Domain 3: Security Architecture and Engineering

Test ID: 175720902

Question #1 of 193

Question ID: 1105091

Your organization is considering whether to construct or purchase a new facility. Which accessibility factor should be considered during the construction or acquisition phase of a facility infrastructure?

A) population of the area

B) traffic

C) hazardous terrain

D) crime rate

Question #2 of 193

Question ID: 1114698

Which of the following statements regarding cloud computing and grid computing are true?

a. Both cloud computing and grid computing are scalable.

b. Grid computing is suited for storing objects as small as 1 byte.

c. Cloud computing may be more environmentally friendly than grid computing.

d. Cloud computing is made up of thin clients, grid computing, and utility computing.

A) options a and b

B) option d

C) options a, c, and d

D) option c

E) all of the options

F) options a, b, and c

G) option b

H) option a

Question #3 of 193

Question ID: 1111720

In which mode does 3DES NOT work?

A) DES-EEE2

B) DES-EEE3

C) DES-EDE3

D) DES-DDD2

Question #4 of 193

Question ID: 1192937

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

One of the planned international offices will perform highly sensitive tasks for a governmental entity. For this reason, you must ensure that the company selects a location where a low profile can be maintained. On which of the following criteria do you base your facility selection?

A) surrounding area

B) construction

C) accessibility

D) visibility

Question #5 of 193

Question ID: 1105079

In PKI, what is the entity that signs a certificate?

A) a principal

B) a subject

C) an issuer

D) a verifier

Question #6 of 193

Question ID: 1105027

You have been specifically asked to implement a stream cipher. Which cryptographic algorithm could you use?

A) RC6

B) RC4

C) MD5

D) RC5

Question #7 of 193

Question ID: 1105106

Which description applies to a surge?

A) a prolonged power supply below normal voltage

B) a momentary low voltage

C) a momentary power outage

D) a prolonged high voltage

E) a prolonged power outage

Question #8 of 193

Question ID: 1105095

During a recent security audit, an outside security contractor has suggested that you trim back the landscaping around entrances. In addition, it has been suggested that you install CCTV at all entrances. Which facet of the Crime Prevention Through Environmental Design (CPTED) approach is being addressed?

A) natural surveillance

B) natural access control

C) territorial reinforcement

D) target hardening

Question #9 of 193

Question ID: 1111719

You have created a cryptographic key on your organization's domain controller. What should you do next?

A) Initialize the key.

B) Terminate the key.

C) Activate the key.

D) Distribute the key.

Question #10 of 193

Question ID: 1111713

Your organization has decided to implement a Web site for customers to purchase your organization's products. The Web site will use the SET protocol. Which statement is true of this protocol?

A) SET uses digital signatures and digital certificates to conduct and verify an electronic transaction.

B) SET automatically transmits a user's credit card information to a CA when an online purchase is made.

C) SET works at the Network layer of the OSI model.

D) SET uses 3DES for symmetric key exchange.

Question #11 of 193

Question ID: 1111704

Which component is NOT associated with the Common Criteria?

A) security target

B) target of evaluation

C) protection profile

D) accreditation

Question #12 of 193

Question ID: 1105039

Which encryption algorithm is based on the Diffie-Hellman key agreement?

A) HAVAL

B) Knapsack

C) International Data Encryption Algorithm

D) El Gamal

Question #13 of 193

Question ID: 1105069

Your manager has asked you to ensure that the password files that are stored on the servers are not vulnerable to attacks. To which type of attack would these files be vulnerable?

A) a SYN flood attack

B) a dictionary attack

C) a side channel attack

D) a Denial of Service (DoS) attack

Question #14 of 193

Question ID: 1105050

What is a trapdoor function?

A) an attack where messages between two entities are intercepted so that an attacker can masquerade as one of the entities

B) a mechanism that enables the implementation of the reverse function in a one-way function

C) an attack that repeatedly tries different values to determine the key used

D) a mechanism built into an algorithm that allows an individual to bypass or subvert the security in some fashion

Question #15 of 193

Question ID: 1114714

What would be considered an environmental error?

a. overheating

b. static electricity

c. authentication problems

d. invalid device configuration

- **A)** options c and d
- **B)** option b
- **C)** options b and c
- **D)** option d
- **E)** options a and b
- **F)** option a
- **G)** option c

Question #16 of 193

Question ID: 1104995

Which attack is considered a passive attack?

- **A)** wiretapping
- **B)** penetration attack
- **C)** denial-of-service (DoS) attack
- **D)** data diddling

Question #17 of 193

Question ID: 1105053

During an XOR operation, two bits are combined. Both values are the same. What will be the result of this combination?

- **A)** 0
- **B)** OR
- **C)** 1
- **D)** X

Question #18 of 193

Question ID: 1105077

You have implemented a public key infrastructure (PKI) to issue certificates to the computers on your organization's network. You must ensure that the certificates that have been validated are protected. What must be secured in a PKI to do this?

A) the public key of a user's certificate

B) the private key of a user's certificate

C) the public key of the root CA

D) the private key of the root CA

Question #19 of 193

Question ID: 1104935

Which statement is true of Compartmented Mode Workstations (CMW)?

A) CMW operates on the principle of maximum privilege.

B) CMW operates in a dedicated security mode.

C) CMW, by default, grants information-related access to all users having security clearance.

D) CMW requires the use of information labels.

Question #20 of 193

Question ID: 1111724

Which of these attacks is an attack on an organization's cryptosystem?

A) Denial of Service (DoS)

B) brute force attack

C) buffer overflow

D) known plaintext attack

Question #21 of 193

Question ID: 1105057

You recently discovered a folder on your computer that contains a secured copy of the private key for all users in your organization. You maintain this copy to ensure that you can recover lost keys. Of which security practice is this an example?

A) CRL

B) quantum cryptography

C) key escrow

D) steganography

Question #22 of 193

Question ID: 1105071

What refers to the type of trust model used by CAs?

A) ring

B) hierarchy

C) bus

D) mesh

Question #23 of 193

Question ID: 1132508

Which TCSEC security rating addresses the use of covert channel analysis?

A) D

B) B1

C) B2

D) A1

Question #24 of 193

Question ID: 1105070

The IT department manager informs you that your organization's network has been the victim of a ciphertext-only attack. Which statement is true regarding this type of attack?

A) It is very difficult for an attacker to gather the ciphertext in a network.

B) A ciphertext-only attack is considered by hackers to be the easiest attack.

C) A ciphertext-only attack is focused on discovering the encryption key.

D) A birthday attack is an example of a ciphertext-only attack.

Question #25 of 193

Question ID: 1114705

Which statement is true of the Rijndael algorithm?

A) Rijndael uses fixed block lengths and fixed key lengths.

B) Rijndael uses variable block lengths and variable key lengths.

