# JK0-022<sup>Q&As</sup>

## CompTIA Security+ Certification

# Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.leads4pass.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**

A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

A. A CRL

B. Make the RA available

C. A verification authority

D. A redundant CA

Correct Answer: A

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. By checking the CRL you can check if a particular certificate has been revoked.

Incorrect Answers:

B: Access to a registration authority (RA) is not required to check for bad certificates. A CRL will do fine. A registration authority (RA) offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities.

C: A verification authority is used to check the uniqueness of a certificate, not primarily to check for bad certificates. The user identity must be unique within each CA domain. The third-party validation authority (VA)/verification authority can provide this information on behalf of the CA. The binding is established through the registration and issuance process.

D: A redundant CA is not required to check for bad certificates. A CRL will do fine.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285

**QUESTION 2**

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system

B. Electrical

C. HVAC

D. Video surveillance

Correct Answer: C

HVAC refers to heating, ventilation and air-conditioning to allow for a zone-based environmental control measure. The fire-alarm system should ideally also be hooked up to the HVAC so that the HVAC can monitor the changes in heating

and ventilation.

Incorrect Answers:

A: A water based sprinkler system is designed to extinguish a fire and not to prevent data loss. It can also cause extreme damage to computers and electrical equipment.

B: Electrical systems are not designed to prevent the spread of fire.

D: Video surveillance is used mainly as a deterrent and will not help to prevent the spread of fire.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 378-380

**QUESTION 3**

A security administrator must implement a system that will support and enforce the following file system access control model:

FILE NAME SECURITY LABEL Employees.doc Confidential Salary.xls Confidential OfficePhones.xls Unclassified PersonalPhones.xls Restricted

Which of the following should the security administrator implement?

A. White and black listing

B. SCADA system

C. Trusted OS

D. Version control

Correct Answer: C

**QUESTION 4**

A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20

B. 21

C. 22

D. 23

Correct Answer: B

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

Incorrect Answers:

A: FTP uses port 20, but it is not the default port.

C: SSH uses TCP port 22.

D: Telnet uses port 23.

References:

http://compnetworking.about.com/od/tcpip/p/port-numbers-21-ftp.htm
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

**QUESTION 5**

Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

A. Architectural review

B. Penetration test

C. Port scanner

D. Design review

Correct Answer: C

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server. A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Incorrect Answers:

A: An architectural review is a review of the network structure (servers, switches, routers, network topology etc.). It does not list running services on computers.

Therefore, this answer is incorrect.

B: Penetration testing evaluates an organization\\'s ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. It is not used to

list services running on computers.

Therefore, this answer is incorrect.

D: A design review is the process of reviewing the design of something; examples include reviewing the design of the network or the design of a software application. It is not used to list services running on computers. Therefore, this

answer

is incorrect.

References: http://en.wikipedia.org/wiki/Port_scanner