

SY0-301_01-10-13_Anontester

Number: SY0-301
Passing Score: 750
Time Limit: 90 min
File Version: 20.1



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

Sections

1. Group 1
2. Group 2
3. Group 3
4. Group 4
5. Group 5
6. Group 6
7. Group 7
8. Group 8
9. Group 9
10. Group 10

ExamA

QUESTION 1

A password history value of three means which of the following?

- A. Three different passwords are used before one can be reused.
- B. A password cannot be reused once changed for three years.
- C. After three hours a password must be re-entered to continue.
- D. The server stores passwords in the database for three days.

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 2

In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

- A. Subnetting
- B. NAT
- C. Firewall
- D. NAC
- E. VPN

Correct Answer: CE

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 3

Which of the following is the BEST approach to perform risk mitigation of user access control rights?

- A. Conduct surveys and rank the results.
- B. Perform routine user permission reviews.
- C. Implement periodic vulnerability scanning.
- D. Disable user accounts that have not been used within the last two weeks.

Correct Answer: B

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 4

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: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 5

All of the following are valid cryptographic hash functions EXCEPT:



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

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

Correct Answer: B

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

- A. 802.1x
- B. DHCP
- C. 802.1q
- D. NIPS

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 7

A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following?

- A. Whaling
- B. Bluesnarfing

- C. Vishing
- D. Dumpster diving

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 8

After verifying that the server and database are running, Jane, the administrator, is still unable to make a TCP connection to the database. Which of the following is the MOST likely cause for this?

- A. The server has data execution prevention enabled
- B. The server has TPM based protection enabled
- C. The server has HIDS installed
- D. The server is running a host-based firewall

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 9

In regards to secure coding practices, why is input validation important?

- A. It mitigates buffer overflow attacks.
- B. It makes the code more readable.
- C. It provides an application configuration baseline.
- D. It meets gray box testing standards.

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 10

Which of the following is a best practice before deploying a new desktop operating system image?

- A. Install network monitoring software
- B. Perform white box testing
- C. Remove single points of failure
- D. Verify operating system security settings

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 11

Which of the following steps should follow the deployment of a patch?

- A. Antivirus and anti-malware deployment
- B. Audit and verification
- C. Fuzzing and exploitation
- D. Error and exception handling

Correct Answer: B

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 12

Which of the following would be used when a higher level of security is desired for encryption key storage?

- A. TACACS+
- B. L2TP
- C. LDAP
- D. TPM

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 13

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

- A. Firewall
- B. Application
- C. IDS
- D. Security

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 14

If Pete, a security administrator, wants to ensure that certain users can only gain access to the system during their respective shifts, which of the following best practices would he implement?

- A. Separation of duties
- B. Time of day restrictions
- C. Implicit deny rule
- D. Least privilege

Correct Answer: B
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 15

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: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 16

A small business owner has asked the security consultant to suggest an inexpensive means to deter physical intrusions at their place of business. Which of the following would **BEST** meet their request?

- A. Fake cameras
- B. Proximity readers
- C. Infrared cameras
- D. Security guards

Correct Answer: A
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 17

Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

- A. Smartcard
- B. Token
- C. Discretionary access control
- D. Mandatory access control

Correct Answer: A
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 18

Which of the following devices would MOST likely have a DMZ interface?

- A. Firewall
- B. Switch
- C. Load balancer
- D. Proxy

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 19

A security administrator is observing congestion on the firewall interfaces and a high number of half open incoming connections from different external IP addresses. Which of the following attack types is underway?

- A. Cross-site scripting
- B. SPIM
- C. Client-side
- D. DDoS

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 20

Which of the following tools would Matt, a security administrator, MOST likely use to analyze a malicious payload?

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

Correct Answer: D

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 21

Which of the following application security testing techniques is implemented when an automated system generates random input data?

- A. Fuzzing
- B. XSRF
- C. Hardening
- D. Input validation

Correct Answer: A
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 22

Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

- A. Cognitive password
- B. Password sniffing
- C. Brute force
- D. Social engineering

Correct Answer: C
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 23

A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

Correct Answer: C
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 24

Certificates are used for: (Select TWO).

- A. client authentication.
- B. WEP encryption.
- C. access control lists.
- D. code signing.
- E. password hashing.

Correct Answer: AD
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 25

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

Correct Answer: C

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 26

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications
- D. Placing a firewall between the Internet and database servers

Correct Answer: C

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 27

Which of the following BEST describes a common security concern for cloud computing?

- A. Data may be accessed by third parties who have compromised the cloud platform
- B. Antivirus signatures are not compatible with virtualized environments
- C. Network connections are too slow
- D. CPU and memory resources may be consumed by other servers in the same cloud

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

Correct Answer: B

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 29

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: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 30

Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

- A. Malicious code on the local system
- B. Shoulder surfing
- C. Brute force certificate cracking
- D. Distributed dictionary attacks

Correct Answer: A

Section: Group 1

Explanation

Explanation/Reference:

Explanation:

QUESTION 31

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production
- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 32

A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

- A. The request needs to be sent to the incident management team.
- B. The request needs to be approved through the incident management process.
- C. The request needs to be approved through the change management process.
- D. The request needs to be sent to the change management team.

Correct Answer: C

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 33

Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

- A. Phishing
- B. Tailgating
- C. Pharming
- D. Vishing

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 34

The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following **MUST** be implemented to allow this type of authorization?

- A. Use of CA certificate
- B. Use of public keys only
- C. Use of private keys only
- D. Use of public and private keys

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 35

A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will **MOST** likely be implemented within the company?

- A. Account lockout policy
- B. Account password enforcement
- C. Password complexity enabled
- D. Separation of duties

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 36

An employee is granted access to only areas of a network folder needed to perform their job. Which of the following describes this form of access control?

- A. Separation of duties
- B. Time of day restrictions
- C. Implicit deny
- D. Least privilege

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 37

A CRL is comprised of:

- A. malicious IP addresses.
- B. trusted CA's.
- C. untrusted private keys.
- D. public keys.

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 38

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?



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

- A. Logic bomb
- B. Worm
- C. Trojan
- D. Adware

Correct Answer: C

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 39

Which of the following may significantly reduce data loss if multiple drives fail at the same time?

- A. Virtualization
- B. RAID
- C. Load balancing
- D. Server clustering

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 40

Which of the following should be considered to mitigate data theft when using CAT5 wiring?

- A. CCTV
- B. Environmental monitoring
- C. Multimode fiber
- D. EMI shielding

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 41

To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

- A. Management
- B. Administrative
- C. Technical
- D. Operational

Correct Answer: C

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

- A. Connect the WAP to a different switch.
- B. Create a voice VLAN.
- C. Create a DMZ.
- D. Set the switch ports to 802.1q mode.

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 43

Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

- A. 10.4.4.125
- B. 10.4.4.158
- C. 10.4.4.165
- D. 10.4.4.189
- E. 10.4.4.199

Correct Answer: CD

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 44

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: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 45

Jane, the security administrator, needs to be able to test malicious code in an environment where it will not harm the rest of the network. Which of the following would allow Jane to perform this kind of testing?

- A. Local isolated environment
- B. Networked development environment
- C. Infrastructure as a Service
- D. Software as a Service

Correct Answer: A
Section: Group 2
Explanation

Explanation/Reference:
Explanation:

QUESTION 46

A company is sending out a message to all users informing them that all internal messages need to be digitally signed. This is a form of which of the following concepts?

- A. Availability
- B. Non-repudiation
- C. Authorization
- D. Cryptography

Correct Answer: B
Section: Group 2
Explanation

Explanation/Reference:
Explanation:

QUESTION 47

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

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

Correct Answer: D
Section: Group 2
Explanation

Explanation/Reference:
Explanation:

QUESTION 48

Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

- A. Incident management
- B. Clean desk policy
- C. Routine audits
- D. Change management

Correct Answer: D
Section: Group 2
Explanation

Explanation/Reference:
Explanation:

QUESTION 49

A server containing critical data will cost the company \$200/hour if it were to be unavailable due to DoS attacks. The security administrator expects the server to become unavailable for a total of two days next year. Which of the following is true about the ALE?

- A. The ALE is \$48.
- B. The ALE is \$400.
- C. The ALE is \$4,800.
- D. The ALE is \$9,600.

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 50

To reduce an organization's risk exposure by verifying compliance with company policy, which of the following should be performed periodically?

- A. Qualitative analysis
- B. Quantitative analysis
- C. Routine audits
- D. Incident management

Correct Answer: C

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

Which of the following is a difference between TFTP and FTP?

- A. TFTP is slower than FTP.
- B. TFTP is more secure than FTP.
- C. TFTP utilizes TCP and FTP uses UDP.
- D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 52

A system administrator decides to use SNMPv3 on the network router in AuthPriv mode. Which of the following algorithm combinations would be valid?

- A. AES-RC4
- B. 3DES-MD5
- C. RSA-DSA

D. SHA1-HMAC

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 53

Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).

