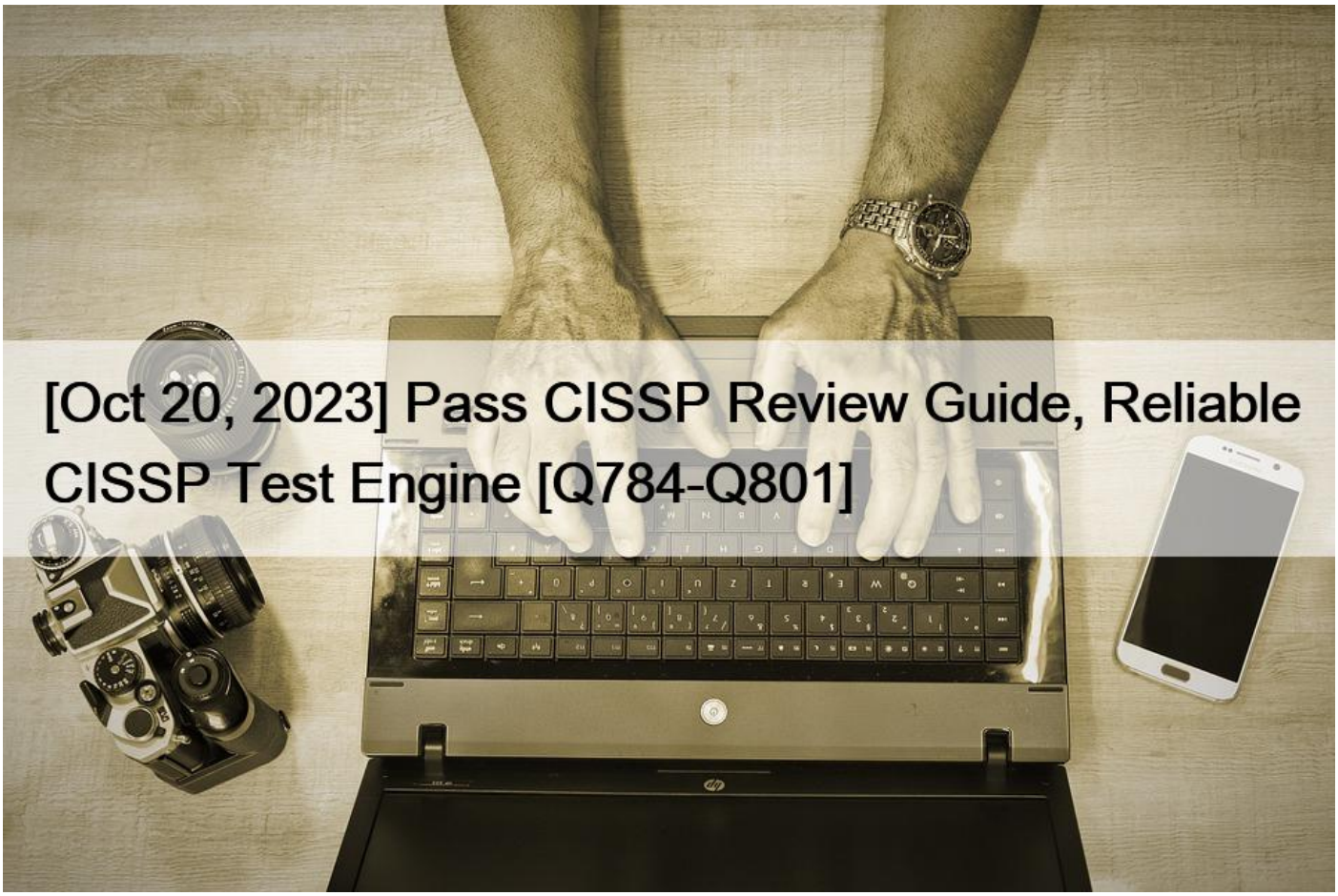
[Oct 20, 2023 Pass CISSP Review Guide, Reliable CISSP Test Engine [Q784-Q801



[Oct 20, 2023] Pass CISSP Review Guide, Reliable CISSP Test Engine
CISSP Test Engine Practice Test Questions, Exam Dumps

NO.784 What works as an E-mail message transfer agent?
* SMTP
* SNMP
* S-RPC
* S/MIME

NO.785 Who should measure the effectiveness of Information System security related controls in an organization?
* The local security specialist
* The business manager
* The systems auditor
* The central security manager

Explanation/Reference:

Explanation:

The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely.

The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met.

CobiT is a model that most information security auditors follow when evaluating a security program. The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.

Incorrect Answers:

A: A local security specialist could be hired to measure the effectiveness of Information System security related controls in an organization. However, in doing so, the local security specialist would be performing the role of systems auditor.

B: The business manager does not measure the effectiveness of Information System security related controls in an organization.

D: The central security manager could measure the effectiveness of Information System security related controls in an organization. However, in doing so, central security manager would be performing the role of systems auditor.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 55, 125

NO.786 Which of the following packets should NOT be dropped at a firewall protecting an organization’s internal network?
* Inbound packets with Source Routing option set
* Router information exchange protocols
* Inbound packets with an internal source IP address
* Outbound packets with an external destination IP address

NO.787 Which of the following is NOT a use of an audit trail?
* Collects information such as passwords or infrastructure configurations
* Enables the security practitioner to trace a transaction’s history
* Provides information about additions, deletions, or modifications to the data
* Assists the monitoring function by helping to recognize patterns of abnormal user behavior

The correct answer is “Collects information such as passwords or infrastructure configurations”. Auditing should not be used to collect user’s passwords. It is used for the other three examples, however.

NO.788 Which of the following is a problem regarding computer investigation issues?
* Information is tangible.
* Evidence is easy to gather.
* Computer-generated records are only considered secondary evidence, thus are not as reliable as best evidence.
* In many instances, an expert or specialist is not required.

Explanation/Reference:

Explanation:

Computer-based evidence is typically considered hearsay evidence. Hearsay is second-hand evidence, as opposed to direct evidence. Second-hand evidence is treated as less reliable.

Incorrect Answers:

A: Tangible information does not cause problem within an investigation.

B: Easily collected information would cause a problem.

D: During a computer investigation an expert or specialist could very well be required.

References:

Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 389

NO.789 The concept of least privilege currently exists within the context of:
* ISO
* TCSEC
* OSI
* IEFT

Ensuring least privilege requires identifying what the user’s job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges couldn’t be used to circumvent the organizational security policy. Although the concept of least privilege currently exists within the context of the TCSEC, requirements restrict those privileges of the system administrator. Through the use of RBAC, enforced minimum privileges for general system users can be easily achieved.

NO.790 A criminal organization is planning an attack on a government network. Which of the following is the MOST severe attack to the network availability?
* Network management communications is disrupted
* Operator loses control of network devices to attacker
* Sensitive information is gathered on the network topology by attacker
* Network is flooded with communication traffic by attacker

NO.791 An organization discovers that its Secure File Transfer Protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization’s general Information Technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.

Which of the following is the MOST probable attack vector used in the security breach?
* Buffer overflow
* Distributed Denial of Service (DDoS)
* Cross-Site Scripting (XSS)
* Weak password due to lack of complexity rules

NO.792 Which of the following BEST describes a rogue Access Point (AP)?
* An AP that is not protected by a firewall
* An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data

Encryption Algorithm (3DES)
* An AP connected to the wired infrastructure but not under the management of authorized network administrators
* An AP infected by any kind of Trojan or Malware

NO.793 Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?
* Application connection successes resulting in data leakage
* Administrative costs for restoring systems after connection failure
* Employee system timeouts from implementing wrong limits
* Help desk costs required to support password reset requests
Section: Identity and Access Management (IAM)

NO.794 The top speed of ISDN BRI is 256 KBS.(True/False)
* True
* False
The top speed of ISDN BRI is 128 KBS. Its two primary channels are each capable of carrying 64 KBS so the combined top speed is 128 KBS.

NO.795 The Wired Equivalency Privacy algorithm (WEP) of the 802.11 Wireless

LAN Standard uses which of the following to protect the confidentiality

of information being transmitted on the LAN?
* A digital signature that is sent between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
* A public/private key pair that is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
* A secret key that is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
* Frequency shift keying (FSK) of the message that is sent between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
The transmitted packets are encrypted with a secret key and an Integrity Check (IC) field comprised of a CRC-32 check sum that is attached to the message. WEP uses the RC4 variable key-size stream cipher encryption algorithm. RC4 was developed in 1987 by Ron Rivest and operates in output feedback mode. Researchers at the University of California at Berkely (wep@isaac.cs.berkeley.edu) have found that the security of the WEP algorithm can be compromised, particularly with the following attacks: Passive attacks to decrypt traffic based on statistical analysis Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext Active attacks to decrypt traffic, based on tricking the access point Dictionary-building attack that, after analysis of about a day’s worth of traffic, allows real-time automated decryption of all traffic The Berkeley researchers have found that these attacks are effective against both the 40-bit and the so-called 128-bit versions of WEP using inexpensive off-the-shelf equipment. These attacks can also be used against networks that use the 802.11b Standard, which is the extension to 802.11 to support higher data rates, but does not change the WEP algorithm. The weaknesses in WEP and 802.11 are being addressed by the IEEE 802.11i Working Group. WEP will be upgraded to WEP2 with the following proposed changes: Modifying the method of creating the initialization vector (IV) Modifying the method of creating the encryption key Protection against replays Protection against IV collision attacks Protection against forged packets In the longer term, it is expected that the Advanced Encryption Standard (AES) will replace the RC4 encryption algorithm currently used in WEP.

