

[September-2021312-50v11 Exam VCE and PDF Free Download in Braindump2go[Q946-Q976

September/2021 Latest Braindump2go 312-50v11 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 312-50v11 Real Exam Questions!

QUESTION 946 Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions. Which of the following master components is explained in the above scenario? A. Kube-controller-manager B. Kube-scheduler C. Kube-apiserver D. Etcd cluster
Answer: B

QUESTION 947 _____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information. A. Spear phishing B. Whaling C. Vishing D. Phishing
Answer: B

QUESTION 948 Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection? A. DMZ B. SMB signing C. VPN D. Switch network
Answer: C

QUESTION 949 An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware. What is the best example of a scareware attack? A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!" B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account." C. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date." D. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
Answer: D

QUESTION 950 Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role? A. FISMA B. HITECH C. PCI-DSS D. Sarbanes-Oxley Act
Answer: C

QUESTION 951 Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program? A. TEA B. CAST-128 C. RC5 D. serpent
Answer: D

QUESTION 952 Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs? A. wash B. nmap C. macof D. net View
Answer: A

QUESTION 953 What type of virus is most likely to remain undetected by antivirus software? A. Cavity virus B. Stealth virus C. File-extension virus D. Macro virus
Answer: B

QUESTION 954 Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario? A. Advanced SMS phishing B. Bypass SSL pinning C. Phishing D. Tap 'n ghost attack
Answer: A

QUESTION 955 Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning? A. Infoga B. WebCopier Pro C. Netsparker D. NCollector Studio
Answer: C

QUESTION 956 Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems? A. Spear-phishing attack B. SMishing attack C. Reconnaissance attack D. HMI-based attack
Answer: A

QUESTION 957 Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system. Which of the following Nmap options must she use to perform service version discovery on the target host? A. -SNB. -SXC. -sVD. -SF
Answer: C

QUESTION 958 Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and

other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?A. Man-in-the-disk attackB. aLTER attackC. SIM card attackD. ASpearphone attackAnswer: BQUESTION 959Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.What is the type of vulnerability assessment that Jude performed on the organization?A. External assessmentB. Passive assessmentC. A Host-based assessmentD. Application assessmentAnswer: CQUESTION 960Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.Which type of threat intelligence is used by Roma to secure the internal network?A. Technical threat intelligenceB. Operational threat intelligenceC. Tactical threat intelligenceD. Strategic threat intelligenceAnswer: BQUESTION 961Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?A. ARINB. APNICC. RIPED. LACNICAnswer: CQUESTION 962Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?A. DNS rebinding attackB. Clickjacking attackC. MarioNet attackD. Watering hole attackAnswer: BQUESTION 963Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?A. Reverse image searchB. Meta search enginesC. Advanced image searchD. Google advanced searchAnswer: CQUESTION 964A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?A. -PYB. -PUC. -PPD. -PnAnswer: CQUESTION 965Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21. What is the service enumerated by James in the above scenario?A. Border Gateway Protocol (BGP)B. File Transfer Protocol (FTP)C. Network File System (NFS)D. Remote procedure call (RPC)Answer: BQUESTION 966Given below are different steps involved in the vulnerability-management life cycle.1) Remediation2) Identify assets and create a baseline3) Verification4) Monitor 5) Vulnerability scan6) Risk assessmentIdentify the correct sequence of steps involved in vulnerability management.A. 2-->5-->6-->1-->3-->4B. 2-->1-->5-->6-->4-->3C. 2-->4-->5-->3-->6-->1D. 1-->2-->3-->4-->5-->6Answer: AQUESTION 967Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.Which of the following tools would not be useful for cracking the hashed passwords?A. John the Ripper B. HashcatC. netcatD. THC-HydraAnswer: AQUESTION 968Which Nmap switch helps evade IDS or firewalls?A. -n/-RB. -0N/-0X/-0GC. -TD. -DAnswer: DQUESTION 969Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 x 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key(Km1)and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?A. CAST-128B. AESC. GOST block cipherD. DESAnswer: CQUESTION 970Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?A. [inurl:]B. [related:]C. [info:]D. [site:]Answer: DQUESTION 971The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?A. WEPB. WPAC. WPA2D. WPA3Answer: CQUESTION 972Stella, a professional hacker, performs an attack

on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?A. XML injectionB. WS-Address spoofingC. SOAPAction spoofingD. Web services parsing attacksAnswer: BQUESTION 973James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open- source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?A. WebSploit FrameworkB. Browser Exploitation FrameworkC. OSINT frameworkD. SpeedPhish FrameworkAnswer: CQUESTION 974Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS. What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?A. Man-in-the-cloud (MITC) attackB. Cloud cryptojackingC. Cloudborne attackD. Metadata spoofing attackAnswer: CQUESTION 975Which among the following is the best example of the third step (delivery) in the cyber kill chain?A. An intruder sends a malicious attachment via email to a target.B. An intruder creates malware to be used as a malicious attachment to an email.C. An intruder's malware is triggered when a target opens a malicious email attachment.D. An intruder's malware is installed on a target's machine.Answer: CQUESTION 976Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?A. Detecting honeypots running on VMwareB. Detecting the presence of Honeyd honeypotsC. A Detecting the presence of Snort_inline honeypotsD. Detecting the presence of Sebek-based honeypotsAnswer: CResources From: 1.2021 Latest Braindump2go 312-50v11 Exam Dumps (PDF & VCE) Free Share: <https://www.braindump2go.com/312-50v11.html>2.2021 Latest Braindump2go 312-50v11 PDF and 312-50v11 VCE Dumps Free Share:<https://drive.google.com/drive/folders/13uhEZnrNlkAP8a1O5NNI-yHndoWuz7Cj?usp=sharing>3.2021 Free Braindump2go 312-50v11 Exam Questions Download:[https://www.braindump2go.com/free-online-pdf/312-50v11-PDF-Dumps\(979-1011\).pdf](https://www.braindump2go.com/free-online-pdf/312-50v11-PDF-Dumps(979-1011).pdf) [https://www.braindump2go.com/free-online-pdf/312-50v11-VCE-Dumps\(946-978\).pdf](https://www.braindump2go.com/free-online-pdf/312-50v11-VCE-Dumps(946-978).pdf)Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!