RC0-C02^Q&As

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

https://www.pass2lead.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation

B. Establish a list of devices that must meet each regulation

C. Centralize management of all devices on the network

D. Compartmentalize the network

E. Establish a company framework

F. Apply technical controls to meet compliance with the regulation

Correct Answer: BDF

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must:

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

To achieve PCI and SOX compliance you should:

Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.

Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.

Apply technical controls to meet compliance with the regulation. Secure the data as required.

QUESTION 2

An IT manager is working with a project manager to implement a new ERP system capable of transacting data between the new ERP system and the legacy system. As part of this process, both parties must agree to the controls utilized to secure data connections between the two enterprise systems. This is commonly documented in which of the following formal documents?

A. Memorandum of Understanding

B. Information System Security Agreement

C. Interconnection Security Agreement

D. Interoperability Agreement

E. Operating Level Agreement

Correct Answer: C

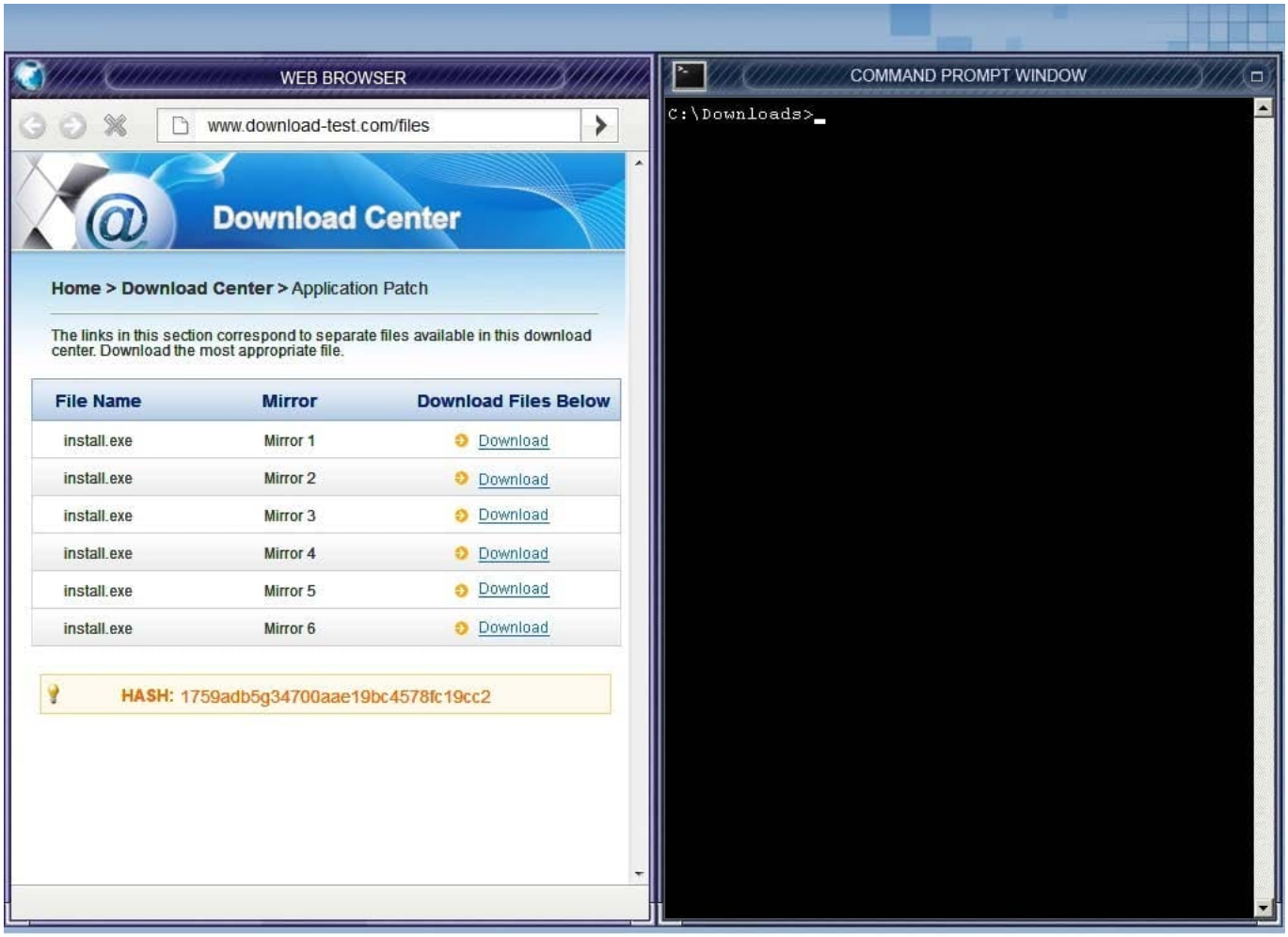
An interconnection security agreement (ISA) is a security document that derails the requirements for establishing, maintaining, and operating an interconnection between systems or networks. It specifies the requirements for connecting the systems and networks and details what security controls are co be used to protect the systems and sensitive data.

QUESTION 3

CORRECT TEXT

An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner.

Instructions: The last install that is completed will be the final submission.



A.

