[Feb-2016 Dumps Download Free 210-260 Study Guide With VCE Dumps Collection

New Updated 210-260 Exam Questions from PassLeader 210-260 PDF dumps! Welcome to download the newest PassLeader 210-260 VCE dumps: **http://www.passleader.com/210-260.html** (185 Q&As) Keywords: 210-260 exam dumps, 210-260 exam questions, 210-260 VCE dumps, 210-260 PDF dumps, 210-260 practice tests, 210-260 study guide, 210-260 braindumps, CCNA Security -- Implementing Cisco Network Security Exam **NEW 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 files **Answer: DEF Explanation:** The key word here is 'Cisco', and Cisco's host-based IPS, CSA, is NOT signature-based and CAN view encrypted files. **NEW 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. **NEW 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. **NEW 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 NEW QUESTION 135** What command can you use to verify the binding table status? A.   show ip dhcp snooping statistics B.   show ip dhcp snooping database C.   show ip dhcp snooping binding D.   show ip dhcp pool E.   show ip dhcp snooping F.   show ip dhcp source binding **Answer: B NEW 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 NEW 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. **NEW 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: D 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. **NEW 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 NEW 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. **NEW QUESTION 141** ..... Download the newest PassLeader 210-260 dumps from passleader.com now! 100% Pass Guarantee! 210-260 PDF dumps & 210-260 VCE dumps: **http://www.passleader.com/210-260.html** (185 Q&As)