C) Rijndael uses fixed block lengths and variable key lengths.

D) Rijndael uses variable block lengths and fixed key lengths.

Question #26 of 193

Question ID: 1105040

What is an algorithm that is used to create a message digest for a file to ensure integrity?

A) hash

B) ciphertext

C) plaintext

D) public key

Question #27 of 193

Question ID: 1105016

Which mechanism retains the HTTP information from the previous connection?

A) HTTPS

B) IPSec

C) cookies

D) SSH

Question #28 of 193

Question ID: 1105063

You want to send a file to a coworker named Maria. You do not want to protect the file contents from being viewed; however, when Maria receives the file, you want her to be able to determine whether the contents of the file were altered during transit.

Which protective measure should you use?

A) symmetric encryption

B) asymmetric encryption

C) a digital certificate

D) a digital signature

Question #29 of 193

Question ID: 1111725

Your organization has implemented a public key infrastructure (PKI) for issuing certificates. Recently, your organization issued several certificates to a partner organization. You revoked the certificates today. However, management is concerned that the revocation request grace period will prevent the certificates from being revoked in a timely manner. Which statement is true of this period?

A) It relates to the maximum response time taken by the CA for a revocation.

B) It refers to the grace period for a backup CA server to update itself.

C) It refers to the validity of a digital signature.

D) It refers to the time taken by a registration authority (RA) to register a user.

Question #30 of 193

Question ID: 1113941

Which type of water sprinkler system is NOT appropriate for a data processing environment?

A) dry pipe water sprinkler system

B) deluge water sprinkler system

C) wet pipe water sprinkler system

D) pre-action water sprinkler system

Question #31 of 193

Question ID: 1105045

You need to decrypt a file that is encrypted using asymmetric encryption. What should be used to decrypt the file?

A) plaintext

B) private key

C) public key

D) message digest

Question #32 of 193

Question ID: 1192923

Which access control model uses the star (*) integrity axiom and the simple integrity axiom?

A) Biba model

B) Chinese Wall model

C) Clark-Wilson model

D) Bell-LaPadula model

Question #33 of 193

Question ID: 1104946

Which security model illustrates the multilevel security mode?

A) Bell-LaPadula model

B) finite transaction model

C) access model

D) Brewer and Nash model

Question #34 of 193

Question ID: 1192926

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

What should you implement on the client computers to best manage the encryption keys, passwords, drive encryption, and digital rights for users?

- **A)** TPM
- **B)** PKI
- **C)** VM
- **D)** DNS

Question #35 of 193

Question ID: 1192929

You have been asked to implement antivirus software for your virtualization environment. Where should you install the antivirus software?

- **A)** on each virtual computer only
- **B)** on the host computer only
- **C)** on the physical computer only
- **D)** on both the host computer and all virtual computers

Question #36 of 193

Question ID: 1105044

Which cipher type replaces the original text in a message with a different text?

- **A)** substitution cipher
- **B)** transposition cipher
- **C)** stream cipher
- **D)** block cipher

Question #37 of 193

Question ID: 1104936

Which statement is true of the information flow model?

A) The information flow model does not permit the flow of information from a lower security level to a higher security level.

B) The information flow model allows the flow of information within the same security level.

C) The Biba model is not built upon the information flow model.

D) The information flow model only deals with the direction of flow.

Question #38 of 193

Question ID: 1113924

What is the purpose of a device using direct memory access (DMA)?

A) It communicates using a logical address.

B) It implements high-speed data transfer between the device and memory.

C) It provides multiprocessing using an interrupt-driven input/output (I/O).

D) It implements high-speed data transfer between the device and CPU.

Question #39 of 193

Question ID: 1105074

What is a list of serial numbers of digital certificates that have not expired, but should be considered invalid?

A) UDP

B) CA

C) CRL

D) KDC

Question #40 of 193

Question ID: 1111710

A file server has unexpectedly rebooted into single-user mode. You are not sure what caused the reboot. What should you do next?

A) Recover damaged file system files.

B) Reboot the file server.

C) Validate critical configuration and system files.

D) Identify the cause of the unexpected reboot.

Question #41 of 193

Question ID: 1113918

Which access control model uses states and state transitions in designing the protection system?

A) Take-Grant model

B) Information Flow model

C) Biba model

D) Bell-LaPadula model

Question #42 of 193

Question ID: 1111709

What is the best description of cache memory?

A) non-volatile memory that holds its contents even during power outages

B) special memory used in portable devices

C) volatile memory that loses its contents during power outages

D) memory used for high-speed transfer of data

Question #43 of 193

Question ID: 1113921

You are reviewing the Common Criteria security standards. Which Common Criteria Evaluation Assurance Level (EAL) is the common benchmark for operating systems and products?

A) EAL 4

B) EAL 3

C) EAL 5

D) EAL 6

E) EAL 7

Question #44 of 193

Question ID: 1113933

Which hashing algorithm uses a 192-bit hashing value and was developed for 64-bit systems?

A) MD5

B) SHA

C) Tiger

D) HAVAL

Question #45 of 193

Question ID: 1192928

You are responsible for managing a Windows Server 2012 computer that hosts several virtual computers. You need to install the latest patches for the operating system. Where should you install the patches?

A) on both the host computer and all Window Server 2012 virtual computers

B) on each Windows Server 2012 virtual computer only

C) on the physical computer only

D) on the host computer only

Question #46 of 193

Question ID: 1105066

Which service does cryptography fulfill by ensuring that a sender cannot deny sending a message once it is transmitted?

A) authenticity

B) non-repudiation

C) integrity

D) confidentiality

Question #47 of 193

Question ID: 1132509

Which feature identifies the TCSEC security level B2?

A) structured protection

B) controlled access protection

C) minimal protection

D) labeled security

Question #48 of 193

Question ID: 1111732

Which type of water sprinkler system is best used in colder climates?

A) wet pipe

B) deluge

C) dry pipe

D) pre-action

Question #49 of 193

Question ID: 1114715

Management has requested that water detectors be installed to ensure that water is detected before major damage is done. In which locations should water detectors be installed?

a. under raised floors

b. between walls

c. under the building's foundation

d. on dropped ceilings

A) options a and d

B) option d

C) option c

D) option a

E) option b

F) options b and c

Question #50 of 193

Question ID: 1105117

Your organization's data center design plans calls for glass panes to be used for one wall of the data center to ensure that personnel in the center can be viewed at all times. Which type of glass should be used?

A) shatter-resistant

B) acrylic

C) tempered

D) wired

E) standard

Question #51 of 193

Question ID: 1105103

Which physical security control is MOST appropriate when discriminating judgment is required for maintaining physical security of a facility?

A) guards

B) closed-circuit television (CCTV)

C) passwords

D) dogs

Question #52 of 193

Question ID: 1104975

What is an integrated circuit with internal logic that is programmable?

