

Security + Exam (SY0-401)

Number: SY0-401
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



<http://www.gratisexam.com/>

CompTIA SY0-401



CompTIA Security+ Certification

Version: 33.0
CompTIA SY0-401 Exam

<http://www.gratisexam.com/>

Exam A

QUESTION 1

A company plans to expand by hiring new engineers who work in highly specialized areas. Each engineer will have very different job requirements and use unique tools and applications in their job. Which of the following is MOST appropriate to use?

- A. Role-based privileges
- B. Credential management
- C. User assigned privileges
- D. User access

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this question, we have engineers who require different tools and applications according to their specialized job function. We can therefore use the Role-Based Access Control model. Role-Based Access Control (RBAC) models approach the problem of access control based on established roles in an organization. RBAC models implement access by job function or by responsibility. Each employee has one or more roles that allow access to specific information. If a person moves from one role to another, the access for the previous role will no longer be available.

Instead of thinking "Denise needs to be able to edit files," RBAC uses the logic "Editors need to be able to edit files" and "Denise is a member of the Editors group." This model is always good for use in an environment in which there is high employee turnover.

QUESTION 2

A file on a Linux server has default permissions of rw-rw-r--. The system administrator has verified that Ann, a user, is not a member of the group owner of the file. Which of the following should be modified to assure that Ann has read access to the file?

- A. User ownership information for the file in question
"Pass Any Exam. Any Time." - www.actualtests.com 553
CompTIA SY0-401 Exam
- B. Directory permissions on the parent directory of the file in question
- C. Group memberships for the group owner of the file in question
- D. The file system access control list (FACL) for the file in question

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The file permissions according to the file system access control list (FACL) are rw-rw-r--. The first `rw-` are the file owner permissions (read and write). The second `rw-` are the group permissions (read and write) for the group that has been assigned the file.

The third `r--` is the All Users permissions; in this case read only. To enable Ann to access the file, we should add Ann to the group that has been assigned to the file.

Topic 6, Cryptography

QUESTION 3

Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

- A. SFTP
- B. HTTPS
- C. TFTP
- D. TLS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SSL establishes a session using asymmetric encryption and maintains the session using symmetric encryption.

QUESTION 4

A company uses PGP to ensure that sensitive email is protected. Which of the following types of cryptography is being used here for the key exchange?



<http://www.gratisexam.com/>

- A. Symmetric
- B. Session-based
- C. Hashing

"Pass Any Exam. Any Time." - www.actualtests.com 554
CompTIA SY0-401 Exam

<http://www.gratisexam.com/>

D. Asymmetric

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

QUESTION 5

Which of the following is true about asymmetric encryption?

- A. A message encrypted with the private key can be decrypted by the same key
- B. A message encrypted with the public key can be decrypted with a shared key.
- C. A message encrypted with a shared key, can be decrypted by the same key.
- D. A message encrypted with the public key can be decrypted with the private key.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 6

Encryption used by RADIUS is BEST described as:

- A. Quantum
- B. Elliptical curve
- C. Asymmetric
- D. Symmetric

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The RADIUS server uses a symmetric encryption method.

Note: Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected.

"Pass Any Exam. Any Time." - www.actualtests.com 555

CompTIA SY0-401 Exam

QUESTION 7

Symmetric encryption utilizes _____, while asymmetric encryption utilizes _____.

- A. Public keys, one time
- B. Shared keys, private keys
- C. Private keys, session keys
- D. Private keys, public keys

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Symmetrical systems require the key to be private between the two parties. With asymmetric systems, each circuit has one key.

In more detail:

* Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

* Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 8

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

- A. Session Key
- B. Public Key
- C. Private Key
- D. Digital Signature

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

"Pass Any Exam. Any Time." - www.actualtests.com 556

CompTIA SY0-401 Exam

QUESTION 9

In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

- A. Import the recipient's public key
- B. Import the recipient's private key
- C. Export the sender's private key
- D. Export the sender's public key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

See step 4 below.

1. When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
2. PGP then creates a session key, which is a one-time-only secret key.
3. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext.
4. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

QUESTION 10

A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

- A. Block cipher
- B. Stream cipher

- C. CRC
- D. Hashing algorithm

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With a block cipher the algorithm works on chunks of data--encrypting one and then moving to the next.

Example: Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds.

"Pass Any Exam. Any Time." - www.actualtests.com 557

CompTIA SY0-401 Exam

QUESTION 11

The concept of rendering data passing between two points over an IP based network impervious to all but the most sophisticated advanced persistent threats is BEST categorized as which of the following?

- A. Stream ciphers
- B. Transport encryption
- C. Key escrow
- D. Block ciphers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Transport encryption is the process of encrypting data ready to be transmitted over an insecure network. A common example of this would be online banking or online purchases where sensitive information such as account numbers or credit card numbers is transmitted.

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION 12

Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?



<http://www.gratisexam.com/>

- A. SSLv2
- B. SSHv1
- C. RSA
- D. TLS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

HTTP Secure HTTP Secure (HTTPS) is the protocol used for "secure" web pages that users should see when they must enter personal information such as credit card numbers, passwords, and other identifiers. It combines HTTP with SSL/TLS to provide encrypted communication. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL, and it is also referred to as SSL 3.1.

"Pass Any Exam. Any Time." - www.actualtests.com 558
CompTIA SY0-401 Exam

QUESTION 13

Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

- A. 110
- B. 137
- C. 139
- D. 143
- E. 161
- F. 443

Correct Answer: BC

Section: (none)

<http://www.gratisexam.com/>

Explanation

Explanation/Reference:

Explanation: NetBIOS provides four distinct services:

Name service for name registration and resolution (port: 137/udp) Name service for name registration and resolution (port: 137/tcp) Datagram distribution service for connectionless communication (port: 138/udp) Session service for connection-oriented communication (port: 139/tcp)

QUESTION 14

Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

- A. Key escrow
- B. Non-repudiation
- C. Multifactor authentication
- D. Hashing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Regarding digital security, the cryptological meaning and application of non-repudiation shifts to mean:

A service that provides proof of the integrity and origin of data. An authentication that can be asserted to be genuine with high assurance.

QUESTION 15

All of the following are valid cryptographic hash functions EXCEPT:

"Pass Any Exam. Any Time." - www.actualtests.com 559
CompTIA SY0-401 Exam

- A. RIPEMD.
- B. RC4.
- C. SHA-512.
- D. MD4.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RC4 is not a hash function. RC4 is popular with wireless and WEP/WPA encryption.

QUESTION 16

Which of the following concepts is used by digital signatures to ensure integrity of the data?

- A. Non-repudiation
- B. Hashing
- C. Transport encryption
- D. Key escrow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

QUESTION 17

A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files?

- A. Integrity
- B. Confidentiality
- C. Steganography
- D. Availability

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be

"Pass Any Exam. Any Time." - www.actualtests.com 560

CompTIA SY0-401 Exam

incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION 18

A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

- A. Symmetric encryption
- B. Non-repudiation
- C. Steganography
- D. Hashing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION 19

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- A. Hashing
- B. Transport encryption
- C. Digital signatures
- D. Steganography

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

"Pass Any Exam. Any Time." - www.actualtests.com 561
CompTIA SY0-401 Exam

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION 20

Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image?

- A. Transport encryption
- B. Steganography
- C. Hashing
- D. Digital signature

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION 21

Digital Signatures provide which of the following?

- A. Confidentiality
- B. Authorization
- C. Integrity
- D. Authentication
- E. Availability

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 562
CompTIA SY0-401 Exam

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

QUESTION 22

Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

- A. Twofish
- B. Diffie-Hellman
- C. ECC
- D. RSA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

QUESTION 23

Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

- A. Block cipher
- B. Elliptical curve cryptography
- C. Diffie-Hellman algorithm
- D. Stream cipher

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Regarding the performance of ECC applications on various mobile devices, ECC is the most suitable PKC (Public-key cryptography) scheme for use in a constrained environment. Note: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided

"Pass Any Exam. Any Time." - www.actualtests.com 563
CompTIA SY0-401 Exam

by keys of smaller size. Using smaller key size would be faster.

QUESTION 24

A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

- A. Spoof the MAC address of an observed wireless network client
- B. Ping the access point to discover the SSID of the network
- C. Perform a dictionary attack on the access point to enumerate the WEP key
- D. Capture client to access point disassociation packets to replay on the local PC's loopback

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With ARP spoofing (also known as ARP poisoning), the MAC (Media Access Control) address of the data is faked. By faking this value, it is possible to make it look as if the data came from a network that it did not. This can be used to gain access to the network, to fool the router into sending data here that was intended for another host, or to launch a DoS attack. In all cases, the address being faked is an address of a legitimate user, and that makes it possible to get around such measures as allow/deny lists.

Note: As an example, the initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

QUESTION 25

The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

- A. Disable the SSID broadcasting
- B. Configure the access points so that MAC filtering is not used
- C. Implement WEP encryption on the access points

D. Lower the power for office coverage only

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

"Pass Any Exam. Any Time." - www.actualtests.com 564

CompTIA SY0-401 Exam

QUESTION 26

Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

- A. Disable default SSID broadcasting.
- B. Use WPA instead of WEP encryption.
- C. Lower the access point's power settings.
- D. Implement MAC filtering on the access point.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

QUESTION 27

Which of the following provides the strongest authentication security on a wireless network?

- A. MAC filter
- B. WPA2
- C. WEP

D. Disable SSID broadcast

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

QUESTION 28

Which of the following is a concern when encrypting wireless data with WEP?

"Pass Any Exam. Any Time." - www.actualtests.com 565

CompTIA SY0-401 Exam

- A. WEP displays the plain text entire key when wireless packet captures are reassembled
- B. WEP implements weak initialization vectors for key transmission
- C. WEP uses a very weak encryption algorithm
- D. WEP allows for only four pre-shared keys to be configured

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

QUESTION 29

Which of the following provides the HIGHEST level of confidentiality on a wireless network?

- A. Disabling SSID broadcast
- B. MAC filtering
- C. WPA2
- D. Packet switching

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

QUESTION 30

While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

- A. EAP-TLS
- B. PEAP
- C. WEP
- D. WPA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WEP is one of the more vulnerable security protocols. The only time to use WEP is when you must have compatibility with older devices that do not support new encryption.

"Pass Any Exam. Any Time." - www.actualtests.com 566

CompTIA SY0-401 Exam

QUESTION 31

Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.

A security technician was asked to prepare a report of files that had changed since last night's integrity scan.

Which of the following could the technician use to prepare the report? (Select TWO).

- A. PGP
- B. MD5
- C. ECC

- D. AES
- E. Blowfish
- F. HMAC

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: MD5 can be used to locate the data which has changed. The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

F: A common method of verifying integrity involves adding a message authentication code (MAC) to the message.

HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key.

QUESTION 32

Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

- A. Whole disk encryption
- B. SSH
- C. Telnet
- D. MD5

"Pass Any Exam. Any Time." - www.actualtests.com 567
CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

MD5 can be used to locate the data which has changed.

The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

QUESTION 33

Which of the following is used to verify data integrity?

- A. SHA

- B. 3DES
- C. AES
- D. RSA

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SHA stands for "secure hash algorithm". SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is used to ensure data integrity.

Note:

A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact. This is how hashing is used to ensure data integrity.

QUESTION 34

Which of the following can be implemented with multiple bit strength?

"Pass Any Exam. Any Time." - www.actualtests.com 568
CompTIA SY0-401 Exam

- A. AES
- B. DES
- C. SHA-1
- D. MD5
- E. MD4

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AES (a symmetric algorithm) uses key sizes of 128, 192, or 256 bits.

QUESTION 35

To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

- A. SHA
- B. MD5
- C. Blowfish
- D. AES

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is used to encrypt data, not to verify data integrity.

QUESTION 36

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

- A. AES
- B. 3DES
- C. TwoFish
- D. Blowfish

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 569
CompTIA SY0-401 Exam

Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is

considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION 37

Which of the following are restricted to 64-bit block sizes? (Select TWO).

- A. PGP
- B. DES
- C. AES256
- D. RSA
- E. 3DES
- F. AES

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity. It is now considered insecure because of the small key size.

E: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION 38

A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

- A. AES
- B. 3DES
- C. RC4
- D. WPA2

"Pass Any Exam. Any Time." - www.actualtests.com 570
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

3DES (Triple DES) is based on DES.

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV). Microsoft OneNote, Microsoft Outlook 2007, and Microsoft System Center Configuration Manager 2012, use Triple DES to password protect user content and system data.

QUESTION 39

Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

- A. ECC
- B. RSA
- C. SHA
- D. 3DES

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

3DES would be less secure compared to ECC, but 3DES would require less computational power. Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION 40

Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

- A. RIPEMD
- B. MD5
- C. SHA
- D. HMAC

"Pass Any Exam. Any Time." - www.actualtests.com 571
CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. The hashing function provides data integrity, while the symmetric key provides authenticity.

QUESTION 41

Which of the following cryptographic algorithms is MOST often used with IPSec?

- A. Blowfish
- B. Twofish
- C. RC4
- D. HMAC

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The HMAC-MD5-96 (also known as HMAC-MD5) encryption technique is used by IPSec to make sure that a message has not been altered.

QUESTION 42

When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?

- A. SHA
- B. AES
- C. DES
- D. RSA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RSA (an asymmetric algorithm) uses keys of a minimum length of 2048 bits.

QUESTION 43

Which of the following uses both a public and private key?

"Pass Any Exam. Any Time." - www.actualtests.com 572
CompTIA SY0-401 Exam

- A. RSA
- B. AES
- C. MD5
- D. SHA

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process.

RSA uses both a public key and a secret.

RSA key generation process:

1. Generate two large random primes, p and q , of approximately equal size such that their product, $n = pq$, is of the required bit length (such as 2048 bits, 4096 bits, and so forth).

Let $n = pq$

Let $m = (p-1)(q-1)$

2. Choose a small number e , co-prime to m (note: Two numbers are co-prime if they have no common factors).

3. Find d , such that

$de \% m = 1$

4. Publish e and n as the public key. Keep d and n as the secret key.

QUESTION 44

Which of the following ciphers would be BEST used to encrypt streaming video?

- A. RSA
- B. RC4
- C. SHA1
- D. 3DES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP.

Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly.

"Pass Any Exam. Any Time." - www.actualtests.com 573
CompTIA SY0-401 Exam

Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than ciphertext because the involutory nature of the XOR function would result in the second operation reversing the first.

It is noteworthy, however, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known weakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers.

QUESTION 45

Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security?

- A. WPA2-AES
- B. 802.11ac
- C. WPA-TKIP
- D. WEP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

WPA-TKIP uses the RC4 cipher.

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC)

To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every

data packet is sent with a unique encryption key.

QUESTION 46

A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of

"Pass Any Exam. Any Time." - www.actualtests.com 574
CompTIA SY0-401 Exam



<http://www.gratisexam.com/>

the following wireless encryption methods should be implemented?

- A. RC4
- B. AES
- C. MD5
- D. TKIP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RC4 is popular with wireless and WEP/WPA encryption. It is a streaming cipher that works with key sizes between 40 and 2048 bits, and it is used in SSL and TLS.

QUESTION 47

Which of the following can use RC4 for encryption? (Select TWO).

- A. CHAP
- B. SSL
- C. WEP
- D. AES
- E. 3DES

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation: B: In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely used software stream cipher and is used in popular Internet protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

C: WEP also uses RC4, however WEP is still unsecure.

QUESTION 48

Which of the following would provide the STRONGEST encryption?

- A. Random one-time pad
- B. DES with a 56-bit key
- C. AES with a 256-bit key
- D. RSA with a 1024-bit key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

One-time pads are the only truly completely secure cryptographic implementations.

"Pass Any Exam. Any Time." - www.actualtests.com 575

CompTIA SY0-401 Exam

They are so secure for two reasons. First, they use a key that is as long as a plaintext message. That means there is no pattern in the key application for an attacker to use. Also, one-time pad keys are used only once and then discarded. So even if you could break a one-time pad cipher, that same key would never be used again, so knowledge of the key would be useless.

QUESTION 49

Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

- A. RC4
- B. 3DES
- C. AES
- D. MD5

- E. PGP
- F. Blowfish

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

C: Advanced Encryption Standard (AES) is a block cipher that has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.

F: Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds.

QUESTION 50

Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

- A. AES
- B. Blowfish
- C. RC5
- D. 3DES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 576
CompTIA SY0-401 Exam

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

QUESTION 51

Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

- A. 3DES

- B. Blowfish
- C. Serpent
- D. AES256

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. Blowfish is a fast, except when changing keys. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

QUESTION 52

Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

- A. Blowfish
- B. DES
- C. SHA256
- D. HMAC

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). Among the alternatives listed above, it is the only cipher that can use a 128-bit key and which does provide additional security through a symmetric key.

"Pass Any Exam. Any Time." - www.actualtests.com 577
CompTIA SY0-401 Exam

QUESTION 53

When using PGP, which of the following should the end user protect from compromise? (Select TWO).

- A. Private key

- B. CRL details
- C. Public key
- D. Key password
- E. Key escrow
- F. Recovery agent

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A: In PGP only the private key belonging to the receiver can decrypt the session key. PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

D: PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key.

QUESTION 54

A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel.

Which of the following implements the required secure key negotiation? (Select TWO).

- A. PBKDF2
- B. Symmetric encryption
- C. Steganography
- D. ECDHE
- E. Diffie-Hellman

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Elliptic curve DiffieHellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric

"Pass Any Exam. Any Time." - www.actualtests.com 578
CompTIA SY0-401 Exam

key cipher. It is a variant of the Diffie-Hellman protocol using elliptic curve cryptography. Note: Adding an ephemeral key to Diffie-Hellman turns it into DHE (which, despite the order of the acronym, stands for Ephemeral Diffie-Hellman). Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE (again, overlook the order of the acronym letters; it is called Ephemeral Elliptic Curve Diffie-Hellman). It is the ephemeral component of each of these that provides the perfect forward secrecy.

QUESTION 55

An administrator has two servers and wants them to communicate with each other using a secure algorithm.

Which of the following choose to provide both CRC integrity checks and RCA encryption?

- A. NTLM
- B. RSA
- C. CHAP
- D. ECDHE

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ECDHE provides both CRC integrity checks and RCA encryption. Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE. It is the ephemeral component of each of these that provides the perfect forward secrecy. Forward secrecy is a property of any key exchange system, which ensures that if one key is compromised, subsequent keys will not also be compromised. Perfect forward secrecy occurs when this process is unbreakable.

QUESTION 56

Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

- A. RIPEMD
- B. PAP
- C. CHAP
- D. RC4
- E. Kerberos

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 579
CompTIA SY0-401 Exam

Explanation:

B: A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources.

C: CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three- way handshake.

QUESTION 57

Which of the following offers the LEAST secure encryption capabilities?

- A. TwoFish
- B. PAP
- C. NTLM
- D. CHAP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP.

QUESTION 58

Which of the following algorithms has well documented collisions? (Select TWO).

- A. AES
- B. MD5
- C. SHA
- D. SHA-256
- E. RSA

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: MD5 biggest weakness is that it does not have strong collision resistance, and thus it is no longer recommended for use.

C: SHA-1 (also known as SHA) is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1

"Pass Any Exam. Any Time." - www.actualtests.com 580

CompTIA SY0-401 Exam

for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010", though that was later relaxed. Note: The hashing algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output. Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that were once thought to be collision resistant were later broken. MD5 and SHA-1 in particular both have published techniques more efficient than brute force for finding collisions.

QUESTION 59

Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

- A. HTTPS
- B. RDP
- C. HTTP
- D. SFTP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

Example of RDP tracing output:

No. Time Delta Source Destination Protocol Length Info 5782, 2013-01-06 09:52:15.407, 0.000, SRC 10.7.3.187, DST 10.0.107.58, TCP, 62, 3389 > 59193 [SYN, ACK]

QUESTION 60

Which of the following cryptographic related browser settings allows an organization to communicate securely?

- A. SSL 3.0/TLS 1.0
- B. 3DES
- C. Trusted Sites
- D. HMAC

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 581
CompTIA SY0-401 Exam

Explanation:

Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

QUESTION 61

Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

- A. SSL
- B. TLS
- C. HTTP
- D. FTP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

QUESTION 62

A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

- A. WPA
- B. HTTPS
- C. WEP
- D. WPA 2

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 582
CompTIA SY0-401 Exam

Explanation:

Wi-Fi Protected Access 2 (WPA2) was intended to provide security that's equivalent to that on a wired network, and it implements elements of the 802.11i standard. In April 2010, the Wi-Fi Alliance announced the inclusion of additional Extensible Authentication Protocol (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. EAP-TLS is included in this certification program.

Note: Although WPA mandates the use of TKIP, WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of a replay attack.

QUESTION 63

Which of the following protocols encapsulates an IP packet with an additional IP header?

- A. SFTP
- B. IPSec
- C. HTTPS
- D. SSL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Authentication Header (AH) is a member of the IPsec protocol suite. AH operates directly on top of IP, using IP protocol number 51.

QUESTION 64

A new MPLS network link has been established between a company and its business partner.

The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

- A. MPLS should be run in IPVPN mode.
- B. SSL/TLS for all application flows.
- C. IPSec VPN tunnels on top of the MPLS link.
- D. HTTPS and SSH for all application flows.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 583
CompTIA SY0-401 Exam

Explanation:

IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top of the MPLS link. Internet Protocol Security (IPSec) isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security.

QUESTION 65

Which of the following would be used as a secure substitute for Telnet?

- A. SSH
- B. SFTP
- C. SSL
- D. HTTPS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also

provides alternative, security- equivalent programs for such Unix standards as Telnet, FTP, and many other communications- oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

QUESTION 66

Which of the following protocols provides transport security for virtual terminal emulation?

- A. TLS
- B. SSH
- C. SCP
- D. S/MIME

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security- equivalent programs for such Unix standards as Telnet, FTP, and many other communications-

"Pass Any Exam. Any Time." - www.actualtests.com 584
CompTIA SY0-401 Exam

oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

QUESTION 67

A security engineer is asked by the company's development team to recommend the most secure method for password storage.

Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO).

- A. PBKDF2
- B. MD5
- C. SHA2
- D. Bcrypt
- E. AES
- F. CHAP

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A: PBKDF2 (Password-Based Key Derivation Function 2) is part of PKCS #5 v. 2.01. It applies some function (like a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.

D: bcrypt is a key derivation function for passwords based on the Blowfish cipher. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power. The bcrypt function is the default password hash algorithm for BSD and many other systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 109-110, 139, 143, 250, 255-256, 256

QUESTION 68

Deploying a wildcard certificate is one strategy to:

"Pass Any Exam. Any Time." - www.actualtests.com 585
CompTIA SY0-401 Exam

- A. Secure the certificate's private key.
- B. Increase the certificate's encryption key length.
- C. Extend the renewal date of the certificate.
- D. Reduce the certificate management burden.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. This saves money and reduces the management burden of managing multiple certificates, one for each subdomain.

A single Wildcard certificate for *.example.com, will secure all these domains:

payment.example.com

contact.example.com

login-secure.example.com

www.example.com

Because the wildcard only covers one level of subdomains (the asterisk doesn't match full stops), these domains would not be valid for the certificate:
test.login.example.com

QUESTION 69

A certificate authority takes which of the following actions in PKI?

- A. Signs and verifies all infrastructure messages
- B. Issues and signs all private keys
- C. Publishes key escrow lists to CRLs
- D. Issues and signs all root certificates

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is part of a public key infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).

Note: In cryptography and computer security, a root certificate is an unsigned public key certificate (also called self-signed certificate) that identifies the Root Certificate Authority (CA).

"Pass Any Exam. Any Time." - www.actualtests.com 586
CompTIA SY0-401 Exam

QUESTION 70

Which of the following is used to certify intermediate authorities in a large PKI deployment?

- A. Root CA
- B. Recovery agent
- C. Root user
- D. Key escrow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The root CA certifies other certification authorities to publish and manage certificates within the organization.

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree. .

QUESTION 71

Which of the following components **MUST** be trusted by all parties in PKI?

- A. Key escrow
- B. CA
- C. Private key
- D. Recovery key

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. In a simple trust model all parties must trust the CA. In a more complicated trust model all parties must trust the Root CA.

QUESTION 72

Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login.

Which of the following is MOST likely the issue?

"Pass Any Exam. Any Time." - www.actualtests.com 587
CompTIA SY0-401 Exam

- A. The IP addresses of the clients have change
- B. The client certificate passwords have expired on the server
- C. The certificates have not been installed on the workstations
- D. The certificates have been installed on the CA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The computer certificates must be installed on the upgraded client computers.

QUESTION 73

A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

- A. Install a registration server.
- B. Generate shared public and private keys.
- C. Install a CA
- D. Establish a key escrow policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA.

QUESTION 74

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

- A. Certification authority
- B. Key escrow
- C. Certificate revocation list
- D. Registration authority

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates.

"Pass Any Exam. Any Time." - www.actualtests.com 588
CompTIA SY0-401 Exam

QUESTION 75

When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

- A. Trust models
- B. CRL
- C. CA
- D. Recovery agent

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. The CA affirms the identity of the certificate owner.

QUESTION 76

Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?

- A. CSR
- B. OCSP
- C. CA
- D. CRL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

QUESTION 77

A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

- A. A CRL

"Pass Any Exam. Any Time." - www.actualtests.com 589
CompTIA SY0-401 Exam

- B. Make the RA available
- C. A verification authority
- D. A redundant CA

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. By checking the CRL you can check if a particular certificate has been revoked.

QUESTION 78

A CRL is comprised of.

- A. Malicious IP addresses.
- B. Trusted CA's.
- C. Untrusted private keys.
- D. Public keys.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked. The certificates for which a CRL should be maintained are often X.509/public key certificates, as this format is commonly used by PKI schemes.

QUESTION 79

Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

- A. Registration
- B. CA
- C. CRL

D. Recovery agent

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Certificates or keys for the terminated employee should be put in the CRL.

"Pass Any Exam. Any Time." - www.actualtests.com 590

CompTIA SY0-401 Exam

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

QUESTION 80

Which of the following provides a static record of all certificates that are no longer valid?

- A. Private key
- B. Recovery agent
- C. CRLs
- D. CA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

QUESTION 81

A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

- A. Key escrow

- B. Private key verification
- C. Public key verification
- D. Certificate revocation list

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If we put the root certificate of the comprised CA in the CRL, users will know that this CA (and the certificates that it has issued) no longer can be trusted. The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In

"Pass Any Exam. Any Time." - www.actualtests.com 591
CompTIA SY0-401 Exam

addition, each list contains a proposed date for the next release.

QUESTION 82

The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

- A. Bank's CRL
- B. Bank's private key
- C. Bank's key escrow
- D. Bank's recovery agent

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The finance department can check if any of the bank's certificates are in the CRL or not. If a certificate is not in the CRL then it is still valid.

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

QUESTION 83

A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

- A. OCSP
- B. PKI
- C. CA
- D. CRL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A CRL is a locally stored record containing revoked certificates and revoked keys.

"Pass Any Exam. Any Time." - www.actualtests.com 592

CompTIA SY0-401 Exam

QUESTION 84

Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

- A. PKI
- B. ACL
- C. CA
- D. CRL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A CRL is a locally stored record containing revoked certificates and revoked keys.

QUESTION 85

Which of the following identifies certificates that have been compromised or suspected of being compromised?

