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.geekcert.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 network architecture concepts is used to securely isolate at the boundary between networks?

A. VLAN

B. Subnetting

C. DMZ

D. NAT

Correct Answer: C

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

A: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

B: Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

D: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 39.

QUESTION 2

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

A. Create a user account and assign the user account to the accounting group.

B. Create an account with role-based access control for accounting.

C. Create a user account with password reset and notify Joe of the account creation.

D. Create two accounts: a user account and an account with full network administration rights.

Correct Answer: B

Role-based Access Control is basically based on a user\\'s job description. When a user is assigned a specific role in an environment, that user\\'s access to objects is granted based on the required tasks of that role. The IT administrator should,

therefore, create an account with role- based access control for accounting for Joe.

Incorrect Answers:

A: Assigning Joe\\'s user account to the accounting group will not necessarily allow Joe the required access, as different users require different access.

C: Creating a user account with password reset will not allow Joe the required access, as permissions still have to be granted.

D: Doing this will give Joe more rights than is required.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 280.

QUESTION 3

Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

A. Shoulder Surfing

B. Dumpster Diving

C. Phishing

D. Impersonation

Correct Answer: B

Incinerating documents (or shredding documents) instead of throwing them into a bin will prevent people being able to read the documents to view sensitive information. Dumpster diving is looking for treasure in someone else\\'s trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn\\'t limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

Incorrect Answers:

A: Shoulder surfing is using direct observation techniques, such as looking over someone\\'s shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it\\'s relatively easy to stand next to

someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To

prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Incinerating documents will not prevent shoulder surfing. Therefore, this answer is incorrect.

C: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an

attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website,

however, is bogus and set up only to steal the information the user enters on the page.

Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate

company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some

will be tempted into biting. Incinerating documents will not prevent phishing. Therefore, this answer is incorrect.

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

While the information gained by viewing documents could be used by an impersonator, incinerating documents alone will not prevent impersonation. Therefore, this answer is incorrect.

References:

http://searchsecurity.techtarget.com/definition/dumpster-diving http://searchsecurity.techtarget.com/definition/shoulder-surfing http://www.webopedia.com/TERM/P/ phishing.html

QUESTION 4

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots

B. Sandboxing

C. Patch management

D. Intrusion detection system

Correct Answer: C

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Incorrect Answers:

A: Snapshots are backups of virtual machines that can be used to quickly recover from errors or poor updates. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential

malware that may be embedded in the new application from being able to cause harm to production systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

D: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 231-232, 249,

QUESTION 5

When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann\\'s workstation. Which of the following could have prevented this from happening?

A. Password complexity policy

B. User access reviews

C. Shared account prohibition policy

D. User assigned permissions policy

Correct Answer: A

The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Since changes were made to Ann\\'s desktop configuration settings while she was not at work, means that her password was compromised.

Incorrect Answers:

B: User access reviews are performed to conclude whether users have been performing their work tasks correctly or if there have been failed and/or successful attempts at violating company policies or the law. It would not have prevented Ann\\'s password being compromised.

C: Shared account prohibition aids in providing user accountability. It would not have prevented Ann\\'s password being compromised.

D: User assigned permissions can be assigned by the user. Since Ann\\'s workstation was accessed using her password, the intruder would also have her permissions.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 294.