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

The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank\\'s certificates are still valid?

A. Bank\\'s CRL

B. Bank\\'s private key

C. Bank\\'s key escrow

D. Bank\\'s recovery agent

Correct Answer: A

The finance department can check if any of the bank\\'s certificates are in the CRL or not. If a certificate is not in the CRL then it is still valid. The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

Incorrect Answers:

B: Within PKI there are only two methods to verify certificates or keys still are valid. One is using a CRL and the other is using the OCSP protocol. Private key verification cannot be used to a comprised CA.

C: Key escrow cannot be used to check if a certification is revoked or not. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee\\'s private messages have been called into question.

D: A recovery agent cannot be used to check if certificates are still valid. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

QUESTION 2

Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.

B. Remove the network from the routing table.

C. Create a virtual switch.

D. Commission a stand-alone switch.

Correct Answer: C

A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels.

Incorrect Answers:

A: The default gateway usually connects the internal networks and the Internet. This could result in the gateway node acting as a proxy server and a firewall. The gateway is also associated with both a router, and a switch. A router makes use of headers and forwarding tables to determine where packets are sent, and a switch supplies the actual path for the packet in and out of the gateway. Therefore, a gateway is necessary.

B: A routing table contains information about the topology of the network immediately around it. Removing the network from it would prevent the virtual servers from connecting to the network.

D: A standalone switch is able to function independently of other hardware. This would involve cost and effort. Using a virtual switch is the best option.

References: https://technet.microsoft.com/en-us/library/hh831823.aspx

QUESTION 3

A security administrator must implement a network that is immune to ARP spoofing attacks. Which of the following should be implemented to ensure that a malicious insider will not be able to successfully use ARP spoofing techniques?

A. UDP

B. IPv6

C. IPSec

D. VPN

Correct Answer: B

QUESTION 4

Which of the following is the MOST intrusive type of testing against a production system?

A. White box testing

B. War dialing

C. Vulnerability testing

D. Penetration testing

Correct Answer: D

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system\\'s security controls to gain access to the system. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in

(either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization\\'s security policy compliance, its employees\\' security awareness and the organization\\'s ability to identify and respond to security incidents. Penetration tests are sometimes called white hat

attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization\\'s IT team and the penetration testing team working together. It\\'s sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company\\'s externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can

get in once they\\'ve gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that\\'s performing the test beforehand. Typically, they may only be given the name of the company.

Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double- blind tests can be useful for testing an

organization\\'s security monitoring and incident identification as well as its response procedures.

Incorrect Answers:

A: White box testing is a software testing technique whereby explicit knowledge of the internal workings of the item being tested are used to select the test data. Unlike black box testing, white box testing uses specific knowledge of

programming code to examine outputs. The test is accurate only if the tester knows what the program is supposed to do. He or she can then see if the program diverges from its intended goal. White box testing does not account for errors

caused by omission, and all visible code must also be readable. White box testing is used to test the code of an application. It is not used to test the security controls of a production system.

Therefore, this answer is incorrect.

B: War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. It is not used to test the

security controls of a production system. Therefore, this answer is incorrect.

C: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and

vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn\\'t actually attempt to circumvent the security controls of a system to gain

access (unlike a penetration test). Therefore, this answer is incorrect.

References:

http://searchsoftwarequality.techtarget.com/definition/penetration-testing
http://www.webopedia.com/TERM/W/White_Box_Testing.html http://en.wikipedia.org/wiki/War_dialing

QUESTION 5

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5

B. WEP

C. PEAP-MSCHAPv2

D. EAP-TLS

Correct Answer: C

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Incorrect Answers:

A: MD5 has been employed in a wide selection of cryptographic applications, and is also commonly used to verify data integrity.

B: Usernames and passwords are not required for WEP authentication.

D: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

References:

https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx http://en.wikipedia.org/ wiki/MD5