

01	A	B	C	D	E
02	A	B	C	D	E
03	A	B	C	D	E
04	A	B	C	D	E
05	A	B	C	D	E
06	A	B	C	D	E
07	A	B	C	D	E
08	A	B	C	D	E
09	A	B	C	D	E
10	A	B	C	D	E
11	A	B	C	D	E
12	A	B	C	D	E
13	A	B	C	D	E

14	A	B	C	D	E
15	A	B	C	D	E
16	A	B	C	D	E
17	A	B	C	D	E
18	A	B	C	D	E
19	A	B	C	D	E
20	A	B	C	D	E
21	A	B	C	D	E
22	A	B	C	D	E
23	A	B	C	D	E
24	A	B	C	D	E
25	A	B	C	D	E
26	A	B	C	D	E

27	A	B	C	D	E
28	A	B	C	D	E
29	A	B	C	D	E
30	A	B	C	D	E
31	A	B	C	D	E
32	A	B	C	D	E
33	A	B	C	D	E
34	A	B	C	D	E
35	A	B	C	D	E
36	A	B	C	D	E
37	A	B	C	D	E
38	A	B	C	D	E
39	A	B	C	D	E

PRACTICE QUESTIONS

DANTES Eligible Military Service Member (DSST)

SN013

Fundamentals of Cybersecurity

EDITION

Demo

QUESTIONS

9

FORMAT

Limited Edition PDF

Before you begin

What this is

9 practice questions for DANTES Eligible Military Service Member (DSST) **SN013**, each with its answer key and an explanation. Answer a question before you read its key — the explanation is worth more once you have committed.

If something looks wrong

Send us three things and we will check it:

- the exam code, **SN013**
- the question number
- the email address on your order

Write to **support@mometrix.net**. We reply within one business day.

QUESTION 1

SINGLE CHOICE

Which of the three core principles of the CIA triad is directly compromised when an unauthorized user modifies a record in a database?

- ☐ A Confidentiality
- ☒ B Integrity
- ☐ C Availability
- ☐ D Authentication

ANSWER B

WHY The CIA triad consists of Confidentiality, Integrity, and Availability. Integrity is the principle that ensures data is accurate and has not been altered by unauthorized parties. When an unauthorized user modifies a database record, the accuracy and trustworthiness of the data is violated, which is a direct compromise of integrity. Confidentiality refers to preventing unauthorized disclosure, availability refers to ensuring systems and data are accessible when needed, and authentication is a control mechanism, not one of the three CIA principles.

QUESTION 2

SINGLE CHOICE

Which type of social engineering attack specifically involves an attacker leaving a malware-infected USB drive in a location where an employee is likely to find and insert it into a workstation?

- ☐ A Phishing
- ☒ B Baiting
- ☐ C Tailgating
- ☐ D Shoulder surfing

ANSWER B

WHY Baiting is a social engineering technique in which an attacker leaves a physical item, such as a USB drive or CD, in a public location hoping that someone will pick it up and plug it into a computer. Once inserted, the media executes malicious code that can compromise the system. Phishing uses fraudulent emails or messages, tailgating involves physically following an authorized person into a restricted area, and shoulder surfing involves observing someone entering credentials or sensitive information.

QUESTION 3

SINGLE CHOICE

In access control terminology, what is the term for the principle that restricts a user's permissions to only the information and resources necessary to perform their assigned job functions?

- ☐ A Mandatory access control
- ☐ B Discretionary access control
- ☒ C Least privilege
- ☐ D Role-based access control

ANSWER C

WHY The principle of least privilege (PoLP) states that users should be granted only the minimum levels of access or permissions needed to perform their job duties. This reduces the risk of accidental misuse or exploitation of elevated privileges. Mandatory access control (MAC) and discretionary access control (DAC) are specific access control models, and role-based access control (RBAC) is a method of assigning permissions based on roles, but least privilege is the overarching principle that guides these implementations.

