[PDF&VCE Lead2pass Latest Cisco 210-260 Exam Questions Free Downloading (131-140)

2016 September Cisco Official New Released **210-260** Dumps in Lead2pass.com!] 100% Free Download! 100% Pass Guaranteed! We are all well aware that a major problem in the IT industry is that there is a lack of quality study materials. Our exam preparation material provides you everything you will need to take a certification examination. Our Cisco 210-260 Exam will provide you with exam questions with verified answers that reflect the actual exam. These questions and answers provide you with the experience of taking the actual test. High quality and value for the 210-260 Exam. 100% guarantee to pass your Cisco 210-260 exam and get your Cisco certification. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/210-260.html QUESTION 131 Which three statements about Cisco host-based IPS solution are true? (Choose three) A. It work with deployed firewalls. B. It can be deployed at the perimeter C. It uses signature-based policies D. It can have more restrictive policies than network-based IPS E. It can generate alerts based on behavior at the desktop level F. It can view encrypted filesAnswer: DEF Explanation: The key word here is 'Cisco', and Cisco's host-based IPS, CSA, is NOT signature-based and CAN view encrypted files. QUESTION 132 What are two users of SIEM software? (Choose two) A. performing automatic network audits B. configuring firewall and IDS devices C. alerting administrators to security events in real time D. scanning emails for suspicious attachments E. collecting and archiving syslog data Answer: CE Explanation: The other choices are not functions of SIEM software. QUESTION 133 If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet? A. the ASA will apply the actions from only the last matching class maps it finds for the feature type. B. the ASA will apply the actions from all matching class maps it finds for the feature type. C. the ASA will apply the actions from only the most specific matching class map it finds for the feature type. D. the ASA will apply the actions from only the first matching class maps it finds for the feature type Answer: D Explanation: If it matches a class map for a given feature type, it will NOT attempt to match to any subsequent class maps. QUESTION 134 What statement provides the best definition of malware? A. Malware is tools and applications that remove unwanted programs. B. Malware is a software used by nation states to commit cyber-crimes. C. Malware is unwanted software that is harmful or destructive D. Malware is a collection of worms, viruses and Trojan horses that is distributed as a single..... Answer: C QUESTION 135 Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What are two possible types of attacks your team discovered? A. social activism B. advanced persistent threat C. drive-by spyware D. targeted malware Answer: B Explanation: If required 2 answers in the real exam, please choose BD. QUESTION 136 Which FirePOWER preprocessor engine is used to prevent SYN attacks? A. Anomaly. B. Rate-Based Prevention C. Portscan Detection D. Inline Normalization Answer: B QUESTION 137 What is the only permitted operation for processing multicast traffic on zone-based firewalls? A. Stateful inspection of multicast traffic is supported only for the self-zone. B. Stateful inspection of multicast traffic is supported only between the self-zone and the internal zone. C. Only control plane policing can protect the control plane against multicast traffic. D. Stateful inspection of multicast traffic is supported only for the internal zone Answer: C Explanation: Stateful inspection of multicast traffic is NOT supported by Cisco Zone based firewalls OR Cisco Classic firewall. QUESTION 138 Which of encryption technology has the broadcast platform support to protect operating systems? A. Middleware B. Hardware C. software D. file-level Answer: C QUESTION 139 Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attack? A. holistic understanding of threats B. graymail management and filtering C. signature-based IPS D. contextual analysis Answer: D QUESTION 140 Which Sourfire secure action should you choose if you want to block only malicious traffic from a particular end-user? A. Trust B. Block C. Allow without inspection D. Monitor E. Allow with inspection Answer: E Explanation: Allow with Inspection allows all traffic except for malicious traffic from a particular end-user. The other options are too restrictive, too permissive, or don't exist. The Cisco 210-260 questions and answers in PDF on Lead2pass are the most reliable study guide for 210-260 exam. Comparing with others', our 210-260 dump is more authoritative and complete. We provide the latest full version of 210-260 PDF and VCE dumps with new real questions and answers to ensure your 210-260 exam 100% pass. **210-260** new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLWhBVC0zekJKUUU **2016 Cisco 210-260** exam dumps (All 193 Q&As) from Lead2pass: http://www.lead2pass.com/210-260.html [100% Exam Pass Guaranteed]