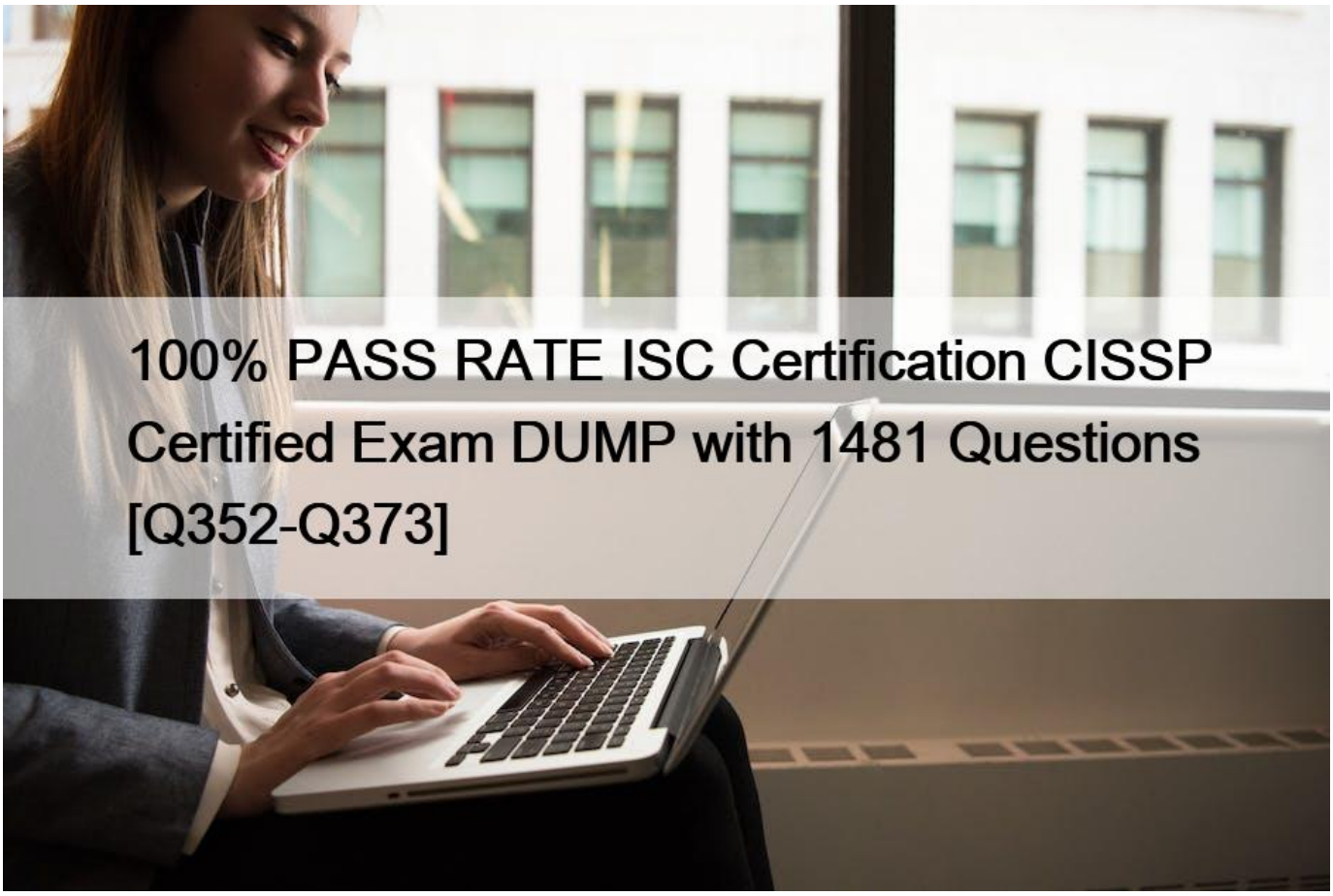
100% PASS RATE ISC Certification CISSP Certified Exam DUMP with 1481 Questions [Q352-Q373



100% PASS RATE ISC Certification CISSP Certified Exam DUMP with 1481 Questions
Updates For the Latest CISSP Free Exam Study Guide!

ISC CISSP (Certified Information Systems Security Professional) Certification Exam is a globally recognized certification for information security professionals. Certified Information Systems Security Professional certification exam is designed to test the knowledge, skills, and experience of individuals in the field of information security. Certified Information Systems Security Professional certification exam covers a broad range of topics, including risk management, asset security, security engineering, and communication and network security.

NEW QUESTION 352

Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:
* Operations Security Domain.
* Operations Security Domain Analysis.
* Telecommunications and Network Security Domain.

