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 MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

A. Risk transference

B. Change management

C. Configuration management

D. Access control revalidation

Correct Answer: B

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company\\'s assets. In this case `scheduled system patching\\'.

Incorrect Answers:

A: Risk transference is when you offload risk to another party akin to risk sharing.

C: Configuration management is an operational control type that is put into action after a risk assessment has been done.

D: Access control revalidation referrers to server-side and client-side validation that has to be repeated.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 14-17

QUESTION 2

The security administrator installed a newly generated SSL certificate onto the company web server. Due to a misconfiguration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

A. The file containing the recovery agent\\'s keys.

B. The file containing the public key.

C. The file containing the private key.

D. The file containing the server\\'s encrypted passwords.

Correct Answer: B

The public key can be made available to everyone. There is no need to reissue the certificate.

Incorrect Answers:

A: The recovery agent has no key.

C: The private key must be secret. If the private key is made available to a third party, then the key must be revoked.

D: Encrypted passwords would not be a security risk. It would be hard to decrypt them.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

QUESTION 3

A network administrator, Joe, arrives at his new job to find that none of the users have changed their network passwords since they were initially hired. Joe wants to have everyone change their passwords immediately. Which of the following policies should be enforced to initiate a password change?

A. Password expiration

B. Password reuse

C. Password recovery

D. Password disablement

Correct Answer: A

QUESTION 4

During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

A. Lessons Learned

B. Preparation

C. Eradication

D. Identification

Correct Answer: B

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/ reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. It is important to stop malware before it ever gets hold of a system thus you should know which malware is out there and take defensive measures - this means preparation to guard against malware infection should be done.

Incorrect Answers:

A: Lessons learned is one of the latter phases in incident response after the event occurred this means that general defense has not been observed.

C: Eradication is done after the infection already occurred and can thus not be considered general defense.

D: Incident Identification presumes that the incident already occurred thus it cannot be considered general defense against malware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 121-122, 429

QUESTION 5

An administrator has a network subnet dedicated to a group of users. Due to concerns regarding data and network security, the administrator desires to provide network access for this group only. Which of the following would BEST address this desire?

A. Install a proxy server between the users\\' computers and the switch to filter inbound network traffic.

B. Block commonly used ports and forward them to higher and unused port numbers.

C. Configure the switch to allow only traffic from computers based upon their physical address.

D. Install host-based intrusion detection software to monitor incoming DHCP Discover requests.

Correct Answer: C

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into

the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.

MAC filtering is commonly used in wireless networks but is considered insecure because a MAC address can be spoofed. However, in a wired network, it is more secure because it would be more difficult for a rogue computer to sniff a MAC

address.

Incorrect Answers:

A: A proxy server is often used to filter web traffic. It is not used in port security or to restrict which computers can connect to a network.

B: You should not block commonly used ports. This would just stop common applications and protocols working. It would not restrict which computers can connect to a network.

D: DHCP Discover requests are part of the DHCP process. A DHCP client will send out a DHCP Discover request to locate a DHCP server. All computers on the network receive the DHCP Discover request because it is a broadcast packet but all computers (except the DHCP server) will just drop the packet. Blocking DHCP Discover requests will not restrict which computers can connect to a network.

References: http://alliedtelesis.com/manuals/awplusv212weba/mac_address_Port_security.html

Latest JK0-022 Dumps JK0-022 PDF Dumps JK0-022 Study Guide