- A. AES
- B. RC4
- C. Twofish
- D. DES
- E. SHA2

Correct Answer: AC

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 54

Matt, an administrator, notices a flood fragmented packet and retransmits from an email server. After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

- A. Spam filter
- B. Protocol analyzer
- C. Web application firewall
- D. Load balancer

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 55

Which of the following specifications would Sara, an administrator, implement as a network access control?

- A. 802.1q
- B. 802.3
- C. 802.11n
- D. 802.1x

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

- A. Whaling
- B. Impersonation
- C. Privilege escalation
- D. Spear phishing

Correct Answer: A

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

Which of the following defines when Pete, an attacker, attempts to monitor wireless traffic in order to perform malicious activities?

- A. XSS
- B. SQL injection
- C. Directory traversal
- D. Packet sniffing

Correct Answer: D

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

Which of the following provides the MOST protection against zero day attacks via email attachments?

- A. Anti-spam
- B. Anti-virus
- C. Host-based firewalls
- D. Patch management

Correct Answer: A

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

Which of the following would MOST likely ensure that swap space on a hard disk is encrypted?

- A. Database encryption
- B. Full disk encryption
- C. Folder and file encryption

D. Removable media encryption

Correct Answer: B

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

Which of the following access controls enforces permissions based on data labeling at specific levels?

- A. Mandatory access control
- B. Separation of duties access control
- C. Discretionary access control
- D. Role based access control

Correct Answer: A

Section: Group 2

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

A username provides which of the following?

- A. Biometrics
- B. Identification
- C. Authorization
- D. Authentication

Correct Answer: B

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

Use of group accounts should be minimized to ensure which of the following?

- A. Password security
- B. Regular auditing
- C. Baseline management
- D. Individual accountability

Correct Answer: D

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

Privilege creep among long-term employees can be mitigated by which of the following procedures?

- A. User permission reviews
- B. Mandatory vacations
- C. Separation of duties
- D. Job function rotation

Correct Answer: A

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

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: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

Configuring the mode, encryption methods, and security associations are part of which of the following?

- A. IPSec
- B. Full disk encryption
- C. 802.1x
- D. PKI

Correct Answer: A

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

- A. Code review
- B. Penetration test
- C. Protocol analyzer
- D. Vulnerability scan

Correct Answer: B

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 67

Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

- A. Penetration test
- B. Code review
- C. Vulnerability scan
- D. Brute Force scan

Correct Answer: C

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 68

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

- A. Confidentiality
- B. Availability
- C. Succession planning
- D. Integrity

Correct Answer: B

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 69

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

- A. Take hashes
- B. Begin the chain of custody paperwork
- C. Take screen shots
- D. Capture the system image
- E. Decompile suspicious files

Correct Answer: AD

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

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: Group 3

Explanation

Explanation/Reference:

Explanation:

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: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 72

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

- A. Steganography images
- B. Internal memory
- C. Master boot records
- D. Removable memory cards
- E. Public keys

Correct Answer: BD

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 73

When checking his webmail, Matt, a user, changes the URL's string of characters and is able to get into another user's inbox. This is an example of which of the following?

- A. Header manipulation
- B. SQL injection
- C. XML injection
- D. Session hijacking

Correct Answer: D

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 74

Elliptic curve cryptography: (Select TWO)

- A. is used in both symmetric and asymmetric encryption.
- B. is used mostly in symmetric encryption.
- C. is mostly used in embedded devices.
- D. produces higher strength encryption with shorter keys.
- E. is mostly used in hashing algorithms.

Correct Answer: CD

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 75

Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

- A. Buffer overflow prevention
- B. Input validation
- C. CSRF prevention
- D. Cross-site scripting prevention

Correct Answer: B

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 76

Which of the following would an antivirus company use to efficiently capture and analyze new and unknown malicious attacks?

- A. Fuzzer
- B. IDS
- C. Proxy
- D. Honeynet

Correct Answer: D

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 77

Why is it important for a penetration tester to have established an agreement with management as to which systems and processes are allowed to be tested?

- A. Penetration test results are posted publicly, and some systems tested may contain corporate secrets.
- B. Penetration testers always need to have a comprehensive list of servers, operating systems, IP subnets, and department personnel prior to ensure a complete test.
- C. Having an agreement allows the penetration tester to look for other systems out of scope and test them for threats against the in-scope systems.
- D. Some exploits when tested can crash or corrupt a system causing downtime or data loss.

Correct Answer: D

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 79

An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame. Which of the following strategies would the administrator MOST likely implement?

- A. Full backups on the weekend and incremental during the week
- B. Full backups on the weekend and full backups every day
- C. Incremental backups on the weekend and differential backups every day
- D. Differential backups on the weekend and full backups every day

Correct Answer: A

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 80

Which of the following can be used in code signing?

- A. AES
- B. RC4

- C. GPG
- D. CHAP

Correct Answer: C

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 81

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: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 82

Which of the following defines a business goal for system restoration and acceptable data loss?

- A. MTTR
- B. MTBF
- C. RPO
- D. Warm site

Correct Answer: C

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 83

Which of the following defines an organization goal for acceptable downtime during a disaster or other contingency?

- A. MTBF
- B. MTTR
- C. RTO
- D. RPO

Correct Answer: C

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 84

If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

- A. Transitive trust
- B. Public key trust
- C. Certificate authority trust
- D. Domain level trust

Correct Answer: A

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 85

Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

- A. CCTV system access
- B. Dial-up access
- C. Changing environmental controls
- D. Ping of death

Correct Answer: C

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 86

Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

- A. Business continuity planning
- B. Continuity of operations
- C. Business impact analysis
- D. Succession planning

Correct Answer: D

Section: Group 3

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

An ACL placed on which of the following ports would block IMAP traffic?

- A. 110
- B. 143

- C. 389
- D. 465

Correct Answer: B
Section: Group 3
Explanation

Explanation/Reference:
Explanation:

QUESTION 88

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: Group 3
Explanation

Explanation/Reference:
Explanation:

QUESTION 89

Which of the following controls should be used to verify a person in charge of payment processing is not colluding with anyone to pay fraudulent invoices?

- A. Least privilege
- B. Security policy
- C. Mandatory vacations
- D. Separation of duties

Correct Answer: C
Section: Group 3
Explanation

Explanation/Reference:
Explanation:

QUESTION 90

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: Group 3
Explanation

Explanation/Reference:

Explanation:

QUESTION 91

Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

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

Correct Answer: C

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

QUESTION 92

In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

- A. Security control frameworks
- B. Best practice
- C. Access control methodologies
- D. Compliance activity

Correct Answer: B

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

QUESTION 93

Which of the following devices is typically used to provide protection at the edge of the network attack surface?

- A. Firewall
- B. Router
- C. Switch
- D. VPN concentrator

Correct Answer: A

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

QUESTION 94

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

- A. ICMP
- B. BGP

- C. NetBIOS
- D. DNS

Correct Answer: C

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

QUESTION 95

In an enterprise environment, which of the following would be the BEST way to prevent users from accessing inappropriate websites when AUP requirements are constantly changing?

- A. Deploy a network proxy server.
- B. Configure Internet content filters on each workstation.
- C. Deploy a NIDS.
- D. Deploy a HIPS.

Correct Answer: A

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

QUESTION 96

How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

- A. Annually
- B. Immediately after an employee is terminated
- C. Every five years
- D. Every time they patch the server

Correct Answer: A

Section: Group 10

Explanation

Explanation/Reference:

Explanation:

ExamB

QUESTION 1

Matt, an IT security technician, needs to create a way to recover lost or stolen company devices. Which of the following BEST meets this need?

- A. Locking cabinets
- B. GPS tracking
- C. Safe
- D. Firewalls

Correct Answer: B

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 2

An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

- A. Implement IIS hardening by restricting service accounts.
- B. Implement database hardening by applying vendor guidelines.
- C. Implement perimeter firewall rules to restrict access.
- D. Implement OS hardening by applying GPOs.

Correct Answer: D

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 3

Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?

- A. Logic bomb
- B. Spyware
- C. Backdoor
- D. Adware

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 4

Which of the following is the MOST specific plan for various problems that can arise within a system?

- A. Business Continuity Plan
- B. Continuity of Operation Plan

- C. Disaster Recovery Plan
- D. IT Contingency Plan

Correct Answer: D

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 5

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: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

Which of the following BEST describes the weakness in WEP encryption?

- A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
- B. The WEP key is stored in plain text and split in portions across 224 packets of random data. Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
- C. The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
- D. The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 7

Which of the following is used to ensure message integrity during a TLS transmission?

- A. RIPEMD
- B. RSA
- C. AES
- D. HMAC

Correct Answer: D

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 8

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company \$3,000. A third party vendor has offered to repair the security hole in the system for \$25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?

- A. Accept the risk saving \$10,000.
- B. Ignore the risk saving \$5,000.
- C. Mitigate the risk saving \$10,000.
- D. Transfer the risk saving \$5,000.

Correct Answer: D

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 9

A company has asked Pete, a penetration tester, to test their corporate network. Pete was provided with all of the server names, configurations, and corporate IP addresses. Pete was then instructed to stay off of the Accounting subnet as well as the company web server in the DMZ. Pete was told that social engineering was not in the test scope as well. Which of the following BEST describes this penetration test?

- A. Gray box
- B. Black box
- C. White box
- D. Blue box

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 10

Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

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

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 11

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

- A. Input validation
- B. Network intrusion detection system
- C. Anomaly-based HIDS
- D. Peer review

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 12

Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

- A. Sign in and sign out logs
- B. Mantrap
- C. Video surveillance
- D. HVAC

Correct Answer: B

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 13

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

- A. Water base sprinkler system
- B. Electrical
- C. HVAC
- D. Video surveillance

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 14

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

- A. Hardware load balancing
- B. RAID

- C. A cold site
- D. A host standby

Correct Answer: B

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 15

Pete has obtained a highly sensitive document and has placed it on a network drive which has been formatted with NTFS and is shared via CIFS. Which of the following access controls apply to the sensitive file on the server?

- A. Discretionary
- B. Rule based
- C. Role based
- D. Mandatory

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 16

Which of the following fire suppression systems is MOST likely used in a datacenter?

- A. FM-200
- B. Dry-pipe
- C. Wet-pipe
- D. Vacuum

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 17

A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 18

Which of the following uses only a private key?

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

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 19

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. Directory traversal

Correct Answer: B

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 20

Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

- A. Vulnerability assessment
- B. Black box testing
- C. White box testing
- D. Penetration testing

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 21

A database server containing personal information and a file server containing non-critical information must be secured. Which of the following would be a BEST practice to secure the servers? (Select TWO).

- A. Place the file server behind a door requiring biometric authorization.

- B. Place both servers under the system administrator's desk.
- C. Place the database server behind a door with a cipher lock.
- D. Place the file server in an unlocked rack cabinet.
- E. Place the database server behind a door requiring biometric authorization.

Correct Answer: AE

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 22

A company is experiencing an extraordinary amount of web traffic that is crippling the server. The web traffic suddenly stops. The mail server experiences the same amount of traffic as before then crashes. Which of the following attacks would this BEST describe?

- A. DoS
- B. Spam
- C. Man-in-the-middle
- D. Replay

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 23

Matt, an account manager, arrives at work early in the morning and cannot log into his workstation. He calls the help desk an hour later to open a trouble ticket, but they tell him there is nothing wrong with his account. Matt tries his login once more and is granted access. Which of the following control types BEST explains this anomaly?

- A. Discretionary access control
- B. Time of day restrictions
- C. Separation of duties
- D. Single sign-on

Correct Answer: B

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 24

Which of the following would ensure confidentiality and authorization to the management interface of a router?

- A. Enable an access list and RADIUS
- B. Enable SSH and TACACS
- C. Enable an access list and PKI
- D. Enable LDAP and strong passwords

Correct Answer: B
Section: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 25

Which of the following BEST describes a demilitarized zone?

- A. A buffer zone between protected and unprotected networks.
- B. A network where all servers exist and are monitored.
- C. A sterile, isolated network segment with access lists.
- D. A private network that is protected by a firewall and a VLAN.

Correct Answer: A
Section: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 26

A security technician is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains the support for fraud detection?

- A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
- B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
- C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
- D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

Correct Answer: D
Section: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 27

A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

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

Correct Answer: A
Section: Group 7
Explanation

Explanation/Reference:

Explanation:

QUESTION 28

Sara, a security administrator, has been tasked with explaining smart cards to the company's management team. Which of the following are smart cards? (Select TWO).

- A. DAC
- B. Tokens
- C. CAC
- D. ACL
- E. PIV

Correct Answer: CE

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 29

Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

- A. Kerberos
- B. Least privilege
- C. TACACS+
- D. LDAP

Correct Answer: A

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 30

Jane, a security architect, is implementing security controls throughout her organization. Which of the following BEST explains the vulnerability in the formula that a Risk = Threat x Vulnerability x Impact?

- A. Vulnerability is related to the risk that an event will take place.
- B. Vulnerability is related to value of potential loss.
- C. Vulnerability is related to the probability that a control will fail.
- D. Vulnerability is related to the probability of the event.

Correct Answer: C

Section: Group 7

Explanation

Explanation/Reference:

Explanation:

QUESTION 31

The information security department regularly walks the campus and around the buildings looking for unauthorized open wireless networks. This is an example of which of the following?

- A. A site survey
- B. Antenna placement
- C. War dialing
- D. War driving

Correct Answer: D

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 32

The lobby of the hotel allows users to plug in their laptops to access the Internet. This network is also used for the IP based phones in the hotel lobby. Mike, the security engineer, wants to secure the phones so that guests cannot electronically eavesdrop on other guests. Which of the following would Mike MOST likely implement?

- A. VLAN
- B. Port security
- C. MPLS
- D. Separate voice gateway

Correct Answer: A

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 33

Jane, the security engineer, is tasked with hardening routers. She would like to ensure that network access to the corporate router is allowed only to the IT group and from authorized machines. Which of the following would MOST likely be implemented to meet this security goal? (Select TWO).

- A. SNMP
- B. HTTPS
- C. ACL
- D. Disable console
- E. SSH
- F. TACACS+

Correct Answer: CF

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 34

Which of the following can be used to discover if a security attack is occurring on a web server?

- A. Creating a new baseline
- B. Disable unused accounts
- C. Implementing full disk encryption
- D. Monitoring access logs

Correct Answer: D
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 35

Jane, the CEO, receives an email wanting her to click on a link to change her username and password. Which of the following attacks has she just received?

- A. Hoaxes
- B. Whaling
- C. Bluejacking
- D. Vishing

Correct Answer: B
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 36

Pete, the system administrator, wishes to monitor and limit users' access to external websites. Which of the following would BEST address this?

- A. Block all traffic on port 80.
- B. Implement NIDS.
- C. Use server load balancers.
- D. Install a proxy server.

Correct Answer: D
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 37

Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

- A. PAT
- B. NAP
- C. DNAT
- D. NAC

Correct Answer: A
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 38

Which of the following settings can Jane, the network administrator, implement in the computer lab to ensure that user credentials cannot be captured by the next computer user?

- A. Implement full drive encryption on all lab computers.
- B. Reverse the computer to its original state upon reboot.
- C. Do not display last username in logon screen.
- D. Deploy privacy screens on all lab computers.

Correct Answer: C

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 39

Jane, a security administrator, is reviewing the company's official documentation to mitigate the risk of data loss due to personally owned devices being connected to perform company related work. Which of the following documentation should Jane MOST likely review and update?

- A. Acceptable risk
- B. Data retention policy
- C. Acceptable use policy
- D. End user license agreement

Correct Answer: C

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 40

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

- A. Succession planning
- B. Disaster recovery plan
- C. Information security plan
- D. Business impact analysis

Correct Answer: B

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 41

Pete, a security administrator, has implemented SSH across all network infrastructure devices in the enterprise. Which of the following protocols will be used to exchange keying material within SSH?

- A. Transport layer protocol
- B. IPSec

- C. Diffie-Hellman
- D. Secure socket layer

Correct Answer: C

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

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: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 43

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is \$300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

- A. \$1,500
- B. \$3,750
- C. \$15,000
- D. \$75,000

Correct Answer: B

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 44

Matt must come up with a design solution which will enable remote users to securely access network resources. Which of the following design elements will enable Matt to meet this objective?

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

Correct Answer: C

Section: Group 8**Explanation****Explanation/Reference:**

Explanation:

QUESTION 45

Sara, a security technician, has been asked to design a solution which will enable external users to have access to a Web server, while keeping the internal network unaffected by this access. Which of the following would BEST meet this objective?

- A. Place the Web server on a VLAN
- B. Place the Web server inside of the internal firewall
- C. Place the Web server in a DMZ
- D. Place the Web server on a VPN

Correct Answer: C

Section: Group 8**Explanation****Explanation/Reference:**

Explanation:

QUESTION 46

Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

- A. TCP 23
- B. UDP 69
- C. TCP 22
- D. TCP 21

Correct Answer: C

Section: Group 8**Explanation****Explanation/Reference:**

Explanation:

QUESTION 47

Matt, a security technician, notices a high number of ARP spoofing attacks on his network. Which of the following design elements would mitigate ARP spoofing attacks?

- A. Flood guards
- B. Implicit deny
- C. VLANs
- D. Loop protection

Correct Answer: A

Section: Group 8**Explanation****Explanation/Reference:**

Explanation:

QUESTION 48

Matt works for an organization that requires data to be recovered in the shortest amount of time possible. Which of the following backup types would BEST meet the organization's needs?

- A. Full backups daily
- B. Differential backups monthly
- C. Full backups weekly
- D. Incremental backups monthly

Correct Answer: A

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 49

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

- A. Warm site
- B. Load balancing
- C. Clustering
- D. RAID

Correct Answer: C

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 50

How would a technician secure a router configuration if placed in an unsecured closet?

