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.pass4itsure.com/CA1-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

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 2

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

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 3

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

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 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.

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.

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 4

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

Answer options C and A are correct.

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

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 5

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

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.