# [2017 PDF&VCE Lead2pass 2017 100% Real 312-50v9 Exam Questions (81-100)

Lead2pass 2017 August New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass provides 100% pass 312-50v9 exam questions and answers for your EC-Council 312-50v9 exam. We provide EC-Council 312-50v9 exam questions from Lead2pass dumps and answers for the training of 312-50v9 practice test. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 81What is the best defense against privilege escalation vulnerability? A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.B. Run administrator and applications on least privileges and use a content registry for tracking.C. Run services with least privileged accounts and implement multi-factor authentication and authorization.D. Review user roles and administrator privileges for maximum utilization of automation services.Answer: C QUESTION 82How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy? A. Defeating the scanner from detecting any code change at the kernelB. Replacing patch system calls with its own version that hides the rootkit (attacker's) actionsC. Performing common services for the application process and replacing real applications with fake onesD. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/ options Answer: D QUESTION 83Which of the following items of a computer system will an anti-virus program scan for viruses? A. Boot SectorB. Deleted FilesC. Windows Process ListD. Password Protected Files Answer: A QUESTION 84Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall? A. UDP 123B. UDP 541C. UDP 514D. UDP 415 Answer: C QUESTION 85A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit? A. Issue the pivot exploit and set the meterpreter.B. Reconfigure the network settings in the meterpreter.C. Set the payload to propagate through the meterpreter.D. Create a route statement in the meterpreter. Answer: D QUESTION 86What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"? A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43. Answer: B QUESTION 87Which of the following is a client-server tool utilized to evade firewall inspection? A. tcp-over-dnsB. kismetC. niktoD. hping Answer: A QUESTION 88 Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker? A. DataThiefB. NetCatC. Cain and AbelD. SQLInjector Answer: A QUESTION 89A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request? A. SemicolonB. Single quoteC. Exclamation markD. Double quote Answer: B QUESTION 90Which of the following identifies the three modes in which Snort can be configured to run? A. Sniffer, Packet Logger, and Network Intrusion Detection SystemB. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection SystemC. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention SystemD. Sniffer, Packet Logger, and Host Intrusion Prevention System Answer: A QUESTION 91When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire? A. Network tapB. Layer 3 switchC. Network bridgeD. Application firewall Answer: A QUESTION 92Which of the following programming languages is most vulnerable to buffer overflow attacks? A. Perl B. C++C. PythonD. Java Answer: B QUESTION 93Smart cards use which protocol to transfer the certificate in a secure manner? A. Extensible Authentication Protocol (EAP)B. Point to Point Protocol (PPP)C. Point to Point Tunneling Protocol (PPTP)D. Layer 2 Tunneling Protocol (L2TP) Answer: A QUESTION 94Which of the following is a hashing algorithm? A. MD5B. PGPC. DESD. ROT13 Answer: A QUESTION 95Which of the following problems can be solved by using Wireshark? A. Tracking version changes of source codeB. Checking creation dates on all webpages on a serverC. Resetting the administrator password on multiple systemsD. Troubleshooting communication resets between two systems Answer: D QUESTION 96What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25? A. tcp.src == 25 and ip.host == 192.168.0.125B. host 192.168.0.125:25C. port 25 and host 192.168.0.125D. tcp.port == 25 and ip.host == 192.168.0.125 Answer: D QUESTION 97Which tool would be used to collect wireless packet data? A. NetStumblerB. John the RipperC. NessusD. Netcat Answer: A QUESTION 98Which of the following is an example of two factor authentication? A. PIN Number and Birth DateB. Username and PasswordC. Digital Certificate and Hardware TokenD. Fingerprint and Smartcard ID Answer: D QUESTION 99Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5? A. 768 bit keyB. 1025 bit keyC. 1536 bit keyD. 2048 bit key Answer: C QUESTION 100After gaining access to the password hashes used to protect

access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application? A. SHA1B. Diffie-HelmanC. RSAD. AES Answer: A More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Lead2pass is the leader in 312-50v9 certification test questions with training materials for EC-Council 312-50v9 exam dumps. Lead2pass EC-Council training tools are constantly being revised and updated. We 100% guarantee EC-Council 312-50v9 exam questions with quality and reliability which will help you pass EC-Council 312-50v9 exam. 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]