**VCE & PDF**

**Pass4itSure.com**

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

# CAS-001<sup>Q&As</sup>

CompTIA Advanced Security Practitioner

## Pass CompTIA CAS-001 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/CAS-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**

A company has decided to use the SDLC for the creation and production of a new information system. The security administrator is training all users on how to protect company information while using the new system, along with being able to recognize social engineering attacks. Senior Management must also formally approve of the system prior to it going live.

In which of the following phases would these security controls take place?

A. Operations and Maintenance

B. Implementation

C. Acquisition and Development

D. Initiation

Correct Answer: B

**QUESTION 2**

Statement: "The system shall implement measures to notify system administrators prior to a security incident occurring." Which of the following BEST restates the above statement to allow it to be implemented by a team of software developers?

A. The system shall cease processing data when certain configurable events occur.

B. The system shall continue processing in the event of an error and email the security administrator the error logs.

C. The system shall halt on error.

D. The system shall throw an error when specified incidents pass a configurable threshold.

Correct Answer: D

**QUESTION 3**

A small bank is introducing online banking to its customers through its new secured website. The firewall has three interfaces: one for the Internet connection, another for the DMZ, and the other for the internal network. Which of the following will provide the MOST protection from all likely attacks on the bank?

A. Implement NIPS inline between the web server and the firewall.

B. Implement a web application firewall inline between the web server and the firewall.

C. Implement host intrusion prevention on all machines at the bank.

D. Configure the firewall policy to only allow communication with the web server using SSL.

Correct Answer: C

**QUESTION 4**

Company XYZ has experienced a breach and has requested an internal investigation be conducted by the IT Department. Which of the following represents the correct order of the investigation process?

A. Collection, Identification, Preservation, Examination, Analysis, Presentation.

B. Identification, Preservation, Collection, Examination, Analysis, Presentation.

C. Collection, Preservation, Examination, Identification, Analysis, Presentation.

D. Identification, Examination, Preservation, Collection, Analysis, Presentation.

Correct Answer: B

**QUESTION 5**

The network administrator has been tracking the cause of network performance problems and decides to take a look at the internal and external router stats.

**External Router**

| | |
|---|---|
| TCP | 50% |
| UDP | 30% |
| OTHER | 20% |

**Traffic Stats over the last hour**

| | |
|---|---|
| TCP port 80 | 1.7M packets |
| TCP port 443 | 0.8M packets |
| TCP port 22 | 0.2M packets |
| TCP port 8080 | 10M packets |

**Internal Router**

| | |
|---|---|
| TCP | 0% |
| UDP | 2% |
| ICMP | 98% |

**Traffic Stats over the last hour**

| | |
|---|---|
| TCP port 80 | 0.5K packets |
| TCP port 443 | 0.8K packets |
| UDP port 53 | 0.2M packets |
| ICMP | 10M packets |

Which of the following should the network administrator do to resolve the performance issue after analyzing the above information?

A. The IP TOS field of business related network traffic should be modified accordingly.

B. The TCP flags of business related traffic should be modified accordingly.

C. An ACL should be placed on the external router to drop incoming ICMP packets.

D. An ACL should be placed on the internal router to drop layer 4 packets to and from port 0.

Correct Answer: A

To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4itsure.com/allproducts

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: