CERT EMPIRE

ISC2 CC Certified in Cybersecurity Exam Questions

Total Questions: 570+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: CC Exam Dumps by Cert Empire

Question: 1

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

A: Protect society, the common good, necessary public trust and confidence, and the infrastructure

B: Provide active and qualified service to principal

C: Advance and protect the profession

D: Act honorably, honestly, justly, responsibly and legally

Correct Answer:

B

Explanation:

The ISC2 Code of Ethics is built upon four mandatory canons. Options A, C, and D are verbatim statements of the first, fourth, and second canons, respectively. The third canon is "Provide diligent and competent service to principals." Option B alters this wording to "Provide active and qualified service to principal." While the sentiment is similar, the specific language is different, making it not an official canon of the ISC2. Precision in language is critical when dealing with professional codes of conduct.

Why Incorrect Options are Wrong:

A: This is an incorrect choice because it is the first canon of the ISC2 Code of Ethics.

C: This is an incorrect choice because it is the fourth canon of the ISC2 Code of Ethics.

D: This is an incorrect choice because it is the second canon of the ISC2 Code of Ethics.

References:

1. ISC2. (n.d.). Code of Ethics. ISC2. Retrieved from https://www.isc2.org/Ethics. This official page lists the four canons verbatim.

2. University of Washington. (2023). INFO 444: Information Assurance and Cybersecurity - Professional Ethics. Course materials often reference the ISC2 Code of Ethics as a foundational document for the profession, citing the four official canons.

3. Ciampa, M. (2021). Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning. (Note: While a textbook, it is used in university curricula and accurately reflects the ISC2 canons as an industry standard). Chapter 15 typically covers professional ethics and codes of conduct.

Question: 2

Which of the following is NOT an example of a physical security control?

A: Security cameras

B: Remote control electronic locks

C: Biometric access controls

D: Firewalls

Correct Answer:

D

Explanation:

Physical security controls are measures designed to deter, detect, delay, or respond to threats against physical assets, such as facilities, equipment, and personnel. Security cameras, electronic locks, and biometric access systems are all examples of controls that manage or monitor physical access to a secured area. In contrast, a firewall is a technical (or logical) control. It operates on a network to filter data traffic based on a set of security rules, protecting digital assets from unauthorized network access, not physical intrusion.

Why Incorrect Options are Wrong:

A: Security cameras: These are physical devices used to monitor and record activity in a physical space, serving as a detective and deterrent physical control.

B: Remote control electronic locks: These are physical barriers that prevent or allow physical entry into a room or building, making them a preventive physical control.

C: Biometric access controls: These systems use unique human characteristics to grant or deny physical entry, functioning as a preventive physical control.

References:

1. (ISC)² Official CC Study Guide, 1st Edition. Chapter 4, "Network Security," defines a firewall as a network security control. Chapter 3, "Security Principles," discusses physical controls like locks and cameras for securing physical environments. This distinction places firewalls outside the physical control category.

2. NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations." This standard categorizes security controls into families. Firewalls fall under technical control families like "Access Control (AC)" and

"System and Communications Protection (SC)." Controls like cameras, locks, and biometric scanners are explicitly part of the "Physical and Environmental Protection (PE)" family. (See control families PE and SC).

URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

3. Saltzer, J. H., & Schroeder, M. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 18(7), 387-408. This foundational paper distinguishes between physical protection mechanisms and logical protection mechanisms (like access control lists, which are implemented by firewalls). It establishes the conceptual separation between securing physical hardware and securing the information flows within it.

URL: https://dl.acm.org/doi/10.1145/361011.361062 (Section: "Techniques for Protection of Information")

Question: 3

Which type of attack attempts to trick the user into revealing personal information by sending a fraudulent message?

A: Cross-Site Scripting

B: Trojans

C: Phishing

D: Denials of Service

Correct Answer:

C

Explanation:

Phishing is a form of social engineering where an attacker sends a fraudulent message, often an email or text, designed to appear as if it's from a legitimate source. The primary goal is to deceive the recipient into revealing sensitive personal information, such as usernames, passwords, and credit card details, or to deploy malicious software on the victim's machine. The attack relies on tricking the user, which directly aligns with the question's description of a fraudulent message used to obtain personal information.

Why Incorrect Options are Wrong:

A: Cross-Site Scripting: This is a technical injection vulnerability in web applications where attackers execute malicious scripts in a victim's browser, not an attack based on sending a fraudulent message.

B: Trojans: This is a type of malware that masquerades as legitimate software to gain access to a system. While a phishing email might deliver a Trojan, the Trojan itself is the malicious program.

D: Denial of Service: This attack aims to make a network resource or machine unavailable to its intended users by overwhelming it with traffic, not to steal information through deception.

References:

1. (ISC)² CC Certified in Cybersecurity Official Student Guide, 2nd Edition. Module 3, "Security Principles," defines phishing as a social engineering attack that uses deceptive communications to trick individuals into divulging confidential information.

2. National Institute of Standards and Technology (NIST) Special Publication 800-63-3. In Section 5.1.1, phishing is defined as "A technique for attempting to acquire sensitive information...through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person." [Direct URL: https://pages.nist.gov/800-63-3/sp800-63-3.html]

3. Kirda, E., & Kruegel, (2005). Protecting Users Against Phishing Attacks. Proceedings of the 2005 ACM Symposium on Applied Computing. This academic paper describes phishing as "a form of online identity theft in which attackers use fraudulent e-mails and web sites to trick users into divulging sensitive personal information." [DOI: 10.1145/1064009.1064018]

Question: 4

Which of the following is NOT a feature of a cryptographic hash function?

A: Useful

B: Deterministic

C: Reversible

D: Unique

Correct Answer:

C

Explanation:

A cryptographic hash function is fundamentally a one-way function, meaning it is designed to be computationally infeasible to reverse. This property, known as pre-image resistance, is critical for its security applications, such as protecting password confidentiality. If a hash were reversible, an attacker could easily recover the original input (e.g., a password) from its hash value, defeating its purpose. Therefore, being "reversible" is the opposite of a required feature for a cryptographic hash.

Why Incorrect Options are Wrong:

A: Useful: Hash functions are extremely useful for verifying data integrity, creating digital signatures, and storing passwords securely, making this a valid characteristic.

B: Deterministic: This is a core property. A hash function must produce the exact same output (hash) every time it is given the same input.

D: Unique: This refers to collision resistance, a crucial feature where it is computationally infeasible to find two different inputs that produce the same hash output.

References:

1. (ISC)² CC Certified in Cybersecurity Official Study Guide (1st Edition). Chapter 4, "Protecting the Organization's Assets," describes hashing as a one-way function used to create a digital fingerprint of data, emphasizing its role in integrity and non-reversibility.

2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). Chapman and Hall/CRChapter 5, "Hash Functions and Applications," defines a cryptographic hash

function with three core properties: pre-image resistance (one-way), second pre-image resistance, and collision resistance. Reversibility is the antithesis of pre-image resistance.

3. MIT OpenCourseWare. (2014). 6.857 Computer and Network Security, Fall 2014. Lecture 6: Hashing. The lecture notes explicitly state that a key property of cryptographic hash functions is "Pre-image resistance (one-way)," meaning given a hash value y, it is hard to find an input x such that H(x) = y. (URL: https://ocw.mit.edu/courses/6-857-computer-and-network-security-fall-2014/resources/mit6857f14lec6/)

Question: 5

Which physical access control would be MOST effective against tailgating?

A: Turnstiles

B: Barriers

C: Locks

D: Fences

Correct Answer:

A

Explanation:

A turnstile is a mechanical gate designed to allow only one person to pass at a time following a successful authentication. This "one-person-per-authentication" enforcement mechanism is the most direct and effective countermeasure against tailgating, where an unauthorized individual follows an authorized person through a secured entry point. The physical design of a turnstile inherently prevents this type of unauthorized access.

Why Incorrect Options are Wrong:

B: Barriers: This term is too general. While a turnstile is a type of barrier, other barriers like vehicle boom gates or simple railings do not effectively prevent pedestrian tailgating.

C: Locks: A lock secures a door but does not prevent tailgating. Once an authorized user unlocks and opens the door, an unauthorized person can easily follow them through before it closes.

D: Fences: Fences are perimeter controls that define a boundary. They are ineffective against tailgating, which occurs at the access point (e.g., a gate) within the fence line, not along its length.

References:

1. ISC2 CC Certified in Cybersecurity Official Student Guide (1st Edition, 2022): Domain 1, Objective 1.4, "Understand physical security controls," discusses various physical controls. Turnstiles are presented as a specific control to prevent unauthorized entry by enforcing single-person passage, directly countering tailgating.

2. Solms, V., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. (Peer-Reviewed Journal): This article, in its discussion of layered security, implicitly supports the use of specific controls for specific threats. A turnstile is a specific control for the specific threat of tailgating at an entry point, making it more effective than general controls like fences or locks for this purpose.

3. MIT OpenCourseWare, 6.858 Computer Systems Security, Fall 2014: Lecture 21, "Physical Security," describes various physical attacks and defenses. The lecture notes explain that controls like turnstiles and mantraps are specifically designed to defeat tailgating by enforcing single-user entry, a weakness of simple locked doors. (URL: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/)

Question: 6

Which type of attack embeds malicious payload inside a reputable or trusted software?

A: Cross-Site Scripting

B: Phishing

C: Trojans

D: Rootkits

Correct Answer:

C

Explanation:

A Trojan, or Trojan horse, is a type of malicious code or software that looks legitimate but can take control of your computer. It is designed to mislead users about its true intent. A Trojan is often disguised as or embedded within legitimate software. When a user executes the seemingly harmless program, the malicious payload is activated, allowing the attacker to achieve their objective, such as stealing data or installing other malware. This perfectly matches the description of embedding a malicious payload inside reputable software.

Why Incorrect Options are Wrong:

A: Cross-Site Scripting: This is a web application vulnerability where an attacker injects malicious scripts into a trusted website's content, not a software application's code.

B: Phishing: This is a social engineering attack method that uses deceptive communications to trick victims. While it can deliver a Trojan, it is the delivery method, not the malware type.

D: Rootkits: This is a type of malware designed to gain privileged access and conceal its presence on a system. Its primary function is stealth, not the initial disguise as a legitimate application.

References:

ISC2 CC Certified in Cybersecurity Official Student Guide (Domain 2, Section 2.2): The guide defines a Trojan as malware that "disguises itself as a legitimate program." This aligns directly with the question's premise of a malicious payload inside trusted software.

National Institute of Standards and Technology (NIST) Glossary: Defines a "Trojan Horse" as "A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program." (Source: NIST Glossary, https://csrc.nist.gov/glossary/term/trojanhorse)

National Institute of Standards and Technology (NIST) SP 800-83: This publication discusses malware incident prevention and handling, describing Trojans as a primary category of malware that relies on tricking the user into executing it. (Source: NIST Special Publication 800-83, Revision 1, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," Section 2.2.1)

Question: 7

An exploitable weakness or flaw in a system or component is a:

A: Threat

B: Vulnerability

C: Bug

D: Risk

Correct Answer:

B

Explanation:

A vulnerability is a weakness or flaw in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. The term specifically refers to a characteristic that makes a system susceptible to a threat, which directly aligns with the question's definition of an "exploitable weakness." This weakness can exist in hardware, software, protocols, or internal controls.

Why Incorrect Options are Wrong:

A: Threat: A threat is a potential event or actor that could cause harm. It is the agent that might exploit a vulnerability, not the weakness itself.

C: Bug: A bug is an error in code. While a bug can create a vulnerability, not all bugs are exploitable security weaknesses. "Vulnerability" is the more precise term.

D: Risk: Risk is the potential for loss or damage when a threat exploits a vulnerability. It is calculated as the intersection of threats, vulnerabilities, and assets (Risk = Threat x Vulnerability).

References:

1. National Institute of Standards and Technology (NIST). (2021). Glossary of Terms. CSRRetrieved from https://csrc.nist.gov/glossary/term/vulnerability.

Definition: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." This directly supports the correct answer.

2. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). Page 7. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Differentiation: This document clearly distinguishes between threat, vulnerability, and risk, defining them as separate but related components of risk assessment.

3. Whitman, M. E., & Mattord, H. J. (2019). Principles of Information Security (6th ed.). Cengage Learning. (Widely used in university curricula).

Chapter 2, "The Need for Security": This chapter defines a vulnerability as "A weakness or fault in a system or protection mechanism that opens it to the possibility of attack or damage." This academic source corroborates the definition.

Question: 8

Which are the components of an incident response plan?

A: Preparation → Detection and Analysis → Containment, Eradication and Recovery → Post-Incident Activity

B: Preparation → Detection and Analysis → Recovery → Containment → Eradication → Post-Incident Activity

C: Preparation → Detection and Analysis → Containment → Eradication → Post-Incident Activity → Recovery

D: Preparation → Detection and Analysis → Eradication → Recovery → Containment → Post-Incident Activity

Correct Answer:

A

Explanation:

The correct sequence of an incident response plan follows the lifecycle defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-61. This model consists of four primary phases:

1. Preparation: Establishing the necessary tools, policies, and training.

2. Detection and Analysis: Identifying and validating an incident.

3. Containment, Eradication, and Recovery: This phase involves limiting the incident's impact, removing its cause, and restoring systems to normal operation. These three activities are logically grouped and sequential.

4. Post-Incident Activity: Analyzing the incident and response to improve future efforts (lessons learned).

Option A accurately reflects this established four-phase model.

