Comptia SY0-301 Exam Bundle

Number: SY0-301
Passing Score: 750
Time Limit: 90 min
File Version: 29.8

Comptia SY0-301 Exam Bundle

Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version

Sections

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
All of the following are valid cryptographic hash functions EXCEPT:

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

Correct Answer: B
Section: Group 1
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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
Section: Group 2
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28

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 29
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 30
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 31
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 32
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 33
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:

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
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
Jane, the CEO, receives an email wanting her to clink 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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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. Steam Cipher
D. Block Cipher

Correct Answer: D
Section: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 42

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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
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 57
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 58
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 59
-- Exhibit