[Lead2pass Official Easily Pass Cisco 210-260 Exam With Lead2pass Latest Cisco 210-260 Brain Dumps (221-240)

2017 September Cisco Official New Released 210-260 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Are you worrying about the 210-260 exam? Lead2pass provides the latest 210-260 braindumps and guarantees you passing 210-260 exam beyond any doubt. Following questions and answers are all new published by Cisco Official Exam Center: https://www.lead2pass.com/210-260.html QUESTION 221Which type of Layer 2 attack can you "do something" for one host? A. MAC spoofingB. CAM overflowAnswer: BExplanation:Cisco implemented a technology into IOS called Port Security that mitigates the risk of a Layer 2 CAM overflow attack.Port Security on a Cisco switch enables you to control how the switch port handles the learning and storing of MAC addresses on a per-interface basis. The main use of this command is to set a limit to the maximum number of concurrent MAC addresses that can be learned and allocated to the individual switch port.If a machine starts broadcasting multiple MAC addresses in what appears to be a CAM overflow attack, the default action of Port Security is to shut down the switch interfacehttp://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2 QUESTION 222How to verify that TACACS+ is working? A. SSH to router and login with ACS credentialsB. loging to the device using enable passwordC. login to the device using ASC passwordD. console the device using some thing Answer: A QUESTION 223What are the challenges faced when deploying host based IPS? A. Must support multi operating systemsB. Does not have full network picture Answer: ABExplanation:Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.Limitations of HIPS: There are two major drawbacks to HIPS:+ HIPS does not provide a complete network picture : Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network.+ HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network. http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3 QUESTION 224What encryption technology has broadest platform support A. hardwareB. middlewareC. SoftwareD. File level Answer: C QUESTION 225With which preprocesor do you detect incomplete TCP handshakes A. rate based preventionB. port scan detection Answer: AExplanation:Rate-based attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate requests. Rate-based attacks usually have one of the following characteristics:+ any traffic containing excessive incomplete connections to hosts on the network, indicating a SYN flood attack+ any traffic containing excessive complete connections to hosts on the network, indicating a TCP/IP connection flood attack+ excessive rule matches in traffic going to a particular destination IP address or addresses or coming from a particular source IP address or addresses.+ excessive matches for a particular rule across all traffic. http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Threat-Detection.html QUESTION 226Which type of PVLAN port allows a host in the same VLAN to communicate only with promiscuous hosts? A. Community host in the PVLANB. Isolated host in the PVLANC. Promiscuous host in the PVLAN D. Span for host in the PVLAN Answer: BExplanation:The types of private VLAN ports are as follows:+ Promiscuous - The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN+ Isolated - This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. + Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html#42874 QUESTION 227Which type of encryption technology has the broadcast platform support? A. MiddlewareB. HardwareC. SoftwareD. File-level Answer: C QUESTION 228The first layer of defense which provides real-time preventive solutions against malicious traffic is provided by? A. Banyan FiltersB. Explicit FiltersC. Outbreak Filters Answer: C QUESTION 229SSL certificates are issued by Certificate Authority(CA) are? A. Trusted rootB. Not trusted Answer: A QUESTION 230SYN flood attack is a form of? A. Reconnaissance attackB. Denial of Service attackC. Man in the middle attackD. Spoofing attack Answer: BExplanation:A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.https://en.wikipedia.org/wiki/SYN_flood QUESTION 231The command debug crypto isakmp results in ? A. Troubleshooting ISAKMP (Phase 1) negotiation problems Answer: AExplanation:#debug crypto isakmpThis output shows an example of the debug crypto isakmp command.processing SA payload. message ID = 0Checking ISAKMP transform against priority 1 policyencryption 3DEShash SHAdefault group 2auth pre-sharelife type in secondslife duration (basic) of 240atts are acceptable. Next payload is 0processing KE payload. message ID = 0processing NONCE payload. message ID = 0processing ID payload. message ID = 0SKEYID state generatedprocessing HASH payload. message ID = 0SA has been authenticatedprocessing SA payload. message ID = 800032287Contains the IPsec Phase1 information. You can view the HAGLE (Hash, Authentication, DH Group, Lifetime, Encryption) process in the output QUESTION 232Which prevent the company data from modification even when the data is in transit? A. ConfidentialityB. IntegrityC. VailabilityD. Scalability Answer: BExplanation:Integrity: Integrity for data means that changes made to data are done only by authorized individuals/systems.Corruption of data is a failure to maintain data integrity. QUESTION 233The stealing of confidential information of a company comes under the scope of A. Reconnaissance B. Spoofing attackC. Social EngineeringD. Denial