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.pass4itsure.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

A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company\\'s online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

A. $60,000

B. $100,000

C. $140,000

D. $200,000

Correct Answer: A

ALE before implementing application caching: ALE = ARO x SLE ALE = 5 x $40,000 ALE = $200,000

ALE after implementing application caching:

ALE = ARO x SLE ALE = 1 x $40,000 ALE = $40,000

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

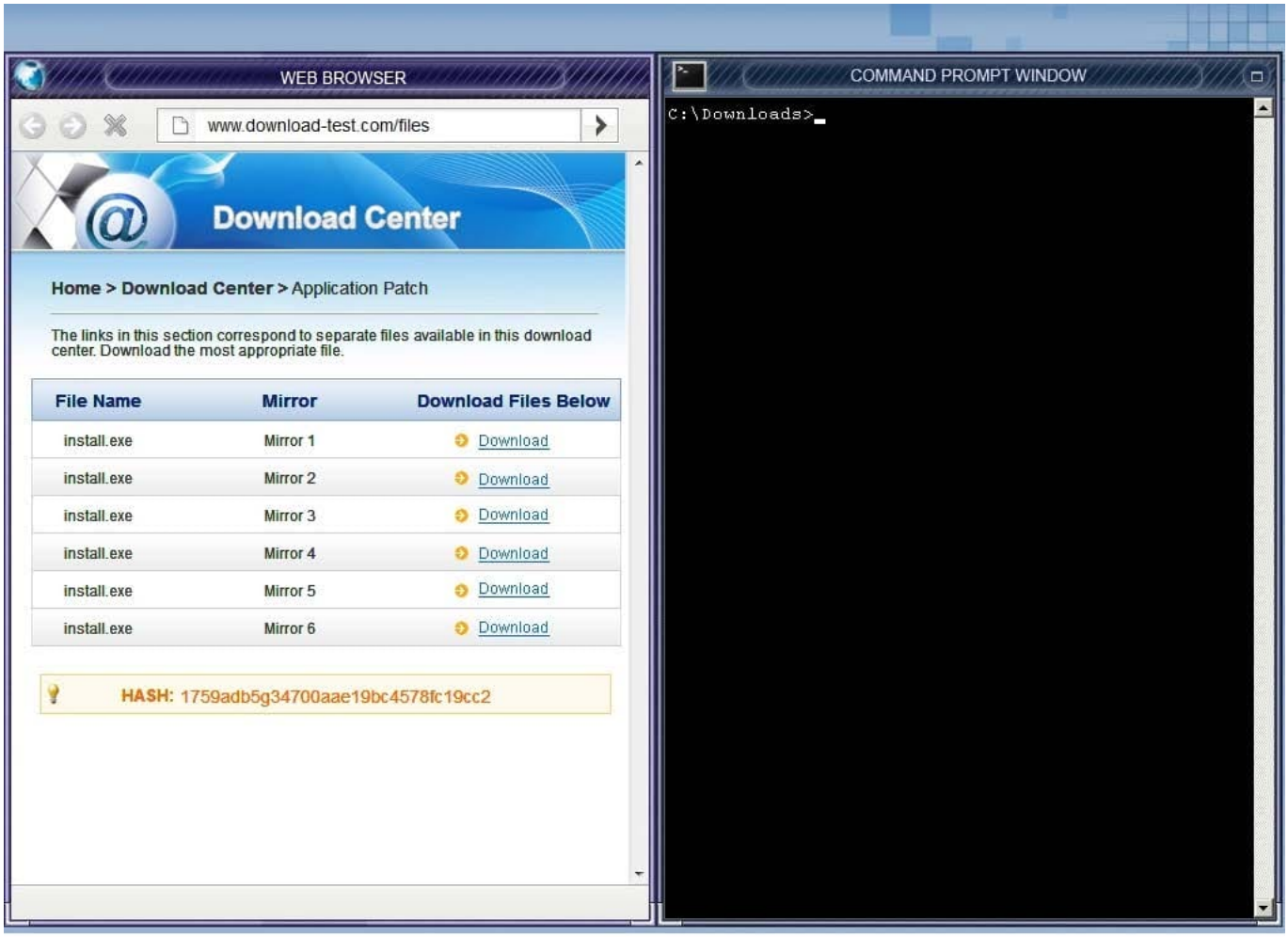
Monetary value earned = $200,000 - $40,000 - $100,000 Monetary value earned = $60,000

QUESTION 2

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.

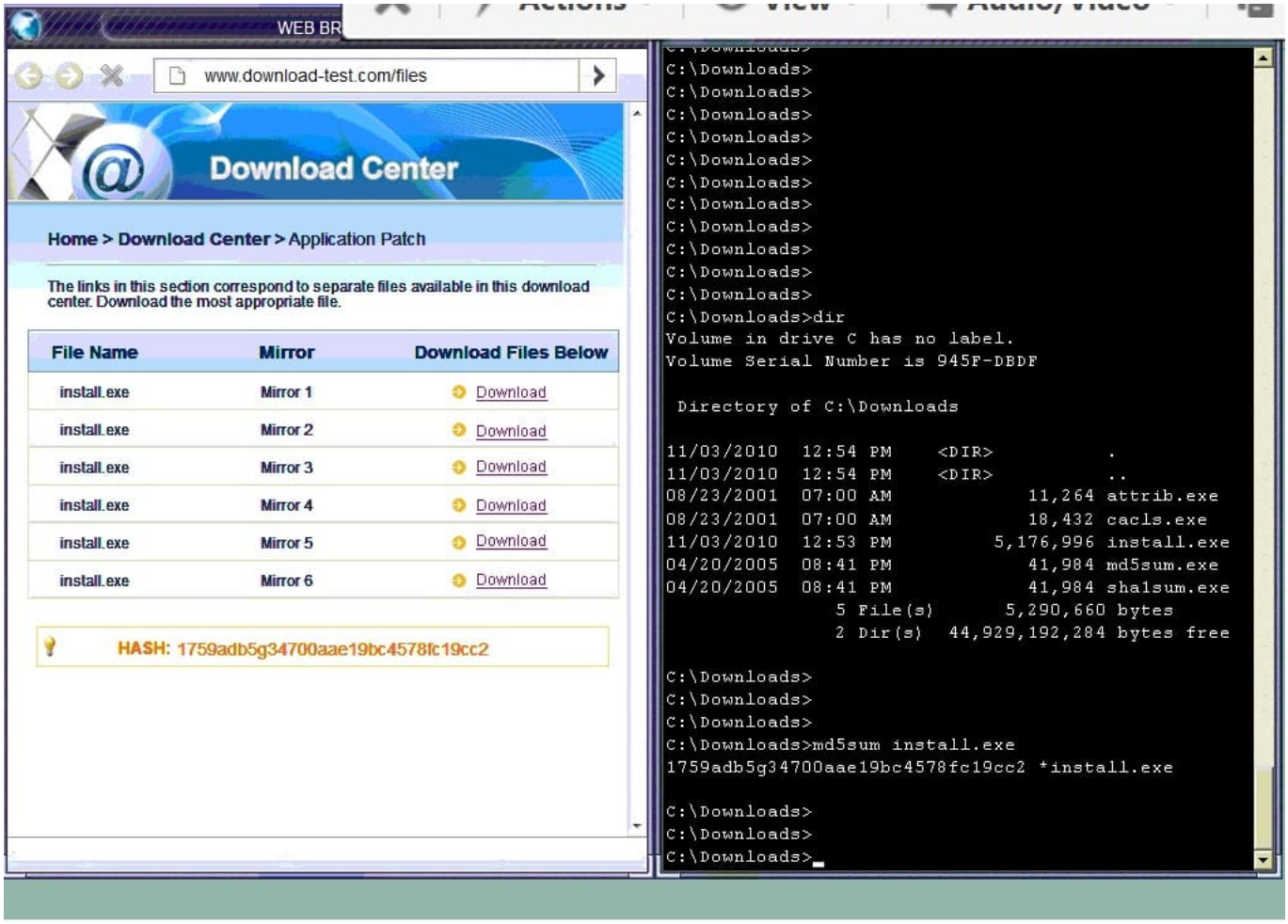
Correct Answer: A

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 3

A medium-sized company has recently launched an online product catalog. It has decided to keep the credit card purchasing in-house as a secondary potential income stream has been identified in relation to sales leads. The company has decided to undertake a PCI assessment in order to determine the amount of effort required to meet the business objectives. Which compliance category would this task be part of?

A. Government regulation

B. Industry standard

C. Company guideline

D. Company policy

Correct Answer: B

QUESTION 4

A company receives an e-discovery request for the Chief Information Officer\\'s (CIO\\'s) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?

A. 1

B. 2

C. 3

D. 5

Correct Answer: D

QUESTION 5

A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company\\'s

security information and event management server.

Logs:

Log 1:

Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets

Log 2:

HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Log 3:

Security Error Alert

Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client

Log 4:

Encoder oe = new OracleEncoder ();

String query = "Select user_id FROM user_data WHERE user_name = ` "

+ oe.encode (req.getParameter("userID")) + " ` and user_password = ` "

+ oe.encode (req.getParameter("pwd")) +" ` ";

Vulnerabilities

Buffer overflow

SQL injection

ACL

XSS

Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1

B. Log 2

C. Log 3

D. Log 4

E. Buffer overflow

F. ACL

G. XSS

H. SQL injection

Correct Answer: BE

Log 2 indicates that the security breach originated from an external source. And the vulnerability that can be associated with this security breach is a buffer overflow that happened when the amount of data written into the buffer exceeded the limit of that particular buffer.