SY0-301 152qa

SY0-301

CompTIA Security+

SY0-301

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 5
All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.

B. RC4.

C. SHA-512.

D. MD4.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is a hardware based encryption device?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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

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

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

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?

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

Correct Answer: C

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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

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

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

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

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 61
A username provides which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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

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

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

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

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:

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:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following can be used in code signing?

A. AES

B. RC4
C. GPG
D. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on
B. IPv6
C. Secure zone transfers
D. VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

A. HIPS
B. Antivirus
C. NIDS
D. ACL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP
B. DNS
C. TLS
D. ICMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following anti-malware solutions can be implemented to mitigate the risk of phishing?

A. Host based firewalls
B. Anti-spyware

C. Anti-spam
D. Anti-virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following can be used to mitigate risk if a mobile device is lost?

A. Cable lock
B. Transport encryption
C. Voice encryption
D. Strong passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset
B. Clean desk policy
C. Cloud computing
D. Routine log review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following is an example of multifactor authentication?

A. Credit card and PIN
B. Username and password
C. Password and PIN
D. Fingerprint and retina scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:
`Please only use letters and numbers on these fields' Which of the following is this an example of?

A. Proper error handling
B. Proper input validation
C. Improper input validation
D. Improper error handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following should the security administrator do when taking a forensic image of a hard drive?

A. Image the original hard drive, hash the image, and analyze the original hard drive.
B. Copy all the files from the original into a separate hard drive, and hash all the files.
C. Hash the original hard drive, image the original hard drive, and hash the image.
D. Image the original hard drive, hash the original hard drive, and analyze the hash.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design
B. Application security
C. Initial baseline configuration
D. Management of interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A marketing employee requests read and write permissions to the finance department's folders. The security administrator partially denies this request and only gives the marketing employee read-only permissions. This is an example of which of the following?

A. Job rotation
B. Separation of duties

C. Least privilege
D. Change management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

A. Acceptable Use Policy
B. Physical security controls
C. Technical controls
D. Security awareness training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS
B. Firewall
C. NIPS
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

QUESTION 105
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

A. War dialing
B. War chalking
C. War driving
D. Bluesnarfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin
B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

A. CRL
B. Non-repudiation
C. Trust models
D. Recovery agents

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following protocols would be used to verify connectivity between two remote devices at the LOWEST level of the OSI model?

A. DNS

B. SCP
C. SSH
D. ICMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card
B. Role based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:

A. false negative.
B. true negative.
C. false positive.
D. true positive.

Correct Answer: C
Section: (none)
Explanation

QUESTION 112
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

A. Packet filtering firewall
B. VPN gateway
C. Switch
D. Router

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.
B. Remove the network from the routing table.
C. Create a virtual switch.
D. Commission a stand-alone switch.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20
B. 21
C. 22
D. 23

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which of the following could cause a browser to display the message below? "The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
B. The website is using a wildcard certificate issued for the company's domain.
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self signed certificate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability
B. Integrity
C. Confidentiality
D. Fire suppression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which of the following pseudocodes can be used to handle program exceptions?

A. If program detects another instance of itself, then kill program instance.
B. If user enters invalid input, then restart program.
C. If program module crashes, then restart program module.
D. If user's input exceeds buffer length, then truncate the input.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following devices can Sara, an administrator, implement to detect and stop known attacks?

A. Signature-based NIDS
B. Anomaly-based NIDS
C. Signature-based NIPS
D. Anomaly-based NIPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following protocols would be implemented to secure file transfers using SSL?

A. TFTP
B. SCP
C. SFTP
D. FTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following security concepts are used for data classification and labeling to protect data? (Select TWO).

A. Need to know
B. Role based access control
C. Authentication
D. Identification
E. Authorization

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
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:

QUESTION 122
Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:

A. that someone has used war chalking to help others access the company's network.
B. that the symbols indicate the presence of an evil twin of a legitimate AP.
C. that someone is planning to install an AP where the symbols are, to cause interference.
D. that a rogue access point has been installed within range of the symbols.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following are used to implement VPNs? (Select TWO).

A. SFTP
B. IPSec
C. HTTPS
D. SNMP
E. SSL

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Matt, a security administrator, is receiving reports about several SQL injections and buffer overflows through his company's website. Which of the following would reduce the amount of these attack types?

A. Antivirus
B. Anti-spam
C. Input validation
D. Host based firewalls

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 126
Enforcing data encryption of removable media ensures that the:

A. lost media cannot easily be compromised.
B. media can be identified.
C. location of the media is known at all times.
D. identification of the user is non-repudiated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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:

QUESTION 128
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:

QUESTION 129
A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?

A. Succession planning
B. Fault tolerance
C. Continuity of operations
D. Removing single points of failure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

A. RAID
B. Clustering
C. Redundancy
D. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image
D. Interview witnesses

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 133
Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?

A. The web server is configured on the firewall's DMZ interface.
B. The VLAN is improperly configured.
C. The firewall's MAC address has not been entered into the filtering list.
D. The firewall executes an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Mike, a user, receives an email from his grandmother stating that she is in another country and needs money. The email address belongs to his grandmother. Which of the following attacks is this?

A. Man-in-the-middle
B. Spoofing
C. Relaying
D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following protocols can be used to secure traffic for telecommuters?

A. WPA
B. IPSec
C. ICMP
D. SMTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA
B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which of the following risk concepts BEST supports the identification of fraud?

A. Risk transference
B. Management controls
C. Mandatory vacations
D. Risk calculation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?

A. Chain of custody
B. Tracking man hours
C. Witnesses
D. Capturing system images

Correct Answer: A
Section: (none)
Explanation

QUESTION 140
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

A. Three factor
B. Single factor
C. Two factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?

A. Intrusion prevention system
B. Web security gateway
C. Network access control
D. IP access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Mike, a server engineer, has received four new servers and must place them in a rack in the datacenter. Which of the following is considered best practice?

A. All servers' air exhaust toward the cold aisle.

B. All servers' air intake toward the cold aisle.
C. Alternate servers' air intake toward the cold and hot aisle.
D. Servers' air intake must be parallel to the cold/hot aisles.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Mike, a security analyst, has captured a packet with the following payloaD.
GET ../../../../system32\cmd.exe

Which of the following is this an example of?

A. SQL injection
B. Directory traversal
C. XML injection
D. Buffer overflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A security administrator needs to open ports on the firewall to allow for secure data transfer. Which of the
following TCP ports would allow for secure transfer of files by default?

A. 21
B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following technologies would allow for a secure tunneled connection from one site to another?
(Select TWO).

A. SFTP
B. IPSec
C. SSH
D. HTTPS
E. ICMP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Which of the following sets numerous flag fields in a TCP packet?

A. XMAS
B. DNS poisoning
C. SYN flood
D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Which of the following network design elements provides for a one-to-one relationship between an internal network address and an external network address?

A. NAT
B. NAC
C. VLAN
D. PAT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Using proximity card readers instead of the traditional key punch doors would help to mitigate:

A. impersonation.
B. tailgating.
C. dumpster diving.
D. shoulder surfing.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic

patterns?

A. Syslog
B. Protocol analyzer
C. Proxy server
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
TKIP uses which of the following encryption ciphers?

A. RC5
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Jane, an administrator, needs to transfer DNS zone files from outside of the corporate network.
Which of the following protocols must be used?

A. TCP
B. ICMP
C. UDP
D. IP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: