



Free Questions for S90.19 by dumpshq

Shared by Lang on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Service A contains a comprehensive message screening routine that can consume a lot of system resources. Service consumers are reporting that sometimes Service A becomes non-responsive, especially after it receives a message containing a large amount of content. This may be an indication of which types of attacks?

Options:

- A- XML parser attack
- B- Denial of service attack
- C- Insufficient authorization
- D- XPath injection

Answer:

A, B

Question 2

Question Type: MultipleChoice

Service A is a Web service that accesses the Student table in a shared database in order to store XML-based student records. When invoked, the GetStudent operation of Service A uses a Student ID value to retrieve the record of a single student by executing an XPath query. An attacker sends a malicious message that manipulates the XPath query to return all the student records. Which of the following attacks was carried out?

Options:

- A- XML parser attack
- B- SQL injection attack
- C- XPath injection attack
- D- None of the above

Answer:

C

Question 3

Question Type: MultipleChoice

The Service Perimeter Guard pattern is applied to position a perimeter service outside of the firewall. The firewall only permits the perimeter service to access services within a specific service inventory. Which of the following statements describes a valid problem with this security architecture?

Options:

- A-** The Trusted Subsystem pattern was not applied to the perimeter service.
- B-** The perimeter service needs to be located inside the firewall and the firewall needs to be configured so that only known service consumers have access to the service inventory.
- C-** The Service Perimeter Guard pattern cannot be applied to a service outside of a service inventory.
- D-** None of the above

Answer:

D

Question 4

Question Type: MultipleChoice

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

Options:

- A- Buffer overrun attack
- B- XPath injection attack
- C- SQL injection attack
- D- Insufficient authorization attack

Answer:

A, B, C

Question 5

Question Type: MultipleChoice

Within a certain service activity, two services are using certificates in order to guarantee the integrity of messages. With every message exchange, certificates are sent and received. These certificates are checked against an external Certificate Authority (CA) in order to verify whether or not they have been revoked. The current security architecture is suffering from increased latency resulting from the extra communication required with the CA. How can this problem be addressed without compromising message integrity?

Options:

- A-** WS-Trust based SAML tokens can be used via an authentication broker.
- B-** WS-Secure-Conversation security context tokens can be used together with session keys and symmetric cryptography.
- C-** The security architecture can be redesigned so that the CA is only accessed for the first message exchange.
- D-** None of the above

Answer:

A

Question 6

Question Type: MultipleChoice

A certain service becomes a victim of an insufficient authorization attack. This service acts as a trusted subsystem for an entire service inventory. Which of the following are under threat as a result of this attack?

Options:

- A-** The core service logic

- B- The underlying resources accessed by the service
- C- Other services in the service inventory
- D- All of the above.

Answer:

D

Question 7

Question Type: MultipleChoice

A common alternative to _____ is the use of a _____.

Options:

- A- Public key cryptography, private key
- B- Digital signatures, symmetric key
- C- Public key cryptography, public key
- D- Private keys, digital signatures

Answer:

C

Question 8

Question Type: MultipleChoice

Message screening logic and exception shielding logic can co-exist in a single perimeter guard service.

Options:

A- True

B- False

Answer:

A

Question 9

Question Type: MultipleChoice

A service uses specialized screening logic that compares the size of a message against a maximum allowable size value. This value is specified for an incoming request message for a specific service capability. Upon a mismatch, the service rejects the request message and instead generates an error message. What type of attack has this security architecture not addressed?

Options:

- A- XML parser attack
- B- Buffer overrun attack
- C- Exception shielding attack
- D- None of the above

Answer:

D

To Get Premium Files for S90.19 Visit

<https://www.p2pexams.com/products/s90.19>

For More Free Questions Visit

<https://www.p2pexams.com/arcitura-education/pdf/s90.19>

