Free Questions for SSCP by certsdeals

Shared by Pratt on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is not a component of a Operations Security 'triples'?

Options:

A) Asset

B) Threat

C) Vulnerability

D) Risk

Answer:

D

Explanation:

The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.

Source: KRUTZ, Ronald L. &amp; VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley &amp; Sons, Page 216.

Question 2

Question Type: MultipleChoice

Which of the following is an IDS that acquires data and defines a 'normal' usage profile for the network or host?

Options:

A) Statistical Anomaly-Based ID

B) Signature-Based ID

C) dynamical anomaly-based ID

D) inferential anomaly-based ID

Answer:

A

Explanation:

Statistical Anomaly-Based ID - With this method, an IDS acquires data and defines a 'normal' usage profile for the network or host that is being monitored.

Source: KRUTZ, Ronald L. &amp; VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley &amp; Sons, Page 49.

Question 3

Question Type: MultipleChoice

What does 'residual risk' mean?

Options:

A) The security risk that remains after controls have been implemented

B) Weakness of an assets which can be exploited by a threat

C) Risk that remains after risk assessment has has been performed

D) A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Answer:

A

Explanation:

Residual risk is 'The security risk that remains after controls have been implemented' ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. 'Weakness of an assets which can be exploited by a threat' is vulnerability. 'The result of unwanted incident' is impact. Risk that remains after risk analysis has been performed is a distracter.

Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

Question 4

Question Type: **MultipleChoice**

A X.509 public key certificate with the key usage attribute 'non repudiation' can be used for which of the following?

Options:

A) encrypting messages

B) signing messages

C) verifying signed messages

D) decrypt encrypted messages

Answer:

C

Explanation:

References: RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide.

Question 5

Question Type: MultipleChoice

Which of the following can best define the 'revocation request grace period'?

Options:

A) The period of time allotted within which the user must make a revocation request upon a revocation reason

B) Minimum response time for performing a revocation by the CA

C) Maximum response time for performing a revocation by the CA

D) Time period between the arrival of a revocation request and the publication of the revocation information

Answer:

D

Explanation:

The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.

A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices.

If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

Question 6

Question Type: **MultipleChoice**

Which of the following can best define the 'revocation request grace period'?

Options:

A) The period of time allotted within which the user must make a revocation request upon a revocation reason

B) Minimum response time for performing a revocation by the CA

C) Maximum response time for performing a revocation by the CA

D) Time period between the arrival of a revocation request and the publication of the revocation information

Answer:

D

Explanation:

The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.

A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices.

If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

Question 7

Question Type: MultipleChoice

Which of the following is an IDS that acquires data and defines a 'normal' usage profile for the network or host?

Options:

A) Statistical Anomaly-Based ID

B) Signature-Based ID

C) dynamical anomaly-based ID

D) inferential anomaly-based ID

Answer:

A

Explanation:

Statistical Anomaly-Based ID - With this method, an IDS acquires data and defines a 'normal' usage profile for the network or host that is being monitored.

Source: KRUTZ, Ronald L. &amp; VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley &amp; Sons, Page 49.

Question 8

Question Type: MultipleChoice

A X.509 public key certificate with the key usage attribute 'non repudiation' can be used for which of the following?

Options:

A) encrypting messages

B) signing messages

C) verifying signed messages

D) decrypt encrypted messages

Answer:

C

Explanation:

References: RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide.

Question 9

Question Type: **MultipleChoice**

Which of the following is not a component of a Operations Security 'triples'?

Options:

A) Asset

B) Threat

C) Vulnerability

D) Risk

Answer:

D

Explanation:

The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.

Source: KRUTZ, Ronald L. &amp; VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley &amp; Sons, Page 216.

Question 10

Question Type: **MultipleChoice**

What does 'residual risk' mean?

Options:

A) The security risk that remains after controls have been implemented

B) Weakness of an assets which can be exploited by a threat

C) Risk that remains after risk assessment has has been performed

D) A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Answer:

A

Explanation:

Residual risk is 'The security risk that remains after controls have been implemented' ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. 'Weakness of an assets which can be exploited by a threat' is vulnerability. 'The result of unwanted incident' is impact. Risk that remains after risk analysis has been performed is a distracter.

Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.