I'm not a bot

Cissp exam sample questions

This CISSP mock test helps you analyze your performance so that you can focus on your weaker areas. If your performance is not satisfactory, you can re-take it any number of times. For further improvement, you can refer our CISSP Certification Training Course. The Cyber Security Expert Master's Program will equip you with the skills needed to become an expert in this rapidly growing domain. You will learn comprehensive approaches to protecting your infrastructure, including securing data and information, running risk analysis and mitigation, architecting cloud-based security, achieving compliance and much more with this best-in-class program. Home / Cyber Security / CISSP / CISSP Practice Exam – FREE 20 Questions and Answers 20 min. readCISSP or Certified Information Systems Security Professional is one of the world's most valued and sought-after certifications in information security. The CISSP certification exam is challenging. Hence, successfully passing it requires in-depth insights and a solid understanding of the core information security concepts. Not just this, you also need to dedicate 40 to 70 hours of study for the exam preparation, you must bear the CISSP certification cost and you must fully understand the CISSP study material and be ready for the exam. And CISSP practice test questions will be one of the most helpful study materials during your CISSP certification journey. The more you practice, the more you will double your chances to pass the CISSP test on your first attempt. Why Should You Go Through the CISSP Practice Exam? Once you have decided to start your CISSP certification journey, make sure you are successful in it. One of the proven 7 steps in the CISSP Study Guide to fully prepare for the CISSP certification exam is to practice the CISSP practice exam multiple times. Going through the CISSP practice exam helps you find out your weaknesses and strengths. With the help of the CISSP practice exam, you will be able to know which domain of the CISSP content you need to focus on more. If you are not scoring over 70% in the CISSP practice exams you are taking, we strongly recommend you enroll and proceed with a comprehensive CISSP certification training program. Note that, before starting your CISSP journey, we recommend you to check CISSP certification requirements if you satisfy them. You can take a look at our 30 mins Free CISSP Training demo. The 20 CISSP Practice Questions The CISSP practice exam that we have prepared in this post covers the key concepts in each of the 8 domains included in the CISSP certification exam. The CISSP practice test questions provide the answers as well as rationales to give you more understanding of the topic. These 20 sample CISSP questions will allow you to familiarize yourself with the CISSP exam questions. These will also help you reinforce your learning and prepare for the real CISSP test in the near future. After helping thousands of professionals in more than 180 countries with a 99.6% first attempt pass rate, we have prepared a seven-step CISSP study guide. Read this CISSP study guide and create your own CISSP prep plan accordingly. Let's Begin the CISSP Practice Exam! Let us take you through our sample CISSP practice exam below. Once you finish this, you may try our free CISSP exam simulator for more CISSP practice exam questions. So, move on and test your knowledge of the CISSP exam content now. CISSP Practice Exam Questions and Answers #1 "The State Machine Model" security model mandates that a system must be protected in all of its states (Startup, Function, and Shutdown), or else the system is not secure. This requirement necessitates responding to security events so that no further compromises can be successful. This method of response is an example of what security concept? a. Open Design b. Closed Design c. Trusted Recovery d. Least Privilege Answer: C Trusted Recovery is necessary for high-security systems and allows a system to terminate its processes in a secure manner. If a system crashes, it must restart in a secure mode in which no further compromise of system policy can occur. The principle of open design states that the security of a mechanism should not depend on the secrecy of its design or implementation. In object-oriented programming, the open-closed principle states that "software entities (classes, modules, functions, etc.) should be open for extension, but closed for modification"; that is, such an entity can allow its behavior to be extended without modifying its source code. The least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. CISSP Sample Questions and Answers #2 The Heartbleed virus recently compromised OpenSSL because versions of OpenSSL were vulnerable to memory content read attempts, which ultimately led to the exposure of protected information including services provider private keys. Many practitioners believe that open design is better than closed design. What one consideration is usually necessary to allow an open design to provide greater security? a. Peer Review b. Security through obscurity c. The complexity of design d. Trusted hierarchy Answer: A Open design is often thought to be better than closed design, as openness allows for review from others in the community. The idea is that if others have access to the code, they will help examine and review the code, and ultimately improve it. That was not the case unfortunately with OpenSSL. If the code is not reviewed, it might as well be a closed source. Also, ultimately the quality of the code dictates the security, much more so than whether it is open or closed. Security through obscurity is the opposite of peer review and open design and could also be referred to as the complexity of the design. The hierarchical trust model is like an upside-down tree structure, the root is the starting point of trust. All nodes of the model have to trust the root CA and keep a root CA's public-key certificate. CISSP Practice Test Questions and Answers #3 When using private keys a security concern is that a user's private key may become lost. In order to mitigate this risk, a practitioner may select a key recovery agent that is able to backup and recover his keys. Granting a single individual