JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

QUESTION 1

When considering a vendor-specific vulnerability in critical industrial control systems which of the following techniques supports availability?

A. Deploying identical application firewalls at the border

B. Incorporating diversity into redundant design

C. Enforcing application white lists on the support workstations

D. Ensuring the systems\\' anti-virus definitions are up-to-date

Correct Answer: B

If you know there is a vulnerability that is specific to one vendor, you can improve availability by implementing multiple systems that include at least one system from a different vendor and so is not affected by the vulnerability.

Incorrect Answers:

A: An application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. We don\\'t know what the vulnerability is but it\\'s unlikely that a firewall will prevent the vulnerability or ensure availability.

C: Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list. It does not prevent vendor-specific vulnerability already inherent in the application, nor does it ensure availability. D. Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Ensuring the systems\\' anti-virus definitions are up-to-date is always a good idea. However, a vendor specific vulnerability is usually not caused by a virus.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 340

QUESTION 2

A company executive\\'s laptop was compromised, leading to a security breach. The laptop was placed into storage by a junior system administrator and was subsequently wiped and re-imaged. When it was determined that the authorities would need to be involved, there was little evidence to present to the investigators. Which of the following procedures could have been implemented to aid the authorities in their investigation?

A. A comparison should have been created from the original system\\'s file hashes

B. Witness testimony should have been taken by the administrator

C. The company should have established a chain of custody tracking the laptop

D. A system image should have been created and stored

Correct Answer: D

QUESTION 3

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

A. Design reviews

B. Baseline reporting

C. Vulnerability scan

D. Code review

Correct Answer: C

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:

A: A design review is not performed primarily to detect security threats on a network. Reviewing the design of a system or network can be performed for many reasons including performance, availability etc. whereas a vulnerability scan is

performed specifically to discover security threats on a network. Therefore, this answer is incorrect.

B: As the name implies, baseline reporting checks to make sure that things are operating status quo, and change detection is used to alert administrators when modifications are made. A changes-from-baseline report can be run to pinpoint

security rule breaches quickly. This is often combined with gap analysis to measure the controls at a particular company against industry standards.

Baseline reporting may alert the security administrator to any changes in the security posture compared to the original baseline configuration. However, a vulnerability scan is performed specifically to discover security threats on a network and

is therefore a better answer. Therefore, this answer is incorrect.

D: A code review is the process of reviewing the programming code in an application. It is not used to discover security threats on a network. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 345

QUESTION 4

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

QUESTION 5

A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement

B. Interference

C. Use WEP

D. Single Sign on

E. Disable the SSID

F. Power levels

Correct Answer: AF

Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot.
Incorrect Answers:

B: Interference could disrupt the signal in the building as well.

C: WEP is not a secure encryption protocol.

D: This allows users access to all the applications and systems they need when they log on.

E: This option would "cloak" the network, not limit its signal strength.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 149, 171, 177, 183.

Latest JK0-022 Dumps JK0-022 Exam Questions JK0-022 Braindumps