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.passapply.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

A security administrator is reviewing the below output from a password auditing tool:

P@ss. @pW1. S3cU4

Which of the following additional policies should be implemented based on the tool\\'s output?

A. Password age

B. Password history

C. Password length

D. Password complexity

Correct Answer: C

The output shows that all the passwords are either 4 or 5 characters long. This is way too short, 8 characters are shown to be the minimum for password length.

Incorrect Answers:

A: The output does not show how long the passwords have been in use.

B: The output does not show the password history.

D: The output shows that the password is indeed making use of complexity when it comes to the types of characters used.

References:

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

QUESTION 2

Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

A. IV attack

B. Interference

C. Blue jacking

D. Packet sniffing

Correct Answer: A

In this question, it\\'s likely that someone it trying to crack the wireless network security. An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred

to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can\\'t be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter. Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

Incorrect Answers:

B: There can be many sources of interference to network communications especially in wireless networks. However, interference would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

C: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol. Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters. Bluejacking is usually harmless, but because bluejacked people generally don\\'t know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it\\'s possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. Bluejacking would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

D: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn\\'t generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. Packet sniffing would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/26858/initialization-vector http://en.wikipedia.org/wiki/Bluejacking http://www.techopedia.com/definition/4113/sniffer

QUESTION 3

Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

A. Employ encryption on all outbound emails containing confidential information.

B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.

C. Employ hashing on all outbound emails containing confidential information.

D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

Correct Answer: A

Encryption is used to ensure the confidentiality of information and in this case the outbound email that contains the confidential information should be encrypted.

Incorrect Answers:

B: DLP system should be set to monitor the outbound emails not the inbound email since the company will be sending out confidential email.

C: Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables.

D: Encrypting inbound email would be futile if the data protection should be carried out on outbound email.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236, 255, 291

QUESTION 4

The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

A. Remove the staff group from the payroll folder

B. Implicit deny on the payroll folder for the staff group

C. Implicit deny on the payroll folder for the managers group

D. Remove inheritance from the payroll folder

Correct Answer: B

Implicit deny is the default security stance that says if you aren\\'t specifically granted access or privileges for a resource, you\\'re denied access by default.

Incorrect Answers:

A: This will not work because the question states: "The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission."

C: This will deny access for the managers group.

D: Removing inheritance from the payroll folder will also affect the manages group.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 44.

QUESTION 5

A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20

B. 21

C. 22

D. 23

Correct Answer: B

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

Incorrect Answers:

A: FTP uses port 20, but it is not the default port.

C: SSH uses TCP port 22.

D: Telnet uses port 23.

References:

http://compnetworking.about.com/od/tcpip/p/port-numbers-21-ftp.htm
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers