Free Share Lead2pass Cisco 500-285 PDF Dumps with New Update Exam Questions

With Lead2pass complete study guide for the Cisco 500-285 Certification exam you will find questions and answers from previous exams as well as ones that our experts believe will be on the upcoming exams due to upgrades and new releases. This gives you the resources you actually need to pass the exam instead of just studying material without any knowledge of what might be on a test. If you want a career in the IT world, a certification is the only answer to ensure you get your dream job. QUESTION 1 Which option is true of the Packet Information portion of the Packet View screen? A.&#160;&#160;&#160; provides a table view of events B.&#160;&#160;&#160; allows you to download a PCAP formatted file of the session that triggered the event C.&#160;&#160;&#160; displays packet data in a format based on TCP/IP layers D.&#160;&#160;&#160; shows you the user that triggered the eventAnswer: C QUESTION 2 Which option is used to implement suppression in the Rule Management user interface? A.&#160;&#160;&#160; Rule Category B.&#160;&#160;&#160; Global C.&#160;&#160;&#160; Source D.&#160;&#160;&#160; Protocol Answer: C QUESTION 3 When you are editing an intrusion policy, how do you know that you have changes? A.&#160;&#160;&#160; The Commit Changes button is enabled. B.&#160;&#160;&#160; A system message notifies you. C.&#160;&#160;&#160; You are prompted to save your changes on every screen refresh. D.&#160;&#160;&#160; A yellow, triangular icon displays next to the Policy Information option in the navigation panel. Answer: D QUESTION 4 FireSIGHT recommendations appear in which layer of the Policy Layers page? A.&#160;&#160;&#160; Layer Summary B.&#160;&#160;&#160; User Layers C.&#160;&#160;&#160; Built-In Layers D.&#160;&#160;&#160; FireSIGHT recommendations do not show up as a layer. Answer: C QUESTION 5 Host criticality is an example of which option? A.&#160;&#160;&#160; a default whitelist B.&#160;&#160;&#160; a default traffic profile C.&#160;&#160;&#160; a host attribute D.&#160;&#160;&#160; a correlation policy Answer: C QUESTION 6 FireSIGHT uses three primary types of detection to understand the environment in which it is deployed. Which option is one of the detection types? A.&#160;&#160;&#160; protocol layer B.&#160;&#160;&#160; application C.&#160;&#160;&#160; objects D.&#160;&#160;&#160; devices Answer: B QUESTION 7 When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery? A.&#160;&#160;&#160; host B.&#160;&#160;&#160; IPS event C.&#160;&#160;&#160; anti-malware D.&#160;&#160;&#160; networks Answer: A QUESTION 8 Which option is derived from the discovery component of FireSIGHT technology? A.&#160;&#160;&#160; connection event table view B.&#160;&#160;&#160; network profile C.&#160;&#160;&#160; host profile Answer: C QUESTION 9 The IP address ::/0 is equivalent to which IPv4 address and netmask? A.&#160;&#160;&#160; 0.0.0.0 B.&#160;&#160;&#160; 0.0.0.0/0 C.&#160;&#160;&#160; 0.0.0.0/24 D.&#160;&#160;&#160; The IP address ::/0 is not valid IPv6 syntax. Answer: B The Cisco 500-285 practice test Materials is designed to offer the user a unique experience to evaluate their knowledge and understanding of the concepts to be tested in the 500-285 actual exam. The Cisco 500-285 practice test Materials can be downloaded easily from Lead2pass. Lead2pass makes your exam much easier. We ensure 100% pass rate. http://www.lead2pass.com/500-285.html