- A. Certificate revocation list

- B. Access control list
- C. Key escrow registry
- D. Certificate authority

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Certificates that have been compromised or are suspected of being compromised are revoked. A CRL is a locally stored record containing revoked certificates and revoked keys.

QUESTION 86

When employees that use certificates leave the company they should be added to which of the following?

- A. PKI
- B. CA
- C. CRL
- D. TKIP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 593
CompTIA SY0-401 Exam

Explanation:

The certificates of the leaving employees must be made unusable. This is done by revoking them.

The revoke certificates end up in the CRL.

Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

QUESTION 87

Which of the following should a security technician implement to identify untrusted certificates?

- A. CA

- B. PKI
- C. CRL
- D. Recovery agent

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Untrusted certificates and keys are revoked and put into the CRL. Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included.

QUESTION 88

Which of the following is true about the CRL?

- A. It should be kept public
- B. It signs other keys
- C. It must be kept secret
- D. It must be encrypted

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The CRL must be public so that it can be known which keys and certificates have been revoked. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for

"Pass Any Exam. Any Time." - www.actualtests.com 594
CompTIA SY0-401 Exam

certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.

QUESTION 89

A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

- A. Revoke the digital certificate
- B. Mark the key as private and import it
- C. Restore the certificate using a CRL
- D. Issue a new digital certificate
- E. Restore the certificate using a recovery agent

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The user's certificate must be revoked to ensure that the stolen computer cannot access resources the user has had access to.

To grant the user access to the resources he must be issued a new certificate.

QUESTION 90

Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?

- A. CRL
- B. PKI
- C. OCSP
- D. RA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. If it cannot process the request, it may return an error code.

"Pass Any Exam. Any Time." - www.actualtests.com 595

CompTIA SY0-401 Exam

QUESTION 91

An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?

- A. CSR
- B. Recovery agent
- C. Private key
- D. CRL

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

When you renew a certificate you send a CSR to the CA to get the certificate resigned.

QUESTION 92

An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

- A. Generate a new private key based on AES.
- B. Generate a new public key based on RSA.
- C. Generate a new public key based on AES.
- D. Generate a new private key based on RSA.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The private key is needed to produce, but it is not part of, the CSR. The private key is an RSA key. The private encryption key that will be used to protect sensitive information.

Note: A CSR or Certificate Signing request is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR.

"Pass Any Exam. Any Time." - www.actualtests.com 596

CompTIA SY0-401 Exam

QUESTION 93

In which of the following scenarios is PKI LEAST hardened?

- A. The CRL is posted to a publicly accessible location.
- B. The recorded time offsets are developed with symmetric keys.
- C. A malicious CA certificate is loaded on all the clients.
- D. All public keys are accessed by an unauthorized user.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A rogue Certification Authority (CA) certificate allows malicious users to impersonate any Web site on the Internet, including banking and e-commerce sites secured using the HTTPS protocol. A rogue CA certificate would be seen as trusted by Web browsers, and it is harmful because it can appear to be signed by one of the root CAs that browsers trust by default. A rogue Certification Authority (CA) certificate can be created using a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure Web sites.

QUESTION 94

Which of the following BEST describes part of the PKI process?

- A. User1 decrypts data with User2's private key
- B. User1 hashes data with User2's public key
- C. User1 hashes data with User2's private key
- D. User1 encrypts data with User2's public key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

Jordan uses his private key to decrypt the message.

QUESTION 95

A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

- A. Transport encryption
- B. IPsec
- C. Non-repudiation
- D. Public key infrastructure

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Public-Key Infrastructure (PKI) is intended to offer a means of providing security to messages and transactions on a grand scale. The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI. A PKI can be used to protect software.

QUESTION 96

Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?

- A. Unmatched key pairs
- B. Corrupt key escrow
- C. Weak public key
- D. Weak private key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The sender and receiver must have

a matching key in order for the receiver to decrypt the data.

QUESTION 97

"Pass Any Exam. Any Time." - www.actualtests.com 598

CompTIA SY0-401 Exam

In PKI, a key pair consists of: (Select TWO).

- A. A key ring
- B. A public key
- C. A private key
- D. Key escrow
- E. A passphrase

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The key pair consists of these two keys.

QUESTION 98

Which of the following is true about PKI? (Select TWO).

- A. When encrypting a message with the public key, only the public key can decrypt it.
- B. When encrypting a message with the private key, only the private key can decrypt it.
- C. When encrypting a message with the public key, only the CA can decrypt it.
- D. When encrypting a message with the public key, only the private key can decrypt it.
- E. When encrypting a message with the private key, only the public key can decrypt it.

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of

which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

D: In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

"Pass Any Exam. Any Time." - www.actualtests.com 599

CompTIA SY0-401 Exam

Jordan uses his private key to decrypt the message.

QUESTION 99

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

- A. Recovery agent
- B. Certificate authority
- C. Trust model
- D. Key escrow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

QUESTION 100

Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

- A. Private hash
- B. Recovery agent
- C. Public key

- D. Key escrow
- E. CRL

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

"Pass Any Exam. Any Time." - www.actualtests.com 600
CompTIA SY0-401 Exam

D: If a key need to be recovered for legal purposes the key escrow can be used. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

QUESTION 101

After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

- A. Recovery agent
- B. Private key
- C. Trust models
- D. Public key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To access the data the hard drive need to be decrypted. To decrypt the hard drive you would need the proper private key. The key recovery agent can retrieve the required key. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

QUESTION 102

Which of the following is true about the recovery agent?

- A. It can decrypt messages of users who lost their private key.
- B. It can recover both the private and public key of federated users.
- C. It can recover and provide users with their lost or private key.
- D. It can recover and provide users with their lost public key.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted

"Pass Any Exam. Any Time." - www.actualtests.com 601
CompTIA SY0-401 Exam

data.

QUESTION 103

The recovery agent is used to recover the:

- A. Root certificate
- B. Key in escrow
- C. Public key
- D. Private key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted data.

QUESTION 104

Which of the following is synonymous with a server's certificate?

- A. Public key
- B. CRL
- C. Private key
- D. Recovery agent

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key.

QUESTION 105

The security administrator installed a newly generated SSL certificate onto the company web server. Due to a misconfiguration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

"Pass Any Exam. Any Time." - www.actualtests.com 602
CompTIA SY0-401 Exam

- A. The file containing the recovery agent's keys.
- B. The file containing the public key.
- C. The file containing the private key.
- D. The file containing the server's encrypted passwords.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The public key can be made available to everyone. There is no need to reissue the certificate.

QUESTION 106

The public key is used to perform which of the following? (Select THREE).

- A. Validate the CRL
- B. Validate the identity of an email sender
- C. Encrypt messages
- D. Perform key recovery
- E. Decrypt messages
- F. Perform key escrow

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

B: The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

C: The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message.

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

QUESTION 107

Public keys are used for which of the following?

"Pass Any Exam. Any Time." - www.actualtests.com 603
CompTIA SY0-401 Exam

- A. Decrypting wireless messages
- B. Decrypting the hash of an electronic signature
- C. Bulk encryption of IP based email traffic
- D. Encrypting web browser traffic

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the

receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

QUESTION 108

Which of the following explains the difference between a public key and a private key?

- A. The public key is only used by the client while the private key is available to all.
Both keys are mathematically related.
- B. The private key only decrypts the data while the public key only encrypts the data.
Both keys are mathematically related.
- C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
- D. The private key is only used by the client and kept secret while the public key is available to all.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The private key must be kept secret at all time. The private key is only by the client.
The public key is available to anybody.

QUESTION 109

Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?

- A. Joe's public key
- B. Joe's private key
- C. Ann's public key
- D. Ann's private key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 604
CompTIA SY0-401 Exam

Explanation:

The sender uses his private key, in this case Ann's private key, to create a digital signature. The message is, in effect, signed with the private key. The sender then

sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. The receiver uses a key provided by the sender--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

QUESTION 110

Which of the following devices is BEST suited for servers that need to store private keys?

- A. Hardware security module
- B. Hardened network firewall
- C. Solid state disk drive
- D. Hardened host firewall

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. By adding a HSM to the server and storing the private keys on HSM, the security of the keys would be improved.

QUESTION 111

Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?

- A. Registration
- B. Public key
- C. CRLs
- D. Private key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

"Pass Any Exam. Any Time." - www.actualtests.com 605
CompTIA SY0-401 Exam

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

Jordan uses his private key to decrypt the message.

QUESTION 112

Which of the following is true about an email that was signed by User A and sent to User B?

- A. User A signed with User B's private key and User B verified with their own public key.
- B. User A signed with their own private key and User B verified with User A's public key.
- C. User A signed with User B's public key and User B verified with their own private key.
- D. User A signed with their own public key and User B verified with User A's private key.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The sender uses his private key, in this case User A's private key, to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver (User B) uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. The receiver uses a key provided by the sender--the public key--to decrypt the message.

QUESTION 113

Which of the following must be kept secret for a public key infrastructure to remain secure?

- A. Certificate Authority
- B. Certificate revocation list
- C. Public key ring
- D. Private key

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The private key, which is also called the secret key, must be kept secret.

"Pass Any Exam. Any Time." - www.actualtests.com 606

CompTIA SY0-401 Exam

QUESTION 114

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

- A. Trust model
- B. Public Key Infrastructure
- C. Private key
- D. Key escrow

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Sensitive PKI data, such as private keys, can be put into key escrow data. The key escrow data can be kept at a trusted third party.

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

QUESTION 115

Which of the following is a requirement when implementing PKI if data loss is unacceptable?

- A. Web of trust
- B. Non-repudiation
- C. Key escrow
- D. Certificate revocation list

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Key escrow is a database of stored keys that later can be retrieved. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

"Pass Any Exam. Any Time." - www.actualtests.com 607
CompTIA SY0-401 Exam

QUESTION 116

Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

- A. Trust Model
- B. Recovery Agent
- C. Public Key
- D. Private Key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In a bridge trust model allows lower level domains to access resources in a separate PKI through the root CA.

A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

In a bridge trust model, a peer-to-peer relationship exists among the root CAs. The root CAs can communicate with one another, allowing cross certification. This arrangement allows a certification process to be established between organizations or departments. Each intermediate CA trusts only the CAs above and below it, but the CA structure can be expanded without creating additional layers of CAs.

QUESTION 117

A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

- A. Trust model
- B. Key escrow
- C. OCSP
- D. PKI

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this scenario we can put a CA in the local network and use an online CA as root CA in a hierarchical trust model.

A trust Model is collection of rules that informs application on how to decide the legitimacy of a

"Pass Any Exam. Any Time." - www.actualtests.com 608

CompTIA SY0-401 Exam

Digital Certificate.

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree.

QUESTION 118

In order to use a two-way trust model the security administrator MUST implement which of the following?

- A. DAC
- B. PKI
- C. HTTPS
- D. TPM

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PKI is a high level concept. Within a PKI you use a trust model to set up trust between Certification Authorities (CAs).

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

QUESTION 119

Which of the following types of trust models is used by a PKI?

- A. Transitive
- B. Open source
- C. Decentralized
- D. Centralized

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

PKI uses a centralized trust model. In a simple PKI a single centralized certification authority (CA). In a hierarchical trust model the root CA is the center of the model, with subordinate CAs lower in the hierarchy.

Note: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and

"Pass Any Exam. Any Time." - www.actualtests.com 609

CompTIA SY0-401 Exam

procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

QUESTION 120

RC4 is a strong encryption protocol that is generally used with which of the following?

- A. WPA2 CCMP
- B. PEAP
- C. WEP
- D. EAP-TLS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Rivest Cipher 4 (RC4) is a 128-bit stream cipher used WEP and WPA encryption.

QUESTION 121

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel.

Which of the following MUST be implemented?



<http://www.gratisexam.com/>

- A. SHA-256
- B. AES
- C. Diffie-Hellman
- D. 3DES

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Diffie-Hellman key exchange (D-H) is a means of securely generating symmetric encryption keys across an insecure medium.

QUESTION 122

A security administrator at a company which implements key escrow and symmetric encryption only, needs to decrypt an employee's file. The employee refuses to provide the decryption key to the file. Which of the following can the administrator do to decrypt the file?

"Pass Any Exam. Any Time." - www.actualtests.com 610
CompTIA SY0-401 Exam

- A. Use the employee's private key
- B. Use the CA private key
- C. Retrieve the encryption key
- D. Use the recovery agent

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

<http://www.gratisexam.com/>

Explanation:

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

QUESTION 123

A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?

- A. AES
- B. IPSec
- C. PGP
- D. SSH

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

With SSH you can use automatically generated public-private key pairs to encrypt a network connection, and then use password authentication to log on. Or you can use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password.

QUESTION 124

Joe, a user, wants to protect sensitive information stored on his hard drive. He uses a program that encrypted the whole hard drive. Once the hard drive is fully encrypted, he uses the same program to create a hidden volume within the encrypted hard drive and stores the sensitive information within the hidden volume. This is an example of which of the following? (Select TWO).

- A. Multi-pass encryption
- B. Transport encryption
"Pass Any Exam. Any Time." - www.actualtests.com 611
CompTIA SY0-401 Exam
- C. Plausible deniability
- D. Steganography
- E. Transitive encryption
- F. Trust models

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. In this case, it is a hidden volume within the encrypted hard drive. In cryptography, deniable encryption may be used to describe steganographic techniques, where the very existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that an encrypted message exists. This then provides you with plausible deniability.

QUESTION 125

A company is concerned that a compromised certificate may result in a man-in-the-middle attack against backend financial servers. In order to minimize the amount of time a compromised certificate would be accepted by other servers, the company decides to add another validation step to SSL/TLS connections. Which of the following technologies provides the FASTEST revocation capability?

- A. Online Certificate Status Protocol (OCSP)
- B. Public Key Cryptography (PKI)
- C. Certificate Revocation Lists (CRL)
- D. Intermediate Certificate Authority (CA)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

CRL (Certificate Revocation List) was first released to allow the CA to revoke certificates, however due to limitations with this method it was succeeded by OSCP. The main advantage to OCSP is that because the client is allowed query the status of a single certificate, instead of having to download and parse an entire list there is much less overhead on the client and network.

QUESTION 126

A technician wants to verify the authenticity of the system files of a potentially compromised system. Which of the following can the technician use to verify if a system file was compromised? (Select TWO).

- A. AES
"Pass Any Exam. Any Time." - www.actualtests.com 612
CompTIA SY0-401 Exam
- B. PGP
- C. SHA
- D. MD5
- E. ECDHE

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Hashing is used to prove the integrity of data to prove that it hasn't been modified. Hashing algorithms are used to derive a key mathematically from a message. The most common hashing standards for cryptographic applications are the SHA and MD algorithms.

QUESTION 127

When confidentiality is the primary concern, and a secure channel for key exchange is not available, which of the following should be used for transmitting company documents?

- A. Digital Signature
- B. Symmetric
- C. Asymmetric
- D. Hashing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. Asymmetric algorithms do not require a secure channel for the initial exchange of secret keys between the parties.

QUESTION 128

A small company wants to employ PKI. The company wants a cost effective solution that must be simple and trusted. They are considering two options: X.509 and PGP. Which of the following would be the BEST option?

- A. PGP, because it employs a web-of-trust that is the most trusted form of PKI.
- B. PGP, because it is simple to incorporate into a small environment.
- C. X.509, because it uses a hierarchical design that is the most trusted form of PKI.
- D. X.509, because it is simple to incorporate into a small environment.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 613
CompTIA SY0-401 Exam

PGP easier to use and setup than the corporate PKI model, but it is also less robust when it comes to issues like authentication and trust. However, the full benefits of public key cryptography are used.

QUESTION 129

Which of the following represents a cryptographic solution where the encrypted stream cannot be captured by a sniffer without the integrity of the stream being compromised?

- A. Elliptic curve cryptography.
- B. Perfect forward secrecy.
- C. Steganography.
- D. Quantum cryptography.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Quantum cryptography is a cryptosystem that is completely secure against being compromised without knowledge of the sender or the receiver of the messages.

QUESTION 130

A new client application developer wants to ensure that the encrypted passwords that are stored in their database are secure from cracking attempts. To implement this, the developer implements a function on the client application that hashes passwords thousands of times prior to being sent to the database. Which of the following did the developer MOST likely implement?

- A. RIPEMD
- B. PBKDF2
- C. HMAC
- D. ECDHE

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Password-Based Key Derivation Function 2 (PBKDF2) makes use of a hashing operation, an encryption cipher function, or an HMAC operation) on the input password, which is combined with a salt and is repeated thousands of times.

"Pass Any Exam. Any Time." - www.actualtests.com 614
CompTIA SY0-401 Exam

QUESTION 131

Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?

- A. A pre-shared private key
- B. His private key
- C. Ann's public key
- D. His public key

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To achieve both authentication and confidentiality, Joe should include Ann's name in the message, sign it using his private key, and then encrypt both the message and the signature using Ann's public key.

QUESTION 132

A system administrator wants to confidentially send a user name and password list to an individual outside the company without the information being detected by security controls. Which of the following would BEST meet this security goal?

- A. Digital signatures
- B. Hashing
- C. Full-disk encryption
- D. Steganography

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal.

Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION 133

"Pass Any Exam. Any Time." - www.actualtests.com 615

CompTIA SY0-401 Exam

Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?

- A. Sender's private key
- B. Recipient's public key
- C. Sender's public key
- D. Recipient's private key

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To achieve both authentication and confidentiality, the sender should include the recipient's name in the message, sign it using his private key, and then encrypt both the message and the signature using the recipient's public key.

Topic 7, Mixed Questions

QUESTION 134

A software developer utilizes cryptographic functions to generate codes that verify message integrity. Due to the nature of the data that is being sent back and forth from the client application to the server, the developer would like to change the cryptographic function to one that verifies both authentication and message integrity. Which of the following algorithms should the software developer utilize?

- A. HMAC
- B. SHA
- C. Two Fish
- D. RIPEMD

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 135

When designing a corporate NAC solution, which of the following is the MOST relevant integration issue?

- A. Infrastructure time sync
"Pass Any Exam. Any Time." - www.actualtests.com 616
CompTIA SY0-401 Exam
- B. End user mobility
- C. 802.1X supplicant compatibility
- D. Network Latency
- E. Network Zoning

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 136

Which of the following access methods uses radio frequency waves for authentication?

- A. Video surveillance
- B. Mantraps
- C. Proximity readers
- D. Biometrics

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 137

Which of the following authentication methods can use the SCTP and TLS protocols for reliable packet transmissions?

- A. TACACS+
- B. SAML
- C. Diameter
- D. Kerberos

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 138

Which of the following authentication protocols makes use of UDP for its services?

- A. RADIUS
"Pass Any Exam. Any Time." - www.actualtests.com 617
CompTIA SY0-401 Exam
- B. TACACS+
- C. LDAP
- D. XTACACS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 139

Which of the following is considered a risk management BEST practice of succession planning?

- A. Reducing risk of critical information being known to an individual person who may leave the organization
- B. Implementing company-wide disaster recovery and business continuity plans
- C. Providing career advancement opportunities to junior staff which reduces the possibility of insider threats
- D. Considering departmental risk management practices in place of company-wide practices

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 140

Which of the following is the BEST technology for the sender to use in order to secure the in-band exchange of a shared key?

- A. Steganography
- B. Hashing algorithm
- C. Asymmetric cryptography
- D. Steam cipher

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 141

Which of the following design components is used to isolate network devices such as web servers?

"Pass Any Exam. Any Time." - www.actualtests.com 618
CompTIA SY0-401 Exam

- A. VLAN
- B. VPN
- C. NAT
- D. DMZ

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 142

Which of the following is MOST critical in protecting control systems that cannot be regularly patched?

- A. Asset inventory
- B. Full disk encryption
- C. Vulnerability scanning
- D. Network segmentation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 143

Identifying residual is MOST important to which of the following concepts?

- A. Risk deterrence
- B. Risk acceptance
- C. Risk mitigation
- D. Risk avoidance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 144

Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?

"Pass Any Exam. Any Time." - www.actualtests.com 619
CompTIA SY0-401 Exam

- A. Preshared keys
- B. Ticket exchange

- C. Initialization vectors
- D. Certificate exchange

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 145

Which of the following steps of incident response does a team analyze the incident and determine steps to prevent a future occurrence?

- A. Mitigation
- B. Identification
- C. Preparation
- D. Lessons learned

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 146

A technician wants to secure communication to the corporate web portal, which is currently using HTTP. Which of the following is the FIRST step the technician should take?

- A. Send the server's public key to the CA
- B. Install the CA certificate on the server
- C. Import the certificate revocation list into the server
- D. Generate a certificate request from the server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 147

An organization has a need for security control that identifies when an organizational system has been unplugged and a rouge system has been plugged in. The security control must also provide the ability to supply automated notifications. Which of the following would allow the organization to

"Pass Any Exam. Any Time." - www.actualtests.com 620

CompTIA SY0-401 Exam

BEST meet this business requirement?

- A. MAC filtering
- B. ACL
- C. SNMP
- D. Port security

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 148

Internet banking customers currently use an account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?

- A. Something you know, something you do, and something you have
- B. Something you do, somewhere you are, and something you have
- C. Something you are, something you do and something you know
- D. Something you have, something you are, and something you know

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 149

A security administrator has concerns that employees are installing unapproved applications on their company provide smartphones. Which of the following would BEST mitigate this?

- A. Implement remote wiping user acceptance policies
- B. Disable removable storage capabilities
- C. Implement an application whitelist
- D. Disable the built-in web browsers

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 621
CompTIA SY0-401 Exam

QUESTION 150

The security manager must store a copy of a sensitive document and needs to verify at a later point that the document has not been altered. Which of the following will accomplish the security manager's objective?

- A. RSA
- B. AES
- C. MD5
- D. SHA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 151

A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

- A. Escalation

- B. Identification
- C. Notification
- D. Quarantine
- E. Preparation

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 152

A security administrator wants to block unauthorized access to a web server using a locally installed software program. Which of the following should the administrator deploy?

- A. NIDS
- B. HIPS
- C. NIPS
- D. HIDS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 622

CompTIA SY0-401 Exam

Explanation:

QUESTION 153

A network administrator has identified port 21 being open and the lack of an IDS as a potential risk to the company. Due to budget constraints, FTP is the only option that the company can use to transfer data and network equipment cannot be purchased. Which of the following is this known as?

- A. Risk transference
- B. Risk deterrence
- C. Risk acceptance
- D. Risk avoidance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 154

A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?

- A. Application log
- B. Setup log
- C. Authentication log
- D. System log

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 155

A user attempts to install new and relatively unknown software recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

"Pass Any Exam. Any Time." - www.actualtests.com 623
CompTIA SY0-401 Exam

- A. Application black listing
- B. Network Intrusion Prevention System
- C. Group policy
- D. Application white listing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 156

A system administrator is configuring shared secrets on servers and clients. Which of the following authentication services is being deployed by the administrator? (Select two.)

- A. Kerberos
- B. RADIUS
- C. TACACS+
- D. LDAP
- E. Secure LDAP

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 157

The finance department just procured a software application that needs to communicate back to the vendor server via SSL. Which of the following default ports on the firewall must the security engineer open to accomplish this task?

- A. 80
- B. 130
- C. 443
- D. 3389

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 158

After an audit, it was discovered that an account was not disabled in a timely manner after an

"Pass Any Exam. Any Time." - www.actualtests.com 624

CompTIA SY0-401 Exam

employee has departed from the organization. Which of the following did the organization fail to properly implement?

- A. Routine account audits
- B. Account management processes
- C. Change management processes
- D. User rights and permission reviews

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 159

The Chief Security Officer (CSO) for a datacenter in a hostile environment is concerned about protecting the facility from car bomb attacks. Which of the following BEST would protect the building from this threat? (Select two.)

- A. Dogs
- B. Fencing
- C. CCTV
- D. Guards
- E. Bollards
- F. Lighting

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 160

Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

- A. Malicious users can exploit local corporate credentials with their social media credentials
- B. Changes to passwords on the social media site can be delayed from replicating to the company
- C. Data loss from the corporate servers can create legal liabilities with the social media site
- D. Password breaches to the social media affect the company application as well

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 625
CompTIA SY0-401 Exam

QUESTION 161

A corporation has experienced several media leaks of proprietary data on various web forums. The posts were made during business hours and it is believed that the culprit is posting during work hours from a corporate machine. The Chief Information Officer (CIO) wants to scan internet traffic and keep records for later use in legal proceedings once the culprit is found. Which of the following provides the BEST solution?

- A. Protocol analyzer
- B. NIPS
- C. Proxy server
- D. HIDS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 162

The security administrator runs an rpm verify command which records the MD5 sum, permissions, and timestamp of each file on the system. The administrator saves this information to a separate server. Which of the following describes the procedure the administrator has performed?

- A. Host software base-lining
- B. File snapshot collection
- C. TPM

D. ROMDB verification

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 163

Users are trying to communicate with a network but are unable to do so. A network administrator sees connection attempts on port 20 from outside IP addresses that are being blocked. How can the administrator resolve this?

- A. Enable stateful FTP on the firewall
- B. Enable inbound SSH connections
"Pass Any Exam. Any Time." - www.actualtests.com 626
CompTIA SY0-401 Exam
- C. Enable NETBIOS connections in the firewall
- D. Enable HTTPS on port 20

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 164

In order to enter a high-security datacenter, users are required to speak the password into a voice recognition system. Ann a member of the sales department over hears the password and upon speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

- A. An authentication factor
- B. Discretionary access
- C. Time of day restrictions
- D. Least privilege restrictions

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 165

Given the following list of corporate access points, which of the following attacks is MOST likely underway if the company wireless network uses the same wireless hardware throughout?

MACSID

00:01:AB:FA:CD:34Corporate AP

00:01:AB:FA:CD:35Corporate AP

00:01:AB:FA:CD:36Corporate AP

00:01:AB:FA:CD:37Corporate AP

00:01:AB:FA:CD:34Corporate AP

- A. Packet sniffing
 - B. Evil Twin
 - C. WPS attack
 - D. Rogue access point
- "Pass Any Exam. Any Time." - www.actualtests.com 627
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 166

A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?

- A. SMTP

- B. iSCSI
- C. SNMP
- D. IPSec

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 167

Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?

- A. RAID
- B. Tape Backup
- C. Load Balancing
- D. Clustering

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 168

An employee needs to connect to a server using a secure protocol on the default port. Which of the following ports should be used?

- A. 21
- B. 22
- C. 80
- D. 110

"Pass Any Exam. Any Time." - www.actualtests.com 628
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 169

Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?

- A. Preshared keys
- B. Ticket exchange
- C. Initialization vectors
- D. Certificate exchange

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 170

A new security policy being implemented requires all email within the organization be digitally signed by the author using PGP. Which of the following would need to be created for each user?

- A. A certificate authority
- B. A key escrow
- C. A trusted key
- D. A public and private key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 171

Which of the following authentication provides users XML for authorization and authentication?

- A. Kerberos
- B. LDAP
- C. RADIUS
- D. SAML

"Pass Any Exam. Any Time." - www.actualtests.com 629
CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 172

A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?

- A. MDM
- B. IDS
- C. DLP
- D. HIPS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 173

The ore-sales engineering team needs to quickly provide accurate and up-to-date information to potential clients. This information includes design specifications and engineering data that is developed and stored using numerous applications across the enterprise. Which of the following authentication technique is MOST appropriate?

