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.pass4itsure.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

FTP/S uses which of the following TCP ports by default?

A. 20 and 21

B. 139 and 445

C. 443 and 22

D. 989 and 990

Correct Answer: D

FTPS uses ports 989 and 990.

Incorrect Answers:

A: FTP makes use of ports 20 and 21.

B: Port 139 is used by NetBIOS, and port 445 is used by Microsoft-DS.

C: Port 443 is used by HTTPS, and port 22 is used by SSH and SCP.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 81-83.

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 2

Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

A. WAF

B. NIDS

C. Routers

D. Switches

Correct Answer: A

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer.

Incorrect Answers:

B: A NIDS (Network Intrusion Detection System) operates in layer 2 of the OSI model, not layer 7.

C: Routers operate in layer 3 of the OSI model, not layer 7.

D: Switches operate in layer 2 of the OSI model, not layer 7.

References: https://owasp.org/index.php/Web_Application_Firewall http://en.wikipedia.org/wiki/OSI_model

QUESTION 3

An auditor\\'s report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors\\' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding?

A. Disable unnecessary contractor accounts and inform the auditor of the update.

B. Reset contractor accounts and inform the auditor of the update.

C. Inform the auditor that the accounts belong to the contractors.

D. Delete contractor accounts and inform the auditor of the update.

Correct Answer: A

A disabled account cannot be used. It is `disabled\\'. Whenever an employee leaves a company, the employee\\'s user account should be disabled. The question states that the accounts are contractors\\' accounts who would be returning in three months. Therefore, it would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time. By disabling the accounts, we can ensure that the accounts cannot be used; in three months when the contractors are back, we can simply re-enable the accounts.

Incorrect Answers:

B: Resetting an account is typically something you would do with a computer account rather than a user account. Resetting an account clears the security identifier associated with the account which effectively creates a different account with the same name. This would prevent any access to resources that was granted to the original account. Disabling the accounts would be a better solution. Therefore, this answer is incorrect.

C: Informing the auditor that the accounts belong to the contractors would not prevent access to the accounts for the three months until the contractors return. This answer does not improve security and is therefore incorrect.

D: It would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time when the contractors return. By disabling the accounts, we can ensure that the accounts cannot be used; then in three months when the contractors are back, we can simply re-enable the accounts. Therefore, this answer is incorrect.

QUESTION 4

A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.

Which of the following activities should be performed by the IT security staff member prior to establishing the link?

A. Baseline reporting

B. Design review

C. Code review

D. SLA reporting

Correct Answer: B

This question is asking about a new private network link (a VPN) with a business partner. This will provide access to the local network from the business partner. When implementing a VPN, an important step is the design of the VPN. The VPN should be designed to ensure that the security of the network and local systems is not compromised. The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the systems or applications. A design review is basically a check to ensure that the design of the system meets the security requirements.

Incorrect Answers:

A: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). In this question, we are implementing a VPN. We need to ensure

that the design of the VPN meets the security requirements BEFORE the VPN is implemented. Therefore, this answer is incorrect.

C: A code review is the process of reviewing the code of a software application. This question is asking about the design and implementation of a VPN. Therefore, this answer is irrelevant and incorrect.

D: SLA (Service Level Agreement) reporting is the process of comparing (and reporting on) current performance in terms of system uptime or deliverables delivered on time to the metrics defined in the SLA. This question is asking about the

design and implementation of a VPN.

Therefore, this answer is irrelevant and incorrect.

QUESTION 5

A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

A. Clustering

B. Mirrored server

C. RAID

D. Tape backup

Correct Answer: C

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

Incorrect Answers:

A: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

B: Mirrored server implies that you have a mirror / duplicate of the server which will provide you with 100 % redundancy, but it does not represent the least cost option.

D: Tape Backup will also incur costs and is means for backing up data to mitigate a loss.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 34, 234, 235