[Mar-2017 Dumps Exam 312-50v9 589q VCE and PDF Dumps Updated By PassLeader For Free (Section A)

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 P.S. New 312-49v8 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpenRpMlNlcjBjQ2M P.S. New 312-49v9 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpSnJrVWZSSFFMVVE **NEW QUESTION 1** You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly. What is the best nmap command you will use? A.   nmap -T4 -F 10.10.0.0/24 B.   nmap -T4 -r 10.10.1.0/24 C.   nmap -T4 -O 10.10.0.0/24 D.   nmap -T4 -q 10.10.0.0/24 **Answer: A Explanation:** command = nmap -T4 -F description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports. https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp **NEW QUESTION 2** You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through. invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING! What seems to be wrong? A.   OS Scan requires root privileges. B.   The nmap syntax is wrong. C.   This is a common behavior for a corrupted nmap application. D.   The outgoing TCP/IP fingerprinting is blocked by the host firewall. **Answer: A Explanation:** You requested a scan type which requires root privileges. http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host **NEW QUESTION 3** Which of the following statements is TRUE? A.   Sniffers operate on Layer 2 of the OSI model B.   Sniffers operate on Layer 3 of the OSI model C.   Sniffers operate on both Layer 2 & Layer 3 of the OSI model D.   Sniffers operate on the Layer 1 of the OSI model **Answer: A Explanation:** The OSI layer 2 is where packet sniffers collect their data. https://en.wikipedia.org/wiki/Ethernet_frame **NEW QUESTION 4** You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line. Which command would you use? A.   c:compmgmt.msc B.   c:services.msc C.   c:ncpa.cp D.   c:gpedit **Answer: A Explanation:** To start the Computer Management Console from command line just type compmgmt.msc / computer:computername in your run box or at the command line and it should automatically open the Computer Management console. http://www.waynezim.com/tag/compmgmtmsc/ **NEW QUESTION 5** What is the best description of SQL Injection? A.   It is an attack used to gain unauthorized access to a database. B.   It is an attack used to modify code in an application. C.   It is a Man-in-the-Middle attack between your SQL Server and Web App Server. D.   It is a Denial of Service Attack. **Answer: A Explanation:** SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). https://en.wikipedia.org/wiki/SQL_injection **NEW QUESTION 6** Which of the following is the BEST way to defend against network sniffing? A.   Using encryption protocols to secure network communications B.   Register all machines MAC Address in a Centralized Database C.   Restrict Physical Access to Server Rooms hosting Critical Servers D.   Use Static IP Address **Answer: A Explanation:** A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish. http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm **NEW QUESTION 7** You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS). What is the best way to evade the NIDS? A.   Encryption B.   Protocol Isolation C.   Alternate Data Streams D.   Out of band signalling **Answer: A Explanation:** When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that

exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/ **NEW QUESTION 8** You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";) A.   An Intrusion Detection System B.   A firewall IPTable C.   A Router IPTable D.   FTP Server rule **Answer: A Explanation:** Snort is an open source network intrusion detection system (NIDS) for networks. Snort rule example: This example is a rule with a generator id of 1000001. alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;) http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html **NEW QUESTION 9** What is the benefit of performing an unannounced Penetration Testing? A.   The tester will have an actual security posture visibility of the target network. B.   Network security would be in a "best state" posture. C.   It is best to catch critical infrastructure unpatched. D.   The tester could not provide an honest analysis. **Answer: A Explanation:** Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry. A possible solution to this danger is to conduct intermittent "unannounced" penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.
http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/ **NEW QUESTION 10** You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back. What is happening? A.   ICMP could be disabled on the target server. B.   The ARP is disabled on the target server. C.   TCP/IP doesn't support ICMP. D.   You need to run the ping command with root privileges. **Answer: A Explanation:** The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages. Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol **NEW QUESTION 11** Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state. Which of the following activities should not be included in this phase? (see exhibit) 1. Removing all files uploaded on the system 2. Cleaning all registry entries 3. Mapping of network state 4. Removing all tools and maintaining backdoor for reporting A.   3 B.   4 C.   3 and 4 D.   All should be included **Answer: A Explanation:** The post-attack phase revolves around returning any modified system(s) to the pretest state. Examples of such activities: - Removal of any files, tools, exploits, or other test-created objects uploaded to the system during testing - Removal or reversal of any changes to the registry made during system testing Computer and Information Security Handbook, John R. Vacca (2012), page 531 **NEW QUESTION 12** It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure. Which of the following regulations best matches the description? A.   HIPAA B.   ISO/IEC 27002 C.   COBIT D.   FISMA **Answer: A Explanation:** The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions). By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule **NEW QUESTION 13** Which of the following is a component of a risk assessment? A.   Administrative safeguards B.   Physical security C.   DMZ D.   Logical interface **Answer: A Explanation:** Risk assessment include: - The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review. - The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. lt includes risk analysis, cost benefit analysis, selection, implementation and test, security

