CA1-001 Q&As

CompTIA Advanced Security Practitioner (CASP) Beta Exam

Pass CompTIA CA1-001 Exam with 100% Guarantee

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

https://www.pass4itsure.com/CA1-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

In which of the following attacks does an attacker intercept call-signaling SIP message traffic and masquerade as the calling party to the called party and vice-versa?

A. Call tampering

B. Man-in-the-middle

C. Eavesdropping

D. Denial of Service

Correct Answer: B

VoIP is more vulnerable to man-in-the-middle attacks. In the man-in-the-middle attack, the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, and vice-versa. The attacker can hijack calls via a redirection server after gaining this position.

Answer option A is incorrect. Call tampering involves tampering a phone call in progress. Answer option D is incorrect. DoS attacks occur by flooding a target with unnecessary SIP call- signaling messages. It degrades the service and causes calls to drop prematurely and halts call processing.

Answer option C is incorrect. In eavesdropping, hackers steal credentials and other information.

QUESTION 2

Which of the following federal regulations requires federal agencies to be able to monitor activity in a "meaningful and actionable way"?

A. FISMA

B. HIPAA

C. Sarbanes-Oxley

D. CAN SPAM

Correct Answer: A

The Federal Information Security Management Act requires continuous monitoring of affected federal systems.

Answer option B is incorrect. The Health Information Portability and Accountability Act Governs the privacy of health records. Answer option C is incorrect. Sarbanes Oxley addresses the retention of documents and records in publically traded companies. Answer option D is incorrect. CAN SPAN regulates unsolicited email, commonly called spam.

QUESTION 3

Which of the following processes is used to ensure that standardized methods and procedures are used for efficient handling of all changes?

A. Exception management

B. Configuration Management

C. Risk Management

D. Change Management

Correct Answer: D

Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CIs)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows:

Minimal disruption of services

Reduction in back-out activities

Economic utilization of resources involved in the change Answer option B is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

Answer option A is incorrect. Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business.

Answer option C is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager.

Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises\\', so at IT Process Maps we decided to assign clear responsibilities for managing risks.

QUESTION 4

Which of the following is the best description of vulnerability assessment?

A. Determining what threats exist to your network.

B. Determining the impact to your network if a threat is exploited.

C. Determining the weaknesses in your network that would allow a threat to be exploited

D. Determining the likelihood of a given threat being exploited.

Correct Answer: C

Weaknesses in your network due to inherent technology weaknesses, mis-configuration, or lapses in security are vulnerabilities.

Answer option A is incorrect. Determining the threats to your network is threat assessment not vulnerability assessment.

In fact this phase is done before vulnerability assessment Answer option D is incorrect. Determining the likelihood of a given attack is likelihood assessment.

This would be done after vulnerability assessment.

Answer option B is incorrect. Impact analysis is certainly important, but this is done after vulnerability assessment.

QUESTION 5

Interceptor is a pseudo proxy server that performs HTTP diagnostics, which of the following features are provided by HTTP Interceptor? Each correct answer represents a complete solution. Choose all that apply.

A. It controls cookies being sent and received.

B. It allows to browse anonymously by withholding Referrer tag, and user agent.

C. It can view each entire HTTP header.

D. It debugs DOC, DOCX, and JPG file.

Correct Answer: ABC

HTTP diagnostics is performed by the HTTP Interceptor which is a pseudo proxy server and it also facilitates viewing the two way communication between the browser and the Internet.

Various features of HTTP Interceptor are as follows:

View each entire HTTP header.

Debug your PHP, ASP. CGI or JavaScript and htaccess file.

Control Cookies being sent and received.

Find out what sort of URL redirection the site may be using.

Browse anonymously by withholding Referrer tag, and user agent.