[January 2018 100% Pass Lead2pass 312-49v9 New Questions Free Version 490q

100% Valid Lead2pass EC-Council 312-49v9 New Questions Free Version: https://www.lead2pass.com/312-49v9.html QUESTION 41Shortcuts are the files with the extension .lnk that are created and are accessed by the users. These files provide you with information about: A. Files or network sharesB. Running applicationC. Application logsD. System logsAnswer: A QUESTION 42A computer forensic report is a report which provides detailed information on the complete forensics investigation process. A. TrueB. False Answer: A QUESTION 43Which one of the following statements is not correct while preparing for testimony? A. Go through the documentation thoroughlyB. Do not determine the basic facts of the case before beginning and examining the evidenceC. Establish early communication with the attorneyD. Substantiate the findings with documentation and by collaborating with other computer forensics professionals Answer: B QUESTION 44Computer security logs contain information about the events occurring within an organization's systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by _____of the compromised system. A. Analyzing log filesB. Analyzing SAM fileC. Analyzing rainbow tablesD. Analyzing hard disk boot records Answer: A QUESTION 45An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network to identify any possible violations of security policy, including unauthorized access, as well as misuse.Which of the following intrusion detection systems audit events that occur on a specific host? A. Network-based intrusion detectionB. Host-based intrusion detectionC. Log file monitoringD. File integrity checking Answer: B QUESTION 46What is a first sector ("sector zero") of a hard disk? A. Master boot recordB. System boot recordC. Secondary boot recordD. Hard disk boot record Answer: A QUESTION 47Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which or the following is an appropriate action for the mobile forensic investigation? A. To avoid unwanted interaction with devices found on the scene, turn on any wireless interfaces such as Bluetooth and Wi-Fi radiosB. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidenceC. If the device's display is ON. the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed iconsD. If the phone is in a cradle or connected to a PC with a cable, then unplug the device from the computer Answer: C QUESTION 48Which of the following is the certifying body of forensics labs that investigate criminal cases by analyzing evidence? A. The American Society of Crime Laboratory Directors (ASCLD)B. International Society of Forensics Laboratory (ISFL)C. The American Forensics Laboratory Society (AFLS)D. The American Forensics Laboratory for Computer Forensics (AFLCF) Answer: A QUESTION 49 When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____. A. 4902B. 3902C. 4904D. 3904 Answer: A QUESTION 50MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network A. 16-bit addressB. 24-bit addressC. 32-bit addressD. 48-bit address Answer: D **312-49v9 dumps full version (PDF&VCE):** https://www.lead2pass.com/312-49v9.html Large amount of free **312-49v9** exam questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDSWJCNkFjOEx1Yms You may also need: 312-50v9 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms