[2017 New 2017 Updated Lead2pass Cisco 210-260 Exam Questions (121-140)

2017 July Cisco Official New Released 210-260 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Are you worring about the 210-260 exam? With the complete collection of 210-260 exam questions and answers, Lead2pass has assembled to take you through your 210-260 exam preparation. Each Q & A set will test your existing knowledge of 210-260 fundamentals, and offer you the latest training products that guarantee you passing 210-260 exam easily. **Following questions and answers are all new published by Cisco Official Exam Center:** https://www.lead2pass.com/210-260.html QUESTION 121Which statement correctly describes the function of a private VLAN? A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomainsB. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomainsC. A private VLAN enables the creation of multiple VLANs using one broadcast domain D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain Answer: A QUESTION 122Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path? A. Unidirectional Link DetectionB. Unicast Reverse Path ForwardingC. TrustSecD. IP Source Guard Answer: B QUESTION 123What is the most common Cisco Discovery Protocol version 1 attack? A. Denial of ServiceB. MAC-address spoofingC. CAM-table overflowD. VLAN hopping Answer: A QUESTION 124What is the Cisco preferred countermeasure to mitigate CAM overflows? A. Port securityB. Dynamic port securityC. IP source guardD. Root guard Answer: B QUESTION 125When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops? A. STP elects the root bridgeB. STP selects the root portC. STP selects the designated portD. STP blocks one of the ports Answer: A QUESTION 126Which countermeasures can mitigate ARP spoofing attacks? (Choose two.) A. Port securityB. DHCP snoopingC. IP source guardD. Dynamic ARP inspection Answer: BD QUESTION 127Which of the following statements about access lists are true? (Choose three.) A. Extended access lists should be placed as near as possible to the destinationB. Extended access lists should be placed as near as possible to the sourceC. Standard access lists should be placed as near as possible to the destinationD. Standard access lists should be placed as near as possible to the sourceE. Standard access lists filter on the source addressF. Standard access lists filter on the destination address Answer: BCE QUESTION 128In which stage of an attack does the attacker discover devices on a target network? A. ReconnaissanceB. Covering tracksC. Gaining accessD. Maintaining access Answer: A QUESTION 129Which type of security control is defense in depth? A. Threat mitigationB. Risk analysisC. Botnet mitigationD. Overt and covert channels Answer: A QUESTION 130On which Cisco Configuration Professional screen do you enable AAA? A. AAA SummaryB. AAA Servers and GroupsC. Authentication PoliciesD. Authorization Policies Answer: A QUESTION 131Which 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 perimeterC. It uses signature-based policiesD. It can have more restrictive policies than network-based IPSE. It can generate alerts based on behavior at the desktop levelF. It can view encrypted files Answer: DEFExplanation:The key word here is 'Cisco', and Cisco's host-based IPS, CSA, is NOT signature-based and CAN view encrypted files. QUESTION 132What are two users of SIEM software? (Choose two) A. performing automatic network auditsB. configuring firewall and IDS devicesC. alerting administrators to security events in real timeD. scanning emails for suspicious attachmentsE. collecting and archiving syslog data Answer: CEExplanation:The other choices are not functions of SIEM software. QUESTION 133If 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: DExplanation:If it matches a class map for a given feature type, it will NOT attempt to match to any subsequent class maps. QUESTION 134What 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 destructiveD. Malware is a collection of worms, viruses and Trojan horses that is distributed as a single..... Answer: C QUESTION 135Your 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 activismB. advanced persistent threatC. drive-by spywareD. targeted malware Answer: BExplanation:If required 2 answers in the real exam, please choose BD. QUESTION 136Which FirePOWER preprocessor engine is used to prevent SYN attacks? A. Anomaly.B. Rate-Based PreventionC. Portscan DetectionD. Inline Normalization Answer: B QUESTION 137What 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: CExplanation:Stateful inspection of multicast traffic is NOT supported by Cisco Zone based firewalls OR Cisco Classic firewall. QUESTION 138Which of encryption technology has the broadcast platform support to protect operating systems? A. MiddlewareB. HardwareC. softwareD. file-level Answer: C QUESTION 139Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attack? A. holistic understanding of threatsB. graymail management and filteringC. signature-based IPSD. contextual analysis Answer: D QUESTION 140Which Sourfire secure action should you choose if you want to block only malicious traffic from a particular end-user? A. TrustB. BlockC. Allow without inspectionD. MonitorE. Allow with inspection Answer: EExplanation: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. At Lead2pass, we are positive that our Cisco 210-260 dumps with questions and answers PDF provide most in-depth solutions for individuals that are preparing for the Cisco 210-260 exam. Our updated 210-260 braindumps will allow you the opportunity to know exactly what to expect on the exam day and ensure that you can pass the exam beyond any doubt. **210-260 new questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDRVJLdVdkMjFoQVk 2017 Cisco 210-260 exam dumps (All 265 Q&As) from Lead2pass: https://www.lead2pass.com/210-260.html **[100% Exam Pass Guaranteed**