[Full Version Ensure Pass 500-285 Exam With Lead2pass New 500-285 Brain Dumps (21-30)

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 yesterday?.Scored 984/1000 in US! Many new exam questions added into the 2017 500-285 test! So I just come here to share with your guys and wish more 500-285 candidates can pass easily! Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/500-285.html QUESTION 21 Which option is a valid whitelist evaluation value? A. pending B. violation C. semi-compliant D. not-evaluatedAnswer: D QUESTION 22 Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations? A. logging to database, SMS, SMTP, and SNMP B. logging to database, SMTP, SNMP, and PCAP C. logging to database, SNMP, syslog, and email D. logging to database, PCAP, SMS, and SNMP Answer: C QUESTION 23 Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule? A. testing password strength when accessing an application B. limiting general user access to administrative file shares C. enforcing two-factor authentication for access to critical servers D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one Answer: D QUESTION 24 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 Group Answer: A QUESTION 25 What does the whitelist attribute value "not evaluated" indicate? A. The host is not a target of the whitelist. B. The host could not be evaluated because no profile exists for it. C. The whitelist status could not be updated because the correlation policy it belongs to is not enabled. D. The host is not on a monitored network segment. Answer: A QUESTION 26 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 27 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 28 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 29 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 30 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 Pass 500-285 is not difficult! But you need more practice tests, I spent 1 month prepared for this exam! Here is full version of the exam dump, I want to share with you, maybe it can help you a little bit: 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]