the ability to recover users' private keys increases nonrepudiation risk because another party has key access. Which principle choice could be implemented to mitigate this risk? a. Segregation of duties b. Principle of least privilege c. Dual control d. Need to know Answer: C Dual Control is a security principle that requires multiple parties to be present for a task that might have severe security implications. In this instance, it is likely best to have at least two network administrators present before a private key can be recovered. A subset of dual control is called M of N control. M and N are variables, but this control requires M out of a total of N administrators to be present to recover a key. Segregation of Duties is the concept of having more than one person required to complete a sensitive task. The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access or permissions needed to perform his job functions. The need-to-know principle is that access to secured data must be necessary for the conduct of the users' job functions CISSP Practice Exam Questions and Answers # 4 At what BCP development phase must Senior Management provide its commitment to support, fund, and assist the BCP's creation? a. Project Initiation b. Planning c. Implementation d. Development Answer: A Project Initiation is traditionally the phase in which senior management pledges its support for the project. Often in this phase, management provides a project charter, which is a formal written document in which the project is officially authorized, a project manager is selected and named, and management makes a commitment to support. Management's BCP support must continue through the whole development process and include review and feedback as well as resources for the BCP to be successful. CISSP Questions and Answers #5 What is the most proactive (and minimum effort) way to mitigate the risk of an attacker gaining network access and using a protocol analyzer to capture and view (sniff) unencrypted traffic? a. Implement a policy that forbids the use of packet analyzers/sniffers. Monitor the network frequently. b. Scan the network periodically to determine if unauthorized devices are connected. If those devices are detected, disconnect them immediately, and provide management a report on the violation c. Provide security such as disabling ports and mac filtering on the enterprise switches to prevent an unauthorized device from connecting to the network. Implement software restriction policies to prevent unauthorized software from being installed on systems. d. Install anti-spyware software on all systems on the network. Answer: C To significantly mitigate risks on the network, we have to implement security that limits connectivity to our network from external devices. Additionally, we are concerned with monitoring software being installed on our hosts, so we want to limit the ability of such software to be installed. Further, we want to ensure that other basic security requirements are satisfied, such as using strong passwords, lockout policies on systems, physical security, etc. Remember: Proactive devices PREVENT an attack, as opposed to responding to it. Network scans often detect these devices, but they rarely prevent them. Policies describe high-level enterprise intentions which can then be implemented. Installing antispyware is a detective/corrective control, not a proactive/preventative one. CISSP Practice Questions and Answers #6 Confidentiality can be breached via social engineering attacks. Though training is helpful in reducing the number of these attacks, it does not eliminate the risk. Which of the following choices would be an administrative policy that is most likely to help mitigate this risk? a. Formal onboarding Policies b. Job Rotation c. Formal Off-boarding Policies d. Segregation of Duties Answer: D Segregation of Duties is frequently used to limit the amount of information to which any one individual has access. E.G. a user cannot likely leak the password for a file server because that information is exclusively available for those for whom jobs require access to that information. Segregation of duties frequently goes hand-in-hand with need-to-know and the principle of least privilege. Formal onboarding would increase user awareness but would not necessarily be a preventative control. Job rotation would limit the risk of a user conducting fraud, but not the risk of social engineering. Formal offboarding would not have any effect on social engineering risk. CISSP Sample Questions and Answers #7 Specific system components determine that system's security. The trust in the system is a reflection of the trust in these components. These components are collectively referred to as the _____ of the system. a. Ring 1 elements b. Trusted Computing Base c. Operating System Kernel d. Firmware Answer: B The TCB (Trusted Computer Base) describes the elements of a system that enforce the security policy and are used to determine the security capabilities of a system. This term was coined by the Orange Book. Ring 1 elements is a mathematical term. The kernel is a computer program at the core of a computer's operating system that has complete control over everything in the system. It is the "portion of the operating system code that is always resident in memory", and facilitates interactions between hardware and software components. (Also known as the Trusted Computer System evaluation criteria). Some components included in the TCB are the system BIOS, the CPU, Memory, and the OS kernel. In computing, firmware[a] is a specific class of computer software that provides low-level control for a device's specific hardware. Firmware can either provide a standardized operating environment for more complex device software (allowing more hardware independence) or, for less complex devices, act as the device's complete operating system, performing all control, monitoring, and data manipulation functions. Learn more in our Free CISSP Training. CISSP Practice Exam Questions and Answers #8 Whenever a subject attempts to access an object, that access must be authorized. During this access, the set of conceptual requirements must be verified by the part of the operating system kernel that deals with security. The conceptual ruleset is known as the _____, while the enforcement mechanism is referred to as the _____ a. Access Control List, Security Enforcer b. Security Enforcer, Access Control List c. Reference Monitor, Security Kernel d. Security Kernel, Reference Monitor Answer: C As a subject attempts to access an object, two of the main elements that control access are the Reference Monitor and the Security Kernel. The Reference Monitor is the conceptual rule set that defines access while the Security Kernel includes the hardware, software, or firmware that enforces the rules set. An access control list (ACL) is a table that tells a computer operating system what access rights each user has to a particular system object, such as a file directory or individual file. Security enforcer is a made-up term. CISSP Sample Questions and Answers #9 A fundamental security principle is that security controls must be aligned with business objectives. Based on the impact security has upon an organization's success, why is the concept of business alignment important? a. There is always a tradeoff for security, so an organization has to weigh the cost vs. benefits of the security measures. b. Security is cheap and easily implemented compared to the potential for loss. Security should be implemented everywhere possible. c. Security is so important that every organization must implement as much as possible. d. Security is too costly to implement in small organizations. Answer: A There is always a trade-off for security. Sometimes the cost comes in actual dollars spent. Often, other times, security negatively affects performance, backward compatibility, and ease of use. An organization must look at the overall objectives of the business considering its primary needs. Sensitive military information must be designed with much more security than a small home/office environment that has information of little to no value to an attacker. The level of implemented security should be commensurate with business needs at a reasonable cost and needs to be crafted to match each enterprise's individual needs. CISSP Practice Exam Questions and Answers #10 A system's minimum security baseline references a system's least acceptable security configuration for a specific environment. Prior to determining the MSB, the system must be categorized based on its data's Confidentiality, Integrity, and Availability needs. When evaluating a system where the potential impact of unauthorized disclosure is "high," the impact of an integrity breach is medium, and the impact of the data being temporarily unavailable is low, what is the overall categorization of the system? a. High b. Medium c. Low d. Medium-high Answer: A For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values from among those security categories that have been determined for each type of information resident in the information system. As the highest category is "High", the system is classified as "High". CISSP Questions and Answers #11 While evaluating a system per the TCSEC and the more recent Common Criteria, Trust and Assurance are two elements that are included in the evaluation scope. Which of the following choices best describes trust and assurance? a. Trust describes how secure the system is, while assurance describes performance capabilities. b. Assurance describes how secure the system is, while trust describes performance capabilities. c. Trust describes the function of the product, while assurance describes the reliability of the process used to create the product. d. Assurance describes the function of the product, while trust describes the reliability of the process used to create the product. Answer: C Trust is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within a system. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome based on the reliability of the processes used to develop the system. CISSP Practice Questions and Answers #12 In 1918, Gilbert Vernam created a means of providing mathematically unbreakable encryption by using a one-time pad that served as a key. Which modern encryption technology is based on the ideas implemented in the Vernam Cipher? a. Asymmetric Cryptography b. Digital Signatures that provide authenticity c. The handshake process used by IPSec and numerous other frameworks d. Session keys Answer: D Sessions keys are used for a single session and are then discarded, as is the one-time pad. Additionally, each session key must be statistically unpredictable and unrelated to the previous key, as the one-time pad requires, as well. Any technology that takes advantage of a short-term password or key can ultimately be traced back to the one-time pad. Asymmetric Cryptography is often used to provide secure session key exchange. Digital signatures are used to verify a message sender and content. IPSec handshaking is used to establish a secure channel. CISSP Practice Exam Questions and Answers #13 During World War II the Germans used the Enigma machine to exchange encrypted messages. It was a rotating disk-based system that used the starting rotor configuration as its secrecy mechanism. When the original system was compromised, the Germans added a fourth rotor to exponentially increase the complexity necessary to break the code. This concept is seen in the relationship between _____. a. AES and Kerberos b. DES/3DES c. RSA and DSA d. RSA and DSA Answer: B DES was originally the standard for protecting sensitive but unclassified information for the US Government. Once DES was compromised the US government needed a quick means to increase its security. 