

[November-2022] 100% Success-Braindump2go 312-49v10 PDF Dumps 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 770 Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT devices?
A. Lack of secure update mechanism
B. Use of insecure or outdated components
C. Insecure default settings
D. Insecure data transfer and storage
Answer: A

QUESTION 771 Assume there is a file named myfile.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_file
B. myfile.dat: stream 1
C. C:MORE < myfile.txt: stream 1
D. C:>ECHO text_message > myfile.txt: stream 1
Answer: A

QUESTION 772 Adam 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 2018
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Electronic Communications Privacy Act
D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Answer: D

QUESTION 773 In a Filesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?
A. /sbin
B. /proc
C. /mm
D. /media
Answer: A

QUESTION 774 Harry 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. Ollydbg
B. oledump
C. HashCalc
D. BinText
Answer: A

QUESTION 775 A 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. Helix
B. R-Studio
C. NetCat
D. Wireshark
Answer: B

QUESTION 776 In 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. init
B. Media server
C. Zygote
D. Daemon
Answer: C

QUESTION 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 1
B. Principle 3
C. Principle 4
D. Principle 2
Answer: D

QUESTION 778 _____ allows a forensic investigator to identify the missing links during investigation.
A. Evidence preservation
B. Chain of custody
C. Evidence reconstruction
D. Exhibit numbering
Answer: C

QUESTION 779 An 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. BitLocker
B. Data duplication tool
C. Backup tool
D. Write blocker
Answer: D

QUESTION 780 During an investigation, Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548. What do the first four digits (89 and 44) in the ICCID represent?
A. TAC and industry identifier
B. Country code and industry identifier
C. Industry identifier and country code
D. Issuer identifier number and TAC
Answer: C

QUESTION 781 Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?
A. Stream Detector
B. TimeStomp
C. Autopsy
D. analyzeMFT
Answer: A

QUESTION 782 Cybercriminals 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) attack
B. Malware attack
C. Ransomware attack
D. Phishing
Answer: C

QUESTION 783 When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?
A. 7680
B. 49667/49668
C. 9150/9151
D. 49664/49665
Answer: C

QUESTION 784 An 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. PWDump
B. HashKey
C. Nuxit
D. FileMerlin
Answer: A

QUESTION 785 William 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 log
B. The common log format of Apache access log
C. Apache error log
D. IIS log
Answer: A

QUESTION 786 What happens to 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: E5h
B. 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 differs.
D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5
Answer: A

QUESTION 787 Sally

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 sniffing B. Anti-forensics C. Brute-force attack D. Network intrusion

Answer: B QUESTION 788 Fred, 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 drives B. Write blockers were used while cloning the evidence C. John did not document the chain of custody D. John investigated the clone instead of the original evidence itself

Answer: C QUESTION 789 Jack 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 0xffd8. Based on the above information, what type of format is the file/image saved as? A. BMP B. GIF C. ASCII D. JPEG

Answer: D QUESTION 790 Brian 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 analysis B. Static malware analysis C. Dynamic malware analysis D. Static OS analysis

Answer: C QUESTION 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 attack B. Cookie poisoning attack C. Cross-site scripting attack D. SQL injection attack

Answer: C QUESTION 792 A 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 space B. Cluster space C. Slack space D. Sector space

Answer: D QUESTION 793 Which 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 SQLite B. Bulk Extractor C. Belkasoft Live RAM Capturer and AccessData FTK imager D. Hex Editor

Answer: C QUESTION 794 Which of the following statements pertaining to First Response is true? A. First Response is a part of the investigation phase B. First Response is a part of the post-investigation phase C. First Response is a part of the pre-investigation phase D. 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 efficiently

Answer: A QUESTION 795 Consider a scenario where the perpetrator of a dark web crime has uninstalled 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 files B. Files in Recycle Bin C. Security logs D. Prefetch files

Answer: A QUESTION 796 A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evidence1.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 space C. The data will become corrupted, making it unrecoverable D. The data will be overwritten with zeroes

Answer: A QUESTION 797 Jeff 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. Volatility B. Autopsy C. RAM Mapper D. Memcheck

Answer: A QUESTION 798 Derrick, 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 acquisition B. Static data acquisition C. Non-volatile data acquisition D. Live data acquisition

Answer: C QUESTION 799 In forensics, _____ are used to view stored or deleted data from both files and disk sectors. A. Hash algorithms B. SIEM tools C. Host interfaces D. Hex editors