* Business Continuity Planning and Disater Recovery Planning.
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

NEW QUESTION 353

In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the best choice below.
* Network Address Translation
* Network Address Hijacking
* Network Address Supernetting
* Network Address Sniffing
Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer.

Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.

Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session. Session hijacking is the act of unauthorized insertion of packets into a data stream. It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.

The following are incorrect answers: Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. See RFC 1918 for more details.

Network Address Supernetting There is no such thing as Network Address Supernetting. However, a supernetwork, or supernet, is an Internet Protocol (IP) network that is formed from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing

(CIDR) prefix. The new routing prefix for the combined network aggregates the prefixes of the

constituent networks.

Network Address Sniffing This is another bogus choice that sound good but does not even exist.

However, sniffing is a common attack to capture cleartext password and information unencrypted

over the network. Sniffier is accomplished using a sniffer also called a Protocol Analyzer. A

network sniffers monitors data flowing over computer network links. It can be a self-contained

software program or a hardware device with the appropriate software or firmware programming.

Also sometimes called “network probes” or “snoops,” sniffers examine network traffic, making a

copy of the data but without redirecting or altering it.

The following reference(s) were 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 8641-8642). Auerbach Publications. Kindle Edition.

http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm

http://wiki.answers.com/Q/What_is_network_address_hijacking

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of

Computer Security, 2001, John Wiley & Sons, Page 239.

NEW QUESTION 354

Which of the following alternatives should NOT be used by law

enforcement to gain access to a password?
* Contacting the developer of the software for information to gain access to the computer or network through a back door
* Compelling the suspect to provide the password
* Data manipulation and trial procedures applied to the original version of the system hard disk
* Using password cracker software

The original disk of a computer involved in a criminal investigation should not be used for any experimental purposes since data may be modified or destroyed. Any operations should be conducted on a copy of the system disk. However, the other answers are the preferred methods of gaining access to a password-protected system. Interestingly, in answer b, there is legal precedent to order a suspect to provide the password of a computer that is in the custody of law enforcement.

NEW QUESTION 355

When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?
* Address Resolution Protocol (ARP).
* Reverse Address Resolution Protocol (RARP).
* Internet Control Message protocol (ICMP).
* User Datagram Protocol (UDP).

The RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address.

ARP does the opposite by broadcasting a request to find the Ethernet address that matches a known IP address.

ICMP supports packets containing error, control, and informational messages (e.g. PING).

UDP runs over IP and is used primarily for broadcasting messages over a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION 356

The main risks that physical security components combat are all of the following EXCEPT:
* SYN flood
* Physical damage
* Theft
* Tailgating
Explanation/Reference:

Explanation:

A SYN flood is a type of software attack on system. The defense against a SYN flood is also software- based, not a physical component.

If an attacker sends a target system SYN packets with a spoofed address, then the victim system replies to the spoofed address with SYN/ACK packets. Each time the victim system receives one of these SYN packets it sets aside resources to manage the new connection. If the attacker floods the victim system with SYN packets, eventually the victim system allocates all of its available TCP connection resources and can no longer process new requests. This is a type of DoS that is referred to as a SYN flood. To thwart this type of attack you can use SYN proxies, which limit the number of open and abandoned network connections. The SYN proxy is a piece of software that resides between the sender and receiver and only sends on TCP traffic to the receiving system if the TCP handshake process completes successfully.

Incorrect Answers:

B: Physical damage is carried out by a person or people. Physical security components can reduce the risk of physical damage. Therefore, this answer is incorrect.

C: Theft is carried out by a person or people. Physical security components can reduce the risk of theft.

Therefore, this answer is incorrect.

D: Tailgating is carried out by a person or people. Physical security components can reduce the risk of tailgating. Therefore, this answer is incorrect.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 539

NEW QUESTION 357

Which of the following can be defined as a unique identifier in the table that unambiguously points to an individual tuple or record in the table?
* primary key
* candidate key
* secondary key
* foreign key
Explanation/Reference:

Explanation:

The primary key is the attribute that is used to make each row or tuple in a table unique.

Incorrect Answers:

B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.

C: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

D: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-

1180

Stewart, James, Ed Tittel and Mike Chapple, CISSP: Certified Information Systems security Professional Study Guide, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312

http://databases.about.com/cs/specificproducts/g/candidate.htm

http://rdbms.opengrass.net/2_Database Design/2.1_TermsOfReference/2.1.2_Keys.html

NEW QUESTION 358

Identity-based access control is a subset of which one of the following access control categories?
* Discretionary access control
* Lattice-based access control
* Non-discretionary access control
* Mandatory access control
The correct answer is “Discretionary access control”. Identity-based access control is a type of discretionary access control that grants access privileges based on the user’s identity. A related type of discretionary access control is user-directed access control that gives the user, with certain limitations, the right to alter the access control to certain objects.

NEW QUESTION 359

A user’s credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?
* Validate passwords using a stored procedure.
* Allow only the application to have access to the password field in order to verify user authentication.
* Use a salted cryptographic hash of the password.
* Encrypt the entire database and embed an encryption key in the application.

NEW QUESTION 360

Which of the following falls under the categories of configuration management?(Choose three)
* Operating system configuration
* Software configuration
* Hardware configuration
* Logical configuration
* Physical configuration
Configuration management controls the changes that take place in hardware,

software, and operating systems.

NEW QUESTION 361

Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?
* Automatically create exceptions for specific actions or files
* Determine which files are unsafe to access and blacklist them
* Automatically whitelist actions or files known to the system
* Build a baseline of normal or safe system events for review

NEW QUESTION 362

Which of the following is a recommended alternative to an integrated email encryption system?
* Sign emails containing sensitive data
* Send sensitive data in separate emails
* Encrypt sensitive data separately in attachments
* Store sensitive information to be sent in encrypted drives

NEW QUESTION 363

Which of the following is covered under Crime Insurance Policy Coverage?
* Inscribed, printed and Written documents
* Manuscripts
* Accounts Receivable
* Money and Securities
Explanation/Reference:

Explanation:

Crime Insurance policy protects organizations from loss of money, securities, or inventory resulting from crime.

Incorrect Answers:

A: Crime Insurance Policy does not protect Inscribed, printed and written documents. You would need Valuable paper insurance for that.

B: Crime Insurance Policy does not protect manuscripts. You would need Valuable paper insurance for that.

C: Crime Insurance Policy does not protect business records such as Accounts Receivable. You would need Valuable paper insurance for that.

References:

http://www.insurecast.com/html/crime_insurance.asp

NEW QUESTION 364

Which security model uses division of operations into different parts and requires different users to perform each part?
* Bell-LaPadula model
* Biba model
* Clark-Wilson model
* Non-interference model
The Clark-Wilson model uses separation of duties, which divides an operation into

different parts and requires different users to perform each part. This prevents authorized users

from making unauthorized modifications to data, thereby protecting its integrity.

The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity

policy for a computing system.

The model is primarily concerned with formalizing the notion of information integrity. Information

integrity is maintained by preventing corruption of data items in a system due to either error or

malicious intent. An integrity policy describes how the data items in the system should be kept

valid from one state of the system to the next and specifies the capabilities of various principals in

the system. The model defines enforcement rules and certification rules.

The model’s enforcement and certification rules define data items and processes that provide the

basis for an integrity policy. The core of the model is based on the notion of a transaction.

A well-formed transaction is a series of operations that transition a system from one consistent

state to another consistent state.

In this model the integrity policy addresses the integrity of the transactions.

The principle of separation of duty requires that the certifier of a transaction and the implementer

be different entities.

The model contains a number of basic constructs that represent both data items and processes

that operate on those data items. The key data type in the Clark-Wilson model is a Constrained

Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are

valid at a certain state. Transactions that enforce the integrity policy are represented by

Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI)

and produces a CDI. A TP must transition the system from one valid state to another valid state.

UDIs represent system input (such as that provided by a user or adversary). A TP must guarantee

(via certification) that it transforms all possible values of a UDI to a “safe” CDI.

In general, preservation of data integrity has three goals:

Prevent data modification by unauthorized parties

Prevent unauthorized data modification by authorized parties

Maintain internal and external consistency (i.e. data reflects the real world)

Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.

References:

HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5:

Security Architecture and Design (Page 341-344).

and

http://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION 365

Which one of the following, if embedded within the ciphertext, will decrease the likelihood of a message being replayed?
* Stop bit
* Checksum
* Timestamp
* Digital signature

CBC is the CBC mode of some block cipher, HMAC is a keyed message digest, MD is a plain message digest, and timestamp is to protect against replay attacks. From the OpenSSL project http://www.mail-archive.com/openssl-users@openssl.org/msg23576.html

NEW QUESTION 366

What is a characteristic of using the Electronic Code Book mode of DES encryption?
* A given block of plaintext and a given key will always produce the same ciphertext.
* Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
* Individual characters are encoded by combining output from earlier encryption routines with plaintext.
* The previous DES output is used as input.

A given message and key always produce the same ciphertext.

The following answers are incorrect:

Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.

Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces

the same ciphertext

Individual characters are encoded by combining output from earlier encryption routines with

plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the

end of the file was reached. This is a characteristic of Cipher Feedback. Cipher Feedback the

ciphertext is run through a key-generating device to create the key for the next block of plaintext.

The previous DES output is used as input. Is incorrect because This is incorrect because with

Electronic Code Book processing 64 bits at a time until the end of the file was reached . This is a

characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous

block to encrypt the next block.

NEW QUESTION 367

Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?
* Data owner
* Data steward
* Data custodian
* Data processor

NEW QUESTION 368

A database View operation implements the principle of:
* Entity integrity.
* Separation of duties.
* Referential integrity.
* Least privilege.

The correct answer is “Least privilege”. Least privilege, in the database context,

requires that subjects be granted the most restricted set of access privileges

to the data in the database that are consistent with the performance

of their tasks.

Separation of duties, assigns parts of security-sensitive tasks to several individuals.

Entity integrity requires that each row in the relation table must have a

non-NULL attribute. Relational integrity, answer d, refers to the

requirement that for any foreign key attribute, the referenced relation

must have the same value for its primary key.

NEW QUESTION 369

What encryption algorithm is best suited for communication with handheld wireless devices?
* ECC
* RSA
* SHA
* RC4
“Eliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An Elliptic Curve Cryptosystem (ECC) provides much of the same functionality that RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC’s efficiency. Some devices have limited processing capacity, storage, power supply, and bandwidth like wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality requiring a smaller percentage of resources required by RSA and other algorithms, so it is used in these types of devices. In most cases, the longer the key length, the protection provided, but ECC can provide the same level of protection with a key size that is smaller than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.” Pg. 491 Shon Harris: All-In-One CISSP Certification Guide.

NEW QUESTION 370

Which of the following best describes the Secure Electronic Transaction (SET) protocol?
* Originated by VISA and MasterCard as an Internet credit card protocol.
* Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
* Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
* Originated by VISA and MasterCard as an Internet credit card protocol using SSL.
This protocol was created by VISA and MasterCard as a common effort to make the buying process over the Internet secure through the distribution line of those companies. It is located in layer 7 of the OSI model.

SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of “encrypting” or scrambling the information exchanged between the shopper and the online store,

SET ensures a payment process that is convenient, private and most of all secure.

Specifically, SET:

*

Establishes industry standards to keep your order and payment information confidential.

*

Increases integrity for all transmitted data through encryption.

*

Provides authentication that a cardholder is a legitimate user of a branded payment card account.

*

Provides authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.

*

Allows the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.

The SET process relies strongly on the use of certificates and digital signatures for the process of authentication and integrity of the information.

NEW QUESTION 371

What is defined as the rules for communicating between computers on a Local Area Network (LAN)?
* LAN Media Access methods
* LAN topologies
* LAN transmission methods
* Contention Access Control
Explanation/Reference:

Explanation:

Media access technologies deal with how these systems communicate over the network media. LAN access technologies set up the rules of how computers will communicate on the Local Area Network.

Incorrect Answers:

B: Network topology is not defined by rules of communication. It is the arrangement of the various elements (links, nodes, etc.) of a computer network.

C: The communications rules on a LAN is called Media Access rules, not transmissions methods.

D: Contention Access Control is just used to avoid collisions. To communicate LAN Media Access methods are used.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 565

NEW QUESTION 372

The Clipper Chip utilizes which concept in public key cryptography?
* Substitution
* Key Escrow
* An undefined algorithm

* Super strong encryption
The Clipper chip is a chipset that was developed and promoted by the U.S.

Government as an encryption device to be adopted by telecommunications companies for voice

transmission. It was announced in 1993 and by 1996 was entirely defunct.

The heart of the concept was key escrow. In the factory, any new telephone or other device with a

Clipper chip would be given a “cryptographic key”, that would then be provided to the government

in “escrow”. If government agencies “established their authority” to listen to a communication, then

the password would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone. The CISSP Prep Guide states, “The idea is to divide the key into two parts, and to escrow two portions of the key with two separate ‘trusted’ organizations. Then, law enforcement officals, after obtaining a court order, can retreive the two pieces of the key from the organizations and decrypt the message.”

References: http://en.wikipedia.org/wiki/Clipper_Chip and Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 166.

NEW QUESTION 373

In what way could Java applets pose a security threat?
* Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
* Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
* Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
* Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

To be eligible for the CISSP certification exam, candidates must have a minimum of five years of professional experience in information security. Candidates who do not meet this requirement may still be eligible for the exam if they have a relevant bachelor's or master's degree or other applicable certifications.

Best CISSP Exam Preparation Material with New Dumps Questions https://www.braindumpsit.com/CISSP_real-exam.html]