
D. Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An agreement is a meeting of minds between two or more legally competent parties, about their relative duties and rights regarding current or future performance. When people feel or think the same way about something, they agree. Sometimes it is important to write down or make a promise to what has been agreed upon. This is called an agreement. Agreements are common in law and business. For example, when a person takes a loan or hires someone to work, an

agreement is usually signed so everyone understands what must be done and in what time it must be done.

Answer option B is incorrect. The Service Improvement Plan (SIP) is a formal plan to implement improvements to services and IT processes. The SIP is used to manage and log improvement initiatives triggered by Continual Service Improvement. Generally, improvement initiatives are either of the following:
· Internal initiatives pursued by the service provider on his own behalf, for example to improve processes or make better use of resources.
· Initiatives which require the customer's cooperation, for example if some of the agreed service levels are found to be no longer adequate.

Answer option C is incorrect. Contract negotiation is a form of discussion held in person or by electronic means. The chief goal of contract negotiation is to come to a written agreement regarding a business matter. It handles the issues such as cost, timeframe, and whether there are any special considerations to take into account.

Answer option A is incorrect. Scope is defined in terms of process, organizing, system alternatives, and geography so that all parties understand what is being delivered. In project management, the term scope has two distinct uses: Project Scope and Product Scope. · Project Scope: The work that needs to be accomplished to deliver a product, service, or result with the specified features and functions.
· Product Scope: It describes the features and functions that characterize a product, service, or result.

QUESTION 124
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 125
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 126
Which of the following is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system?

A. Total cost of acquisition
B. Total cost of ownership

C. Total benefits of ownership
D. Activity-based costing
"Certification Depends on Only One Thing" - www.actualanswers.com 97 CompTIA CAS-001 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Total cost of ownership (TCO) is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system.

QUESTION 127
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 128
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
"Certification Depends on Only One Thing" - www.actualanswers.com 98 CompTIA CAS-001 Exam
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 129
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 130
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 131
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 132
Elaine is conducting an AAR after a hacker managed to breach the network security and steal data from the database server. Which of the following should not be part of the AAR?

A. Getting input from multiple perspectives
B. Describe what happened
C. Remain unbiased
D. Assessing who is responsible for the breach

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Assessing blame is counter productive. You do not want blame to be part of the process of the AAR.

Answer option C is incorrect. Any biases will keep you from seeing all the possible solutions. It is impossible to conduct a good AAR unless you are unbiased.

Answer option A is incorrect. The more perspectives that provide input, the more likely that creative answers are likely to be found.

"Certification Depends on Only One Thing" - www.actualanswers.com 101 CompTIA CAS-001 Exam

Answer option B is incorrect. The first step in an AAR is to accurately and completely describe what happened.

QUESTION 133
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 134
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 135
Susan is trying to find a solution that will verify emails come from the source claimed. Which of the following solutions is most likely to accomplish this?

A. Any hashing
B. AES encryption
C. SHA hashing
D. Digital signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Digital signatures encrypt with tine senders private key, then anyone with the public key can decrypt and verify the sender.

QUESTION 136
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 137
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 138
Which of the following elements of security means that the only authorized users are able to modify data?

"Certification Depends on Only One Thing" - www.actualanswers.com 104 CompTIA CAS-001 Exam

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 139
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 140
Each organization has a documented SDLC policy and guideline that supports its business needs and complements its unique culture. Which of the following should be documented in the SDLC guideline?

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

A. Reward points for stakeholder
B. System maintenance, security, and operational considerations
C. Requirement identification number
D. Project accomplishments
E. Specified outputs that provide essential information into system design
F. Decision points or control gates

Correct Answer: BDEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SDLC guideline offers utilities by documenting the following:
· Insight into the major activities and milestones
· Decision points or control gates
· Specified outputs that provide essential information into system design · Project accomplishments
· System maintenance, security, and operational considerations

QUESTION 141
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 142
Which of the following protocols is used by voice terminal to communicate with the VoIP server? Each correct answer represents a complete solution. Choose all that apply.

A. SIP
B. H.323
C. MGCP
D. RSTP

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The voice terminal communicates with the VoIP server using H.323, SIP and MGCP protocols. H.323 is a group of protocols defined by the International Telecommunication Union for multimedia conferences over Local Area Networks. The H.323 collection of protocols collectively may use up to two TCP connections and four to six UDP connections. H.323 inspection is used for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 application inspection does not support Network Address Translation between same-security-level interfaces.

Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a

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

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

Answer option D is incorrect. Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. RSTP is also known as the IEEE 802.iw. It provides a loop-free switching environment. Standard IEEE 802.1D-2004 incorporates

RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within 6 seconds.

QUESTION 143
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.
"Certification Depends on Only One Thing" - www.actualanswers.com 108 CompTIA CAS-001 Exam

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 144
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 145
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 146
Which of the following security services will you use for enabling message-level security for Web services?

A. WS-Security
B. WSRP security
C. WebLogic Server security
D. Trading Partner security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Web Service Security (WS-Security) is a security service that is used for enabling message- level security for Web services. For enabling this service, a user needs to ensure that the related

WSSE policy files are available to the Managed Servers. The SOAP messages that are passed between two or more Web services can be secured by WS-Security using security tokens, digital signatures, and encryption.

Answer option C is incorrect. The WebLogic Server security is used for enabling SSL transport traffic.

Answer option B is incorrect The WSRP security is used for enabling security for the Web Services for the WSRP feature of the WebLogic Portal.

Answer option D is incorrect. The Trading Partner security is used for enabling the security for trading partners.

QUESTION 147
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 148
Which of the following statements best describe the role of a programmer in an organization?

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

A. He writes, tests, debugs, and maintains the detailed instructions in computer programs.
B. He monitors and improves database performance and capacity.
C. He plans, co-ordinates and implements security measures for safety of the database.
D. He conceives, designs, and tests logical structures in order to solve computer problems.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A programmer writes, tests, debugs, and maintains the detailed instructions in computer programs that computers follow for performing their functions. He also conceives, designs, and tests logical structures in order to solve computer problems. A number of technical innovations in programming, advanced computing technologies, and sophisticated programming languages and tools have redefined the role of a programmer in an organization.

Answer options B and C are incorrect. A database administrator develops and designs database strategies, monitors and improves database performance and capacity, and plans for future expansion requirements. He also plans, co-ordinates and implements security measures for safety of the organization's database. A database administrator is also known as database coordinator or database programmer. He is closely related to the database analyst, database modeler, programmer analyst, and systems manager.

QUESTION 149
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 150
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 151
Which of the following are the benefits of public cloud computing? Each correct answer represents a complete solution. Choose three.

A. Sensitive data
B. Scalability
C. Automation

D. Elasticity

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the benefits of public cloud computing that you get with a private cloud computing:
· Reliability and predictability
· Automation (self healing and self-service)
· Scalability
· Elasticity

Answer option A is incorrect. In public cloud computing, sensitive data is not secure since sensitive data is shared beyond the corporate firewall.

QUESTION 152
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 153
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 154
SCADA stands for supervisory control and data acquisition. Which of the following statements are true about SCADA? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

QUESTION 155
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 156
Which of the following solutions best accomplishes storage integration?

"Certification Depends on Only One Thing" - www.actualanswers.com 117 CompTIA CAS-001 Exam

A. Virtualization
B. Cloud computing
C. Co-location
D. Raid 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cloud computing uses integrated storage across multiple servers, sometimes in diverse locations (such as Apples iCloud).

Answer option C is incorrect. Co-location involves placing all the servers in one location. There is no shared storage.

Answer option D is incorrect. Raid 5 is a method of having hard drive failover in a single server.

Answer option A is incorrect. Virtualized systems are usually completely isolated from each other, thus preventing storage integration.

QUESTION 157
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.

QUESTION 158
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 159
Mary is responsible for getting rid of old hard drives that are no longer used. It is important that all data be removed from the drive and none recoverable, but that the drive still be useable. Which of the following steps should she take before disposing of the drives?

A. Degauss the drive
B. Delete all data and defragment the drive.
C. Delete all data and do a high-level format of the drive.
D. Use a utility like Linux DD to overwrite all drive bits with zero's

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Linux DD command is even recommended for use in forensically wiping a drive. It will erase all data. It works at the bit level of the drive itself, changing all bits to zeros.

Answer option B is incorrect. Even with defragmenting, common undelete programs will be able to retrieve large amounts of data.

Answer option C is incorrect. Even with a high-level format, common undelete programs will be able to retrieve large amounts of data.

Answer option A is incorrect. Degaussing can damage the drive (it won't always, but it can) and render it unusable.

QUESTION 160
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 161
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 162
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 163
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 164
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 165
_____ is the concept that disclosure of the long-term secret keying material that is used to derive an agreed key does not compromise the secrecy of agreed keys that had previously been generated.

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

Correct Answer: C
Section: (none)
Explanation

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

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

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

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

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

QUESTION 166
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 167
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

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 168
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 169
Fred is a network administrator for an insurance company. Lately there has been an issue with the antivirus software not updating. What is the first thing Fred should do to solve the problem?

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

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

Correct Answer: B
Section: (none)
Explanation

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

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

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

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

QUESTION 170
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 126 CompTIA CAS-001 Exam

QUESTION 171
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 172
Continuous Monitoring is the fourth phase of the Security Certification and Accreditation process, which of the following activities can be involved in the Continuous Monitoring process?

Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Continuous monitoring in any system takes place after initial system security accreditation. It involves tracking changes to the information system that occur during its lifetime, and then determines the impact of those changes on the system security. Due to the necessary changes in hardware, software, and firmware during the lifetime of an information system, an evaluation ofthe results of these modifications has to be conducted to determine whether corresponding changes necessarily have to be made to security controls, to bring the system to the desired security state.

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

The Continuous Monitoring process involves the following three activities:

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

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

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

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

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

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

QUESTION 173
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 174
You are completing the requirements for vendor selection and need to create a procurement form that will ask the vendor to provide only a price for commercial-off-the-shelf solution. What type of procurement form will you need to provide to the vendor?

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

Correct Answer: D
Section: (none)
Explanation

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

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

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

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

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

QUESTION 175
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 176
Which of the following attacks are computer threats that try to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer?

A. FMS
B. Spoofing
C. Buffer overflow
D. Zero-day

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.

Answer option A is incorrect. The Fluhrer, Mantin, and Shamir (FMS) attack is a particular stream cipher attack, a dedicated form of cryptanalysis for attacking the widely-used stream cipher RC4. The attack allows an attacker to recover the key in an RC4 encrypted stream from a large number of messages in that stream. The FMS attack gained popularity in tools such as AirSnort and aircrack, both of which can be used to attack WEP encrypted wireless networks. Answer option C is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

Answer option B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc.

because forging the source IP address causes the responses to be misdirected.

QUESTION 177
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 178
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 132 CompTIA CAS-001 Exam

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 179
Which of the following counters measures the rate at which the bytes are sent through or received by a network?

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

D. Network Interface: Bytes/sec

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 180
Which of the following statements are true about Mean Time to Repair (MTTR)? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

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

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

QUESTION 181
Which of the following is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash?

A. Hashing
B. Non-repudiation

C. Code signing
D. Entropy
"Certification Depends on Only One Thing" - www.actualanswers.com 134 CompTIA CAS-001 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not beenalteredor corrupted since it was signed by use of a cryptographic hash.

Overview
Code signing can provide several valuable features. The most common use of code signing is to provide security when deploying: in some languages, it can also be used to help prevent namespace conflicts. Almost every code signing implementation will provide some sort of digitalsignature mechanism to verify the identity of the author or build system, and a checksum to verify that the object has not been modified. It can also be used to provide versioning information about an object or to store other meta data about an object.

Providing security
Many code signing implementations will provide a way to sign the code using private and public key systems, similar to the process employed by SSL or SSH. For example, in the case of .NET, the developer uses a key to sign his libraries or executables each time he builds. This key will be unique to a developer or group or sometimes per application or object. The developer can either generate this key on his own or obtain one from a trusted certificate authority (CA).

It is particularly valuable in distributed environments, where the source of a given piece of code may not be immediately evident - for example Java applets. ActiveX controls and other active web and browser scripting code. Another major usage is to safely provide updates and patches to existing software. Most Linux distributions, as well as both Apple Mac OS X and Microsoft Windows update services use code signing to ensure that it is not possible to maliciously distribute code via the patch system. It allows them to not have to worry about distribution security, such as mirror sites which may not be under the authors complete control, or any other intermediate piece of the deployment.

Trusted identification using a certificate authority (CA) The public key used for code signing should be traceable back to a trusted root authority, preferably using a secure public key infrastructure (PKI). This does not ensure that the code itself can be trusted, only that it comes from the stated source or more explicitly, from a particular private key. A certificate authority provides a root trust level which is able to assign trust to others by proxy. If a user is set to trust one of these certificate authorities and receives an executable signed with a key generated by that CA. he can choose to trust the executable by proxy. In many frameworks and operating systems, a number of existing publicly trusted authorities will be pre- installed such as Version, TC TrustCenter, COMOOO, GoDaddy and GlobalSign. When inside a large group of users, such as a large company, it is commonplace to employ a private internal certificate authority suitable for providing the same features of public certificate authority but for

"Certification Depends on Only One Thing" - www.actualanswers.com 135 CompTIA CAS-001 Exam

deploying signed objects internally.

Alternative to CAs
The other model is where developers can choose to provide their own self-generated key. In this scenario, the user would normally have to obtain the public key in some fashion directly from the developer to verify the object is from him for the first time. Many code signing systems will store the public key inside the signature. Some software frameworks and OSs that check the codes signature before executing will allow you to choose to trust that developer from that point on after the first run. An application developer can provide a similar system by including thepublic keys with the installer. The key can then be used to ensure that any subsequent objects that need to run, such as upgrades, plugins, or another application, are all verified as coming from that same developer.

Problems
Like any security measure, code signing can be defeated. Users can be tricked into running unsigned code, or even into running code that refuses to validate, and the system only remains secure as long as the private key remains private.
It is also important to note that code signing does not protect the end user from any malicious activity or unintentional software bugs by the software author - it merely ensures that the software has not been modified by anyone other than the author.

Implementations
IBM's Lotus Notes has had PKI signing of code from Release 1 - and both client and server software have execution control lists to control what levels of access to data, environment and file system are permitted for given users, individual design elements, including active items such as scripts, actions and agents, are always signed using the editors ID file, which includes both the editor's and the domain's public keys. Core templates such as the mail template are signed with a dedicated ID held by the Lotus template development team.

Signed JavaScript is also popular: signed scripts are allowed to perform additional actions such as cross-domain referencing.

Microsoft implements a form of code signing based on Authenticode provided for Microsoft tested drivers. Since drivers run in the kernel, they can destabilize the system or open the system to security holes. For this reason. Microsoft tests drivers submitted to its WHQL program. After the driver has passed, Microsoft signs that version of the driver as being safe. On 32-bit systems only, installing drivers that are not validated with Microsoft is possible after accepting to allow the installation in a prompt warning the user that the code is unsigned. For .NET managed code, there is an additional mechanism called Strong Name Signing that uses Public/Private keys and SHA1 hash as opposed to Certificates. However, Microsoft discourages reliance on Strong Name Signing as a replacement for Authenticode

"Certification Depends on Only One Thing" - www.actualanswers.com 136 CompTIA CAS-001 Exam

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

QUESTION 182
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 183
Which of the following can monitor any application input, output, and/or system service calls made from, to, or by an application?

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

Correct Answer: C
Section: (none)
Explanation

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

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

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

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

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

Answer option B is incorrect. A dynamic packet-filtering firewall is a fourth generation firewall technology. It is also known as a stateful firewall. The dynamic packet-filtering firewall tracks the state of active connections, and then determines which network packets are allowed to enter through the firewall. It records session information, such as IP addresses and port numbers to implement a more secure network. The dynamic packet-filtering firewall operates at Layer3, Layer4, and Layers.

QUESTION 184
Which of the following security principles would be most helpful in preventing privilege escalation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By assigning the least privileges needed for each user, the odds of privilege escalation are reduced. The principle of least privilege gives a user only those privileges that are essential to do his/her work. In information security, computer science, and other fields, the principle of least privilege is also known as the principle of

minimal privilege or least privilege. It defines that in a particular abstraction layer of a computing environment, every module must be able to access only the information and resources that are essential for its legitimate purpose, it requires that each subject in a system be granted the most restrictive set of privileges required for authorized tasks.

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

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

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

QUESTION 185
John is hosting several Web sites on a single server. One is an e-commerce site that handles credit card transactions, while the other sites do not handle credit card data. Does this present a security problem, and if so, what?

A. There is no issue with different types of sites on one server
B. Credit card processing requires HIPAA compliance, the other sites do not
C. Credit card processing requires PCI compliance, the other sites do not
D. The other sites may allow privilege escalation to the e-commerce site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PCI requirements are very specific. When commingling the different sites, they will all need to be PCI compliant.

Answer option B is incorrect. Credit cards require PCI compliance, not HIPAA.

Answer option A is incorrect. There can be significant security concerns.

"Certification Depends on Only One Thing" - www.actualanswers.com 139 CompTIA CAS-001 Exam

Answer option D is incorrect. Privilege escalation is not the most significant concern.

QUESTION 186
Which of the following is a key agreement protocol that allows two users to exchange a secret key over an insecure medium without any prior secrets?

A. One-way encryption
B. XML encryption
C. SecureFiles Encryption
D. Diffie-Hellman encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Diffie-Hellman encryption was developed by Diffie and Hellman in 1976 and published in the paper "New Directions in Cryptography." It is a key agreement protocol (also called exponential key agreement) that allows two users to exchange a secret key over an insecure medium (such as the Internet) without any prior secrets.

The original protocol had two system parameters, i.e.. p and g. They are both public and may be used by all users in a system. The Diffie-Hellman key exchange was vulnerable to a man-in-the-middle attack, as the Diffie-Hellman key exchange does not authenticate the participants.

The current form of the Diffie-Hellman protocol (also known as the authenticated Diffie-Hellman key agreement protocol, or the Station-to-Station (STS) protocol), was developed by Diffie, Van Oorschot, and Wiener in 1992 to overcome the man-in-the-middle attack. This is achieved by allowing the two parties to authenticate themselves to each other by the use of digital signatures and public-key certificates. The Diffie-Hellman protocol is an example of a much more general cryptographic technique, the common element being the derivation of a shared secret value (that is, key) from one party's public key and another party's private key. The parties'' key pairs may be generated anew at each run of the protocol as in the original Diffie-Hellman protocol. The public keys may be certified so that the parties can be authenticated and there may be a combination of these attributes.

Answer option A is incorrect. One-way encryption is also known as hash function. It is used to determine whether the data has changed. The message gets converted into a numerical value. The recipient then verifies the hash value using a known algorithm. This method checks the integrity of messages but it does not provide confidentiality.

Answer option B is incorrect. XML encryption is used to encrypt the entire XML document or its

selected portions. An XML document has different portions that can be encrypted, which are as follows:
· Complete XML document
· A resource reference that is provided outside the XML document · The content portions of an XML document
· Elements and all their sub-elements

Answer option C is incorrect. SecureFiles Encryption extends the capability of Transparent Data Encryption (TDE) by encrypting LOB data. In this encryption, the data is encrypted using Transparent Data Encryption (TDE) and allows encrypted data to be stored securely. SecureFiles Encryption allows random reads and writes on the encrypted data. Automatic key management issupported by Oracle database for all LOB columns within a table and transparently encrypts/decrypts data, backups, and redo/undo log files.

QUESTION 187
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 188
Which of the following is a deterministic algorithm to generate a sequence of numbers with little or no discernible pattern in the numbers, apart from broad statistical properties?

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

Correct Answer: C
Section: (none)
Explanation

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

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

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

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

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

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

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

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

QUESTION 189
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

"Certification Depends on Only One Thing" - www.actualanswers.com 143 CompTIA CAS-001 Exam

· 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 190
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.

"Certification Depends on Only One Thing" - www.actualanswers.com 144 CompTIA CAS-001 Exam

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 191
Which of the following statements best describe the responsibilities of a facility manager in an organization? Each correct answer represents a complete solution. Choose three.

A. Analyze and manage project in order to provide desired output in given deadlines.
B. Develop written physical security plans for critical infrastructures.
C. Improve current activities with minimum interruption for excellent result.
D. Make an attractive plan with the help of different business strategies.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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. He makes a text document that includes proposals for client or contractor.

The responsibilities of a facility manager are as follows:
· Analyze and manage project in order to provide desired output in given deadlines.
· Plan new offers with reliability and availability.

