JK0-022 Q&As

CompTIA Security+ Certification

QUESTION 1

Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

A. Authentication server

B. Server certificate

C. Key length

D. EAP method

Correct Answer: C

Key length is the main issue of concern since the wireless network uses a shared password. With risks of shared passwords makes the length of the password a crucial factor to risk mitigation.

Incorrect Answers:

A: An authentication server is used to authenticate access points and switches on 802.1X. This is the norm.

B: Server certificates are used when authentication and trust relationships are established. This is normal.

D: EAP (Extensible Authentication protocol) method being used is normal.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140, 158

QUESTION 2

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

A. Steganography images

B. Internal memory

C. Master boot records

D. Removable memory cards

E. Public keys

Correct Answer: BD

All useable data on the device should be encrypted. This data can be located on the hard drive, or removable drives, such as USB devices and memory cards, and on internal memory. Incorrect Answers:

A: Steganography is a process of hiding one communication inside another communication. It can use passwords to prevent unauthorized extraction of the hidden communication and can also use encryption to mitigate against brute-force attempts at extraction. Steganography can also be used to detect theft, fraud, or modification when the hidden communication is a watermark.

C: The master boot record (MBR) stores information on how the logical partitions on a hard drive are organized and contains loaders for the operating system. This is not data at risk and does not need to be encrypted.

E: Public keys are used in asymmetrical cryptography. It is publicly available and is derived from the user\\'s private key. It does not hold any useable data as the private key cannot be used to reverse engineer the user\\'s private key.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 323,

QUESTION 3

The system administrator has deployed updated security controls for the network to limit risk of attack. The security manager is concerned that controls continue to function as intended to maintain appropriate security posture.

Which of the following risk mitigation strategies is MOST important to the security manager?

A. User permissions

B. Policy enforcement

C. Routine audits

D. Change management

Correct Answer: C

After you have implemented security controls based on risk, you must perform routine audits. These audits should include reviews of user rights and permissions as well as specific events. You should pay particular attention to false positives and negatives.

Incorrect Answers:

A: User permissions are part of the routine checks that should be followed.

B: Policy enforcement usually refers to account policies and these determine the security parameters regarding who may and may not access the system. These are already in place and should be routine checked in this scenario.

D: Change management is the structured approach that is followed to secure a company\\'s assets.

References:

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

QUESTION 4

Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

A. Unexpected input

B. Invalid output

C. Parameterized input

D. Valid output

Correct Answer: A

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.

Incorrect Answers:

B, D: Fuzzing uses invalid input and not output to test the application\\'s response, such as crashes, or failed validation, or memory leaks, to such input.

C: Parameterized input may be one of the invalid, unexpected, or random data that would be used in fuzz testing. Other forms of invalid data should also be tested.

References: http://en.wikipedia.org/wiki/Fuzz_testing Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 218 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 229

QUESTION 5

A company hosts its public websites internally. The administrator would like to make some changes to the architecture.

The three goals are:

(1)

reduce the number of public IP addresses in use by the web servers (2) drive all the web traffic through a central point of control

(3)

mitigate automated attacks that are based on IP address scanning

Which of the following would meet all three goals?

A. Firewall

B. Load balancer

C. URL filter

D. Reverse proxy

Correct Answer: D