- A. Common access cards
- B. TOTP
- C. Single sign-on
- D. HOTP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 174

A network engineer is configuring a VPN tunnel connecting a company's network to a business partner. Which of the following protocols should be used for key exchange?

A. SHA-1

B. RC4

"Pass Any Exam. Any Time." - www.actualtests.com 630
CompTIA SY0-401 Exam

C. Blowfish

D. Diffie-Hellman

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 175

Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?

A. Hybrid Cloud

B. Private cloud

C. Community cloud

D. Community cloud

E. Public cloud

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 176

The database server used by the payroll system crashed at 3 PM and payroll is due at 5 PM. Which of the following metrics is MOST important in this instance?

- A. ARO
- B. SLE
- C. MTTR
- D. MTBF

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 177

Which of the following is an attack designed to activate based on time?

- A. Logic Bomb
"Pass Any Exam. Any Time." - www.actualtests.com 631
CompTIA SY0-401 Exam
- B. Backdoor
- C. Trojan
- D. Rootkit

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 178

A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?

- A. Disable unnecessary services on servers
- B. Disable unused accounts on servers and network devices
- C. Implement password requirements on servers and network devices
- D. Enable auditing on event logs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 179

Which of the following documents outlines the responsibility of both participants in an agreement between two organizations?

- A. RFC
- B. MOU
- C. RFQ
- D. SLA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 180

Users in the HR department were recently informed that they need to implement a user training and awareness program which is tailored to their department. Which of the following types of training would be the MOST appropriate for this department?

"Pass Any Exam. Any Time." - www.actualtests.com 632
CompTIA SY0-401 Exam

- A. Handling PII
- B. Risk mitigation
- C. Input validation
- D. Hashing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 181

Which of the following incident response plan steps would MOST likely engaging business professionals with the security team to discuss changes to existing procedures?

- A. Recovery
- B. Incident identification
- C. Isolation / quarantine
- D. Lessons learned
- E. Reporting

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 182

A company is starting to allow employees to use their own personal without centralized management. Employees must contract IT to have their devices configured to use corporate email; access is also available to the corporate cloud-based services. Which of the following is the BEST policy to implement under these circumstances?

- A. Acceptable use policy
- B. Security policy
- C. Group policy
- D. Business Agreement policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 183

"Pass Any Exam. Any Time." - www.actualtests.com 633

CompTIA SY0-401 Exam

Which of the following BEST explains Platform as a Service?

- A. An external entity that provides a physical or virtual instance of an installed operating system
- B. A third party vendor supplying support services to maintain physical platforms and servers
- C. An external group providing operating systems installed on virtual servers with web applications
- D. An internal group providing physical server instances without installed operating systems or support

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 184

One of the senior managers at a company called the help desk to report a problem. The manager could no longer access data on a laptop equipped with FDE. The manager requested that the FDE be removed and the laptop restored from a backup. The help desk informed the manager that the recommended solution was to decrypt the hard drive prior to reinstallation and recovery. The senior manager did not have a copy of the private key associated with the FDE on the laptop. Which of the following tools or techniques did the help desk use to avoid losing the data on the laptop?

- A. Public key
- B. Recovery agent
- C. Registration details
- D. Trust Model

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 185

An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was not received by the end of the business day. The employee clicked on the link and the machine was infected with

malware. Which of the following principles BEST describes why this social engineering ploy was successful?

- A. Scarcity
- B. Familiarity
- C. Social proof
"Pass Any Exam. Any Time." - www.actualtests.com 634
CompTIA SY0-401 Exam
- D. Urgency

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 186

A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?

- A. Create a separate printer network
- B. Perform penetration testing to rule out false positives
- C. Install patches on the print server
- D. Run a full vulnerability scan of all the printers

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 187

A systems administrator has made several unauthorized changes to the server cluster that resulted in a major outage. This event has been brought to the attention of the Chief Information Office (CIO) and he has requested immediately implement a risk mitigation strategy to prevent this type of event from reoccurring. Which of the following would be the BEST risk mitigation strategy to implement in order to meet this request?

- A. Asset Management

- B. Change Management
- C. Configuration Management
- D. Incident Management

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 188

"Pass Any Exam. Any Time." - www.actualtests.com 635

CompTIA SY0-401 Exam

An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?

- A. Password history
- B. Password complexity
- C. Account lockout
- D. Account expiration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 189

Joe needs to track employees who log into a confidential database and edit files. In the past, critical files have been edited, and no one admits to making the edits. Which of the following does Joe need to implement in order to enforce accountability?



<http://www.gratisexam.com/>

- A. Non-repudiation
- B. Fault tolerance
- C. Hashing
- D. Redundancy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 190

A new mobile banking application is being developed and uses SSL / TLS certificates but penetration tests show that it is still vulnerable to man-in-the-middle attacks, such as DNS hijacking. Which of the following would mitigate this attack?

- A. Certificate revocation
- B. Key escrow
- C. Public key infrastructure
- D. Certificate pinning

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 636
CompTIA SY0-401 Exam

<http://www.gratisexam.com/>

QUESTION 191

One month after a software developer was terminated the helpdesk started receiving calls that several employees' computers were being infected with malware. Upon further research, it was determined that these employees had downloaded a shopping toolbar. It was this toolbar that downloaded and installed the errant code. Which of the following attacks has taken place?

- A. Logic bomb
- B. Cross-site scripting
- C. SQL injection
- D. Malicious add-on

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 192

Which of the following would an attacker use to penetrate and capture additional traffic prior to performing an IV attack?

- A. DNS poisoning
- B. DDoS
- C. Replay attack
- D. Dictionary attacks

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 193

An administrator has concerns regarding the company's server rooms Proximity badge readers were installed, but it is discovered this is not preventing unapproved personnel from tailgating into these area. Which of the following would BEST address this concern?

- A. Replace proximity readers with turn0based key locks
- B. Install man-traps at each restricted area entrance

- C. Configure alarms to alert security when the areas are accessed "Pass Any Exam. Any Time." - www.actualtests.com 637
CompTIA SY0-401 Exam
- D. Install monitoring cameras at each entrance

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 194

Which of the following would be a reason for developers to utilize an AES cipher in CCM mode (Counter with Chain Block Message Authentication Code)?

- A. It enables the ability to reverse the encryption with a separate key
- B. It allows for one time pad inclusions with the passphrase
- C. Counter mode alternates between synchronous and asynchronous encryption
- D. It allows a block cipher to function as a stream cipher

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 195

One of the findings of risk assessment is that many of the servers on the data center subnet contain data that is in scope for PCI compliance. Everyone in the company has access to these servers, regardless of their job function. Which of the following should the administrator do?

- A. Segment the network
- B. Use 802.1X
- C. Deploy a proxy sever
- D. Configure ACLs
- E. Write an acceptable use policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 196

Various employees have lost valuable customer data due to hard drives failing in company provided laptops. It has been discovered that the hard drives used in one model of laptops provided by the company has been recalled by the manufactory, The help desk is only able to replace the hard drives after they fail because there is no centralized records of the model of

"Pass Any Exam. Any Time." - www.actualtests.com 638

CompTIA SY0-401 Exam

laptop given to each specific user. Which of the following could have prevented this situation from occurring?

- A. Data backups
- B. Asset tracking
- C. Support ownership
- D. BYOD policies

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 197

Attempting to inject 50 alphanumeric key strokes including spaces into an application input field that only expects four alpha characters in considered which of the following attacks?

- A. XML injection
- B. Buffer overflow
- C. LDAP Injection
- D. SQL injection

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 198

An organization is required to log all user internet activity. Which of the following would accomplish this requirement?

- A. Configure an access list on the default gateway router. Configure the default gateway router to log all web traffic to a syslog server
- B. Configure a firewall on the internal network. On the client IP address configuration, use the IP address of the firewall as the default gateway, configure the firewall to log all traffic to a syslog server
- C. Configure a proxy server on the internal network and configure the proxy server to log all web traffic to a syslog server
- D. Configure an access list on the core switch, configure the core switch to log all web traffic to a syslog server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 639
CompTIA SY0-401 Exam

Explanation:

QUESTION 199

An agent wants to create fast and efficient cryptographic keys to use with Diffie-Hellman without using prime numbers to generate the keys. Which of the following should be used?

- A. Elliptic curve cryptography
- B. Quantum cryptography
- C. Public key cryptography
- D. Symmetric cryptography

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 200

Joe an application developer is building an external facing marketing site. There is an area on the page where clients may submit their feedback to articles that are posted. Joe filters client-side JAVA input. Which of the following is Joe attempting to prevent?

- A. SQL injections
- B. Watering holes
- C. Cross site scripting
- D. Pharming

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 201

A video surveillance audit recently uncovered that an employee plugged in a personal laptop and used the corporate network to browse inappropriate and potentially malicious websites after office hours. Which of the following could BEST prevent a situation like this from occurring again?

- A. Intrusion detection
 - B. Content filtering
 - C. Port security
 - D. Vulnerability scanning
- "Pass Any Exam. Any Time." - www.actualtests.com 640
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 202

A server administrator notes that a fully patched application often stops running due to a memory error. When reviewing the debugging logs they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describes?

- A. Malicious add-on
- B. SQL injection
- C. Cross site scripting
- D. Zero-day

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 203

A resent OS patch caused an extended outage. It took the IT department several hours to uncover the cause of the issue due to the system owner who installed the patch being out of the office. Which of the following could help reduce the likelihood of this situation occurring in the future?

- A. Separation of duties
- B. Change management procedures
- C. Incident management procedures
- D. User rights audits and reviews

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 204

The Chief Information Security Officer (CISO) is concerned that users could bring their personal laptops to work and plug them directly into the network port under their desk. Which of the following should be configured on the network switch to prevent this from happening?

"Pass Any Exam. Any Time." - www.actualtests.com 641

CompTIA SY0-401 Exam

- A. Access control lists
- B. Loop protection
- C. Firewall rule
- D. Port security

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 205

Ann a network administrator has been tasked with strengthening the authentication of users logging into systems in area containing sensitive information. Users log in with usernames and passwords, following by a retinal scan. Which of the following could she implement to add an additional factor of authorization?

- A. Requiring PII usage
- B. Fingerprint scanner
- C. Magnetic swipe cards
- D. Complex passphrases

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 206

In an environment where availability is critical such as Industrial control and SCADA networks, which of the following technologies in the MOST critical layer of defense for such systems?

- A. Log consolidation
- B. Intrusion Prevention system
- C. Automated patch deployment
- D. Antivirus software

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 207

A security manager installed a standalone fingerprint reader at the data center. All employees that

"Pass Any Exam. Any Time." - www.actualtests.com 642
CompTIA SY0-401 Exam

need to access the data center have been enrolled to the reader and local reader database is always kept updates. When an employee who has been enrolled uses the fingerprint reader the door to the data center opens. Which of the following does this demonstrate? (Select THREE)

- A. Two-factor authentication
- B. Single sign-on
- C. Something you have
- D. Identification
- E. Authentication
- F. Authorization

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 208

A network technician is configuring clients for VLAN access. The network address for the sales department is 192.168.0.64 with a broadcast address of 192.168.0.71. Which of the following IP address/subnet mask combinations could be used to correctly configure a client machine in the sales department?

- A. 192.168.0.64/29
- B. 192.168.0.66/27
- C. 192.168.0.67/29
- D. 192.168.0.70/28

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 209

The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due, in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?

- A. Load balancer

- B. Spam filter
- C. VPN Concentrator
- "Pass Any Exam. Any Time." - www.actualtests.com 643
CompTIA SY0-401 Exam
- D. NIDS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 210

Two organizations want to share sensitive data with one another from their IT systems to support a mutual customer base. Both organizations currently have secure network and security policies and procedures. Which of the following should be the PRIMARY security considerations by the security managers at each organization prior to sharing information? (Select THREE)

- A. Physical security controls
- B. Device encryption
- C. Outboarding/Offboarding
- D. Use of digital signatures
- E. SLA/ISA
- F. Data ownership
- G. Use of smartcards or common access cards
- H. Patch management

Correct Answer: BEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 211

A company's password and authentication policies prohibit the use of shared passwords and transitive trust. Which of the following if implemented would violate company policy? (Select TWO)

- A. Discretionary access control

- B. Federation
- C. Single sign-on
- D. TOTP
- E. Two-factor authentication

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 644
CompTIA SY0-401 Exam

QUESTION 212

Which of the following types of attacks is based on coordinating small slices of a task across multiple systems?

- A. DDos
- B. Spam
- C. Spoofing
- D. Dos

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 213

A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?

- A. Taking screenshots
- B. Analyzing Big Data metadata
- C. Analyzing network traffic and logs
- D. Capturing system image

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 214

The security manager reports that the process of revoking certificates authority is too slow and should be automated. Which of the following should be used to automate this process?

- A. CRL
- B. GPG
- C. OCSP
- D. Key escrow

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 645
CompTIA SY0-401 Exam

QUESTION 215

A user attempts to install a new and relatively unknown software program recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

- A. Application black listing
- B. Network Intrusion Prevention System
- C. Group Policy
- D. Application White Listing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 216

A company needs to provide web-based access to shared data sets to mobile users, while maintaining a standardized set of security controls. Which of the following technologies is the MOST appropriate storage?

- A. Encrypted external hard drives
- B. Cloud storage
- C. Encrypted mobile devices
- D. Storage Area Network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 217

An employee's mobile device associates with the company's guest WiFi SSID, but then is unable to retrieve email. The email settings appear to be correct. Which of the following is the MOST likely cause?

- A. The employee has set the network type to WPA instead of WPA2
- B. The network uses a captive portal and requires a web authentication
- C. The administrator has blocked the use of the personal hot spot feature
- D. The mobile device has been placed in airplane mode

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 646

CompTIA SY0-401 Exam

Explanation:

QUESTION 218

A malicious individual used an unattended customer service kiosk in a busy store to change the prices of several products. The alteration was not noticed until several days later and resulted in the loss of several thousand dollars for the store. Which of the following would BEST prevent this from occurring again?

- A. Password expiration
- B. Screen locks
- C. Inventory control
- D. Asset tracking

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 219

In order to enter a high-security data center, users are required to speak the correct password into a voice recognition system. Ann, a member of the sales department, overhears the password and later speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

- A. An authentication factor
- B. Discretionary Access
- C. Time of Day Restrictions
- D. Least Privilege Restrictions

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 220

A company requires that all users enroll in the corporate PKI structure and digitally sign all emails. Which of the following are primary reasons to sign emails with digital certificates? (Select TWO)

- A. To establish non-repudiation
"Pass Any Exam. Any Time." - www.actualtests.com 647
CompTIA SY0-401 Exam
- B. To ensure integrity
- C. To prevent SPAM
- D. To establish data loss prevention

- E. To protect confidentiality
- F. To establish transport encryption

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 221

The Chief Information Officer (CIO) has asked a security analyst to determine the estimated costs associated with each potential breach of their database that contains customer information. Which of the following is the risk calculation that the CIO is asking for?

- A. Impact
- B. SLE
- C. ARO
- D. ALE

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 222

A security assurance officer is preparing a plan to measure the technical state of a customer's enterprise. The testers employed to perform the audit will be given access to the customer facility and network. The testers will not be given access to the details of custom developed software used by the customer. However the testers will have access to the source code for several open source applications and pieces of networking equipment used at the facility, but these items will not be within the scope of the audit. Which of the following BEST describes the appropriate method of testing or technique to use in this scenario? (Select TWO)

- A. Social engineering
- B. All source
- C. Black box
- D. Memory dumping
- E. Penetration

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 648
CompTIA SY0-401 Exam

QUESTION 223

Which of the following authentication services combines authentication and authorization in a use profile and use UDP?

- A. LDAP
- B. Kerberos
- C. TACACS+
- D. RADIUS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 224

A security administrator is designing an access control system, with an unlimited budget, to allow authenticated users access to network resources. Given that a multifactor authentication solution is more secure, which of the following is the BEST combination of factors?

- A. Retina scanner, thumbprint scanner, and password
- B. Username and password combo, voice recognition scanner, and retina scanner
- C. Password, retina scanner, and proximity reader
- D. One-time password pad, palm-print scanner, and proximity photo badges

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 225

The access control list (ACL) for a file on a server is as follows:

User: rwx

User: Ann: r- -

User: Joe: r- -

Group: rwx

"Pass Any Exam. Any Time." - www.actualtests.com 649

CompTIA SY0-401 Exam

Group: sales: r-x

Other: r-x

Joe and Ann are members of the Human Resources group. Will Ann and Joe be able to run the file?

- A. No since Ann and Joe are members of the Sales group owner of the file
- B. Yes since the regular permissions override the ACL for the file
- C. No since the ACL overrides the regular permissions for the file
- D. Yes since the regular permissions and the ACL combine to create the effective permissions on the file

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 226

Using a protocol analyzer, a security consultant was able to capture employee's credentials. Which of the following should the consultant recommend to the company, in order to mitigate the risk of employees credentials being captured in the same manner in the future?

- A. Wiping of remnant data
- B. Hashing and encryption of data in-use
- C. Encryption of data in-transit
- D. Hashing of data at-rest

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 227

A Company has recently identified critical systems that support business operations. Which of the following will once defined, be the requirement for restoration of these systems within a certain period of time?

A. Mean Time Between Failure

B. Mean Time to Restore

C. Recovery Point Objective

D. Recovery Time Objective

"Pass Any Exam. Any Time." - www.actualtests.com 650

CompTIA SY0-401 Exam

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 228

The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the application servers. Which of the following practices are they following to ensure application integrity?

A. Job rotation

B. Implicit deny

C. Least privilege

D. Separation of duties

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 229

Ann is traveling for business and is attempting to use the hotel's wireless network to check for new messages. She selects the hotel's wireless SSID from a list of networks and successfully connects. After opening her email client and waiting a few minutes, the connection times out. Which of the following should Ann do to retrieve her email messages?

- A. Change the authentication method for her laptop's wireless card from WEP to WPA2
- B. Open a web browser and authenticate using the captive portal for the hotel's wireless network
- C. Contact the front desk and have the MAC address of her laptop added to the MAC filter on the hotel's wireless network
- D. Change the incoming email protocol from IMAP to POP3

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 230

Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?

"Pass Any Exam. Any Time." - www.actualtests.com 651
CompTIA SY0-401 Exam

- A. Dictionary
- B. Hybrid
- C. Watering hole
- D. Brute Force

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 231

Ann, a security administrator, is strengthening the security controls of the company's campus. Her goal is to prevent people from accessing open locations that are not supervised, such as around the receiving dock. She is also concerned that employees are using these entry points as a way of bypassing the security guard at

the main entrance. Which of the following should Ann recommend that would BEST address her concerns?

- A. Increase the lighting surrounding every building on campus
- B. Build fences around campus with gate entrances
- C. Install cameras to monitor the unsupervised areas
- D. Construct bollards to prevent vehicle entry in non-supervised areas

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 232

While an Internet café a malicious user is causing all surrounding wireless connected devices to have intermittent and unstable connections to the access point. Which of the following is MOST likely being used?

- A. Evil Twin
- B. Interference
- C. Packet sniffer
- D. Rogue AP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 652
CompTIA SY0-401 Exam

QUESTION 233

A password audit has revealed that a significant percentage of end-users have passwords that are easily cracked. Which of the following is the BEST technical control that could be implemented to reduce the amount of easily "crackable" passwords in use?

- A. Credential management
- B. Password history

- C. Password complexity
- D. Security awareness training

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 234

While working on a new project a security administrator wants to verify the integrity of the data in the organizations archive library. Which of the following is the MOST secure combination to implement to meet this goal? (Select TWO)

- A. Hash with SHA
- B. Encrypt with Diffie-Hellman
- C. Hash with MD5
- D. Hash with RIPEMD
- E. Encrypt with AES

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 235

A company has been attacked and their website has been altered to display false information. The security administrator disables the web server service before restoring the website from backup. An audit was performed on the server and no other data was altered. Which of the following should be performed after the server has been restored?

- A. Monitor all logs for the attacker's IP
- B. Block port 443 on the web server
- C. Install and configure SSL to be used on the web server
- D. Configure the web server to be in VLAN 0 across the network "Pass Any Exam. Any Time." - www.actualtests.com 653
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 236

A security administrator suspects that an employee in the IT department is utilizing a reverse proxy to bypass the company's content filter and browse unapproved and non-work related sites while at work. Which of the following tools could BEST be used to determine how the employee is connecting to the reverse proxy?

- A. Port scanner
- B. Vulnerability scanner
- C. Honeypot
- D. Protocol analyzer

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 237

Joe, a company's network engineer, is concerned that protocols operating at the application layer of the OSI model are vulnerable to exploitation on the network. Which of the following protocols should he secure?

- A. SNMP
- B. SSL
- C. ICMP
- D. NetBIOS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 238

Ann a security technician receives a report from a user that is unable to access an offsite SSH server. Ann checks the firewall and sees the following rules:

Allow TCP 80

"Pass Any Exam. Any Time." - www.actualtests.com 654
CompTIA SY0-401 Exam
Allow TCP 443

Deny TCP 23

Deny TCP 20

Deny TCP 21

Which of the following is preventing the users from accessing the SSH server?

- A. Deny TCP 20
- B. Deny TCP 21
- C. Deny TCP 23
- D. Implicit deny

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 239

An administrator uses a server with a trusted OS and is configuring an application to go into production tomorrow. In order to make a new application work properly, the administrator creates a new policy that labels the application and assigns it a security context within the trusted OS. Which of the following control methods is the administrator using by configuring this policy?

- A. Time based access control
- B. Mandatory access control
- C. Role based access control
- D. Rule based access control

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 240

A security administrator has been tasked with assisting in the forensic investigation of an incident relating to employee misconduct. The employee's supervisor believes evidence of this misconduct can be found on the employee's assigned workstation. Which of the following choices BEST describes what should be done? (Select TWO)

- A. Record time as offset as required and conduct a timeline analysis "Pass Any Exam. Any Time." - www.actualtests.com 655
CompTIA SY0-401 Exam
- B. Update antivirus definitions and conduct a full scan for infected files
- C. Analyze network traffic, system, and file logs
- D. Create an additional local admin account on that workstation to conduct work from
- E. Delete other user profiles on the system to help narrow down the search space
- F. Patch the system before reconnecting it to the network

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 241

Joe a web developer wants to make sure his application is not susceptible to cross-site request forgery attacks. Which of the following is one way to prevent this type of attack?

- A. The application should always check the HTTP referrer header
- B. The application should always check the HTTP Request header
- C. The application should always check the HTTP Host header
- D. The application should always use SSL encryption

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 242

A security technician has been tasked with opening ports on a firewall to allow users to browse the internet. Which of the following ports should be opened on the firewall? (Select Three)

- A. 22
- B. 53
- C. 80
- D. 110
- E. 443
- F. 445
- G. 8080

Correct Answer: CEG

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 656
CompTIA SY0-401 Exam

QUESTION 243

A rogue programmer included a piece of code in an application to cause the program to halt at 2:00 PM on Monday afternoon when the application is most utilized. This is Which of the following types of malware?

- A. Trojan
- B. Virus
- C. Logic Bomb
- D. Botnets

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 244

After connecting to the corporate network a user types the URL of a popular social media website in the browser but reports being redirected to a login page with the corporate logo. Which of the following is this an example of?

- A. LEAP
- B. MAC filtering
- C. WPA2-Enterprise
- D. Captive portal

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 245

The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?

- A. Grey box testing
- B. White box testing
- C. Penetration testing
- D. Black box testing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 657

CompTIA SY0-401 Exam

Explanation:

QUESTION 246

A user Ann has her assigned token but she forgotten her password. Which of the following appropriately categorizes the authentication factor that will fail in this scenario?

- A. Something you do
- B. Something you know
- C. Something you are
- D. Something you have

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 247

An employee from the fire Marshall's office arrives to inspect the data center. The operator allows him to bypass the multi-factor authentication to enter the data center. Which of the following types of attacks may be underway?

- A. Impersonation
- B. Hoax
- C. Tailgating
- D. Spoofing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 248

A company recently received accreditation for a secure network, In the accreditation letter, the auditor specifies that the company must keep its security plan current with changes in the network and evolve the systems to adapt to new threats. Which of the following security controls will BEST achieve this goal?

- A. Change management
- B. Group Policy
"Pass Any Exam. Any Time." - www.actualtests.com 658
CompTIA SY0-401 Exam
- C. Continuous monitoring
- D. Credential management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 249

A cyber security administrator receives a list of IPs that have been reported as attempting to access the network. To identify any possible successful attempts across the enterprise, which of the following should be implemented?

- A. Monitor authentication logs
- B. Disable unnecessary accounts
- C. Time of day restrictions
- D. Separation of duties

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 250

Which of the following exploits either a host file on a target machine or vulnerabilities on a DNS server in order to carry out URL redirection?

- A. Pharming
- B. Spoofing
- C. Vishing
- D. Phishing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 251

Ann a new small business owner decides to implement WiFi access for her customers. There are several other businesses nearby who also have WiFi hot spots. Ann is concerned about security of the wireless network and wants to ensure that only her customers have access. Which of the following choices BEST meets her intent of security and access?

"Pass Any Exam. Any Time." - www.actualtests.com 659
CompTIA SY0-401 Exam

- A. Enable port security
- B. Enable WPA
- C. Disable SSID broadcasting
- D. Enable WEP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 252

A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Select TWO)

- A. PGP/GPG
- B. S/MIME
- C. IPSEC
- D. Secure POP3
- E. IMAP
- F. HMAC

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 253

Which of the following is the GREATEST security concern of allowing employees to bring in their personally owned tablets and connecting to the corporate network?

- A. Tablet network connections are stored and accessible from the corporate network
- B. The company's attack surface increases with the non-corporate devices
- C. Personally purchased media may be available on the network for others to stream
- D. Encrypted tablets are harder to access to determine if they are infected

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 254

Searching for systems infected with malware is considered to be which of the following phases of

"Pass Any Exam. Any Time." - www.actualtests.com 660

CompTIA SY0-401 Exam

incident response?

- A. Containment
- B. Preparation
- C. Mitigation
- D. Identification

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 255

A technician has deployed a new VPN concentrator. The device needs to authenticate users based on a backend directory service. Which of the following services could be run on the VPN concentrator to perform this authentication?

- A. Kerberos
- B. RADIUS
- C. GRE

D. IPSec

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 256

A webpage displays a potentially offensive advertisement on a computer. A customer walking by notices the displayed advertisement and files complaint. Which of the following can BEST reduce the likelihood of this incident occurring again?

- A. Clean-desk policies
- B. Screen-locks
- C. Pop-up blocker
- D. Antispyware software

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 661
CompTIA SY0-401 Exam

QUESTION 257

Which of the following is an attack designed to activate based on date?

- A. Logic bomb
- B. Backdoor
- C. Trojan
- D. Rootkit

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 258

A malicious user has collected the following list of information:

192.168.1.5 OpenSSH-Server_5.8

192.168.1.7 OpenSSH-Server_5.7

192.168.1.9 OpenSSH-Server_5.7

Which of the following techniques is MOST likely to gather this type of data?

- A. Banner grabbing
- B. Port scan
- C. Host scan
- D. Ping scan

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 259

A company wants to prevent unauthorized access to its secure data center. Which of the following security controls would be MOST appropriate?

