[Dec-2018Exam 210-250 PDF and VCE 152Q Free Offered by Braindump2go[Q110-120

Dec/2018 Braindump2go 210-250 Exam Dumps with PDF and VCE New Updated Today! Following are some new 210-250 Real Exam Questions:1.|2018 Latest 210-250 Exam Dumps (PDF & VCE) 152Q Download:https://www.braindump2go.com/210-250.html2.|2018 Latest 210-250 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNekdxX05OVnFXRXc?usp=sharingQUESTION 110Netflow uses which format?A. base 10B. ASCIIC. BinaryD. HexadecimalAnswer: CExplanation: QUESTION 111A zombie process occurs when which of the following happens?A. A process holds its associated memory and resources but is released from the entry table.B. A process continues to run on its own.C. A process holds on to associate memory but releases resources.D. A process releases the associated memory and resources but remains in the entry table.Answer: DExplanation: QUESTION 111A zombie process occurs when which of the following happens?A. A process holds its associated memory and resources but is released from the entry table.B. A process continues to run on its own.C. A process holds on to associate memory but releases resources.D. A process releases the associated memory and resources but remains in the entry table.Answer: DExplanation: QUESTION 112Early versions of the Microsoft PPTP virtual private network software used the same RC4 key for the sender and the receiver. Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?A. forgery attackB. meet-in-the-middle attackC. ciphertext-only attackD. plaintext-only attackAnswer: CExplanation:Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions solved this problem but may still have other problems). In any case where a stream cipher like RC4 is used twice with the same key, it is open to ciphertext-only attack.QUESTION 113How does NTP help with security monitoring?A. It synchronizes the time of day so that you can correlate events when you receive system logs.B. It enables you to look up the IP addresses a browser navigated to using the FQON.C. It allows you receive system-generated email traffic from log servers.D. It uses TCP, which allows you to see the HTTP conversations between servers and clients.**Answer: A**QUESTION 114Which hash algorithm is cryptography used in certificate generation?A. SHA-256B. MD5C. RSA 4096D. SHA-512**Answer: B**QUESTION 115 Which description is an example of whaling?A. when attackers use fraudulent websites that look like legitimate onesB. when attackers go after the CEO C. when attackers target specific individualsD. when attackers target a group of individuals**Answer: B**QUESTION 116Which tool provides universal query access to text based data such as event logs and file system?A. service viewerB. log parserC. handlesD. Windows Management InstrumentationAnswer: BExplanation:Log parser is a powerful, versatile tool that provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows?operating system such as the Event Log, the Registry, the file system, and Active Directory?QUESTION 117You have deployed an enterprise-wide host/endpoint technology for all of the company corporate PCs. Management asks you to block a selected set of applications on all corporate PCs. Which technology is the best option?A. antivirus/antispyware softwareB. application whitelisting/blacklistingC. host-based IDSD. network NGFW**Answer: B**QUESTION 118What does the sum of the risks presented by an application represent for that application?A. application attack surfaceB. security violationC. vulnerabilityD. HIPPA violation**Answer: A**QUESTION 119The FMC can share HTML, PDF and CSV data types that relate to a specific event type.Which event type?A. hostB. connectionC. intrusionD. NetFlow**Answer: C**QUESTION 120What are two Features of NGFW:A. Data Mining,B. Host Based AVC. Application visibility and controlD. SIEME. IDS**Answer: CE**
!!!RECOMMEND!!!1.|2018 Latest 210-250 Exam Dumps (PDF & VCE) 152Q Download:https://www.braindump2go.com/210-250.html 2.|2018 Latest 210-250 Study Guide Video: YouTube Video: YouTube.com/watch?v=GCdivGceqpY