[July-2022Exam Pass 100%!Braindump2go 312-49v10 Exam VCE and PDF 312-49v10 769Q Instant Download[Q701-Q752

July/2022 Latest Braindump2go 312-49v10 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 312-49v10 Real Exam Questions!QUESTION 701You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?A. All three servers need to be placed internallyB. A web server and the database server facing the Internet, an application server on the internal networkC. A web server facing the Internet, an application server on the internal network, a database server on the internal networkD. All three servers need to face the Internet so that they can communicate between themselvesAnswer: DQUESTION 702The NMAP command above performs which of the following?> NMAP -sn 192.168.11.200-215A. A trace sweepB. A port scanC. A ping scanD. An operating system detectAnswer: CQUESTION 703 You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?A. Inverse TCP flag scanningB. ACK flag scanningC. TCP ScanningD. IP Fragment ScanningAnswer: DQUESTION 704In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?A. Both pharming and phishing attacks are purely technical and are not considered forms of social engineeringB. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain nameC. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain nameD. Both pharming and phishing attacks are identicalAnswer: BQUESTION 705As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?A. Project ScopeB. Rules of EngagementC. Non-Disclosure AgreementD. Service Level AgreementAnswer: BQUESTION 706A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?A. tcp.port = 23B. tcp.port == 21C. tcp.port == 21 || tcp.port == 22D. tcp.port != 21Answer: BQUESTION 707To reach a bank web site, the traffic from workstations must pass through a firewall.You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https.Which of the following firewall rules meets this requirement?A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permitB. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permitC. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permitAnswer: AQUESTION 708companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.A. Source code reviewB. Reviewing the firewalls configurationC. Data items and vulnerability scanningD. Interviewing employees and network engineersAnswer: AQUESTION 709Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?A. Encrypt the backup tapes and use a courier to transport them.B. Encrypt the backup tapes and transport them in a lock boxC. Degauss the backup tapes and transport them in a lock box.D. Hash the backup tapes and transport them in a lock box.Answer: BQUESTION 710As part of extracting the system data, Jenifer has used the netstat command. What does this tool reveal?A. Status of users connected to the internetB. Net status of computer usageC. Information about network connectionsD. Status of network hardwareAnswer: CQUESTION 711Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?A. Virtual FilesB. Image FilesC. Shortcut FilesD. Prefetch FilesAnswer: CQUESTION 712Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it

on a popular ad-network that displays across various websites. What is she doing?A. MalvertisingB. Compromising a legitimate siteC. Click-jackingD. SpearphishingAnswer: AQUESTION 713Buffer overflow vulnerabilities, of web applications, occurs when the application fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.A. Adjacent buffer locationsB. Adjacent string locationsC. Adjacent bit blocksD. Adjacent memory locationsAnswer: DQUESTION 714Which of the following is NOT an anti-forensics technique?A. Data DeduplicationB. Password ProtectionC. EncryptionD. SteganographyAnswer: AQUESTION 715Select the tool appropriate for finding the dynamically linked lists of an application or malware.A. SysAnalyzerB. ResourcesExtractC. PEiDD. Dependency WalkerAnswer: DQUESTION 716Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. He wants to recover all the data, which includes his personal photos, music, documents, videos, official emails, etc. Which of the following tools shall resolve Bob's purpose?A. Cain & AbelB. RecuvaC. XplicoD. Colasoft's CapsaAnswer: BQUESTION 717In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?A. config.dbB. install.dbC. sigstore.dbD. filecache.dbAnswer: AQUESTION 718Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?A. Hex EditorB. Internet Evidence FinderC. Process MonitorD. Report ViewerAnswer: CQUESTION 719What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?A. Windows Services MonitoringB. System BaseliningC. Start-up Programs MonitoringD. Host integrity MonitoringAnswer: DQUESTION 720Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?A. Power Off timeB. Logs of high temperatures the drive has reachedC. All the states (running and discontinued) associated with the OSD. List of running processesAnswer: BQUESTION 721Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?A. Data Rows store the actual dataB. Data Rows present Page type. Page ID, and so onC. Data Rows point to the location of actual dataD. Data Rows spreads data across multiple databasesAnswer: BQUESTION 722In Windows, prefetching is done to improve system performance. There are two types of prefetching:boot prefetching and application prefetching.During boot prefetching, what does the Cache Manager do?A. Determines the data associated with value EnablePrefetcherB. Monitors the first 10 seconds after the process is startedC. Checks whether the data is processedD. Checks hard page faults and soft page faultsAnswer: CQUESTION 723The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?A. File Allocation Table (FATB. New Technology File System (NTFS)C. Hierarchical File System (HFS)D. Global File System (GFS)Answer: BQUESTION 724Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?A. XSS AttackB. DDoS Attack (Distributed Denial of Service)C. Man-in-the-cloud AttackD. EDoS Attack (Economic Denial of Service)Answer: BQUESTION 725What is the role of Alloc.c in Apache core?A. It handles allocation of resource poolsB. It is useful for reading and handling of the configuration filesC. It takes care of all the data exchange and socket connections between the client and the serverD. It handles server start-ups and timeoutsAnswer: AQUESTION 726Which of the following statements is true regarding SMTP Server?A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS ServerB. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS ServerC. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS ServerD. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS ServerAnswer: CQUESTION 727Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?A. ISO/IEC 16025B. ISO/IEC 18025C. ISO/IEC 19025D. ISO/IEC 17025Answer: DQUESTION 728Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?A. Rule-Based AttackB. Brute-Forcing AttackC. Dictionary AttackD. Hybrid

