

## [Mar-2017 Dumps Learning New PassLeader 312-50v9 Exam Questions To Pass Exam Easily (Section B)

New Updated 312-50v9 Exam Questions from PassLeader 312-50v9 PDF dumps! Welcome to download the newest PassLeader 312-50v9 VCE dumps: <http://www.passleader.com/312-50v9.html> (589 Q&As) Keywords: 312-50v9 exam dumps, 312-50v9 exam questions, 312-50v9 VCE dumps, 312-50v9 PDF dumps, 312-50v9 practice tests, 312-50v9 study guide, 312-50v9 braindumps, Certified Ethical Hacker v9 Exam P.S. New 312-50v9 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpdnh4LVZhSV9hYm8](https://drive.google.com/open?id=0B-ob6L_QjGLpdnh4LVZhSV9hYm8) P.S. New 312-49v8 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpenRpMINIcjBjQ2M](https://drive.google.com/open?id=0B-ob6L_QjGLpenRpMINIcjBjQ2M) P.S. New 312-49v9 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpSnJrVWZSSFFMVVE](https://drive.google.com/open?id=0B-ob6L_QjGLpSnJrVWZSSFFMVVE) **NEW QUESTION 26** In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving. Which Algorithm is this referring to?

- A.&#160;&#160;&#160; Wired Equivalent Privacy (WEP) B.&#160;&#160;&#160; Wi-Fi Protected Access (WPA)  
C.&#160;&#160;&#160; Wi-Fi Protected Access 2 (WPA2) D.&#160;&#160;&#160; Temporal Key Integrity Protocol (TKIP)

**Answer: A Explanation:** WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases. Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

<https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html> **NEW QUESTION 27** Which of the following is considered an acceptable option when managing a risk? A.&#160;&#160;&#160; Reject the risk. B.&#160;&#160;&#160; Deny the risk.

C.&#160;&#160;&#160; Mitigate the risk. D.&#160;&#160;&#160; Initiate the risk. **Answer: C NEW QUESTION 28** Which

security control role does encryption meet? A.&#160;&#160;&#160; Preventative B.&#160;&#160;&#160; Detective

C.&#160;&#160;&#160; Offensive D.&#160;&#160;&#160; Defensive **Answer: A NEW QUESTION 29** Which type of

access control is used on a router or firewall to limit network activity? A.&#160;&#160;&#160; Mandatory

B.&#160;&#160;&#160; Discretionary C.&#160;&#160;&#160; Rule-based D.&#160;&#160;&#160; Role-based **Answer: C**

**NEW QUESTION 30** At a Windows Server command prompt, which command could be used to list the running services?

- A.&#160;&#160;&#160; Sc query type= running B.&#160;&#160;&#160; Sc query \servername C.&#160;&#160;&#160; Sc query  
D.&#160;&#160;&#160; Sc config **Answer: C NEW QUESTION 31** A security consultant decides to use multiple

layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which

kind of attack? A.&#160;&#160;&#160; Forensic attack B.&#160;&#160;&#160; ARP spoofing attack

C.&#160;&#160;&#160; Social engineering attack D.&#160;&#160;&#160; Scanning attack **Answer: C NEW QUESTION 32**

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB,

HTTP and FTP? A.&#160;&#160;&#160; Metasploit scripting engine B.&#160;&#160;&#160; Nessus scripting engine

C.&#160;&#160;&#160; NMAP scripting engine D.&#160;&#160;&#160; SAINT scripting engine **Answer: C NEW**

**QUESTION 33** Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows

products? A.&#160;&#160;&#160; Microsoft Security Baseline Analyzer B.&#160;&#160;&#160; Retina

C.&#160;&#160;&#160; Core Impact D.&#160;&#160;&#160; Microsoft Baseline Security Analyzer **Answer: D NEW**

**QUESTION 34** A security analyst is performing an audit on the network to determine if there are any deviations from the security

policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy

must the security analyst check to see if dial-out modems are allowed? A.&#160;&#160;&#160; Firewall-management policy

B.&#160;&#160;&#160; Acceptable-use policy C.&#160;&#160;&#160; Remote-access policy D.&#160;&#160;&#160;

Permissive policy **Answer: C NEW QUESTION 35** When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy? A.&#160;&#160;&#160; A bottom-up approach

B.&#160;&#160;&#160; A top-down approach C.&#160;&#160;&#160; A senior creation approach D.&#160;&#160;&#160;

An IT assurance approach **Answer: B NEW QUESTION 36** Which of the following processes evaluates the adherence of an

organization to its stated security policy? A.&#160;&#160;&#160; Vulnerability assessment B.&#160;&#160;&#160; Penetration

testing C.&#160;&#160;&#160; Risk assessment D.&#160;&#160;&#160; Security auditing **Answer: D NEW 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.&#160;&#160;&#160; 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 NEW 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 NEW 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 NEW 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 NEW QUESTION 41** Which type of antenna is used in wireless communication? A. Omnidirectional B. Parabolic C. Uni-directional D. Bi-directional **Answer: A NEW 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 NEW 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 NEW 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 NEW 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 NEW 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 NEW 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 NEW 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 NEW 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 NEW 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 NEW QUESTION 51 ??**

Download the newest PassLeader 312-50v9 dumps from passleader.com now! 100% Pass Guarantee! 312-50v9 PDF dumps & 312-50v9 VCE dumps: <http://www.passleader.com/312-50v9.html> (589 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New 312-50v9 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpdnh4LVZhSV9hYm8](https://drive.google.com/open?id=0B-ob6L_QjGLpdnh4LVZhSV9hYm8) P.S. New 312-49v8 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpenRpMINlcjBjQ2M](https://drive.google.com/open?id=0B-ob6L_QjGLpenRpMINlcjBjQ2M) P.S. New 312-49v9 dumps PDF:

[https://drive.google.com/open?id=0B-ob6L\\_QjGLpSnJrVWZSSFFMVVE](https://drive.google.com/open?id=0B-ob6L_QjGLpSnJrVWZSSFFMVVE)