A) cache

B) ROM

C) a PLD

D) flash memory

Question #53 of 193

Question ID: 1192925

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

What is the correct description for the Common Criteria level that certain systems must reach because they are part of third-party contracts?

A) methodically designed, tested, and reviewed
B) semi-formally designed and tested
C) semi-formally verified design and tested
D) formally verified design and tested

Question #54 of 193

Question ID: 1105087

Management decides to use message authentication code (MAC) to protect network messages. Which type of attack does this prevent?

A) masquerading attacks
B) denial-of-service attacks
C) logic bomb attacks
D) SYN flood attacks

Question #55 of 193

Question ID: 1105058

Given the key, what is an algorithm that calculates the subkeys for each round of ciphering?

A) key clustering
B) one-way function
C) key escrow
D) key schedule

Question #56 of 193

Question ID: 1105105

Which facility feature can pose the most significant security threat of a facility infrastructure?

A) mantraps

B) anti-static carpets and sprays

C) suspended floors

D) drop ceilings

Question #57 of 193

Question ID: 1114699

Which of the following represents security concerns in cloud computing?

a. access of privileged users

b. location of data

c. segregation of data

d. recovery of data

A) option a

B) option d

C) options c and d

D) option c

E) all of the options

F) options a and b

G) option b

Question #58 of 193

Question ID: 1104992

What is OVAL?

A) an application that checks your network for any known security issues

B) an application that is designed to infect a computer system

C) a piece of hardware that isolates one network from another

D) a standard written in XML that provides open and publicly available security content

Question #59 of 193

Question ID: 1105119

Recently, your organization had a new heating and air conditioning system installed for your facility. Now, when the heat or air turns on, the lights in the facility dim for a small amount of time. What is occurring when the lights dim?

A) a power brown-out

B) a power black-out

C) a power surge

D) a power sag

Question #60 of 193

Question ID: 1104941

Which security principle used in the Bell-LaPadula model prevents the security level of subjects and objects from being changed once they have been created?

A) domination principle

B) static principle

C) principle of least privilege

D) tranquility principle

Question #61 of 193

Question ID: 1114700

Which safeguards should you employ to protect cell phones owned by an organization?

a. Enable wireless interfaces.

b. Maintain physical control.

c. Enable user authentication.

d. Disable unneeded features.

A) option d

B) option c

C) option a

D) option b

E) options b, c, and d

F) options a, b, and c

Question #62 of 193

Question ID: 1192934

What is an example of a brute force attack?

A) using a program to guess passwords from a SAM file

B) searching through a company's trash

C) gathering packets from a network connection

D) sending multiple ICMP messages to a Web server

Question #63 of 193

Question ID: 1105098

You need to store some magnetic storage devices in a temporary storage facility. At which temperature could damage start to occur?

A) 175 degrees Fahrenheit

B) 100 degrees Fahrenheit

C) 90 degrees Fahrenheit

D) 350 degrees Fahrenheit

Question #64 of 193

Question ID: 1105109

Which location would be MOST appropriate for the data center of a company's information processing facility?

A) the facility's top floor

B) the facility's core

C) the facility's ground floor

D) the facility's basement

Question #65 of 193

Question ID: 1105030

Of which type of encryption algorithm is Diffie-Hellman an example?

A) asymmetric with authorization

B) asymmetric with authentication

C) symmetric with digital signature

D) symmetric with authentication

Question #66 of 193

Question ID: 1104972

What is the best description of an open system?

A) a system that contains a single point of control

B) a system that is built upon standards and protocols from published specifications

C) a system that does not follow industry standards

D) a system that contains multiple points of control

Question #67 of 193

Question ID: 1105078

In PKI, which term refers to a public key that can be used to verify the certificate used in a digital signature?

A) a target

B) an issuer

C) a relying party

D) a trust anchor

Question #68 of 193

Question ID: 1113936

Which statement is true of symmetric cryptography?

A) Symmetric cryptography is faster than asymmetric cryptography.

B) Symmetric cryptography provides better security compared to asymmetric cryptography.

C) Symmetric cryptography does not require a secure mechanism to properly deliver keys.

D) Symmetric cryptography uses different keys to encrypt and decrypt messages.

Question #69 of 193

Question ID: 1105014

You have decided to attach a digital timestamp to a document that is shared on the network. Which attack does this prevent?

A) a side channel attack

B) a ciphertext-only attack

C) a replay attack

D) a known-plaintext attack

Question #70 of 193

Question ID: 1113937

Which factor does NOT affect the relative strength of a cryptosystem?

A) the secret key secrecy

B) the encryption algorithm

C) the secret key length

D) the key exchange value

Question #71 of 193

Question ID: 1105064

You need to determine whether the information in a file has changed. What should you use?

A) a digital signature

B) a digital certificate

C) private key encryption

D) public key encryption

Question #72 of 193

Question ID: 1104969

What is the best description of absolute addresses as used in memory architecture?

A) the memory used in complex searches

B) the memory addresses that are not unique

C) the indexed memory addresses that software uses

D) the physical memory addresses that a CPU uses

Question #73 of 193

Question ID: 1104942

Which processes control the flow of information in the lattice-based access control (LBAC) model?

A) star (*) integrity and simple integrity axioms

B) access triple rule

C) simple security, star property, and strong star property rules

D) least upper and greatest lower bound operators

Question #74 of 193

Question ID: 1104938

Which access control model ensures integrity through the implementation of integrity-monitoring rules and integrity-preserving rules?

A) Chinese Wall model

B) Clark-Wilson model

C) Bell-LaPadula model

D) Biba model

Question #75 of 193

Question ID: 1105032

Which statement is NOT true of the operation modes of the data encryption standard (DES) algorithm?

A) Cipher Block Chaining (CBC) and Cipher Feedback (CFB) mode are best used for authentication.

B) Electronic Code Book (ECB) mode operation is best suited for database encryption.

C) ECB is the easiest and fastest DES mode that can be used.

D) ECB repeatedly uses produced ciphertext to encipher a message consisting of blocks.

Question #76 of 193

Question ID: 1114716

Your company's fire safety plan states that the heating and air conditioning system should be shut down in case of a fire. Which of the following does NOT represent reasons for doing this?

a. The fire suppression systems will not function if the heating and air conditioning system is on.

b. The fire detection systems will not function if the heating and air conditioning system is on.

c. The spread of smoke throughout the building will be prevented.

d. Oxygen will be prevented from reaching the fire.

A) option c

B) options a and b

C) option d

D) option b

E) option a

F) options c and d

Question #77 of 193

Question ID: 1114703

Which types of encryption require private keys to be shared?

a. asymmetric encryption

b. private key encryption

c. public key encryption

d. symmetric encryption

A) option a
B) options a and c
C) option c
D) option d
E) option b
F) options b and d

Question #78 of 193

Question ID: 1105023

Which service provided by a cryptosystem turns information into unintelligible data?

