

## [2017-New-VersionBraindump2go 70Q 210-250 PDF Free Download[31-40

2017 March New 210-250 Exam Dumps and Exam Questions Free Shared Here Today! Free Instant Download [210-250 Exam Dumps \(PDF & VCE\) 70Q&As](#) from [www.Braindump2go.com](http://www.Braindump2go.com) Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1. |NEW 210-250 Exam Dumps (PDF & VCE) 70Q&As Download: <http://www.braindump2go.com/210-250.html> 2. |NEW 210-250 Exam Questions & Answers Download: <https://1drv.ms/f/s!AvI7wzKf6QBjgnzFpAHsSmXP9zrJ> QUESTION 31 Which two options are recognized forms of phishing? (Choose two ) A. spear B. whaling C. mailbomb D. hooking E. mailnet Answer: AB QUESTION 32 While viewing packet capture data, you notice that one IP is sending and receiving traffic for multiple devices by modifying the IP header, Which option is making this behavior possible? A. TOR B. NAT C. encapsulation D. tunneling Answer: A QUESTION 33 Which definition of an antivirus program is true? A. program used to detect and remove unwanted malicious software from the system B. program that provides real time analysis of security alerts generated by network hardware and application C. program that scans a running application for vulnerabilities D. rules that allow network traffic to go in and out Answer: A QUESTION 34 Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IPS phones? A. replay B. man-in-the-middle C. dictionary D. known-plaintext Answer: B QUESTION 35 An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate? A. traffic fragmentation B. resource exhaustion C. timing attack D. tunneling Answer: A QUESTION 36 Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target? A. man in the middle B. denial of service C. distributed denial of service D. replay Answer: D QUESTION 37 In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully? A. ACK B. SYN ACK C. RST D. PSH, ACK Answer: B QUESTION 38 Which definition of a fork in Linux is true? A. daemon to execute scheduled commands B. parent directory name of a file pathname C. macros for manipulating CPU sets D. new process created by a parent process Answer: C QUESTION 39 Which two features must a next generation firewall include? (Choose two.) A. data mining B. host-based antivirus C. application visibility and control D. Security Information and Event Management E. intrusion detection system Answer: DE QUESTION 40 Which encryption algorithm is the strongest? A. AES B. CESC. DES D. 3DES Answer: A !!!RECOMMEND!!! 1. |NEW 210-250 Exam Dumps (PDF & VCE) 70Q&As Download: <http://www.braindump2go.com/210-250.html> 2. |NEW 210-250 Study Guide Video: YouTube Video: [YouTube.com/watch?v=LMVKGDJtwow](https://www.YouTube.com/watch?v=LMVKGDJtwow)