

[Lead2pass New Lead2pass Offering Free 312-50v9 Dumps Files For Free Downloading By 312-50v9 Exam Candidates (401-420)]

Lead2pass 2017 November New EC-Council [312-50v9 Exam Dumps!](#) 100% Free Download! 100% Pass Guaranteed!

Amazing, 100% candidates have passed the 312-50v9 exam by practising the preparation material of Lead2pass, because the braindumps are the latest and cover every aspect of 312-50v9 exam. Download the braindumps for an undeniable success in 312-50v9 exam. Following questions and answers are all new published by EC-Council Official Exam Center:

<https://www.lead2pass.com/312-50v9.html> QUESTION 401 Which of the following is an application that requires a host application for replication? A. MicroB. WormC. TrojanD. Virus Answer: D Explanation: Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing it self or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". https://en.wikipedia.org/wiki/Computer_virus QUESTION 402

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack? A. Paros ProxyB. BBProxyC. BBcrackD. Bloover Answer: B Explanation: Blackberry users warned of hacking tool threat. Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

<http://www.computerweekly.com/news/2240062112/Technology-news-in-brief> QUESTION 403 Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety? A. Restore a random file.B. Perform a full restore. C. Read the first 512 bytes of the tape.D. Read the last 512 bytes of the tape. Answer: B Explanation: A full restore is required.

QUESTION 404 Which of the following describes the characteristics of a Boot Sector Virus? A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBRB. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR C. Modifies directory table entries so that directory entries point to the virus code instead of the actual programD. Overwrites the original MBR and only executes the new virus code Answer: B Explanation: A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive. <https://www.techopedia.com/definition/26655/boot-sector-virus> QUESTION 405 Which statement is TRUE regarding network firewalls preventing Web Application attacks? A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.C. Network firewalls can prevent attacks if they are properly configured.D. Network firewalls cannot prevent attacks because they are too complex to configure. Answer: B Explanation: Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.

[https://en.wikipedia.org/wiki/Firewall_\(computing\)#Network_layer_or_packet_filters](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters) QUESTION 406 Which of the following programs is usually targeted at Microsoft Office products? A. Polymorphic virusB. Multipart virusC. Macro virusD. Stealth virus Answer: C Explanation: A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

https://en.wikipedia.org/wiki/Macro_virus QUESTION 407 Bluetooth uses which digital modulation technique to exchange information between paired devices? A. PSK (phase-shift keying)B. FSK (frequency-shift keying)C. ASK (amplitude-shift keying)D. QAM (quadrature amplitude modulation) Answer: A Explanation: Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK. <http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php> QUESTION 408

In order to show improvement of security over time, what must be developed? A. ReportsB. Testing toolsC. MetricsD. Taxonomy of vulnerabilities Answer: C Explanation: Today, management demands metrics to get a clearer view of security. Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs. <http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html> QUESTION 409 Passive reconnaissance involves collecting information through which of the following? A. Social engineeringB. Network

traffic sniffingC. Man in the middle attacksD. Publicly accessible sources Answer: D QUESTION 410How can rainbow tables be defeated? A. Password saltingB. Use of non-dictionary wordsC. All uppercase character passwordsD. Lockout accounts under brute force password cracking attempts Answer: A QUESTION 411The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106: What is most likely taking place? A. Ping sweep of the 192.168.1.106 networkB. Remote service brute force attemptC. Port scan of 192.168.1.106D. Denial of service attack on 192.168.1.106 Answer: BExplanation: QUESTION 412Which statement best describes a server type under an N-tier architecture? A. A group of servers at a specific layerB. A single server with a specific roleC. A group of servers with a unique roleD. A single server at a specific layer Answer: C QUESTION 413If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as? A. SDLC processB. Honey potC. SQL injectionD. Trap door Answer: D QUESTION 414A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred? A. The gateway is not routing to a public IP address.B. The computer is using an invalid IP address.C. The gateway and the computer are not on the same network. D. The computer is not using a private IP address. Answer: A QUESTION 415Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/ IP specifications? A. Ping of deathB. SYN floodingC. TCP hijackingD. Smurf attack Answer: A QUESTION 416Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS? A. Timing options to slow the speed that the port scan is conductedB. Fingerprinting to identify which operating systems are running on the networkC. ICMP ping sweep to determine which hosts on the network are not availableD. Traceroute to control the path of the packets sent during the scan Answer: A QUESTION 417When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is A. OWASP is for web applications and OSSTMM does not include web applications.B. OSSTMM is gray box testing and OWASP is black box testing.C. OWASP addresses controls and OSSTMM does not.D. OSSTMM addresses controls and OWASP does not. Answer: D QUESTION 418Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities? A. WebBugsB. WebGoatC. VULN_HTMLD. WebScarab Answer: B QUESTION 419What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes? A. Legal, performance, auditB. Audit, standards based, regulatoryC. Contractual, regulatory, industryD. Legislative, contractual, standards based Answer: D QUESTION 420Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest? A. MD5B. SHA-1C. RC4 D. MD4 Answer: B More free Lead2pass 312-50v9 exam new questions on Google Drive: <https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms> You can pass EC-Council 312-50v9 exam if you get a complete hold of 312-50v9 braindumps in Lead2pass. What's more, all the 312-50v9 Certification exam Q and As provided by Lead2pass are the latest. 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]