[Full Version Offering New 500-285 Exam PDF And 500-285 Exam VCE Dumps For Free Downloading (11-20)

2017 February Cisco Official New Released 500-285 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! I have already passed Cisco 500-285 certification exam today! Scored 989/1000 in Australia. SO MANY new added exam questions which made me headache?.. Anyway, I finally passed 500-285 exam with the help of Lead2pass! Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/500-285.html QUESTION 11 Which one of the following statements is true regarding tuned signatures? A.   require that you create subsignatures that can then be tuned to your needs B.   require that you create custom signatures that can then be tuned to your needs C.   contain modified parameters of built-in signatures D.   begin with signature number 60000 E.   are tuned using the Cisco IDM Custom Signature WizardAnswer: C QUESTION 12 Which TCP stream reassembly mode disables TCP window-evasion checking? A.   Loose B.   Strict C.   Asymmetric D.   Symmetric E.   Disable Answer: C QUESTION 13 Which three values are used to calculate the risk rating for an event? (Choose three.) A.   attack severity rating B.   fidelity severity rating C.   target fidelity rating D.   target value rating E.   signature fidelity rating F.   signature attack rating Answer: ADE QUESTION 14 A context box opens when you click on an event icon in the Network File Trajectory map for a file. Which option is an element of the box? A.   Scan B.   Application Protocol C.   Threat Name D.   File Name Answer: B QUESTION 15 Which policy controls malware blocking configuration? A.   file policy B.   malware policy C.   access control policy D.   IPS policy Answer: A QUESTION 16 Which statement is true regarding malware blocking over HTTP? A.   It can be done only in the download direction. B.   It can be done only in the upload direction. C.   It can be done in both the download and upload direction. D.   HTTP is not a supported protocol for malware blocking. Answer: C QUESTION 17 Which option describes Spero file analysis? A.   a method of analyzing the SHA-256 hash of a file to determine whether a file is malicious or not B.   a method of analyzing the entire contents of a file to determine whether it is malicious or not C.   a method of analyzing certain file characteristics, such as metadata and header information, to determine whether a file is malicious or not D.   a method of analyzing a file by executing it in a sandbox environment and observing its behaviors to determine if it is malicious or not Answer: C QUESTION 18 Which event source can have a default workflow configured? A.   user events B.   discovery events C.   server events D.   connection events Answer: B QUESTION 19 Where do you configure widget properties? A.   dashboard properties B.   the Widget Properties button in the title bar of each widget C.   the Local Configuration page D.   Context Explorer Answer: B QUESTION 20 Which option describes the two basic components of Sourcefire Snort rules? A.   preprocessor configurations to define what to do with packets before the detection engine sees them, and detection engine configurations to define exactly how alerting is to take place B.   a rule statement characterized by the message you configure to appear in the alert, and the rule body that contains all of the matching criteria such as source, destination, and protocol C.   a rule header to define source, destination, and protocol, and the output configuration to determine which form of output to produce if the rule triggers D.   a rule body that contains packet-matching criteria or options to define where to look for content in a packet, and a rule header to define matching criteria based on where a packet originates, where it is going, and over which protocol Answer: D Lead2pass 500-285 PDF dumps is perfect! Totally! Thanks so much! 500-285 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVFZxRktsQzNaNU0 2017 Cisco 500-285 exam dumps (All 65 Q&As) from Lead2pass: http://www.lead2pass.com/500-285.html [100% Exam Pass Guaranteed]