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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is a security incident in which sensitive or confidential data is copied, transmitted, viewed, or stolen by unauthorized person?

A. Security token

B. Data masking

C. Data breach

D. Data erasure

Correct Answer: C

A data breach is the planned or unplanned release of secure information to an environment that is not trusted. Incidents range from concerted attack by black hats with the backing of organized crime or national governments to careless disposal of used computer equipment or data storage media.

A data breach is a security incident in which sensitive or confidential data is copied- transmitted, viewed, or stolen by unauthorized person. Financial information like credit card or bank details, personal health information (PHI), personally identifiable information (PII), and trade secrets of corporations or intellectual property can also be involved in a data breach. Answer options A, D, and B are incorrect. These are not valid options.

QUESTION 2

A user can divide network traffic into which of the following classes of service? Each correct answer represents a complete solution. Choose three.

A. Video payload

B. Voice and video payload

C. Voice payload

D. Voice and video signal traffic

Correct Answer: ACD

A user can divide network traffic into the following three classes of service:

Voice payload: Voice calls are a major part of network traffic, so a network traffic is mainly divided in this class.

Video payload: Video traffic has variable packet rates and slightly variable bit rates, so this class is used to separate the video traffic.

Voice and video signal traffic: This traffic is treated as a data application in QoS. In this class, protocols are used to tolerate jitter and delay.

Answer option B is incorrect. It is not a valid option.

QUESTION 3

Which of the following phases of the System Development Life Cycle (SDLC) describes that the system should be modified on a regular basis through the addition of hardware and software?

A. Operation/Maintenance

B. Development/Acquisition

C. Initiation

D. Implementation

Correct Answer: A

There are five phases in the SDLC. The characteristics of each of these phases are enumerated below:

Phase 1: Phase i of the SDLC is known as initiation. In this phase, the need for an IT system is expressed and the purpose and scope of the IT system is documented.

Phase 2: Phase 2 of the SDLC is known as development or acquisition. In this phase, the IT system is designed, purchased, and programmed.

Phase 3: Phase 3 of the SDLC is known as implementation. This phase involves the system security features. The system security features should be configured, enabled, tested, and verified.

Phase 4: Phase 4 of the SDLC is known as operation or maintenance. This phase describes that the system should be modified on a regular basis through the addition of hardware and software.

Phase 5: Phase 5 of the SDLC is known as disposal. This phase involves disposition of information, hardware, and software.

QUESTION 4

Which of the following is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program?

A. Gray box testing

B. White box testing

C. Black box testing

D. Fuzzing

Correct Answer: D

The programs and frameworks that are used to create fuzz tests or perform fuzz testing are called fuzzers. Fuzzing has evolved from a niche technique into a full testing discipline with support from both the security research and traditional QA testing communities. Fuzzing (Fuzz testing) is an automated software testing technique that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Answer option C is incorrect. Black box testing is also known as specification-based testing. It ignores the internal logic

of an application. It refers to test activities using specification-based testing methods to discover errors in an application. The test activities are based on requirements and specifications of the application. It focuses on the following errors:

Specification-based function errors

Specification-based

component/system behavior errors

Specification-based

performance errors

User-oriented usage errors

Black box interface errors

Answer option B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods:

Control flow-based testing

o Create a graph from source code.

o Describe the flow of control through the control flow graph. o Design test cases to cover certain elements of the graph.

Data flow-based testing

o Test connections between variable definitions.

o Check variation of the control flow graph.

o Set DEF (n) contains variables that are defined at node n.

o Set USE (n) are variables that are read.

Answer option A is incorrect. Gray box testing is a combination of black box and white box testing. It is non-intrusive and impartial, as it does not require that a tester have access to the source code. It treats a system as a black box in the sense that it must be analyzed from the outside. Basically, it is used to find out defects related to bad design or bad implementation of the system. This type of testing is more commonly used with Web applications, as the Internet has a pretty stable interface.

QUESTION 5

Which of the following attacks are computer threats that try to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer?

A. FMS

B. Spoofing

C. Buffer overflow

D. Zero-day

Correct Answer: D

A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.

Answer option A is incorrect. The Fluhrer, Mantin, and Shamir (FMS) attack is a particular stream cipher attack, a dedicated form of cryptanalysis for attacking the widely-used stream cipher RC4. The attack allows an attacker to recover the key in an RC4 encrypted stream from a large number of messages in that stream. The FMS attack gained popularity in tools such as AirSnort and aircrack, both of which can be used to attack WEP encrypted wireless networks. Answer option C is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

Answer option B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else\\'s IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.