NO.796 You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you’re seeing a series of bits placed in the “Urgent Pointer” field of a TCP packet. This is only 16 bits which isn’t much but it concerns you because:
* This could be a sign of covert channeling in bank network communications and should be investigated.
* It could be a sign of a damaged network cable causing the issue.

* It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
* It is normal traffic because sometimes the previous fields 16 bit checksum value can over run into the urgent pointer’s 16 bit field causing the condition.

The Urgent Pointer is used when some information has to reach the server ASAP. When the TCP/IP stack at the other end sees a packet using the Urgent Pointer set, it is duty bound to stop all ongoing activities and immediately send this packet up the stack for immediate processing. Since the packet is plucked out of the processing queue and acted upon immediately, it is known as an Out Of Band (OOB) packet and the data is called Out Of Band (OOB) data.

The Urgent Pointer is usually used in Telnet, where an immediate response (e.g. the echoing of characters) is desirable. Covert Channels are not directly synonymous with backdoors. A covert channel is simply using a communication protocol in a way it was not intended to be used or sending data without going through the proper access control mechanisms or channels. For example, in a Mandatory Access Control systems a user at secret has found a way to communicate information to a user at Confidential without going through the normal channels.

In this case the Urgent bit could be use for a few reasons:

1.It could be to attempt a Denial of service where the host receiving a packet with the Urgent bit set will give immediate attention to the request and will be in wait state until the urgent message is receive, if the sender does not send the urgent message then it will simply sit there doing nothing until it times out. Some of the TCP/IP stacks used to have a 600 seconds time out, which means that for 10 minutes nobody could use the port. By sending thousands of packet with the URGENT flag set, it would create a very effective denial of service attack.

2.It could be used as a client server application to transmit data back and forward without going through the proper channels. It would be slow but it is possible to use reserved fields and bits to transmit data outside the normal communication channels.

The other answers are incorrect The following reference(s) were/was used to create this question: http://www.vijaymukhi.com/vmis/tcp.htm and http://www.fas.org/irp/nsa/rainbow/tg030.htm document covering the subject of covert channels and also see: http://gray-world.net/papers.shtml which is a large collection of documents on Covert Channels

NO.797 Which of the BEST internationally recognized standard for evaluating security products and systems?
* Payment Card Industry Data Security Standards (PCI-DSS)
* Common Criteria (CC)
* Health Insurance Portability and Accountability Act (HIPAA)
* Sarbanes-Oxley (SOX)

NO.798 Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?
* dig
* ipconfig
* ifconfig
* nbstat

Section: Software Development Security

NO.799 What is the maximum key size for the RC5 algorithm?
* 128 bits
* 256 bits
* 1024 bits
* 2040 bits

Explanation/Reference:

Explanation:

RC5 is a block cipher that has a variety of parameters it can use for block size, key size, and the number of rounds used. It was created by Ron Rivest and analyzed by RSA Data Security, Inc. The block sizes used in this algorithm are 32, 64, or 128 bits, and the key size goes up to 2,048 bits. The number of rounds used for encryption and decryption is also variable. The number of rounds can go up to 255.

Incorrect Answers:

A: The maximum key size for the RC5 algorithm is 2048 bits, not 128 bits.

B: The maximum key size for the RC5 algorithm is 2048 bits, not 256 bits.

C: The maximum key size for the RC5 algorithm is 2048 bits, not 1024 bits.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 810

NO.800 Which term below MOST accurately describes the Trusted Computing

Base (TCB)?
* A piece of information that represents the security level of an object
* A computer that controls all access to objects by subjects
* Formal proofs used to demonstrate the consistency between a systems specification and a security model
* The totality of protection mechanisms within a computer system

The Trusted Computing Base (TCB) The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a users clearance) related to the security policy. *Answer “A computer that controls all access to objects by subjects” describes the reference monitor concept. The reference monitor is an access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. The Security Kernel consists of the hardware, firmware, and software elements of a Trusted Computing Base (or Network Trusted Computing Base partition) that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct. *Answer “A piece of information that represents the security level of an object” refers to a sensitivity label. Asensitivity label is a piece of information that represents the extra security level of an object and describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions. *Answer “Formal proofs used to demonstrate the consistency between a systems specification and a security model” describes formal verification. This is the process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation. Source: DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria

NO.801 What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?
* False Rejection Rate (FRR) or Type I Error
* False Acceptance Rate (FAR) or Type II Error
* Crossover Error Rate (CER)
* Failure to enroll rate (FTE or FER)

The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.

Equal error rate or crossover error rate (EER or CER)

It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

The other choices were all wrong answers:

The following are used as performance metrics for biometric systems: False accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38 And https://en.wikipedia.org/wiki/Biometrics

100% Free CISSP Daily Practice Exam With 1481 Questions:
https://www.examslabs.com/ISC/ISCCertification/best-CISSP-exam-dumps.html]