JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

Which of the following database designs provides the BEST security for the online store?

A. Use encryption for the credential fields and hash the credit card field

B. Encrypt the username and hash the password

C. Hash the credential fields and use encryption for the credit card field

D. Hash both the credential fields and the credit card field

Correct Answer: C

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables. One main characteristic of hashing is that the algorithm must have few or no collisions in hashing two different inputs does not give the same output. Thus the credential fields should be hashed because anyone customer will have a unique credit card number/identity and since they will use their credit cards for many different transactions, the credit card field should be encrypted only, not hashed.

Incorrect Answers:

A: Encryption should be used on the credit card field because the customers could be making many separate transactions using the same credit card. The credential field should be hashed and not encrypted because anyone customer would most likely use a credit card to make purchases and not many credit cards to make purchases at the same online store.

B: Credit card customers would not be using usernames and passwords to make purchases from an online store.

D: Hashing the credit card field will limit the customers to one transaction only and not multiple separate transactions.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 255, 291

QUESTION 2

Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports

B. Use channels 1, 4 and 7 only

C. Enable MAC filtering

D. Disable SSID broadcast

E. Switch from 802.11a to 802.11b

Correct Answer: CD

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it\\'s a discoverable value using a wireless

packet sniffer. Thus, the SSID should be disabled if the network isn\\'t for public use.

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Incorrect Answers:

A: Disabling the wired ports will not prevent outsiders from connecting to the AP and gaining unauthorized access.

B: Selecting the correct channels will prevent interference, not unauthorized access.

E: Doing this will decrease the bandwidth and increase the risk of interference.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.
https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx

QUESTION 3

Which of the following authentication services should be replaced with a more secure alternative?

A. RADIUS

B. TACACS

C. TACACS+

D. XTACACS

Correct Answer: B

Terminal Access Controller Access-Control System (TACACS) is less secure than XTACACS, which is a proprietary extension of TACACS, and less secure than TACACS+, which replaced TACACS and XTACACS.

Incorrect Answers:

A, C: TACACS+ and RADIUS have mostly replaced TACACS and XTACACS in modern networks.

D: XTACACS is a proprietary extension of TACACS.

References: http://en.wikipedia.org/wiki/TACACS

QUESTION 4

A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interface.

PERMIT TCP ANY ANY 80 PERMIT TCP ANY ANY 443

Which of the following rules would accomplish this task? (Select TWO).

A. Change the firewall default settings so that it implements an implicit deny

B. Apply the current ACL to all interfaces of the firewall

C. Remove the current ACL

D. Add the following ACL at the top of the current ACL DENY TCP ANY ANY 53

E. Add the following ACL at the bottom of the current ACL DENY ICMP ANY ANY 53

F. Add the following ACL at the bottom of the current ACL DENY IP ANY ANY 53

Correct Answer: AF

Implicit deny is the default security stance that says if you aren\\'t specifically granted access or privileges for a resource, you\\'re denied access by default. Implicit deny is the default response when an explicit allow or deny isn\\'t present.

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. These are zone file exchanges between DNS servers, special manual queries, or used when a response exceeds 512 bytes. UDP port 53 is used for most typical DNS queries.

Incorrect Answers:

B: Applying the current ACL to all interfaces of the firewall, and adding a deny clause will also prevent internal users from performing the actions included in the deny clause.

C: Removing the current ACL will block web traffic coming in.

D: An implicit deny clause is implied at the end of each ACL.

E: ICMP is a network health and link-testing protocol, and is not related to the question.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 44.

QUESTION 5

In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

A. Continuous security monitoring

B. Baseline configuration and host hardening

C. Service Level Agreement (SLA) monitoring

D. Security alerting and trending

Correct Answer: A

The company is investing in a Governance, Risk, and Compliance (GRC) system to provide overall security posture coverage. This is great for testing the security posture. However, to be effective and ensure the company always has a good security posture, you need to monitor the security continuously.

Once a baseline security configuration is documented, it is critical to monitor it to see that this baseline is maintained or exceeded. A popular phrase among personal trainers is "that which gets measured gets improved." Well, in network security, "that which gets monitored gets secure." Continuous monitoring means exactly that: ongoing monitoring. This may involve regular measurements of network traffic levels, routine evaluations for regulatory compliance, and checks of network security device configurations.

Incorrect Answers:

B: Baseline configuration and host hardening should be performed initially or when new computer systems are implemented. However, after that has been done, you should continue to monitor the security of the system. Therefore, this answer is incorrect.

C: Service Level Agreement (SLA) monitoring is performed to ensure that the availability of the system meets SLA\\'s agreed with your customers. It does not affect or ensure the security of the system. Therefore, this answer is incorrect.

