[Full Version Easily Pass 312-50v9 Exam With Lead2pass Updated EC-Council 312-50v9 Dumps (36-50)

2017 March EC-Council Official New Released 312-50v9 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass 312-50v9 braindumps including the exam questions and the answer, completed by our senior IT lecturers and the EC-Council product experts, include the current newest 312-50v9 exam questions. Following questions and answers are all new published by EC-Council Official Exam Center: http://www.lead2pass.com/312-50v9.html QUESTION 36 Which of the following processes evaluates the adherence of an organization to its stated security policy? A.   Vulnerability assessment B.   Penetration testing C.   Risk assessment D.   Security auditingAnswer: D QUESTION 37 A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result? A.   The consultant will ask for money on the bid because of great work. B.   The consultant may expose vulnerabilities of other companies. C.   The company accepting bids will want the same type of format of testing. D.   The company accepting bids will hire the consultant because of the great work performed. Answer: B QUESTION 38 Which type of scan is used on the eye to measure the layer of blood vessels? A.   Facial recognition scan B.   Retinal scan C.   Iris scan D.   Signature kinetics scan Answer: B QUESTION 39 What is the main reason the use of a stored biometric is vulnerable to an attack? A.   The digital representation of the biometric might not be unique, even if the physical characteristic is unique. B.   Authentication using a stored biometric compares a copy to a copy instead of the original to a copy. C.   A stored biometric is no longer "something you are" and instead becomes "something you have". D.   A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric. Answer: D QUESTION 40 During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key? A.   The tester must capture the WPA2 authentication handshake and then crack it. B.   The tester must use the tool inSSIDer to crack it using the ESSID of the network. C.   The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard. D.   The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key. Answer: A QUESTION 41 Which type of antenna is used in wireless communication? A.   Omnidirectional B.   Parabolic C.   Uni-directional D.   Bi-directional Answer: A QUESTION 42 What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation? A.   Blue Book B.   ISO 26029 C.   Common Criteria D.   The Wassenaar Agreement Answer: C QUESTION 43 One way to defeat a multi-level security solution is to leak data via A.   a bypass regulator. B.   steganography. C.   a covert channel. D.   asymmetric routing. Answer: C QUESTION 44 Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application? A.   The victim user must open the malicious link with an Internet Explorer prior to version 8. B.   The session cookies generated by the application do not have the HttpOnly flag set. C.   The victim user must open the malicious link with a Firefox prior to version 3. D.   The web application should not use random tokens. Answer: D QUESTION 45 What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability? A.   The request to the web server is not visible to the administrator of the vulnerable application. B.   The attack is called "Blind" because, although the application properly filters user input, it is still vulnerable to code injection. C.   The successful attack does not show an error message to the administrator of the affected application. D.   The vulnerable application does not display errors with information about the injection results to the attacker. Answer: D QUESTION 46 During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system? A.   Using the Metasploit psexec module setting the SA / Admin credential B.   Invoking the stored procedure xp_shell to spawn a Windows command shell C.   Invoking the stored procedure cmd_shell to spawn a Windows command shell D.   Invoking the stored procedure xp_cmdshell to spawn a Windows command

shell Answer: D QUESTION 47 The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control? A.   Physical B.   Procedural C.   Technical D.   Compliance Answer: B QUESTION 48 A pentester gains access to a Windows application server and needs to determine the settings of the built- in Windows firewall. Which command would be used? A.   Netsh firewall show config B.   WMIC firewall show config C.   Net firewall show config D.   Ipconfig firewall show config Answer: A QUESTION 49 In the software security development life cycle process, threat modeling occurs in which phase? A.   Design B.   Requirements C.   Verification D.   Implementation Answer: A QUESTION 50 A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation? A.   True negatives B.   False negatives C.   True positives D.   False positives Answer: D If you use Lead2pass braindump as your 312-50v9 exam prepare material, we guarantee your success in the first attempt. Lead2pass 312-50v9 dump provides you everything you will need to take your 312-50v9 Exam. EC-Council 312-50v9 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDSHZpNDRNRXpLekE 2017 **EC-Council 312-50v9** exam dumps (All 589 Q&As) from Lead2pass: http://www.lead2pass.com/312-50v9.html [100% Exam Pass Guaranteed]