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.pass2lead.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Knowledge-based Intrusion Detection Systems (IDS) are more common than:

A. Network-based IDS

B. Host-based IDS

C. Behavior-based IDS

D. Application-Based IDS

Correct Answer: C

Knowledge-based IDS are more common than behavior-based ID systems.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 63.

Application-Based IDS - "a subset of HIDS that analyze what\\'s going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87

Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197

Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK

p. 196

CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:

Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network-based and host-based, and knowledge- based and behavior-based:

Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system -- IPS) is a system that\\'s configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in- line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven\\'t been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that\\'s configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn\\'t capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn\\'t monitor the entire network.

Knowledge-based and behavior-based IDS A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained.

New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomalybased) IDS references a baseline or learned pattern of normal

system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm

to be triggered.

Advantages of behavior-based systems include that they

Dynamically adapt to new, unique, or original attacks.

Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective behavior-

based IDS.

QUESTION 2

Which type of firewall can be used to track connectionless protocols such as UDP and RPC?

A. Stateful inspection firewalls

B. Packet filtering firewalls

C. Application level firewalls

D. Circuit level firewalls

Correct Answer: A

Packets in a stateful inspection firewall are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC).

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 3: Telecommunications and Network Security (page 91).

QUESTION 3

Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.

B. To control the stability of the test environment.

C. To segregate user and development staff.

D. To secure access to systems under development.

Correct Answer: B

The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.

Reference(s) used for this question:

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 4

What is a decrease in amplitude as a signal propagates along a transmission medium best known as?

A. Crosstalk

B. Noise

C. Delay distortion

D. Attenuation

Correct Answer: D

Attenuation is the loss of signal strength as it travels. The longer a cable, the more at tenuation occurs, which causes the signal carrying the data to deteriorate. This is why standards include suggested cable-run lengths. If a networking cable is too long, attenuation may occur. Basically, the data are in the form of electrons, and these electrons have to "swim" through a copper wire. However, this is more like swimming upstream, because there is a lot of resistance on the electrons working in this media. After a certain distance, the electrons start to slow down and their encoding format loses form. If the form gets too degraded, the receiving system cannot interpret them any longer. If a network administrator needs to run a cable longer than its recommended segment length, she needs to insert a repeater or some type of device that will amplify the signal and ensure it gets to its destination in the right encoding format.

Attenuation can also be caused by cable breaks and malfunctions. This is why cables should be tested. If a cable is suspected of attenuation problems, cable testers can inject signals into the cable and read the results at the end of the cable.

The following answers are incorrect:

Crosstalk - Crosstalk is one example of noise where unwanted electrical coupling between adjacent lines causes the signal in one wire to be picked up by the signal in an adjacent wire.

Noise - Noise is also a signal degradation but it refers to a large amount of electrical fluctuation that can interfere with the interpretation of the signal by the receiver.

Delay distortion - Delay distortion can result in a misinterpretation of a signal that results from transmitting a digital signal with varying frequency components. The various components arrive at the receiver with varying delays.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and CISSP All-In-One Exam guide 6th Edition Page Number 561

QUESTION 5

Unshielded Twisted Pair (UTP) cables comes in several categories. The categories are based on:

A. The level of performance

B. How thick the shielding is.

C. The length of the cable

D. The diameter of the copper.

Correct Answer: A

TIA/EIA-568 is a set of telecommunications standards from the Telecommunications Industry Association, an offshoot of the EIA. The standards address commercial building cabling for telecom products and services.

The standard is currently (2009) at revision C, replacing the 2001 revision B, the 1995 revision A, and the initial issue of 1991, which are now obsolete.

Perhaps the best known features of TIA/EIA-568 are the pin/pair assignments for eight- conductor 100ohm balanced twisted pair cabling. These assignments are named T568A and T568B, and are frequently referred to (erroneously) as TIA/EIA-568A and TIA/EIA-568B. An IEC standard ISO/IEC 11801 provides similar standards for network cables.

The standard defines categories of unshielded twisted pair cable systems, with different levels of performance in signal bandwidth, attenuation, and cross-talk. Generally increasing category numbers correspond with a cable system suitable for higher rates of data transmission. Category 3 cable was suitable for telephone circuits and data rates up to 16 million bits per second. Category 5 cable, with more restrictions on attenuation and cross talk, has a bandwidth of 100 MHz. The 1995 edition of the standard defined categories 3, 4, and 5. Categories 1 and 2 were excluded from the standard since these categories were only used for voice circuits, not for data.

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.

SOME OF THE LIMITATION OF UTP UTP has several drawbacks. Because it does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.

Resource(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6511). Auerbach Publications. Kindle Edition.

http://en.wikipedia.org/wiki/TIA/EIA-568#cite_note-7

http://en.wikipedia.org/wiki/Twisted_pair

AIOv3 Telecommunication and Networking Security (page 455)