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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An administrator is concerned that a company\\'s web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

A. Vulnerability scan

B. Risk assessment

C. Virus scan

D. Network sniffer

Correct Answer: A

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:

B: A risk assessment is the process of determining risk. A risk assessment alone would not determine if a web server has been patched. A vulnerability scan should be performed first. The results of the vulnerability scan can then be used in a risk assessment. Therefore, this answer is incorrect.

C: A virus scan will scan a computer for known viruses. It is not used to determine if a system has been patched. Therefore, this answer is incorrect.

D: A network sniffer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It is not used to determine if a system has been patched. Therefore, this answer is incorrect.

References: http://www.webopedia.com/TERM/V/vulnerability_scanning.html

QUESTION 2

Which of the following describes the purpose of an MOU?

A. Define interoperability requirements

B. Define data backup process

C. Define onboard/offboard procedure

D. Define responsibilities of each party

Correct Answer: D

MOU or Memorandum of Understanding is a document outlining which party is responsible for what portion of the work.

Incorrect Answers:

A: The memorandum of understanding is a part of the interoperability agreement between the parties involved.

B: Data backup processes are part of data recovery and incidence response and are not the purpose of a memorandum of understanding.

C: Onboard and offboard procedures are not part of the MOU, it just refers to the transitioning phase that both parties have to engage in.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 398

QUESTION 3

A security technician wishes to gather and analyze all Web traffic during a particular time period. Which of the following represents the BEST approach to gathering the required data?

A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.

B. Configure a proxy server to log all traffic destined for ports 80 and 443.

C. Configure a switch to log all traffic destined for ports 80 and 443.

D. Configure a NIDS to log all traffic destined for ports 80 and 443.

Correct Answer: B

A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data.

Incorrect Answers:

A: The VPN concentrator creates an encrypted tunnel session between hosts, and many use two- factor authentication for additional security. A proxy server would still be the best tool to gather the required information.

C: A switch can provide a monitoring port for troubleshooting and diagnostic purposes in addition to the virtual circuit that they can create between systems in a network. This helps to reduce network trafffic, but a proxy server would be a

better tool to gather the required data.

D: A network-based IDS (NIDS) approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic. However a proxy server would be the best tool to gather the required data.

References:

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

105, 111

QUESTION 4

Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training

B. Personally owned device policy training

C. Tailgating awareness policy training

D. Information classification training

Correct Answer: D

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

public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data.

Incorrect Answers:

A: Social networking can sometimes be a useful marketing tool, however most companies would rather choose to avoid social networking since the exposure of your data would be too great. Risk avoidance would be better.

B: It is best policy for companies not to allow users to bring their own devises why would they provide training for own devices other than informing users that they are not allowed to bring their own devices.

C: Tailgating refers to the act of following someone through a door they just unlocked. This is a physical security issue.

References:

Dul Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

QUESTION 5

Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.

B. Install anti-virus software on the USB drives.

C. Disable USB within the workstations BIOS.

D. Apply the concept of least privilege to USB devices.

E. Run spyware detection against all workstations.

Correct Answer: AC

A: The USB root hub can be disabled from within the operating system.

C: USB can also be configured and disabled in the system BIOS.

Incorrect Answers:

B: Anti-virus is installed on a device, not on removable storage. Anti-virus also does not prevent the unauthorized copying of data.

D: The principle of least privilege is used to ensure that users are only provided with the minimum privileges and permissions to resources that allow them to perform their duties.

E: Spyware monitors a user\\'s activity and uses network protocols to reports it to a third party without the user\\'s knowledge. Detecting spyware does not prevent the unauthorized copying of data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 153, 247-248, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82,