CA1-001^Q&As^

CompTIA Advanced Security Practitioner (CASP) Beta Exam

QUESTION 1

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

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 2

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

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). alien registration 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

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 3

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

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 4

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

A. It allows the user to install and run more advanced applications based on a specific platform.

B. It can be simple software-based Softphones or purpose-built hardware devices that appear much like an ordinary telephone or a cordless phone.

C. It allows telephone calls to be made over an IP network.

D. It is a mobile phone with advanced PC like capabilities.

Correct Answer: AD

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 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:

QUESTION 5

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

Each correct answer represents a complete solution. Choose three.

A. Security control monitoring

B. Status reporting and documentation

C. Configuration Management and Control

D. Network impact analysis

Correct Answer: ABC

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.

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.