Password Guessing AttackAnswer: AQUESTION 729In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?A. Chosen-message attackB. Known-cover attackC. Known-message attackD. Known-stego attackAnswer: AQUESTION 730 Which of these Windows utility help you to repair logical file system errors?A. Resource MonitorB. Disk cleanupC. Disk defragmenterD. CHKDSKAnswer: DQUESTION 731Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.A. Expert WitnessB. Evidence ExaminerC. Forensic ExaminerD. Defense WitnessAnswer: AQUESTION 732Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?A. PUB.EDBB. PRIV.EDBC. PUB.STMD. PRIV.STMAnswer: BQUESTION 733Which of the following information is displayed when Netstat is used with -ano switch?A. Ethernet statisticsB. Contents of IP routing tableC. Details of routing tableD. Details of TCP and UDP connectionsAnswer: DQUESTION 734While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?A. Start and end points for log sequence numbers are specifiedB. Start and end points for log files are not specifiedC. Start and end points for log files are specifiedD. Start and end points for log sequence numbers are not specifiedAnswer: BQUESTION 735Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRunOnce.A. All the values in this subkey run when specific user logs on, as this setting is user-specificB. The string specified in the value run executes when user logs onC. All the values in this key are executed at system start-upD. All values in this subkey run when specific user logs on and then the values are deletedAnswer: DQUESTION 736Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?A. PaaS modelB. IaaS modelC. SaaS modelD. SecaaS modelAnswer: BQUESTION 737An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?A. Set the registry value of HKLMSYSTEMCurrentControlSetControlFileSystemNtfsDisableLastAccessUpdate to 0B. Run the command fsutil behavior set disablelastaccess 0C. Set the registry value of HKLMSYSTEMCurrentControlSetControlFileSystemNtfsDisableLastAccessUpdate to 1D. Run the command fsutil behavior set enablelastaccess 0Answer: CQUESTION 738Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?A. SafariB. Mozilla FirefoxC. Microsoft Edge D. Google ChromeAnswer: CQUESTION 739Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?A. NO-SPAM ActB. American: NAVSO P-5239-26 (RLL)C. CAN-SPAM ActD. American: DoD 5220.22-MAnswer: CQUESTION 740Which of the following statements is TRUE about SQL Server error logs?A. SQL Server error logs record all the events occurred on the SQL Server and its databasesB. Forensic investigator uses SQL Server Profiler to view error log filesC. Error logs contain IP address of SQL Server client connectionsD. Trace files record, user-defined events, and specific system eventsAnswer: BQUESTION 741Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?A. RegistryChangesViewB. RegDIIViewC. RegRipperD. ProDiscoverAnswer: CQUESTION 742Consider that you are investigating a machine running an Windows OS released prior to Windows VistA. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:Recycler<USER SID>. You read an entry named "Dd5.exe". What does Dd5.exe mean?A. D drive. fifth file deleted, a .exe fileB. D drive, fourth file restored, a .exe fileC. D drive, fourth file deleted, a .exe fileD. D drive, sixth file deleted, a .exe fileAnswer: BQUESTION 743Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?A. pgrepB. dmesgC. fsckD. grepAnswer: BQUESTION 744A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?A. Class BB. Class DC. Class CD. Class AAnswer: CQUESTION 745Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity.What does the icon in the checkpoint logs represent?A. The firewall rejected a connectionB. A virus was detected in an emailC. The firewall dropped a connectionD. An email was marked as potential spamAnswer: CQUESTION 746In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?A. Cloud as an ObjectB. Cloud as a ToolC. Cloud as an ApplicationD.

Cloud as a SubjectAnswer: DQUESTION 747POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?A. 110B. 143C. 25D. 993Answer: AQUESTION 748 James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?A. Cross Site Request ForgeryB. Cookie TamperingC. Parameter TamperingD. Session Fixation AttackAnswer: DQUESTION 749Which of the following components within the android architecture stack take care of displaying windows owned by different applications?A. Media FrameworkB. Surface ManagerC. Resource ManagerD. Application FrameworkAnswer: DQUESTION 750Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?A. Remote File InclusionB. Cross Site ScriptingC. Insecure Direct Object ReferencesD. Cross Site Request ForgeryAnswer: CQUESTION 751What does Locard's Exchange Principle state?A. Any information of probative value that is either stored or transmitted in a digital formB. Digital evidence must have some characteristics to be disclosed in the court of lawC. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leaveD. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidenceAnswer: CQUESTION 752Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?A. Their first step is to make a hypothesis of what their final findings will be.B. Their first step is to create an initial Executive report to show the management team.C. Their first step is to analyze the data they have currently gathered from the company or interviews.D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.Answer: 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(701-752).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!