CA1-001 Q&As

CompTIA Advanced Security Practitioner (CASP) Beta Exam

Pass CompTIA CA1-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/CA1-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

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 2

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

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 3

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

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 4

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

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

Budget management

Grants management

Salary administration

Property management

Purchasing

Handling cash

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

Answer option A is incorrect. The responsibilities of HR (Human Resource) depend on the size of the organization. HR directors and HR managers head up several different departments that are 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 5

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

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 6

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

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 7

Bob 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. Digital signatures

B. AES encryption

C. SHA hashing

D. Any hashing

Correct Answer: A

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

QUESTION 8

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

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 9

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

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.

QUESTION 10

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

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

The SIEM capabilities are as follows:

Data aggregation

Correlation

Alerting

Dashboard

Compliance

Retention

QUESTION 11

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

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 12

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

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.