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 is the MOST specific plan for various problems that can arise within a system?

A. Business Continuity Plan

B. Continuity of Operation Plan

C. Disaster Recovery Plan

D. IT Contingency Plan

Correct Answer: D

An IT contingency plan would focus on the IT aspect in particular to ensure business continuity.

Incorrect Answers:

A: Business continuity planning (BCP) is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes. BCP is primarily a management tool that ensures that critical business functions can be performed when normal business operations are disrupted.

B: Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies

C: A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 433-434

QUESTION 2

Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.

B. TFTP is more secure than FTP.

C. TFTP utilizes TCP and FTP uses UDP.

D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D

FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69.

Incorrect Answers:

A: UDP is faster than TCP is because there is no form of flow control or error correction.

B: TFTP requires no authentication, whereas FTP allows authenticated connections.

C: As stated above, FTP employs TCP ports 20 and 21 and TFTP makes use of UDP port 69.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 49, 50.

http://www.skullbox.net/tcpudp.php

QUESTION 3

Which of the following is the term for a fix for a known software problem?

A. Skiff

B. Patch

C. Slipstream

D. Upgrade

Correct Answer: B

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: A skiff is a small boat.

C: Slipstreaming is the process of making an installation image of an operating system that includes the latest service packs and required applications. This is used to install new systems rather than fix software problems.

D: Upgrades are replacement of the existing software with newer and better versions of the oftware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 231

QUESTION 4

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation

B. Network intrusion detection system

C. Anomaly-based HIDS

D. Peer review

Correct Answer: A

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

B: A network-based IDS (NIDS) is an intrusion detection system that scans network traffic in real time and is useful for detecting network-based attacks.

C: A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It does not prevent attacks, such as cross-site scripting attacks and buffer overflows, but detects it.

D: Peer review is the process of reviewing source code before the software is released. This is performed by a peer rather than by the programmer.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117, 257, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21,

197, 216, 319

QUESTION 5

An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning

B. Quantitative assessment

C. Data classification

D. Qualitative assessment

Correct Answer: C

Information classification is done by confidentiality and comprises of three categories, namely:

public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data `unknown sensitivity\\'

Incorrect Answers:

A: Business continuity planning (BCP) is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes. BCP is primarily a management tool that ensures

that critical business functions can be performed when normal business operations are disrupted.

B: Quantitative assessment is cost-based and objective risk assessment.

D: Qualitative assessment is opinion-based and subjective risk assessment.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 7, 404, 431

QUESTION 6

Which of the following is a concern when encrypting wireless data with WEP?

A. WEP displays the plain text entire key when wireless packet captures are reassembled

B. WEP implements weak initialization vectors for key transmission

C. WEP uses a very weak encryption algorithm

D. WEP allows for only four pre-shared keys to be configured

Correct Answer: B

The initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

Incorrect Answers:

A: WEP does not display the entire key as plain text.

B: The WEP encryption algorithm is not the main WEP weakness.

D: WEP has no restrictions on the number of pre-shared keys.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 258

QUESTION 7

Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.

B. Scanning of outbound IM (Instance Messaging).

C. Scanning copying of documents to USB.

D. Scanning of SharePoint document library.

E. Scanning of shared drives.

F. Scanning of HTTP user traffic.

Correct Answer: BF

DLP systems monitor the contents of systems (workstations, servers, networks) to make sure key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Outbound IM and HTTP user traffic refers to data over a network which falls within the DLP strategy.

Incorrect Answers:

A: Printing of documents will not necessarily result in data loss since it is a hard copy of the soft copy that is already there.

C: Copying documents to USB amounts to duplicating data.

D: A SharePoint document Library is a list of the documents and not the data itself. This is not a data in transit issue

E: Shared drive scanning is not data in transit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236-237, 364

QUESTION 8

Which of the following are examples of network segmentation? (Select TWO).

A. IDS

B. IaaS

C. DMZ

D. Subnet

E. IPS

Correct Answer: CD

C:

A demilitarized zone (DMZ) is a part of the network that is separated of segmented from the rest of the network by means of firewalls and acts as a buffer between the untrusted public Internet and the trusted local area network (LAN).

D.

IP subnets can be used to separate or segment networks while allowing communication between the network segments via routers.

Incorrect Answers:

A: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not feature or offer network segmentation.

B: The Infrastructure as a Service (IaaS) model is a cloud computing business model uses virtualization, with the clients paying for resources used.

E: An intrusion prevention system (IPS) is an automated system that attempts to prevent intrusions or security policy violations on networks or host systems. It does not feature or offer network segmentation.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 26, 27-28 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 65, 110-111

QUESTION 9

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.

B. The switch has several VLANs configured on it.

C. The sub-interfaces are configured for VoIP traffic.

D. The sub-interfaces each implement quality of service.

Correct Answer: B

A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the

networking standard that supports virtual LANs (VLANs) on an Ethernet network.

Incorrect Answers:

A, C, D: Subnets, VoIP, and QoS do not make use of this standard.

References:

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

http://en.wikipedia.org/wiki/IEEE_802.1Q

QUESTION 10

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

A. 1

B. 2

C. 3

D. 4

Correct Answer: C

Three different types of authentication factors have been used in this question:

Something you know username and password.

Something you have - client side certificate.

Somewhere you are - authentication to the VPN is only allowed from the U.S. territory.

Incorrect Answers:

A: This option refers to single factor authentication, which only makes use of one authentication factor.

B: This option refers to two-factor authentication, which makes use of two different authentication factors.

D: This option refers to four-factor authentication, which makes use of four different authentication factors.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 282.

QUESTION 11

Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

A. Set up a honeypot and place false project documentation on an unsecure share.

B. Block access to the project documentation using a firewall.

C. Increase antivirus coverage of the project servers.

D. Apply security updates and harden the OS on all project servers.

Correct Answer: A

In this scenario, we would use a honeypot as a `trap\\' to catch unauthorized employees who are accessing critical project information. A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack

to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the

system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization\\'s environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

Incorrect Answers:

B: Blocking access to the project documentation by using a firewall would block all access to the documentation including access to authorized employees. It would not help to determine which unauthorized employees are attempting to access the documentation. Therefore, this answer is incorrect.

C: Antivirus software is used to scan a system for known virus threats. It would not detect unauthorized users attempting to access the project documentation. Therefore, this answer is incorrect.

D: Applying security updates to harden a server is always a good idea. However, security updates would not detect unauthorized users attempting to access the project documentation. Therefore, this answer is incorrect.

References: https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

QUESTION 12

A security administrator is notified that users attached to a particular switch are having intermittent connectivity issues. Upon further research, the administrator finds evidence of an ARP spoofing attack. Which of the following could be utilized to provide protection from this type of attack?

A. Configure MAC filtering on the switch.

B. Configure loop protection on the switch.

C. Configure flood guards on the switch.

D. Configure 802.1x authentication on the switch.

Correct Answer: C

QUESTION 13

Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80 PERMIT TCP ANY HOST 192.168.0.10 EQ 443

A. It implements stateful packet filtering.

B. It implements bottom-up processing.

C. It failed closed.

D. It implements an implicit deny.

Correct Answer: D

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. Implicit deny is the default response when an explicit allow or deny isn\\'t present.

Incorrect Answers:

A: Stateful packet filtering automatically creates a response rule for the replay on the fly. But that rule exists only as long as the conversation is taking place.

B: Bottom-up processing is a type of information processing based on incoming data from the environment to form a perception.

C: This option is a reaction to a failure, which has nothing to do with ACL\\'s

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 26.
http://en.wikipedia.org/wiki/Top-down_and_bottom-up_design

QUESTION 14

Which of the following would MOST likely involve GPS?

A. Wardriving

B. Protocol analyzer

C. Replay attack

D. WPS attack

Correct Answer: A

QUESTION 15

Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

A. WPA2-Enterprise wireless network

B. DNS secondary zones

C. Digital certificates

D. Intrusion detection system

Correct Answer: A

WPA2-Enterprise is designed for enterprise networks and requires a RADIUS authentication server.

Incorrect Answers:

B: A secondary zone is merely a copy of a primary zone that is hosted on another server.

C: Digital certificates are used for proving the identity of a user or the source of an object.

D: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

References:

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

https://technet.microsoft.com/en-us/library/cc771898.aspx Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.