JK0-022$^{\text{Q\&As}}$

CompTIA Security+ Certification

QUESTION 1

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

A. More experienced employees from less experienced employees

B. Changes to program code and the ability to deploy to production

C. Upper level management users from standard development employees

D. The network access layer from the application access layer

Correct Answer: B

Separation of duties means that there is differentiation between users, employees and duties per se which form part of best practices.

Incorrect Answers:

A: It is not an issue regarding experience of employees, but rather the difference in duties of employees.

C: Developers and administrators are not necessarily upper level management and standard development employees.

D: This is a network distinction and not a job description distinction.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 153

QUESTION 2

Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

A. Capture system image

B. Record time offset

C. Screenshots

D. Network sniffing

Correct Answer: D

Network sniffing is the process of capturing and analyzing the packets sent between systems on the network. A network sniffer is also known as a Protocol Analyzer. A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent to the web server will help determine the source IP address of the system sending the packets. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

Incorrect Answers:

A: Capturing an image of the system is the process of making an exact copy of the contents of the hard drive in the system. This would not help in determining the source of an attack on the system. Therefore, this answer is incorrect.

B: Recording the time offset of the system will determine the difference between the time on the system compared to the actual current time. This would not help in determining the source of an attack on the system. Therefore, this answer is incorrect.

C: Taking screenshots of the system will not help in determining the source of an attack on the system. A screenshot is a copy of what is displayed on the computer screen at the time of the screenshot. Therefore, this answer is incorrect.

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

QUESTION 3

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 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

Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

A. Bollards

B. Video surveillance

C. Proximity readers

D. Fencing

Correct Answer: B