[Full Version Free 312-50v9 Exam Dumps With PDF And VCE Download (21-35)

2017 March EC-Council Official New Released 312-50v9 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! 312-50v9 dumps free share: Lead2pass presents the highest quality of 312-50v9 exam dump which helps candidates to pass the 312-50v9 exams in the first attempt. Following questions and answers are all new published by EC-Council Official Exam Center: http://www.lead2pass.com/312-50v9.html QUESTION 21A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.Based on this information, what should be one of your key recommendations to the bank? A. Place a front-end web server in a demilitarized zone that only handles external web trafficB. Require all employees to change their passwords immediatelyC. Move the financial data to another server on the same IP subnetD. Issue new certificates to the web servers from the root certificate authorityAnswer: AExplanation:A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. https://en.wikipedia.org/wiki/DMZ_(computing) QUESTION 22Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.If a scanned port is open, what happens? A. The port will ignore the packets.B. The port will send an RST.C. The port will send an ACK.D. The port will send a SYN. Answer: AExplanation:An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out- of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.https://capec.mitre.org/data/definitions/303.html QUESTION 23During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.What is this type of DNS configuration commonly called? A. Split DNSB. DNSSECC. DynDNSD. DNS Scheme Answer: AExplanation:In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.http://www.webopedia.com/TERM/S/split_DNS.html QUESTION 24This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.Which of the following tools is being described? A. Aircrack-ngB. AirguardC. WLAN-crackD. wificracker Answer: AExplanation:Aircrack-ng is a complete suite of tools to assess WiFi network security.The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.http://www.aircrack-ng.org/doku.php?id=aircrack-ng QUESTION 25The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy? A. PrivateB. PublicC. SharedD. Root Answer: AExplanation:The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.An attack may also reveal private keys of compromised parties. https://en.wikipedia.org/wiki/Heartbleed QUESTION 26In 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. Wired Equivalent Privacy (WEP)B. Wi-Fi Protected Access (WPA)C. Wi-Fi Protected Access 2 (WPA2)D. Temporal Key Integrity Protocol (TKIP) Answer: AExplanation: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 QUESTION 27Which of the following is considered an acceptable option when managing a risk? A. Reject the risk.B. Deny the risk.C. Mitigate the risk.D. Initiate the risk. Answer: C QUESTION 28Which security control role does encryption meet? A. PreventativeB. DetectiveC. OffensiveD. Defensive Answer: A QUESTION 29Which type of access control is used on a router or firewall to limit network activity? A. MandatoryB. DiscretionaryC. Rule-basedD. Role-based Answer: C QUESTION 30At a Windows Server command prompt, which command could be used to list the running services? A. Sc query type= runningB. Sc query \servernameC. Sc queryD. Sc config Answer: C QUESTION 31A 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. Forensic attackB. ARP spoofing attackC. Social engineering attackD. Scanning attack Answer: C QUESTION 32Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP? A. Metasploit scripting engineB. Nessus scripting engineC. NMAP scripting engineD. SAINT scripting engine Answer: C QUESTION 33Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products? A. Microsoft Security Baseline AnalyzerB. RetinaC. Core ImpactD. Microsoft Baseline Security Analyzer Answer: D QUESTION 34A 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. Firewall-management policyB. Acceptable-use policyC. Remote-access policyD. Permissive policy Answer: C QUESTION 35When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy? A. A bottom-up approachB. A top-down approachC. A senior creation approachD. An IT assurance approach Answer: B Lead2pass is now offering Lead2pass 312-50v9 PDF dumps with 100% passing guarantee. Use Lead2pass 312-50v9 PDF and pass your exam easily. Download EC-Council 312-50v9 exam dumps and prepare for 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]