[2025-September-NewBraindump2go 100-160 Practice Test Free[Q1-Q26

2025/September Latest Braindump2go 100-160 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindum2go 100-160 Exam Questions!QUESTION 1Why is it necessary to update firmware to the latest version?A. To support the latest operating systems and applicationsB. To patch firmware in the kernel of the operating systemC. To correct security holes and weaknessesD. To explore new hardware featuresAnswer: CExplanation:Keeping firmware up to date is necessary to patch security vulnerabilities and weaknesses that could be exploited by threat actors. Vendors release firmware updates to correct security flaws, enhance stability, and ensure compatibility with updated security protocols.QUESTION 2How do threat actors launch ransomware attacks on organizations?A. They implant malware to collect data from the corporation's financial system.B. They deface an organization's public-facing website.C. They lock data and deny access to the data until they receive money.D. They secretly spy on employees and collect employees' personal information.Answer: CExplanation:Ransomware is a type of malware that denies access to data by encrypting it and demands payment from the victim to restore access. Threat actors may deliver ransomware through phishing emails, malicious downloads, or exploiting vulnerabilities in exposed systems.QUESTION 3 You are planning to work from home. Your company requires that you connect to the company network through a VPN.Which three critical functions do VPNs provide to remote workers? (Choose three.)A. WAN managementB. Authorization of usersC. Integrity of dataD. Authentication of usersE. Confidentiality of informationF. Password managementAnswer: CDE Explanation:Authentication of users: VPNs verify the identity of users to ensure only authorized individuals can access the company network.Integrity of data: VPNs ensure the data transmitted between the remote worker and company network is not altered or tampered with.Confidentiality of information: VPNs encrypt data to keep it private and protect sensitive information from being intercepted by unauthorized parties.QUESTION 4A threat actor sets up a rogue access point (AP) at a local cafe. The rogue AP captures traffic and then forwards the traffic to the cafe AP.Which type of attack does this scenario describe?A. ReconnaissanceB. Man-in-the-middleC. DDoSD. RansomwareAnswer: BExplanation:In a MITM attack, the attacker places themselves between the sender and receiver, intercepting and possibly altering data in transit. Rogue access points can facilitate MITM attacks in wireless environments.QUESTION 5What is the main purpose of a disaster recovery plan as compared to a business continuity plan?A. Limiting operational downtime.B. Keeping the business open in some capacity during a disaster.C. Restoring data access and an IT infrastructure as quickly as possible.D. Allowing staff to continue to serve customers throughout a disaster.Answer: CExplanation:A disaster recovery plan outlines procedures for restoring data and critical IT infrastructure to operational status following a disruptive incident. The goal is to resume normal IT operations as quickly as possible.QUESTION 6A restaurant installs a second wireless router that only employees can use. Which statement describes how to securely configure the new router?A. Configure the new router to filter IP addresses.B. Configure the SSID with broadcast disabled.C. Configure a higher signal strength to allow coverage in the parking lot.D. Configure the SSID with the same SSID used by the customer router.Answer: BExplanation:Disabling SSID broadcast can reduce the visibility of a wireless network, making it less likely to be detected by casual attackers. This should be combined with strong encryption and authentication.QUESTION 7You need to transfer configuration files to a router across an unsecured network. Which protocol should you use to encrypt the files in transit?A. Telnet B. HTTPC. TFTPD. SSHAnswer: DExplanation:SSH encrypts all data exchanged between client and server, protecting credentials and file contents from interception. It is the preferred protocol for secure device management and file transfers across untrusted networks.QUESTION 8Your company is creating a BYOD policy to allow employees to join their personal smartphones to the company network.Which three requirements are commonly included in a BYOD policy? (Choose three.)A. Deletion of all personal data from the phoneB. Synchronization of phone lock screen password with network access passwordC. Encryption of stored confidential corporate dataD. Configuration of a strong passwordE. Upgrade of data plan to maximum availableF. Installation of secure apps onlyAnswer: CDFExplanation:Common requirements include:Device encryption for stored sensitive corporate data.Strong password or PIN configuration for device access.Restriction to secure and approved applications to reduce malware risk.BYOD policies typically mandate strong authentication, encryption of sensitive corporate data on personal devices, and installation of secure or approved applications. The goal is to protect corporate information while respecting personal ownership of the device.QUESTION 9You notice that a new CVE has been shared to an email group that you belong to.What should you do first with the CVE?A. Look up details of the vulnerability to determine whether it applies to your network.B. Research measures to prevent the CVE from attacking the network.C. Record the CVE as part of the disaster recovery plan.D. Add the CVE to the firewall rules for your organization.Answer: AExplanation:Upon learning of a new CVE, security teams should analyze the vulnerability description, affected products, and CVSS score to determine applicability and urgency of mitigation.QUESTION 10 Which encryption type is commonly used to secure WiFi networks?A. Data Encryption Standard (DES)B. Triple Data

Encryption Algorithm (Triple DES)C. Advanced Encryption Algorithm (AES)D. RSA (Rivest-Shamir-Adleman)Answer: C Explanation:WPA2 and WPA3 use the Advanced Encryption Standard (AES) for securing wireless traffic. AES provides strong symmetric encryption, replacing outdated methods like WEP and TKIP.QUESTION 11How does sandboxing help with the analysis of malware?A. It defines the suspicious or malicious applications that should be blocked.B. It specifies the applications that are authorized for use on the network.C. It allows suspicious applications to run in a safe and isolated testing environment.D. It restricts traffic from passing from one network to another.Answer: CExplanation:Sandboxing isolates a suspected application in a secure, controlled environment where it can be executed and analyzed without risking damage to the host system or network.QUESTION 12Which network security technology passively monitors network traffic and compares the captured packet stream with known malicious signatures?A. IDSB. IPSC. Proxy ServerD. HoneypotAnswer: AExplanation:IDS devices inspect network traffic, compare it to known malicious signatures or anomalies, and generate alerts for suspicious activity without actively blocking traffic.QUESTION 13Your supervisor tells you that you will participate in a CVSS assessment.What will you be doing?A. Performing penetration tests on internal network devices and end systemsB. Analyzing host logs to identify abnormal activitiesC. Interviewing users to determine their level of cybersecurity awarenessD. Evaluating end system security and scoring software vulnerabilitiesAnswer: DExplanation:The Common Vulnerability Scoring System (CVSS) provides a numerical score that reflects the severity of a vulnerability, enabling prioritization of remediation efforts.QUESTION 14The company web server collects information through a form. The form is accessed by using port 80. The form content is transferred to an encrypted database for storage. You are investigating a complaint that the form content has been compromised.What is the cause of the security breach?A. The database was compromised.B. The data was transferred to the database using a nonsecure protocol.C. The website was accessed using HTTP, which is an unencrypted protocol.D. The web browser used to access the site was not updated to the latest version.Answer: CExplanation:When HTTP is used instead of HTTPS, all form inputs and transmitted data are sent in plaintext over the network, where they can be intercepted by attackers.QUESTION 15You work for a hospital that stores electronic protected health information (ePHI) in an online portal. Authorized employees can use their mobile devices to access patient ePHI. You need to ensure that employees' mobile devices comply with HIPAA regulations.Which safeguard should you develop and implement?A. An ownership policy for employees' mobile devicesB. A contingency planC. A policy that requires multi-factor authentication to use the mobile deviceD. A policy to govern how ePHI is removed from mobile devicesAnswer: DExplanation:HIPAA requires procedures for the removal of electronic protected health information (ePHI) from devices before disposal, reuse, or reassignment.QUESTION 16You need to design your company's password policy to adhere to the National Institute of Standards and Technology (NIST) guidelines for user password security. What is the minimum password length that you should require to be consistent with the NIST guidelines?A. 4 charactersB. 8 charactersC. 16 charactersD. No minimum lengthAnswer: B Explanation:NIST guidelines specify that user-generated passwords must be at least 8 characters in length, and systems should allow passwords up to at least 64 characters.QUESTION 17You need a software solution that performs the following tasks:- Compiles network data- Logs information from many sources- Provides orchestration in the form of case management- Automates incident response workflowsWhat product should you use?A. SIEMB. SOARC. NextGen IPSD. SnortAnswer: BExplanation:SOAR solutions provide orchestration, automation, and response capabilities. They collect security data from multiple systems, enable analysts to manage incidents, and automate repetitive tasks in the response process.QUESTION 18You are collecting data after a suspected intrusion on the local LAN. You need to capture incoming IP packets to a file for an investigator to analyze.Which two tools should you use? (Choose two.)A. WiresharkB. tcpdumpC. NmapD. netstatAnswer: ABExplanation:Wireshark provides a graphical interface for packet capture and analysis. Tcpdump is a command- line tool that captures packets for detailed offline review.QUESTION 19What should an incident response team do immediately after detecting an incident?A. Update threat intelligence databasesB. Prepare a final reportC. Eradicate the threatD. Notify stakeholdersAnswer: DQUESTION 20Which vulnerabilities can a risk assessment reveal? (Choose two)A. Outdated softwareB. Excessive packet lossC. Misconfigured access controlsD. Insufficient power supplyAnswer: ACQUESTION 21What are components of a comprehensive risk management process? (Choose two)A. Using outdated toolsB. Risk mitigationC. Ignoring minor risksD. Risk assessmentAnswer: BDQUESTION 22Which metric is used in risk assessment to evaluate the severity of a vulnerability?A. CVSS scoreB. Response timeC. Threat level indexD. Packet loss percentageAnswer: AQUESTION 23What is the main role of a Host-Based Intrusion Prevention System (HIPS)?A. To block unauthorized usersB. To encrypt network trafficC. To monitor and prevent suspicious activity on endpointsD. To perform data backupsAnswer: CQUESTION 24Which of the following are examples of secure network protocols? (Choose two)A. SSHB. HTTPS C. FTPD. TelnetAnswer: ABQUESTION 25What tools can help identify network vulnerabilities? (Choose two)A. Email clientsB. Word processorsC. Vulnerability assessment toolsD. Network scannersAnswer: CDQUESTION 26Which protocol is commonly used for secure data transmission over the

internet?A. TelnetB. HTTPSC. FTPD. HTTPAnswer: BResources From:1.2025 Latest Braindump2go 100-160 Exam Dumps (PDF & VCE) Free Share:**https://www.braindump2go.com/100-160.html**2.2025 Latest Braindump2go 100-160 PDF and 100-160 VCE Dumps Free Share:**https://drive.google.com/drive/folders/1_TbGz4Mrh814Lqo3ueLUn6HNOyOXL7xv?usp=sharing**
3.2025 Free Braindump2go 100-160 Exam Questions Download:
https://www.braindump2go.com/free-online-pdf/100-160-VCE-Dumps(1-26).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!