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.pass2lead.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

Which of the following types of security services are used to support authentication for remote users and devices?

A. Biometrics

B. HSM

C. RADIUS

D. TACACS

Correct Answer: C

RADIUS authentication phase takes place when a network client connects to a network access server (NAS) and provides authentication credentials. The NAS will then make use of the authentication credentials to issue a RADIUS authentication request to the RADIUS server, which will then exchange RADIUS authentication messages with the NAS.

Incorrect Answers:

A: Biometrics refers to a collection of physical attributes of the human body that can be used as identification or an authentication factor. Devices cannot use this.

B: HSM is a physical computing device that protects and oversees digital keys for strong authentication and provides cryptoprocessing. It is not used for the authentication of remote users and devices?

D: TACACS was used for communicating with an authentication server, not the actual authentication.

References:

http://cloudessa.com/products/cloudessa-radius-service/what-is-a-radius-server/ Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 285.

http://en.wikipedia.org/wiki/Hardware_security_module

http://en.wikipedia.org/wiki/TACACS

QUESTION 2

A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system\\'s services to the list of standard services on the company\\'s system image. This review process depends on:

A. MAC filtering.

B. System hardening.

C. Rogue machine detection.

D. Baselining.

Correct Answer: D

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

Incorrect Answers:

A: MAC Filtering is used to secure access to wireless network access points. It is used to explicitly allow MAC addresses on a whitelist, blocking all other MAC addresses.

B: 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.

C: Rogue machine detection attempt to identify the presence of unauthorized systems on a network.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 178, 215-217, 219 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 206, 207, 208

QUESTION 3

Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

A. ECC

B. RSA

C. SHA

D. 3DES

Correct Answer: D

3DES would be less secure compared to ECC, but 3DES would require less computational power. Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it\\'s more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

Incorrect Answers:

A: Elliptic Curve Cryptography (ECC) provides similar functionality to RSA but uses smaller key sizes to obtain the same level of security. ECC encryption systems are based on the idea of using points on a curve combined with a point at infinity and the difficulty of solving discrete logarithm problems.

B: The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process. RSA encryption and decryption would require more computation compared to 3DES.

C: SHA is not an encryption algorithm. The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 253, 255, 255-256

QUESTION 4

The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

A. WEP

B. WPA2 CCMP

C. Disable SSID broadcast and increase power levels

D. MAC filtering

Correct Answer: B

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:

A: WEP is not a secure encryption protocol.

C: This will only cloak the network, and increase the signal strength.

D: MAC filtering is vulnerable to spoof attacks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.

QUESTION 5

Which of the following is the MOST intrusive type of testing against a production system?

A. White box testing

B. War dialing

C. Vulnerability testing

D. Penetration testing

Correct Answer: D

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system\\'s security controls to gain access to the system. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization\\'s security policy compliance, its employees\\' security awareness and the organization\\'s ability to identify and respond to security incidents. Penetration tests are sometimes called white hat

attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization\\'s IT team and the penetration testing team working together. It\\'s sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company\\'s externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can

get in once they\\'ve gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that\\'s performing the test beforehand. Typically, they may only be given the name of the company.

Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double- blind tests can be useful for testing an

organization\\'s security monitoring and incident identification as well as its response procedures.

Incorrect Answers:

A: White box testing is a software testing technique whereby explicit knowledge of the internal workings of the item being tested are used to select the test data. Unlike black box testing, white box testing uses specific knowledge of

programming code to examine outputs. The test is accurate only if the tester knows what the program is supposed to do. He or she can then see if the program diverges from its intended goal. White box testing does not account for errors

caused by omission, and all visible code must also be readable. White box testing is used to test the code of an application. It is not used to test the security controls of a production system.

Therefore, this answer is incorrect.

B: War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. It is not used to test the

security controls of a production system. Therefore, this answer is incorrect.

C: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and

vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn\\'t actually attempt to circumvent the security controls of a system to gain

access (unlike a penetration test). Therefore, this answer is incorrect.

References:

http://searchsoftwarequality.techtarget.com/definition/penetration-testing
http://www.webopedia.com/TERM/W/White_Box_Testing.html http://en.wikipedia.org/wiki/War_dialing