[2017 PDF&VCE Lead2pass 2017 100% Real 312-50v9 Exam Questions (101-120)

Lead2pass 2017 August New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Pass 312-50v9 exam with the latest Lead2pass 312-50v9 dumps: Lead2pass 312-50v9 exam questions and answers in PDF are prepared by our experts. Moreover, they are based on the recommended syllabus that covering all the 312-50v9 exam objectives. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 101What statement is true regarding LM hashes? A. LM hashes consist in 48 hexadecimal characters.B. LM hashes are based on AES128 cryptographic standard.C. Uppercase characters in the password are converted to lowercase.D. LM hashes are not generated when the password length exceeds 15 characters.Answer: D QUESTION 102A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field? A. if (billingAddress = 50) {update field} else exitB. if (billingAddress != 50) {update field} else exitC. if (billingAddress >= 50) {update field} else exitD. if (billingAddress <= 50) {update field} else exit Answer: D QUESTION 103A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field: IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox ("Vulnerable");>" When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable". Which web applications vulnerability did the analyst discover? A. Cross-site request forgeryB. Command injectionC. Cross-site scriptingD. SQL injection Answer: C Explanation: QUESTION 104A security administrator notices that the log file of the company's webserver contains suspicious entries: Based on source code analysis, the analyst concludes that the login.php script is vulnerable to A. command injection.B. SQL injection.C. directory traversal.D. LDAP injection. Answer: B QUESTION 105Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions? A. FirewallB. HoneypotC. Core serverD. Layer 4 switch Answer: B QUESTION 106Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools? A. ping 192.168.2.B. ping 192.168.2.255C. for %V in (1 1 255) do PING 192.168.2.%VD. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply" Answer: D QUESTION 107What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'? A. A stealth scan, opening port 123 and 153B. A stealth scan, checking open ports 123 to 153C. A stealth scan, checking all open ports excluding ports 123 to 153D. A stealth scan, determine operating system, and scanning ports 123 to 153 Answer: D QUESTION 108Which of the following parameters enables NMAP's operating system detection feature? A. NMAP -sVB. NMAP -oSC. NMAP -sRD. NMAP -O Answer: D QUESTION 109Which of the following open source tools would be the best choice to scan a network for potential targets? A. NMAPB. NIKTOC. CAIND. John the Ripper Answer: A QUESTION 110A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use? A. -sOB. -sPC. -sSD. -sU Answer: B QUESTION 111A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network? A. FraggleB. MAC FloodC. SmurfD. Tear Drop Answer: B QUESTION 112Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity? A. Netstat WMI ScanB. Silent DependenciesC. Consider unscanned ports as closedD. Reduce parallel connections on congestion Answer: D QUESTION 113How does an operating system protect the passwords used for account logins? A. The operating system performs a one-way hash of the passwords.B. The operating system stores the passwords in a secret file that users cannot find.C. The operating system encrypts the passwords, and decrypts them when needed.D. The operating system stores all passwords in a protected segment of non-volatile memory. Answer: A QUESTION 114Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run? A. Cavity virusB. Polymorphic virusC. Tunneling virusD. Stealth virus Answer: D QUESTION 115An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price? A. By using SQL injectionB. By changing hidden form valuesC. By using cross site scriptingD. By utilizing a buffer overflow attack Answer: B QUESTION 116Which tool can be used to silently copy files from USB devices? A. USB GrabberB. USB DumperC. USB SnifferD. USB Snoopy Answer: B

QUESTION 117Which of the following is used to indicate a single-line comment in structured query language (SQL)? A. --B. || C. %%D. " Answer: A QUESTION 118A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command: NMAP -n -sS -P0 -p 80 ***.***.**.** What type of scan is this? A. Quick scanB. Intense scanC. Stealth scanD. Comprehensive scan Answer: CExplanation: QUESTION 119What is the broadcast address for the subnet 190.86.168.0/22? A. 190.86.168.255B. 190.86.255.255C. 190.86.171.255D. 190.86.169.255 Answer: C QUESTION 120A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users? A. Perform a dictionary attack.B. Perform a brute force attack.C. Perform an attack with a rainbow table.D. Perform a hybrid attack. Answer: C More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Comparing with others', you will find our 312-50v9 exam questions are more helpful and precise since all the 312-50v9 exam content is regularly updated and has been checked for accuracy by our team of EC-Council expert professionals. 2017 EC-Council 312-50v9 (All 589 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/312-50v9.html [100% Exam Pass Guaranteed]