[2017 Newest Ensure Pass 312-50v9 Exam By Training Lead2pass New PDF Dumps (181-200)

Lead2pass 2017 September New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! In recent years, many people choose to take EC-Council 312-50v9 certification exam which can make you get the EC-Council certificate and that is the passport to get a better job and get promotions. How to prepare for EC-Council 312-50v9 exam and get the certificate? Please refer to EC-Council 312-50v9 exam questions and answers on Lead2pass. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 181A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response? A. Say no; the friend is not the owner of the account.B. Say yes; the friend needs help to gather evidence.C. Say yes; do the job for free.D. Say no; make sure that the friend knows the risk she's asking the CEH to take.Answer: A QUESTION 182This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low- level hackers sometimes known as script kiddies from causing a data breach.Which of the following organizations is being described? A. Payment Card Industry (PCI)B. Center for Disease Control (CDC)C. Institute of Electrical and Electronics Engineers (IEEE)D. International Security Industry Organization (ISIO) Answer: AExplanation:The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard QUESTION 183Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.What should you do? A. Immediately stop work and contact the proper legal authorities.B. Copy the data to removable media and keep it in case you need it.C. Confront the client in a respectful manner and ask her about the data.D. Ignore the data and continue the assessment until completed as agreed. Answer: AExplanation: QUESTION 184Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATAlocal directory and begins to beacon to a C2 server to download additional malicious binaries.What type of malware has Jesse encountered? A. TrojanB. WormC. Macro VirusD. Key-Logger Answer: AExplanation:In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.https://en.wikipedia.org/wiki/Trojan_horse_(computing) QUESTION 185Which tool allows analysts and pen testers to examine links between data using graphs and link analysis? A. MaltegoB. Cain & AbelC. MetasploitD. Wireshark Answer: AExplanation:Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva.Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.https://en.wikipedia.org/wiki/Maltego QUESTION 186While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.Which type of vulnerability is present on this site? A. Web Parameter TamperingB. Cookie TamperingC. XSS ReflectionD. SQL injection Answer: AExplanation:The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.https://www.owasp.org/index.php/Web_Parameter_Tampering QUESTION 187Perspective clients want to see sample reports from previous penetration tests.What should you do next? A. Decline but, provide references.B. Share full reports, not redacted.C. Share full reports with redactions.D. Share reports, after NDA is signed. Answer: AExplanation:Penetration tests data should not be disclosed to third parties. QUESTION 188During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.What type of firewall is inspecting outbound traffic? A. ApplicationB. CircuitC. StatefulD. Packet Filtering Answer: C QUESTION 189Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an

authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.What just happened? A. PiggybackingB. MasqueradingC. PhishingD. Whaling Answer: AExplanation:In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. https://en.wikipedia.org/wiki/Piggybacking_(security) QUESTION 190You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts? A. CHNTPWB. Cain & AbelC. SETD. John the Ripper Answer: AExplanation:chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.https://en.wikipedia.org/wiki/Chntpw QUESTION 191An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.Which file does the attacker need to modify? A. HostsB. SudoersC. Boot.iniD. Networks Answer: AExplanation:The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names. https://en.wikipedia.org/wiki/Hosts_(file) QUESTION 192After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first? A. Create User AccountB. Disable Key ServicesC. Disable IPTablesD. Download and Install Netcat Answer: A QUESTION 193What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host? env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd' A. Display passwd content to promptB. Removes the passwd fileC. Changes all passwords in passwdD. Add new user to the passwd file Answer: AExplanation:To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:() {:;}; /bin/cat /etc/passwdThat reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.https://blog.cloudflare.com/inside-shellshock/ QUESTION 194Using Windows CMD, how would an attacker list all the shares to which the current user context has access? A. NET USEB. NET CONFIGC. NET FILED. NET VIEW Answer: AExplanation:Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.https://technet.microsoft.com/en-us/library/bb490717.aspx QUESTION 195A common cryptographical tool is the use of XOR. XOR the following binary values: 1011000100111010 A. 10001011B. 11011000C. 10011101D. 10111100 Answer: AExplanation:The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".https://en.wikipedia.org/wiki/XOR_gate QUESTION 196Which of the following is the successor of SSL? A. TLSB. RSAC. GRED. IPSec Answer: AExplanation:Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.https://en.wikipedia.org/wiki/Transport_Layer_Security QUESTION 197You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number? A. TCPB. UPDC. ICMPD. UPX Answer: AExplanation:At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped. https://www.exploit-db.com/papers/13587/ QUESTION 198Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name.What should be the first step in security testing the client? A. ReconnaissanceB. EnumerationC. ScanningD. Escalation Answer: AExplanation:Phases of hackingPhase 1--ReconnaissancePhase 2--ScanningPhase 3--Gaining AccessPhase 4--Maintaining AccessPhase 5--Covering TracksPhase 1: Passive and Active ReconnaissancePassive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge.Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html QUESTION 199Which regulation defines security and privacy controls for Federal information systems and organizations? A. NIST-800-53B. PCI-DSSC. EU Safe HarborD. HIPAA Answer: AExplanation:NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53 QUESTION 200How does the Address Resolution Protocol (ARP) work? A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.B.

It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.C. It sends a reply packet for a specific IP, asking for the MAC address.D. It sends a request packet to all the network elements, asking for the domain name from a specific IP. Answer: AExplanation:When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Lead2pass is a good website that provides all candidates with the latest IT certification exam materials. Lead2pass will provide you with the exam questions and verified answers that reflect the actual exam. The EC-Council 312-50v9 exam dumps are developed by experienced IT professionals. 99.9% of hit rate. Guarantee you success in your 312-50v9 exam with our exam materials. 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]