[May 2018 Free Updated Lead2pass CISSP Exam Dumps Download 2873q

Free Version Lead2pass (ISC)2 CISSP PDF Dumps With Exam Questions Download: https://www.lead2pass.com/cissp.html QUESTION 31Which of the following monitors network traffic in real time? A. network-based IDSB. host-based IDSC. application-based IDSD. firewall-based IDSAnswer: AExplanation:This type of IDS is called a network-based IDS because monitors network traffic in real time. QUESTION 32A host-based IDS is resident on which of the following? A. On each of the critical hostsB. decentralized hostsC. central hostsD. bastion hosts Answer: AExplanation:A host-based IDS is resident on a host and reviews the system and event logs in order to detect an attack on the host and to determine if the attack was successful. All critical serves should have a Host Based Intrusion Detection System (HIDS) installed. As you are well aware, network based IDS cannot make sense or detect pattern of attacks within encrypted traffic. A HIDS might be able to detect such attack after the traffic has been decrypted on the host. This is why critical servers should have both NIDS and HIDS. FROM WIKIPEDIA: A HIDS will monitor all or part of the dynamic behavior and of the state of a computer system. Much as a NIDS will dynamically inspect network packets, a HIDS might detect which program accesses what resources and assure that (say) a word-processor hasn't suddenly and inexplicably started modifying the system password-database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file-system, or elsewhere; and check that the contents of these appear as expected. One can think of a HIDS as an agent that monitors whether anything/anyone - internal or external - has circumvented the security policy that the operating system tries to enforce. http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system QUESTION 33Which of the following usually provides reliable, real-time information without consuming network or host resources? A. network-based IDSB. host-based IDSC. application-based IDSD. firewall-based IDS Answer: AExplanation:A network-based IDS usually provides reliable, real-time information without consuming network or host resources. QUESTION 34The fact that a network-based IDS reviews packets payload and headers enable which of the following? A. Detection of denial of serviceB. Detection of all virusesC. Detection of data corruptionD. Detection of all password guessing attacks Answer: AExplanation:Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected. This question is an easy question if you go through the process of elimination. When you see an answer containing the keyword: ALL It is something a give away that it is not the proper answer. On the real exam you may encounter a few question where the use of the work ALL renders the choice invalid. Pay close attention to such keyword. The following are incorrect answers: Even though most IDSs can detect some viruses and some password guessing attacks, they cannot detect ALL viruses or ALL password guessing attacks. Therefore these two answers are only detractors.Unless the IDS knows the valid values for a certain dataset, it can NOT detect data corruption. QUESTION 35Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful? A. host-based IDSB. firewall-based IDSC. bastion-based IDSD. server-based IDS Answer: AExplanation:A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful. QUESTION 36What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)? A. It can be very invasive to the host operating systemB. Monitors all processes and activities on the host system onlyC. Virtually eliminates limits associated with encryptionD. They have an increased level of visibility and control compared to NIDS Answer: A Explanation: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. QUESTION 37Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS)? A. signature-based IDSB. statistical anomaly-based IDSC. event-based IDSD. inferent-based IDS Answer: A QUESTION 38Which of the following is an issue with signature-based intrusion detection systems? A. Only previously identified attack signatures are detected.B. Signature databases must be augmented with inferential elements.C. It runs only on the windows operating systemD. Hackers can circumvent signature evaluations. Answer: AExplanation:An issue with signature-based ID is that only attack signatures that are stored in their database are detected.New attacks without a signature would not be reported. They do require constant updates in order to maintain their effectiveness. QUESTION 39Which of the following is an IDS that acquires data and defines a "normal" usage profile for the network or host? A. Statistical Anomaly-Based IDB. Signature-Based IDC. dynamical anomaly-based IDD. inferential anomaly-based ID Answer: AExplanation:Statistical Anomaly-Based ID - With this method, an IDS acquires data and defines a "normal" usage profile for the network or host that is being monitored. QUESTION 40Which of the following is most relevant to determining the maximum effective cost of access control? A. the value of information that is protected.B. management's perceptions regarding data importance.C. budget planning related to base versus incremental spending.D. the cost to replace lost data. Answer: AExplanation:The cost of access control must be commensurate with the value of the information that is being protected. **CISSP dumps full version (PDF&VCE):** https://www.lead2pass.com/cissp.html Large amount of free **CISSP** exam questions on Google Drive: https://drive.google.com/open?id=1393N8RayZN4QJ8sxg6_3cIRxwNv8QGTq