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.passapply.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

Mary is responsible for getting rid of old hard drives that are no longer used. It is important that all data be removed from the drive and none recoverable, but that the drive still be useable. Which of the following steps should she take before disposing of the drives?

A. Degauss the drive

B. Delete all data and defragment the drive.

C. Delete all data and do a high-level format of the drive.

D. Use a utility like Linux DD to overwrite all drive bits with zero\\'s

Correct Answer: D

The Linux DD command is even recommended for use in forensically wiping a drive. It will erase all data. It works at the bit level of the drive itself, changing all bits to zeros.

Answer option B is incorrect. Even with defragmenting, common undelete programs will be able to retrieve large amounts of data. Answer option C is incorrect. Even with a high-level format, common undelete programs will be able to retrieve large amounts of data. Answer option A is incorrect. Degaussing can damage the drive (it won\\'t always, but it can) and render it unusable.

QUESTION 2

What security objectives does cryptography meet:

Each correct answer represents a complete solution. Choose all that apply.

A. Authentication

B. Confidentiality

C. Data integrity

D. Authorization

Correct Answer: ABC

Cryptography is used to meet the following security objectives:

Confidentiality is used to restrict access to the sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals/processes.

Data integrity is used to address the unauthorized/accidental modification of data. This includes data insertion, deletion, and modification. In order to ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Authentication is used to establish the validity of a transmission, message, or an originator. It also verifies an individual\\'s authorization to receive specific categories of information, but it is not specific to cryptography. Therefore, authentication applies to both individuals and the information itself. The goal is for the receiver of the data to determine

its origin.

Non-repudiation is used to prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender\\'s identity.

QUESTION 3

You work as a Network Administrator for uCertify Inc. You need to conduct network reconnaissance, which is carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized/allowed.

What will you do?

A. Use a SuperScan

B. Use a netcat utility

C. Use a vulnerability scanner

D. Use an idle scan

Correct Answer: C

In the given scenario, you will use a vulnerability scanner. The vulnerability scanner can be used to conduct network reconnaissance. Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

Answer option B is incorrect. Netcat is a freely available networking utility that reads and writes data across network connections by using the TCP/IP protocol. Netcat has the following features: It provides outbound and inbound connections for TCP and UDP ports.

It provides special tunneling such as UDP to TCP, with the possibility of specifying all network parameters.

It is a good port scanner.

It contains advanced usage options, such as buffered send-mode (one line every N seconds), and hexdump (to stderr or to a specified file) of transmitted and received data.

It is an optional RFC854 telnet code parser and responder.

Answer option A is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the hostname of the remote system. It can also be used as

an enumeration tool for the following:

NetBIOS information

User and Group Accounts information

Network shares

Trusted Domains

Services probing

QUESTION 4

Which of the following refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements?

A. Trusted OS

B. Distributed operating system

C. Network operating system

D. Real time operating system

Correct Answer: A

Trusted Operating System (TOS) refers to an operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements.

The Common Criteria, combined with the Security Functional Requirements (SFRs) for Labeled Security Protection Profile (LSPP) and Mandatory Access Control(MAC) is the most common set of criteria for trusted operating system design. The Common Criteria is the outcome of a multi-year effort by the governments of the U.S., Canada. United Kingdom, France, Germany- the Netherlands and other countries with an aim to develop a harmonized security criteria for IT products.

Answer option D is incorrect. A real-time operating system (RTOS) is an operating system used to serve real-time application requests. It is an operating system that guarantees a certain capability within a specified time constraint. A key characteristic of an RTOS is the level of its consistency concerning the amount of time it takes to accept and complete an application s task. A real-time OS has an advanced algorithm for scheduling and is more frequently dedicated to a narrow set of applications. Answer option C is incorrect. The network operating system (NOS) manages resources on a network, offers services to one or more clients, and enables clients to access remote drives as if the drives where on clients own computer. The functions provided by a network operating system are as follows:

File and print sharing

Account administration for users

Security

Answer option B is incorrect. A distributed operating system is the logical aggregation of operating system software over a collection of independent, networked, communicating, and spatially disseminated computational nodes.

QUESTION 5

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.