

[November-2020Braindump2go PT0-001 (PDF and VCE)Exam Dumps PT0-001 213Q Free Offer[Q191-Q213]

November/2020 Latest Braindump2go PT0-001 Exam Dumps with PDF and VCE Free Updated Today! Following are some new PT0-001 Real Exam Questions!

QUESTION 191 You can find XSS vulnerabilities in which of the following? A. Search fields that echo a search string back to the user B. HTTP headers C. Input fields that echo user data D. All of the above Answer: A

QUESTION 192 A potential customer is looking to test the security of its network. One of the customer's primary concerns is the security awareness of its employees. Which type of test would you recommend that the company perform as part of the penetration test? A. Social engineering testing B. Wireless testing C. Network testing D. Web application testing Answer: A

QUESTION 193 Which tool included in Kali is most helpful in compiling a quality penetration testing report? A. Nmap B. Metasploit C. Dradis D. SET Answer: C

QUESTION 194 Software developers should escape all characters (including spaces but excluding alphanumeric characters) with the HTML entity `&#xHH;` format to prevent what type of attack? A. DDoS attacks B. XSS attacks C. CSRF attacks D. Brute-force attacks Answer: B

QUESTION 195 A security consultant finds a folder in "C:\Program Files" that has writable permission from an unprivileged user account. Which of the following can be used to gain higher privileges? A. Retrieving the SAM database B. Kerberoasting C. Retrieving credentials in LSASS D. DLL hijacking E. VM sandbox escape Answer: C

QUESTION 196 Which of the following documents BEST describes the manner in which a security assessment will be conducted? A. BIAB. SOW C. SLAD. MSA Answer: A

QUESTION 197 A penetration tester found a network with NAC enabled. Which of the following commands can be used to bypass the NAC? A. `macchanger` B. `sslstrip` C. `iptables` D. `proxychains` Answer: A

QUESTION 198 An internal network penetration test is conducted against a network that is protected by an unknown NAC system. In an effort to bypass the NAC restrictions, the penetration tester spoofs the MAC address and hostname of an authorized system. Which of the following devices if impersonated would be MOST likely to provide the tester with network access? A. Network-attached printer B. Power-over-Ethernet injector C. User workstation D. Wireless router Answer: A

QUESTION 199 A penetration tester is performing a code review against a web application. Given the following URL and source code: Which of the following vulnerabilities is present in the code above? A. SQL injection B. Cross-site scripting C. Command injection D. LDAP injection Answer: C

QUESTION 200 After an Nmap NSE scan, a security consultant is seeing inconsistent results while scanning a host. Which of the following is the MOST likely cause? A. Services are not listening B. The network administrator shut down services C. The host was not reachable D. A firewall/IPS blocked the scan Answer: D

QUESTION 201 Which of the following wordlists is BEST for cracking MD5 password hashes of an application's users from a compromised database? A. `./wordlists/rockyou.txt` B. `./dirb/wordlists/big.txt` C. `./wfuzz/wordlist/vulns/sql_inj.txt` D. `./wordlists/raeta3ploit/roet_uaerpass.txt` Answer: A

QUESTION 202 A penetration tester calls human resources and begins asking open-ended questions. Which of the following social engineering techniques is the penetration tester using? A. Interrogation B. Elicitation C. Impersonation D. Spear phishing Answer: B

QUESTION 203 An attacker is attempting to gain unauthorized access to a Wi-Fi network that uses WPA2-PSK. Which of the following attack vectors would the attacker MOST likely use? A. Capture a three-way handshake and crack it B. Capture a mobile device and crack its encryption C. Create a rogue wireless access point D. Capture a four-way handshake and crack it Answer: D

QUESTION 204 The SELinux and AppArmor security frameworks include enforcement rules that attempt to prevent which of the following attacks? A. Lateral movement B. Sandbox escape C. Cross-site request forgery (CSRF) D. Cross-site-scripting (XSS) Answer: B

QUESTION 205 A _____ vulnerability scan would typically be focused on a specific set of requirements. A. Full B. Stealth C. Compliance D. Discovery Answer: C

QUESTION 206 Which of the following can be used for post-exploitation activities? A. WinDbg B. IDAC. Maltego D. PowerShell Answer: D