- A. Alarm to local police
 - B. Camera
 - C. Security guard
 - D. Motion detector
- "Pass Any Exam. Any Time." - www.actualtests.com 662
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 260

Company policy requires employees to change their passwords every 60 days. The security manager has verified all systems are configured to expire passwords after 60 days. Despite the policy and technical configuration, weekly password audits suggest that some employees have had the same weak passwords in place longer than 60 days. Which of the following password parameters is MOST likely misconfigured?

- A. Minimum lifetime
- B. Complexity
- C. Length
- D. Maximum lifetime

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 261

An administrator would like to utilize encryption that has comparable speed and strength to the AES cipher without using AES itself. The cipher should be able to operate in the same modes as AES and utilize the same minimum bit strength. Which of the following algorithms should the administrator select?

- A. RC4
- B. Rijndael
- C. SHA
- D. TwoFish
- E. 3DES

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 262

"Pass Any Exam. Any Time." - www.actualtests.com 663

CompTIA SY0-401 Exam

A security analyst has a sample of malicious software and needs to know what the sample does. The analyst runs the sample in a carefully-controlled and monitored virtual machine to observe the software's behavior. The approach of malware analysis can BEST be described as:

- A. Static testing
- B. Security control testing
- C. White box testing
- D. Sandboxing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 263

An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)

- A. Symmetrical encryption
- B. Ephemeral Key generation
- C. Diffie-Hellman
- D. AES
- E. RSA
- F. Asymmetrical encryption

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 264

Company A and Company B both supply contractual services to a fast paced and growing auto parts manufacturer with a small local Area Network (LAN) at its local site. Company A performs in-house billing and invoices services for the local auto parts manufacturer. Company B provides in-house parts and widgets services for the local auto parts manufacturers. Which of the following is the BEST method to mitigate security risk within the environment?

- A. Virtual Private Network
 - B. Role-Based access
 - C. Network segmentation
 - D. Public Key Infrastructure
- "Pass Any Exam. Any Time." - www.actualtests.com 664
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 265

The Chief Executive Officer (CEO) Joe notices an increase in the wireless signal in this office and thanks the IT director for the increase in network speed. Upon investigation the IT department finds an access point hidden in the dropped ceiling outside of Joe's office. Which of the following types of attack is MOST likely occurring?

- A. Packet sniffing
- B. Bluesnarfing
- C. Man-in-the-middle
- D. Evil twin

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 266

A security administrator is reviewing the company's data backup plan. The plan implements nightly offsite data replication to a third party company. Which of the following documents specifies how much data can be stored offsite, and how quickly the data can be retrieved by the company from the third party?

- A. MTBF
- B. SLA
- C. RFQ

D. ALE

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 267

Which of the following authentication services uses a default TCP port of 88?

A. Kerberos



<http://www.gratisexam.com/>

B. TACACS+

C. SAML

D. LDAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 268

A technician has been tasked with installing and configuring a wireless access point for the engineering department. After the AP has been installed, there have been reports the employees from other departments have been connecting to it without approval. Which of the following would BEST address these concerns?

A. Change the SSID of the AP so that it reflects a different department, obscuring its ownership

B. Implement WPA2 encryption in addition to WEP to protect the data-in-transit

C. Configure the AP to allow only to devices with pre-approved hardware addresses

<http://www.gratisexam.com/>

D. Lower the antenna's power so that it only covers the engineering department's offices

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 269

A company has implemented full disk encryption. Clients must authenticate with a username and password at a pre-boot level to unlock the disk and again a username and password at the network login. Which of the following are being used? (Select TWO)

- A. Multifactor authentication
- B. Single factor authentication
- C. Something a user is
- D. Something a user has
- E. Single sign-on
- F. Something a user knows

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 666
CompTIA SY0-401 Exam

QUESTION 270

Anne an employee receives the following email:

From: Human Resources

To: Employee

Subject: Updated employee code of conduct

Please click on the following link: <http://external.site.com/codeofconduct.exe> to review the updated code of conduct at your earliest convenience.

After clicking the email link, her computer is compromised. Which of the following principles of social engineering was used to lure Anne into clicking the phishing link in the above email?

- A. Authority
- B. Familiarity
- C. Intimidation
- D. Urgency

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 271

During a review a company was cited for allowing requestors to approve and implement their own change request. Which of the following would resolve the issue? (Select TWO)

- A. Separation duties
- B. Mandatory access
- C. Mandatory vacations
- D. Audit logs
- E. Job Rotation
- F. Time of day restrictions

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 272

A security administrator wishes to protect session keys should a private key become discovered.

"Pass Any Exam. Any Time." - www.actualtests.com 667
CompTIA SY0-401 Exam

Which of the following should be enabled in IPSec to allow this?

- A. Perfect forward secrecy
- B. Key escrow
- C. Digital signatures
- D. CRL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 273

A workstation is exhibiting symptoms of malware and the network security analyst has decided to remove the system from the network. This represents which of the following stages of the Incident Handling Response?

- A. Plan of action
- B. Mitigation
- C. Lesson Learned
- D. Recovery

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 274

Which of the following would provide the MOST objective results when performing penetration testing for an organization?

- A. An individual from outside the organization would be more familiar with the system
- B. AN inside support staff member would know more about how the system could be compromised
- C. An outside company would be less likely to skew the results in favor if the organization
- D. An outside support staff member would be more likely to report accurate results due to familiarity with the system

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 668
CompTIA SY0-401 Exam

QUESTION 275

An administrator would like users to authenticate to the network using only UDP protocols. Which of the following would meet this goal?

- A. RADIUS
- B. TACACS+
- C. Kerberos
- D. 802.1x

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 276

When employing PKI to send signed and encrypted data the individual sending the data must have: (Select TWO)

- A. The receiver's private key
- B. The root certificate
- C. The sender's private key
- D. The sender's public key
- E. The receiver's public key

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 277

Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

- A. OS hardening
- B. Application control
- C. Virtualization
- D. Sandboxing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 669
CompTIA SY0-401 Exam

Explanation:

QUESTION 278

A custom PKI application downloads a certificate revocation list (CRL) once per day. Management requests the list be checked more frequently. Which of the following is the BEST solution?

- A. Refresh the CA public key each time a user logs in
- B. Download the CRK every 60 seconds
- C. Implement the OCSP protocol
- D. Prompt the user to trust a certificate each time it is used

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 279

A security technician wants to improve the strength of a weak key by making it more secure against brute force attacks. Which of the following would achieve this?

- A. Blowfish
- B. Key stretching
- C. Key escrow
- D. Recovery agent

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 280

Joe uses his badge to enter the server room, Ann follows Joe entering without using her badge. It is later discovered that Ann used a USB drive to remove confidential data from a server. Which of the following principles is potentially being violated? (Select TWO)

- A. Clean desk policy
 - B. Least privilege
 - C. Tailgating
 - D. Zero-day exploits
 - E. Data handling
- "Pass Any Exam. Any Time." - www.actualtests.com 670
CompTIA SY0-401 Exam

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 281

Ann the IT director wants to ensure that as hoc changes are not making their way to the production applications. Which of the following risk mitigation strategies should she implement in her department?

- A. Change management
- B. Permission reviews
- C. Incident management

D. Perform routine audits

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 282

Which of the following would allow users from outside of an organization to have access to internal resources?

- A. NAC
- B. VLANs
- C. VPN
- D. NAT

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 283

Which of the following is BEST described by a scenario where management chooses not to implement a security control for a given risk?

- A. Mitigation
"Pass Any Exam. Any Time." - www.actualtests.com 671
CompTIA SY0-401 Exam
- B. Avoidance
- C. Acceptance
- D. Transference

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 284

Which of the following ports is used for TELNET by default?

- A. 22
- B. 23
- C. 21
- D. 20

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 285

When confidentiality is the primary concern which of the following types of encryption should be chosen?

- A. Digital Signature
- B. Symmetric
- C. Asymmetri
- D. Hashing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 286

A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

- A. Kill all system processes
- "Pass Any Exam. Any Time." - www.actualtests.com 672
CompTIA SY0-401 Exam

- B. Enable the firewall
- C. Boot from CD/USB
- D. Disable the network connection

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 287

Ann a member of the Sales Department has been issued a company-owned laptop for use when traveling to remote sites. Which of the following would be MOST appropriate when configuring security on her laptop?

- A. Configure the laptop with a BIOS password
- B. Configure a host-based firewall on the laptop
- C. Configure the laptop as a virtual server
- D. Configure a host based IDS on the laptop

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 288

A security technician has removed the sample configuration files from a database server. Which of the following application security controls has the technician attempted?

- A. Application hardening
- B. Application baselines
- C. Application patch management
- D. Application input validation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 289

Data confidentiality must be enforced on a secure database. Which of the following controls meets this goal? (Select TWO)

"Pass Any Exam. Any Time." - www.actualtests.com 673

CompTIA SY0-401 Exam

- A. MAC
- B. Lock and key
- C. Encryption
- D. Non-repudiation
- E. Hashing

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 290

A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site do not record any footage. Which of the following types of controls was being used?

- A. Detective
- B. Corrective
- C. Deterrent
- D. Preventive

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 291

A network security administrator is trying to determine how an attacker gained access to the corporate wireless network. The network is configured with SSID broadcast disabled. The senior network administrator explains that this configuration setting would only have determined an unsophisticated attacker because of which of the following?

- A. The SSID can be obtained with a wireless packet analyzer
- B. The required information can be brute forced over time
- C. Disabling the SSID only hides the network from other WAPs
- D. The network name could be obtained through a social engineering campaign

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 292

"Pass Any Exam. Any Time." - www.actualtests.com 674

CompTIA SY0-401 Exam

Joe a system administrator receives reports that users attempting to reach the corporate website are arriving at an unfamiliar website instead. An investigation by a forensic analyst found that the name server log has several corporate IP addresses that were changed using Joe's credentials.

Which of the following is this attack called?

- A. Xmas attack
- B. DNS poisoning
- C. Web server attack
- D. Spoofing attack

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 293

Joe a technician initiated scans if the company's 10 routers and discovered that half if the routers were not changed from their default configuration prior installed on the network. Which of the following would address this?

- A. Secure router configuration
- B. Implementing 802.1x
- C. Enabling loop protection
- D. Configuring port security

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 294

An employee attempts to go to a well-known bank site using the company-standard web browser by correctly typing in the address of the site into the web browser. The employee is directed to a website that looks like the bank's site but is not the actual bank site. The employee's user name and password are subsequently stolen. This is an example of which of the following?

- A. Watering hole attack
- B. Cross-site scripting
- C. DNS poisoning
- D. Man-in-the-middle attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 675
CompTIA SY0-401 Exam

Explanation:

QUESTION 295

A user authenticates to a local directory server. The user then opens a virtualization client to connect to a virtual server. Instead of supplying a username/password combination, the user simply checks a use directory credentials checkbox to authenticate to the virtual server. Which of the following authentication types has been utilized?

- A. Transitive trust
- B. Common access card

- C. Multifactor authentication
- D. Single sign-on

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 296

The new Chief Information Officer (CIO) of company ABC, Joe has noticed that company XWY is always one step ahead with similar products. He tasked his Chief Security Officer to implement new security controls to ensure confidentiality of company ABC's proprietary data and complete accountability for all data transfers. Which of the following security controls did the Chief Security Officer implement to BEST meet these requirements? (Select Two)

- A. Redundancy
- B. Hashing
- C. DRP
- D. Digital Signatures
- E. Encryptions

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 297

A worker dressed in a fire suppression company's uniform asks to be let into the server room to perform the annual check in the fire extinguishers. The system administrator allows the worker into

"Pass Any Exam. Any Time." - www.actualtests.com 676

CompTIA SY0-401 Exam

the room, only to discover hours later that the worker was actually a penetration tester. Which of the following reasons allowed the penetration tester to access the server room?

- A. Testing the fire suppression system represented a critical urgency
- B. The pen tester assumed the authority of a reputable company

- C. The pen tester used an intimidation technique on the administrator
- D. The administrator trusted that the server room would remain safe

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 298

A company uses port security based on an approved MAC list to secure its wired network and WPA2 to secure its wireless network. Which of the following prevents an attacker from learning authorized MAC addresses?

- A. Port security prevents access to any traffic that might provide an attacker with authorized MAC addresses
- B. Port security uses certificates to authenticate devices and is not part of a wireless protocol
- C. Port security relies in a MAC address length that is too short to be cryptographically secure over wireless networks
- D. Port security encrypts data on the network preventing an attacker from reading authorized MAC addresses

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 299

A security technician is implementing PKI on a Network. The technician wishes to reduce the amount of bandwidth used when verifying the validity of a certificate. Which of the following should the technician implement?

- A. CSR
- B. Key escrow
- C. OSCR
- D. CRL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 677
CompTIA SY0-401 Exam

Explanation:

QUESTION 300

The network security manager has been notified by customer service that employees have been sending unencrypted confidential information via email. Which of the following should the manager select to BEST detect and provide notification of these occurrences?

- A. DLP
- B. SSL
- C. DEP
- D. UTM

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 301

While troubleshooting a new wireless 802.11 ac network an administrator discovers that several of the older systems cannot connect. Upon investigation the administrator discovers that the older devices only support 802.11 and RC4. The administrator does not want to affect the performance of the newer 802.11 ac devices on the network. Which of the following should the administrator do to accommodate all devices and provide the MOST security?

- A. Disable channel bonding to allow the legacy devices and configure WEP fallback
- B. Configure the AP in protected mode to utilize WPA2 with CCMP
- C. Create a second SSID on the AP which utilizes WPA and TKIP
- D. Configure the AP to utilize the 5Gh band only and enable WEP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 302

A security administrator is troubleshooting an authentication issues using a network sniffer. The security administrator reviews a packet capture of the authentication process and notices that authentication is performed using extensible markup over SOAP. Which of the following authentication services is the security administrator troubleshooting?

"Pass Any Exam. Any Time." - www.actualtests.com 678
CompTIA SY0-401 Exam

- A. SAML
- B. XTACACS
- C. Secure LDAP
- D. RADIUS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 303

Given a class C network a technician has been tasked with creating a separate subnet for each of the eight departments in the company. Which of the following network masks would allow for each department to have a unique network space and what is the maximum number of hosts each department could have?

- A. Network 255.255.255.192, 62 hosts
- B. Network 255.255.255.224, 30 hosts
- C. Network 255.255.255.240, 16 hosts
- D. Network 255.255.255.248, 32 hosts

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 304

A software security concern when dealing with hardware and devices that have embedded software or operating systems is:

- A. Patching may not always be possible

- B. Configuration support may not be available
- C. There is no way to verify if a patch is authorized or not
- D. The vendor may not have a method for installation of patches

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 305

A major medical corporation is investigating deploying a web based portal for patients to access

"Pass Any Exam. Any Time." - www.actualtests.com 679

CompTIA SY0-401 Exam

their medical records. The medical corporation has a long history of maintaining IT security but is considering having a third party vendor create the web portal. Which of the following areas is MOST important for the Chief Information Security Officer to focus on when reviewing proposal from vendors interested in creating the web portal?

- A. Contractor background check
- B. Confidentiality and availability
- C. Redundancy and privacy
- D. Integrity and confidentiality

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 306

Which of the following authentication methods requires the user, service provider and an identity provider to take part in the authentication process?

- A. RADIUS
- B. SAML
- C. Secure LDAP
- D. Kerberos

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 307

Which of the following types of malware is designed to provide access to a system when normal authentication fails?

- A. Rootkit
- B. Botnet
- C. Backdoor
- D. Adware

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 680
CompTIA SY0-401 Exam

QUESTION 308

Ann is concerned that the application her team is currently developing is vulnerable to unexpected user input that could lead to issues within the memory is affected in a detrimental manner leading to potential exploitation. Which of the following describes this application threat?

- A. Replay attack
- B. Zero-day exploit
- C. Distributed denial of service
- D. Buffer overflow

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 309

Which of the following can be used for both encryption and digital signatures?

- A. 3DES
- B. AES
- C. RSA
- D. MD5

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 310

A user tries to visit a web site with a revoked certificate. In the background a server from the certificate authority only sends the browser revocation information about the domain the user is visiting. Which of the following is being used by the certificate authority in this exchange?

- A. CSR
- B. Key escrow
- C. OCSP
- D. CRL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 681
CompTIA SY0-401 Exam

QUESTION 311

Joe wants to employ MD5 hashing on the company file server. Which of the following is Joe trying to achieve?

- A. Availability
- B. Confidentiality
- C. Non repudiation
- D. Integrity

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 312

By hijacking unencrypted cookies an application allows an attacker to take over existing web sessions that do not use SSL or end to end encryption. Which of the following choices BEST mitigates the security risk of public web surfing? (Select TWO)

- A. WPA2
- B. WEP
- C. Disabling SSID broadcasting
- D. VPN
- E. Proximity to WIFI access point

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 313

The security administration team at a company has been tasked with implementing a data-at-rest solution for its company storage. Due to the large amount of storage the Chief Information Officer (CISO) decides that a 128-bit cipher is needed but the CISO also does not want to degrade system performance any more than necessary. Which of the following encryptions needs BOTH of these needs?

- A. SHA1
 - B. DSA
 - C. AES
- "Pass Any Exam. Any Time." - www.actualtests.com 682
CompTIA SY0-401 Exam

D. 3DES

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 314

A company has a BYOD policy that includes tablets and smart phones. In the case of a legal investigation, which of the following poses the greatest security issues?

- A. Recovering sensitive documents from a device if the owner is unable or unwilling to cooperate
- B. Making a copy of all of the files on the device and hashing them after the owner has provided the PIN
- C. Using GPS services to locate the device owner suspected in the investigation
- D. Wiping the device from a remote location should it be identified as a risk in the investigation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 315

After several thefts a Chief Executive Officer (CEO) wants to ensure unauthorized do not have to corporate grounds or its employees. The CEO just approved new budget line items for fences, lighting, locks and CCTVs. Which of the following is the primary focus?

- A. Safety
- B. Confidentiality
- C. Availability
- D. Integrity

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 316

Which of the following steps in incident response procedures entails of the incident and identification of knowledge gained that can be applied to future handling of incidents?

"Pass Any Exam. Any Time." - www.actualtests.com 683
CompTIA SY0-401 Exam

- A. Recovery procedures
- B. Escalation and notification
- C. Reporting
- D. Lessons learned

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 317

Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?

- A. Fuzzing
- B. Black box
- C. Fault injection
- D. SQL injection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 318

A company's BYOD policy requires the installation of a company provide mobile agent on their on their personally owned devices which would allow auditing when an employee wants to connect a device to the corporate email system. Which of the following concerns will MOST affect the decision to use a personal device to

receive company email?

- A. Personal privacy
- B. Email support
- C. Data ownership
- D. Service availability

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 319

A penetration tester is measuring a company's posture on social engineering. The penetration

"Pass Any Exam. Any Time." - www.actualtests.com 684

CompTIA SY0-401 Exam

tester sends a phishing email claiming to be from IT asking employees to click a link to update their VPN software immediately. Which of the following reasons would explain why this attack could be successful?

- A. Principle of Scarcity
- B. Principle of Intimidation
- C. Principle of Urgency
- D. Principle of liking

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 320

A new employee has joined the accounting department and is unable to access the accounting server. The employee can access other network resources and the Internet. Other accounting employees are able to access the accounting server without any issues. Which of the following is the MOST likely issue?

- A. The server's IDS is blocking the new employee's connection

- B. The workstation is unable to join the domain
- C. The server's drive is not mapped on the new employee's workstation
- D. The new account is not in the proper role-based profile

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 321

Joe a sales employee is connecting to a wireless network and has entered the network information correctly. His computer remains connected to the network but he cannot access any resources on the network. Which of the following is the MOST likely cause of this issue?

- A. The encryption is too strong
- B. The network SSID is disabled
- C. MAC filtering is enabled
- D. The wireless antenna power is set too low

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 685
CompTIA SY0-401 Exam

QUESTION 322

Which of the following is used to inform users of the repercussions of releasing proprietary information?

- A. OLA
- B. SLA
- C. NDA
- D. MOU

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 323

A review of administrative access has discovered that too many accounts have been granted administrative rights. Which of the following will alert the security team when elevated access is applied?

- A. Establishing user access reviews
- B. Establishing user based privileges
- C. Establishing monitoring on accounts
- D. Establishing group based privileges

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 324

When an authorized application is installed on a server, the application triggers an alert on the HIDS. This is known as a:

- A. Vulnerability
- B. False negative
- C. False positive
- D. Threat vector

"Pass Any Exam. Any Time." - www.actualtests.com 686
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 325

In which of the following scenarios would it be preferable to implement file level encryption instead of whole disk encryption?

- A. A server environment where the primary security concern is integrity and not file recovery
- B. A cloud storage environment where multiple customers use the same hardware but possess different encryption keys
- C. A SQL environment where multiple customers access the same database
- D. A large datacenter environment where each customer users dedicated hardware resources

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 326

For high availability which of the following would be MOST appropriate for fault tolerance?

- A. RAID 0
- B. Clustering
- C. JBOD
- D. Load Balancing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 327

When implementing a Public Key Infrastructure, which of the following should the sender use to digitally sign a document?

- A. A CSR
- B. A private key
- C. A certificate authority
- D. A public key

"Pass Any Exam. Any Time." - www.actualtests.com 687
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 328

A military base wants to incorporate biometrics into its new security measures, but the head of security does not want them to be the sole method of authentication. For unmanned entry points, which of the following solutions would work BEST?

- A. Use voice print and a bollard
- B. Use a retina scanner and a thumbprint
- C. Use CCTV and a PIN
- D. Use a retina scan and a PIN code

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 329

Ann a security administrator wants a limit access to the wireless network. Which of the following can be used to do this without using certificates?

- A. Employ EPA-TLS
- B. Employ PEAP on all laptops
- C. Enable MAC filtering
- D. Disable SSID broadcasting

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 330

A user has an Android smartphone that supports full device encryption. However when the user plugs into a computer all of the files are immediately accessible. Which of the following should the user do to enforce full device confidentiality should the phone be lost or stolen?

- A. Establish a PIN passphrase
- B. Agree to remote wipe terms
"Pass Any Exam. Any Time." - www.actualtests.com 688
CompTIA SY0-401 Exam
- C. Generate new media encryption keys
- D. Download the encryption control app from the store

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 331

The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow for proper communication between internet users and the internal systems?

- A. VLAN
- B. DNS
- C. NAT
- D. HTTP
- E. SSL

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 332

After a new RADIUS server is added to the network, an employee is unable to connect to the company's WPA2-Enterprise WIFI network, which is configured to prompt for the employee's network username and password. The employee reports receiving an error message after a brief connection attempt, but is never

prompted for credentials. Which of the following issues could be causing the problem?

- A. The employee's account is locked out in the directory service
- B. The new RADIUS server is overloading the wireless access point
- C. The new RADIUS server's certificate is not trusted by the employee's PC
- D. The employee's account is disabled in the RADIUS server's local database

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 689
CompTIA SY0-401 Exam

QUESTION 333

Ann the security administrator has been reviewing logs and has found several overnight sales personnel are accessing the finance department's network shares. Which of the following security controls should be implemented to BEST remediate this?

- A. Mandatory access
- B. Separation of duties
- C. Time of day restrictions
- D. Role based access

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 334

A fiber company has acquired permission to bury a fiber cable through a farmer's land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

- A. No farm animals will graze near the burial site of the cable
- B. No digging will occur near the burial site of the cable

- C. No buildings or structures will be placed on top of the cable
- D. No crops will be planted on top of the cable

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 335

The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

- A. Threat
- B. Risk
- C. Attack
- D. Vulnerability

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 690
CompTIA SY0-401 Exam

QUESTION 336

A security technician would like to use ciphers that generate ephemeral keys for secure communication. Which of the following algorithms support ephemeral modes? (Select TWO)

- A. Diffie-Hellman
- B. RC4
- C. RIPEMD
- D. NTLMv2
- E. PAP
- F. RSA

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 337

A security technician would like an application to use random salts to generate short lived encryption keys during the secure communication handshake process to increase communication security. Which of the following concepts would BEST meet this goal?

- A. Ephemeral keys
- B. Symmetric Encryption Keys
- C. AES Encryption Keys
- D. Key Escrow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 338

A security administrator wishes to implement a method of generating encryption keys from user passwords to enhance account security. Which of the following would accomplish this task?

- A. NTLMv2
- B. Blowfish
- C. Diffie-Hellman
- D. PBKDF2

"Pass Any Exam. Any Time." - www.actualtests.com 691
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 339

An administrator needs to allow both secure and regular web traffic into a network. Which of the following ports should be configured? (Select TWO)

- A. 25
- B. 53
- C. 80
- D. 110
- E. 143
- F. 443

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 340

A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

- A. Deploy a honeypot
- B. Disable unnecessary services
- C. Change default password
- D. Implement an application firewall
- E. Penetration testing

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 341

A local hospital with a large four-acre campus wants to implement a wireless network so that doctors can use tablets to access patients' medical data. The hospital

also wants to provide guest access to the internet for hospital patients and visitors in select areas. Which of the following areas

"Pass Any Exam. Any Time." - www.actualtests.com 692
CompTIA SY0-401 Exam
should be addressed FIRST?

- A. MAC filters
- B. Site Survey
- C. Power level controls
- D. Antenna types

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 342

After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he did not accidentally make a change during his investigation. Which of the following should he perform?

- A. Take a hash of the image and compare it to the one being investigated
- B. Compare file sizes of all files prior to and after investigation
- C. Make a third image and compare it to the second image being investigated
- D. Compare the logs of the copy to the actual server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 343

Which of the following attacks is generally initiated from a botnet?

- A. Cross site scripting attack
- B. HTTP header injection

- C. Distributed denial of service
- D. A war driving attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 344

"Pass Any Exam. Any Time." - www.actualtests.com 693

CompTIA SY0-401 Exam

A network security analyst has confirmed that the public facing web server has been compromised. Which of the following stages if the Incident Handling Response does this describe?

- A. Analyzing
- B. Recovering
- C. Identification
- D. Mitigation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 345

Deploying compensating security controls is an example of:

- A. Risk avoidance
- B. Risk mitigation
- C. Risk transference
- D. Risk acceptance

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 346

A web startup wants to implement single sign-on where its customers can log on to the site by using their personal and existing corporate email credentials regardless of which company they work for. Is this directly supported by SAML?



<http://www.gratisexam.com/>

- A. No not without extensive partnering and API integration with all required email providers
- B. Yes SAML is a web based single sign-on implementation exactly for this purpose
- C. No a better approach would be to use required email providers LDAP or RADIUS repositories
- D. Yes SAML can use OAuth2 to provide this functionality out of the box

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 694
CompTIA SY0-401 Exam

QUESTION 347

A security administrator is installing a single camera outside in order to detect unauthorized vehicles in the parking lot. Which of the following is the MOST important consideration when deploying a CCTV camera to meet the requirement?

- A. Training
- B. Expense
- C. Resolution
- D. Field of view

<http://www.gratisexam.com/>

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 348

A system administrator wants to configure a setting that will make offline password cracking more challenging. Currently the password policy allows upper and lower case characters a minimum length of 5 and a lockout after 10 invalid attempts. Which of the following has the GREATEST impact on the time it takes to crack the passwords?

- A. Increase the minimum password length to 8 while keeping the same character set
- B. Implement an additional password history and reuse policy
- C. Allow numbers and special characters in the password while keeping the minimum length at 5
- D. Implement an account lockout policy after three unsuccessful logon attempts

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 349

Establishing a method to erase or clear memory is an example of securing which of the following?

- A. Data in transit
- B. Data at rest
- C. Data in use
- D. Data in motion

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 350

Joe processes several requisitions during the day and during the night shift they are approved by Ann. This is an example of which of the following?

- A. Separation of duties
- B. Discretionary access
- C. Mandatory access
- D. Time of day restrictions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 351

A security administrator would like to write an access rule to block the three IP addresses given below. Which of the following combinations should be used to include all of the given IP addresses?

192.168.12.255

192.168.12.227

192.168.12.229

- A. 192.168.12.0/25
- B. 192.168.12.128.28
- C. 192.168.12.224/29
- D. 192.168.12.225/30

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 352

After installing a new Linux system the administrator runs a command that records the size, permissions, and MD5 sum of all the files on the system. Which of the following describes what the administrator is doing?

"Pass Any Exam. Any Time." - www.actualtests.com 696
CompTIA SY0-401 Exam

- A. Identifying vulnerabilities
- B. Design review
- C. Host software baselining
- D. Operating system hardening

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 353

An intrusion has occurred in an internet facing system. The security administrator would like to gather forensic evidence while the system is still in operation. Which of the following procedures should the administrator perform FIRST on the system?

- A. Make a drive image
- B. Take hashes of system data
- C. Collect information in RAM
- D. Capture network traffic

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 354

Which of the following wireless standards is backwards compatible with 802.11g?

- A. 802.11a
- B. 802.11b
- C. 802.11n
- D. 802.1q

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 355

Which of the following ports will be used for logging into secure websites?

"Pass Any Exam. Any Time." - www.actualtests.com 697
CompTIA SY0-401 Exam

- A. 80
- B. 110
- C. 142
- D. 443

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 356

The below report indicates that the system is MOST likely infected by which of the following?

Protocol LOCAL IP FOREIGN IP STATE

TCP 0.0.0:445 0.0.0.0:0 Listening

TCP 0.0.0.0:3390 0.0.0.0:0 Listening

- A. Trojan
- B. Worm
- C. Logic bomb
- D. Spyware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 357

A security administrator is required to submit a detailed implementation plan and back out plan to get approval prior to updating the firewall and other security devices. Which of the following types of risk mitigation strategies is being followed?

- A. Change management
- B. Routine audit
- C. Rights and permissions review
- D. Configuration management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 698
CompTIA SY0-401 Exam

QUESTION 358

Which of the following authentication services uses a default TCP of 389?

- A. SAML
- B. TACACS+
- C. Kerberos
- D. LDAP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 359

A software company sends their offsite backup tapes to a third party storage facility. TO meet confidentiality the tapes should be:

- A. Labeled
- B. Hashed
- C. Encrypted
- D. Duplicated

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 360

Ann, a technician, wants to implement a single protocol on a remote server which will enable her to encrypt and proxy all of her traffic though the remote server via SOCKS5. Which of the following should Ann enable to support both encryption and proxy services?

- A. SSH
- B. IPSEC
- C. TLS
- D. HTTPS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 699

QUESTION 361

Ann, a system analyst, discovered the following log. Which of the following or techniques does this indicate?

```
{bp1@localmachine}$ ls-al
```

Total 12

```
Drwxrwxr-x
```

```
drwxrwxr-x.  2 bp1 businesspartner 4096 Apr 18 05:19 .
drwx----- 22 bp1 businesspartner 4096   Apr 19 05:19 ..
-rw-rw-r--.  1 bp1 businesspartner 5023801 Apr 19 05:19 businesspartnerstatements18-4.csv
-rw-rw-r--.  1 bp1 businesspartner 7812851 Apr 20 05:19 businesspartnerstatements17-4.txt
-rw-rw-r--.  1 bp1 businesspartner 1739017 Apr 21 05:19 businesspartnerstatements16-4.csv
[nessus log] evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
[nessus log] evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
```

- A. Protocol analyzer
- B. Port scanner
- C. Vulnerability
- D. Banner grabbing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 362

A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client. Which of the following should the company implement?

- A. Port security
- B. WPA2
- C. Mandatory Access Control
- D. Network Intrusion Prevention

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 700
CompTIA SY0-401 Exam

QUESTION 363

The helpdesk is receiving numerous reports that a newly installed biometric reader at the entrance of the data center has a high of false negatives. Which of the following is the consequence of this reported problem?

- A. Unauthorized employees have access to sensitive systems
- B. All employees will have access to sensitive systems
- C. No employees will be able to access the datacenter
- D. Authorized employees cannot access sensitive systems

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 364

A software developer places a copy of the source code for a sensitive internal application on a company laptop to work remotely. Which of the following policies is MOST likely being violated?

- A. Clean desk
- B. Data handling
- C. Chain of custody

D. Social media

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 365

While testing a new host based firewall configuration a security administrator inadvertently blocks access to localhost which causes problems with applications running on the host. Which of the following addresses refer to localhost?

- A. ::0
- B. 127.0.0.0
- C. 120.0.0.1
- D. 127.0.0/8
- E. 127::0.1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 701
CompTIA SY0-401 Exam

Explanation:

QUESTION 366

A user has reported inadvertently sending an encrypted email containing PII to an incorrect distribution group. Which of the following potential incident types is this?

- A. Data sharing
- B. Unauthorized viewing
- C. Data breach
- D. Unauthorized access

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 367

A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?

- A. Credential management
- B. Support ownership
- C. Device access control
- D. Antivirus management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 368

A security engineer discovers that during certain times of day, the corporate wireless network is dropping enough packets to significantly degrade service. Which of the following should be the engineer's FIRST step in troubleshooting the issues?

- A. Configure stronger encryption
- B. Increase the power level
- C. Change to a higher gain antenna
- D. Perform a site survey

"Pass Any Exam. Any Time." - www.actualtests.com 702
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 369

A security administrator is reviewing the web logs and notices multiple attempts by users to access: http://www.comptia.org/idapsearch?user-*

Having identified the attack, which of the following will prevent this type of attack on the web server?

- A. Input validation on the web server
- B. Block port 389 on the firewall
- C. Segregate the web server by a VLAN
- D. Block port 3389 on the firewall

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 370

A breach at a credit card company resulted in customers credit card information being exposed . The company has conducted a full forensic investigation and identified the source of the breach.

Which of the following should the company do NEXT?

- A. Move to the incident identification phase
- B. Implement the risk assessment plan
- C. Implement damage and loss control procedures
- D. Implement first responder processes

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 371

Joe a user upon arriving to work on Monday morning noticed several files were deleted from the system. There were no records of any scheduled network outages or upgrades to the system. Joe notifies the security department of the anomaly found and removes the system from the network.

"Pass Any Exam. Any Time." - www.actualtests.com 703

CompTIA SY0-401 Exam

Which of the following is the NEXT action that Joe should perform?

- A. Screenshots of systems
- B. Call the local police
- C. Perform a backup
- D. Capture system image

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 372

The user of a news service accidentally accesses another user's browsing history. From this the user can tell what competitors are reading, querying, and researching. The news service has failed to properly implement which of the following?

- A. Application white listing
- B. In-transit protection
- C. Access controls
- D. Full disk encryption

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 373

A system requires administrators to be logged in as the "root" in order to make administrator changes. Which of the following controls BEST mitigates the risk associated with this scenario?

- A. Require that all administrators keep a log book of times and justification for accessing root
- B. Encrypt all users home directories using file-level encryption
- C. Implement a more restrictive password rotation policy for the shared root account
- D. Force administrator to log in with individual accounts and switch to root
- E. Add the administrator to the local group

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 704
CompTIA SY0-401 Exam

QUESTION 374

A defense contractor wants to use one of its classified systems to support programs from multiple intelligence agencies. Which of the following **MUST** be in place between the intelligence agencies to allow this?

- A. A DRP
- B. An SLA
- C. A MOU
- D. A BCP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 375

A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate these issues? (Select TWO)

- A. Separation of duties
- B. Least privilege
- C. Time of day restrictions
- D. Account expiration
- E. Discretionary access control
- F. Password history

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 376

Which of the following is considered the MOST effective practice when securing printers or scanners in an enterprise environment?

- A. Routine vulnerability scanning of peripherals
- B. Install in a hardened network segment
- C. Turn off the power to the peripherals at night
- D. Enable print sharing only from workstations

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 705

CompTIA SY0-401 Exam

Explanation:

QUESTION 377

After a few users report problems with the wireless network, a system administrator notices that a new wireless access point has been powered up in the cafeteria. The access point has the same SSID as the corporate network and is set to the same channel as nearby access points. However, the AP has not been connected to the Ethernet network. Which of the following is the MOST likely cause of the user's wireless problems?

- A. AP channel bonding
- B. An evil twin attack
- C. Wireless interference
- D. A rogue access point

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 378

A network technician at a company, Joe is working on a network device. He creates a rule to prevent users from connecting to a toy website during the holiday shopping season. This website is blacklisted and is known to have SQL injections and malware. Which of the following has been implemented?

- A. Mandatory access
- B. Network separation
- C. Firewall rules
- D. Implicit Deny

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 379

Company XYZ has suffered leaks of internally distributed confidential documents. Ann the network security analyst has been tasked to track down the culprit. She has decided to embed a four letter string of characters in documents containing proprietary information. Which of the following initial

"Pass Any Exam. Any Time." - www.actualtests.com 706
CompTIA SY0-401 Exam
steps should Ann implement before sending documents?

- A. Store one of the documents in a honey pot
- B. Start antivirus scan on all the suspected computers
- C. Add a signature to the NIDS containing the four letter string
- D. Ask employees to report suspicious behaviors

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 380

Which of the following should a company deploy to prevent the execution of some types of malicious code?

- A. Least privilege accounts
- B. Host-based firewalls
- C. Intrusion Detection systems
- D. Application white listing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 381

An administrator is investigating a system that may potentially be compromised and sees the following log entries on the router.

*Jul 15 14:47:29.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 3 packets.

*Jul 15 14:47:38.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 6 packets.

*Jul 15 14:47:45.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 8 packets.

Which of the following BEST describes the compromised system?

- A. It is running a rogue web server
"Pass Any Exam. Any Time." - www.actualtests.com 707
CompTIA SY0-401 Exam
- B. It is being used in a man-in-the-middle attack
- C. It is participating in a botnet
- D. It is an ARP poisoning attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 382

A security administrator implements a web server that utilizes an algorithm that requires other hashing standards to provide data integrity. Which of the following algorithms would meet the requirement?

- A. SHA
- B. MD5
- C. RIPEMD
- D. HMAC

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 383

Which of the following is the FIRST step in a forensics investigation when a breach of a client's workstation has been confirmed?

- A. Transport the workstation to a secure facility
- B. Analyze the contents of the hard drive
- C. Restore any deleted files and / or folders
- D. Make a bit-for-bit copy of the system

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 384

Company XYZ's laptops was recently stolen from a user which led to the exposure of confidential information. Which of the following should the security team implement on laptops to prevent future compromise?

"Pass Any Exam. Any Time." - www.actualtests.com 708
CompTIA SY0-401 Exam

- A. Cipher locks
- B. Strong passwords
- C. Biometrics
- D. Full Disk Encryption

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 385

A wireless site survey has been performed at a company. One of the results of the report is that the wireless signal extends too far outside the building. Which of the following security issues could occur as a result of this finding?

- A. Excessive wireless access coverage
- B. Interference with nearby access points
- C. Exhaustion of DHCP address pool
- D. Unauthorized wireless access

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 386

Which of the following is a software vulnerability that can be avoided by using input validation?

- A. Buffer overflow
- B. Application fuzzing
- C. Incorrect input
- D. Error handling

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 387

A university has a building that holds the power generators for the entire campus. A risk assessment was completed for the university and the generator building was labeled as a high risk. Fencing and lighting was installed to reduce risk. Which of the following security goals would

"Pass Any Exam. Any Time." - www.actualtests.com 709
CompTIA SY0-401 Exam
this meet?

- A. Load balancing
- B. Non-repudiation
- C. Disaster recovery
- D. Physical security

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 388

Log file analysis on a router reveals several unsuccessful telnet attempts to the virtual terminal (VTY) lines. Which of the following represents the BEST configuration used in order to prevent unauthorized remote access while maintaining secure availability for legitimate users?

- A. Disable telnet access to the VTY lines, enable SHH access to the VTY lines with RSA encryption
- B. Disable both telnet and SSH access to the VTY lines, requiring users to log in using HTTP
- C. Disable telnet access to the VTY lines, enable SHH access to the VTY lines with PSK encryption
- D. Disable telnet access to the VTY lines, enable SSL access to the VTY lines with RSA encryption

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 389

Four weeks ago a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff begins to spread, the IDS alerted the network administrator that access to sensitive client files had risen for above normal. Which of the following kind of IDS is in use?

- A. Protocol based
- B. Heuristic based
- C. Signature based
- D. Anomaly based

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 710
CompTIA SY0-401 Exam

QUESTION 390

A BYOD policy in which employees are able to access the wireless guest network is in effect in an organization. Some users however are using the Ethernet port in personal laptops to the wired network. Which of the following could an administrator use to ensure that unauthorized devices are not allowed to access the wired network?

- A. VLAN access rules configured to reject packets originating from unauthorized devices
- B. Router access lists configured to block the IP addresses of unauthorized devices
- C. Firewall rules configured to block the MAC addresses of unauthorized devices
- D. Port security configured shut down the port when unauthorized devices connect

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 391

During an office move a sever containing the employee information database will be shut down and transported to a new location. Which of the following would BEST ensure the availability of the employee database should happen to the server during the move?

- A. The contents of the database should be encrypted; the encryption key should be stored off-site
- B. A hash of the database should be taken and stored on an external drive prior to the move
- C. The database should be placed on a drive that consists of a RAID array prior to the move

D. A backup of the database should be stored on an external hard drive prior to the move

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 392

Which of the following is primarily used to provide fault tolerance at the application level? (Select TWO)

A. Load balancing

B. RAID array

C. RAID 6

"Pass Any Exam. Any Time." - www.actualtests.com 711

CompTIA SY0-401 Exam

D. Server clustering

E. JBOD array

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 393

A security administrator would like the corporate webserver to select perfect forward secrecy ciphers first. Which of the following cipher suites should the administrator select to accomplish this goal?

A. DH-DSS-CAMELLA256-SHA

B. ECDHE-RSA-AES1280SHA

C. DH-RSA-AES128-SHA256

D. ADH-AES256-SHA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 394

An administrator is having difficulty configuring WPA2 Enterprise using EAP-PEAP-MSCHAPv2. The administrator has configured the wireless access points properly, and has configured policies on the RADIUS server and configured settings on the client computers. Which of the following is missing?

- A. Client certificates are needed
- B. A third party LEAP client must be installed
- C. A RADIUS server certificate is needed
- D. The use of CCMP rather than TKIP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 395

A business has recently adopted a policy allowing employees to use personal cell phones and tablets to access company email accounts while out of the office. Joe an employee was using a

"Pass Any Exam. Any Time." - www.actualtests.com 712

CompTIA SY0-401 Exam

personal cell phone for email access and was recently terminated. It is suspected that Joe saved confidential client emails on his personal cell phone. Joe claims that the data on the phone is completely personal and refuse to allow the company access to inspect the cell phone. Which of the following is the MOST likely cause of this dispute?

- A. Onboarding procedures
- B. Fair use policy
- C. Device ownership
- D. User acceptance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 396

Mobile tablets are used by employees on the sales floor to access customer data. Ann a customer recently reported that another customer was able to access her personal information on the tablet after the employee left the area. Which of the following would BEST prevent these issues from reoccurring?

- A. Screen Locks
- B. Full-device encryption
- C. Application control
- D. Asset tracking

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 397

Which of the following metrics is important for measuring the extent of data required during backup and recovery?

- A. MOU
- B. ARO
- C. ALE
- D. RPO

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 713
CompTIA SY0-401 Exam

QUESTION 398

Which of the following can be used to ensure that sensitive records stored on a backend server can only be accessed by a front end server with the appropriate record key?

- A. File encryption
- B. Storage encryption
- C. Database encryption
- D. Full disk encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 399

Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?

- A. Access control list
- B. 802.1X
- C. Port security
- D. Load balancers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 400

A company has identified a watering hole attack. Which of the following Best describes this type of attack?

- A. Emails are being spoofed to look like they are internal emails
- B. A cloud storage site is attempting to harvest user IDS and passwords
- C. An online news site is hosting ads in iframes from another site
- D. A local restaurant chains online menu is hosting malicious code

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 714
CompTIA SY0-401 Exam

Explanation:

QUESTION 401

A security manager is discussing change in the security posture of the network, if a proposed application is approved for deployment. Which of the following is the MOST important the security manager must rely upon to help make this determination?

- A. Ports used by new application
- B. Protocols/services used by new application
- C. Approved configuration items
- D. Current baseline configuration

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 402

Joe the system administrator has noticed an increase in network activity from outside sources. He wishes to direct traffic to avoid possible penetration while heavily monitoring the traffic with little to no impact on the current server load. Which of the following would be BEST course of action?

- A. Apply an additional firewall ruleset on the user PCs.
- B. Configure several servers into a honeynet
- C. Implement an IDS to protect against intrusion
- D. Enable DNS logging to capture abnormal traffic

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 403

An assessment tool reports that the company's web server may be susceptible to remote buffer overflow. The web server administrator insists that the finding is a false positive. Which of the following should the administrator do to verify if this is indeed a false positive?

- A. Use a banner grabbing tool
- B. Run a vulnerability scan
"Pass Any Exam. Any Time." - www.actualtests.com 715
CompTIA SY0-401 Exam
- C. Enforce company policies
- D. Perform a penetration test

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 404

The sales force in an organization frequently travel to remote sites and requires secure access to an internal server with an IP address of 192.168.0.220. Assuming services are using default ports, which of the following firewall rules would accomplish this objective? (Select Two)

- A. Permit TCP 20 any 192.168.0.200
- B. Permit TCP 21 any 192.168.0.200
- C. Permit TCP 22 any 192.168.0.200
- D. Permit TCP 110 any 192.168.0.200
- E. Permit TCP 139 any 192.168.0.200
- F. Permit TCP 3389 any 192.168.0.200

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 405

Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?

- A. Deploy a HIDS suite on the users' computer to prevent application installation
- B. Maintain the baseline posture at the highest OS patch level
- C. Enable the pop-up blockers on the user's browsers to prevent malware
- D. Create an approved application list and block anything not on it

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 406

"Pass Any Exam. Any Time." - www.actualtests.com 716

CompTIA SY0-401 Exam

Which of the following will provide data encryption, key management and secure application launching?

- A. TKIP
- B. HSM
- C. EFS
- D. DLP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 407

It is MOST difficult to harden against which of the following?

- A. XSS
- B. Zero-day
- C. Buffer overflow
- D. DoS

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 408

A company has experienced problems with their ISP, which has failed to meet their informally agreed upon level of service. However the business has not negotiated any additional formal agreements beyond the standard customer terms. Which of the following is the BEST document that the company should prepare to negotiate with the ISP?

- A. ISA
- B. SLA
- C. MOU
- D. PBA

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 717
CompTIA SY0-401 Exam

QUESTION 409

A company would like to implement two-factor authentication for its vulnerability management database to require system administrators to use their token and random PIN codes. Which of the following authentication services accomplishes this objective?

- A. SAML
- B. TACACS+
- C. Kerberos
- D. RADIUS

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 410

A company has a corporate infrastructure where end users manage their own certificate keys. Which of the following is considered the MOST secure way to handle master keys associated with these certificates?

- A. Key escrow with key recovery
- B. Trusted first party
- C. Personal Identity Verification
- D. Trusted third party

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 411

A recent audit has revealed that several users have retained permissions to systems they should no longer have rights to after being promoted or changed job positions. Which of the following controls would BEST mitigate this issue?

- A. Separation of duties
- B. User account reviews
- C. Group based privileges
- D. Acceptable use policies

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 718

CompTIA SY0-401 Exam

Explanation:

QUESTION 412

Ann a new security specialist is attempting to access the internet using the company's open wireless network. The wireless network is not encrypted; however, once associated, ANN cannot access the internet or other company resources. In an attempt to troubleshoot, she scans the wireless network with NMAP, discovering the only other device on the wireless network is a firewall. Which of the following BEST describes the company's wireless network solution?

- A. The company uses VPN to authenticate and encrypt wireless connections and traffic
- B. The company's wireless access point is being spoofed
- C. The company's wireless network is unprotected and should be configured with WPA2
- D. The company is only using wireless for internet traffic so it does not need additional encryption

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 413

Which of the following, if implemented, would improve security of remote users by reducing vulnerabilities associated with data-in-transit?

- A. Full-disk encryption
- B. A virtual private network
- C. A thin-client approach
- D. Remote wipe capability

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 414

A company wants to improve its overall security posture by deploying environmental controls in its datacenter. Which of the following is considered an environmental control that can be deployed to meet this goal?

- A. Full-disk encryption
"Pass Any Exam. Any Time." - www.actualtests.com 719
CompTIA SY0-401 Exam
- B. Proximity readers
- C. Hard ward locks
- D. Fire suppression

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 415

A programmer must write a piece of code to encrypt passwords and credit card information used by an online shopping cart. The passwords must be stored using one-way encryption, while credit card information must be stored using reversible encryption. Which of the following should be used to accomplish this task? (Select TWO)

- A. SHA for passwords
- B. 3DES for passwords
- C. RC4 for passwords
- D. AES for credit cards
- E. MD5 for credit cards
- F. HMAC for credit cards

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 416

A company needs to provide a secure backup mechanism for key storage in a PKI. Which of the following should the company implement?

- A. Ephemeral keys
- B. Steganography
- C. Key escrow
- D. Digital signatures

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 417

"Pass Any Exam. Any Time." - www.actualtests.com 720

CompTIA SY0-401 Exam

A security analyst must ensure that the company's web server will not negotiate weak ciphers with connecting web browsers. Which of the following supported list of ciphers MUST the security analyst disable? (Select THREE)

- A. SHA
- B. AES
- C. RIMMED
- D. NULL
- E. DES
- F. MD5
- G. TWOFISH

Correct Answer: AEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 418

A company's application is hosted at a data center. The data center provides security controls for the infrastructure. The data center provides a report identifying several vulnerabilities regarding out of date OS patches. The company recommends the data center assumes the risk associated with the OS vulnerabilities. Which of the following concepts is being implemented?

- A. Risk Transference
- B. Risk Acceptance
- C. Risk Avoidance
- D. Risk Deterrence

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 419

Which of the following cryptographic methods is most secure for a wireless access point?

- A. WPA with LEAP
- B. TKIP
- C. WEP with PSK
- D. WPA2 with PSK

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 721
CompTIA SY0-401 Exam

Explanation:

QUESTION 420

Which of the following is considered an environmental control?

- A. Video surveillance
- B. Proper lighting
- C. EMI shielding
- D. Fencing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 421

An attacker Joe configures his service identifier to be the same as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following Best describes this type of attack?

- A. Bluejacking
- B. WPS attack
- C. Evil twin
- D. War driving
- E. Relay attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 422

A company used a partner company to develop critical components of an application. Several employees of the partner company have been arrested for cybercrime activities. Which of the following should be done to protect the interest of the company?

- A. Perform a penetration test against the application
- B. Conduct a source code review of the application
"Pass Any Exam. Any Time." - www.actualtests.com 722
CompTIA SY0-401 Exam
- C. Perform a baseline review of the application
- D. Scan the application with antivirus and anti-spyware products.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 423

Which of the following is a black box testing methodology?

- A. Code, function, and statement coverage review
- B. Architecture and design review
- C. Application hardening
- D. Penetration testing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 424

A security administrator wishes to prevent certain company devices from using specific access points, while still allowing them on others. All of the access points use the same SSID and wireless password. Which of the following would be MOST appropriate in this scenario?

- A. Require clients to use 802.1x with EAPOL in order to restrict access
- B. Implement a MAC filter on the desired access points
- C. Upgrade the access points to WPA2 encryption
- D. Use low range antennas on the access points that needed to be restricted

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 425

An attacker Joe configures his service identifier to be as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following BEST describes this of attack?

"Pass Any Exam. Any Time." - www.actualtests.com 723
CompTIA SY0-401 Exam

- A. Bluejacking
- B. WPS attack
- C. Evil twin
- D. War driving
- E. Replay attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 426

Which of the following may be used with a BNC connector?

- A. 10GBaseT
- B. 1000BaseSX
- C. 100BaseFX
- D. 10Base2

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 427

A network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST information about the path taken across the network to this website?

- A. Ping
- B. Netstat
- C. telnet
- D. tracer

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 428

A technician is configuring a switch to support VOIP phones. The technician wants to ensure the phones do not require external power packs. Which of the

following would allow the phones to be

"Pass Any Exam. Any Time." - www.actualtests.com 724
CompTIA SY0-401 Exam
powered using the network connection?

- A. PoE+
- B. PBX
- C. PSTN
- D. POTS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 429

A technician reports a suspicious individual is seen walking around the corporate campus. The individual is holding a smartphone and pointing a small antenna, in order to collect SSIDs. Which of the following attacks is occurring?

- A. Rogue AP
- B. Evil Twin
- C. Man-in-the-middle
- D. War driving

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 430

Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?

- A. Proxy server

- B. Spam filter
- C. Network firewall
- D. Application firewall.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 431

"Pass Any Exam. Any Time." - www.actualtests.com 725

CompTIA SY0-401 Exam

A company uses SSH to support internal users. They want to block external SSH connections from reaching internal machines. Which of the following should be blocked on the firewall?

- A. 22
- B. 23
- C. 443
- D. 8080

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 432

If an organization wants to implement a BYOD policy, which of the following administrative control policy considerations MUST be addressed? (Select two)

- A. Data archiving
- B. Data ownership
- C. Geo-tagging
- D. Acceptable use
- E. Remote wipe

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 433

A security technician wants to implement stringent security controls over web traffic by restricting the client source TCP ports allowed through the corporate firewall. Which of the following should the technician implement?

- A. Deny port 80 and 443 but allow proxies
- B. Only allow port 80 and 443
- C. Only allow ports above 1024
- D. Deny ports 80 and allow port 443

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 726
CompTIA SY0-401 Exam

QUESTION 434

An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups? (Select two)

- A. NAC
- B. NAT
- C. Subnetting
- D. VLAN
- E. DMZ
- F. VPN

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 435

A datacenter has suffered repeated burglaries which led to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps were installed to prevent tailgating, the thieves crashed through the wall of datacenter with a vehicle after normal business hours. Which of the following options could improve the safety and security of the datacenter further? (Select two)

- A. Cipher locks
- B. CCTV
- C. Escape routes
- D. K rated fencing
- E. Fm200 fire suppression

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 436

Which of the following can take advantage of man in the middle techniques to prevent data exfiltration?

- A. DNS poisoning
 - B. URL hijacking
 - C. ARP spoofing
 - D. HTTPS inspection
- "Pass Any Exam. Any Time." - www.actualtests.com 727
CompTIA SY0-401 Exam

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 437

An administrator must select an algorithm to encrypt data at rest. Which of the following could be used?

- A. RIPEMD
- B. Diffie-hellman
- C. ECDSA
- D. CHAP
- E. Blowfish

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 438

RC4 is a strong encryption protocol that is general used with which of the following?

- A. WPA2 CCMP
- B. PEAP
- C. WEP
- D. EAP-TLS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 439

An outside security consultant produces a report of several vulnerabilities for a particular server. Upon further investigation, it is determine that the vulnerability reported does not apply to the platform the server is running on. Which of the following should the consultant do in order to produce more accurate results?

"Pass Any Exam. Any Time." - www.actualtests.com 728
CompTIA SY0-401 Exam

- A. A black box test should be used to increase the validity of the scan

- B. Perform a penetration test in addition to a vulnerability scan
- C. Use banner grabbing to identify the target platform
- D. Use baseline reporting to determine the actual configuration

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 440

A programmer has allocated a 32 bit variable to store the results of an operation between two user supplied 4 byte operands. To which of the following types of attack is this application susceptible?

- A. XML injection
- B. Command injection
- C. Integer overflow
- D. Header manipulation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 441

A security administrator is reviewing logs and notices multiple attempts to access the HVAC controls by a workstation with an IP address from the open wireless network. Which of the following would be the best way to prevent this type of attack from occurring again?

- A. Implement VLANs to separate the HVAC
- B. Enable WPA2 security for the wireless network
- C. Install a HIDS to protect the HVAC system
- D. Enable Mac filtering for the wireless network

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 442

An application developer needs to allow employees to use their network credentials to access a new application being developed. Which of the following should be configured in the new

"Pass Any Exam. Any Time." - www.actualtests.com 729

CompTIA SY0-401 Exam

application to enable this functionality?

- A. LDAP
- B. ACLs
- C. SNMP
- D. IPSec

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 443

During a routine audit it is discovered that someone has been using a state administrator account to log into a seldom used server. The person used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could BEST prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policies
- D. Account expiration policies

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 444

A security engineer would like to analyze the effect of deploying a system without patching it to discover potential vulnerabilities. Which of the following practices would best allow for this testing while keeping the corporate network safe?

- A. Perform grey box testing of the system to verify the vulnerabilities on the system
- B. Utilize virtual machine snapshots to restore from compromises
- C. Deploy the system in a sandbox environment on the virtual machine
- D. Create network ACLs that restrict all incoming connections to the system

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 730
CompTIA SY0-401 Exam

QUESTION 445

The internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?

- A. Periodic access review
- B. Group based privileges
- C. Least privilege
- D. Account lockout

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 446

In order to gain an understanding of the latest attack tools being used in the wild, an administrator puts a Unix server on the network with the root users password to set root. Which of the following best describes this technique?

- A. Pharming
- B. Honeypot
- C. Gray box testing
- D. phishing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 447

An administrator, Ann, wants to ensure that only authorized devices are connected to a switch. She decides to control access based on MAC addresses. Which of the following should be configured?

- A. Implicit deny
- B. Private VLANS
- C. Flood guard
- D. Switch port security

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 731

CompTIA SY0-401 Exam

Explanation:

QUESTION 448

A one time security audit revealed that employees do not have the appropriate access to system resources. The auditor is concerned with the fact that most of the accounts audited have unneeded elevated permission to sensitive resources. Which of the following was implemented to detect this issue?

- A. Continuous monitoring
- B. Account review
- C. Group based privileges

D. Credential management

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 449

A security analyst has a sample of malicious software and needs to know what the sample in a carefully controlled and monitored virtual machine to observe the software's behavior. After the software has run, the analyst returns the virtual machines OS to a pre-defined known good state using what feature of virtualization?

- A. Host elasticity
- B. Antivirus
- C. sandbox
- D. snapshots

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 450

Joe, the chief technical officer (CTO) is concerned that the servers and network devices may not be able to handle the growing needs of the company. He has asked his network engineer to begin monitoring the performance of these devices and present statistics to management for capacity planning. Which of the following protocols should be used to this?

"Pass Any Exam. Any Time." - www.actualtests.com 732
CompTIA SY0-401 Exam

- A. SNMP
- B. SSH
- C. TLS
- D. ICMP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 451

A security administrator is responsible for ensuring that there are no unauthorized devices utilizing the corporate network. During a routine scan, the security administrator discovers an unauthorized device belonging to a user in the marketing department. The user is using an android phone in order to browse websites. Which of the following device attributes was used to determine that the device was unauthorized?

- A. An IMEI address
- B. A phone number
- C. A MAC address
- D. An asset ID

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 452

A website is breached, exposing the usernames and MD5 password hashes of its entire user base. Many of these passwords are later cracked using rainbow tables. Which of the following actions could have helped prevent the use of rainbow tables on the password hashes?

- A. use salting when computing MD5 hashes of the user passwords
- B. Use SHA as a hashing algorithm instead of MD5
- C. Require SSL for all user logins to secure the password hashes in transit
- D. Prevent users from using a dictionary word in their password

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 733

QUESTION 453

Joe a network administrator is setting up a virtualization host that has additional storage requirements. Which of the following protocols should be used to connect the device to the company SAN? (Select Two)

- A. Fibre channel
- B. SCP
- C. iSCSI
- D. FDDI
- E. SSL

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 454

A security administrator finds that an intermediate CA within the company was recently breached. The certificates held on this system were lost during the attack, and it is suspected that the attackers had full access to the system. Which of the following is the NEXT action to take in this scenario?

- A. Use a recovery agent to restore the certificates used by the intermediate CA
- B. Revoke the certificate for the intermediate CA
- C. Recover the lost keys from the intermediate CA key escrow
- D. Issue a new certificate for the root CA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 455

A recent online password audit has identified that stale accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?

- A. Password length

- B. Account disablement
- C. Account lockouts
- D. Password complexity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 734
CompTIA SY0-401 Exam

Explanation:

QUESTION 456

The security administrator generates a key pair and sends one key inside a rest file to a third party. The third party sends back a signed file. In this scenario, the file sent by the administrator is

a:

- A. CA
- B. CRL
- C. KEK
- D. PKI
- E. CSR

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 457

Joe, a security technician, is configuring two new firewalls through the web on each. Each time Joe connects, there is a warning message in the browser window about the certificate being untrusted. Which of the following will allow Joe to configure a certificate for the firewall so that firewall administrators are able to connect both firewalls without experiencing the warning message?

- A. Apply a permanent override to the certificate warning in the browser
- B. Apply a wildcard certificate obtained from the company's certificate authority

- C. Apply a self-signed certificate generated by each of the firewalls
- D. Apply a single certificate obtained from a public certificate authority

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 458

A company has had their web application become unavailable several times in the past few months due to increased demand. Which of the following should the company perform to increase availability?

"Pass Any Exam. Any Time." - www.actualtests.com 735
CompTIA SY0-401 Exam

- A. Implement a web application firewall to prevent DDoS attacks'
- B. Configure the firewall to work with the IPS to rate limit customer requests
- C. Implement a load balancer to distribute traffic based on back end server utilization
- D. Configure the web server to detect race conditions and automatically restart the web services

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 459

A system administrator wants to prevent password compromises from offline password attacks. Which of the following controls should be configured to BEST accomplish this task? (Select TWO)

- A. Password reuse
- B. Password length
- C. Password complexity
- D. Password history
- E. Account lockouts

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 460

A company recently experienced several security breaches that resulted in confidential data being infiltrated from the network. The forensic investigation revealed that the data breaches were caused by an insider accessing files that resided in shared folders who then encrypted the data and sent it to contacts via third party email. Management is concerned that other employees may also be sending confidential files outside of the company to the same organization. Management has requested that the IT department implement a solution that will allow them to:

Track access and use of files marked confidential, provide documentation that can be used for investigations, prevent employees from sending confidential data via secure third party email, identify other employees that may be involved in these activities.

Which of the following would be the best choice to implement to meet the above requirements?

- A. Web content filtering capable of inspecting and logging SSL traffic used by third party webmail providers
- B. Full disk encryption on all computers with centralized event logging and monitoring enabled
- C. Host based firewalls with real time monitoring and logging enabled "Pass Any Exam. Any Time." - www.actualtests.com 736
CompTIA SY0-401 Exam
- D. Agent-based DLP software with correlations and logging enabled

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 461

Which of the following BEST describes malware that tracks a user's web browsing habits and injects the attacker's advertisements into unrelated web pages?
(Select TWO)

- A. Logic bomb
- B. Backdoor
- C. Ransomware
- D. Adware

- E. Botnet
- F. Spyware

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 462

The chief security officer (CSO) has issued a new policy to restrict generic or shared accounts on company systems. Which of the following sections of the policy requirements will have the most impact on generic and shared accounts?

- A. Account lockout
- B. Password length
- C. Concurrent logins
- D. Password expiration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 463

Joe an end user has received a virus detection warning. Which of the following is the first course of action that should be taken?

"Pass Any Exam. Any Time." - www.actualtests.com 737
CompTIA SY0-401 Exam

- A. Recovery
- B. Reporting
- C. Remediation
- D. Identification

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 464

A company has several public conference room areas with exposed network outlets. In the past, unauthorized visitors and vendors have used the outlets for internet access. The help desk manager does not want the outlets to be disabled due to the number of training sessions in the conference room and the amount of time it takes to get the ports either patched in or enabled. Which of the following is the best option for meeting this goal?

- A. Flood guards
- B. Port security
- C. 802.1x
- D. Loop protection
- E. IPSec

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 465

An attacker unplugs the access point at a coffee shop. The attacker then runs software to make a laptop look like an access point and advertises the same network as the coffee shop normally does. Which of the following describes this type of attack?

- A. IV
- B. Xmas
- C. Packet sniffing
- D. Evil twin
- E. Rouge AP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 466

A network administrator argues that WPA2 encryption is not needed, as MAC filtering is enabled on the access point. Which of the following would show the administrator that wpa2 is also needed?

- A. Deploy an evil twin with mac filtering
- B. Flood access point with random mac addresses
- C. Sniff and clone a mac address
- D. DNS poison the access point

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 467

A security director has contracted an outside testing company to evaluate the security of a newly developed application. None of the parameters or internal workings of the application have been provided to the testing company prior to the start of testing. The testing company will be using:

- A. Gray box testing
- B. Active control testing
- C. White box testing
- D. Black box testing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 468

While preparing for an audit a security analyst is reviewing the various controls in place to secure the operation of financial processes within the organization. Based on the pre assessment report, the department does not effectively maintain a strong financial transaction control environment due to conflicting responsibilities held by key personnel. If implemented, which of the following security concepts will most effectively address the finding?

- A. Least privilege
 - B. Separation of duties
 - C. Time-based access control
 - D. Dual control
- "Pass Any Exam. Any Time." - www.actualtests.com 739
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 469

A chief privacy officer, Joe, is concerned that employees are sending emails to addresses outside of the company that contain PII. He asks that the security technician to implement technology that will mitigate this risk. Which of the following would be the best option?

- A. DLP
- B. HIDS
- C. Firewall
- D. Web content filtering

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 470

The key management organization has implemented a key escrowing function. Which of the following technologies can provide protection for the PKI's escrowed keys?

- A. CRL
- B. OCSP
- C. TPM
- D. HSM

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 471

Which of the following are unique to white box testing methodologies? (Select two)

- A. Application program interface API testing
 - B. Bluesnarfing
 - C. External network penetration testing
 - D. Function, statement and code coverage
 - E. Input fuzzing
- "Pass Any Exam. Any Time." - www.actualtests.com 740
CompTIA SY0-401 Exam

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 472

A technician installed two ground plane antennae on 802.11n bridges connecting two buildings 500 feet apart. After configuring both radios to work at 2.4ghz and implementing the correct configuration, connectivity tests between the two buildings are unsuccessful. Which of the following should the technician do to resolve the connectivity problem?

- A. Substitute wireless bridges for wireless access points
- B. Replace the 802.11n bridges with 802.11ac bridges
- C. Configure both bridges to use 5GHz instead of 2.4GHz
- D. Replace the current antennae with Yagi antennae

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 473

A company has had several security incidents in the past six months. It appears that the majority of the incidents occurred on systems with older software on development workstations. Which of the following should be implemented to help prevent similar incidents in the future?

- A. Peer code review
- B. Application whitelisting
- C. Patch management
- D. Host-based firewall

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 474

A router was shut down as a result of a DoS attack. Upon review of the router logs, it was determined that the attacker was able to connect to the router using a console cable to complete the attack. Which of the following should have been implemented on the router to prevent this

"Pass Any Exam. Any Time." - www.actualtests.com 741

CompTIA SY0-401 Exam

attack? (Select two)

- A. IP ACLs should have been enabled on the console port on the router
- B. Console access to the router should have been disabled
- C. Passwords should have been enabled on the virtual terminal interfaces on the router
- D. Virtual terminal access to the router should have been disabled
- E. Physical access to the router should have been restricted

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 475

A systems administrator is configuring a new file server and has been instructed to configure writeable to by the department manager, and read only for the individual employee. Which of the following is the name for the access control methodology used?

- A. Duty separation
- B. Mandatory
- C. Least privilege
- D. Role-based

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 476

An administrator is implementing a security control that only permits the execution of allowed programs. Which of the following are cryptography concepts that should be used to identify the allowed programs? (Select two.)

- A. Digital signatures
- B. Hashing
- C. Asymmetric encryption
- D. openID
- E. key escrow

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 742
CompTIA SY0-401 Exam

QUESTION 477

While responding to an incident on a Linux server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

- A. Lsof
- B. Tcpdump
- C. Top
- D. Ifconfig

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 478

A bank chief information security officer (CISO) is responsible for a mobile banking platform that operates natively on iOS and Android. Which of the following security controls helps protect the associated publicly accessible API endpoints?

- A. Mobile device management
- B. Jailbreak detection
- C. Network segmentation
- D. Application firewalls

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 479

A company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a:

- A. Vulnerability assessment
- B. White box test
- C. Penetration test

"Pass Any Exam. Any Time." - www.actualtests.com 743

CompTIA SY0-401 Exam

D. Peer review

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 480

Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is Joe attempting to complete?

- A. Black hat testing
- B. Vulnerability scanning
- C. Black box testing
- D. Penetration testing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 481

A classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?

- A. The maximum-mac settings of the ports should be set to zero
- B. The maximum-mac settings of the ports should be set to one
- C. The maximum-mac settings of the ports should be set to two
- D. The maximum mac settings of the ports should be set to three

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 482

Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

"Pass Any Exam. Any Time." - www.actualtests.com 744

CompTIA SY0-401 Exam

- A. Replay
- B. Smurf
- C. Xmas
- D. Fraggle

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 483

A Company transfers millions of files a day between their servers. A programmer for the company has created a program that indexes and verifies the integrity of each file as it is replicated between servers. The programmer would like to use the fastest algorithm to ensure integrity. Which of the following should the programmer use?

- A. SHA1
- B. RIPEMD
- C. DSA
- D. MD5

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 484

A system administrator is conducting baseline audit and determines that a web server is missing several critical updates. Which of the following actions should the administrator perform first to correct the issue?

- A. Open a service ticket according to the patch management plan
- B. Disconnect the network interface and use the administrative management console to perform the updates
- C. Perform a backup of the server and install the require patches
- D. Disable the services for the web server but leave the server alone pending patch updates

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 745
CompTIA SY0-401 Exam

QUESTION 485

The IT department has been tasked with reducing the risk of sensitive information being shared with unauthorized entities from computers it is saved on, without impeding the ability of the employees to access the internet. Implementing which of the following would be the best way to accomplish this objective?

- A. Host-based firewalls
- B. DLP
- C. URL filtering
- D. Pop-up blockers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 486

A server crashes at 6 pm. Senior management has determined that data must be restored within two hours of a server crash. Additionally, a loss of more than one hour worth of data is detrimental to the company's financial well-being. Which of the following is the RTO?

- A. 7pm

- B. 8pm
- C. 9pm
- D. 10pm

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 487

To mitigate the risk of intrusion, an IT Manager is concerned with using secure versions of protocols and services whenever possible. In addition, the security technician is required to monitor the types of traffic being generated. Which of the following tools is the technician MOST likely to use?

- A. Port scanner
- B. Network analyzer
- C. IPS
- D. Audit Logs

"Pass Any Exam. Any Time." - www.actualtests.com 746
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 488

An administrator is implementing a new management system for the machinery on the company's production line. One requirement is that the system only be accessible while within the production facility. Which of the following will be the MOST effective solution in limiting access based on this requirement?

- A. Access control list
- B. Firewall policy
- C. Air Gap
- D. MAC filter

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 489

A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

- A. The CPS utilizes encryption for data at rest and in motion
- B. The CSP takes into account multinational privacy concerns
- C. The financial review indicates the company is a startup
- D. SLA state service tickets will be resolved in less than 15 minutes

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 490

A company wishes to prevent unauthorized employee access to the data center. Which of the following is the MOST secure way to meet this goal?



<http://www.gratisexam.com/>

- A. Use Motion detectors to signal security whenever anyone entered the center
- B. Mount CCTV cameras inside the center to monitor people as they enter "Pass Any Exam. Any Time." - www.actualtests.com 747
CompTIA SY0-401 Exam
- C. Install mantraps at every entrance to the data center in conjunction with their badges
- D. Place biometric readers at the entrances to verify employees' identity

Correct Answer: C

<http://www.gratisexam.com/>

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 491

A company hosts a web server that requires entropy in encryption initialization and authentication. To meet this goal, the company would like to select a block cipher mode of operation that allows an arbitrary length IV and supports authenticated encryption. Which of the following would meet these objectives?

- A. CFB
- B. GCM
- C. ECB
- D. CBC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 492

A chief information security officer (CISO) is providing a presentation to a group of network engineers. In the presentation, the CISO presents information regarding exploit kits. Which of the following might the CISO present?

- A. Exploit kits are tools capable of taking advantage of multiple CVEs
- B. Exploit kits are vulnerability scanners used by penetration testers
- C. Exploit kits are WIFI scanning tools that can find new honeypots
- D. Exploit kits are a new type of malware that allow attackers to control their computers

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 493

During a company-wide initiative to harden network security, it is discovered that end users who have laptops cannot be removed from the local administrator group. Which of the following could

"Pass Any Exam. Any Time." - www.actualtests.com 748

CompTIA SY0-401 Exam

be used to help mitigate the risk of these machines becoming compromised?

- A. Security log auditing
- B. Firewalls
- C. HIPS
- D. IDS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 494

An administrator receives a security alert that appears to be from one of the company's vendors. The email contains information and instructions for patching a serious flaw that has not been publicly announced. Which of the following can an employee use to validate the authenticity of the email?

- A. Hashing algorithm
- B. Ephemeral Key
- C. SSL certificate chain
- D. Private key
- E. Digital signature

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 495

A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the

following would be added requirements will satisfy the regulatory requirement? (Select THREE.)

- A. Digital certificate
- B. Personalized URL
- C. Identity verification questions
- D. Keystroke dynamics
- E. Tokenized mobile device
- F. Time-of-day restrictions
- G. Increased password complexity
- H. Rule-based access control

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 496

A bank is planning to implement a third factor to protect customer ATM transactions. Which of the following could the bank implement?

- A. SMS
- B. Fingerprint
- C. Chip and Pin
- D. OTP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 497

Which of the following internal security controls is aimed at preventing two system administrators from completing the same tasks?

- A. Least privilege
- B. Separation of Duties
- C. Mandatory Vacation
- D. Security Policy

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 498

An administrator performs a risk calculation to determine if additional availability controls need to be in place. The administrator estimates that a server fails and needs to be replaced once every 2 years at a cost of \$8,000. Which of the following represents the factors that the administrator would use to facilitate this calculation?

"Pass Any Exam. Any Time." - www.actualtests.com 750
CompTIA SY0-401 Exam

- A. ARO= 0.5; SLE= \$4,000; ALE= \$2,000
- B. ARO=0.5; SLE=\$8,000; ALE=\$4,000
- C. ARO=0.5; SLE= \$4,000; ALE=\$8,000
- D. ARO=2; SLE= \$4,000; ALE=\$8,000
- E. ARO=2; SLE= \$8,000; ALE= \$16,000

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 499

A security administrator needs to implement a technology that creates a secure key exchange. Neither party involved in the key exchange will have pre-existing knowledge of one another. Which of the following technologies would allow for this?

- A. Blowfish
- B. NTLM

- C. Diffie-Hellman
- D. CHAP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 500

A technician has been assigned a service request to investigate a potential vulnerability in the organization's extranet platform. Once the technician performs initial investigative measures, it is determined that the potential vulnerability was a false-alarm. Which of the following actions should the technician take in regards to the findings?

- A. Write up the findings and disable the vulnerability rule in future vulnerability scans
- B. Refer the issue to the server administrator for resolution
- C. Mark the finding as a false-negative and close the service request
- D. Document the results and report the findings according to the incident response plan

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 751
CompTIA SY0-401 Exam

QUESTION 501

A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program. Which of the following attacks is this an example of?

- A. WPS
- B. IV
- C. Deauth
- D. Replay

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 502

A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?

- A. Setup the email security with her new certificates
- B. Recover her old private certificate
- C. Reinstall her previous public certificate
- D. Verify the correct email address is associated with her certificate

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 503

Which of the following is a best practice when setting up a client to use the LDAPS protocol with a server?

- A. The client should follow LDAP referrals to other secure servers on the network
- B. The client should trust the CA that signed the server's certificate
- C. The client should present a self-signed certificate to the server
- D. The client should have access to port 389 on the server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 752

QUESTION 504

A network manager needs a cost-effective solution to allow for the restoration of information with a RPO of 24 hours. The disaster recovery plan also requires that backups occur within a restricted timeframe during the week and be take offsite weekly. Which of the following should the manager choose to BEST address these requirements?

- A. Daily incremental backup to tape
- B. Disk-to-disk hourly server snapshots
- C. Replication of the environment at a hot site
- D. Daily differential backup to tape
- E. Daily full backup to tape

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 505

Given the following set of firewall rules:

From the inside to outside allow source any destination any port any

From inside to dmz allow source any destination any port tcp-80

From inside to dmz allow source any destination any port tcp-443

Which of the following would prevent FTP traffic from reaching a server in the DMZ from the inside network?

- A. Implicit deny
- B. Policy routing
- C. Port forwarding
- D. Forwarding proxy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 753
CompTIA SY0-401 Exam

QUESTION 506

During a routine configuration audit, a systems administrator determines that a former employee placed an executable on an application server. Once the system was isolated and diagnosed, it was determined that the executable was programmed to establish a connection to a malicious command and control server. Which of the following forms of malware is best described in the scenario?

- A. Logic bomb
- B. Rootkit
- C. Back door
- D. Ransomware

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 507

The chief information officer (CIO) of a major company intends to increase employee connectivity and productivity by issuing employees mobile devices with access to their enterprise email, calendar, and contacts. The solution the CIO intends to use requires a PKI that automates the enrollment of mobile device certificates. Which of the following, when implemented and configured securely, will meet the CIO's requirement?

- A. OCSP
- B. SCEP
- C. SAML
- D. OSI

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 508

An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fine. Which of the following reasons make this effective? (Select two.)

- A. Consensus
 - B. Authority
 - C. Intimidation
 - D. Trust
 - E. Scarcity
- "Pass Any Exam. Any Time." - www.actualtests.com 754
CompTIA SY0-401 Exam

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 509

In the course of troubleshooting wireless issues from users a technician discovers that users are connecting to their home SSIDs which the technician scans but detects none of these SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

- A. Configure the device to verify access point MAC addresses
- B. Disable automatic connection to known SSIDs
- C. Only connect to trusted wireless networks
- D. Enable MAC filtering on the wireless access point

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 510

Which of the following describes the implementation of PAT?

- A. Translating the source and destination IPS, but not the source and destination ports
- B. A one to one persistent mapping between on private IP and one Public IP
- C. Changing the priority of a TCP stream based on the source address
- D. Associating multiple public IP addresses with one private address

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 511

Which of the following forms of software testing can best be performed with no knowledge of how a system is internally structured or functions? (Select Two.)

- A. Boundary testing
"Pass Any Exam. Any Time." - www.actualtests.com 755
CompTIA SY0-401 Exam
- B. White box
- C. Fuzzing
- D. Black box
- E. Grey Box

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 512

A load balancer has the ability to remember which server a particular client is using and always directs that client to the same server. This feature is called:

- A. Cookie tracking
- B. URL filtering
- C. Session affinity
- D. Behavior monitoring

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 513

A company has recently begun to provide internal security awareness for employees. Which of the following would be used to demonstrate the effectiveness of the training?

- A. Metrics
- B. Business impact analysis
- C. Certificate of completion
- D. Policies

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 514

Users in an organization are experiencing when attempting to access certain websites. The users report that when they type in a legitimate URL, different boxes appear on the screen, making it difficult to access the legitimate sites. Which of the following would best mitigate this issue?

"Pass Any Exam. Any Time." - www.actualtests.com 756
CompTIA SY0-401 Exam

- A. Pop-up blockers
- B. URL filtering
- C. Antivirus
- D. Anti-spam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 515

A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

- A. Static analysis
- B. Gray Box
- C. White box
- D. Black box

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 516

A web administrator has just implemented a new web server to be placed in production. As part of the company's security plan, any new system must go through a security test before it is placed in production. The security team runs a port scan resulting in the following data:

- 21 tcp open FTP
- 23 tcp open Telnet
- 22 tcp open SSH
- 25 UDP open smtp
- 110 tcp open pop3
- 443 tcp open https

Which of the following is the BEST recommendation for the web administrator?

"Pass Any Exam. Any Time." - www.actualtests.com 757
CompTIA SY0-401 Exam

- A. Implement an IPS
- B. Disable unnecessary services
- C. Disable unused accounts
- D. Implement an IDS
- E. Wrap TELNET in SSL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 517

Which of the following best describes the reason for using hot and cold aisles?

- A. To ensure air exhaust from one aisle doesn't blow into the air intake of the next aisle
- B. To ensure the dewpoint stays low enough that water doesn't condensate on equipment
- C. To decrease amount of power wiring that is run to each aisle
- D. To maintain proper humidity in the datacenter across all aisles

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 518

An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizing the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?

- A. EAP-FAST
- B. LEAP
- C. PEAP
- D. EAP-TLS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 519

An attacker is attempting to insert malicious code into an installer file that is available on the

"Pass Any Exam. Any Time." - www.actualtests.com 758

CompTIA SY0-401 Exam

internet. The attacker is able to gain control of the web server that houses both the installer and the web page which features information about the downloadable file. To implement the attack and delay detection, the attacker should modify both the installer file and the:

- A. SSL certificate on the web server
- B. The HMAC of the downloadable file available on the website
- C. Digital signature on the downloadable file
- D. MD5 hash of the file listed on the website

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 520

After receiving the hard drive from detectives, the forensic analyst for a court case used a log to capture corresponding events prior to sending the evidence to lawyers. Which of the following do these actions demonstrate?

- A. Chain of custody
- B. Order of volatility
- C. Data analysis
- D. Tracking man hours and expenses

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 521

A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?

