OFFER Pass4sure and Lead2pass 312-49v8 PDF & VCE

Vendor: EC-Council Exam Code: 312-49v8 Exam Name: Computer Hacking Forensic Investigator v8 Exam QUESTION 1 Which of the following statements does not support the case assessment? A. Review the case investigator's request for service B. Identify the legal authority for the forensic examination request C. Do not document the chain of custody D. Discuss whether other forensic processes need to be performed on the evidence Answer: C QUESTION 2 Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it? A. War driving B. Rogue access points C. MAC spoofing D. Client mis-association Answer: D QUESTION 3 File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7? A. The last letter of a file name is replaced by a hex byte code E5h B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted C. Corresponding clusters in FAT are marked as used D. The computer looks at the clusters occupied by that file and does not avails space to store a new file Answer: B QUESTION 4 What is cold boot (hard boot)? A. It is the process of starting a computer from a powered-down or off state B. It is the process of restarting a computer that is already turned on through the operating system C. It is the process of shutting down a computer from a powered-on or on state D. It is the process of restarting a computer that is already in sleep mode Answer: A QUESTION 5 When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____. A. Restart Windows B. Kill the running processes in Windows task manager C. Run the antivirus tool on the system D. Run the anti-spyware tool on the system Answer: A QUESTION 6 MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network A. 16-bit address B. 24-bit address C. 32-bit address D. 48-bit address Answer: D QUESTION 7 Log management includes all the processes and techniques used to collect, aggregate, and analyze computer-generated log messages. It consists of the hardware, software, network and media used to generate, transmit, store, analyze, and dispose of log data. A. True B. False Answer: A QUESTION 8 You can interact with the Registry through intermediate programs. Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32 exe are commonly used as intermediate programs in Windows 7. Which of the following is a root folder of the registry editor? A. HKEY_USERS B. HKEY_LOCAL_ADMIN C. HKEY_CLASSES_ADMIN D. HKEY_CLASSES_SYSTEM Answer: A QUESTION 9 You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at which sessions the machine has opened with other systems? A. Net sessions B. Net use C. Net config D. Net share Answer: B QUESTION 10 What is a SCSI (Small Computer System Interface)? A. A set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives. CD-ROM drives, printers, and scanners B. A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices C. A "plug-and-play" interface, which allows a device to be added without an adapter card and without rebooting the computer D. A point-to-point serial bi-directional interface for transmitting data between computer devices at data rates of up to 4 Gbps Answer: A QUESTION 11 The status of the network interface cards (NICs) connected to a system gives information about whether the system is connected to a wireless access point and what IP address is being used. Which command displays the network configuration of the NICs on the system? A. ipconfig /all B. netstat C. net session D. tasklist Answer: A QUESTION 12 Which Is a Linux journaling file system? A. Ext3 B. HFS C. FAT D. BFS Answer: A QUESTION 13 Which of the following steganography types hides the secret message in a specifically designed pattern on the document that is unclear to the average reader? A. Open code steganography B. Visual semagrams steganography C. Text semagrams steganography D. Technical steganography Answer: A QUESTION 14 Web applications provide an Interface between end users and web servers through a set of web pages that are generated at the server-end or contain script code to be executed dynamically within the client Web browser. A. True B. False Answer: A QUESTION 15 Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings? A. DNS Poisoning B. Cookie Poisoning Attack C. DNS Redirection D. Session poisoning Answer: A QUESTION 16 Which table is used to convert huge word lists (i .e. dictionary files and brute-force lists) into password hashes? A. Rainbow tables B. Hash tables C. Master file tables D. Database tables Answer: A If you want to pass EC-Council 312-49v8 successfully, donot missing to read latest lead2pass EC-Council 312-49v8 practice tests. If you can master all lead2pass questions you will able to pass 100%

guaranteed. http://www.lead2pass.com/312-49v8.html