[2017-Oct.-New100% Valid 210-260 VCE Dumps 362Q Provided by Braindump2go[123-135

2017 Oct New 210-260 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 210-250 Questions:
1.|2017 New 210-260 Exam Dumps (PDF & VCE) 362Q&As Download:https://www.braindump2go.com/210-260.html 2.|2017 New 210-260 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNV1RGaFJYZkxGWFk?usp=sharing 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 129 Which 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. !!!RECOMMEND!!! 1.|2017 New 210-260 Exam Dumps (PDF & VCE) 362Q&As Download:https://www.braindump2go.com/210-260.html 2.|2017 New 210-260 Study Guide Video: YouTube Video: YouTube.com/watch?v=9yy5IlptXYw