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.lead4pass.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

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 2

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

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 3

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

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 GSSAPI Negotiation 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 GSSAPI mechanisms 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 4

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

Correct Answer: A

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 5

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

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