# [November-2022100% Success-Braindump2go 312-49v10 VCE and 312-49v10 PDF 312-49v10 869Q Instant Download[Q770-Q836

November/2022 Latest Braindump2go 312-49v10 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go 312-49v10 Real Exam Questions!QUESTION 770Which OWASP loT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on loT devices?A. Lack of secure update mechanismB. Use of insecure or outdated componentsC. Insecure default settingsD. Insecure data transfer and storageAnswer: AQUESTION 771Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?A. echo text > program: source_fileB. myfile.dat: st ream 1C. C:MORE < myfile.txt:siream1 D. C:>ECHO text_message > myfile.txt:stream1Answer: AQUESTION 772Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?A. Data Protection Act of 2018B. Payment Card Industry Data Security Standard (PCI DSS)C. Electronic Communications Privacy ActD. Health Insurance Portability and Accountability Act of 1996 (HIPAA)Answer: DQUESTION 773In a Fllesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?A. /sbinB. /procC. /mmD. /mediaAnswer: AQUESTION 774Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?A. OllydbgB. oledumpC. HashCalcD. BinTextAnswer: AQUESTION 775A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?A. HelixB. R-StudioC. NetCatD. WiresharkAnswer: BQUESTION 776In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?A. initB. Media serverC. ZygoteD. DaemonAnswer: CQUESTION 777"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?A. Principle 1B. Principle 3C. Principle 4D. Principle 2Answer: DQUESTION 778_____allows a forensic investigator to identify the missing links during investigation.A. Evidence preservationB. Chain of custodyC. Evidence reconstructionD. Exhibit numberingAnswer: CQUESTION 779An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?A. BitLockerB. Data duplication toolC. Backup toolD. Write blockerAnswer: DQUESTION 780During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.What does the first four digits (89 and 44) In the ICCID represent?A. TAC and industry identifierB. Country code and industry identifierC. Industry identifier and country codeD. Issuer identifier number and TACAnswer: CQUESTION 781Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?A. Stream DetectorB. TimeStompC. AutopsyD. analyzeMFTAnswer: AQUESTION 782Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or Illegal Information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?A. Denial-of-Service (DoS) attackB. Malware attackC. Ransomware attackD. PhishingAnswer: CQUESTION 783When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?A. 7680B. 49667/49668C. 9150/9151D. 49664/49665Answer: CQUESTION 784An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?A. PWdump7B. HashKeyC. NuixD. FileMerlinAnswer: AQUESTION 785William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000) "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?A. The combined log format of Apache access logB. The common log format of Apache access logC. Apache error logD. IIS logAnswer: AQUESTION 786What happens lo the header of the file once It Is deleted from the Windows OS file systems?A. The OS replaces the first letter of a deleted file name with a hex byte code: E5hB. The OS replaces the entire hex byte coding of the file.C. The hex byte coding of the file remains the same, but the file location differsD. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5Answer: AQUESTION 787Sally

accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored. To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?A. Password sniffingB. Anti-forensicsC. Brute-force attackD. Network intrusionAnswer: BQUESTION 788Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?A. Block clones cannot be created with solid-state drivesB. Write blockers were used while cloning the evidenceC. John did not document the chain of custodyD. John investigated the clone instead of the original evidence itselfAnswer: CQUESTION 789Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?A. BMPB. GIF C. ASCIID. JPEGAnswer: DQUESTION 790Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from client that has undergone a cyberattack. Brian ran the executable file In the virtual environment to see what it would do. What type of analysis did Brian perform?A. Static malware analysisB. Status malware analysisC. Dynamic malware analysisD. Static OS analysisAnswer: CQUESTION 791 When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?A. Brute-force attackB. Cookie poisoning attackC. Cross-site scripting attackD. SQL injection attackAnswer: CQUESTION 792A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be Identified as_____.A. Swap spaceB. Cluster spaceC. Slack spaceD. Sector spaceAnswer: DQUESTION 793Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?A. DB Browser SQLiteB. Bulk ExtractorC. Belkasoft Live RAM Capturer and AccessData FTK imagerD. Hex EditorAnswer: CQUESTION 794Which of the following statements pertaining to First Response is true?A. First Response is a part of the investigation phaseB. First Response is a part of the post-investigation phaseC. First Response is a part of the pre-investigation phaseD. First Response is neither a part of pre-investigation phase nor a part of investigation phase. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficientlyAnswer: AQUESTION 795Consider a scenario where the perpetrator of a dark web crime has unlnstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?A. Swap filesB. Files in Recycle BinC. Security logsD. Prefetch filesAnswer: AQUESTION 796A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. What will happen to the data?A. The data will remain in its original clusters until it is overwritten B. The data will be moved to new clusters in unallocated spaceC. The data will become corrupted, making it unrecoverableD. The data will be overwritten with zeroesAnswer: AQUESTION 797Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?A. VolatilityB. AutopsyC. RAM MapperD. MemcheckAnswer: AQUESTION 798Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used In an Incident that occurred earlier. He started Inspecting and gathering the contents of RAM, cache, and DLLs to Identify Incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.A. Dead data acquisitionB. Static data acquisitionC. Non-volatile data acquisitionD. Live data acquisitionAnswer: CQUESTION 799In forensics._____are used lo view stored or deleted data from both files and disk sectors.A. Hash algorithmsB. SI EM toolsC. Host interfaces D. Hex editorsAnswer: DQUESTION 800 Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?A. Manual acquisitionB. Logical acquisitionC. Direct acquisitionD. Physical

acquisitionAnswer: DQUESTION 801Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant Is immaterial and certain characteristics of the declarant such as present sense Impression, excited utterance, and recorded recollection are also observed while giving their testimony?A. Rule 801B. Rule 802C. Rule 804D. Rule 803Answer: DQUESTION 802What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?A. APK AnalyzerB. SDK ManagerC. Android Debug BridgeD. XcodeAnswer: CQUESTION 803An Investigator Is checking a Cisco firewall log that reads as follows:Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outsideWhat does %ASA-1-106021 denote?A. Mnemonic messageB. Type of trafficC. Firewall actionD. Type of requestAnswer: CQUESTION 804A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?A. FilelessB. TrojanC. JavaScriptD. SpywareAnswer: AQUESTION 805Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN- DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?A. relay-log.infoB. WIN-DTRAl83202Xrelay-bin.indexC. WIN-DTRAI83202Xslow.logD. WIN-DTRAI83202X-bin.nnnnnnAnswer: CQUESTION 806Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?A. The digital camera was not listed as one of the digital devices in the warrantB. The vehicle Debbie was using to transport the evidence was already full and could not carry more itemsC. Debbie overlooked the digital camera because it is not a computer systemD. The digital camera was old. had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.Answer: AQUESTION 807Place the following In order of volatility from most volatile to the least volatile.A. Registers and cache, routing tables, temporary file systems, disk storage, archival mediaB. Register and cache, temporary file systems, routing tables, disk storage, archival mediaC. Registers and cache, routing tables, temporary file systems, archival media, disk storageD. Archival media, temporary file systems, disk storage, archival media, register and cacheAnswer: BQUESTION 808Fill In the missing Master Boot Record component.1. Master boot code2. Partition table3._____A. Boot loaderB. Signature wordC. Volume boot recordD. Disk signatureAnswer: AQUESTION 809Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.A. MalvertisingB. Internet relay chatsC. Drive-by downloadsD. PhishingAnswer: CQUESTION 810"To ensure that the digital evidence is collected, preserved, examined, or transferred In a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:A. NCISB. NISTC. EC-CouncilD. SWGDEAnswer: BQUESTION 811James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the Investigation, he recovered certain deleted files from Recycle Bin to Identify attack clues.Identify the location of Recycle Bin in Windows XP system.A. Drive:$Recycle.BinB. Iocal/sha re/TrashC. Drive:RECYCLERD. DriveARECYCLEDAnswer: CQUESTION 812Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)B. Wireshark capture does not show anything unusual and the issue is related to the web applicationC. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)Answer: CQUESTION 813During an Investigation, the first responders stored mobile devices In specific containers to provide network Isolation. All the following are examples of such pieces of equipment, except for:A. Wireless StrongHold bagB. VirtualBoxC. Faraday bagD. RF shield boxAnswer: DQUESTION 814Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?A. Event ID 4657B. Event ID 4624C. Event ID 4688D. Event ID 7040Answer: AQUESTION 815SO/IEC 17025 is an accreditation for which of the following:A. CHFI issuing agencyB. EncryptionC. Forensics lab licensingD. Chain of custodyAnswer: CQUESTION 816 Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know

how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.What type of malware analysis is Edgar performing?A. Malware disassemblyB. VirusTotal analysisC. Static analysisD. Dynamic malware analysis/behavioral analysisAnswer: DQUESTION 817A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?A. To create an investigation reportB. To fill the chain of custodyC. To recover data from suspect devicesD. To enforce the security of all devices and software in the sceneAnswer: DQUESTION 818This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.A. The CAN-SPAM actB. Federal Spam actC. Telemarketing actD. European Anti-Spam actAnswer: AQUESTION 819A clothing company has recently deployed a website on Its latest product line to Increase Its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from Intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?A. ModSecurityB. CryptaPixC. RecuvaD. Kon-BootAnswer: AQUESTION 820A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:



What type of attack was performed on the companies' web application?A. Directory transversalB. Unvalidated inputC. Log tamperingD. SQL injectionAnswer: DQUESTION 821On NTFS file system, which of the following tools can a forensic Investigator use In order to identify timestomping of evidence files?A. wbStegoB. Exiv2C. analyzeMFTD. TimestompAnswer: DQUESTION 822Rule 1002 of Federal Rules of Evidence (US) talks about_____A. Admissibility of original B. Admissibility of duplicatesC. Requirement of originalD. Admissibility of other evidence of contentsAnswer: CQUESTION 823Which of the following Ii considered as the starting point of a database and stores user data and database objects in an MS SQL server?A. Ibdata1B. Application data files (ADF)C. Transaction log data files (LDF)D. Primary data files (MDF)Answer: CQUESTION 824Which of the following statements is true with respect to SSDs (solid-state drives)?A. Like HDDs. SSDs also have moving partsB. SSDs cannot store non-volatile dataC. SSDs contain tracks, clusters, and sectors to store dataD. Faster data access, lower power usage, and higher reliability are some of the m<ijor advantages of SSDs over HDDsAnswer: DQUESTION 825To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate the content of the:A. MBRB. GRUBC. UEFID. BIOSAnswer: AQUESTION 826 During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to Identify attributes such as "author name," "organization name." "network name," or any additional supporting data that is meant for the owner's Identification purpose. Which term describes these attributes?A. Data headerB. Data indexC. MetabaseD. MetadataAnswer: DQUESTION 827The working of the Tor browser is based on which of the following concepts?A. Both static and default routingB. Default routingC. Static routingD. Onion routingAnswer: DQUESTION 828An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?A. They should pause the running instanceB. They should keep the instance running as it stores critical dataC. They should terminate all instances connected via the same VPCD. They should terminate the instance after taking necessary backupAnswer: DQUESTION 829You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern EuropeB. Internal systems are downloading automatic Windows updatesC. Data is being exfiltrated by an advanced persistent threat (APT)D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entitiesAnswer: CQUESTION 830Choose the layer in iOS architecture that provides frameworks for iOS app development?A. Media servicesB. Cocoa TouchC. Core servicesD. Core OSAnswer: CQUESTION 831Data density of a disk drive is calculated by using_____A. Slack space, bit density, and slack density.B.

Track space, bit area, and slack space.C. Track density, areal density, and slack density.D. Track density, areal density, and bit density.Answer: DQUESTION 832Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?A. Most Recently Used (MRU) listB. MZCacheViewC. Google Chrome Recovery UtilityD. Task ManagerAnswer: BQUESTION 833For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?A. Relevant circumstances surrounding the collectionB. General description of the evidenceC. Exact location the evidence was collected fromD. SSN of the person collecting the evidenceAnswer: DQUESTION 834This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?A. Testimony by the accusedB. Limited admissibilityC. Hearsay ruleD. Rule 1001Answer: CQUESTION 835The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?A. Report the incident to senior managementB. Update the anti-virus definitions on the file serverC. Disconnect the file server from the networkD. Manually investigate to verify that an incident has occurredAnswer: CQUESTION 836Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?A. CoreographyB. DatagrabC. EtherealD. HelixAnswer: DResources From:1.2022 Latest Braindump2go 312-49v10 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/312-49v10.html2.2022 Latest Braindump2go 312-49v10 PDF and 312-49v10 VCE Dumps Free Share:https://drive.google.com/drive/folders/1r0yGepG-AIO5ksrNsA_-GhqjWWFE7IQ4?usp=sharing3.2021 Free Braindump2go 312-49v10 Exam Questions Download: https://www.braindump2go.com/free-online-pdf/312-49v10-PDF-Dumps(770-836).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!