

[January 2018 2018 New Lead2pass EC-Council 312-49v9 Dumps Free Download 490q

2018 New Released EC-Council 312-49v9 Exam Dumps Free Download In Lead2pass: <https://www.lead2pass.com/312-49v9.html>

QUESTION 41 Shortcuts 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 shares B. Running application C. Application logs D. System logs Answer: A

QUESTION 42 A computer forensic report is a report which provides detailed information on the complete forensics investigation process. A. True B. False Answer: A

QUESTION 43 Which one of the following statements is not correct while preparing for testimony? A. Go through the documentation thoroughly B. Do not determine the basic facts of the case before beginning and examining the evidence C. Establish early communication with the attorney D. Substantiate the findings with documentation and by collaborating with other computer forensics professionals Answer: B

QUESTION 44 Computer 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 files B. Analyzing SAM file C. Analyzing rainbow tables D. Analyzing hard disk boot records Answer: A

QUESTION 45 An 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 detection B. Host-based intrusion detection C. Log file monitoring D. File integrity checking Answer: B

QUESTION 46 What is a first sector ("sector zero") of a hard disk? A. Master boot record B. System boot record C. Secondary boot record D. Hard disk boot record Answer: A

QUESTION 47 Ever-changing advancement or mobile devices increases the complexity of mobile device examinations. Which of 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 radios B. Do not wear gloves while handling cell phone evidence to maintain integrity of physical evidence C. 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 icons D. 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 48 Which 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. 4902 B. 3902 C. 4904 D. 3904 Answer: A

QUESTION 50 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

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>