[2017 Newest Ensure Pass 312-50v9 Exam By Training Lead2pass New PDF Dumps (241-260)

Lead2pass 2017 September New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! How to 100% pass 312-50v9 exam? Lead2pass provides the guaranteed 312-50v9 exam dumps to boost up your confidence in 312-50v9 exam. Successful candidates have provided their reviews about our 312-50v9 dumps. Now Lead2pass supplying the new version of 312-50v9 VCE and PDF dumps. We ensure our 312-50v9 exam questions are the most complete and authoritative compared with others', which will ensure your 312-50v9 exam pass. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 241To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.What term is commonly used when referring to this type of testing? A. FuzzingB. RandomizingC. MutatingD. BoundingAnswer: AExplanation:Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.https://en.wikipedia.org/wiki/Fuzz_testing QUESTION 242To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit? A. Vulnerability scannerB. Protocol analyzerC. Port scannerD. Intrusion Detection System Answer: AExplanation:A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.
https://en.wikipedia.org/wiki/Vulnerability_scanner QUESTION 243Which of these options is the most secure procedure for storing backup tapes? A. In a climate controlled facility offsiteB. On a different floor in the same buildingC. Inside the data center for faster retrieval in a fireproof safeD. In a cool dry environment Answer: AExplanation:An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.
http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery- strategy QUESTION 244What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed? A. Residual riskB. Inherent riskC. Deferred riskD. Impact risk Answer: AExplanation:The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.https://en.wikipedia.org/wiki/Residual_risk QUESTION 245Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.Which tool can be used to perform session splicing attacks? A. WhiskerB. tcpspliceC. BurpD. Hydra Answer: AExplanation:One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.https://en.wikipedia.org/wiki/
Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets QUESTION 246Which of the following tools can be used for passive OS fingerprinting? A. tcpdumpB. nmapC. pingD. tracert Answer: AExplanation:The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.
http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html QUESTION 247You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring.Which tool would allow you to accomplish this goal? A. Network-based IDSB. FirewallC. ProxyD. Host-based IDS Answer: AExplanation:A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.
https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids QUESTION 248What does a firewall

check to prevent particular ports and applications from getting packets into an organization? A. Transport layer port numbers and application layer headersB. Presentation layer headers and the session layer port numbersC. Network layer headers and the session layer port numbersD. Application layer port numbers and the transport layer headers Answer: AExplanation:Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.
https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters
http://howdoesinternetwork.com/2012/application-layer-firewalls QUESTION 249You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving? A. False NegativeB. False PositiveC. True NegativeD. True Positive Answer: AExplanation:A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.
https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error QUESTION 250Which of the following types of firewalls ensures that the packets are part of the established session? A. Stateful inspection firewallB. Circuit-level firewallC. Application-level firewallD. Switch-level firewall Answer: AExplanation:A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.https://en.wikipedia.org/wiki/Stateful_firewall QUESTION 251Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization? A. Preparation phaseB. Containment phaseC. Identification phaseD. Recovery phase Answer: AExplanation:There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:Policy - a policy provides a written set of principles, rules, or practices within an Organization.Response Plan/Strategy - after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. This would include the creation of a backup plan.Communication - having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident.Documentation - it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response.
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 QUESTION 252Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.What technique is Ricardo using? A. SteganographyB. Public-key cryptographyC. RSA algorithmD. Encryption Answer: AExplanation:Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.https://en.wikipedia.org/wiki/Steganography QUESTION 253During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do? A. Identify and evaluate existing practicesB. Create a procedures documentC. Conduct compliance testingD. Terminate the audit Answer: AExplanation:The auditor should first evaluated existing policies and practices to identify problem areas and opportunities. QUESTION 254Which of the following statements regarding ethical hacking is incorrect? A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.B. Testing should be remotely performed offsite.C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.D. Ethical hacking should not involve writing to or modifying the target systems. Answer: AExplanation:Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.http://searchsecurity.techtarget.com/definition/ethical-hacker QUESTION 255Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report? A. a port scannerB. a vulnerability scannerC. a virus scannerD. a malware scanner Answer: B QUESTION 256What two conditions must a digital signature meet? A. Has to be unforgeable, and has to be authentic.B. Has to be legible and neat.C. Must be unique and have special characters.D. Has to be the same number of characters as a physical signature and must be unique. Answer: A QUESTION 257An attacker is trying to redirect the traffic of a small office. That office is using their

own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack? A. ARP PoisoningB. Smurf AttackC. DNS spoofingD. MAC Flooding Answer: C QUESTION 258If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation? A. CivilB. InternationalC. CriminalD. Common Answer: A QUESTION 259What is the role of test automation in security testing? A. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.B. It is an option but it tends to be very expensive.C. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.D. Test automation is not usable in security due to the complexity of the tests. Answer: A QUESTION 260The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition? A. Hack attackB. SniffingC. Dumpster divingD. Spying Answer: C More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms All the 312-50v9 braindumps are updated. Get a complete hold of 312-50v9 PDF dumps and 312-50v9 practice test with free VCE player through Lead2pass and boost up your skills. 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]