- A. Mount the router into an immovable rack.
- B. Enable SSH for maintenance of the router.
- C. Disable the console port on the router.
- D. Label the router with contact information.

Correct Answer: C

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

Which of the following firewall rules would only block tftp traffic and record it?

- A. deny udp any server log
- B. deny udp any server eq 69
- C. deny tcp any server log
- D. deny udp any server eq 69 log

Correct Answer: D

Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 52

Which of the following services should be disabled to stop attackers from using a web server as a mail relay?

- A. IMAP
- B. SMTP
- C. SNMP
- D. POP3

Correct Answer: B
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 53

A security administrator has a requirement to encrypt several directories that are non-hierarchical. Which of the following encryption models would BEST meet this requirement?

- A. AES512
- B. Database encryption
- C. File encryption
- D. Full disk encryption

Correct Answer: D
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 54

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are backdoors and logic bombs. Which of the following differentiates these two types of malware?

- A. A backdoor is a coding issue that can be discovered by proper configuration management processes.
- B. A logic bomb is typically hidden within the boot sector of the hard drive and is used to cause DDoS.
- C. A backdoor is a third generation attack which is typically low risk because only highly trained staff can achieve it.
- D. A logic bomb is undetectable by current antivirus signatures because a patch has not been issued.

Correct Answer: A
Section: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 55

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

- A. Viruses are a subset of botnets which are used as part of SYN attacks.
- B. Botnets are a subset of malware which are used as part of DDoS attacks.
- C. Viruses are a class of malware which create hidden openings within an OS.
- D. Botnets are used within DR to ensure network uptime and viruses are not.

Correct Answer: B

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

Which of the following BEST explains the use of an HSM within the company servers?

- A. Thumb drives present a significant threat which is mitigated by HSM.
- B. Software encryption can perform multiple functions required by HSM.
- C. Data loss by removable media can be prevented with DLP.
- D. Hardware encryption is faster than software encryption.

Correct Answer: D

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

Which of the following technologies can store multi-tenant data with different security requirements?

- A. Data loss prevention
- B. Trusted platform module
- C. Hard drive encryption
- D. Cloud computing

Correct Answer: D

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

Which of the following technologies prevents USB drives from being recognized by company systems?

- A. Registry keys
- B. Full disk encryption
- C. USB encryption
- D. Data loss prevention

Correct Answer: A

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

- A. Matt should implement access control lists and turn on EFS.
- B. Matt should implement DLP and encrypt the company database.
- C. Matt should install Truecrypt and encrypt the company server.
- D. Matt should install TPMs and encrypt the company database.

Correct Answer: B

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

Which of the following types of encryption will help in protecting files on a PED?

- A. Mobile device encryption
- B. Transport layer encryption
- C. Encrypted hidden container
- D. Database encryption

Correct Answer: A

Section: Group 8

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

Which of the following is MOST closely associated with BitLocker?

- A. ACL
- B. DOS
- C. DLP
- D. TPM

Correct Answer: D

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

Which of the following does full disk encryption prevent?

- A. Client side attacks

- B. Clear text access
- C. Database theft
- D. Network-based attacks

Correct Answer: B

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

- A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
- B. Tell the application development manager to code the application to adhere to the company's password policy.
- C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
- D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Correct Answer: B

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

- A. A recent security breach in which passwords were cracked.
- B. Implementation of configuration management processes.
- C. Enforcement of password complexity requirements.
- D. Implementation of account lockout procedures.

Correct Answer: A

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

Which of the following presents the STRONGEST access control?

- A. MAC
- B. TACACS
- C. DAC
- D. RBAC

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 66

Which of the following encompasses application patch management?

- A. Configuration management
- B. Policy management
- C. Cross-site request forgery
- D. Fuzzing

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 67

Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

- A. Buffer overflow
- B. Pop-up blockers
- C. Cross-site scripting
- D. Fuzzing

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 68

Which of the following is the LEAST volatile when performing incident response procedures?

- A. Registers
- B. RAID cache
- C. RAM
- D. Hard drive

Correct Answer: D
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 69

Which of the following can allow Sara, a security analyst, to encrypt individual files on a system?

- A. EFS
- B. Single sign-on
- C. TLS
- D. Journaled file system

Correct Answer: A

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 70

An encryption method where the plain text and cipher text are always the same size is an example of which of the following types of encryption?

- A. RC4
- B. MD5
- C. Stream Cipher
- D. Block Cipher

Correct Answer: D

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

- A. Rainbow tables attacks
- B. Brute force attacks
- C. Birthday attacks
- D. Cognitive passwords attacks

Correct Answer: D

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 72

The compliance team comes out with a new policy that all data stored on tapes over 3 years must be degaussed. This BEST describes which of the following types of policies?

