[Full Version Pass 500-290 Exam By Exercising Lead2pass Latest 500-290 VCE And PDF Dumps (21-30)

2017 February Cisco Official New Released 500-290 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
Are you worring about the 500-290 exam? With the complete collection of 500-290 exam questions and answers, Lead2pass has assembled to take you through your 500-290 exam preparation. Each Q & A set will test your existing knowledge of 500-290 fundamentals, and offer you the latest training products that guarantee you passing 500-290 exam easily. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/500-290.html QUESTION 21 Which option is a remediation module that comes with the Sourcefire System? A.   Cisco IOS Null Route B.   Syslog Route C.   Nmap Route Scan D.   Response GroupAnswer: A QUESTION 22 Which statement represents detection capabilities of the HTTP preprocessor? A.   You can configure it to blacklist known bad web servers. B.   You can configure it to normalize cookies in HTTP headers. C.   You can configure it to normalize image content types. D.   You can configure it to whitelist specific servers. Answer: B QUESTION 23 Which feature of the preprocessor configuration pages lets you quickly jump to a list of the rules associated with the preprocessor that you are configuring? A.   the rule group accordion B.   a filter bar C.   a link below the preprocessor heading D.   a button next to each preprocessor option that has a corresponding rule Answer: C QUESTION 24 Suppose an administrator is configuring an IPS policy and attempts to enable intrusion rules that require the operation of the TCP stream preprocessor, but the TCP stream preprocessor is turned off. Which statement is true in this situation? A.   The administrator can save the IPS policy with the TCP stream preprocessor turned off, but the rules requiring its operation will not function properly. B.   When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the TCP stream preprocessor will be turned on for the IPS policy. C.   The administrator will be prevented from changing the rule state of the rules that require the TCP stream preprocessor until the TCP stream preprocessor is enabled. D.   When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the rules that require the TCP stream preprocessor will be turned off for the IPS policy. Answer: B QUESTION 25 Controlling simultaneous connections is a feature of which type of preprocessor? A.   rate-based attack prevention B.   detection enhancement C.   TCP and network layer preprocessors D.   performance settings Answer: A QUESTION 26 A one-to-many type of scan, in which an attacker uses a single host to scan a single port on multiple target hosts, indicates which port scan type? A.   port scan B.   portsweep C.   decoy port scan D.   ACK scan Answer: B QUESTION 27 What does packet latency thresholding measure? A.   the total elapsed time it takes to process a packet B.   the amount of time it takes for a rule to process C.   the amount of time it takes to process an event D.   the time span between a triggered event and when the packet is dropped Answer: A QUESTION 28 What are the two categories of variables that you can configure in Object Management? A.   System Default Variables and FireSIGHT-Specific Variables B.   System Default Variables and Procedural Variables C.   Default Variables and Custom Variables D.   Policy-Specific Variables and Procedural Variables Answer: C QUESTION 29 Which option is true regarding the $HOME_NET variable? A.   is a policy-level variable B.   has a default value of "all" C.   defines the network the active policy protects D.   is used by all rules to define the internal network Answer: C QUESTION 30 Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence? A.   subscribe to a URL intelligence feed B.   subscribe to a VRT C.   upload a list that you create D.   automatically upload lists from a network share Answer: C At Lead2pass, we are positive that our Cisco 500-290 dumps with questions and answers PDF provide most in-depth solutions for individuals that are preparing for the Cisco 500-290 exam. Our updated 500-290 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. 500-290 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDbVYtOTNZU0FUYTQ 2017 Cisco 500-290 exam dumps (All 70 Q&As) from Lead2pass: http://www.lead2pass.com/500-290.html [100% Exam Pass Guaranteed]