[2017-New-Version312-50v9 Free Dumps Can Be Downloaded in Braindump2go(1-10)

2017 March New Updated EC-Council 312-50v9 Exam Dumps and 312-50v9 Exam Questions Updated Today!Free Instant Download 312-50v9 Exam Dumps (PDF & VCE) 589Q&As from www.Braindump2go.com **Today!** 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|NEW 312-50v9 Exam Dumps (PDF & VCE) 589Q&As Download: http://www.braindump2go.com/312-50v9.html 2.|NEW 312-50v9 Exam Questions & Answers Download: https://1drv.ms/f/s!AvI7wzKf6QBjgyJbM5f2lpRuMdO8 QUESTION 1You 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 10.10.0.0/24B. nmap -T4 -r 10.10.1.0/24C. nmap -T4 -O 10.10.0.0/24D. nmap -T4 -q 10.10.0.0/24 Answer: AExplanation:command = nmap -T4 -Fdescription = 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 QUESTION 2You 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 10.10.0.0/24TCP/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 QUESTION 3Which of the following statements is TRUE? A. Sniffers operate on Layer 2 of the OSI modelB. Sniffers operate on Layer 3 of the OSI modelC. 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 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.mscB. c:services.mscC. c:ncpa.cpD. 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/ QUESTION 5What 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 QUESTION 6Which of the following is the BEST way to defend against network sniffing? A. Using encryption protocols to secure network communicationsB. Register all machines MAC Address in a Centralized DatabaseC. Restrict Physical Access to Server Rooms hosting Critical ServersD. 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 QUESTION 7You 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. EncryptionB. Protocol IsolationC. Alternate Data StreamsD. Out of band signalling Answer: AExplanation: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/ QUESTION 8You 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 SystemB. A firewall IPTableC. A Router IPTableD. FTP Server rule Answer: AExplanation: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

QUESTION 9What 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: AExplanation: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/ QUESTION 10You 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 !!!RECOMMEND!!! 1.|NEW 312-50v9 Exam Dumps (PDF & VCE) 589Q&As Download:http://www.braindump2go.com/312-50v9.html 2.|NEW 312-50v9 Study Guide Video: YouTube Video: YouTube.com/watch?v=YSA9ckpy_7k