JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

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

QUESTION 1

A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

A. Detect security incidents

B. Reduce attack surface of systems

C. Implement monitoring controls

D. Hardening network devices

E. Prevent unauthorized access

Correct Answer: AC

By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is implementing monitoring controls. With the monitoring controls in place, by monitoring the security logs, reviewing the footage from the security cameras and analyzing trend reports, the security analyst is able to detect security incidents.

Incorrect Answers:

B: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not reducing the attack surface of systems. The security analyst is not making any changes to the systems; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

D: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not hardening the network devices. The security analyst is not making any changes to the network devices; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

E: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not preventing unauthorized access. The security analyst is not making any changes to the systems and so cannot prevent unauthorized access; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

QUESTION 2

An organizations\\' security policy requires that users change passwords every 30 days. After a security audit, it was determined that users were recycling previously used passwords. Which of the following password enforcement policies would have mitigated this issue?

A. Password history

B. Password complexity

C. Password length

D. Password expiration

Correct Answer: A

QUESTION 3

The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

A. Disable the SSID broadcasting

B. Configure the access points so that MAC filtering is not used

C. Implement WEP encryption on the access points

D. Lower the power for office coverage only

Correct Answer: D

On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

Incorrect Answers:

A: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

B: Disabling MAC filtering would lower the network security. If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users\\' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

C: WEP encryption is weak and has many vulnerabilities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

QUESTION 4

Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity

B. Data confidentiality

C. Availability of servers

D. Integrity of data

Correct Answer: B

Data that is not kept separate or segregated will impact on that data\\'s confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root-level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database. Data segregation is crucial; keep your data on secure servers.

Incorrect Answers:

A: Hardware integrity is not an issue for the customer when making use of cloud computing.

C: Making use of cloud computing is in essence providing availability of servers for the customers.

D: Data integrity is not at risk in this scenario.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17-18

QUESTION 5

The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by:

A. Utilizing the already present TPM.

B. Configuring secure application sandboxes.

C. Enforcing whole disk encryption.

D. Moving data and applications into the cloud.

Correct Answer: A

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system\\'s motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential harm it may cause to production systems.

C:

Whole disk encryption can be implemented by either a software-based cryptography solutions or by a hardware based solution such as a Trusted Platform Module (TPM) or a Hardware Security Module (HSM).

D.

Moving data and applications to the cloud does not ensure that the data or applications are encrypted in its new location.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 237 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 250