- A. Mandatory access control
- B. Rule-based access
- C. Group based privileges
- D. User assigned privileges

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 759
CompTIA SY0-401 Exam

QUESTION 522

Which of the following technologies when applied to android and iOS environments, can an organization use to add security restrictions and encryption to existing mobile applications? (Select Two)

- A. Mobile device management
- B. Containerization
- C. Application whitelisting
- D. Application wrapping
- E. Mobile application store

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 523

A server administrator discovers the web farm is using weak ciphers and wants to ensure that only stronger ciphers are accepted. Which of the following ciphers should the administrator implement in the load balancer? (Select Two)

- A. SHA-129
- B. DES
- C. MD5
- D. RC4
- E. CRC-32

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 524

An application developer has coded a new application with a module to examine all user entries for the graphical user interface. The module verifies that user entries match the allowed types for each field and that OS and database commands are rejected before entries are sent for further processing within the application. These are example of:

- A. Input validation
"Pass Any Exam. Any Time." - www.actualtests.com 760
CompTIA SY0-401 Exam
- B. SQL injection
- C. Application whitelisting
- D. Error handling

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 525

Ann, a security administrator is hardening the user password policies. She currently has the following in place.

Passwords expire every 60 days

Password length is at least eight characters

Passwords must contain at least one capital letter and one numeric character

Passwords cannot be reused until the password has been changed eight times

She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?

- A. Lower the password expiry time to every 30days instead of every 60 days
- B. Require that the password contains at least one capital, one numeric, and one special character
- C. Change the re-usage time from eight to 16 changes before a password can be repeated
- D. Create a rule that users can only change their passwords once every two weeks

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 526

Which of the following BEST describes disk striping with parity?

- A. RAID 0
- B. RAID 1
- C. RAID 2
- D. RAID 5

"Pass Any Exam. Any Time." - www.actualtests.com 761
CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 527

Which of the following will allow the live state of the virtual machine to be easily reverted after a failed upgrade?

- A. Replication
- B. Backups
- C. Fault tolerance
- D. Snapshots

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 528

An organization currently uses FTP for the transfer of large files, due to recent security enhancements, is now required to use a secure method of file transfer and is testing both SFTP and FTPS as alternatives. Which of the following ports should be opened on the firewall in order to test the two alternatives? (Select Two)

- A. TCP 22
- B. TCP 25
- C. TCP 69
- D. UDP 161
- E. TCP 990
- F. TCP 3380

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 529

Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?

"Pass Any Exam. Any Time." - www.actualtests.com 762
CompTIA SY0-401 Exam

- A. Armored virus
- B. Ransomware
- C. Trojan
- D. Keylogger

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 530

An attacker went to a local bank and collected disposed paper for the purpose of collecting data that could be used to steal funds and information from the bank's customers. This is an example of:

- A. Impersonation
- B. Whaling
- C. Dumpster diving
- D. Hoaxes

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 531

An employee reports work was being completed on a company owned laptop using a public wireless hot-spot. A pop-up screen appeared and the user closed the pop-up. Seconds later the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

- A. Ransomware
- B. Rootkit
- C. Scareware
- D. Spyware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 763

CompTIA SY0-401 Exam

QUESTION 532

A small IT security firm has an internal network composed of laptops, servers, and printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

- A. Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building.
- B. Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access.
- C. Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers.
- D. Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment; install CCTVs to deter social engineering; enable SELinux in permissive mode.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 533

A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open standard for the exchange of authentication and authorization across numerous web based applications. Which of the following solutions is most appropriate for the analyst to recommend in this scenario?

- A. SAML
- B. XTACACS
- C. RADIUS
- D. TACACS+

E. Secure LDAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 534

A thief has stolen mobile device and removed its battery to circumvent GPS location tracking. The device user is a four digit PIN. Which of the following is a mobile device security control that

"Pass Any Exam. Any Time." - www.actualtests.com 764

CompTIA SY0-401 Exam

ensures the confidentiality of company data?

- A. Remote wiping
- B. Mobile Access control
- C. Full device encryption
- D. Inventory control

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 535

A user has called the help desk to report an enterprise mobile device was stolen. The technician receiving the call accesses the MDM administration portal to identify the device's last known geographic location. The technician determines the device is still communicating with the MDM. After taking note of the last known location, the administrator continues to follow the rest of the checklist. Which of the following identifies a possible next step for the administrator?

- A. Remotely encrypt the device
- B. Identify the mobile carrier's IP address
- C. Reset the device password
- D. Issue a remote wipe command

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 536

A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

- A. Deterrence
- B. Transference
- C. Avoidance
- D. Acceptance
- E. sharing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 765

CompTIA SY0-401 Exam

Explanation:

QUESTION 537

During a recent audit, the auditors cited the company's current virtual machine infrastructure as a concern. The auditors cited the fact that servers containing sensitive customer information reside on the same physical host as numerous virtual machines that follow less stringent security guidelines. Which of the following would be the best choice to implement to address this audit concern while maintain the current infrastructure?

- A. Migrate the individual virtual machines that do not contain sensitive data to separate physical machines
- B. Implement full disk encryption on all servers that do not contain sensitive customer data
- C. Move the virtual machines that contain the sensitive information to a separate host
- D. Create new VLANs and segment the network according to the level of data sensitivity

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 538

A switch is set up to allow only 2 simultaneous MAC addresses per switch port. An administrator is reviewing a log and determines that a switch port has been deactivated in a conference room after it detected 3 or more MAC addresses on the same port. Which of the following reasons could have caused this port to be disabled?

- A. A pc had a NIC replaced and reconnected to the switch
- B. An ip telephone has been plugged in
- C. A rouge access point was plugged in
- D. An arp attack was launched from a pc on this port

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 539

A network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and

"Pass Any Exam. Any Time." - www.actualtests.com 766

CompTIA SY0-401 Exam

UDP protocols. Which of the following network controls would meet these requirements?

- A. Stateful firewall
- B. Web security gateway
- C. URL filter
- D. proxy server
- E. web application firewall

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 540

Client computers login at specified times to check and update antivirus definitions using a dedicated account configured by the administrator. One day the clients are unable to login with the account, but the server still responds to ping requests. The administrator has not made any changes. Which of the following most likely happened?

- A. Group policy is blocking the connection attempts
- B. The administrator account has been disabled
- C. The switch port for the server has died
- D. The password on the account has expired

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 541

In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?

- A. Protocol analyzer
- B. Banner grabbing
- C. Port scanning
- D. Code review

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 767
CompTIA SY0-401 Exam

QUESTION 542

a company is deploying an new video conferencing system to be used by the executive team for board meetings. The security engineer has been asked to choose the strongest available asymmetric cipher to be used for encryption of board papers, and chose the strongest available stream cipher to be configured for video streaming. Which of the following ciphers should be chosen? (Select two)

- A. RSA
- B. RC4
- C. 3DES
- D. HMAC
- E. SJA-256

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 543

Joe has hired several new security administrators and have been explaining the design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

- A. Load balancers
- B. Defense in depth
- C. Network segmentation
- D. UTM security appliance

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 544

A security administrator is selecting an MDM solution for an organization, which has strict security requirements for the confidentiality of its data on end user devices. The organization decides to allow BYOD, but requires that users wishing to participate agree to the following specific device configurations; camera disablement, password enforcement, and application whitelisting. The organization must be able to support a device portfolio of differing mobile operating systems.

"Pass Any Exam. Any Time." - www.actualtests.com 768

CompTIA SY0-401 Exam

Which of the following represents the MOST relevant technical security criteria for the MDM?

- A. Breadth of support for device manufacturers' security configuration APIs
- B. Ability to extend the enterprise password policies to the chosen MDM
- C. Features to support the backup and recovery of the stored corporate data
- D. Capability to require the users to accept an AUP prior to device onboarding

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 545

Employees are reporting that they have been receiving a large number of emails advertising products and services. Links in the email direct the users' browsers to the websites for the items being offered. No reports of increased virus activity have been observed. A security administrator suspects that the users are the targets of:

- A. A watering hole attack
- B. Spear phishing
- C. A spoofing attack
- D. A spam campaign

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 546

An employee finds a usb drive in the employee lunch room and plugs the drive into a shared workstation to determine who owns the drive. When the drive is inserted, a command prompt opens and a script begins to run. The employee notifies a technician who determines that data on a server have been compromised. This is an example of:

- A. Device removal
- B. Data disclosure
- C. Incident identification
- D. Mitigation steps

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 769
CompTIA SY0-401 Exam

QUESTION 547

A chief information officer (CIO) is concerned about PII contained in the organization's various data warehouse platforms. Since not all of the PII transferred to the organization is required for proper operation of the data warehouse application, the CIO requests the in needed PII data be parsed and securely discarded. Which of the following controls would be MOST appropriate in this scenario?

- A. Execution of PII data identification assessments
- B. Implementation of data sanitization routines
- C. Encryption of data-at-rest
- D. Introduction of education programs and awareness training
- E. Creation of policies and procedures

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 548

The security administrator receives a service ticket saying a host based firewall is interfering with the operation of a new application that is being tested in development. The administrator asks for clarification on which ports need to be open. The software vendor replies that it could use up to 20 ports and many customers have disabled the host based firewall. After examining the system the administrator sees several ports that are open for database and application servers that only used locally. The vendor continues to recommend disabling the host based firewall. Which of the following is the best course of action for the administrator to take?

- A. Allow ports used by the application through the network firewall
- B. Allow ports used externally through the host firewall
- C. Follow the vendor recommendations and disable the host firewall
- D. Allow ports used locally through the host firewall

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 549

A corporate wireless guest network uses an open SSID with a captive portal to authenticate guest users. Guests can obtain their portal password at the service desk. A security consultant alerts the

"Pass Any Exam. Any Time." - www.actualtests.com 770

CompTIA SY0-401 Exam

administrator that the captive portal is easily bypassed, as long as one other wireless guest user is on the network. Which of the following attacks did the security consultant use?

- A. ARP poisoning
- B. DNS cache poisoning
- C. MAC spoofing
- D. Rouge DHCP server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 550

A company requires that all wireless communication be compliant with the Advanced encryption standard. The current wireless infrastructure implements WEP + TKIP. Which of the following wireless protocols should be implemented?

- A. CCMP

- B. 802.1x
- C. 802.3
- D. WPA2
- E. AES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 551

A security analyst, while doing a security scan using packet capture security tools, noticed large volumes of data images of company products being exfiltrated to foreign IP addresses. Which of the following is the FIRST step in responding to scan results?

- A. Incident identification
- B. Implement mitigation
- C. Chain of custody
- D. Capture system image

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 771

CompTIA SY0-401 Exam

QUESTION 552

An administrator deploys a WPA2 Enterprise wireless network with EAP-PEAP-MSCHAPv2. The deployment is successful and company laptops are able to connect automatically with no user intervention. A year later, the company begins to deploy phones with wireless capabilities. Users report that they are receiving a warning when they attempt to connect to the wireless network from their phones. Which of the following is the MOST likely cause of the warning message?

- A. Mutual authentication on the phone is not compatible with the wireless network
- B. The phones do not support WPA2 Enterprise wireless networks
- C. User certificates were not deployed to the phones

- D. The phones' built in web browser is not compatible with the wireless network
- E. Self-signed certificates were used on the RADIUS servers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 553

An attacker has gained access to the company's web server by using the administrator's credentials. The attacker then begins to work on compromising the sensitive data on other servers. Which off the following BEST describes this type of attack?

- A. Privilege escalation
- B. Client-side attack
- C. Man-in-the-middle
- D. Transitive access

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 554

A security technician is concerned there4 is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?

- A. HIPS & SIEM
"Pass Any Exam. Any Time." - www.actualtests.com 772
CompTIA SY0-401 Exam
- B. NIPS & HIDS
- C. HIDS& SIEM
- D. NIPS&HIPS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 555

Which of the following best describes the objectives of succession planning?

- A. To identify and document the successive order in which critical systems should be reinstated following a disaster situation
- B. To ensure that a personnel management plan is in place to ensure continued operation of critical processes during an incident
- C. To determine the appropriate order in which contract internal resources, third party suppliers and external customers during a disaster response
- D. To document the order that systems should be reinstated at the primary site following a failover operation at a backup site.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 556

A system administrator wants to use open source software but is worried about the source code being comprised. As a part of the download and installation process, the administrator should verify the integrity of the software by:

- A. Creating a digital signature of the file before installation
- B. Using a secure protocol like HTTPS to download the file
- C. Checking the hash against an official mirror that contains the same file
- D. Encryption any connections the software makes

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 557

"Pass Any Exam. Any Time." - www.actualtests.com 773

CompTIA SY0-401 Exam

The chief security officer (CSO) has reported a rise in data loss but no break-ins have occurred. By doing which of the following would the CSO MOST likely to

reduce the number of incidents?

- A. Implement protected distribution
- B. Employ additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 558

In an effort to test the effectiveness of an organization's security awareness training, a penetrator tester crafted an email and sent it to all of the employees to see how many of them clicked on the enclosed links. Which of the following is being tested?

- A. How many employees are susceptible to a SPAM attack
- B. How many employees are susceptible to a cross-site scripting attack
- C. How many employees are susceptible to a phishing attack
- D. How many employees are susceptible to a vishing attack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 559

Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?

- A. Application firewall
- B. IPSec
- C. Hardware encryption
- D. VLANs

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 774

CompTIA SY0-401 Exam

QUESTION 560

When information is shared between two separate organizations, which of the following documents would describe the sensitivity as well as the type and flow of the information?

- A. SLA
- B. ISA
- C. BPA
- D. MOA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 561

Joe noticed that there is a larger than normal account of network on the printer VLAN of his organization, causing users to have to wait a long time for a print job. Upon investigation Joe discovers that printers were ordered and added to the network without his knowledge. Which of the following will reduce the risk of this occurring again in the future?

- A. Log analysis
- B. Loop protection
- C. Access control list
- D. Rule-based management

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 562

Jo an employee reports to the security manager that several files in a research and development folder that only JOE has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?

- A. Generic account prohibition
- B. Account lockout
- C. Password complexity
"Pass Any Exam. Any Time." - www.actualtests.com 775
CompTIA SY0-401 Exam
- D. User access reviews

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 563

A user contacts the help desk after being unable to log in to a corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has user restart the NTP service. Afterwards the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?

- A. Secure LDAP
- B. RADIUS
- C. NTLMv2
- D. Kerberos

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 564

A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a, malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

- A. DNS poisoning
- B. XSS
- C. Iframe
- D. Session hijacking

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 776

CompTIA SY0-401 Exam

QUESTION 565

A news and weather toolbar was accidentally installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?

- A. Man-in-the-browser
- B. Flash cookies
- C. Session hijacking
- D. Remote code execution
- E. Malicious add-on

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 566

A project manager is working with an architectural firm that focuses on physical security. The project manager would like to provide requirements that support the

primary goal of safety. Based on the project manager's desires, which of the following controls would the BEST to incorporate into the facility design?

- A. Biometrics
- B. Escape routers
- C. Reinforcements
- D. Access controls

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 567

While performing surveillance activities an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security controls?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

"Pass Any Exam. Any Time." - www.actualtests.com 777

CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 568

An administrator wants to configure a switch port so that it separates voice and data traffic. Which of the following MUST be configured on the switch port to enforce separation of traffic?

- A. DMZ
- B. VLAN
- C. Subnetting

D. NAC

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 569

A company must send sensitive data over a non-secure network via web services. The company suspects that competitors are actively trying to intercept all transmissions. Some of the information may be valuable to competitors, even years after it has been sent. Which of the following will help mitigate the risk in the scenario?

- A. Digitally sign the data before transmission
- B. Choose stream ciphers over block ciphers
- C. Use algorithms that allow for PFS
- D. Enable TLS instead of SSL
- E. Use a third party for key escrow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 570

When implementing a mobile security strategy for an organization which of the following is the MOST influential concern that contributes to that organization's ability to extend enterprise policies to mobile devices?

"Pass Any Exam. Any Time." - www.actualtests.com 778
CompTIA SY0-401 Exam

- A. Support for mobile OS
- B. Support of mobile apps
- C. Availability of mobile browsers
- D. Key management for mobile devices

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 571

A recent review of accounts on various systems has found that after employees passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO)

- A. Reverse encryption
- B. Minimum password age
- C. Password complexity
- D. Account lockouts
- E. Password history
- F. Password expiration

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 572

A system administrator runs a network inventory scan every Friday at 10:00 am to track the progress of a large organization's operating system upgrade of all laptops. The system administrator discovers that some laptops are now only being reported as IP addresses. Which of the following options is MOST likely the cause of this issue?

- A. HIDS
- B. Host-based firewalls rules
- C. All the laptops are currently turned off
- D. DNS outage

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 779
CompTIA SY0-401 Exam

QUESTION 573

A security administrator working for a law enforcement organization is asked to secure a computer system at the scene of a crime for transport to the law enforcement forensic facility. In order to capture as much evidence as possible, the computer system has been left running. The security administrator begins information by image which of the following system components FIRST?

- A. NVRAM
- B. RAM
- C. TPM
- D. SSD

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 574

A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?

- A. Implement transitive trust across security domains
- B. Enable the trusted OS feature across all enterprise computers
- C. Install and configure the appropriate CA certificate on all domain controllers
- D. Verify that system administrators are in the domain administrator group in the main office

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 575

An administrator is hardening systems and wants to disable unnecessary services. One Linux server hosts files used by a Windows web server on another machine. The Linux server is only used for secure file transfer, but requires a share for the Windows web server as well. The administrator sees the following output from a netstat -1p command:

"Pass Any Exam. Any Time." - www.actualtests.com 780
CompTIA SY0-401 Exam

Proto	Recv-Q	Send-Q	Local Addr	Foreign Addr	State	PID
tcp	0	0	*:mysql	*;* LISTEN		1488/mysqld
tcp	0	0	*:ftp	*;* LISTEN		2120/vsftpd
tcp	0	0	*:80	*;* LISTEN		1680/httpd
udp	0	0	*:69	*;* LISTEN		2680/tftp
tcp	0	0	*:139	*;* LISTEN		8217/smbd
tcp	0	0	*:6667	*;* LISTEN		2121/badBunny_FTP

Which of the following processes can the administrator kill without risking impact to the purpose and function of the Linux or Windows servers? (Select Three)

- A. 1488
- B. 1680
- C. 2120
- D. 2121
- E. 2680
- F. 8217

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 576

A project manager is evaluating proposals for a cloud commuting project. The project manager is particularly concerned about logical security controls in place at the service provider's facility. Which of the following sections of the proposal would be MOST important to review, given the project manager's concerns?

- A. CCTV monitoring
- B. Perimeter security lighting system
- C. Biometric access system
- D. Environmental system configuration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 577

A security administrator would like to ensure that some members of the building's maintenance staff are only allowed access to the facility during weekend hours. Access to the facility is

"Pass Any Exam. Any Time." - www.actualtests.com 781

CompTIA SY0-401 Exam

controlled by badge swipe and a man trap. Which of the following options will BEST accomplish this goal?

- A. CCTV
- B. Security Guard
- C. Time of day restrictions
- D. Job rotation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 578

A security manager received reports of several laptops containing confidential data stolen out of a lab environment. The lab is not a high security area and is secured with physical key locks. The security manager has no information to provide investigators related to who may have stolen the laptops. Which of the following should the security manager implement to improve legal and criminal investigations in the future?

- A. Motion sensors
- B. Mobile device management
- C. CCTV
- D. Cable locks
- E. Full-disk encryption

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 579

During a Linux security audit at a local college, it was noted that members of the dean's group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean's group should only have the ability to modify student records. Assuming that the correct user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?

- A. R-x---rwx
- B. Rwxrwxrwx
- C. Rwx---wx
"Pass Any Exam. Any Time." - www.actualtests.com 782
CompTIA SY0-401 Exam
- D. Rwxrwxr--

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 580

An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

- A. Ransomware
- B. Rootkit
- C. Scareware
- D. Spyware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 581

Which of the following can be mitigated with proper secure coding techniques?

- A. Input validation
- B. Error handling
- C. Header manipulation
- D. Cross-site scripting

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 582

Recently the desktop support group has been performing a hardware refresh and has replaced numerous computers. An auditor discovered that a number of the new computers did not have the company's antivirus software installed on them, Which of the following could be utilized to notify the network support group when computers without the antivirus software are added to the

"Pass Any Exam. Any Time." - www.actualtests.com 783

CompTIA SY0-401 Exam
network?

- A. Network port protection
- B. NAC
- C. NIDS
- D. Mac Filtering

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 583

An administrator needs to protect against downgrade attacks due to various vulnerabilities in SSL/TLS. Which of the following actions should be performed? (Select TWO)

- A. Set minimum protocol supported
- B. Request a new certificate from the CA
- C. Configure cipher order
- D. Disable flash cookie support
- E. Re-key the SSL certificate
- F. Add the old certificate to the CRL

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 584

A developer needs to utilize AES encryption in an application but requires the speed of encryption and decryption to be as fast as possible. The data that will be secured is not sensitive so speed is valued over encryption complexity. Which of the following would BEST satisfy these requirements?

- A. AES with output feedback
- B. AES with cipher feedback
- C. AES with cipher block chaining

D. AES with counter mode

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 784
CompTIA SY0-401 Exam

QUESTION 585

During a code review a software developer discovers a security risk that may result in hundreds of hours of rework. The security team has classified these issues as low risk. Executive management has decided that the code will not be rewritten. This is an example of:

- A. Risk avoidance
- B. Risk transference
- C. Risk mitigation
- D. Risk acceptance

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 586

A network was down for several hours due to a contractor entering the premises and plugging both ends of a network cable into adjacent network jacks. Which of the following would have prevented the network outage? (Select Two)

- A. Port security
- B. Loop Protection
- C. Implicit deny
- D. Log analysis
- E. Mac Filtering
- F. Flood Guards

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 587

After disabling SSID broadcast, a network administrator still sees the wireless network listed in available networks on a client laptop. Which of the following attacks may be occurring?

- A. Evil Twin
- B. ARP spoofing
- C. Disassociation flooding
"Pass Any Exam. Any Time." - www.actualtests.com 785
CompTIA SY0-401 Exam
- D. Rogue access point
- E. TKIP compromise

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 588

A security manager is preparing the training portion of an incident plan. Which of the following job roles should receive training on forensics, chain of custody, and the order of volatility?

- A. System owners
- B. Data custodians
- C. First responders
- D. Security guards

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 589

Virtualization that allows an operating system kernel to run multiple isolated instances of the guest is called:

- A. Process segregation
- B. Software defined network
- C. Containers
- D. Sandboxing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 590

Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?

- A. SAML
"Pass Any Exam. Any Time." - www.actualtests.com 786
CompTIA SY0-401 Exam
- B. TACACS
- C. LDAP
- D. RADIUS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 591

While responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

- A. IPCONFIG
- B. Netstat
- C. PSINFO
- D. Net session

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 592

A system administrator must configure the company's authentication system to ensure that users will be unable to reuse the last ten passwords within a six months period. Which of the following settings must be configured? (Select Two)

- A. Minimum password age
- B. Password complexity
- C. Password history
- D. Minimum password length
- E. Multi-factor authentication
- F. Do not store passwords with reversible encryption

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 593

"Pass Any Exam. Any Time." - www.actualtests.com 787

CompTIA SY0-401 Exam

An administrator requests a new VLAN be created to support the installation of a new SAN. Which of the following data transport?

- A. Fibre Channel
- B. SAS
- C. Sonet

D. ISCSI

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 594

Which of the following access control methodologies provides an individual with the most restrictive access rights to successfully perform their authorized duties?

- A. Mandatory Access Control
- B. Rule Based Access Control
- C. Least Privilege
- D. Implicit Deny
- E. Separation of Duties

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 595

An administrator wants to provide onboard hardware based cryptographic processing and secure key storage for full-disk encryption. Which of the following should the administrator use to fulfil the requirements?

- A. AES
- B. TPM
- C. FDE
- D. PAM

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 788
CompTIA SY0-401 Exam

QUESTION 596

When viewing IPS logs the administrator see systems all over the world scanning the network for servers with port 22 open. The administrator concludes that this traffic is a(N):

- A. Risk
- B. Vulnerability
- C. Exploit
- D. Threat

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 597

Ann a user has been promoted from a sales position to sales manager. Which of the following risk mitigation strategies would be MOST appropriate when a user changes job roles?

- A. Implement data loss prevention
- B. Rest the user password
- C. User permissions review
- D. Notify incident management

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 598

A system administrator is implementing a firewall ACL to block specific communication to and from a predefined list of IP addresses, while allowing all other communication. Which of the following rules is necessary to support this implementation?

- A. Implicit allow as the last rule
- B. Implicit allow as the first rule
- C. Implicit deny as the first rule
- D. Implicit deny as the last rule

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 789
CompTIA SY0-401 Exam

QUESTION 599

Joe a system architect wants to implement appropriate solutions to secure the company's distributed database. Which of the following concepts should be considered to help ensure data security? (Select TWO)

- A. Data at rest
- B. Data in use
- C. Replication
- D. Wiping
- E. Retention
- F. Cloud Storage

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 600

A forensics analyst is tasked identifying identical files on a hard drive. Due to the large number of files to be compared, the analyst must use an algorithm that is known to have the lowest collision rate. Which of the following should be selected?

- A. MD5

- B. RC4
- C. SHA-128
- D. AES-256

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 601

A government agency wants to ensure that the systems they use have been deployed as security as possible. Which of the following technologies will enforce protections on these systems to prevent files and services from operating outside of a strict rule set?

- A. Host based Intrusion detection
- B. Host-based firewall
"Pass Any Exam. Any Time." - www.actualtests.com 790
CompTIA SY0-401 Exam
- C. Trusted OS
- D. Antivirus

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 602

An organization receives an email that provides instruction on how to protect a system from being a target of new malware that is rapidly infecting systems. The incident response team investigates the notification and determines it to be invalid and notifies users to disregard the email. Which of the following Best describes this occurrence?

- A. Phishing
- B. Scareware
- C. SPAM
- D. Hoax

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 603

Joe an employee has reported to Ann a network technician an unusual device plugged into a USB port on a workstation in the call center. Ann unplugs the workstation and brings it to the IT department where an incident is opened. Which of the following should have been done first?

- A. Notify the incident response team lead
- B. Document chain of custody
- C. Take a copy of volatile memory
- D. Make an image of the hard drive

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 604

A company is implementing a system to transfer direct deposit information to a financial institution. One of the requirements is that the financial institution must be certain that the deposit amounts

"Pass Any Exam. Any Time." - www.actualtests.com 791

CompTIA SY0-401 Exam

within the file have not been changed. Which of the following should be used to meet the requirement?

- A. Key escrow
- B. Perfect forward secrecy
- C. Transport encryption
- D. Digital signatures
- E. File encryption

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 605

An organization uses a Kerberos-based LDAP service for network authentication. The service is also utilized for internal web applications. Finally access to terminal applications is achieved using the same authentication method by joining the legacy system to the Kerberos realm. This company is using Kerberos to achieve which of the following?

- A. Trusted Operating System
- B. Rule-based access control
- C. Single sign on
- D. Mandatory access control

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 606

A recent audit has revealed that all employees in the bookkeeping department have access to confidential payroll information, while only two members of the bookkeeping department have job duties that require access to the confidential information. Which of the following can be implemented to reduce the risk of this information becoming compromised in this scenario? (Select TWO)

- A. Rule-based access control
- B. Role-based access control
- C. Data loss prevention
- D. Separation of duties
- E. Group-based permissions

"Pass Any Exam. Any Time." - www.actualtests.com 792
CompTIA SY0-401 Exam

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 607

A Chief Executive Officer (CEO) is steering company towards cloud computing. The CEO is requesting a federated sign-on method to have users sign into the sales application. Which of the following methods will be effective for this purpose?