3DES tripled the length of the key from 56 bits to 168 bits. Often a quick means to strengthen a compromised algorithm is to increase the key length or the length of the initialization vector. CISSP Practice Exam Questions and Answers #14 A user receives an email that they believe to have been sent by a colleague. In actuality, the email was spoofed by an attacker. What security services would have indicated that the message was spoofed? a. Privacy b. Authorization c. Integrity d. Non-repudiation Answer: D Non-repudiation is the combination of authenticity and integrity and is implemented through the use of digital signatures. Privacy is involved in protecting private data from disclosure. Authorization is granting users access rights to objects. CISSP Practice Exam Questions and Answers #15 In mail messages, the contents of the message are often encrypted by a symmetric algorithm, likely AES. Non-repudiation, however, is obtained through a combination of hashing and an asymmetric algorithm. How is non-repudiation accomplished? a. By encrypting the document with the sender's private key, then hashing document b. By encrypting the document with the sender's public key, then hashing the document c. By hashing the document and then encrypting the hash with the sender's private key d. By hashing the document then encrypting the hash with the receiver's public key Answer: C A digital signature provides non-repudiation (a combination of integrity and authenticity) for a message. With a digital signature, the message is hashed with a hashing algorithm like SHA-1 or SHA-256. The hash is then encrypted with the sender's private key using an algorithm like RSA. The recipient decrypts the signature with the sender's public key and recalculates the hash from the message. If the two match then both the sender and the message's contents are authenticated. CISSP Practice Exam Questions and Answers #16 A hash should not be able to be reversed to reveal the source contents of the message or file. What provides this secrecy in a hashing algorithm? a. A public key b. A private key c. One-way math d. A digital signature Answer: C Hashes are based on one-way math e.g. math that is very easy to perform one way, but exceedingly difficult to reverse. Passwords are frequently stored as hashes for this reason. If a password is forgotten, a network administrator can't view the password, though they can reset it. CISSP Practice Exam Questions and Answers #17 What is a birthday attack? a. An attack on passwords based on the idea that many users choose weak passwords based on personal information such as birthdays. b. A logic bomb that triggers on the date of the attacker's birthday. c. An attack that attempts to find collisions in separate messages. d. An attack that focuses on personnel databases in an attempt to compromise personal information for the purpose of identity theft. Answer: C A birthday attack is based on the idea that it is easier to find two hashes that just happen to match rather than trying to produce a specific hash. It is called a birthday attack based on the fact that it is easier to find two people in a group whose birthdays just happen to match, rather than someone with a specific birthday. CISSP Practice Exam Questions and Answers #18 If a Layer 1 network issue has caused the lack of communication between hosts, which choice would be the most likely cause? a. Cable b. Router c. Switch d. NIC Answer: A Layer 1 of the OSI Reference Model is referred to as the "Physical Layer" and provides physical connectivity to the network. Cable, connectors, hubs, and any device that is only concerned with creating a means for the physical signal to traverse the network are Layer 1 devices. Though there is an element of a NIC (Network Interface Card) that does provide physical connectivity, most consider it to be a Layer 2 device. A switch is a layer 2 device and a router is a layer 3 device. CISSP Practice Exam Questions and Answers #19 The Data Link Layer (layer 2 of the OSI Model) has two sublayers. The first is MAC (Media Access Control) and it provides a means for determining which system or systems can have access to the transmission media and be allowed to transmit at any given time. Ethernet uses the second method called CSMA/CD (Carrier Sense Multiple Access with Collision Detection.) What does CSMA/CD imply? a. Ethernet environments avoid collisions by detecting their likelihood before transmitting. b. Ethernet environments only allow an individual host to access the cable at any given time and are capable of detecting collisions as they happen. c. Even though Ethernet traffic is prone to collisions, a hub can all but eliminate them. d. Though multiple systems can access the media simultaneously, the result will be a collision, which should be immediately detected. Answer: D Ethernet Media Access uses CSMA/CD. This indicates that hosts will "sense" the cable to determine if data is transmitting. However, multiple hosts could have sensed that the media was available at the same time. In this case, if multiple hosts transmit on the cable it causes a collision which should be detected immediately. A hub would not help with this problem. In order to limit collisions, a switch is necessary. CISSP Practice Exam Questions and Answers #20 If an enterprise is considering migrating resources to the cloud and wishes to ensure that the Cloud Service Provider has the ability to provision and de-provision resources in an automatic manner, so that available resources match the current demand as closely as possible, which technique choice would be most appropriate? a. Scalability b. Elasticity c. Availability d. Reliability Answer: B One of the big benefits of cloud infrastructure is the elasticity it offers. Elasticity is the degree to which systems are able to adapt to changes in workload by provisioning and de-provisioning needed resources automatically so that at each moment, the available resources match the current demand as closely as possible. Master of Project Academy CISSP Exam Simulator In addition to these sample 20 questions, we at Master of Project Academy also offer a free CISSP Exam simulator. It is available to try for free. The free CISSP exam simulator has 15 CISSP practice exam questions and these let you get an idea of the quality of our CISSP questions in the paid simulator. Yes, we also have a paid CISSP exam simulator. Our paid CISSP exam simulator contains 1050 sample real-like CISSP exam questions. The simulator offers you seven CISSP mock exams to help you achieve the best result. The exam content in the simulator is from the latest CISSP Common Body of Knowledge. Every question gives you an answer with a rationale. When you end your mock exam in the simulator, you get a detailed report of your performance in the exam. Both of our exam simulators are web-based, so you don't even need to download any software before you could use them.