

[Jan-2019] High Quality Braindump2go 312-50v10 PDF and VCE 772Q Free Share(Q720-Q738)

2019/January Braindump2go 312-50v10 Exam Dumps with PDF and VCE New Updated Today! Following are some new 312-50v10 Real Exam Questions:]

1. [2019 Latest 312-50v10 Exam Dumps (PDF & VCE) 772Q&As Download: <https://www.braindump2go.com/312-50v10.html>]

2. [2019 Latest 312-50v10 Exam Questions & Answers Download: https://drive.google.com/drive/folders/1g15jl9W8jnovDp0b_CsOg86BZSP5ualP?usp=sharing]

QUESTION 720 The "black box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. Only the external operation of a system is accessible to the tester.
Answer: D

QUESTION 721 NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?
A. A port scan
B. A ping scan
C. An operating system detect
D. A trace sweep
Answer: A

QUESTION 722 An LDAP directory can be used to store information similar to a SQL database. LDAP uses a ____ database structure instead of SQL's ____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.
A. Strict, Abstract
B. Simple, Complex
C. Relational, Hierarchical
D. Hierarchical, Relational
Answer: D

QUESTION 723 What is the purpose of DNS AAAA record?
A. Address prefix record
B. Address database record
C. Authorization, Authentication and Auditing record
D. IPv6 address resolution record
Answer: D

QUESTION 724 Which of the following statements is FALSE with respect to Intrusion Detection Systems?
A. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
B. Intrusion Detection Systems can examine the contents of the data in context of the network protocol
C. Intrusion Detection Systems can be configured to distinguish specific content in network packets
D. Intrusion Detection Systems require constant update of the signature library
Answer: A

QUESTION 725 You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
A. list domain=abccorp.local type=zone
B. Is -d accorp.local
C. list server=192.168.10.2 type=all
D. Iserver 192.168.10.2 -t all
Answer: B

QUESTION 726 Which command can be used to show the current TCP/IP connections?
A. Netsh
B. Net use connection
C. Netstat
D. Net use
Answer: C

QUESTION 727 You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it. What tool will help you with the task?
A. Armitage
B. Dmitry
C. Metagoofil
D. cdpnsnarf
Answer: C

QUESTION 728 You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions. Which command-line utility are you most likely to use?
A. Relational Database
B. MS Excel
C. Notepad
D. Grep
Answer: D

QUESTION 729 This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering and it will tell you the "landscape" looks like. What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?
A. network mapping
B. footprinting
C. escalating privileges
D. gaining access
Answer: B

QUESTION 730 When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?
A. site: target.com filetype:xls username password email
B. domain: target.com archive:xls username password email
C. inurl: target.com filename:xls username password email
D. site: target.com file:xls username password email
Answer: A

QUESTION 731 You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled. Which port would you see listening on these Windows machines in the network?
A. 161
B. 3389
C. 445
D. 1433
Answer: C

QUESTION 732 Which of the following is assured by the use of a hash?
A. Authentication
B. Confidentiality
C. Availability
D. Integrity
Answer: D

QUESTION 733 Risks=Threats x Vulnerabilities is referred to as the:
A. BIA equation
B. Disaster recovery formula
C. Risk equation
D. Threat assessment
Answer: C

QUESTION 734 The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?
A. Network Sniffer
B. Vulnerability Scanner
C. Intrusion Prevention Server
D. Security Incident and Event Monitoring
Answer: D

QUESTION 735 You have just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk. What is one of the first things you should do when given the job?
A. Establish attribution to suspected attackers
B. Interview all employees in the company to rule out possible insider threats
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable

levels.D. Start the wireshark application to start sniffing network traffic.**Answer: C**QUESTION 736The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.A. Wireless AnalyzerB. Wireless JammerC. Wireless Access PointD. Wireless Access Control List**Answer: D**QUESTION 737What does the -oX flag do in an Nmap scan?A. Perform an Xmas scanB. Perform an eXpress scanC. Output the results in truncated format to the screenD. Output the results in XML format to a file**Answer: D**QUESTION 738During an Xmas scan, what indicates a port is closed?A. RSTB. SYNC. ACKD. No return response**Answer: A**!!!RECOMMEND!!!1.|2019 Latest 312-50v10 Exam Dumps (PDF & VCE) 772Q&As Download:<https://www.braindump2go.com/312-50v10.html2>.|2019 Latest 312-50v10 Study **Guide Video:** YouTube Video: [YouTube.com/watch?v=c9tsGRT4pa4](https://www.youtube.com/watch?v=c9tsGRT4pa4)