A) authorization
B) nonrepudiation
C) integrity
D) confidentiality

Question #79 of 193

Question ID: 1113929

Which type of password attack is often referred to as an exhaustive attack?

A) phishing attack

B) dictionary attack

C) brute force attack

D) spoofing attack

Question #80 of 193

Question ID: 1192931

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

Which of the following policies and controls should you deploy for the client systems based on their identified risks? (Choose all that apply.)

A) Use drive encryption on all client system hard drives.

B) Deploy anti-malware and anti-virus software on all client systems.

C) Deploy only licensed, supported operating systems.

D) Deploy firewall and host-based intrusion detection systems on the client systems.

Question #81 of 193

Question ID: 1105083

Your organization has implemented a public key infrastructure (PKI). You need to ensure that each user's browser automatically checks the status of the user's certificate. What should you implement?

A) CRL

B) OCSP

C) MIME

D) PGP

Question #82 of 193

Question ID: 1113931

What is an encryption algorithm?

A) an encryption key

B) a mathematical formula

C) data before encryption

D) data after encryption

Question #83 of 193

Question ID: 1192936

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

What should you deploy for the research department files?

A) RC6

B) Diffie-Hellman

C) SHA-3

D) 3DES

Question #84 of 193

Question ID: 1104979

You have been asked to ensure that data at rest on organizational computers remains confidential. Which security control should you implement?

A) link encryption

B) access control lists

C) baselines

D) drive encryption

Question #85 of 193

Question ID: 1111718

Which characteristic of PGP is different from the use of formal trust certificates?

A) the use of trust domains by the servers and the clients

B) the use of Certificate Authority servers

C) the deployment of private keys for authentication and encryption

D) the establishment of a web of trust between the users

Question #86 of 193

Question ID: 1105072

Which task does a key revocation system accomplish?

A) key generation

B) key invalidation

C) private key protection

D) key validation

Question #87 of 193

Question ID: 1104954

To what does ISO 15408 refer?

A) ITSEC

B) Common Criteria

C) TCSEC

D) security policy

Question #88 of 193

Question ID: 1114709

A new security policy implemented by your organization states that all official e-mail messages must be signed with digital signatures. Which elements are provided when these are used?

a. integrity

b. availability

c. encryption

d. authentication

e. non-repudiation

A) option c

B) options c, d, and e

C) option d

D) option b

E) options a, d, and e

F) option a

G) option e

H) options a, b, and c

Question #89 of 193

Question ID: 1114691

Which of the following entities are NOT subjects?

a. user

b. process

c. file

d. group

e. directory

f. computer

A) option d

B) option c

C) all of the options

D) option f

E) option b

F) option a

G) option e

H) options c, e, and f only

I) options a, b, and d only

Question #90 of 193

Question ID: 1192933

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

You have been asked to identify any natural threats that could affect any and all offices in the United States. Which of the following should you include?

A) electrical, communications, and utilities outages

B) strikes, riots, and terrorist acts

C) explosions, vandalism, and fraud

D) tornadoes, floods, and earthquakes

Question #91 of 193

Question ID: 1192924

Which access control model uses the simple security rule, the star property rule, and the strong star property rule?

A) Biba model

B) Bell-LaPadula model

C) Clark-Wilson model

D) Chinese Wall model

Question #92 of 193

Question ID: 1105101

As part of your organization's security plan, security guards are stationed at each publicly accessible entrance to the facility. In the context of physical security, which statement about security guard personnel is most appropriate?

A) Security guard personnel are one of the administrative controls in a layered security architecture.

B) Security guard personnel act as the last line of defense in securing the facility infrastructure.

C) Security guard personnel are a cost effective countermeasure to reduce physical security risk.

D) Security guard personnel are the most expensive countermeasure for reducing the physical security risk.

Question #93 of 193

Question ID: 1105084

While developing your organization's Web site, the Web developer needs to ensure that certain messages are transmitted securely. Which technology would be the best choice for this purpose?

A) S-HTTP

B) HTTP

C) SET

D) HTTPS

Question #94 of 193

Question ID: 1105094

Your organization has decided to build a new facility. During the design phase, you are asked to consider the combustibility of building materials. Which items should you NOT consider for this issue?

A) ceilings

B) doors

C) walls

D) windows

Question #95 of 193

Question ID: 1105075

What is contained within an X.509 CRL?

A) private keys

B) serial numbers

C) digital certificates

D) public keys

Question #96 of 193

Question ID: 1113943

Your organization protects its data center using a smart lock. Each user has a unique code to enter in the smart lock to access the data center. The code is configured to only allow access during certain times and days. Which type of lock is implemented?

A) combination lock

B) cipher lock

C) tumbler lock

D) mechanical lock

Question #97 of 193

Question ID: 1113934

Your organization is working with an international partner on a new and innovative product. All communication regarding this must be encrypted using a public domain symmetric algorithm. Which algorithm should you use?

A) DES

B) IDEA

C) 3DES

D) Blowfish

Question #98 of 193

Question ID: 1114712

What is the first step in designing an effective physical security program?

A) Determine performance baselines from acceptable risk levels.

B) Carry out the physical security risk analysis.

C) Identify the physical security program team.

D) Define an acceptable risk level for each physical security threat.

Question #99 of 193

Question ID: 1104956

Which Rainbow Series book covers security issues for networks and network components?

A) the Red Book

B) the Black Book

C) the Orange Book

D) the Green Book

Question #100 of 193

Question ID: 1113940

Recently, management has become concerned that RFI is causing issues in your organization's facility. What can cause this type of interference?

A) electric motors

B) electric wiring

C) fluorescent lighting

D) lightning

Question #101 of 193

Question ID: 1105031

You have recently implemented a public key infrastructure on a Windows Server 2008 network. Digital certificates will be issued to all valid users and computers. Which statement is NOT true of digital certificates?

A) Level 1 assurance for a digital certificate only requires an e-mail address.

B) X.509 is a digital certificate standard.

C) Digital certificates provide authentication before securely sending information to a Web server.

D) Level 2 assurance for a digital certificate only verifies a user's name and e-mail address.

Question #102 of 193

Question ID: 1113923

Which statement is true of complex instruction set computers (CISC)?

A) The access calls to main memory are fewer as compared to RISC.

B) The programmer is explicitly required to call the loading and storing functions.

C) An instruction set executes a single low-level operation.

D) The instruction set supports all the low-level programming languages.

Question #103 of 193

Question ID: 1105054

What is key clustering?

A) the act of transforming data into a readable format

B) the practice of breaking cryptographic systems

C) when two different keys encrypt a plaintext message into the same ciphertext

D) the estimated time, effort, and resources needed to break a cryptographic system

Question #104 of 193

Question ID: 1104993

In which situation does cross-site scripting (XSS) pose the most danger?