"Certification Depends on Only One Thing" - www.actualanswers.com 145 CompTIA CAS-001 Exam

· Notify all expenses in providing services and goods used in project completion and then, find out the profit earned in a particular project.
· Make an attractive plan with the help of different business strategies. · Improve current activities with

minimum interruption for excellent result. · Check health and security point before approval of a building. · Encourage all team members and maintain interaction between them.

Answer option B is incorrect. It is the responsibility of a physical security manager.

QUESTION 192
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 193
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 194
Which of the following are the primary rules to apply RBAC-based delegation for a user on a network? Each correct answer represents a complete solution. Choose all that apply.

A. Authorization of Role
B. Assignment of Roles
C. Assignment of Permission
D. Authorization of Permission

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Role-based access control (or role-based security) is an approach to restricting system access to authorized users within an organization. In role-based access control, roles are created for various job functions. To perform certain operations, permissions are assigned to specific roles rather than individuals. Since users are not assigned permission directly, management of individual user rights becomes a matter of simply assigning appropriate roles to the user. There are three primary rules defined for RBAC:
· Assignment of Roles: A subject can exercise a permission only if the subject has selected or been assigned a role.
· Authorization of Role: A subjects active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized. · Authorization of Permission: A subject can exercise a permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

According to the requirements of an organization, additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.

Answer option C is incorrect. In role-based access control, no permission is assigned to a user directly. Instead, permissions are assigned to a role and that role is assigned to the user.

"Certification Depends on Only One Thing" - www.actualanswers.com 147 CompTIA CAS-001 Exam

QUESTION 195
In which of the following can a user access resources according to his role in the organization?

A. Discretionary access control
B. Network-based access control
C. Role-based access control
D. Mandatory Access Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model.

Answer option A is incorrect. Discretionary access control (DAC) is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.

Two important concepts in DAC are as follows:
· File and data ownership: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
· Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

Access controls may be discretionary in ACL-based or capability-based access control systems.

Note: In capability-based systems, there is no explicit concept of owner, but the creator of an object has a similar degree of control over its access policy.

Answer option D is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the

appropriate permission.

Answer option B is incorrect. There in no such access control as Network-based access control (NBAC).

QUESTION 196
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.

QUESTION 197
Which of the following processes is used to ensure that standardized methods and procedures are used for efficient handling of all changes?

A. Exception management
B. Configuration Management
C. Risk Management

D. Change Management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 (CIs)" 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 Answer option B is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

Answer option A is incorrect. Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business.

Answer option C is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager.

Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises', so at IT Process

Maps we decided to assign clear responsibilities for managing risks.

QUESTION 198
Which of the following are the main aims of Change Management?

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

A. Reduction in back-out activities
B. Economic utilization of resources involved in the change
C. Tracking all of the individual Configuration Items (CI) in an IT system
D. Minimal disruption of services

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 199
Which of the following saves time and efforts of creating own programs and services by purchasing the products from a third-party vendor?

A. Collaboration platform
B. End-to-end solution
C. Change Management
D. COTS product

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 A 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 a wiki. 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

Answer option B is incorrect. 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 customers requirement and no other supplier is required to be involved.

QUESTION 200
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

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 201
In which of the following phases of the System Development Life Cycle (SDLC) is the IT system designed, purchased, and programmed?

A. Operation/Maintenance

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 202
Which of the following are the key security activities for the initiation phase? Each correct answer represents a complete solution. Choose two.

A. Determination of privacy requirements.
B. Perform functional and security testing.
C. Initial delineation of business requirements in terms of confidentiality, integrity, and availability.
D. Analyze security requirements.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation: Answer options C and A are correct.

Key security activities for the initiation phase are as follows:

"Certification Depends on Only One Thing" - www.actualanswers.com 154 CompTIA CAS-001 Exam

· Initial definition of business requirements in terms of confidentiality, integrity, and availability · Determination of information categorization and identification of known special handling requirements in transmitting, storing, or creating information · Determination of privacy requirements

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

QUESTION 203
The help desk is flooded with calls from users who receive an e-mail warning about a new virus. The e-mail instructs them to search and delete a number of files from their systems. Many of them attempt to reboot the systems after deleting the specified files and find that the systems are not rebooting properly, which of the following types of attacks has occurred?

A. Hoax
B. Phishing
C. Spam
D. Pharming

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hoax messages may warn of emerging threats that do not exist. These messages instruct users to delete certain files in order to ensure their security against a new virus, while actually only rendering the system more susceptible to later viral agents.

Answer option D is incorrect. Pharming is an attack made by a hacker in which the traffic of a Website is redirected to another bogus Website.

Answer option B is incorrect. Phishing is an attempt to obtain sensitive information by masquerading as a trustworthy entity using an electronic communication, such as e-mail. Answer option C is incorrect. Spam is an unwanted e-mail communication.

"Certification Depends on Only One Thing" - www.actualanswers.com 155 CompTIA CAS-001 Exam

QUESTION 204
You work as a Security Administrator for uCertify Inc. The company has a TCP/IP based network and uses the WS-Security service to enable message-level security for Web services. Which of the following mechanisms does it describe?

Each correct answer represents a complete solution. Choose three.

A. How to attach security tokens to ascertain the identity of sender.
B. How to encrypt SOAP messages to assure confidentiality.
C. How to sign SOAP messages to assure integrity.
D. How to provide a guarantee of security.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The WS-Security describes the following mechanisms:
· How to sign SOAP messages to assure integrity.
· How to encrypt SOAP messages to assure confidentiality. · How to attach security tokens to ascertain the identity of sender.

QUESTION 205
Which of the following protocols encrypt the segments of network connections at the Transport Layer end-to-end? Each correct answer represents a complete solution. Choose two.

A. SSL
B. HTTPS
C. SNMP
D. TLS

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Transport Layer Security (TLS) and its predecessor. Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks, such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end- to-end.

Several versions of the protocols are in widespread use in applications like web browsing,

electronic mail,Internet faxing, instant messaging and voice-over-IP (VoIP).

The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. TLS provides RSA security with 1024 and 2048 bit strengths.

In typical end-user/browser usage, TLS authentication is unilateral: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous).

TLS also supports the more secure bilateral connection mode (typically used in enterprise applications), in which both ends of the "conversation"' can be assured with whom they are communicating (provided they diligently scrutinize the identity information in the other party's certificate). This is known as mutual authentication, or 2SSL. Mutual authentication requires that the TLS client-side also hold a certificate (which is not usually the case in the end-user/browser scenario). Unless, that is. TLS-PSK. the Secure Remote Password (SRP) protocol or some other protocol is used that can provide strong mutual authentication in the absence of certificates.

Typically, the key information and certificates necessary for TLS are handled in the form of X.509 certificates, which define required fields and data formats. SSL operates in modular fashion. It is extensible by design, with support for forward and backward compatibility and negotiation between peers.

Answer option B is incorrect. Hypertext Transfer Protocol Secure (HTTPS) is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site. When an SSL connection is established between a Web browser and a Web server,HTTPS should be entered, instead of HTTP, as the protocol type in the URL. HTTPS uses TCP port 443 as the default port.

Answer option C is incorrect. The Simple Network Management Protocol (SNMP) allows a monitored device (for example, a router or a switch) to run an SNMP agent. This protocol is used for managing many network devices remotely.

When a monitored device runs an SNMP agent, an SNMP server can then query the SNMP agent running on the device to collect information such as utilization statistics or device configuration information. An SNMP-managed network typically consists of three components: managed devices, agents, and one or more network management systems.

QUESTION 206
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 207
Which of the following are the benefits of the Single sign-on? Each correct answer represents a complete solution. Choose three.

A. Reducing password fatigue from different user name and password combinations
B. Increasing IT costs due to lower number of IT help desk calls about passwords
C. Centralized reporting for compliance adherence

D. Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the benefits of the Single sign-on:
· Reduces phishing success, because users are not trained to enter password everywhere without thinking.
· Reducing password fatigue from different user name and password combinations. · Reducing time spent re-entering passwords for the same identity. · Can support conventional authentications, such as windows credentials (i.e., username/password).
· Reducing IT costs due to lower number of IT help desk calls about passwords. · Security on all levels of entry/ exit/access to systems without the inconvenience of re-prompting users.
· Centralized reporting for compliance adherence.

QUESTION 208
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:

"Certification Depends on Only One Thing" - www.actualanswers.com 159 CompTIA CAS-001 Exam

· Data aggregation
· Correlation
· Alerting
· Dashboard
· Compliance
· Retention

"Certification Depends on Only One Thing" - www.actualanswers.com 160