312-38 Exam Dumps - Try Best 312-38 Exam Questions from Training Expert DumpsMaterials [Q16-Q35

312-38 Exam Dumps - Try Best 312-38 Exam Questions from Training Expert DumpsMaterials
Practice Examples and Dumps & Tips for 2022 Latest 312-38 Valid Tests Dumps

Q16. Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?
* NNTP
* BOOTP
* DCAP
* NTP
The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read.

Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these

issues.

Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

Q17. John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

* PsPasswd
* Kismet
* AirSnort
* Cain

AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows: pspasswd [\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

Q18. Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

* Wireless sniffer
* Spectrum analyzer
* Protocol analyzer
* Performance Monitor

Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and software components of a server.

Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition

of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

Q19. CORRECT TEXT

Fill in the blank with the appropriate term. _____ encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.
Asymmetric

Explanation:

Asymmetric encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses the public key to encrypt the data. The receiver uses his private key to decrypt the data.

Q20. If a network is at risk from unskilled individuals, what type of threat is this?
* External Threats
* Structured Threats
* Unstructured Threats
* Internal Threats

Q21. Which of the following statements are true about a wireless network?

Each correct answer represents a complete solution. Choose all that apply.
* Data can be shared easily between wireless devices.
* It provides mobility to users to access a network.
* Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
* It is easy to connect.

The advantages of a wireless network are as follows:

It provides mobility to users to access a network.

It is easy to connect.

The initial cost to set up a wireless network is low as compared to that of manual cable

network.Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC,

etc.Data can be shared easily between the wireless devices.

Q22. Which of the following organizations is responsible for managing the assignment of domain names and IP addresses?
* ISO
* ICANN
* W3C
* ANSI

ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN’s tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. Answer option A is incorrect. The International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization

promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most nongovernmental organizations. In practice, ISO acts as a consortium with strong links to governments. Answer option C is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated , with support from DARPA and the European Commission. Answer option D is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC).
Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

Q23. Which of the following is a malicious program that looks like a normal program?
* Impersonation
* Worm
* Virus
* Trojan horse

Q24. Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?
* RSVP
* DVMRP
* RPC
* LWAPP

The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet’s multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP’s flat unicast routing mechanism also affects its capability to scale. Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness. RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path. Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results. Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

Q25. Which of the following is a method of authentication that uses physical characteristics?
* COMSEC
* ACL
* Honeypot
* Biometrics

Q26. Token Ring is standardized by which of the following IEEE standards?
* 802.2

* 802.4
* 802.3
* 802.1

Q27. FILL BLANK

Fill in the blank with the appropriate term. The _____ protocol is a feature of packet-based data

transmission protocols. It is used to keep a record of the frame sequences sent and their respective

acknowledgements received by both the users.
Sliding Window

Explanation:

The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link

layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame

sequences sent, and their respective acknowledgements received, by both the users. Its additional feature

over a simpler protocol is that can allow multiple packets to be “in transmission” simultaneously, rather than

waiting for each packet to be acknowledged before sending the next.In transmit flow control, sliding window is

a variable-duration window that allows a sender to transmit a specified number of data units before an

acknowledgment is received or before a specified event occurs.An example of a sliding window is one in

which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender “slides”

the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified

number of times before the sender interrupts transmission. Sliding window is sometimes called

acknowledgment delay period.

Q28. Which of the following IEEE standards is an example of a DQDB access method?
* 802.3
* 802.5
* 802.6
* 802.4

Q29. John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____.
* Mitigation, Security policies
* Verification, Security Policies
* Vulnerability scanning, Risk Analysis
* Risk analysis, Risk matrix

Q30. Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer and logs activities of the network that is matched with the predefined signatures?

* Dsniff
* KisMAC
* Snort
* Kismet

Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer option A is incorrect. Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc. Answer option D is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option B is incorrect. KisMAC is a wireless network discovery tool for Mac OS X.

It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared towards the network security professionals, and is not as novice-friendly as the similar applications. KisMAC will scan for networks passively on supported cards, including Apple’s AirPort, AirPort Extreme, and many third-party cards. It will scan for networks actively on any card supported by Mac OS X itself. Cracking of WEP and WPA keys, both by brute force, and exploiting flaws, such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and when packet reinsertion can be done with a supported card. The GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs, such as Wireshark.

Q31. Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.

* Class C
* Class D
* Class A
* Class B
* Class E

Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254. Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to 16,777,214 client devices (hosts), and their address range can extend from 1 to 126. Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to 65,534 client devices, and their address range can extend from 128 to 191. Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to

223.

Q32. Which of the following organizations is responsible for managing the assignment of domain names and IP addresses?

* ISO
* ICANN
* W3C
* ANSI

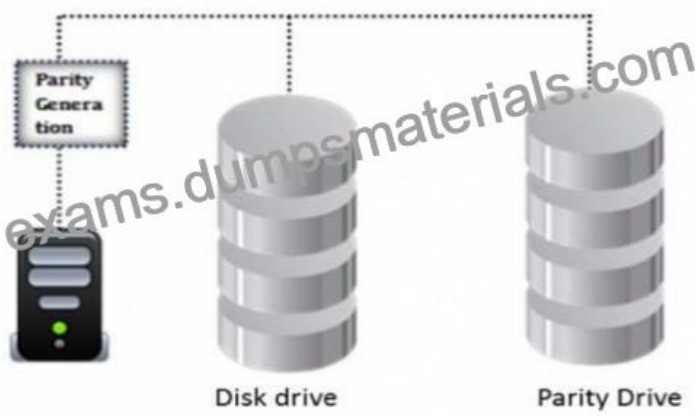
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN’s tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions.

Answer option A is incorrect. The International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non- governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments.

Answer option C is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated, with support from DARPA and the European Commission.

Answer option D is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

Q33. Identify the minimum number of drives required to setup RAID level 5.



* Multiple
* 3
* 4
* 2

Q34. Which of the following protocols is a method of implementing virtual private networks?
* OSPF
* PPTP

* IRDP
* DHCP

Q35. Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents a complete solution. Choose all that apply.
* In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.
* Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.
* The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
* Hosts in the DMZ have full connectivity to specific hosts in the internal network.

A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization’s Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

Preparation Process

Understanding the exam topics is very critical to success in the test. Therefore, the potential candidates must download the exam blueprint to review the comprehensive details of these domains. After exploring the scope of the test, they can proceed to choose ample resources to prepare for EC-Council 312-38 with great deliberation.

Latest 100% Passing Guarantee - Brilliant 312-38 Exam Questions PDF:
https://www.dumpsmaterials.com/312-38-real-torrent.html]