A) A user accesses a static content Web site.

B) A user accesses a publicly accessible Web site.

C) A user accesses a financial organization's site using his or her login credentials.

D) A user accesses a knowledge-based site using his or her login credentials.

Question #105 of 193

Question ID: 1192932

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded financial institution to help manage organizational security. The company's main office is in New York, NY, and it has additional branch offices throughout the United States.

Current Issues

The current infrastructure includes Windows servers, UNIX servers, Windows clients, Mac clients, Windows mobile devices, and Mac mobile devices deployed over all offices. The company's IT department has a large staff located in the NY office. Each branch office has a few local IT personnel who only handle issues for that branch.

You have identified several instances where attacks against client systems were not prevented or detected at the client level because no controls were deployed to prevent the attack. Data was stolen from some devices. An entire branch office was infected with malware and viruses and required several days recovery time, which meant lost revenue. Finally, you recently discovered that several client systems have non- licensed versions of OSs installed. You must ensure that the appropriate controls are deployed to mitigate these risks.

In a recent audit, you discovered that several mobile devices lacked the appropriate updates to their operating systems or applications. In addition, users had disabled the remote wiping and GPS location features on these devices and had installed several unauthorized applications. You need a solution to mitigate these risks and control mobile device settings and applications when those devices are attached to the enterprise.

Because of several contracts between your company and third parties, you must ensure that certain systems within your infrastructure achieve EAL7 in the Common Criteria evaluation model.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operational status. During that time, personnel in the main office were unable to access the important human resources information stored on the affected server.

Users are expected to use symmetric and asymmetric encryption to ensure data confidentiality. You need to implement an appropriate system for managing the encryption keys, hashes, and digital certificates on all client computers. You must also protect passwords, encrypt drives, and manage digital rights for these same computers.

Data integrity has become an increasingly serious concern for the files created and maintained by the research department. You must deploy the appropriate solution for these files. All of the files are located on a single server that is accessible only by users in the research department.

A thorough risk analysis was never formally completed for the entire organization. You have been asked to spearhead this project. As part of this process, you must identify the geographical threats to each individual office.

Your organization will be deploying two international offices later this year. You have been invited to participate in the facility selection and internal building security process to provide particular security input.

What should you deploy to help with the mobile device issues?

A) group policies

B) Kerberos

C) MDM

D) Active Directory

Question #106 of 193

Question ID: 1132519

Which Web technology provides the highest level of security?

A) ActiveX

B) JavaScript

C) HTTPS

D) S-HTTP

Question #107 of 193

Question ID: 1105028

What is the primary problem of symmetric cryptography?

A) hardware and software implementation

B) key management

C) different keys for encryption and decryption

D) high processing

Question #108 of 193

Question ID: 1105059

Your organization has decided to implement the Diffie-Hellman asymmetric algorithm. Which statement is true of this algorithm's key exchange?

A) Authorized users need not exchange secret keys.

B) Authorized users exchange public keys over a secure medium.

C) Unauthorized users exchange public keys over a nonsecure medium.

D) Authorized users exchange secret keys over a nonsecure medium.

Question #109 of 193

Question ID: 1105009

What are confidentiality services?

A) digital signatures

B) authentication schemes

C) RAID arrays

D) encryption technologies

Question #110 of 193

Question ID: 1114708

Your organization implements hybrid encryption to provide a high level of protection of your data. Which statements are true of this type of encryption?

a. The secret key protects the encryption keys.

b. Public keys decrypt the secret key for distribution.

c. Asymmetric cryptography is used for secure key distribution.

d. The symmetric algorithm generates public and private keys.

e. Symmetric cryptography is used for encryption and decryption of data.

A) option b

B) option d

C) option e

D) option a

E) options c and d

F) options a and b

G) options c and e

H) option c

Question #111 of 193

Question ID: 1113944

Gaining unauthorized access to the data center by using another user's credentials when following them into the building is an example of which option?

A) turnstile

B) mantrap

C) intrusion

D) piggybacking

Question #112 of 193

Question ID: 1114707

Which option is a public key encryption algorithm?

A) IDEA

B) Skipjack

C) RSA

D) RC5

Question #113 of 193

Question ID: 1113939

Which element can be a threat to electrical systems in an information processing facility?

A) a sag

B) a spike buster

C) an uninterruptible power supply (UPS)

D) a power line conditioner

Question #114 of 193

Question ID: 1105073

Which entity must certify the public key pair of a root CA?

A) an external CA

B) a subordinate CA

C) a Kerberos server

D) the root CA

Question #115 of 193

Question ID: 1105038

Which cipher is based on the clues of the physical factors rather than the hardware or a software cryptosystem?

A) a transposition cipher

B) a concealment cipher

C) a DES cipher

D) a 3DES cipher

Question #116 of 193

Question ID: 1113919

Which two factors ensure that information is compartmentalized in the information flow model?

A) classification and flow

B) classification and role

C) classification and need to know

D) role and need to know

Question #117 of 193

Question ID: 1111705

Which Orange Book level is considered mandatory protections and is based on the Bell-LaPadula security model?

A) D

B) B

C) A

D) C

Question #118 of 193

Question ID: 1104962

Which section of the Minimum Security Requirements for Multi-User Operating System (NISTIR 5153) document addresses end-to-end user accountability?

A) access control
B) data integrity
C) system integrity
D) audit

Question #119 of 193

Question ID: 1105127

You have been asked to implement a plan whereby the server room for your company will remain online for three hours after a power failure. This will give your IT department enough time to implement the alternate site. Which technology would be best in this scenario?

A) RAID
B) backup generator
C) UPS
D) clustering

Question #120 of 193

Question ID: 1105025

All of the following affect the strength of encryption, EXCEPT:

A) the length of the data being encrypted
B) the secrecy of the key
C) the algorithm
D) the length of the key

Question #121 of 193

Question ID: 1105085

You need to ensure that a single document transmitted from your Web server is encrypted. You need to implement this solution as simply as possible.

What should you do?

A) Use JavaScript.

B) Use HTTPS.

C) Use ActiveX.

D) Use S-HTTP.

Question #122 of 193

Question ID: 1113935

What is the purpose of authentication in a cryptosystem?

A) verifying the user's or system's identity

B) turning information into unintelligible data

C) ensuring that the data's sender cannot deny having sent the data

D) ensuring that data has not been changed by an unauthorized user

Question #123 of 193

Question ID: 1113920

Which security model ensures that the activities performed at a higher security level do not affect the activities at a lower security level?

A) Brewer and Nash model

B) information flow model

C) Biba model

D) noninterference model

Question #124 of 193

Question ID: 1105125

An IT user has been asked to replace a hard drive in a server. However, when the user opens the case, he notices that the current hard drive is connected to the hard drive opening using a steel cable. He indicates that he does not know where the key is. Which type of lock is being described?