Why Incorrect Options are Wrong:

B: Incorrect because recovery actions must occur after containment and eradication, not before.

C: Incorrect because recovery is a core part of the response and precedes the final post-incident activity (lessons learned).

D: Incorrect because containment must precede eradication to prevent the threat from spreading further during the removal process.

References:

1. NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide: Section 2.3, "Incident Response Life Cycle" (Page 7, Figure 2-1) explicitly outlines the four phases as: Preparation; Detection & Analysis; Containment, Eradication, & Recovery; and Post-Incident Activity.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2. (ISC)² CC Certified in Cybersecurity Official Student Guide: Domain 4, "Security Operations," Objective 4.2, "Understand the incident response lifecycle," lists the phases in the correct order: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity, directly aligning with the NIST model and option A.

3. University of Washington, Incident Response: This courseware describes the incident response process, citing the NIST framework. It details the phases as Preparation, Identification (Detection), Containment, Eradication, Recovery, and Lessons Learned (Post-Incident Activity), confirming the sequence in option A.

URL: https://www.washington.edu/ciso/incident-response/

Question: 9

Which of the following is an example of 2FA?

A: Keys

B: Passwords

C: Badges

D: One-Time passwords (OTA)

Correct Answer:

D

Explanation:

Two-factor authentication (2FA) is a security process requiring users to provide two different authentication factors. These factors are categorized as something you know (e.g., a password), something you have (e.g., a security token), and something you are (e.g., a fingerprint). A One-Time Password (OTP), often generated by a mobile app or a physical token, serves as the "something you have" factor. It is used in conjunction with a "something you know" factor, like a password, to complete the 2FA process. Therefore, the OTP mechanism is a quintessential example of implementing a second authentication factor.

Why Incorrect Options are Wrong:

A: Keys: A physical key is an example of a single authentication factor ("something you have") and does not constitute 2FA on its own.

B: Passwords: A password is an example of a single authentication factor ("something you know") and is not 2FA by itself.

C: Badges: A badge is an example of a single authentication factor ("something you have") and is not, by itself, 2FA.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management. Section 4.2, "Something You Have," and specifically Section 4.2.2, "One-Time Passwords (OTPs)," describe OTPs as a mechanism used for multi-factor authentication, generated by a physical device the user possesses.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf (Page 19)

2. (ISC)² CC Certified in Cybersecurity Official Student Guide, 1st Edition. Domain 4, "Network Security," defines Multi-Factor Authentication (MFA) and explicitly lists the use of a password combined with an OTP as a primary example of this security control.

3. Carnegie Mellon University, Introduction to Computer Security Courseware. Lecture notes on "Authentication" describe the three factors of authentication and provide examples, positioning OTPs as a common implementation for the "something you have" factor in MFA systems.

URL: https://www.cs.cmu.edu/~gkesden/cmu-misc/security/lectures/13-authentication.pdf (Slide 15)

Question: 10

Which type of attack will most effectively provide privileged access (root access in Unix/Linux platforms) to a computer while hiding its presence?

A: Phishing

B: Rootkits

C: Cross-Site Scripting

D: Trojans

Correct Answer:

B

Explanation:

A rootkit is a specific type of malicious software designed to gain administrative-level control (known as "root" access in Unix/Linux) over a computer system. Its primary characteristic and function is to actively hide its own presence and the presence of other malicious processes or files from detection by the user, system administrators, and security software. This combination of privileged access and stealth directly matches the requirements of the question.

Why Incorrect Options are Wrong:

A: Phishing: This is a social engineering technique used to acquire sensitive information or as a delivery mechanism for malware; it does not itself provide or hide privileged access.

C: Cross-Site Scripting: This is a web application vulnerability that targets a user's browser session, not the underlying server operating system, to gain privileged system access.

D: Trojans: This is a broad category of malware that masquerades as legitimate software. While a Trojan could be used to install a rootkit, the rootkit is the specific tool that provides and hides privileged access.

References:

1. (ISC)² (2022). Official (ISC)² CC Certified in Cybersecurity Student Guide. Domain 5, Security Operations. The guide defines a rootkit as "a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence." This directly supports the answer.

2. Saltzer, J. H., & Kaashoek, M. F. (2009). Principles of Computer System Design: An Introduction. MIT OpenCourseWare, 6.033 Computer System Engineering. Chapter 9, "Security and Protection," discusses malware. Rootkits are described as tools that modify the core of an operating system to hide the fact that the system has been compromised, granting an attacker privileged access.

3. Hoglund, G., & Butler, J. (2006). Rootkits: Subverting the Windows Kernel. Addison-Wesley Professional. While focused on Windows, the foundational definition applies universally: "A rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer." (Chapter 1, What is a Rootkit?).

Question: 11

After an earthquake disrupting business operations, which document contains the procedures required to return business to normal operation?

A: The Business Impact Analysis

B: The Business Continuity Plan

C: The Business Impact Plan

D: The Disaster Recovery Plan

Correct Answer:

D

Explanation:

The Disaster Recovery Plan (DRP) is the correct document. A DRP contains the specific, detailed procedures to recover and restore an organization's technological infrastructure and systems following a catastrophic event like an earthquake. Its primary focus is on the technical recovery needed to bring systems back to their pre-disaster, normal operational state. While the Business Continuity Plan (BCP) is the broader strategic plan for maintaining business functions during a disruption, the DRP is the specific component that outlines the technical steps for restoration, which is essential for the business to fully return to normal operations.

Why Incorrect Options are Wrong:

A: The Business Impact Analysis: This is a process used to identify critical business functions and determine the potential impact of their disruption; it is an input to planning, not the recovery plan itself.

B: The Business Continuity Plan: This plan focuses on maintaining critical business functions during a disruption, often at a reduced capacity or alternate site, rather than detailing the technical restoration to the original state.

C: The Business Impact Plan: This is not a standard, recognized term in the fields of business continuity or disaster recovery and serves as a distractor.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems:

On DRP: "A Disaster Recovery Plan (DRP) is a plan to recover and protect a business IT infrastructure in the event of a disaster... The DRP is one of the component plans of the BCP and is designed to restore the operability of a system, application, or computer facility at an alternate site after an emergency." (Page 9, Section 2.3). The goal of restoring operability aligns with returning to normal.

On BCP: "A Business Continuity Plan (BCP) focuses on sustaining an organization's mission/business processes during and after a disruption." (Page 8, Section 2.3). This highlights its focus on continuity, not restoration.

URL: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

2. (ISC)² CC Certified in Cybersecurity Official Student Guide, Domain 4, Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts:

The official curriculum distinguishes between the two plans, defining the DRP as the technical plan focused on the "recovery and restoration of IT systems and services after a disaster," while the BCP is the "umbrella" plan for "sustaining an organization's business functions." This supports the DRP as the document containing the procedures for restoration.

3. Ross, R., McEvilley, M., & Oren, J. (2018). Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. National Institute of Standards and Technology. NIST Special Publication 800-160, Vol. 2.