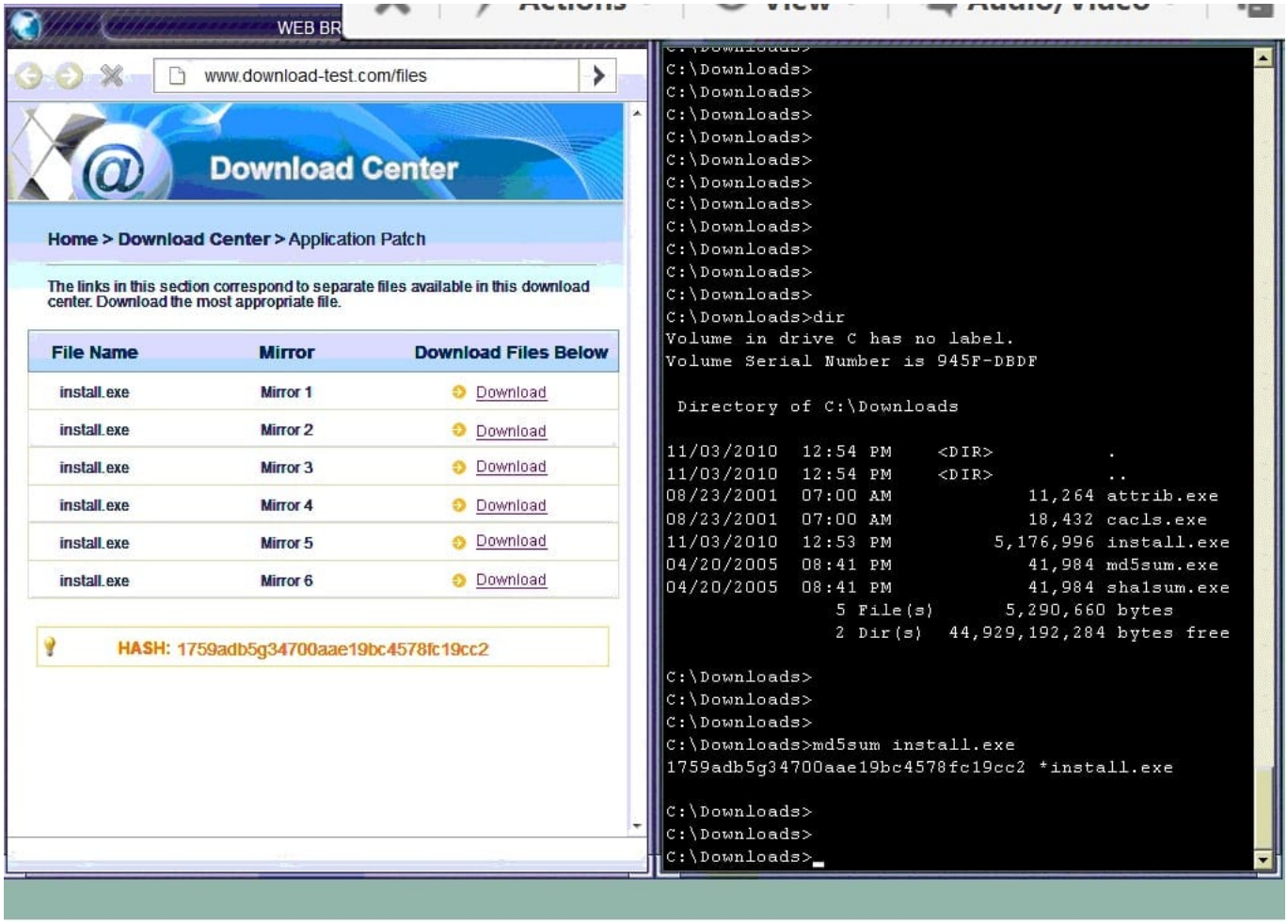
Correct Answer: A

Answer: Please check the explanation part for full details on solution. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

Also, two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:

Since we need to do this in the most secure manner possible, they should not be used.

Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



Finally, type in install.exe to install it and make sure there are no signature verification errors.

We use the MD5Sum utility to view the hash of the downloaded file. If the hash matches the hash shown on the download page, then we know that the file we are downloading has not been modified.

md5sum is a computer program that calculates and verifies 128-bit MD5 hashes, as described in RFC 1321. The MD5 hash (or checksum) functions as a compact digital fingerprint of a file.

Virtually any non-malicious change to a file will cause its MD5 hash to change; therefore md5sum is used to verify the integrity of files. Most commonly, md5sum is used to verify that a file has not changed as a result of a faulty file transfer, a

disk error or non-malicious meddling. The md5sum program is installed by default in most Unix, Linux, and Unix-like operating systems or compatibility layers. Other operating systems, including Microsoft Windows and BSD variants -- such as

Mac OS X - have similar utilities.

References:

https://en.wikipedia.org/wiki/Md5sum

QUESTION 4

A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs

B. Interview employees and managers to discover the industry hot topics and trends

C. Attend meetings with staff, internal training, and become certified in software management

D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Correct Answer: D

Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.

QUESTION 5

The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer\\'s (CSO) request to harden the corporate network\\'s perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.

B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.

C. Home networks are unknown to attackers and less likely to be targeted directly.

D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Correct Answer: B

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more that on an employee\\'s home network, and is therefore more valuable.