A) cable trap

B) slot lock

C) switch control

D) port control

Question #125 of 193

Question ID: 1111723

Your organization has decided to use one-time pads to ensure that certain confidential data is protected. All of the following statements are true regarding this type of cryptosystem, EXCEPT:

A) Each one-time pad can be used only once.

B) The pad must be distributed and stored in a secure manner.

C) The pad must be as long as the message.

D) The pad must be made up of sequential values.

Question #126 of 193

Question ID: 1114702

Which attacks are considered common access control attacks?

a. spoofing

b. phreaking

c. SYN flood

d. dictionary attacks

e. brute force attacks

A) option b

B) all of the options

C) option a

D) option d

E) option e

F) options a, d, and e only

G) options b and c only

H) option c

Question #127 of 193

Question ID: 1104944

Which processes define the supervisor mode?

A) processes that are executed in the outer protection rings

B) processes with no protection mechanism

C) processes in the outer protection ring that have more privileges

D) processes that are executed in the inner protection rings

Question #128 of 193

Question ID: 1154292

Which statements do NOT define the requirements of a security kernel?

a. The reference monitor should be verified as correct.

b. The reference monitor should provide process isolation.

c. The security kernel should be verified in a comprehensive manner.

d. A method to circumvent the security should be implemented by the reference monitor.

A) option c

B) options b and d

C) option a

D) options a and c

E) option b

F) option d

Question #129 of 193

Question ID: 1192930

You are responsible for managing the virtual computers on your network. Which guideline is important when managing virtual computers?

A) Implement a firewall only on the host computer.

B) Isolate the host computer and each virtual computer from each other.

C) Update the operating system and applications only on the host computer.

D) Install and update the antivirus program only on the host computer.

Question #130 of 193

Question ID: 1104945

What happens when a trusted computing base (TCB) failure occurs as a result of a lower-privileged process trying to access restricted memory segments?

A) Operating system reinstallation is required.

B) The system goes into maintenance mode.

C) Administrator intervention is required.

D) The system reboots immediately.

Question #131 of 193

Question ID: 1105080

Your organization has recently signed a contract with a governmental agency. The contract requires that you implement the X.509 standard. What does this standard govern?

A) IPSec

B) HTTP

C) PKI

D) IKE

Question #132 of 193

Question ID: 1105033

Which statement is NOT true of an RSA algorithm?

A) RSA can prevent man-in-the-middle attacks.

B) RSA is a public key algorithm that performs both encryption and authentication.

C) An RSA algorithm is an example of symmetric cryptography.

D) RSA encryption algorithms do not deal with discrete logarithms.

E) RSA uses public and private key signatures for integrity verification.

Question #133 of 193

Question ID: 1114701

Management at your organization has recently become aware that the Internet of Things (IoT) movement has resulted in many security issues. They have asked that you identify some of the vulnerabilities presented by IoT from the following list:

A. insecure management Web interface

B. insufficient or lack of authentication

C. lack of transport encryption

D. insecure software/firmware

E. insufficient or lack of physical security

Which would apply?

A) A, B, C, and D

B) All of the above

C) A and B only

D) C and D only

E) D and E only

F) B and C only

Question #134 of 193

Question ID: 1111711

Which term is an evaluation of security components and their compliance prior to formal acceptance?

A) security control

B) accreditation

C) certification

D) information system control

Question #135 of 193

Question ID: 1105128

You need to ensure that data on your organization's computers is not lost when a power outage occurs. Users must have enough time to save their data if a power outage occurs. What should you use?

A) a sprinkler

B) a door lock

C) a UPS

D) an air conditioner

Question #136 of 193

Question ID: 1105012

While researching Internet Protocol Security (IPSec), you discover that it uses Internet Key Exchange (IKE). What is the main purpose of IKE?

A) to encrypt the data across the network

B) to manage the security associations (SAs) across the network

C) to replay the data across the network

D) to authenticate the data across the network

Question #137 of 193

Question ID: 1105107

Several rooms in your facility have traverse-mode noise. Which factor influences the generation of this noise?

A) positive pressurization

B) difference between hot and ground wires

C) difference between hot and neutral wires

D) uninterruptible power supply

Question #138 of 193

Question ID: 1105026

Management has asked you to research encryption and make a recommendation on which encryption technique to use. During this research, you examine several different cryptosystems. Which parameter determines their strength?

A) the length of the key

B) the key management infrastructure

C) the security framework

D) the message authentication code (MAC)

Question #139 of 193

Question ID: 1111722

You are preparing a proposal for management about the value of using cryptography to protect your network. Which statement is true of cryptography?

A) Availability is a primary concern of cryptography.

B) Cryptography is used to detect fraudulent disclosures.

C) The keys in cryptography can be made public.

D) Key management is a primary concern of cryptography.

Question #140 of 193

Question ID: 1105056

What is the purpose of the BitLocker technology?

A) It locks your computer so that it cannot be booted.

B) It encrypts data as it is transmitted over a network.

C) It locks your hard drive so that it cannot be booted.

D) It encrypts the drive contents so that data cannot be stolen.

Question #141 of 193

Question ID: 1105002

Your organization's management has recently spent time discussing attacks against companies and their infrastructure. During the meeting, the Stuxnet attack was discussed. Against which type of system did this attack occur?

A) Kerberos

B) SCADA

C) VoIP

D) RADIUS

Question #142 of 193

Question ID: 1105076

Which entity issues digital certificates?

A) BDC

B) CA

C) DC

D) EFS

Question #143 of 193

Question ID: 1105052

Which of the following was a German rotor machine used in World War II?

A) Lucifer

B) Ultra Project

C) Enigma

D) Purple Machine

Question #144 of 193

Question ID: 1105068

Which statement is NOT true of cryptanalysis?

A) It is a tool used to develop a secure cryptosystem.

B) It is used to test the strength of an algorithm.

C) It is a process of attempting reverse engineering of a cryptosystem.

D) It is used to forge coded signals that will be accepted as authentic.

Question #145 of 193

Question ID: 1114694

Which options are components of the security kernel?

a. software

b. hardware

c. reference monitor

d. trusted computing base

A) options a and b

B) options c and d

C) option d

D) option a

E) option b

F) option c

Question #146 of 193

Question ID: 1111729

Which control includes mantraps and turnstiles?

A) environmental control

B) administrative control

C) technical control

D) physical control

Question #147 of 193

Question ID: 1104960

Which entity can operate as both a subject and an object?

- **A)** program
- **B)** group
- **C)** file
- **D)** user

Question #148 of 193

Question ID: 1113938

Your organization has identified several sites as options for relocation. One of the locations has a positive drain system. What does this system ensure with reference to physical security?

- **A)** the air flows out of the room as soon as the door is opened
- **B)** the contents of the water, gas, and steam pipelines flows into the building
- **C)** the clean and steady supply of power from electrical distribution boxes to electrical devices
- **D)** the contents of the water, gas, and steam pipelines flows out of the building

Question #149 of 193

Question ID: 1104950

What differentiates ITSEC from TCSEC?

- **A)** Functionality and assurance are evaluated separately by ITSEC.
- **B)** Development practices and documentation are evaluated as a part of the system functionality.
- **C)** Auditing and authentication services are not provided to the users by ITSEC.
- **D)** ITSEC ratings are not mapped to the Orange Book.

Question #150 of 193

Question ID: 1114697

What is the best description of reduced instruction set computing (RISC)?

A) computing using instructions that perform many operations per instruction

B) processing that executes one instruction at a time

C) processing that enables concurrent execution of multiple instructions

D) computing using instructions that are simpler and require fewer clock cycles to execute

Question #151 of 193

Question ID: 1114717

Which statements are true of halon as a fire suppression agent?

a. Halon is safe for humans.

b. Halon deals with Class A category of fire.

c. Halon gas suppresses fire by a chemical reaction.

d. FM-200 is an EPA-approved replacement for halon.

e. Halon is currently approved by the Environmental Protection Agency (EPA).

A) option a

B) option d

C) option b

D) option e

E) options b, c, and d

F) option c

G) options c and d

H) options a and b

Question #152 of 193

Question ID: 1114710

You are part of the design team for an organization's information processing facility. Which option or options represent potential physical security risks to the design?

a. spoofing

b. physical theft

c. power failure

d. hardware damage

e. denial of service (DoS) attack

- **A)** option b
- **B)** option e
- **C)** option d
- **D)** options a, b, and c
- **E)** options b, c, and d
- **F)** option c
- **G)** options c, d, and e
- **H)** option a

Question #153 of 193

Question ID: 1192935

You are the security administrator for an organization. Management decides that all communication on the network should be encrypted using the data encryption standard (DES) algorithm. Which statement is true of this algorithm?

- **A)** The effective key size of DES is 64 bits.
- **B)** A 56-bit DES encryption is 256 times more secure than a 40-bit DES encryption.
- **C)** A DES algorithm uses 32 rounds of computation.
- **D)** A Triple DES (3DES) algorithm uses 48 rounds of computation.

Question #154 of 193

Question ID: 1111717

Which statement is true of FIPS 140?

- **A)** FIPS deals with hardware products.
- **B)** FIPS only deals with cryptographic software.
- **C)** FIPS does not validate software to be used by government agencies.

D) FIPS specifies security requirements for hardware and software cryptographic modules.

Question #155 of 193

Question ID: 1111730

Which security practice does NOT address the physical and environmental protection for a facility?

A) The flood-warning systems are upgraded once a year.

B) The entry codes in the facility are changed at regular intervals.

C) The entry and exit to the facility are continuously monitored by CCTVs.

D) Measures are taken to prevent theft of information by unauthorized individuals.

Question #156 of 193

Question ID: 1105055

Which technology requires Trusted Platform Module (TPM) hardware?

A) IPSec

B) NTFS

C) BitLocker

D) EFS

Question #157 of 193

Question ID: 1104989

Your organization has decided to implement cloud computing and has set up Platform as a Service (PaaS) with a cloud provider. What is the main focus of this type of cloud deployment?

A) virtual machine management

B) access control

C) data protection

D) application access management

Question #158 of 193

Question ID: 1104998

Which of the following is NOT a countermeasure for mitigating maintenance hooks?

A) Encrypt all sensitive information contained in the system.

B) Use a host-based IDS to record any attempt to access the system using one of these hooks.

C) Implement auditing to supplement the IDS.

D) Ensure that if critical sets of instructions do not execute in order and in entirety, any changes they make are rolled back or prevented.

Question #159 of 193

Question ID: 1105024

What is another term for cryptography strength?

A) initialization vector

B) public key

C) work factor

D) private key

Question #160 of 193

Question ID: 1105096

Your organization is using the Crime Prevention Through Environmental Design (CPTED) approach to ensure that your site is designed properly. Which facet of this approach includes door, fence, lighting, and landscaping placement?

A) target hardening

B) natural surveillance

C) territorial reinforcement

D) natural access control

Question #161 of 193

Question ID: 1105042

What produces 160-bit checksums?

A) AES

B) DES

C) MD5

D) SHA

Question #162 of 193

Question ID: 1132516

Which attack sends unsolicited messages over a Bluetooth connection?

A) blue jacking

B) spamming

C) bluesnarfing

D) war driving

Question #163 of 193

Question ID: 1113942

What is NOT a component of a transponder system-sensing card?

A) spread spectrum

B) transmitter

C) battery

D) receiver

Question #164 of 193

Question ID: 1105051

Given two messages, M1 and M2, what is the LEAST likely outcome when using the same one-way hash function, H, to encrypt the messages?

A) H(M1) > H(M2)

B) H(M1) is not equal to H(M2)

C) H(M1) = H(M2)

D) H(M1) < H(M2)

Question #165 of 193

Question ID: 1192927

You are responsible for managing your company's virtualization environment. Which feature should NOT be allowed on a virtualization host?

A) implementing IPsec

B) implementing a firewall

C) monitoring the event logs

D) browsing the Internet

Question #166 of 193

Question ID: 1192938

Which suppression methods are recommended when paper, laminates, and wooden furniture are the elements of a fire in the facility?

a. Halon

b. Water

c. Soda acid

d. Dry powder

A) options c and d

B) option b

C) option d

D) options a and b

E) options b and c

F) option a

G) option c

Question #167 of 193

Question ID: 1105062

Which hashing algorithm was designed to be used with the Digital Signature Standard (DSS)?

A) Message Digest 5 (MD5)

B) HAVAL

C) Secure Hash Algorithm (SHA)

D) Tiger

Question #168 of 193

Question ID: 1104990

Your company hosts several public Web sites on its Web server. Some of the sites implement the secure sockets layer (SSL) protocol. Which statement is NOT true of this protocol?

A) SSL operates at the Network layer of the OSI model.

B) SSL version 2 provides client-side authentication.

C) SSL is used to protect Internet transactions.

D) SSL has two possible session key lengths: 40 bit and 128 bit.

E) SSL with TLS supports both server and client authentication.

Question #169 of 193

Question ID: 1114706

You have been hired as a security administrator. Management informs you that the network uses SKIP encryption. Which statement is true of this protocol?

A) SKIP is a key distribution protocol.

B) SKIP works on a response-by-session basis.

C) SKIP is only a key storage protocol.

D) SKIP deploys IKE for key distribution and management.

Question #170 of 193

Question ID: 1105048

Which of the following is NOT based on the Feistel cipher?