- A. SAML
- B. RADIUS
- C. Kerberos
- D. LDAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 608

An administrator is configuring a new Linux web server where each user account is confined to a chroot jail. Which of the following describes this type of control?

- A. SysV
- B. Sandbox
- C. Zone
- D. Segmentation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 609

Recently clients are stating they can no longer access a secure banking site's webpage. In reviewing the clients' web browser settings, the certificate chain is showing the following:

Certificate Chain:

X Digi Cert

"Pass Any Exam. Any Time." - www.actualtests.com 793
CompTIA SY0-401 Exam
Digi Cert High assurance C3

* banksite.com

Certificate Store:

Digi Cert Others Certificate Store

Digi Cert High assurance C3 Others Certificate Store

Based on the information provided, which of the following is the problem when connecting to the website?

- A. The certificate signature request was invalid
- B. Key escrow is failing for the certificate authority
- C. The certificate authority has revoked the certificate
- D. The clients do not trust the certificate authority

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 610

A company often processes sensitive data for the government. The company also processes a large amount of commercial work and as such is often providing tours to potential customers that take them into various workspaces. Which of the following security methods can provide protection against tour participants viewing sensitive information at minimal cost?

- A. Strong passwords
- B. Screen protectors
- C. Clean-desk policy
- D. Mantraps

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 611

Joe is a helpdesk specialist. During a routine audit, a company discovered that his credentials were used while he was on vacation. The investigation further confirmed that Joe still has his badge and it was last used to exit the facility. Which of the following access control methods is

"Pass Any Exam. Any Time." - www.actualtests.com 794

CompTIA SY0-401 Exam

MOST appropriate for preventing such occurrences in the future?

- A. Access control where the credentials cannot be used except when the associated badge is in the facility
- B. Access control where system administrators may limit which users can access their systems
- C. Access control where employee's access permissions is based on the job title
- D. Access control system where badges are only issued to cleared personnel

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 612

A security architect is designing an enterprise solution for the sales force of a corporation which handles sensitive customer data. The solution must allow users to work from remote offices and support traveling users. Which of the following is the MOST appropriate control for the architect to focus onto ensure confidentiality of data stored on laptops?

- A. Full-disk encryption
- B. Digital sign
- C. Federated identity management
- D. Cable locks

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 613

A security administrator needs a method to ensure that only employees can get onto the internal network when plugging into a network switch. Which of the following BEST meets that requirement?

- A. NAC
- B. UTM
- C. DMZ
- D. VPN

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 795
CompTIA SY0-401 Exam

QUESTION 614

Having adequate lighting on the outside of a building is an example of which of the following security controls?

- A. Deterrent
- B. Compensating
- C. Detective
- D. Preventative

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 615

During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

- A. Time-of-day restrictions
- B. User access reviews
- C. Group-based privileges
- D. Change management policies

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 616

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
 - B. Interconnection security agreement
 - C. Non-disclosure agreement
 - D. Business process analysis
- "Pass Any Exam. Any Time." - www.actualtests.com 796
CompTIA SY0-401 Exam

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 617

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

- A. Mandatory access control
- B. Discretionary access control
- C. Role based access control
- D. Rule-based access control

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 618

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

- A. Spear phishing
- B. Man-in-the-middle
- C. URL hijacking
- D. Transitive access

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 619

A security administrator wishes to implement a secure method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

- A. SCP
"Pass Any Exam. Any Time." - www.actualtests.com 797
CompTIA SY0-401 Exam
- B. TFTP
- C. SNMP
- D. FTP
- E. SMTP
- F. FTPS

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 620

A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.

Which of the following **MUST** the technician implement?

- A. Dual factor authentication
- B. Transitive authentication
- C. Single factor authentication
- D. Biometric authentication

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 621

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the **MOST** likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared likely is incorrect
- D. The company's DHCP server scope is full

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 622

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?

Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

- A. Rule 1: deny from inside to outside source any destination any service smtp
- B. Rule 2: deny from inside to outside source any destination any service ping
- C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
- D. Rule 4: deny from any to any source any destination any service any

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 623

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

- A. armored virus
- B. logic bomb
- C. polymorphic virus
- D. Trojan

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 624

A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

- A. RSA
- B. TwoFish
- C. Diffie-Helman
"Pass Any Exam. Any Time." - www.actualtests.com 799
CompTIA SY0-401 Exam
- D. NTLMv2
- E. RIPEMD

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 625

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- A. MOU
- B. ISA
- C. BPA
- D. SLA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 626

Which of the following are MOST susceptible to birthday attacks?

- A. Hashed passwords
- B. Digital certificates
- C. Encryption passwords
- D. One time passwords

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 627

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

- A. Order of volatility
"Pass Any Exam. Any Time." - www.actualtests.com 800
CompTIA SY0-401 Exam
- B. Chain of custody
- C. Recovery procedure
- D. Incident isolation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 628

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

- A. Bcrypt
- B. Blowfish
- C. PGP
- D. SHA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 629

Given the log output:

Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: msmith] [Source: 10.0.12.45]

[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015

Which of the following should the network administrator do to protect data security?

- A. Configure port security for logons
- B. Disable telnet and enable SSH
- C. Configure an AAA server
- D. Disable password and enable RSA authentication

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 801
CompTIA SY0-401 Exam

QUESTION 630

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

- A. Certificate revocation list
- B. Intermediate authority
- C. Recovery agent
- D. Root of trust

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 631

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 632

In an effort to reduce data storage requirements, a company decides to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems. Which of the following algorithms is BEST suited for this purpose?

- A. MD5
"Pass Any Exam. Any Time." - www.actualtests.com 802
CompTIA SY0-401 Exam
- B. SHA
- C. RIPEMD
- D. AES

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 633

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently,

the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

- A. Replace FTP with SFTP and replace HTTP with TLS
- B. Replace FTP with FTPS and replaces HTTP with TFTP
- C. Replace FTP with SFTP and replace HTTP with Telnet
- D. Replace FTP with FTPS and replaces HTTP with IPSec

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 634

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes. Which of the following risk management strategies BEST describes management's response?

- A. Deterrence
- B. Mitigation
- C. Avoidance
- D. Acceptance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 635

"Pass Any Exam. Any Time." - www.actualtests.com 803

CompTIA SY0-401 Exam

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

- A. Account lockout
- B. Group Based Privileges

- C. Least privilege
- D. Password complexity

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 636

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

- A. Key escrow
- B. Digital signatures
- C. PKI
- D. Hashing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 637

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- A. Transitive trust
- B. Symmetric encryption
- C. Two-factor authentication
- D. Digital signatures
- E. One-time passwords

"Pass Any Exam. Any Time." - www.actualtests.com 804
CompTIA SY0-401 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 638

Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

- A. Digital signatures
- B. File integrity monitoring
- C. Access controls
- D. Change management
- E. Stateful inspection firewall

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 639

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- A. Collision resistance
- B. Rainbow table
- C. Key stretching
- D. Brute force attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 640

Which of the following is commonly used for federated identity management across multiple organizations?

- A. SAML
"Pass Any Exam. Any Time." - www.actualtests.com 805
CompTIA SY0-401 Exam
- B. Active Directory
- C. Kerberos
- D. LDAP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 641

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 642

A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

- A. MD5
- B. AES

- C. UDP
- D. PKI

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 643

A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

"Pass Any Exam. Any Time." - www.actualtests.com 806
CompTIA SY0-401 Exam

- A. It provides authentication services
- B. It uses tickets to identify authenticated users
- C. It provides single sign-on capability
- D. It uses XML for cross-platform interoperability

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 644

Which of the following can affect electrostatic discharge in a network operations center?

- A. Fire suppression
- B. Environmental monitoring
- C. Proximity card access
- D. Humidity controls

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 645

a malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

- A. Header manipulation
- B. Cookie hijacking
- C. Cross-site scripting
- D. Xml injection

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 646

A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

"Pass Any Exam. Any Time." - www.actualtests.com 807
CompTIA SY0-401 Exam

- A. Whitelisting
- B. Anti-malware
- C. Application hardening
- D. Blacklisting
- E. Disable removable media

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 647

A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

- A. Asset control
- B. Device access control
- C. Storage lock out
- D. Storage segmentation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 648

A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and low performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

- A. The switch also serves as the DHCP server
- B. The switch has the lowest MAC address
- C. The switch has spanning tree loop protection enabled
- D. The switch has the fastest uplink port

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 808
CompTIA SY0-401 Exam

QUESTION 649

An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

- A. Rule-based access control
- B. Role-based access control
- C. Mandatory access control
- D. Discretionary access control

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 650

While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

- A. Minimum complexity
- B. Maximum age limit
- C. Maximum length
- D. Minimum length
- E. Minimum age limit
- F. Minimum re-use limit

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 651

A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

"Pass Any Exam. Any Time." - www.actualtests.com 809
CompTIA SY0-401 Exam

- A. Deploy antivirus software and configure it to detect and remove pirated software
- B. Configure the firewall to prevent the downloading of executable files
- C. Create an application whitelist and use OS controls to enforce it
- D. Prevent users from running as administrator so they cannot install software.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 652

A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

- A. LDAP server 10.55.199.3
- B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
- C. SYSLOG SERVER 172.16.23.50
- D. TACAS server 192.168.1.100

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 653

A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

- A. Cryptography
- B. Time of check/time of use
- C. Man in the middle
- D. Covert timing

E. Steganography

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 810
CompTIA SY0-401 Exam

QUESTION 654

An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to. This is because the encryption scheme in use adheres to:

- A. Asymmetric encryption
- B. Out-of-band key exchange
- C. Perfect forward secrecy
- D. Secure key escrow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 655

Many employees are receiving email messages similar to the one shown below:

From IT department

To employee

Subject email quota exceeded

Please click on the following link <http://www.website.info/email.php?quota=1Gb> and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.

Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

- A. BLOCK http://www.*.info/"
- B. DROP http://"website.info/email.php?*
- C. Redirect http://www,*. Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
- D. DENY http://*.info/email.php?quota=1Gb

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 811
CompTIA SY0-401 Exam

QUESTION 656

A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags[S]  
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags[S]  
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags[S]  
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags[S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

- A. DENY TCO From ANY to 172.31.64.4
- B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
- C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
- D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 657

The IT department needs to prevent users from installing untested applications. Which of the following would provide the BEST solution?

- A. Job rotation
- B. Least privilege
- C. Account lockout
- D. Antivirus

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 658

"Pass Any Exam. Any Time." - www.actualtests.com 812

CompTIA SY0-401 Exam

An attack that is using interference as its main attack to impede network traffic is which of the following?

- A. Introducing too much data to a targets memory allocation
- B. Utilizing a previously unknown security flaw against the target
- C. Using a similar wireless configuration of a nearby network
- D. Inundating a target system with SYN requests

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 659

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

- A. DES
- B. Blowfish
- C. DSA
- D. Diffie-Hellman
- E. 3DES

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 660

Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remarks. Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

- A. Data Labeling and disposal
- B. Use of social networking
- C. Use of P2P networking
- D. Role-based training

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 813
CompTIA SY0-401 Exam

QUESTION 661

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment

that was performed to discover this issue?

- A. Network mapping
- B. Vulnerability scan
- C. Port Scan
- D. Protocol analysis

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 662

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

- A. RC4
- B. MD5
- C. HMAC
- D. SHA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 663

The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

- A. In-transit
- B. In-use
- C. Embedded
- D. At-rest

"Pass Any Exam. Any Time." - www.actualtests.com 814
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 664

Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

- A. TACACS+
- B. RADIUS
- C. Kerberos
- D. SAML

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 665

A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

- A. Proxy
- B. Protocol analyzer
- C. Switch
- D. Firewall

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 666

The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

- A. Create a honeynet
- B. Reduce beacon rate
"Pass Any Exam. Any Time." - www.actualtests.com 815
CompTIA SY0-401 Exam
- C. Add false SSIDs
- D. Change antenna placement
- E. Adjust power level controls
- F. Implement a warning banner

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 667

A security administrator suspects that data on a server has been exfiltrated as a result of un-authorized remote access. Which of the following would assist the administrator in confirming the suspicions? (Select TWO)

- A. Networking access control
- B. DLP alerts
- C. Log analysis
- D. File integrity monitoring
- E. Host firewall rules

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 668

A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will provide the

best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

- A. Put the VoIP network into a different VLAN than the existing data network.
- B. Upgrade the edge switches from 10/100/1000 to improve network speed
- C. Physically separate the VoIP phones from the data network
- D. Implement flood guards on the data network

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 816
CompTIA SY0-401 Exam

QUESTION 669

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

- A. TLS
- B. MPLS
- C. SCP
- D. SSH

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 670

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

- A. LDAP
- B. Kerberos
- C. SAML

D. TACACS+

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 671

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- A. Use of OATH between the user and the service and attestation from the company domain
- B. Use of active directory federation between the company and the cloud-based service
- C. Use of smartcards that store x.509 keys, signed by a global CA
- D. Use of a third-party, SAML-based authentication service for attestation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 817
CompTIA SY0-401 Exam

Explanation:

QUESTION 672

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes what the company?

- A. The system integration phase of the SDLC
- B. The system analysis phase of SSDSLC
- C. The system design phase of the SDLC
- D. The system development phase of the SDLC

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 673

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

- A. Job rotation
- B. Log failure
- C. Lack of training
- D. Insider threat

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 674

A security administrator needs an external vendor to correct an urgent issue with an organization's

"Pass Any Exam. Any Time." - www.actualtests.com 818

CompTIA SY0-401 Exam

physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

- A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- B. Have the external vendor come onsite and provide access to the PACS directly
- C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 675

A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

- A. Communications software
- B. Operating system software
- C. Weekly summary reports to management
- D. Financial and production software

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 676

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

- A. SQL injection
- B. Session hijacking
- C. Cross-site scripting
- D. Locally shared objects
- E. LDAP injection

Correct Answer: BC

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 819
CompTIA SY0-401 Exam

QUESTION 677

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- A. On the client
- B. Using database stored procedures
- C. On the application server
- D. Using HTTPS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 678

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- A. Egress traffic is more important than ingress traffic for malware prevention
- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources
- D. To prevent DDoS attacks originating from external network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 679

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

- A. Password Reuse
- B. Password complexity
- C. Password History
- D. Password Minimum age

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 820
CompTIA SY0-401 Exam

QUESTION 680

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- A. Block level encryption
- B. SAML authentication
- C. Transport encryption
- D. Multifactor authentication
- E. Predefined challenge questions
- F. Hashing

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 681

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

VPN log:

```
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
```

Corporate firewall log:

```
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
```

Workstation host firewall log:

```
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

- A. Network latency is causing remote desktop service request to time out
- B. User1 has been locked out due to too many failed passwords
- C. Lack of network time synchronization is causing authentication mismatches
- D. The workstation has been compromised and is accessing known malware sites
- E. The workstation host firewall is not allowing remote desktop connections "Pass Any Exam. Any Time." - www.actualtests.com 821
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 682

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem best be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons learned

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 683

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most likely recommend during the audit out brief?

- A. Discretionary access control for the firewall team
- B. Separation of duties policy for the firewall team
- C. Least privilege for the firewall team
- D. Mandatory access control for the firewall team

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 684

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

- A. NAC
- B. VLAN
"Pass Any Exam. Any Time." - www.actualtests.com 822
CompTIA SY0-401 Exam
- C. DMZ
- D. Subnet

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 685

An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

- A. Create an ACL to allow the FTP service write access to user directories
- B. Set the Boolean selinux value to allow FTP home directory uploads
- C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 686

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

- A. Enable verbose system logging
- B. Change the permissions on the user's home directory

- C. Implement remote syslog
- D. Set the bash_history log file to "read only"

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 823
CompTIA SY0-401 Exam

QUESTION 687

A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- A. Firmware version control
- B. Manual software upgrades
- C. Vulnerability scanning
- D. Automatic updates
- E. Network segmentation
- F. Application firewalls

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 688

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

- A. Time of day restrictions
- B. Principle of least privilege
- C. Role-based access control
- D. Separation of duties

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 689

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

- A. Enter random or invalid data into the application in an attempt to cause it to fault
- B. Work with the developers to eliminate horizontal privilege escalation opportunities
- C. Test the applications for the existence of built-in- back doors left by the developers
- D. Hash the application to verify it won't cause a false positive on the HIPS.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 824

CompTIA SY0-401 Exam

Explanation:

QUESTION 690

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

- A. full-disk encryption
- B. Host-based firewall
- C. Current antivirus definitions
- D. Latest OS updates

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 691

An attacker uses a network sniffer to capture the packets of a transaction that adds \$20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another \$20 to the gift card. This can be done many times. Which of the following describes this type of attack?

- A. Integer overflow attack
- B. Smurf attack
- C. Replay attack
- D. Buffer overflow attack
- E. Cross-site scripting attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 692

An organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which

"Pass Any Exam. Any Time." - www.actualtests.com 825

CompTIA SY0-401 Exam

of the following options meets all of these requirements?

- A. Two-factor authentication
- B. Account and password synchronization
- C. Smartcards with PINS
- D. Federated authentication

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 693

The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate servers at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote servers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 694

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

- A. Set up the scanning system's firewall to permit and log all outbound connections
- B. Use a protocol analyzer to log all pertinent network traffic
- C. Configure network flow data logging on all scanning system
- D. Enable debug level logging on the scanning system and all scanning tools used.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 826
CompTIA SY0-401 Exam

QUESTION 695

Which of the following best describes the initial processing phase used in mobile device forensics?

- A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
- B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
- C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
- D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 696

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain \. Which of the following tools would aid her to decipher the network traffic?

- A. Vulnerability Scanner
- B. NMAP
- C. NETSTAT
- D. Packet Analyzer

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 697

An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

- A. Find two identical messages with different hashes
- B. Find two identical messages with the same hash
- C. Find a common has between two specific messages
- D. Find a common hash between a specific message and a random message

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

"Pass Any Exam. Any Time." - www.actualtests.com 827
CompTIA SY0-401 Exam

Explanation:

QUESTION 698

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administrator has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

- A. Upgrade the encryption to WPA or WPA2
- B. Create a non-zero length SSID for the wireless router
- C. Reroute wireless users to a honeypot
- D. Disable responses to a broadcast probe request

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 699

Which of the following should be used to implement voice encryption?

- A. SSLv3
- B. VDSL
- C. SRTP
- D. VoIP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 700

During an application design, the development team specifies a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

- A. Application control
- B. Data in-transit
- C. Identification
"Pass Any Exam. Any Time." - www.actualtests.com 828
CompTIA SY0-401 Exam
- D. Authentication

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 701

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- A. Time-of-day restrictions
- B. Change management
- C. Periodic auditing of user credentials
- D. User rights and permission review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 702

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics

- B. Backups are being performed and tested
- C. Data ownership is being maintained and audited
- D. Risk awareness is being adhered to and enforced

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 703

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- A. Calculate the ALE
"Pass Any Exam. Any Time." - www.actualtests.com 829
CompTIA SY0-401 Exam
- B. Calculate the ARO
- C. Calculate the MTBF
- D. Calculate the TCO

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 704

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

- A. Signature based
- B. Heuristic
- C. Anomaly-based
- D. Behavior-based

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 705

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

- A. Implement protected distribution
- B. Empty additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 706

During a data breach cleanup it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

"Pass Any Exam. Any Time." - www.actualtests.com 830
CompTIA SY0-401 Exam

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons Learned

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 707

New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

- A. Fail safe
- B. Fault tolerance
- C. Fail secure
- D. Redundancy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 708

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

- A. It can protect multiple domains
- B. It provides extended site validation
- C. It does not require a trusted certificate authority
- D. It protects unlimited subdomains

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 709

After a merger between two companies a security analyst has been asked to ensure that the

"Pass Any Exam. Any Time." - www.actualtests.com 831

CompTIA SY0-401 Exam

organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

- A. Monitor VPN client access
- B. Reduce failed login out settings
- C. Develop and implement updated access control policies
- D. Review and address invalid login attempts
- E. Increase password complexity requirements
- F. Assess and eliminate inactive accounts

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 710

A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

- A. Architecture review
- B. Risk assessment
- C. Protocol analysis
- D. Code review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 711

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?

- A. 192.168.0.16 255.25.255.248
- B. 192.168.0.16/28
- C. 192.168.1.50 255.255.25.240

D. 192.168.2.32/27
"Pass Any Exam. Any Time." - www.actualtests.com 832
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 712

A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements?

- A. Virtual desktop infrastructure (VDI)
- B. WS-security and geo-fencing
- C. A hardware security module (HSM)
- D. RFID tagging system
- E. MDM software
- F. Security Requirements Traceability Matrix (SRTM)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 713

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

- A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
- B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
- C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files

D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 833
CompTIA SY0-401 Exam

QUESTION 714

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this Scenario?

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power
- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 715

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 716

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to

"Pass Any Exam. Any Time." - www.actualtests.com 834
CompTIA SY0-401 Exam
implement?

- A. Revision control system
- B. Client side exception handling
- C. Server side validation
- D. Server hardening

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 717

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described?

- A. Zero-day exploit
- B. Remote code execution
- C. Session hijacking
- D. Command injection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 718

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

"Pass Any Exam. Any Time." - www.actualtests.com 835
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 719

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

- A. Require the use of two different passwords held by two different individuals to open an account
- B. Administer account creation on a role based access control approach
- C. Require all new accounts to be handled by someone else other than a teller since they have different duties
- D. Administer account creation on a rule based access control approach

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 720

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

- A. Implement a clean desk policy
- B. Security training to prevent shoulder surfing
- C. Enable group policy based screensaver timeouts
- D. Install privacy screens on monitors

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 721

"Pass Any Exam. Any Time." - www.actualtests.com 836

CompTIA SY0-401 Exam

Company policy requires the use of passphrases instead of passwords. Which of the following technical controls **MUST** be in place in order to promote the use of passphrases?

- A. Reuse
- B. Length
- C. History
- D. Complexity

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 722

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policy
- D. Account expiration policy

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 723

Which of the following should identify critical systems and components?

- A. MOU
- B. BPA
- C. ITCP
- D. BCP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 837
CompTIA SY0-401 Exam

QUESTION 724

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

- A. Logic bomb
- B. Trojan
- C. Scareware
- D. Ransomware

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 725

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

- A. SQL injection
- B. Header manipulation
- C. Cross-site scripting
- D. Flash cookie exploitation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 726

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to correct this issue?

- A. Decrease the room temperature
- B. Increase humidity in the room
- C. Utilize better hot/cold aisle configurations
- D. Implement EMI shielding

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 838
CompTIA SY0-401 Exam

QUESTION 727

A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

- A. Format the device
- B. Re-image the device
- C. Perform virus scan in the device
- D. Physically destroy the device

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 728

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement?

- A. CSR
- B. OCSP
- C. CRL
- D. SSH

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 729

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

- A. Gray box vulnerability testing
- B. Passive scan
- C. Credentialed scan

- D. Bypassing security controls
"Pass Any Exam. Any Time." - www.actualtests.com 839
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 730

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 731

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

- A. Firewall logs
- B. IDS logs

- C. Increased spam filtering
 - D. Protocol analyzer
- "Pass Any Exam. Any Time." - www.actualtests.com 840
CompTIA SY0-401 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 732

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

- A. Enforce authentication for network devices
- B. Configure the phones on one VLAN, and computers on another
- C. Enable and configure port channels
- D. Make users sign an Acceptable use Agreement

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 733

An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
- B. Configure the smart phones so that the stored data can be destroyed from a centralized location
- C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
- D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 734

A user of the wireless network is unable to gain access to the network. The symptoms are:

1.) Unable to connect to both internal and Internet resources

"Pass Any Exam. Any Time." - www.actualtests.com 841

CompTIA SY0-401 Exam

2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate. Which of the following is the MOST likely cause of the connectivity issues?

- A. The wireless signal is not strong enough
- B. A remote DDoS attack against the RADIUS server is taking place
- C. The user's laptop only supports WPA and WEP
- D. The DHCP scope is full
- E. The dynamic encryption key did not update while the user was offline

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 735

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

- A. Password complexity policies
- B. Hardware tokens
- C. Biometric systems
- D. Role-based permissions

- E. One time passwords
- F. Separation of duties
- G. Multifactor authentication
- H. Single sign-on
- I. Least privilege

Correct Answer: DFI

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 736

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting

"Pass Any Exam. Any Time." - www.actualtests.com 842

CompTIA SY0-401 Exam

without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- A. Device access control
- B. Location based services
- C. Application control
- D. GEO-Tagging

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 737

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first. Which of the following is the correct order in which Joe should collect the data?

- A. CPU cache, paging/swap files, RAM, remote logging data
- B. RAM, CPU cache, Remote logging data, paging/swap files

- C. Paging/swap files, CPU cache, RAM, remote logging data
- D. CPU cache, RAM, paging/swap files, remote logging data

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 738

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

- A. Use a honeypot
- B. Disable unnecessary services
- C. Implement transport layer security
- D. Increase application event logging

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 843
CompTIA SY0-401 Exam

QUESTION 739

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

- A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- B. Recommend classifying each application into like security groups and segmenting the groups from one another
- C. Recommend segmenting each application, as it is the most secure approach
- D. Recommend that only applications with minimal security features should be segmented to protect them

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 740

A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

- A. Architecture evaluation
- B. Baseline reporting
- C. Whitebox testing
- D. Peer review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 741

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to

"Pass Any Exam. Any Time." - www.actualtests.com 844

CompTIA SY0-401 Exam

the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

- A. Tailgating
- B. Shoulder surfing
- C. Impersonation
- D. Hoax

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 742

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test. Which of the following has the administrator been tasked to perform?

- A. Risk transference
- B. Penetration test
- C. Threat assessment
- D. Vulnerability assessment

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 743

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- A. Transitive access
- B. Spoofing
- C. Man-in-the-middle
- D. Replay

"Pass Any Exam. Any Time." - www.actualtests.com 845
CompTIA SY0-401 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 744

Which of the following use the SSH protocol?

- A. Stelnet
- B. SCP
- C. SNMP
- D. FTPS
- E. SSL
- F. SFTP

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 745

A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

- A. Utilizing a single question for password recovery
- B. Sending a PIN to a smartphone through text message
- C. Utilizing CAPTCHA to avoid brute force attacks
- D. Use a different e-mail address to recover password

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 746

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

"Pass Any Exam. Any Time." - www.actualtests.com 846
CompTIA SY0-401 Exam

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 747

A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentally opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

- A. Install host-based firewalls on all computers that have an email client installed
- B. Set the email program default to open messages in plain text
- C. Install end-point protection on all computers that access web email
- D. Create new email spam filters to delete all messages from that sender

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 748

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?

- A. Recovery agent
- B. Ocsp

- C. Crl
- D. Key escrow

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 749

"Pass Any Exam. Any Time." - www.actualtests.com 847

CompTIA SY0-401 Exam

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

- A. GMAC
- B. PCBC
- C. CBC
- D. GCM
- E. CFB

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 750

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca
- D. Use a self-signed certificate on each internal server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 751

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

- A. Peer review
- B. Component testing
- C. Penetration testing
- D. Vulnerability testing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



<http://www.gratisexam.com/>