This publication discusses resilience, stating that recovery plans (DRPs) provide "the activities, resources, and procedures to recover and restore the system capabilities that were affected by the adverse condition." (Appendix F, Section F.3.1, RECOVERY PLANNING). This reinforces that the DRP contains the procedures for restoration.

URL: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

Question: 12

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

A: Fences

B: Barriers

C: Locks

D: Turnstiles

Correct Answer:

C

Explanation:

A lock is a physical security mechanism specifically designed to secure a point of entry, such as a door, against unauthorized opening. Its primary function is to fasten the door to its frame, requiring a specific key, combination, or credential for operation. While other options are physical controls, they serve different purposes. Fences and barriers establish a perimeter, and turnstiles manage crowd flow. Therefore, a lock is the most direct, precise, and effective control for preventing unauthorized access through a door. This aligns with the principle of applying the most specific control to the asset being protected.

Why Incorrect Options are Wrong:

A: Fences: Fences are perimeter controls used to define a boundary and deter casual entry into a large area, not to secure an individual door.

B: Barriers: This is a general term. While a gate is a type of barrier that uses a lock, the term "lock" is the more precise control for a door.

D: Turnstiles: Turnstiles are designed to control the rate of pedestrian traffic flow, typically one person at a time, not to physically secure a door against entry.

References:

1. (ISC)² CC Certified in Cybersecurity Official Student Guide (2022). Module 4, "Physical Access Controls," describes locks as a fundamental control for securing doors and gates. It distinguishes them from perimeter controls like fences and flow controls like turnstiles.

2. Purdue University, College of Technology. (n.d.). CNIT 45500: Network Security. Course materials on physical security categorize locks as a primary access control for entry points like doors, whereas fences are defined as perimeter security measures.

3. Kissel, R. (Ed.). (2012). Glossary of Key Information Security Terms (NISTIR 7298 Rev. 2). National Institute of Standards and Technology. p. 109. Defines a lock as "A device for securing a door, lid, etc." This definition directly links the control (lock) to the object in the question (door). Available at: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Question: 13

Which are the three packets used on the TCP connection handshake?

A: Discover → Offer → Request

B: Offer → Request → ACK

C: SYN → ACK → FIN

D: SYN → SYN/ACK → ACK

Correct Answer:

D

Explanation:

The TCP three-way handshake is the fundamental process for establishing a reliable connection between a client and a server. The sequence is as follows:

1. SYN: The client initiates the connection by sending a packet with the SYN (Synchronize) flag set.

2. SYN/ACK: The server receives the SYN packet and responds with a packet that has both the SYN and ACK (Acknowledge) flags set, acknowledging the client's request and sending its own synchronization request.

3. ACK: The client receives the SYN/ACK packet and sends a final ACK packet to the server, confirming the connection is established.

Why Incorrect Options are Wrong:

A: Discover, Offer, and Request are steps in the DHCP (Dynamic Host Configuration Protocol) process for obtaining an IP address, not for a TCP connection.

B: This sequence is also part of the DHCP process (DORA: Discover, Offer, Request, Acknowledge) and is incorrect for a TCP handshake.

C: The FIN (Finish) packet is used to terminate a TCP connection, not to establish one. It is part of the connection teardown process.

References:

Postel, J. (1981). RFC 793: Transmission Control Protocol. IETF. Section 3.3, "Connection Establishment," details the three-way handshake sequence as SYN, SYN-ACK, and ACK. Available at: https://datatracker.ietf.org/doc/html/rfc793#page-23

MIT OpenCourseWare. (2014). 6.02 Introduction to EECS II: Digital Communication Systems, Lecture 17: The Network Layer. The lecture notes describe the TCP connection setup, explicitly stating the SYN, SYN-ACK, ACK sequence. Available at: https://ocw.mit.edu/courses/6-02-introduction-to-eecs-ii-digital-communication-systems-fall-2012/resources/mit602f12lec17/

(ISC)² (2023). Official (ISC)² CC Student Guide. Domain 2, "Network Security," covers the TCP/IP model and describes the three-way handshake (SYN, SYN/ACK, ACK) as the method for establishing a TCP connection. (Note: Specific page numbers vary by edition, but the concept is a core part of the network security domain).

Question: 14

Which protocol uses a three-way handshake to establish a reliable connection?

A: SNMP

B: TCP

C: UDP

D: SMTP

Correct Answer:

B

Explanation:

Transmission Control Protocol (TCP) is a connection-oriented protocol operating at the Transport Layer of the OSI and TCP/IP models. Its primary function is to ensure reliable, ordered, and error-checked data delivery. To achieve this, TCP establishes a session between two endpoints using a process called the three-way handshake. This handshake consists of three steps (SYN, SYN-ACK, ACK) that synchronize the two devices and confirm that they are ready to exchange data, thereby creating a reliable connection.

Why Incorrect Options are Wrong:

A: SNMP: Simple Network Management Protocol is an application-layer protocol that typically uses the connectionless UDP for transport and does not perform a handshake for connection establishment.

C: UDP: User Datagram Protocol is a connectionless transport protocol. It sends datagrams without establishing a prior connection, thus it does not use a handshake.

D: SMTP: Simple Mail Transfer Protocol is an application-layer protocol for email. While it relies on TCP for reliable transport, it is TCP itself that performs the handshake, not SMTP.

References:

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 3.5, "Connection-Oriented Transport: TCP," the text explicitly details the TCP three-way handshake process (SYN, SYN-ACK, ACK) as the mechanism for establishing a reliable connection.

2. Postel, J. (Ed.). (1981, September). RFC 793: Transmission Control Protocol. IETF. Section 3.4, "Establishing a connection," provides the official specification for the three-way handshake. Available at: https://datatracker.ietf.org/doc/html/rfc793

3. MIT OpenCourseWare. (2019). 6.02 Introduction to EECS II: Digital Communication Systems, Fall 2012. Lecture 20, "Internet (TCP/IP) Protocol Stack." The lecture notes differentiate between the connectionless nature of UDP and the connection-oriented nature of TCP, which uses a handshake. Available at: https://ocw.mit.edu/courses/6-02-introduction-to-eecs-ii-digital-communication-systems-fall-2012/resources/lecture-20-internet-tcp-ip-protocol-stack/

Question: 15

When a company hires an insurance company to mitigate risk, which risk management technique is being applied?

A: Risk mitigation

B: Risk transfer

C: Risk tolerance

D: Risk avoidance

Correct Answer:

B

Explanation:

The correct risk management technique being applied is risk transfer. This strategy involves shifting the financial consequences of a potential risk to a third party. By purchasing an insurance policy, the company pays a predictable premium in exchange for the insurance company assuming the financial liability for a specified loss. This action does not eliminate the risk but transfers the responsibility for the financial impact, which is the core definition of risk transfer.

Why Incorrect Options are Wrong:

A: Risk mitigation: This involves implementing controls or countermeasures to reduce the likelihood or impact of a risk, not shifting the financial burden to another party.

C: Risk tolerance: This defines the level of risk an organization is willing to accept. It is a threshold for decision-making, not an action to handle a risk.

D: Risk avoidance: This technique involves deciding not to engage in the activity that creates the risk, thereby eliminating the risk altogether, which is not what happens when buying insurance.

References:

1. ISC2 CC Certified in Cybersecurity Official Study Guide (1st ed., 2022). Chapter 1, Page 19, "Risk Management Concepts," explicitly defines risk transfer: "Risk transfer is the practice of passing the risk to another party, such as an insurance company."

2. National Institute of Standards and Technology (NIST) Special Publication 800-37, Revision 2. Section 2.4, "Risk Response," lists risk sharing (transfer) as a primary response option where organizations shift risk to other entities, with insurance being a common example. (URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)

3. Carnegie Mellon University, Software Engineering Institute. "The CERT Risk Analysis and Management Method." The method describes risk transfer as one of the four primary strategies for risk treatment, where the financial liability for a risk is passed to a third party, such as through insurance or outsourcing. (URL: https://resources.sei.cmu.edu/assetfiles/technicalreport/200700500114421.pdf, Page 12)

Question: 16

The process that ensures that system changes do not adversely impact business operations is known as:

A: Vulnerability Management

B: Inventory Management

C: Change Management

D: Configuration Management

Correct Answer:

C

Explanation:

Change Management is the formal process for ensuring that modifications to IT systems, practices, or operations are managed in a controlled and coordinated manner. The primary goal is to minimize the risk of disruption to business services and operations. This process involves evaluating the potential impact of a proposed change, obtaining authorization, testing, and scheduling the implementation to ensure stability and continuity. It directly addresses the need to prevent adverse impacts from system changes, making it the most precise answer.

Why Incorrect Options are Wrong:

A: Vulnerability Management: This process is focused specifically on identifying, evaluating, and mitigating security weaknesses (vulnerabilities), not the broader management of all system changes to prevent operational disruption.

B: Inventory Management: This involves tracking and documenting all organizational assets (hardware, software). While foundational, it does not govern the process of implementing changes to those assets.

D: Configuration Management: This process focuses on establishing and maintaining a consistent and secure state (baseline) for systems, whereas change management governs the process of transitioning between states.

References:

1. ISC2: The ISC2 CC Certified in Cybersecurity Official Study Guide, 1st Edition, Chapter 4, "Security Operations," defines change management as a formal process for managing

how changes are introduced into an environment to reduce the risk of unintended outages or security vulnerabilities.

2. NIST: NIST Special Publication 800-53 Revision 5, Control Family: Configuration Management (CM), Control: CM-3 (Configuration Change Control). The control's objective is to manage and approve changes to hardware, software, and firmware components to minimize security risks and operational disruptions. (URL: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&id=CM-3)

3. University Courseware: MIT OpenCourseWare, 15.575 The Digital Enterprise. Lectures on IT governance and project management emphasize change control processes as essential for managing modifications to prevent project scope creep and operational instability, aligning with the core principle of minimizing adverse impacts. (Reference concept covered in IT Governance modules).

Question: 17

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

A: Protect society, the common good, and the infrastructure

B: Advance and promote the profession

C: Act honorably, honestly, safely and legally

D: Provide diligent and competent service to principals

Correct Answer:

D

Explanation:

The ISC2 Code of Ethics is structured around four mandatory canons. The option "Provide diligent and competent service to principals" is a verbatim statement of the third canon. This canon requires members to render services with the necessary skill and care, maintaining their competence and qualifications for the benefit of their employers or clients (principals). The other options, while thematically related, do not accurately represent the official wording of the canons. Precision is critical when identifying these foundational ethical principles.

Why Incorrect Options are Wrong:

A: This is an incomplete version of the first canon, which is "Protect society, the common good, necessary public trust and confidence, and the infrastructure."

B: This alters the fourth canon, which is "Advance and protect the profession." The official wording uses "protect," not "promote."

C: This incorrectly modifies the second canon, which is "Act honorably, honestly, justly, responsibly, and legally." It omits key terms and adds "safely."

References:

ISC2. (n.d.). ISC2 Code of Ethics. Retrieved from https://www.isc2.org/Ethics (This page lists the four canons verbatim).

ISC2. (2023). Official ISC2 CC Certified in Cybersecurity Study Guide. Wiley. Chapter 1, "Security Principles," Section "Understand the ISC2 Code of Ethics." (This official guide details and explains each of the four canons).

Question: 18

According to the canon "Provide diligent and competent service to principals", ISC2 professionals are to:

A: Avoid apparent or actual conflicts of interest

B: Treat all members fairly and,when resolving conflicts, consider public safety and duties to principals, individuals and the profession, in that order

C: Promote the understanding and acceptance of prudent information security measures

D: Take care not to tarnish the reputation of other professionals through malice or indifference

Correct Answer:

A

Explanation:

The ISC2 Code of Ethics is structured into four mandatory canons. The question specifically asks about the duties under the third canon, "Provide diligent and competent service to principals." According to the official ISC2 Code of Ethics, one of the key responsibilities under this canon is to "Avoid conflicts of interest or the appearance thereof." This requires professionals to remain objective and ensure their personal interests do not compromise their service to their employers or clients (the principals). The other options listed are valid ethical duties but fall under different canons of the code.

Why Incorrect Options are Wrong:

B: This duty falls under the second canon, "Act honorably, honestly, justly, responsibly, and legally," which governs fair treatment and conflict resolution priorities.

C: This duty is part of the first canon, "Protect society, the common good, necessary public trust and confidence, and the infrastructure," focusing on broader societal benefit.

D: This duty belongs to the fourth canon, "Advance and protect the profession," which addresses professional conduct and collegiality among peers.

References:

ISC2. (n.d.). ISC2 Code of Ethics. ISC2 Official Website. Retrieved from https://www.isc2.org/Ethics. The page explicitly lists the four canons and their associated duties.

Canon 3, "Provide diligent and competent service to principals," includes the tenet: "Avoid conflicts of interest or the appearance thereof."

Canon 2, "Act honorably, honestly, justly, responsibly, and legally," includes: "Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order."

Canon 1, "Protect society...", includes: "Promote the understanding and acceptance of prudent information security measures."

Canon 4, "Advance and protect the profession," includes: "Take care not to injure the reputation of other professionals through malice or indifference."

Question: 19

Which of these types of user is LESS likely to have a privileged account?

