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.geekcert.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

An IT manager is working with a project manager from another subsidiary of the same multinational organization. The project manager is responsible for a new software development effort that is being outsourced overseas, while customer acceptance testing will be performed in house. Which of the following capabilities is MOST likely to cause issues with network availability?

A. Source code vulnerability scanning

B. Time-based access control lists

C. ISP to ISP network jitter

D. File-size validation

E. End to end network encryption

Correct Answer: B

The new software development effort is being outsourced overseas. Overseas means a different country and therefore a different time zone. Time-based access control lists allow access to resources only at defined times, for example: during office hours. If time-based access control lists are used at the overseas location while customer acceptance testing will be performed in house, it is likely that the testing would be performed at a time which is not allowed by the time-based access control lists.

Time-based ACLs are types of control lists that allow for network access based on time or day. Its function is similar to that of the extended ACLs. Time-based ACLs is implemented by creating a time range that defines specific times of the day and week. This time range created have to be identified with a specific name and then refer to it by a function. The time restrictions are imposed on the function itself. Time-based ACLs are especially useful when you want to place restriction(s) on inbound or outbound traffic based on the time of day. For example, you might apply time-based ACLs if you wanted to only allow access to the Internet during a particular time of the day or allow access to a particular server only during work hours. The time range relies on the router system clock.

QUESTION 2

An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

A. File system information, swap files, network processes, system processes and raw disk blocks.

B. Raw disk blocks, network processes, system processes, swap files and file system information.

C. System processes, network processes, file system information, swap files and raw disk blocks.

D. Raw disk blocks, swap files, network processes, system processes, and file system information.

Correct Answer: C

The order in which you should collect evidence is referred to as the Order of volatility. Generally, evidence should be collected from the most volatile to the least volatile. The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives Logs

stored on remote systems Archive media

QUESTION 3

An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

A. $4,800

B. $24,000

C. $96,000

D. $120,000

Correct Answer: C

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

Thus if SLE = $ 24,000 and EF = 25% then the Asset value is SLE/EF = $ 96,000

References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

QUESTION 4

Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 0

B. 1

C. 3

D. 6

Correct Answer: C

You would need three wildcard certificates: *. east.company.com *. central.company.com *. west.company.com

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover ".company.com" but it won\\'t cover "..company.com". You can only have one wildcard in a domain. For example: *.company.com. You cannot have *.*.company.com. Only the leftmost wildcard (*) is counted.

QUESTION 5

Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology.

Which of the following would be the advantage of conducting this kind of penetration test?

A. The risk of unplanned server outages is reduced.

B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.

C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.

D. The results should reflect what attackers may be able to learn about the company.

Correct Answer: D

A black box penetration test is usually done when you do not have access to the code, much the same like an outsider/attacker. This is then the best way to run a penetration test that will also reflect what an attacker/outsider can learn about the company. A black box test simulates an outsiders attack.