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.geekcert.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

A. Application patch management

B. Cross-site scripting prevention

C. Creating a security baseline

D. System hardening

Correct Answer: D

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

Incorrect Answers:

A: Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

B: 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.

C: A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 61, 215-217, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 195, 207-208,

QUESTION 2

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

A. Intrusion Detection System

B. Flood Guard Protection

C. Web Application Firewall

D. URL Content Filter

Correct Answer: 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.

Incorrect Answers:

A: An Intrusion Detection System (IDS) is used to detect attempts to access a system. It cannot be used to detect cross-site scripting attacks where a malicious user is injecting malicious content into content being downloaded by a user.

B: Flood Guard Protection is used to prevent a network being flooded by data such as DoS, SYN floods, ping floods etc. The flood of data saturates the network and prevents the successful transmission of valid data across the network. Flood Guard Protection is not used to prevent cross-site scripting attacks. D. A URL Content Filter is used to permit access to allowed URLs (Websites) only or to block access to URLs that are not allowed according to company policy. For example, a company might use a URL Content Filter to block access to social networking sites. A URL Content Filter is not used to prevent cross-site scripting attacks.

References: http://en.wikipedia.org/wiki/Cross-site_scripting
https://www.owasp.org/index.php/Web_Application_Firewall

QUESTION 3

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

A. Block all traffic on port 80.

B. Implement NIDS.

C. Use server load balancers.

D. Install a proxy server.

Correct Answer: D

A proxy is a device that acts on behalf of other(s). In the interest of security, all internal user interaction with the Internet should be controlled through a proxy server. The proxy server should automatically block known malicious sites. The proxy server should cache often-accessed sites to improve performance.

Incorrect Answers:

A: A network-based IDS (NIDS) approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic.

B: This would block all web traffic, as port 80 is used for World Wide Web.

C: In its most common implementation, a load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 98, 103, 111.

QUESTION 4

Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

A. DLP

B. CRL

C. TPM

D. HSM

Correct Answer: A

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

Incorrect Answers:

B: A certificate revocation list is used to revoke a certificate or key. This means that a specific CA state should no longer be used.

C: TPM is used to assist with hash key generation. This will enhance security, but a DLP control would better serve the needs of the company in this instance.

D: HSM is also a crypto-processor which is used with PKI systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 262, 290

QUESTION 5

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

Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means. Furthermore best practices are applied to all aspects in the work environment.

Incorrect Answers:

A: Security control frameworks refer to the backbone of SAFE (architecture) and unification is the underlying key to security which incorporates all ptrs of the network, including the WAN, the extranet, the Internet, and the intranet.

C: Access control methodologies refer to Mandatory- Discretionary- and Rule-based access control types that can be implemented.

D: Compliance activity usually comes into focus when a third party involvement is being considered.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 29