[July-2017-New100% Real 312-50v9 VCE 312-50v9 Exam Dumps 589Q-Braindump2go[51-60

2017 July New 312-50v9 Exam Dumps with PDF and VCE Free Updated in www.Braindump2go.com Today! 1.|2017 New 312-50v9 Exam Dumps (VCE & PDF) 589Q&As Download:https://www.braindump2go.com/312-50v9.html 2.|2017 New 312-50v9 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNWml5eng1ZVh6aHM?usp=sharing QUESTION 51Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service? A. Port scanningB. Banner grabbingC. Injecting arbitrary dataD. Analyzing service response Answer: D QUESTION 52Which of the following business challenges could be solved by using a vulnerability scanner? A. Auditors want to discover if all systems are following a standard naming convention.B. A web server was compromised and management needs to know if any further systems were compromised.C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.D. There is a monthly requirement to test corporate compliance with host application usage and security policies. Answer: D QUESTION 53A security policy will be more accepted by employees if it is consistent and has the support of A. coworkers.B. executive management.C. the security officer.D. a supervisor. Answer: B QUESTION 54A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:- Firewall log files are at the expected value of 4 MB. - The current time is 12am. Exactly two hours later the size has decreased considerably. - Another hour goes by and the log files have shrunk in size again.Which of the following actions should the security administrator take? A. Log the event as suspicious activity and report this behavior to the incident response team immediately.B. Log the event as suspicious activity, call a manager, and report this as soon as possible.C. Run an anti-virus scan because it is likely the system is infected by malware.D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy. Answer: DExplanation: QUESTION 55Which type of scan measures a person's external features through a digital video camera? A. Iris scanB. Retinal scanC. Facial recognition scanD. Signature kinetics scan Answer: C QUESTION 56WPA2 uses AES for wireless data encryption at which of the following encryption levels? A. 64 bit and CCMPB. 128 bit and CRCC. 128 bit and CCMPD. 128 bit and TKIP Answer: C QUESTION 57An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel? A. ClassifiedB. OvertC. EncryptedD. Covert Answer: D QUESTION 58What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack? A. Injecting parameters into a connection string using semicolons as a separatorB. Inserting malicious Javascript code into input parametersC. Setting a user's session identifier (SID) to an explicit known valueD. Adding multiple parameters with the same name in HTTP requests Answer: A QUESTION 59A newly discovered flaw in a software application would be considered which kind of security vulnerability? A. Input validation flawB. HTTP header injection vulnerabilityC. 0-day vulnerabilityD. Time-to-check to time-to-use flaw Answer: C QUESTION 60During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability? A. The web application does not have the secure flag set.B. The session cookies do not have the HttpOnly flag set.C. The victim user should not have an endpoint security solution.D. The victim's browser must have ActiveX technology enabled. Answer: B QUESTION 61The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities? A. An attacker, working slowly enough, can evade detection by the IDS.B. Network packets are dropped if the volume exceeds the threshold.C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.D. The IDS will not distinguish among packets originating from different sources. Answer: A QUESTION 62What is the main advantage that a network-based IDS/IPS system has over a host-based solution? A. They do not use host system resources.B. They are placed at the boundary, allowing them to inspect all traffic.C. They are easier to install and configure.D. They will not interfere with user interfaces. Answer: A QUESTION 63The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data? A. AsymmetricB. ConfidentialC. SymmetricD. Non-confidential Answer: A QUESTION 64When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following? A. Drops the packet and moves on to the next oneB. Continues to evaluate the packet until all rules are checkedC. Stops checking rules, sends an alert, and lets the packet continueD. Blocks the connection with the source IP address in the packet Answer: B QUESTION 65Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them? A. DetectiveB. PassiveC. IntuitiveD. Reactive Answer: B QUESTION 66An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control

packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets? A. The wireless card was not turned on.B. The wrong network card drivers were in use by Wireshark.C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.D. Certain operating systems and adapters do not collect the management or control packets. Answer: D QUESTION 67From the two screenshots below, which of the following is occurring?First one:1 [10.0.0.253]# nmap -sP 10.0.0.0/243 Starting Nmap5 Host 10.0.0.1 appears to be up.6 MAC Address: 00:09:5B:29:FD:96 (Netgear) 7 Host 10.0.0.2 appears to be up.8 MAC Address: 00:0F:B5:96:38:5D (Netgear)9 Host 10.0.0.4 appears to be up.10 Host 10.0.0.5 appears to be up.11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.) 12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399 secondsSecond one:1 [10.0.0.252]# nmap -sO 10.0.0.23 Starting Nmap 4.01 at 2006-07-14 12:56 BST4 Interesting protocols on 10.0.0.2:5 (The 251 protocols scanned but not shown below are6 in state: closed)7 PROTOCOL STATE SERVICE8 1 open icmp9 2 open|filtered igmp10 6 open tcp11 17 open udp12 255 open|filtered unknown14 Nmap finished: 1 IP address (1 host up) scanned in15 1.259 seconds1 [10.0.0.253]# nmap -sP 1 [10.0.0.253]# nmap -sP A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2. Answer: AExplanation: QUESTION 68Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations? A. CainB. John the RipperC. NiktoD. Hping Answer: A QUESTION 69Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common? A. They are written in Java.B. They send alerts to security monitors.C. They use the same packet analysis engine.D. They use the same packet capture utility. Answer: D !!!RECOMMEND!!! 1.|2017 New 312-50v9 Exam Dumps (VCE & PDF) 589Q&As Download:https://www.braindump2go.com/312-50v9.html 2.|2017 New 312-50v9 Study Guide Video: YouTube Video: YouTube.com/watch?v=U8B7_OOPx00