ISC2

CC

Certified in Cybersecurity (CC)

QUESTION & ANSWERS

Question: 1

The address 8be2:4382:8d84:7ce2:ec0f:3908:d29a:903a is an:

A. Web address

B. IPv4 address

C. IPv6 address

D. Mac address

Answer: C

Explanation/Reference:

An IPv6 address is a 128-bit address represented as a sequence of eight groups of 16-bit hexadecimal values. An IPv4 address is a 32-bit address represented as a sequence of four 8-bit integers. A Mac address is a 48-bit address represented as six groups of 8 bits values in hexadecimal. A web address consists of a protocol name, a server address, and a resource path (see ISC2 Study Guide, chapter 4, module 1 - Understand Computer Networking).

Question: 2

Which of the following canons is found in the ISC2 code of ethics?

A. Advance and promote the profession

B. Protect society, the common good, and the infrastructure

C. Provide diligent and competent service to principals

D. Act honorably, honestly, safely and legally

Answer: C

Explanation/Reference:

Only "Provide diligent and competent service to principals" contains the accurate text of the ISC2 code of ethics. Although a security professional should discourage unsafe practices, no direct reference to acting safely exists in the canons. Aside from society, the common good and infrastructure, security professionals are expected to protect public trust and confidence. Finally, they are expected to protect the profession, and not just advance and promote it.

Question: 3

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

A. Advance and protect the profession

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

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

D. Provide active and qualified service to principal

Answer: D

Explanation/Reference:

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).

Question: 4

The cloud deployment model where a company has resources on-premise and in the cloud is known as:

A. Hybrid cloud

B. Multi-tenant

C. Private cloud

D. Community cloud

Answer: A

Explanation/Reference:

A hybrid cloud is a model that combines (i.e. orchestrates) on-premise infrastructure, private cloud services, and a public cloud to handle storage and service. A community cloud is an infrastructure where multiple organizations share resources and services based on common technological and regulatory necessities. Multi-tenancy refers to a context where several of a cloud vendor's customers share the same computing resources. A private cloud is a cloud computing model where the cloud infrastructure is dedicated to a single organization.

Question: 5

Which of the following is a public IP?

A. 13.16.123.1

B. 192.168.123.1

C. 172.16.123.1

D. 10.221.123.1

Answer: A

Explanation/Reference:

The ranges of IP addresses 10.0.0.0 to 10.255.255.254, 172.16.0.0 to 172.31.255.254, and 192.168.0.0 to 192.168.255.254 are reserved for private use (see ISC2 Study Guide, chapter 4, module 1, under Internet Protocol - IPv4 and IPv6). Therefore, the IP address 13.16.123.1 is the only address in a public range.

Question: 6

Which of the following is a data handling policy procedure?

A. Transform

B. Collect

C. Encode

D. Destroy

Answer: D

Explanation/Reference:

The data handling procedures are 'Classify', 'Categorize', 'Label', 'Store', 'Encrypt', 'Backup', and 'Destroy' (see ISC2 Study Guide, chapter 5, module 3).

Question: 7

Which devices would be more effective in detecting an intrusion into a network?

A. Routers

B. HIDS

C. Firewalls

D. NIDS

Answer: D

Explanation/Reference:

Network intrusion detection systems (NIDS) are network devices that detect malicious traffic on a network. Host intrusion detection systems (HIDS) are applications that monitor computer systems for intrusion. Typically, HIDS are not concerned with network devices. A firewall is a device that filters incoming Internet traffic. Routers receive and forward traffic, but (typically) do not analyze it.

Question: 8

Which concept describes an information security strategy that integrates people, technology and operations in order to establish security controls across multiple layers of the organization?

A. Least Privilege

B. Defense in Depth

C. Separation of Duties

D. Privileged Accounts

Answer: B

Explanation/Reference:

Defense in depth describes a cybersecurity approach that uses multiple layers of security for holistic protection (see ISC2 Study Guide Chapter 1, Module 3). According to the principle of Separation of Duties, no user should ever be given enough privileges to misuse the system on their own. The principle of Least Privilege dictates that users should be given only those privileges required to complete their specific tasks. Privileged Accounts are a class of accounts that have permissions exceeding those of regular users, such as manager and administrator accounts.

Question: 9

Which access control is more effective at protecting a door against unauthorized access?

A. Fences

B. Turnstiles

C. Barriers

D. Locks

Answer: D