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.pass4itsure.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA

B. Disable SSID

C. Adjust antenna placement

D. Implement WEP

Correct Answer: A

Of the options supplied, WiFi Protected Access (WPA) is the most secure and is the replacement for WEP.

Incorrect Answers:

B: Disabling the SSID will only hide the wireless network, and is not more secure than WPA.

C: This will increase or decrease signal strength and availability, but will not make the network secure.

D: WEP was replaced by WPA to offer a more secure solution.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 59- 62.

QUESTION 2

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

A. Design reviews

B. Baseline reporting

C. Vulnerability scan

D. Code review

Correct Answer: C

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network\\'s security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Incorrect Answers:

A: A design review is not performed primarily to detect security threats on a network. Reviewing the design of a system or network can be performed for many reasons including performance, availability etc. whereas a vulnerability scan is

performed specifically to discover security threats on a network. Therefore, this answer is incorrect.

B: As the name implies, baseline reporting checks to make sure that things are operating status quo, and change detection is used to alert administrators when modifications are made. A changes-from-baseline report can be run to pinpoint

security rule breaches quickly. This is often combined with gap analysis to measure the controls at a particular company against industry standards.

Baseline reporting may alert the security administrator to any changes in the security posture compared to the original baseline configuration. However, a vulnerability scan is performed specifically to discover security threats on a network and

is therefore a better answer. Therefore, this answer is incorrect.

D: A code review is the process of reviewing the programming code in an application. It is not used to discover security threats on a network. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 345

QUESTION 3

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 4

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

A. SSL 1.0

B. RC4

C. SSL 3.0

D. AES

E. DES

F. TLS 1.0

Correct Answer: AE

TLS 1.0 and SSL 1.0 both have known vulnerabilities and have been replaced by later versions. Any systems running these ciphers should have them disabled. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer

(SSL), are cryptographic protocols designed to provide communications security over a computer network. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating,

and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product,

message authentication Netscape developed the original SSL protocol. Version 1.0 was never publicly released because of serious security flaws in the protocol; version 2.0, released in February 1995, "contained a number of security flaws

which ultimately led to the design of SSL version 3.0". TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but

they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security.

TLS 1.1 and then TLS 1.2 were created to replace TLS 1.0.

Incorrect Answers:

B: In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). Whilst some argue that RC4 does have a weakness, it is still commonly used today.

SSL 1.0 and TLS 1.0 are considered to be weaker ciphers. Therefore, this answer is incorrect.

C: Although TLS 1.2 has been created to replace SSL 3.0, SSL 3.0 is still commonly used today. SSL 1.0 and TLS 1.0 are considered to be weaker ciphers.

Therefore, this answer is incorrect.

D: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a

symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is not considered to be a weak cipher.

Therefore, this answer is incorrect.

F: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Although

DES has been superseded by 3DES and AES, DES is still used today. SSL 1.0 and TLS 1.0 are considered to be weaker ciphers.

Therefore, this answer is incorrect.

References: http://en.wikipedia.org/wiki/Transport_Layer_Security http://en.wikipedia.org/wiki/Triple_DES

QUESTION 5

Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor\\'s number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.

Which of the following attack types is this?

A. Hoax

B. Impersonation

C. Spear phishing

D. Whaling

Correct Answer: B

In this question, the impersonator is impersonating a vendor and asking for payment. They have managed to `spoof\\' their calling number so that their caller ID matches the vendor\\'s number. Impersonation is where a person, computer,

software application or service pretends to be someone or something it\\'s not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

Incorrect Answers:

A: A hoax is something that makes a person believe that something is real when it is not. A hoax is usually not malicious or theft. Therefore, this answer is incorrect.

C: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient\\'s own company and generally someone in a position of authority. Spear phishing involves email spoofing rather than telephone spoofing. Therefore this answer is incorrect.

D: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. This is not what is described in this question. Therefore, this answer is incorrect.

References:

http://searchsecurity.techtarget.com/definition/spear-phishing http://www.techopedia.com/definition/28643/whaling