of Service Answer: CExplanation:Social engineeringThis is a tough one because it leverages our weakest (very likely) vulnerability in a secure system (data, applications, devices, networks): the user. If the attacker can get the user to reveal information, it is much easier for the attacker than using some other method of reconnaissance. This could be done through e-mail or misdirection of web pages, which results in the user clicking something that leads to the attacker gaining information. Social engineering can also be done in person or over the phone. QUESTION 234The Oakley cryptography protocol is compatible with following for managing security? A. IPSecB. ISAKMPC. Port security Answer: B Explanation:IKE (Internet Key Exchange)A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key-exchange QUESTION 235Which two features of Cisco Web Reputation tracking can mitigate web-based threats? (Choose Two) A. outbreak filterB. buffer overflow filterC. bayesian overflow filterD. web reputation filterE. exploit filtering Answer: ADExplanation:Cisco IronPort Outbreak Filters provide a critical first layer of defense against new outbreaks. With this proven preventive solution, protection begins hours before signatures used by traditional antivirus solutions are in place. Real-world results show an average 14-hour lead time over reactive antivirus solutions.SenderBase, the world's largest email and web traffic monitoring network, provides real-time protection. The Cisco IronPort SenderBase Network captures data from over 120,000 contributing organizations around the world. http://www.cisco.com/c/en/us/products/security/email-security-appliance/outbreak_filters_index.html QUESTION 236I had the "nested" question (wording has been different). Two answers ware related to hierarchy: A. there are only two levels of hierarchy possibleB. the higher level hierarchy becomes the parent for lower one parentC. inspect something is only possible with in a hierachy...D. some command question.... Answer: C QUESTION 237Which statement about command authorization and security contexts is true? A. If command authorization is configured, it must be enabled on all contextsB. The changeto command invokes a new context session with the credentials of the currently logged-in userC. AAA settings are applied on a per-context basisD. The enable_15 user and admins with changeto permissions have different command authorization levels per context Answer: BExplanation:The capture packet function works on an individual context basis. The ACE traces only the packets that belong to the context where you execute the capture command. You can use the context ID, which is passed with the packet, to isolate packets that belong to a specific context. To trace the packets for a single specific context, use the changeto command and enter the capture command for the new context.To move from one context on the ACE to another context, use the changeto command Only users authorized in the admin context or configured with the changeto feature can use the changeto command to navigate between the various contexts. Context administrators without the changeto feature, who have access to multiple contexts, must explicitly log in to the other contexts to which they have access. http://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/command/ reference/ACE_cr/execmds.html QUESTION 238Unicast Reverse Path Forwarding definition: A. Pending Answer: AExplanation: Unicast Reverse Path ForwardingUnicast Reverse Path Forwarding (uRPF) can mitigate spoofed IP packets. When this feature is enabled on an interface, as packets enter that interface the router spends an extra moment considering the source address of the packet. It then considers its own routing table, and if the routing table does not agree that the interface that just received this packet is also the best egress interface to use for forwarding to the source address of the packet, it then denies the packet. QUESTION 239 The NAT traversal definition: A. Pending Answer: AExplanation:NAT-T (NAT Traversal)If both peers support NAT-T, and if they detect that they are connecting to each other through a Network Address Translation (NAT) device (translation is happening), they may negotiate that they want to put a fake UDP port 4500 header on each IPsec packet (before the ESP header) to survive a NAT device that otherwise may have a problem tracking an ESP session (Layer 4 protocol 50). https://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec QUESTION 240Man-in-the-middle attack definition: A. Pending Answer: AExplanation:Man-in-the-middle attacks: Someone or something is between the two devices who believe they are communicating directly with each other. The "man in the middle" may be eavesdropping or actively changing the data that is being sent between the two parties. You can prevent this by implementing Layer 2 dynamic ARP inspection (DAI) and Spanning Tree Protocol (STP) guards to protect spanning tree. You can implement it at Layer 3 by using routing protocol authentication. Authentication of peers in a VPN is also a method of preventing this type of attack. Lead2pass offers the latest 210-260 PDF and VCE dumps with new version VCE player for free download, and the new 210-260 dump ensures your exam 100% pass. 210-260 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDYUk3WWFWOEhsSU0 2017 Cisco 210-260 exam dumps (All 362 Q&As) from Lead2pass: https://www.lead2pass.com/210-260.html [100% Exam Pass Guaranteed]