Answer: D QUESTION 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 acquisition B. Logical acquisition C. Direct acquisition D. Physical

acquisition
Answer: DQUESTION 801 Which 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 803
Answer: DQUESTION 802 What 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. Xcode
Answer: CQUESTION 803 An 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 outside
What does %ASA-1-106021 denote?
A. Mnemonic messageB. Type of trafficC. Firewall actionD. Type of request
Answer: CQUESTION 804 A 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. Spyware
Answer: AQUESTION 805 Ronald, 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-DTRAI83202Xrelay-bin.indexC. WIN-DTRAI83202Xslow.logD. WIN-DTRAI83202X-bin.nnnnnn
Answer: CQUESTION 806 Debbie has obtained a warrant to search a known pedophile's 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 807 Place 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 cache
Answer: BQUESTION 808 Fill in the missing Master Boot Record component.
1. Master boot code2. Partition table3. _____
A. Boot loaderB. Signature wordC. Volume boot recordD. Disk signature
Answer: AQUESTION 809 Which 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. Phishing
Answer: 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. SWGDE
Answer: BQUESTION 811 James, 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. local/sha re/TrashC. Drive:RECYCLERD. Drive:ARECYCLED
Answer: CQUESTION 812 Recently, 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 Wireshark 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 813 During 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 box
Answer: DQUESTION 814 Maria 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 7040
Answer: AQUESTION 815 SO/IEC 17025 is an accreditation for which of the following:
A. CHFI issuing agencyB. EncryptionC. Forensics lab licensingD. Chain of custody
Answer: 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 disassembly B. VirusTotal analysis C. Static analysis D. Dynamic malware analysis/behavioral analysis Answer: DQUESTION 817 A 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 report B. To fill the chain of custody C. To recover data from suspect devices D. To enforce the security of all devices and software in the scene Answer: DQUESTION 818 This 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 act B. Federal Spam act C. Telemarketing act D. European Anti-Spam act Answer: AQUESTION 819 A 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. ModSecurity B. CryptaPix C. Recuva D. Kon-Boot Answer: AQUESTION 820 A 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:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or 1=1 - 12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah" or exec master..xp_cmdshell 'dir c:\windows\system32\cmd.exe'
```

What type of attack was performed on the companies' web application? A. Directory transversal B. Unvalidated input C. Log tampering D. SQL injection Answer: DQUESTION 821 On NTFS file system, which of the following tools can a forensic Investigator use In order to identify timestomping of evidence files? A. wbStego B. Exiv2 C. analyzeMFT D. Timestomp Answer: DQUESTION 822 Rule 1002 of Federal Rules of Evidence (US) talks about ____ A. Admissibility of original B. Admissibility of duplicates C. Requirement of original D. Admissibility of other evidence of contents Answer: CQUESTION 823 Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server? A. Idata1 B. Application data files (ADF) C. Transaction log data files (LDF) D. Primary data files (MDF) Answer: CQUESTION 824 Which of the following statements is true with respect to SSDs (solid-state drives)? A. Like HDDs, SSDs also have moving parts B. SSDs cannot store non-volatile data C. SSDs contain tracks, clusters, and sectors to store data D. Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs Answer: DQUESTION 825 To 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. MBR B. GRUB C. UEFID. BIOS Answer: 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 header B. Data index C. Metabase D. Metadata Answer: DQUESTION 827 The working of the Tor browser is based on which of the following concepts? A. Both static and default routing B. Default routing C. Static routing D. Onion routing Answer: DQUESTION 828 An 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 instance B. They should keep the instance running as it stores critical data C. They should terminate all instances connected via the same VPC D. They should terminate the instance after taking necessary backup Answer: DQUESTION 829 You 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 SFTP servers in Eastern Europe B. Internal systems are downloading automatic Windows updates C. 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 entities Answer: CQUESTION 830 Choose the layer in iOS architecture that provides frameworks for iOS app development? A. Media services B. Cocoa Touch C. Core services D. Core OS Answer: CQUESTION 831 Data 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 Manager
Answer: 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 evidence
Answer: 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 1001
Answer: 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 occurred
Answer: CQUESTION 836Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?A. CoreographyB. DatagrabC. EtherealD. Helix
Answer: DResources From: 1.2022 Latest Braindump2go 312-49v10 Exam Dumps (PDF & VCE) Free Share:<https://www.braindump2go.com/312-49v10.html> 2.2022 Latest Braindump2go 312-49v10 PDF and 312-49v10 VCE Dumps Free Share:https://drive.google.com/drive/folders/1r0yGepG-AIO5ksrNsA_-GhqjWWFE7IQ4?usp=sharing 3.2021 Free Braindump2go 312-49v10 Exam Questions Download: [https://www.braindump2go.com/free-online-pdf/312-49v10-PDF-Dumps\(770-836\).pdf](https://www.braindump2go.com/free-online-pdf/312-49v10-PDF-Dumps(770-836).pdf) Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!