evaluation of safeguards, and overall security review. https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment **NEW QUESTION 14** A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk? A.   Delegate B.   Avoid C.   Mitigate D.   Accept **Answer: A Explanation:** There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation. http://www.dbpmanagement.com/15/5-ways-to-manage-risk **NEW QUESTION 15** Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer? A.   Use a scan tool like Nessus B.   Use the built-in Windows Update tool C.   Check MITRE.org for the latest list of CVE findings D.   Create a disk image of a clean Windows installation **Answer: A Explanation:** Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix-or Windows-based operating systems. Note: Significant capabilities of Nessus include: - Compatibility with computers and servers of all sizes. - Detection of security holes in local or remote hosts. - Detection of missing security updates and patches. - Simulated attacks to pinpoint vulnerabilities. - Execution of security tests in a contained environment. - Scheduled security audits. **NEW QUESTION 16** Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability. What is this style of attack called? A.   zero-day B.   zero-hour C.   zero-sum D.   no-day **Answer: A Explanation:** Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. https://en.wikipedia.org/wiki/Stuxnet **NEW QUESTION 17** An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database. <iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe> What is this type of attack (that can use either HTTP GET or HTTP POST) called? A.   Cross-Site Request Forgery B.   Cross-Site Scripting C.   SQL Injection D.   Browser Hacking **Answer: A Explanation:** Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts. Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers. https://en.wikipedia.org/wiki/Cross-site_request_forgery **NEW QUESTION 18** It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers). Which of the following vulnerabilities is being described? A.   Shellshock B.   Rootshock C.   Rootshell D.   Shellbash **Answer: A Explanation:** Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. https://en.wikipedia.org/wiki/Shellshock_(software_bug) **NEW QUESTION 19** When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it. What should you do? A.   Forward the message to your company's security response team and permanently delete the message from your computer B.   Reply to the sender and ask them for more information about the message contents C.   Delete the email and pretend nothing happened D.   Forward the message to your supervisor and ask for her opinion on how to handle the situation **Answer: A Explanation:** By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites. https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_ConfigureScanEmailInboundAction.html **NEW QUESTION 20** The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task. What tool can you use to view the network traffic being sent and received by the wireless router? A.   Wireshark

B.   Nessus C.   Netcat D.   Netstat **Answer: A Explanation:** Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Incorrect Answers: B: Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. C: Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. D: Netstat provides network statistics. https://en.wikipedia.org/wiki/Wireshark **NEW QUESTION 21** A 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 traffic B.   Require all employees to change their passwords immediately C.   Move the financial data to another server on the same IP subnet D.   Issue new certificates to the web servers from the root certificate authority **Answer: A Explanation:** 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) **NEW QUESTION 22** Port 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: A Explanation:** 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 **NEW QUESTION 23** During 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 DNS B.   DNSSEC C.   DynDNS D.   DNS Scheme **Answer: A Explanation:** 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 **NEW QUESTION 24** This 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-ng B.   Airguard C.   WLAN-crack D.   wificracker **Answer: A Explanation:** 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 **NEW QUESTION 25** The 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.   Private B.   Public C.   Shared D.   Root **Answer: A Explanation:** 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 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 P.S. New 312-49v8 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpenRpMlNlcjBjQ2M P.S. New 312-49v9 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpSnJrVWZSSFFMVVE