DUMPSQUEEN

Certified in Cybersecurity

ISC2 CC

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1312

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Mix Questions	461
Topic 2, Security Principles	150
Topic 3, Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	149
Topic 4, Access Controls Concepts	170
Topic 5, Network Security	217
Topic 6, Security Operations	165
Total	1312

QUESTION NO: 1

What access control principle states that users should only be granted access to resources necessary to perform their job duties and nothing more?

A. Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

ANSWER: A

Explanation:

The Principle of Least Privilege states that users should only be granted access to resources necessary to perform their job duties and nothing more, reducing the risk of unauthorized access and limiting the potential impact of security breaches.

QUESTION NO: 2

Which of the following is a key objective of security incident response?

A. To assign blame for security incidents

B. To recover all lost data immediately after an incident

C. To minimize the impact of security incidents on operations

D. To increase the complexity of security controls

ANSWER: C

Explanation:

A key objective of security incident response is to minimize the impact of security incidents on operations, restoring normal business functions efficiently and effectively.

QUESTION NO: 3

Which of the following is a characteristic of a stateful firewall?

A. It operates at the application layer of the OSI model.

B. It inspects network packets without considering their context.

C. It maintains a record of the state of active connections.

D. It only allows traffic based on IP addresses.

ANSWER: C

Explanation:

A stateful firewall maintains a record of the state of active connections, allowing it to make more informed decisions about allowing or blocking traffic based on the context of the connection.

QUESTION NO: 4

What is the role of administrative security controls in an organization?

A. To physically secure systems against unauthorized access

B. To implement technical mechanisms that limit data access

C. To establish policies, procedures, and guidelines for security

D. To detect security breaches through automated monitoring

ANSWER: C

Explanation:

Administrative controls consist of policies, procedures, and guidelines that define how the organization manages and protects its information, directing the implementation and maintenance of security measures.

QUESTION NO: 5

Which containment strategy aims at preventing the spread of an incident beyond

the network perimeter?

A. Endpoint containment

B. Account containment

C. Perimeter containment

D. Internal network containment

ANSWER: C

Explanation:

Perimeter containment strategies are designed to prevent the spread of an incident beyond the network perimeter. This can involve methods such as inbound/outbound traffic blocking, updating firewall policies, and switching to alternate communication links to isolate and mitigate the spread of threats.

QUESTION NO: 6

In access control terminology, what is a "Mantrap"?

A. A software tool used to detect unauthorized access attempts

B. An encryption method designed to trap cybercriminals

C. A physical security device or enclosure that allows the passage of individuals, where entry and exit are controlled

D. A type of malware that lures users into compromising their credentials

ANSWER: C

Explanation:

A Mantrap refers to a physical security mechanism designed to control access to secure areas through a small enclosure or vestibule with two or more doors. The design ensures that only one door can open at a time, allowing individual passage while preventing unauthorized access.

QUESTION NO: 7

Which of the following best describes the role of the incident response "Containment, Eradication, and Recovery" phase?

A. To document the incident and communicate with external stakeholders

B. To prevent the incident from occurring through proactive measures

C. To contain the incident, remove the threat, and restore normal operations

D. To focus exclusively on legal proceedings related to the incident

ANSWER: C

Explanation:

The "Containment, Eradication, and Recovery" phase involves containing the spread of the incident, eradicating the threat from the organization's environment, and recovering affected systems to resume normal operations. This phase is critical for limiting damage and restoring business continuity.

QUESTION NO: 8

What is the purpose of implementing access control mechanisms in network load balancers?

A. To authenticate users attempting to access resources.

B. To assign access rights to authenticated users.

C. To enforce security policies by distributing network traffic across multiple servers.

D. To record and monitor user activities for auditing purposes.

ANSWER: C

Explanation:

Access control mechanisms in network load balancers enforce security policies by distributing network traffic across multiple servers, ensuring optimal performance and availability while preventing overload and denial-of-service attacks.

QUESTION NO: 9

Which access control mechanism uses cryptographic keys to authenticate users?

A. Biometric authentication.

B. Password-based authentication.

C. Token-based authentication.

D. Certificate-based authentication.

ANSWER: D

Explanation:

Certificate-based authentication uses cryptographic keys to authenticate users, providing a secure and reliable method of verifying their identity.

QUESTION NO: 10

What access control principle ensures that access rights are separated among multiple individuals to prevent fraud and errors?

A.

Principle of Least Privilege.

B. Separation of Duties.

C. Defense in Depth.

D. Need-to-Know Principle.

Answer: B

Explanation:

Separation of Duties ensures that access rights are separated among multiple individuals to prevent fraud and errors, reducing the risk of unauthorized activities and ensuring accountability.

A. Separation of Duties.

B. Defense in Depth.

C. Need-to-Know Principle.

ANSWER: A

Explanation:

Separation of Duties ensures that access rights are separated among multiple individuals to prevent fraud and errors, reducing the risk of unauthorized activities and ensuring accountability.

QUESTION NO: 11

What is the primary purpose of a continuity of operations plan (COOP)?

A. To prevent all business disruptions

B. To recover all lost data immediately after an incident

C. To ensure that critical business functions can continue during and after disruptions

D. To wait for external assistance before taking any action

ANSWER: C

Explanation:

A continuity of operations plan (COOP) ensures that critical business functions can continue during and after disruptions, minimizing downtime and maintaining operations to the extent possible.

QUESTION NO: 12

Which of these is an attack whose PRIMARY goal is to gain access to a target system through falsified identity?

A. Ransomware

B. Amplification

C. SpoofingD. DDoS

ANSWER: C

Explanation:

Spoofing is an attack whose primary goal is to gain access to a target system through a falsified identity. In a spoofing attack, the attacker creates or manipulates a digital identity or communication, so as to deceive the target into believing that the attacker is someone or something else. There are many different types of spoofing attacks, including email spoofing, IP spoofing, and URL spoofing. Such attacks are used to gain unauthorized access to systems or networks, steal sensitive information, or spread malware (see ISC2 Study Guide, chapter 4, module 2).

The other types of attacks listed above have different primary goals. DDoS (Distributed Denial of Service) attacks aim at overwhelming a target system with traffic to disrupt its operation; amplification attacks involve using a third-party system to

amplify the strength of an attack; and ransomware attacks typically encrypt a target system's data, and then demand a ransom in exchange for the decryption code.

QUESTION NO: 13

The PRIMARY objective of a security baseline is to establish ...

A. . a minimum understood and a good level of security requirements

B. ... a minimum understood and acceptable level of security requirements

C. ... security and configuration requirements

D. ... a maximum understood and an acceptable level of security requirements

ANSWER: B

Explanation:

A security baseline is a set of security standards, guidelines and procedures used to ensure that a system or network meets a minimum level of security. Security baselines are typically based on industry best practices, regulatory requirements, and an organization's specific security needs. The primary objective of a security baseline is to establish a minimum understood and acceptable level of security requirements. While it is true that a security baseline specifies security and configuration requirements that must be met to ensure that the system or network is adequately protected, that is actually not its primary goal (see ISC2 Study Guide, chapter 5, module 2). The other options do not apply, since they do not align the definition of a security baseline. Moreover, enforcing a maximum number of security requirements is not necessarily a good practice, since practically no organization could bear such a cost.

QUESTION NO: 14

What is the primary purpose of conducting employee security awareness training?

A. To increase network bandwidth

B. To educate employees about cybersecurity risks and best practices

C. To restrict employee access to information resources

D. To install antivirus software on employee devices

ANSWER: B

Explanation:

Employee security awareness training educates employees about cybersecurity risks, threats, and best practices to empower them to recognize and respond appropriately to security incidents.

QUESTION NO: 15

During which phase of the incident response process does the lessons learned assessment take place?

A. Detection and analysis

B. Containment, eradication, and recovery

C. Preparation

D. Post-incident activity

ANSWER: D

Explanation:

The lessons learned assessment occurs during the post-incident activity phase of the incident response process.

QUESTION NO: 16

What are the primary responsibilities of a Security Operations Center (SOC) analyst?

A. Managing network infrastructure devices

B. Developing encryption algorithms

C. Monitoring security alerts and events

D. Designing software applications

ANSWER: C

Explanation:

SOC analysts are responsible for monitoring security alerts and events, identifying potential threats, and initiating appropriate responses to mitigate risks.

QUESTION NO: 17

The Bell and LaPadula access control model is a form of: (★)

A. ABAC

B. RBAC

C. MAC

D. DAC

ANSWER: C

Explanation:

The Bell and LaPadula access control model arranges subjects and objects into security levels and defines access specifications, whereby subjects can only access objects at certain levels based on their security level. Typical access specifications can be things like "Unclassified personnel cannot read data at confidential levels" or "Top-Secret data cannot be written into the files at unclassified levels". Since subjects cannot change access specifications, this model is a form of mandatory access control (MAC). In contrast, Discretionary Access Control (DAC) leaves a certain level of access control to the discretion of the object's owner. The Attribute Based Access Control (ABAC) is based on subject and object attributes (not only classification). Finally, Role Based Access Control (RBAC) is a model for controlling access to objects where permitted actions are identified with roles rather than individual subject identities.

QUESTION NO: 18

What is the main function of an Intrusion Prevention System (IPS)?

A. To create backups of critical data

B. To detect and prevent specific types of network traffic based on security policies

C. To encrypt data transmissions

D. To audit financial transactions

ANSWER: B

Explanation:

An IPS monitors network traffic to detect and prevent identified threats according to predefined security policies, actively blocking attacks in real-time.

QUESTION NO: 19

Which of the following is not a protocol of the OSI Level 3?

A. IGMP

B. ICMP

C. SNMP

D. IP

ANSWER: C

Explanation:

Internet Protocol (IP) is known to be a level 3 protocol. Internet Control Message Protocol (ICMP) and

Internet Group Management Protocol (IGMP) are also level 3 protocols. Simple Network Management Protocol (SNMP) is a protocol used to configure and monitor devices attached to networks. It is an application-level protocol (level 7), and therefore the only option that is not from level 3.

QUESTION NO: 20

Which of the following is NOT an ethical canon of the ISC2?

A. Provide active and qualified service to principal

B. Act honorably, honestly, justly, responsibly and legally

C. Advance and protect the profession

D. Protect society, the common good, necessary public trust and confidence, and the infrastructure

ANSWER: A

Explanation:

In the code of ethics, we read "Provide diligent and competent service to principals", and not "Provide active and qualified service to principals."; all the other options are valid canons of the code of ethics (see ISC2 Study Guide Chapter 1, Module 5).