DUMPSARENA

Systems Security Certified Practitioner

ISC2 SSCP

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1074

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

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 protocol is used to match an IP address to the appropriate hardware address of the packet's destination so it can be sent?

A. Routing tables

B. Address resolution protocol (ARP)

C. Reverse address resolution protocol (RARP)

D. Internet Control Message Protocol (ICMP)

ANSWER: B

Explanation:

The Address Resolution Protocol (ARP) is used to match an IP address to an Ethernet address so the packet can be sent to the appropriate node.

Shon Harris in her book says:

MAC and IP addresses must be properly mapped so they can be correctly resolved. This happens through the Address Resolution Protocol (ARP). When the data link layer receives a frame, the network layer has already attached the destination IP address to it, but the data link layer cannot understand the IP address and thus invokes ARP for help.

ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it.

The computer that has the destination IP address responds with its MAC address. Now ARP knows what hardware address corresponds with that specific IP address. The data link layer takes the frame, adds the hardware address to it, and passes it on to the physical layer, which enables the frame to hit the wire and go to the destination computer.

ARP maps the hardware address and associated IP address and stores this mapping in its table for a predefined amount of time. This caching is done so that when another frame destined for the same IP address needs to hit the wire, ARP does not need to broadcast its request again. It just looks in its table for this information.

Man-In-The-Middle attack

Because ARP does not require authentication, an attacker could place bogus entries into the ARP cache of a remote host (gratuitous ARP replies) to carry out attacks, such as a man-in-themiddle attacks. This attack is called ARP poisoning.

The following answers were incorrect:

RARP is used to match an Ethernet address to an IP address.

ICMP is a management protocol whose function is to send message between network devices.

Routing tables are used by routers to choose the appropriate interface to route packets.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition, Chapter 6 Telecommunications and Network Security, Pages 580-581 or on the Kindle edition look around Locations 12298-12306. McGraw-Hill. Kindle Edition.

and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK , Third Edition: Telecommunications and Network Security, Page 342.

QUESTION NO: 2

Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

A. Internet Security Association and Key Management Protocol (ISAKMP)

B. Simple Key-management for Internet Protocols (SKIP)

C. Diffie-Hellman Key Distribution Protocol

D. IPsec Key exchange (IKE)

ANSWER: B

Explanation:

RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:

A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.

IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally.

Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

The following are incorrect answers:

ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

IPsec Key exchange (IKE) is only a detracto.

Reference(s) used for this question:

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

and

http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol and

http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

QUESTION NO: 3

Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organisation

B. Quick Recovery

C. A secondary location is available to reconstruct the environment

D. Low Cost

ANSWER: B

Explanation:

A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

Dedicated site owned or operated by the organization. Also called redundant or alternate sites; Reciprocal agreement or memorandum of agreement with an internal or external entity; and Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.

Progressing from basic to advanced, the sites are described below:

Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities. ƒWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.

Two examples of variations to the site types are:

ƒMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. ƒMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.

The following reference(s) were used for this question:

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

QUESTION NO: 4

Which of the following is NOT true about IPSec Tunnel mode?

A. Fundamentally an IP tunnel with encryption and authentication

B. Works at the Transport layer of the OSI model

C. Have two sets of IP headers

D. Established for gateway service

E. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

ANSWER: B

Explanation:

IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

As Figure 1 shows, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else. (Refer to the figure for the following discussion.) Figure 1 Tunnel and transport modes in IPSec.

Figure 1 displays some examples of when to use tunnel versus transport mode:

Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such

as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up between the gateways.

Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.

In example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. Note that Cisco IOS software and the PIX Firewall sets tunnel mode as the default IPSec mode.

Transport mode is used between end-stations supporting IPSec, or between an end-station and a gateway, if the gateway is being treated as a host. In example D, transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software to terminate at the PIX Firewall, enabling Alice to remotely configure the PIX Firewall securely.

AH Tunnel Versus Transport Mode

Figure 2 shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header, if present, and other higher-layer protocols.

In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.

Figure 2 AH tunnel versus transport mode.

AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which breaks the AH header and causes the packets to be rejected by the IPSec peer.

ESP Tunnel Versus Transport Mode

Figure 3 shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.

NOTE Higher-layer information is not available because it's part of the encrypted payload.

When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

Figure 3 ESP tunnel versus transport mode.

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP hashed message authentication code (HMAC). Authentication is calculated after the encryption is done. The current IPSec standard specifies SHA-1 and MD5 as the mandatory HMAC algorithms.

The main difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP doesn't protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). Figure 4 illustrates the fields protected by ESP HMAC.

Figure 4 ESP encryption with a keyed HMAC.

IPSec Transforms

An IPSec transform specifies a single IPSec security protocol (either AH or ESP) with its corresponding security algorithms and mode. Example transforms include the following:

The AH protocol with the HMAC with MD5 authentication algorithm in tunnel mode is used for authentication.

The ESP protocol with the triple DES (3DES) encryption algorithm in transport mode is used for confidentiality of data.

The ESP protocol with the 56-bit DES encryption algorithm and the HMAC with SHA-1 authentication algorithm in tunnel mode is used for authentication and confidentiality.

Transform Sets

A transform set is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. During the ISAKMP IPSec security association negotiation that occurs in IKE phase 2 quick mode, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine the following IPSec factors: Mechanism for payload authentication—AH transform

Mechanism for payload encryption—ESP transform IPSec mode (transport versus tunnel)

Transform sets equal a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).

This brings us to the end of the second part of this five-part series of articles covering IPSec. Be sure to catch the next installment.

Cisco Press at: http://www.ciscopress.com/articles/printerfriendly.asp?p=25477 and

Source: TIPTON, Harold

F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

QUESTION NO: 5

Which of the following statements pertaining to protection rings is false?

A. They provide strict boundaries and definitions on what the processes that work within each ring can access.

B. Programs operating in inner rings are usually referred to as existing in a privileged mode.

C. They support the CIA triad requirements of multitasking operating systems.

D. They provide users with a direct access to peripherals

ANSWER: D

Explanation:

In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level.

Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

"They provide strict boundaries and definitions on what the processes that work within each ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system.

"Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system.

"They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.

Reference(s) used for this question:

CBK, pp. 310-311

AIO3, pp. 253-256

AIOv4 Security Architecture and Design (pages 308 - 310)

AIOv5 Security Architecture and Design (pages 309 - 312)

QUESTION NO: 6

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics

B. Micrometrics

C. Macrometrics

D. MicroBiometrics

ANSWER: A

Explanation:

The Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

QUESTION NO: 7

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems

B. Acceptability of biometrics systems

C. Availability of biometrics systems

D. Adaptability of biometrics systems

ANSWER: B

Explanation:

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

QUESTION NO: 8

What is the Biba security model concerned with?

A. Confidentiality

B. Reliability

C. Availability

D. Integrity

ANSWER: D

Explanation:

The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (Page 244).

QUESTION NO: 9

Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D

B. C

C. B

D. A

ANSWER: B

Explanation:

C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.

B is incorrect. B deals with mandatory protection.

A is incorrect. A deals with verified protection.

Reference(s) used for this question: CBK, p. 329 – 330

and

Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

QUESTION NO: 10

External consistency ensures that the data stored in the database is:

A. in-consistent with the real world.

B. remains consistant when sent from one system to another.

C. consistent with the logical world.

D. consistent with the real world.

ANSWER: D

Explanation:

External consistency ensures that the data stored in the database is consistent with the real world.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 33.

QUESTION NO: 11

Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?

A. design, development, publication, coding, and testing.

B. design, evaluation, approval, publication, and implementation.

C. initiation, evaluation, development, approval, publication, implementation, and maintenance.

D. feasibility, development, approval, implementation, and integration.

E. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

ANSWER: C

Explanation:

The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...

Reference: TIPTON, Harold

F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

QUESTION NO: 12

To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

A. Access Rules

B. Access Matrix

C. Identification controls

D. Access terminal

ANSWER: A

Explanation:

Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.

These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.

An access matrix is one of the means used to implement access control.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION NO: 13

What is the goal of the Maintenance phase in a common development process of a security policy?

A. to review the document on the specified review date

B. publication within the organization

C. to write a proposal to management that states the objectives of the policy

D. to present the document to an approving body

E. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications. Also: 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 286).

ANSWER: A

Explanation:

"publication within the organization" is the goal of the Publication Phase "write a proposal to management that states the objectives of the policy" is part of Initial and Evaluation Phase "Present the document to an approving body" is part of Approval Phase.

Reference: TIPTON, Harold

F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

Also: 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 286).

QUESTION NO: 14

What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering

B. Steganography

C. Cryptology

D. Vernam cipher

ANSWER: B

Explanation:

Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 134).

QUESTION NO: 15

Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?

A. Internet Key exchange (IKE)

B. Security Association Authentication Protocol (SAAP)

C. Simple Key-management for Internet Protocols (SKIP)

D. Key Exchange Algorithm (KEA)

ANSWER: A

Explanation:

RFC 2828 (Internet Security Glossary) defines IKE as an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

The following are incorrect answers:

SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

The Key Exchange Algorithm (KEA) is defined as a key agreement algorithm that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the secret level by the NSA.

Security Association Authentication Protocol (SAAP) is a distracter.

Reference(s) used for this question:

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

QUESTION NO: 16

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: 17

A contingency plan should address:

A. Potential risks.

B. Residual risks.

C. Identified risks.

D. All answers are correct.

ANSWER: D

Explanation:

Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.

The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set.

As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION NO: 18

Domain Name Service is a distributed database system that is used to map:

A. Domain Name to IP addresses.

B. MAC addresses to domain names.

C. MAC Address to IP addresses.

D. IP addresses to MAC Addresses.

ANSWER: A

Explanation:

The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names.

The Domain Name System is maintained by a distributed database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information

about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.

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 100.

and

https://en.wikipedia.org/wiki/Domain_Name_System

QUESTION NO: 19

Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover

B. Large plans can take a lot of work to maintain

C. Continous auditing makes a Disaster Recovery plan irrelevant

D. Infrastructure and environment changes

ANSWER: C

Explanation:

Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date. Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 609).

QUESTION NO: 20

Which of the following best allows risk management results to be used knowledgeably?

A. A vulnerability analysis

B. A likelihood assessment

C. An uncertainty analysis

D. A threat identification

ANSWER: C

Explanation:

Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an

uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.

Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).