System Security Certified Practitioner (SSCP)

ISC SSCP

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1074

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

Topic Break Down

Topic	No. of Questions
Topic 1, Access Control	250
Topic 2, Security Operation Adimnistration	171
Topic 3, Analysis and Monitoring	60
Topic 4, Risk, Response and Recovery	180
Topic 5, Cryptography	151
Topic 6, Network and Telecommunications	250
Topic 7, Malicious Code	12
Total	1074

QUESTION NO: 1

What is malware that can spread itself over open network connections?

A. Worm

B. Rootkit

C. Adware

D. Logic Bomb

ANSWER: A

Explanation:

Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.

A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.

Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.

Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.

The following answers are incorrect:

- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkitisn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisementsin order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to

the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.

- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.

The following reference(s) was used to create this question:

The CCCure CompTIA Holistic Security+ Tutorial and CBT and

http://en.wikipedia.org/wiki/Rootkit and

http://en.wikipedia.org/wiki/Computer_worm and

http://en.wikipedia.org/wiki/Adware

QUESTION NO: 2

Which of the following would best classify as a management control?

A. Review of security controls

B. Personnel security

C. Physical and environmental protection

D. Documentation

ANSWER: A

Explanation:

Management controls focus on the management of the IT security system and the management of risk for a system.

They are techniques and concerns that are normally addressed by management.

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls.

SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.

The following are incorrect answers:

Personnel security, physical and environmental protection and documentation are forms of operational controls.

Reference(s) used for this question:

http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and

FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

QUESTION NO: 3

Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.

B. It is computationally infeasible to construct two different messages with the same digest.

C. It converts a message of arbitrary length into a message digest of a fixed length.

D. Given a digest value, it is computationally infeasible to find the corresponding message.

ANSWER: A

Explanation:

An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.

A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main or significant properties:

it is easy (but not necessarily quick) to compute the hash value for any given message it is infeasible to generate a message that has a given hash it is infeasible to modify a message without changing the hash it is infeasible to find two different messages with the same hash

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

Source:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

and

http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION NO: 4

Computer-generated evidence is considered:

A. Best evidence

B. Second hand evidence

C. Demonstrative evidence

D. Direct evidence

ANSWER: B

Explanation:

Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computergenerated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

QUESTION NO: 5

In Synchronous dynamic password tokens:

A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).

B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).

C. The unique password is not entered into a system or workstation along with an owner's PIN.

D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

ANSWER: A

Explanation:

Synchronous dynamic password tokens:

- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key). - the unique password is entered into a system or workstation along with an owner's PIN.

- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid timewindow.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

QUESTION NO: 6

The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer

B. The Reference monitor

C. The Transport layer of the TCP/IP stack model

D. Change management control

ANSWER: A

Explanation:

The OSI/ISO Data Link layer is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION NO: 7

What mechanism does a system use to compare the security labels of a subject and an object?

A. Validation Module.

B. Reference Monitor.

C. Clearance Check.

D. Security Module.

ANSWER: B

Explanation:

Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object.

According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.

The following are incorrect:

Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.

Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility.

Security Module. Is typically a general purpose module that prerforms a variety of security related functions.

References:

OIG CBK, Security Architecture and Design (page 324)

AIO, 4th Edition, Security Architecture and Design, pp 328-328.

Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

QUESTION NO: 8

Smart cards are an example of which type of control?

A. Detective control

B. Administrative control

C. Technical control

D. Physical control

ANSWER: C

Explanation:

Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (p. 245). McGraw-Hill. Kindle Edition. and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

QUESTION NO: 9

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

A. B

B. A

C. C

D. D

ANSWER: A

Explanation:

B level is the first Mandatory Access Control Level.

First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

Reference used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition. and

THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

QUESTION NO: 10

What algorithm was DES derived from?

A. Twofish.

B. Skipjack.

C. Brooks-Aldeman.

D. Lucifer.

ANSWER: D

Explanation:

NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.

The following answers are incorrect:

Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.

Skipjack. This is incorrect, Skipjack was developed after DES by the NSA .

Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

QUESTION NO: 11

Which type of attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number?

A. IP spoofing attack

B. SYN flood attack

C. TCP sequence number attack

D. Smurf attack

ANSWER: C

Explanation:

A TCP sequence number attack exploits the communication session which was established between the target and the trusted host that initiated the session. It involves hijacking the session between the host and the target by predicting the target's choice of an initial TCP sequence number. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION NO: 12

Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

A. Full Interruption test

B. Checklist test

C. Simulation test

D. Structured walk-through test

ANSWER: A

Explanation:

The difference between this and the full-interruption test is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. This is the most common type of disaster recovery plan testing.

A checklist test is only considered a preliminary step to a real test.

In a structured walk-through test, business unit management representatives meet to walk through the plan, ensuring it accurately reflects the organization's ability to recover successfully, at least on paper.

A simulation test is aimed at testing the ability of the personnel to respond to a simulated disaster, but not recovery process is actually performed.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 289).

QUESTION NO: 13

The security of a computer application is most effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.

B. The system is procured off-the-shelf.

C. The system is customized to meet the specific security threat.

D. The system is originally designed to provide the necessary security.

ANSWER: D

Explanation:

The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.

The following answers are incorrect:

The system is optimized prior to the addition of security. Is incorrect because if you wait to implement security after a system is completed the cost of adding security increases dramtically and can become much more complex.

The system is procured off-the-shelf. Is incorrect because it is often difficult to add security to off-the shelf systems.

The system is customized to meet the specific security threat. Is incorrect because this is a distractor. This implies only a single threat.

QUESTION NO: 14

A business continuity plan is an example of which of the following?

A. Corrective control

B. Detective control

C. Preventive control

D. Compensating control

ANSWER: A

Explanation:

Business Continuity Plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capacity. They are for use "after the fact", thus are examples of corrective controls.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 273). and

Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location 8069). Elsevier Science (reference). Kindle Edition. and

QUESTION NO: 15

Which type of attack involves impersonating a user or a system?

A. Smurfing attack

B. Spoofing attack

C. Spamming attack

D. Sniffing attack

ANSWER: B

Explanation:

A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION NO: 16

Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment

B. The use of physical force

C. The operation of access control devices

D. The need to detect unauthorized access

ANSWER: A

Explanation:

The The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.

The following answers are incorrect:

The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.

The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc. The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.

The following reference(s) were/was used to create this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).

Source: ISC2 Offical Guide to the CBK page 288-289.

QUESTION NO: 17

Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP

B. PPTP

C. IPSec

D. L2F

ANSWER: D

Explanation:

L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links. IPSec is now considered the best VPN solution for IP environments.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

QUESTION NO: 18

Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.

B. Chief Operating Officer.

C. Disaster Recovery Manager.

D. Chief Executive Officer.

ANSWER: C

Explanation:

The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.

The following answers are incorrect:

Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

Chief Executive Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

QUESTION NO: 19

Which of the following is not an encryption algorithm?

A. Skipjack

B. SHA-1

C. Twofish

D. DEA

ANSWER: B

Explanation:

The SHA-1 is a hashing algorithm producing a 160-bit hash result from any data. It does not perform encryption.

In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard.

SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use. NIST required many applications in federal agencies to move to SHA-2 after 2010 because of the weakness. Although no successful attacks have yet been reported on SHA-2, they are algorithmically similar to SHA-1. In 2012, following a long-running competition, NIST selected an additional algorithm, Keccak, for standardization as SHA-3

NOTE:

A Cryptographic Hash Function is not the same as an Encryption Algorithm even thou both are Algorithms. An algorithm is defined as a step-by-step procedure for calculations. Hashing Algorithm do not encrypt the data. People sometimes will say they encrypted a password with SHA-1 but really they simply created a Message Digest of the password using SHA-1, putting the input through a series of steps to come out with the message digest or hash value.

A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.

Encryption Algorithms are reversible but Hashing Algorithms are not meant to be reversible if the input is large enough.

The following are incorrect answers:

The Skipjack algorithm is a Type II block cipher with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level.

Twofish is a freely available 128-bit block cipher designed by Counterpane Systems (Bruce Schneier et al.).

DEA is a symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard (DES). DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

Reference(s) used for this question: http://en.wikipedia.org/wiki/SHA-1 and

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

and

Counterpane Labs, at http://www.counterpane.com/twofish.html.

QUESTION NO: 20

Hierarchical Storage Management (HSM) is commonly employed in:

A. very large data retrieval systems

B. very small data retrieval systems

C. shorter data retrieval systems

D. most data retrieval systems

ANSWER: A

Explanation:

Hierarchical Storage Management (HSM) is commonly employed in very large data retrieval systems.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

DUMPSARENA