A) CAST-128

B) Diffie-Hellman

C) Blowfish

D) Skipjack

Question #171 of 193

Question ID: 1105093

Your organization's new facility must be built of fire-resistant material. Which material should be used in its frame construction?

A) steel

B) heavy timber with a fire rating of one hour

C) steel rods encased in concrete walls

D) untreated lumber

Question #172 of 193

Question ID: 1105021

Which service provided by a cryptosystem is most important for the military?

A) integrity

B) nonrepudiation

C) confidentiality

D) authentication

Question #173 of 193

Question ID: 1114711

Your team is tasked with identifying a secure site for facility infrastructure for an organization. Which option represents the visibility considerations involved in this process?

a. lighting

b. types of neighbors

c. environmental controls

d. building markings and signs

e. closed-circuit television (CCTV)

- **A)** option e
- **B)** options a and c
- **C)** option a
- **D)** option b
- **E)** options b and e
- **F)** option d
- **G)** option c
- **H)** options b and d

Question #174 of 193

Question ID: 1111734

Your company's secondary data center recently experienced a fire. The electronic equipment in the data center has been exposed to both water and smoke. You need to ensure that all equipment is cleaned properly. All of the equipment has been powered down. You have also opened all cabinets, panels, and covers to allow water to flow out. What should you do next?

- **A)** Wipe with alcohol or Freon-alcohol solutions, or spray with water-displacement aerosol sprays.
- **B)** Use Freon or Freon-alcohol solvents to spray connectors, backplanes, and printed circuit boards.
- **C)** Spray corrosion-inhibiting aerosol to stabilize metal contact surfaces.
- **D)** Move all the equipment to an environment with proper temperature and humidity controls.

Question #175 of 193

Question ID: 1104964

Which statement is true of indirect memory addressing?

A) The address field points to a memory cell that contains the address of the operand.

B) The address field contains the address of the operand.

C) A single memory access is used to find the operand.

D) It has no memory reference to fetch data.

Question #176 of 193

Question ID: 1104996

What is a rootkit?

A) an application that uses tracking cookies to collect and report a user's activities

B) a software application that displays advertisements while the application is executing

C) a program that spreads itself through network connections

D) a collection of programs that grants a hacker administrative access to a computer or network

Question #177 of 193

Question ID: 1105036

Which binary function is the basis of the functioning of a one-time pad?

A) AND

B) XOR

C) XAND

D) OR

Question #178 of 193

Question ID: 1113930

A customer has requested a computer with a Clipper chip. What is a Clipper chip?

A) It is a modem chip.

B) It is an encryption chip.

C) It is a unique serial number in the computer chip.

D) It is an encryption algorithm.

Question #179 of 193

Question ID: 1114713

Which methods can be used to reduce static electricity?

a. anti-static sprays

b. lower humidity

c. anti-static flooring

d. power line conditioning

A) option d

B) option b

C) option a

D) options b and d

E) option c

F) options a and c

Question #180 of 193

Question ID: 1111699

Your company has an e-commerce site that is publicly accessible over the Internet. The e-commerce site accepts credit card information from a customer and then processes the customer's transaction. Which standard or law would apply for this type of data?

A) Basel II

B) The Economic Espionage Act of 1996

C) PCI DSS

D) SOX

Question #181 of 193

Question ID: 1104970

What is meant by the term fail-safe?

- **A)** a system's ability to recover automatically through a reboot
- **B)** a system's ability to switch over to a backup system in the event of a failure
- **C)** a system's ability to preserve a secure state before and after failure
- **D)** a system's ability to terminate processes when a failure is identified

Question #182 of 193

Question ID: 1104952

Which component is NOT a part of the protection profile information used by the Common Criteria to evaluate products?

- **A)** EAL rating
- **B)** assurance requirements
- **C)** functionality requirements
- **D)** product test results

Question #183 of 193

Question ID: 1105049

Which chip implements the U.S. Escrowed Encryption Standard and was developed by the National Security Agency (NSA)?

- **A)** HSM
- **B)** TPM
- **C)** Capstone
- **D)** Clipper chip

Question #184 of 193

Question ID: 1114693

What is the best description of an execution domain?

A) an isolated area that is used by trusted processes when they are run in privileged state

B) memory space insulated from other running processes in a multiprocessing system

C) components that fall outside the security perimeter of the TCB

D) a communication channel between an applications and the kernel in the TCB

Question #185 of 193

Question ID: 1132511

Which statement is true of reverse engineering?

A) It is used to hide the details of an object's functionality.

B) It removes security flaws from object code.

C) It involves compiling vendor object codes.

D) It analyzes the operation of an application.

Question #186 of 193

Question ID: 1105088

Which option will have the least effect on the confidentiality, integrity, and availability of the resources within the organization?

A) lost keys to the door

B) damaged hard drive

C) primary power failure

D) stolen computer

Question #187 of 193

Question ID: 1105004

During a recent network attack, a hacker used rainbow tables to guess network passwords. Which type of attack occurred?

A) privilege escalation

B) denial-of-service attack

C) brute force password attack

D) social engineering attack

Question #188 of 193

Question ID: 1104982

Which types of computers are targeted by RedPill and Scooby Doo attacks?

A) virtual machines

B) Windows Vista clients

C) terminal servers

D) Windows Server 2008 computers

Question #189 of 193

Question ID: 1104980

Which security risk does the /etc/hosts.equiv file pose on a UNIX system?

A) It allows all users to connect remotely without authenticating.

B) It allows all users to locally edit the DNS configuration.

C) It allows all users to connect locally without authenticating.

D) It allows all users to remotely edit the DNS configuration.

Question #190 of 193

Question ID: 1114704

Your organization must ensure that messages are protected from hackers using encryption. Management decides to implement Secure Hash Algorithm (SHA-1). Which statements are NOT true of this algorithm?

a. SHA-1 produces a 128-bit hash value.

b. SHA-1 was designed by NIST and NSA.

c. SHA-1 is a two-way hash function of variable length.

d. SHA-1 was designed for use in digital signatures.

A) option a

B) option c

C) options b and d

D) option d

E) option b

F) options a and c

Question #191 of 193

Question ID: 1114690

Which characteristics of a system are evaluated by the Trusted Computer System Evaluation Criteria (TCSEC)?

a. assurance

b. authenticity

c. functionality

d. response-time

A) options b and d

B) option b

C) option c

D) option d

E) options a and c

F) option a

G) options a and b

Question #192 of 193

Question ID: 1105043

What does the message authentication code (MAC) ensure?

A) message replay

B) message integrity

C) message confidentiality

D) message availability

Question #193 of 193

Question ID: 1105089

Why should device driver files be digitally signed?

A) to ensure that they are installed by a trusted user

B) to ensure that they are not changed after installation

C) to ensure that they are from a trusted publisher

D) to record the installation timestamp