156-110^{Q&As}

Check Point Certified Security Principles Associate (CCSPA)

Pass CheckPoint 156-110 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/156-110.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

_____ can mimic the symptoms of a denial-of-service attack, and the resulting loss in productivity can be no less devastating to an organization.

A. ICMP traffic

B. Peak traffic

C. Fragmented packets

D. Insufficient bandwidth

E. Burst traffic

Correct Answer: D

QUESTION 2

Which of the following calculations is used when selecting countermeasures?

A. Annualized Rate of Occurrence

B. Single Loss Expectancy

C. Annualized Loss Expectancy

D. Business Impact Analysis

E. Business Continuity Plan

Correct Answer: C

QUESTION 3

Why does the (ISC)2 access-control systems and methodology functional domain address both the confidentiality and integrity aspects of the Information Security Triad? Access-control systems and methodologies:

A. are required standards in health care and banking.

B. provide redundant systems and data backups.

C. control who is allowed to view and modify information.

D. are academic models not suitable for implementation.

E. set standards for acceptable media-storage devices.

Correct Answer: C

QUESTION 4

Virtual corporations typically use a(n) _____ for maintaining centralized information assets.

A. Off-line repository

B. Floppy disk

C. Data warehouse

D. CD-ROM burner

E. Colocation

Correct Answer: E

QUESTION 5

Distinguish between the role of the data owner and the role of the data custodian. Complete the following sentence. The data owner is the:

A. department in the organization responsible for the data\\'s physical storage location. The data custodian is anyone who has access the data for any reason.

B. person or entity who accesses/and or manipulates data or information, in the course of assigned duties. The data custodian is a person or process with the appropriate level of privilege to access the data.

C. person or entity ultimately responsible for the security of an information asset. The data custodian is the person or entity responsible for imposing and enforcing policies and restrictions, dictated by the data owner.

D. person or process that originally creates the information. The data custodian is a role that shifts to any person or process currently accessing the data, and passes to the next person or process to access the data.

E. person or entity responsible for imposing and enforcing policies and restrictions, dictated by the functional user. The data custodian is a person or process who accesses and/or manipulates the information.

Correct Answer: C

QUESTION 6

Why should the number of services on a server be limited to required services?

A. Every open service represents a potential vulnerability.

B. Closed systems require special connectivity services.

C. Running extra services makes machines more efficient.

D. All services are inherently stable and secure.

E. Additional services make machines more secure.

Correct Answer: A

QUESTION 7

At ABC Corporation, access to critical information resources, such as database and e-mail servers, is controlled by the information-technology (IT) department. The supervisor in the department grants access to printers where the printer is located. Managers grant and revoke rights to files within their departments\' directories on the file server, but the IT department controls who has access to the directories. Which type of access-management system is in use at ABC Corporation?

A. Centralized access management

B. Role-based access management

C. Hybrid access management

D. Decentralized access management

E. Privileged access management

Correct Answer: C

QUESTION 8

The items listed below are examples of _____ controls.

*Smart cards *Access control lists *Authentication servers *Auditing

A. Role-based

B. Administrative

C. Technical

D. Physical

E. Mandatory

Correct Answer: C

QUESTION 9

You are a system administrator for a pool of Web servers. The vendor who sells your Web server posts a patch and sample exploit for a newly discovered vulnerability. You will take all of the actions listed below. Which of the following actions should you take first?

A. Run the sample exploit against a test server.

B. Run the sample exploit against a production server.

C. Apply the patch to all production servers.

D. Test the patch on a production server.

E. Test the patch on a non-production server.

Correct Answer: A

QUESTION 10

Operating-system fingerprinting uses all of the following, EXCEPT _____, to identify a target operating system.

A. Sequence Verifier

B. Initial sequence number

C. Address spoofing

D. Time to Live

E. IP ID field

Correct Answer: C

QUESTION 11

_____ is a smaller, enhanced version of the X.500 protocol. It is used to provide directory-service information. (Choose the BEST answer.)

A. Lightweight Directory Access Protocol

B. X.400 Directory Access Protocol

C. Access control list

D. Lightweight Host Configuration Protocol

E. Role-based access control

Correct Answer: A

QUESTION 12

A(n) _____ occurs when intrusion-detection measures fail to recognize suspicious traffic or activity.

A. False positive

B. False negative

C. CIFS pop-up

D. Threshold

E. Alarm

Correct Answer: B

QUESTION 13

Embedding symbols in images or common items, such as pictures or quilts, is an example of _____.

A. Espionage

B. Transposition cipher

C. Key exchange

D. Arithmancy

E. Steganography

Correct Answer: E

QUESTION 14

_____ intrusion-detection systems learn the behavior of a machine or network, and create a baseline.

A. Behavioral analysis

B. Statistical anomaly

C. Network

D. Pattern matching

E. Host

Correct Answer: B

QUESTION 15

_____ is the process of confirming that implemented security safeguards work as expected.

A. Penetration testing

B. Exploitation

C. Baselining

D. A vulnerability

E. A countermeasure

Correct Answer: A