QUESTION 207 Which of the following can be used to perform online password attacks against RDP? A. Hashcat B. John the Ripper C. Aircrack-ng D. Ncrack Answer: D

QUESTION 208 A company received a report with the following finding: While on the internal network, the penetration tester was able to successfully capture SMB broadcasted user ID and password information on the network and decode this information. This allowed the penetration tester to then join their own computer to the ABC domain. Which of the following remediations are appropriate for the reported findings? (Select TWO) A. Set the Schedule Task Service from Automatic to Disabled B. Enable network-level authentication C. Remove the ability from Domain Users to join domain computers to the network D. Set the netlogon service from Automatic to Disabled E. Set up a SIEM alert to monitor Domain joined machines F. Set "Digitally sign network communications" to Always Answer: BC

QUESTION 209 Which of the following actions BEST matches a script kiddie's threat actor? A. Exfiltrate network diagrams to perform lateral movement B. Steal credit cards from the database and sell them in the deep web C. Install a rootkit to maintain access to the corporate network D. Deface the website of a company in search of retribution Answer: B

QUESTION 210 A penetration tester has compromised a system and

wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?A. nc looalhot 4423B. nc -nvlp 4423 -?/bin/bashC. nc 10.0.0.1 4423D. nc 127.0.0.1 4423 -e /bin/bashAnswer: BQUESTION 211

An organization has requested that a penetration test be performed to determine if it is possible for an attacker to gain a foothold on the organization's server segment During the assessment, the penetration tester identifies tools that appear to have been left behind by a prior attack Which of the following actions should the penetration tester take?A. Attempt to use the remnant tools to achieve persistenceB. Document the presence of the left-behind tools in the report and proceed with the testC. Remove the tools from the affected systems before continuing on with the testD. Discontinue further testing and report the situation to managementAnswer: AQUESTION 212

A penetration tester has obtained access to an IP network subnet that contains ICS equipment intercommunication. Which of the following attacks is MOST likely to succeed in creating a physical effect?A. DNS cache poisoningB. Record and replayC. Supervisory server SMBD. Blind SQL injectionAnswer: AQUESTION 213

Which of the following BEST describes the difference between a red team engagement and a penetration test?A. A penetration test has a broad scope and emulates advanced persistent threats while a red team engagement has a limited scope and focuses more on vulnerability identificationB. A red team engagement has a broad scope and emulates advanced persistent threats, while a penetration test has a limited scope and focuses more on vulnerability identificationC. A red team engagement has a broad scope and focuses more on vulnerability identification, while a penetration test has a limited scope and emulates advanced persistent threatsD. A penetration test has a broad scope and focuses more on vulnerability identification while a red team engagement has a limited scope and emulates advanced persistent threatsAnswer: DResources From:1.2020 Latest Braindump2go PT0-001 Exam Dumps (PDF & VCE) Free Share:

<https://www.braindump2go.com/pt0-001.html>2.2020 Latest Braindump2go PT0-001 PDF and PT0-001 VCE Dumps Free Share:

<https://drive.google.com/drive/folders/1upxI-JhgoyePRzSCJXgkSKrKo53vIXSw?usp=sharing>3.2020 Free Braindump2go PT0-001 PDF Download:[https://www.braindump2go.com/free-online-pdf/PT0-001-Dumps\(194-204\).pdf](https://www.braindump2go.com/free-online-pdf/PT0-001-Dumps(194-204).pdf)

[https://www.braindump2go.com/free-online-pdf/PT0-001-PDF\(183-193\).pdf](https://www.braindump2go.com/free-online-pdf/PT0-001-PDF(183-193).pdf)

[https://www.braindump2go.com/free-online-pdf/PT0-001-PDF-Dumps\(159-169\).pdf](https://www.braindump2go.com/free-online-pdf/PT0-001-PDF-Dumps(159-169).pdf)

[https://www.braindump2go.com/free-online-pdf/PT0-001-VCE\(170-182\).pdf](https://www.braindump2go.com/free-online-pdf/PT0-001-VCE(170-182).pdf)

[https://www.braindump2go.com/free-online-pdf/PT0-001-VCE-Dumps\(205-213\).pdf](https://www.braindump2go.com/free-online-pdf/PT0-001-VCE-Dumps(205-213).pdf)Free Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!