SSCP Q&As

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

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

https://www.pass4itsure.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication

B. Administration

C. Accounting

D. Authorization

Correct Answer: B

Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

also see:

The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A\\'s" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.

Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

QUESTION 2

Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography

B. Digital watermarking

C. Digital enveloping

D. Digital signature

Correct Answer: B

RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data\\'s origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 3

In discretionary access environments, which of the following entities is authorized to grant information access to other people?

A. Manager

B. Group Leader

C. Security Manager

D. Data Owner

Correct Answer: D

In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/ user that is authorized to grant information access to other people.

security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE: The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data. The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

QUESTION 4

What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?

A. It can be very invasive to the host operating system

B. Monitors all processes and activities on the host system only

C. Virtually eliminates limits associated with encryption

D. They have an increased level of visibility and control compared to NIDS

Correct Answer: A

The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this

can sometimes interfere with normal system processing.

HIDS versus NIDS

A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

So, whereas the NIDS understands and monitors the network traffic, a HIDS\\'s universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system\\'s activity. Each has its own job and stays out of the other\\'s way.

The ISC2 official study book defines an IDS as:

An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS.

An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the

suspected attack.

What about IPS?

In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will

automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a

predetermined set of functions and actions to occur on a network or system; anything that is not permitted

is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an

event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but

also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is

considered an access control and policy enforcement technology, whereas IDS is considered network

monitoring and audit technology.

The following answers were incorrect:

All of the other answer were advantages and not drawback of using HIDS

TIP FOR THE EXAM:

Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS\\'s are mostly

detective but IPS are preventive. IPS\\'s are considered an access control and policy enforcement

technology, whereas IDS\\'s are considered network monitoring and audit technology.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (Kindle Locations 5817- 5822).

McGraw-Hill. Kindle Edition.

and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :

Access Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations

3199-3203. Auerbach Publications.

QUESTION 5

What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?

A. Registration authority

B. Certification authority

C. Issuing authority

D. Vouching authority

Correct Answer: B

A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.