QUESTION 4

MULTIPLE CHOICE

Which of the following are examples of symmetric-key cryptographic algorithms? (Choose two.)

- ☒ A AES
- ☐ B RSA
- ☒ C 3DES
- ☐ D ECC

ANSWER A - C

WHY AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard) are both symmetric-key algorithms, meaning they use the same secret key for both encryption and decryption. RSA and ECC (Elliptic Curve Cryptography) are asymmetric (public-key) algorithms that use a mathematically related key pair consisting of a public key and a private key.

QUESTION 5

SINGLE CHOICE

Which type of firewall inspects each packet against a set of defined rules that include source and destination IP addresses, ports, and protocols, and makes forwarding decisions based on those header values alone?

- ☐ A Stateful inspection firewall
- ☐ B Application-layer firewall
- ☒ C Packet-filtering firewall
- ☐ D Next-generation firewall

ANSWER C

WHY A packet-filtering firewall examines packet headers and applies rules based on source IP, destination IP, port numbers, and protocol. It does not inspect packet payloads or maintain connection state, which makes it the fastest but least secure type. A stateful inspection firewall tracks the state of active connections, an application-layer firewall inspects the contents of packets at the application layer, and a next-generation firewall combines multiple advanced features such as deep packet inspection and intrusion prevention.

QUESTION 6

SINGLE CHOICE

A user's computer begins to perform very slowly and the task manager shows several unfamiliar processes consuming significant CPU resources. The user later learns that their machine was secretly being used to send large volumes of spam email. Which category of malware best describes this situation?

- ☐ A Trojan horse
- ☐ B Worm
- ☒ C Botnet agent (zombie)
- ☐ D Rootkit

ANSWER C

WHY A botnet agent, also called a zombie or bot, is a piece of malware that infects a host and allows an attacker to control it remotely as part of a larger network of compromised machines. Infected machines are often used to send spam, launch distributed denial-of-service attacks, or mine cryptocurrency. A Trojan disguises itself as legitimate software, a worm self-replicates across networks, and a rootkit is designed to hide the presence of other malware on a system.

QUESTION 7

SINGLE CHOICE

In risk management terminology, what is the term for the potential loss, damage, or destruction of an asset resulting from a threat exploiting a vulnerability?

- ☐ A Threat
- ☐ B Vulnerability
- ☒ C Impact
- ☐ D Likelihood

ANSWER C

WHY Impact refers to the magnitude of harm or loss that would result if a threat successfully exploits a vulnerability. A threat is any potential cause of an unwanted event, a vulnerability is a weakness that could be exploited, and likelihood is the probability that a threat will exploit a vulnerability. Risk itself is typically calculated as a function of threat, vulnerability, likelihood, and impact.

QUESTION 8

MULTIPLE CHOICE

Which of the following are valid phases of the incident response lifecycle as defined by NIST? (Choose two.)

- ☒ **A** Containment, eradication, and recovery
- ☒ **B** Preparation, detection, and analysis
- ☐ **C** Exploitation and payload delivery
- ☐ **D** Installation and command and control

ANSWER A - B

WHY NIST SP 800-61 defines the incident response process as having four main phases: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Options C and D refer to stages of the cyber kill chain, which is a different framework describing the stages of a cyberattack rather than the response to one.

QUESTION 9

SINGLE CHOICE

At which layer of the OSI reference model does the Transmission Control Protocol (TCP) operate?

- ☐ **A** Application
- ☒ **B** Transport
- ☐ **C** Network
- ☐ **D** Data Link

ANSWER B

WHY TCP operates at Layer 4, the Transport layer, of the OSI model. It provides connection-oriented, reliable transport of segments between applications identified by port numbers. The Application layer (Layer 7) hosts protocols such as HTTP and DNS, the Network layer (Layer 3) hosts IP, and the Data Link layer (Layer 2) handles framing and physical addressing.