CISA

ISACA

ISACA CISA (Certified Information Systems Auditor)

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your CISA exam in first attempt and also get high scores to acquire ISACA certification.

If you use OfficialCerts CISA Certification questions and answers, you will experience actual CISA exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ISACA exam prep covers over 95% of the questions and answers that may be appeared in your CISA exam. Every point from pass4sure CISA PDF, CISA review will help you take ISACA CISA exam much easier and become ISACA certified.

Here's what you can expect from the OfficialCerts ISACA CISA course:

** Up-to-Date ISACA CISA questions as experienced in the real exam.*
** 100% correct ISACA CISA answers you simply can't find in other CISA courses.*
** All of our tests are easy to download. Your file will be saved as a CISA PDF.*
** ISACA CISA brain dump free content featuring the real CISA test questions.*

ISACA CISA certification exam is of core importance both in your Professional life and ISACA certification path. With ISACA certification you can get a good job easily in the market and get on your path for success. Professionals who passed ISACA CISA exam training are an absolute favorite in the industry.
You will pass ISACA CISA certification test and career opportunities will be open for you.

http://tripleamarine.com/?cert=exams.asp?examcode=CISA

QUESTION: 1
The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.
D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Answer: A

Explanation:
The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed; its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

QUESTION: 2
The most common problem in the operation of an intrusion detection system (IDS) is:

A. the detection of false positives.
B. receiving trap messages.
C. reject-error rates.
D. denial-of-service attacks.

Answer: A

Explanation:
Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents-false positives, the equivalent of a false alarm. An IS auditor needs to be aware of this and should check for implementation of related controls, such as IDS tuning, and incident handling procedures, such as the screening process to know if an event is a security incident or a false positive. Trap messages are generated by the Simple Network

Management Protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs. Reject-error rate is related to biometric technology and is not related to IDSs. Denial-of-service is a type of attack and is not a problem in the operation of IDSs.

QUESTION: 3
Which of the following provides no repudiation services for e-commerce transactions?

A. Public key infrastructure (PKI)
B. Data Encryption Standard (DES)
C. Message authentication code (MAC)
D. Personal identification number (PIN)

Answer: A

Explanation:
PKl is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it; it is capable of verification; it is under the sole control of the person using it; and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKl meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address no repudiation . A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission; it has nothing to do with no repudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

QUESTION: 4
While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

A. A scan of all floppy disks before use
B. A virus monitor on the network file server

C. Scheduled daily scans of all network drives
D. A virus monitor on the user's personal computer

Answer: C

Explanation:
Scheduled daily scans of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

QUESTION: 5
Which of the following message services provides the strongest evidence that a specific action has occurred?

A. Proof of delivery
B. Nonrepudiation
C. Proof of submission
D. Message origin authentication

Answer: B

Explanation:
Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and message origin authentication. However, nonrepudiation provides stronger evidence because the proof can be demonstrated to a third party. Digital signatures are used to provide nonrepudiation . Message origination authentication will only confirm the source of the message and does not confirm the specification that has been completed.

QUESTION: 6
The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

A. only the sender and receiver are able to encrypt/decrypt the data.
B. the sender and receiver can authenticate their respective identities.
C. the alteration of transmitted data can be detected.
D. the ability to identify the sender by generating a one-time session key.

Answer: A

Explanation:
SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

QUESTION: 7
The role of the certificate authority (CA) as a third party is to:

A. provide secured communication and networking services based on certificates.
B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
C. act as a trusted intermediary between two communication partners.
D. confirm the identity of the entity owning a certificate issued by that CA.

Answer: D

Explanation:
The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

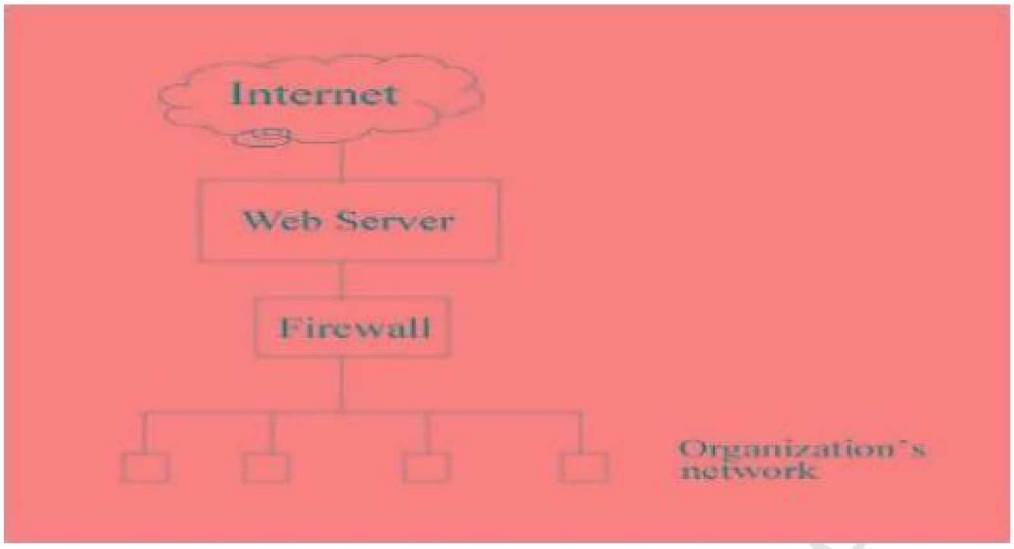
QUESTION: 8
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
B. All personal SET certificates are stored securely in the buyer's computer.
C. The buyer is liable for any transaction involving his/her personal SET certificates.
D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Answer: C

Explanation:
The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e-commerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

QUESTION: 9
E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

Answer: C

Explanation:
Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been be caused by an attack from a hacker. Closing firewa!l-2 is the first thing that should be done, thus preventing damage to the internal network. After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

QUESTION: 10
An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

A. The data collected on attack methods
B. The information offered to outsiders on the honeypot
C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
D. The risk that the honeypot would be subject to a distributed denial-of-service attack

Answer: C

Explanation:
Choice C represents the organizational risk that the honeypot could be used as a point of access to launch further attacks on the enterprise's systems. Choices A and B are purposes for deploying a honeypot , not a concern. Choice D, the risk that thehoneypot would be subject to a distributed denial-of-service (DDoS) attack, is not relevant, as the honeypot is not a critical device for providing service.

QUESTION: 11
Which of the following should be a concern to an IS auditor reviewing a wireless network?

A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
B. SSID (Service SetIDentifier) broadcasting has been enabled.
C. Antivirus software has been installed in all wireless clients.
D. MAC (Media Access Control) access control filtering has been deployed.

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google