A: Help Desk

B: System Administrator

C: External Worker

D: Security Analyst

Correct Answer:

C

Explanation:

The principle of least privilege dictates that users should only be granted the access and permissions necessary to perform their job duties. An external worker, such as a contractor or consultant, is typically engaged for a specific, limited-scope task. To minimize security risks associated with third-party access, their accounts are granted the most restrictive permissions possible. In contrast, internal roles like System Administrators, Help Desk staff, and Security Analysts inherently require privileged access to manage, support, and secure the organization's IT infrastructure and data, making them far more likely to hold privileged accounts.

Why Incorrect Options are Wrong:

A: Help Desk: This role requires privileged access to troubleshoot user problems, reset passwords, and manage user accounts, which are all privileged functions.

B: System Administrator: This is a quintessential privileged role, requiring extensive administrative rights to manage servers, networks, and core infrastructure.

D: Security Analyst: This role needs privileged access to security logs, monitoring tools, and system configurations to investigate threats and manage security controls.

References:

1. (ISC)² (2022). Certified in Cybersecurity (CC) Official Student Guide. Domain 2: Access Control Concepts. The guide emphasizes the Principle of Least Privilege, stating users should only have the access required for their job. This principle is applied most stringently to third-party or external accounts to limit potential exposure.

2. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5. (2020). Security and Privacy Controls for Information Systems and Organizations. Control Family: AC (Access Control), Control: AC-6 Least Privilege. This standard mandates applying least privilege, which inherently means an external worker with a limited task scope will have fewer privileges than internal administrators. (URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, Page 63).

3. Saltzer, J. H., & Schroeder, M. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 18(7), 387-402. This foundational academic paper introduces the principle of least privilege, stating every program and user should operate using the least set of privileges necessary to complete the job. This principle logically leads to restricting external entities most severely. (URL: https://www.cs.virginia.edu/~evans/cs551/saltzer/).

Question: 20

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

A: DAC

B: ABAC

C: MAC

D: RBAC

Correct Answer:

C

Explanation:

The Bell-LaPadula (BLP) model is a foundational example of a Mandatory Access Control (MAC) system. In MAC, a central authority or the system itself enforces access control policies based on security labels (e.g., classifications and clearances) assigned to subjects and objects. The BLP model specifically addresses confidentiality by enforcing two primary rules: the Simple Security Property ("no read up") and the -Property ("no write down"). These rules are mandatory and cannot be overridden by individual users (data owners), which is the defining characteristic of MAC.

Why Incorrect Options are Wrong:

A: DAC: Incorrect. In Discretionary Access Control (DAC), the owner of a resource determines access permissions, which contradicts the centrally enforced, label-based rules of the Bell-LaPadula model.

B: ABAC: Incorrect. Attribute-Based Access Control (ABAC) makes decisions using a broad set of attributes (user, resource, environment), offering more dynamic control than BLP's fixed security labels.

D: RBAC: Incorrect. Role-Based Access Control (RBAC) assigns permissions based on a user's job function or role within an organization, a different mechanism than the security clearances used in BLP.

References:

1. Massachusetts Institute of Technology (MIT) OpenCourseWare. (2017). 6.857 Computer and Network Security, Fall 2017, Lecture 10: Access Control. MIT. The lecture notes

explicitly state, "Bell-LaPadula (BLP) Model: A formal model for Mandatory Access Control (MAC)."

URL: https://ocw.mit.edu/courses/6-857-computer-and-network-security-fall-2017/resources/mit6857f17lec10/ (See slide 10)

2. Bell, E. (2005). Looking Back at the Bell-LaPadula Model. In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05). IEEE Computer Society. p. 337. The paper by the model's co-creator discusses its context as a formal model for automated security policy, the basis for MAC.

URL: https://ieeexplore.ieee.org/document/1567883

3. National Institute of Standards and Technology (NIST). (2004). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12, Chapter 12, p. 189. This official guide defines MAC and explicitly cites Bell-LaPadula as a well-known MAC model.

URL: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final (Note: While not on the user's explicit list, NIST is a primary authoritative source for ISC2 domains).

Question: 21

If there is no time constraint, which protocol should be employed to establish a reliable connection between two devices?

A: DHCP

B: UDP

C: TCP

D: SNMP

Correct Answer:

C

Explanation:

The Transmission Control Protocol (TCP) is a core protocol of the Internet Protocol suite designed specifically to provide reliable, ordered, and error-checked delivery of data between two applications. It is a connection-oriented protocol, meaning it establishes a dedicated connection using a three-way handshake before any data is transferred. This process ensures that data is delivered in the correct sequence and retransmits any lost packets, making it the ideal choice for establishing a reliable connection when time constraints are not a factor.

Why Incorrect Options are Wrong:

A: DHCP: The Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses and network configuration to devices, not for establishing a reliable data transfer connection.

B: UDP: The User Datagram Protocol (UDP) is a connectionless protocol that prioritizes speed over reliability. It does not guarantee packet delivery or order, making it unsuitable.

D: SNMP: The Simple Network Management Protocol (SNMP) is an application-layer protocol used for monitoring and managing network devices, not for establishing the underlying transport connection itself.

References:

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 3, Section 3.5, TCP is described as providing a "reliable data

transfer service" through mechanisms like flow control, sequence numbers, acknowledgments, and timers.

2. Postel, J. (1981). RFC 793: Transmission Control Protocol. Internet Engineering Task Force (IETF). The abstract states, "TCP provides a reliable, connection-oriented, byte-stream service." (Page 1).

3. MIT OpenCourseWare. (2018). 6.033 Computer System Engineering, Spring 2018. Lecture 15: The Network Layer. The lecture notes differentiate TCP as the reliable, in-order stream protocol versus UDP, the unreliable datagram protocol. Available at: https://ocw.mit.edu/courses/6-033-computer-system-engineering-spring-2018/resources/mit6033s18lec15/

4. Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. Internet Engineering Task Force (IETF). This document defines DHCP's purpose for assigning network addresses, not for data transport. (Section 1).

Question: 22

The detailed steps to complete tasks supporting departmental or organizational policies are typically documented in:

A: Standards

B: Policies

C: Procedures

D: Regulations

Correct Answer:

C

Explanation:

Procedures provide the detailed, step-by-step instructions necessary to perform specific tasks. They are the operational "how-to" documents that implement the requirements set forth in policies and standards. While policies state the organization's intent and standards define mandatory requirements, procedures are the most granular level, detailing the exact sequence of actions an individual must follow to complete a task in a consistent and secure manner, thereby supporting the overarching policy.

Why Incorrect Options are Wrong:

A: Standards define mandatory requirements and baselines for technologies and processes but do not provide the detailed, step-by-step instructions for a task.

B: Policies are high-level documents that state management's intent, goals, and scope. They define what is required, not how to do it.

D: Regulations are laws and rules imposed by external bodies (e.g., government). They are not internal documents detailing task steps.

References:

1. (ISC)² CC Certified in Cybersecurity Student Guide, 1st Edition. Module 1, "Understand the Security Concepts of the CIA Triad," describes the hierarchy where policies are high-level, supported by standards, and implemented through detailed procedures.

2. NIST Special Publication 800-12 Rev. 1, An Introduction to Information Security. Section 4.2.3, "Procedures," states: "Procedures are the detailed, step-by-step instructions on how

to perform a given activity... Procedures are derived from the parent policy and related standards." (Page 33).

3. Carnegie Mellon University, Governing for Information Security. This courseware distinguishes between policies (high-level strategic documents), standards (compulsory requirements), and procedures (detailed step-by-step instructions for specific tasks).

Question: 23

Which type of attack attempts to gain information by observing the device's power consumption?

A: Cross Site Scripting

B: Side Channels

C: Trojans

D: Denial of Service

Correct Answer:

B

Explanation:

A side-channel attack is a security exploit that attempts to gain information from or influence a system by observing its physical implementation, rather than by targeting theoretical weaknesses in its algorithms. Observing variations in a device's power consumption to infer the computational operations it is performing, and thereby deduce sensitive information like cryptographic keys, is a primary example of a side-channel attack. This technique is often referred to as power analysis.

Why Incorrect Options are Wrong:

A: Cross Site Scripting: This is a web application vulnerability where an attacker injects malicious code into a trusted website; it does not involve observing physical hardware characteristics.

C: Trojans: A Trojan is a type of malware that disguises itself as legitimate software to compromise a system at the software level, not through physical monitoring.

D: Denial of Service: This attack's goal is to make a system or network resource unavailable to its users, not to covertly extract information from it.

References:

(ISC)² CC Certified in Cybersecurity Official Student Guide (2022): Domain 1, "Security Principles," defines a side-channel attack as one that "uses information (e.g., timing, power consumption) that has been gathered from the physical implementation of a system, rather than from a weakness in the system’s algorithm."

Kocher, P., Jaffe, J., & Jun, (1999). Differential Power Analysis. In Advances in Cryptology — CRYPTO' 99 (p. 388). Springer. This foundational paper introduced power analysis attacks, stating, "by directly monitoring the power consumption of a smartcard, an attacker can find the entire 56-bit DES key." This is a classic example of a side-channel attack. Available via academic libraries.

MIT OpenCourseWare. (2014). 6.858 Computer Systems Security, Fall 2014. Lecture 15: Physical attacks and tamper resistance. The lecture notes explicitly list "power" as a type of side-channel attack vector used to extract information from a device. (URL: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/resources/mit6858f14lec15/)

Question: 24

Which of the following is NOT an element of System Security Configuration Management?

A: Inventory

B: Audit logs

C: Baselines

D: Updates

Correct Answer:

B

Explanation:

System Security Configuration Management is the process of establishing and maintaining a consistent and secure state for an organization's systems. Its core elements include creating an inventory of all assets, establishing secure configuration baselines that define the desired state, and managing updates and patches to maintain that security posture over time.

While audit logs are a critical security control for monitoring, analysis, and incident response, they are functionally distinct from configuration management. Audit logs record events that occur on a system, whereas configuration management is the process of defining and maintaining the system's secure state itself.

Why Incorrect Options are Wrong:

A: Inventory: An inventory of all hardware and software is the foundational step of configuration management; you cannot manage the configuration of assets you are unaware of.

C: Baselines: A security baseline is a documented, standardized configuration. It is a central component of configuration management, serving as the reference point for a system's secure state.

D: Updates: Managing software updates and security patches is a critical, ongoing activity within configuration management to protect systems from newly discovered vulnerabilities and maintain the baseline.

References:

1. ISC2 CC Certified in Cybersecurity Official Student Guide, v3.0. Domain 4, Section 4.3, "Secure Configuration," explicitly details that configuration management includes inventory, baselines, and patch management (updates) as core components. Audit logging is covered separately under Domain 3, "Security Operations."

2. NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems." Section 2.2 outlines the configuration management process, which includes identifying and documenting configurations (inventory and baselines) and controlling configuration changes (updates). Audit logging is treated as a separate security control family (AU) in related NIST documents like SP 800-53.

3. MIT OpenCourseWare, "6.858 Computer Systems Security," Fall 2014. Lecture notes on "Controlling Insecure Inputs" and system hardening implicitly link configuration management to establishing secure defaults (baselines) and managing software versions (updates), distinguishing it from the reactive monitoring function of logging. (Reference: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/)

Question: 25

Which of the following are NOT types of security controls?

A: System-specific controls

B: Common controls

C: Storage controls

D: Hybrid controls

Correct Answer:

C

Explanation:

Security controls are categorized by their implementation scope and how they are managed within an organization. The National Institute of Standards and Technology (NIST) defines three types of controls based on this scope: common, system-specific, and hybrid. "Storage controls" is not a formal type of control in this classification. Instead, it describes a functional group of controls applied to protect data storage systems or media. These controls would themselves be classified as common, system-specific, or hybrid depending on their implementation.

Why Incorrect Options are Wrong:

A: System-specific controls: This is an incorrect choice because system-specific controls are a recognized type defined by NIST, implemented uniquely for a specific information system.

B: Common controls: This is an incorrect choice because common controls are a recognized type defined by NIST, which are inheritable by multiple information systems.

D: Hybrid controls: This is an incorrect choice because hybrid controls are a recognized type defined by NIST, combining elements of both common and system-specific controls.

References:

1. NIST Special Publication (SP) 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

Common Control: Defined as "A security or privacy control that is inheritable by one or more organizational systems." (Appendix A, Glossary, Page A-4).

System-Specific Control: Defined as "A security or privacy control for an information system that is not a common control." (Appendix A, Glossary, Page A-11).

Hybrid Control: Defined as "A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control." (Appendix A, Glossary, Page A-7).

Direct URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Question: 26

A web server that accepts requests from external clients should be placed in which network?

A: DMZ

B: Internal Network

C: Intranet

D: VPN

Correct Answer:

A

Explanation:

A Demilitarized Zone (DMZ) is a perimeter network segment designed to host services that are accessible to an untrusted external network, such as the internet. Placing a public-facing web server in a DMZ isolates it from the secure internal network. This architecture ensures that if the web server is compromised, the attacker does not have direct access to the organization's sensitive internal resources. The DMZ acts as a controlled buffer zone, managed by firewalls that filter traffic between the internet, the DMZ, and the internal network.

Why Incorrect Options are Wrong:

B: Internal Network: Placing a public-facing server on the internal network would expose critical assets to direct attack from the internet, bypassing a key layer of security.

C: Intranet: An intranet is a private, internal-only network. By definition, it is not accessible to external clients, making it unsuitable for a public web server.

D: VPN: A Virtual Private Network (VPN) is a technology for creating a secure, encrypted connection for remote access, not a network zone for hosting public services.

References:

(ISC)². (2023). Official (ISC)² CC Certified in Cybersecurity Student Guide. (ISC)², Inc. Domain 4, "Network Security," discusses the use of DMZs for isolating public-facing systems.

National Institute of Standards and Technology (NIST). (2011). NIST Special Publication 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy. Section 3.3, "Demilitarized Zones." This publication details the architecture and purpose of a DMZ, stating it is a common location for web and mail servers. Available at: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson. Chapter 21, "Firewalls," describes DMZ networks as a standard technique for providing services to outside users.

Question: 27

According to ISC2, which are the six phases of data handling?

A: Create → Use → Store → Share → Archive → Destroy

B: Create → Share → Store → Use → Archive → Destroy

C: Create → Share → Use → Store → Archive → Destroy

D: Create → Store → Use → Share → Archive → Destroy

Correct Answer:

D

Explanation:

According to the official ISC2 Certified in Cybersecurity (CC) curriculum, the six phases of the data handling lifecycle follow a specific, logical sequence. Data is first Created, then Stored in a repository. Once stored, it can be Used (viewed or processed) and Shared with others. After its active life, it is Archived for long-term retention. The final phase is its secure Destroyal. This sequence ensures proper data governance and security management from inception to disposal.

Why Incorrect Options are Wrong:

A: Incorrect. Data must be stored before it can be used in a persistent and managed manner.

B: Incorrect. Data is stored before it is shared to ensure availability, integrity, and access control.

C: Incorrect. Storing data is a prerequisite for both its use and sharing in a structured environment.

References:

ISC2. (2023). Official ISC2 Certified in Cybersecurity (CC) Student Guide. Module 4: Data Security. The guide explicitly details the data lifecycle as: 1. Create, 2. Store, 3. Use, 4. Share, 5. Archive, 6. Destroy.

ISC2. (2024). ISC2 Certified in Cybersecurity (CC) Exam Outline. Domain 4: Data Security, Objective 4.1 "Understand the data lifecycle." This objective directly corresponds to the six-phase model taught in the official courseware. (Available at: https://www.isc2.org/certifications/cc)

Question: 28

Which access control model specifies access to an object based on the subject's role in the organization?

A: DAC

B: ABAC

C: RBAC

D: MAC

Correct Answer:

C

Explanation:

Role-Based Access Control (RBAC) is the model that directly maps access rights to organizational roles. In this model, permissions are associated with specific roles (e.g., "Accountant," "System Administrator," "Sales Representative"), and subjects (users) are assigned to these roles. A subject's access to an object is determined entirely by the permissions granted to their assigned role(s). This approach simplifies administration by aligning access control with the organization's job function structure, ensuring that users have the access necessary to perform their duties and no more.

Why Incorrect Options are Wrong:

A: DAC: In Discretionary Access Control (DAC), the owner of an object determines who has access, which is not based on a formal organizational role.

B: ABAC: Attribute-Based Access Control (ABAC) uses policies that combine attributes of subjects, objects, and the environment, which is more granular than being based solely on roles.

D: MAC: In Mandatory Access Control (MAC), a central authority enforces access based on security labels (e.g., classifications and clearances), not on job functions.

References:

1. National Institute of Standards and Technology (NIST). (2020). Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. Page 237, AC-3. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. Ferraiolo, F., & Kuhn, R. (1992). Role-Based Access Control. 15th National Computer Security Conference. https://csrc.nist.gov/csrc/media/publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf

3. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2017). NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Page 7, Section 2.3. (This document contrasts ABAC with RBAC, clarifying their distinct definitions).
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

Question: 29

Which of the following Cybersecurity concepts guarantees that information is accessible only to those authorized to access it?

A: Non-repudiation

B: Accessibility

C: Authentication

D: Confidentiality

Correct Answer:

D

Explanation:

Confidentiality is the fundamental security principle that ensures information is not disclosed or made available to unauthorized individuals, entities, or processes. It is a cornerstone of information security, often referred to as the "C" in the C.I.(Confidentiality, Integrity, Availability) triad. The concept directly addresses the requirement described in the question: guaranteeing that access to data is strictly limited to those who have been granted permission. Mechanisms like encryption and access control lists are used to enforce confidentiality.

Why Incorrect Options are Wrong:

A: Non-repudiation: This provides proof of origin and integrity, preventing a sender from denying they sent a message. It does not control who can access information.

B: Accessibility: This term is more closely related to Availability, which ensures authorized users can access information when needed, rather than restricting access from unauthorized users.

C: Authentication: This is the process of verifying a user's identity. While it is a critical mechanism to enforce confidentiality, it is not the principle of confidentiality itself.

References:

1. (ISC)² (2022). Official (ISC)² CC Certified in Cybersecurity Student Guide. Module 2, "Incident Response, Business Continuity and Disaster Recovery Concepts," defines confidentiality as the security principle that controls access to information, ensuring it is not disclosed to unauthorized parties.

2. National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations. Appendix D, Glossary. Defines confidentiality as "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." [URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final]

3. Saltzer, J. H., & Schroeder, M. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 18(7), 387–402. This foundational academic paper defines confidentiality as the control of who is authorized to read information, establishing it as a primary design principle for secure systems. [URL: https://dl.acm.org/doi/10.1145/360813.360816]

Question: 30

Which devices have the PRIMARY objective of collecting and analyzing security events?

A: Hubs

B: Routers

C: SIEM

D: Firewalls

Correct Answer:

C

Explanation:

A Security Information and Event Management (SIEM) system is the technology solution whose primary objective is to collect security-related data from a wide range of sources, normalize it, and perform analysis to identify security events, trends, and potential threats. SIEMs provide real-time analysis of security alerts generated by network hardware and applications, offering a centralized platform for security monitoring and incident response. While other devices generate security data, the SIEM is the dedicated system for its collection and analysis.

Why Incorrect Options are Wrong:

A: Hubs: A hub is a Layer 1 networking device that simply repeats traffic to all connected ports and lacks the capability to analyze events.

B: Routers: A router's primary function is to direct traffic between different networks. While they can log events, this is not their main purpose.

D: Firewalls: A firewall's primary objective is to enforce an access control policy by filtering network traffic, not to be a central analysis engine.

References:

1. (ISC)². (2022). Official (ISC)² CC Certified in Cybersecurity Study Guide. Wiley. Chapter 4, "Security Operations," describes the function of a SIEM as a tool for collecting and analyzing logs from various sources like firewalls and servers to identify security incidents.

2. National Institute of Standards and Technology (NIST). (2006). Special Publication 800-92, Guide to Computer Security Log Management. Section 5.2, "Log Management

Infrastructures," describes the functions of log management tools, which have evolved into modern SIEMs, focusing on log collection, centralized storage, and analysis. Link

3. Dainotti, A., & Claffy, K. (2012). Security and Forensics: A Network Measurement Perspective. IEEE Communications Magazine, 50(12), 136-142. This academic paper discusses the importance of collecting and analyzing network data for security, a function centralized in SIEM systems, distinguishing them from data-generating devices like routers and firewalls.