D: Security alerting and trending is important. However, this can only happen with continuous security monitoring. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 61

QUESTION 6

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

EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. Thus all wiring should be shielded to mitigate data theft.

Incorrect Answers:

A: CCTV is used to record everything it sees, thus creating evidence in case of theft. Though data theft can also occur over a network and a camera will only record the area where it is set up. Shielding is a more important data theft mitigation measure.

B: Environmental monitoring is carried out by means of a HVAC system and furthermore shielding the wiring is part of environmental monitoring.

C: Multimode fiber is not used to mitigate data theft.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 380

QUESTION 7

The Chief Technical Officer (CTO) has been informed of a potential fraud committed by a database administrator performing several other job functions within the company. Which of the following is the BEST method to prevent such activities in the future?

A. Job rotation

B. Separation of duties

C. Mandatory Vacations

D. Least Privilege

Correct Answer: B

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that you are employing best practices. The segregation of duties and separation of environments is a way to reduce the likelihood of misuse of systems or information. A separation of duties policy is designed to reduce the risk of fraud and to prevent other losses in an organization.

Incorrect Answers:

A: A job rotation policy defines intervals at which employees must rotate through positions. This is so that the company does not become too dependent on one person.

C: A mandatory vacation policy requires all users to take time away from work to refresh. If the company becomes too dependent on one person, they can end up in a real bind if something should happen to that person.

D: Least Privilege means giving users only the permissions that they need to do their work and no more.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014,pp 24, 25, 26, 153 http://en.wikipedia.org/wiki/Separation_of_duties

QUESTION 8

Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP

B. 21/TCP

C. 22/UDP

D. 22/TCP

Correct Answer: D

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

A, C: FTP ,and SSH do not make use of UDP ports.

B: FTP uses TCP port 21.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.

QUESTION 9

An administrator needs to secure RADIUS traffic between two servers. Which of the following is the BEST solution?

A. Require IPSec with AH between the servers

B. Require the message-authenticator attribute for each message

C. Use MSCHAPv2 with MPPE instead of PAP

D. Require a long and complex shared secret for the servers

Correct Answer: A

QUESTION 10

A security administrator develops a web page and limits input into the fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

A. Spoofing

B. XSS

C. Fuzzing

D. Pharming

Correct Answer: B

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug- in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the

compromised

site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts

into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

By validating user input and preventing special characters, we can prevent the injection of client- side scripting code.

Incorrect Answers:

A: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any

email that claims it requires your password or any personal information could be a trick.

In a caller ID attack, the spoofer will falsify the phone number he/she is calling from. Input validation is not used to prevent spoofing. Therefore, this answer is incorrect.

C: Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt

to make it crash. If a vulnerability is found, a tool called a fuzz tester (or fuzzer), indicates potential causes. Fuzz testing was originally developed by Barton Miller at the University of Wisconsin in 1989. This is not what is described in this

---

QUESTION 11

Joe, a technician, is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

A. OS hardening

B. Application control

C. Virtualization

D. Sandboxing

Correct Answer: C

QUESTION 12

Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow.

B. Anti-virus identifies a benign application as malware.

C. Anti-virus protection interferes with the normal operation of an application.

D. A user account is locked out after the user mistypes the password too many times.

Correct Answer: A

With a false negative, you are not alerted to a situation when you should be alerted.

Incorrect Answers:

B, C, D: This would be an example of a false positive. False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28

QUESTION 13

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

Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

Incorrect Answers:

B: Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code. This does not entail error and exception handling alongside input validation.

C: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

D: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

References: http://en.wikipedia.org/wiki/Fuzz_testing Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study

Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 338, 218 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 192, 197, 229, 246

QUESTION 14

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

Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. It provides a fast solution for the for large asymmetrical encryption calculations and is much faster than software-based cryptographic solutions.

Incorrect Answers:

A: Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. HSM is usually used in conjunction with PKI to enhance security with certification authorities (CAs). PKI secures communication. It does not secure thumb drives.

B: Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. HSM is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It provides encryption functions rather than requiring it.

C: Data loss prevention (DLP) is designed detect and prevent unauthorized access to sensitive information. It may involve content inspection, storage and transmission encryption, contextual assessment, monitoring authorizations, and centralized management. It can make use of software-based cryptographic solutions, of hardware-based cryptographic solutions such as HSM.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 238, 278 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 254

QUESTION 15

Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:

Ann: read/write

Sales Group: read

IT Group: no access

If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?

A. Add Joe to the Sales group.

B. Have the system administrator give Joe full access to the file.

C. Give Joe the appropriate access to the file directly.

D. Remove Joe from the IT group and add him to the Sales group.

Correct Answer: C