RC0-C02$^{Q\&As}$

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

Pass CompTIA RC0-C02 Exam with 100% Guarantee

QUESTION 1

As part of a new wireless implementation, the Chief Information Officer\\'s (CIO\\'s) main objective is to immediately deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard was not ratified by the IETF. The wireless vendor\\'s products do support the pre-ratification version of 802.11r. The security and network administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. Which of the following is the BEST way to proceed?

A. Purchase the equipment now, but do not use 802.11r until the standard is ratified.

B. Do not purchase the equipment now as the client devices do not yet support 802.11r.

C. Purchase the equipment now, as long as it will be firmware upgradeable to the final 802.11r standard.

D. Do not purchase the equipment now; delay the implementation until the IETF has ratified the final 802.11r standard.

Correct Answer: C

QUESTION 2

An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation

B. Security test and evaluation

C. Risk assessment

D. Ongoing authorization

Correct Answer: D

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and

unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or

closely after events in which the key controls are utilized.

QUESTION 3

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.

B. A DLP gateway should be installed at the company border.

C. Strong authentication should be implemented via external biometric devices.

D. Full-tunnel VPN should be required for all network communication.

E. Full-drive file hashing should be implemented with hashes stored on separate storage.

F. Split-tunnel VPN should be enforced when transferring sensitive data.

Correct Answer: BD

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control

what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For

example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

QUESTION 4

A company is trying to decide how to manage hosts in a branch location connected via a slow WAN link. The company desires to provide the same level of performance and functionality to the branch office as it provides to the main campus. The company uses Active Directory for its directory service and host configuration management. The branch location does not have a datacenter, and the physical security posture of the building is weak. Which of the following designs is MOST appropriate for this scenario?

A. Deploy a branch location Read-Only Domain Controller in the DMZ at the main campus with a two-way trust.

B. Deploy a corporate Read-Only Domain Controller to the branch location.

C. Deploy a corporate Domain Controller in the DMZ at the main campus.

D. Deploy a branch location Read-Only Domain Controller to the branch office location with a one-way trust.

E. Deploy a corporate Domain Controller to the branch location.

F. Deploy a branch location Domain Controller to the branch location with a one-way trust.

Correct Answer: B

A read-only domain controller (RODC) is a new type of domain controller in the Windows Server?2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory?Domain Services (AD DS) database. Before the release of Windows Server 2008, if users had to authenticate with a domain controller over a wide area network (WAN), there was no real alternative. In many cases, this was not an efficient solution. Branch offices often cannot provide the adequate physical security that is required for a writable domain controller. Furthermore, branch offices often have poor network bandwidth when they are connected to a hub site. This can increase the amount of time that is required to log on. It can also hamper access to network resources. Beginning with Windows Server 2008, an organization can deploy an RODC to address these problems. As a result, users in this situation can receive the following benefits: Improved security Faster logon times More efficient access to resources on the network

QUESTION 5

A Security Manager is part of a team selecting web conferencing systems for internal use. The system will only be used for internal employee collaboration. Which of the following are the MAIN concerns of the security manager? (Select THREE).

A. Security of data storage

B. The cost of the solution

C. System availability

D. User authentication strategy

E. PBX integration of the service

F. Operating system compatibility

Correct Answer: ACD

QUESTION 6

Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

A. Aggressive patch management on the host and guest OSs.

B. Host based IDS sensors on all guest OSs.

C. Different antivirus solutions between the host and guest OSs.

D. Unique Network Interface Card (NIC) assignment per guest OS.

Correct Answer: A

This question is asking "Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform. In other words, what is the primary method protecting VMs.

The first thing we should do to protect the VMs is to ensure that the guest OS\\'s are patched and ensure that the host is patched. The host provides the virtualization software to enable the running of the virtual machines. Any floors in the virtualization software that affect the VM separation enabling an attack between VMs running on the host would hopefully be fixed by the virtualization software vendor in a patch. The most important step and therefore "the basis" for protecting

VMs would be aggressive patch management.

QUESTION 7

A large financial company has a team of security-focused architects and designers that contribute into broader IT architecture and design solutions. Concerns have been raised due to the security contributions having varying levels of quality and consistency. It has been agreed that a more formalized methodology is needed that can take business drivers, capabilities, baselines, and re-usable patterns into account. Which of the following would BEST help to achieve these objectives?

A. Construct a library of re-usable security patterns

B. Construct a security control library

C. Introduce an ESA framework

D. Include SRTM in the SDLC

Correct Answer: C

QUESTION 8

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim\\'s privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

A. Integer overflow

B. Click-jacking

C. Race condition

D. SQL injection

E. Use after free

F. Input validation

Correct Answer: E

Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full

remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been

freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

QUESTION 9

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable

and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart\\'s items?

A. Input validation

B. SQL injection

C. TOCTOU

D. Session hijacking

Correct Answer: C

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item. In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition. A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

QUESTION 10

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:

Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks. Student devices must have network access, not simple access to hosts on the lab networks.

Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students.

All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment

B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment

C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment

D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Correct Answer: C

IPSec VPN with mutual authentication meets the certificates requirements.

RADIUS can be used with the directory service for the user authentication. ACLs (access control lists) are the best solution for restricting access to network hosts.

QUESTION 11

A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent

B. 5.5 percent

C. 45 percent

D. 82 percent

Correct Answer: D

Return on investment = Net profit / Investment

where:Net profit = gross profit ?expenses

investment = stock + market outstanding[when defined as?] + claims

or

Return on investment = (gain from investment ?cost of investment) / cost of investment Thus (100 000 ?55 000)/50 000 = 0,82 = 82 %

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley and Sons, Indianapolis, 2012, p. 337 http://www.financeformulas.net/Return_on_Investment.html

QUESTION 12

A firm\\'s Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product\\'s reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO\\'s requirements?

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.

B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.

C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.

D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Correct Answer: C

Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

QUESTION 13

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 14

A developer has implemented a piece of client-side JavaScript code to sanitize a user\\'s provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

```
10.235.62.11 ?- [02/Mar/2014:06:13:04] "GET /site/script.php?user=adminandpass=pass%20or%201=1 HTTP/1.1" 200
5724
```

Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.

B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.

C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.

D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Correct Answer: C

The code in the question is an example of a SQL Injection attack. The code `1=1\\' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table. In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION 15

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.

RC0-C02 PDF Dumps RC0-C02 Exam Questions RC0-C02 Braindumps