DUMPSBOSS.

Advanced SOA Security

SOA S90.19

Version Demo

Total Demo Questions: 10

Total Premium Questions: 83

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which of the following statements regarding the usage of security tokens for authentication and authorization are true?

A. Security tokens can be validated without resorting to pre-shared secrets.

B. Security tokens issued by a token issuer in the same security domain can be used with a different token issuer in a different security domain in order to get access to services in that domain.

C. Security token issuance and cancellation are done by the relying party.

D. Security tokens can only be issued by a legitimate token issuer.

ANSWER: A B

QUESTION NO: 2

The exception shielding logic resulting from the application of the Exception Shielding pattern can be centralized by applying which additional pattern?

A. Message Screening

B. Trusted Subsystem

C. Service Perimeter Guard

D. None of the above.

ANSWER: C

QUESTION NO: 3

A service composition is made up of services from a particular domain service inventory. All of the services belonging to the domain service inventory are deployed on the same server. Service A is part of the same domain inventory but is not part of this service composition. Service A becomes a victim of an XML parser attack resulting in its unavailability. However, because the services in the service composition rely on the same XML parser used by Service

A. the service composition can also be affected by this attack.

True

B. False

ANSWER: A

QUESTION NO: 4

Service A contains reporting logic that collects statistical data from different sources in order to produce a report document. One of the sources is a Web service that exists outside of the organizational boundary. Some of Service A's service consumers are encountering slow response times and periods of unavailability when invoking Service

A. While investigating the cause, it has been discovered that some of the messages received from the external Web service contain excessive data and links to files (that are not XML schemas or policies). What can be done to address this issue?

define cardinality in message schemas

B. correlate request and response messages across different services

C. use precompiled XPath expressions

D. avoid downloading XML schemas at runtime

ANSWER: A D

QUESTION NO: 5

The application of the Message Screening pattern can help avoid which of the following attacks?

A. Buffer overrun attack

B. XPath injection attack

C. SQL injection attack

D. Insufficient authorization attack

ANSWER: A B C

QUESTION NO: 6

The use of derived keys is based on symmetric encryption. This is similar to asymmetric encryption because different keys can be derived from a session key and used separately for encryption and decryption.

A. True

B. False

ANSWER: B

QUESTION NO: 7

Which of the following are types of security sessions?

A. Authentication

B. Authorization

C. asymmetric key agreement

D. single sign-on

ANSWER: A D

QUESTION NO: 8

A malicious passive intermediary intercepts messages sent between two services. Which of the following is the primary security concern raised by this situation?

A. The integrity of the message can be affected.

B. The confidentiality of the message can be affected.

C. The reliability of the message can be affected.

D. The availability of the message can be affected.

ANSWER: B

QUESTION NO: 9

Service A's logic has been implemented using managed code. An attacker sends an XML bomb to Service

A. As a result, Service A's memory consumption started increasing at an alarming rate and then decreased back to normal. The service was not affected by this attack and quickly recovered. Which of the following attacks were potentially avoided?

XML parser attack

B. Buffer overrun attack

C. Insufficient authorization attack

D. Denial of service

ANSWER: A D

QUESTION NO: 10

An alternative to using a _____ is to use a _____.

A. Public key, private key

B. Digital signature, symmetric key

C. Public key, key agreement security session

D. Digital signature, asymmetric key

ANSWER: C