- A. Data handling
- B. Data classification
- C. Data labeling
- D. Data disposal

Correct Answer: D

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 73

Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

- A. Collusion
- B. Impersonation
- C. Pharming
- D. Transitive Access

Correct Answer: B

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 74

Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

- A. Interference
- B. Man-in-the-middle
- C. ARP poisoning
- D. Rogue access point

Correct Answer: D

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 75

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

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

Correct Answer: A

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 76

Jane, the security administrator, is having issues with unauthorized users connecting to the wireless network. For administrative reasons, she cannot implement any wireless encryption methods. Which of the following can she implement to prevent unauthorized users from connecting to the network?

- A. NIPS
- B. Disable unused ports
- C. MAC filtering
- D. WEP

Correct Answer: C

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 77

Matt, the security administrator, wants to secure the wireless network. Which of the following encryption methods offers the MOST security?

- A. WPA2 ENT AES
- B. WPA2 PSK AES
- C. WPA2 ENT TKIP
- D. WPA2 PSK TKIP

Correct Answer: A

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

Sara, the IT administrator, wants to control which devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

- A. WPA2 Enterprise with AES encryption
- B. Decrease the WAP's power levels
- C. Static IP addressing
- D. MAC address filtering

Correct Answer: D

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 79

Pete, the system administrator, has instituted a policy banning personal digital music and video players from the company premises. Which of the following would be the BEST reason for such a policy?

- A. The company would be legally liable for any personal device that is lost on its premises.
- B. It is difficult to verify ownership of offline device's digital rights management and ownership.

- C. The media players may act as distractions during work hours and adversely affect user productivity.
- D. If connected to a computer, unknown malware may be introduced into the environment.

Correct Answer: D

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 80

Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

- A. No competition with the company's official social presence
- B. Protection against malware introduced by banner ads
- C. Increased user productivity based upon fewer distractions
- D. Elimination of risks caused by unauthorized P2P file sharing

Correct Answer: B

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 81

Pete, the system administrator, is concerned about unauthorized access at all entrances into the building. PIN pad readers have been installed, but users have developed the habit of holding the door for others behind them. Which of the following would BEST prevent this?

- A. Install mantraps at every unmanned entrance.
- B. Replace the PIN pad readers with card readers.
- C. Implement video and audio surveillance equipment.
- D. Require users to sign conduct policies forbidding these actions.

Correct Answer: A

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 82

Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

- A. Use hardware already at an offsite location and configure it to be quickly utilized.
- B. Move the servers and data to another part of the company's main campus from the server room.
- C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
- D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Correct Answer: A

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 83

Jane, a network administrator, has configured a 48-port switch to isolate four different departments. Which of the following has Jane MOST likely configured on the switch?

- A. NAC
- B. 802.1x
- C. VLAN
- D. DMZ

Correct Answer: C

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 84

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: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 85

Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

- A. PAP, MSCHAPv2
- B. CHAP, PAP
- C. MSCHAPv2, NTLMv2
- D. NTLM, NTLMv2

Correct Answer: A

Section: Group 9**Explanation****Explanation/Reference:**

Explanation:

QUESTION 86

Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

- A. Authentication server
- B. Server certificate
- C. Key length
- D. EAP method

Correct Answer: C

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

- A. EAP-MD5
- B. WEP
- C. PEAP-MSCHAPv2
- D. EAP-TLS

Correct Answer: C

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 88

A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

- A. DMZ
- B. Cloud computing
- C. VLAN
- D. Virtualization

Correct Answer: A

Section: Group 9

Explanation

Explanation/Reference:

Explanation:

QUESTION 89

Layer 7 devices used to prevent specific types of html tags are called:

- A. firewalls.
- B. content filters.
- C. routers.
- D. NIDS.

Correct Answer: B
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 90

Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

- A. Attributes based
- B. Implicit deny
- C. Role based
- D. Rule based

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 91

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

- A. The network uses the subnet of 255.255.255.128.
- B. The switch has several VLANs configured on it.
- C. The sub-interfaces are configured for VoIP traffic.
- D. The sub-interfaces each implement quality of service.

Correct Answer: B
Section: Group 10
Explanation

Explanation/Reference:
Explanation:

QUESTION 92

Digital Signatures provide which of the following?

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

Correct Answer: C
Section: Group 10
Explanation

Explanation/Reference:
Explanation:

QUESTION 93

-- Exhibit

