



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.passapply.com/rc0-c02.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 storage as a service company implements both encryption at rest as well as encryption in transit of customers' data. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

- A. key = NULL ; for (int i=0; i < 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0
- G. Nmap

Correct Answer: AFG

Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.

The output displayed in option F includes information commonly examined to fingerprint the OS.

Nmap provides features that include host discovery, as well as service and operating system detection.

QUESTION 5

Ann, the VoIP administrator, starts receiving reports that users are having problems placing phone calls. She cannot determine the issue, and asks Joe, the security administrator, for help. Joe reviews the switch interfaces and does not see an excessive amount of network traffic on the voice network. Using a protocol analyzer, he does see an excessive number of SIP INVITE packets destined for the SIP proxy. Based on the information given, which of the following types of attacks is underway and how can it be remediated?

- A. Man in the middle attack; install an IPS in front of SIP proxy.
- B. Man in the middle attack; use 802.1x to secure voice VLAN.
- C. Denial of Service; switch to more secure H.323 protocol.
- D. Denial of Service; use rate limiting to limit traffic.

Correct Answer: D

QUESTION 6

The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

- A. Race condition
- B. Click-jacking



- C. Integer overflow
- D. Use after free
- E. SQL injection

Correct Answer: C

Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.

QUESTION 7

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
- B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
- C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
- D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.

Correct Answer: D

Good preventive security practices are a must. These include installing and keeping firewall policies carefully matched to business and application needs, keeping antivirus software updated, blocking potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion- prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.

QUESTION 8

Three companies want to allow their employees to seamlessly connect to each other's wireless corporate networks while keeping one consistent wireless client configuration. Each company wants to maintain its own authentication infrastructure and wants to ensure that an employee who is visiting the other two companies is authenticated by the home office when connecting to the other companies' wireless network. All three companies have agreed to standardize on 802.1x EAP-PEAP-MSCHAPv2 for client configuration. Which of the following should the three companies implement?

- A. The three companies should agree on a single SSID and configure a hierarchical RADIUS system which implements trust delegation.
- B. The three companies should implement federated authentication through Shibboleth connected to an LDAP backend and agree on a single SSID.



- C. The three companies should implement a central portal-based single sign-on and agree to use the same CA when issuing client certificates.
- D. All three companies should use the same wireless vendor to facilitate the use of a shared cloud based wireless controller.

Correct Answer: A

To enable "employees to seamlessly connect to each other's wireless corporate networks while keeping one consistent wireless client configuration", the wireless networks must all use the same SSID.

We should use RADIUS (Remote Authentication Dial-In User Service). RADIUS is a protocol that was originally used to authenticate users over dialup connections, but is increasingly used for other authentication scenarios, including the

wireless network. A RADIUS hierarchy with delegated trust will enable a user connecting to one company wireless network (not his home company network) to be authenticated by the RADIUS server in his home network. For example: if a

user from Company A connects to the wireless network in Company C, the Company C RADIUS server will see that the user is not from Company A and forward the authentication request to the RADIUS server in Company A.

QUESTION 9

An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

- A. Implementing federated network access with the third party.
- B. Using a HSM at the network perimeter to handle network device access.
- C. Using a VPN concentrator which supports dual factor via hardware tokens.
- D. Implementing 802.1x with EAP-TTLS across the infrastructure.

Correct Answer: D

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.



EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.

QUESTION 10

An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

- A. Deploy custom HIPS signatures to detect and block the attacks.
- B. Validate and deploy the appropriate patch.
- C. Run the application in terminal services to reduce the threat landscape.
- D. Deploy custom NIPS signatures to detect and block the attacks.

Correct Answer: B

If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION 11

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be \$150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time

employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be \$100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.



Internal employee costs are averaged to be \$80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

- A. Based on cost alone, having an outsourced solution appears cheaper.
- B. Based on cost alone, having an outsourced solution appears to be more expensive.
- C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
- D. Based on cost alone, having a purchased product solution appears cheaper.

Correct Answer: A

The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the

company expense if \$80,000 per year per FTE.

For the company to go alone it will cost \$80,000 per annum per FTE = \$400,000 over 5 years.

With Vendor a \$150,000 + \$200,000 (?FTE) = \$350,000 With Vendor B = \$100,000 it will be more expensive.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley and Sons, Indianapolis, 2012, p. 130

QUESTION 12

A company runs large computing jobs only during the overnight hours. To minimize the amount of capital investment in equipment, the company relies on the elastic computing services of a major cloud computing vendor. Because the virtual resources are created and destroyed on the fly across a large pool of shared resources, the company never knows which specific hardware platforms will be used from night to night. Which of the following presents the MOST risk to confidentiality in this scenario?

- A. Loss of physical control of the servers
- B. Distribution of the job to multiple data centers
- C. Network transmission of cryptographic keys
- D. Data scraped from the hardware platforms

Correct Answer: D

QUESTION 13

A recently hired security administrator is advising developers about the secure integration of a legacy in-house application with a new cloud based processing system. The systems must exchange large amounts of fixed format data such as names, addresses, and phone numbers, as well as occasional chunks of data in unpredictable formats. The developers want to construct a new data format and create custom tools to parse and process the data. The security administrator instead suggests that the developers:



- A. Create a custom standard to define the data.
- B. Use well formed standard compliant XML and strict schemas.
- C. Only document the data format in the parsing application code.
- D. Implement a de facto corporate standard for all analyzed data.

Correct Answer: B

Explanation: To ensure the successful parsing of the data, the XML code containing the data should be well-formed. We can use strict schemas to ensure the correct formatting of the data.

XML has two main advantages: first, it offers a standard way of structuring data, and, second, we can specify the vocabulary the data uses. We can define the vocabulary (what elements and attributes an XML document can use) using either

a document type definition (DTD) or the XML Schema language.

Schemas provide the ability to define an element's type (string, integer, etc.) and much finer constraints (a positive integer, a string starting with an uppercase letter, etc.). DTDs enforce a strict ordering of elements; schemas have a more

flexible range of options. Finally schemas are written in XML, whereas DTDs have their own syntax. For an application to accept an XML document, it must be both well formed and valid. A document that is not well formed is not really XML

and doesn't conform to the W3C's stipulations for an XML document. A parser will fail when given that document, even if validation is turned off.

QUESTION 14

The element in SAML can be provided in which of the following predefined formats? (Select TWO).

- A. X.509 subject name
- B. PTR DNS record
- C. EV certificate OID extension
- D. Kerberos principal name
- E. WWN record name

Correct Answer: AD

QUESTION 15

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

- A. Static and dynamic analysis is run as part of integration



- B. Security standards and training is performed as part of the project
- C. Daily stand-up meetings are held to ensure security requirements are understood
- D. For each major iteration penetration testing is performed
- E. Security requirements are story boarded and make it into the build
- F. A security design is performed at the end of the requirements phase

Correct Answer: AD

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

[RC0-C02 VCE Dumps](#)

[RC0-C02 Study Guide](#)

[RC0-C02 Exam Questions](#)