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

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

QUESTION 1

A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement

B. Interference

C. Use WEP

D. Single Sign on

E. Disable the SSID

F. Power levels

Correct Answer: AF

Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot. Incorrect Answers:

B: Interference could disrupt the signal in the building as well.

C: WEP is not a secure encryption protocol.

D: This allows users access to all the applications and systems they need when they log on.

E: This option would "cloak" the network, not limit its signal strength.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 149, 171, 177, 183.

QUESTION 2

A company\\'s security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

A. Install a registration server.

B. Generate shared public and private keys.

C. Install a CA

D. Establish a key escrow policy.

Correct Answer: C

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA.

Incorrect Answers:

A: When you implement a PKI you are not required to install a registration server. You can rely on a public registration authority server.

B: To generate shared public and private keys you would need a CA.

D: A key escrow policy is not required for a PKI.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages)

and made available if that third party requests them. The third party in question is generally the government, but it could also be an employee\\'s private messages have been called into question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

QUESTION 3

Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

A. Product baseline report

B. Input validation

C. Patch regression testing

D. Code review

Correct Answer: D

The problems listed in this question can be caused by problems with the application code.

Reviewing the code will help to prevent the problems.

The purpose of code review is to look at all custom written code for holes that may exist. The review needs also to examine changes that the code--most likely in the form of a finished application--may make: configuration files, libraries, and

the like. During this examination, look for threats such as opportunities for injection to occur (SQL, LDAP, code, and so on), cross-site request forgery, and authentication. Code review is often conducted as a part of gray box testing. Looking

at source code can often be one of the easiest ways to find weaknesses within the application. Simply reading the code is known as manual assessment, whereas using tools to scan the code is known as automated assessment.

Incorrect Answers:

A: A product baseline report is a report that compares the current state of the product to the original product specification. It is not used to prevent race conditions, buffer overflows, and other similar vulnerabilities in an application. Therefore, this answer is incorrect.

B: Input validation can improve application performance by catching malformed input in the application that could cause problems with the output. For example, if a user is expected to enter a number into a field in the application, input validation can be used to ensure that the input is numeric and not text. It can also be used to prevent attacks such as cross-site scripting and SQL injection. It is not used to prevent race conditions, buffer overflows, and other similar vulnerabilities in an application. Therefore, this answer is incorrect.

C: Regression testing is a type of software testing that seeks to uncover new software bugs, or regressions, in existing functional and non-functional areas of a system after changes such as enhancements, patches or configuration changes, have been made to them. The intent of regression testing is to ensure that changes such as those mentioned above have not introduced new faults. One of the main reasons for regression testing is to determine whether a change in one part of the software affects other parts of the software. Application patches may be released after the original application has been released. However, a code review should be performed before the application is released in the first place. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 345
http://en.wikipedia.org/wiki/Regression_testing

QUESTION 4

To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management

B. Administrative

C. Technical

D. Operational

Correct Answer: C

controls such as preventing unauthorized access to PC\\'s and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

Incorrect Answers:

A: Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment.

B: Administrative tools are used when applying technical control types.

D: Operational control types include Personnel Security, Physical and Environmental Protection, Contingency planning, Configuration Management, Maintenance, System and Information Integrity, Media Protection, Incident Response and

Awareness and Training.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 27

QUESTION 5

A security administrator at a company which implements key escrow and symmetric encryption only, needs to decrypt an employee\\'s file. The employee refuses to provide the decryption key to the file. Which of the following can the administrator do to decrypt the file?

A. Use the employee\\'s private key

B. Use the CA private key

C. Retrieve the encryption key

D. Use the recovery agent

Correct Answer: C