DUMPSARENA

Certified Network Defender (CND)

ECCouncil 312-38

Version Demo

Total Demo Questions: 20

Total Premium Questions: 563

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

The agency Jacob works for stores and transmits vast amounts of sensitive government data that cannot be compromised. Jacob has implemented Encapsulating Security Payload (ESP) to encrypt IP traffic. Jacob wants to encrypt the IP traffic by inserting the ESP header in the IP datagram before the transport layer protocol header. What mode of ESP does Jacob need to use to encrypt the IP traffic?

A. Jacob should use ESP in pass-through mode.

B. Jacob should utilize ESP in tunnel mode.

C. He should use ESP in gateway mode.

D. He should use ESP in transport mode.

ANSWER: B

QUESTION NO: 2

CSMA/CD is specified in which of the following IEEE standards?

A. 802.3

B. 802.2

C. 802.1

D. 802.15

ANSWER: A

QUESTION NO: 3

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. Read-Only Memory (ROM) is an example of volatile memory.

B. The content is stored permanently, and even the power supply is switched off.

C. The volatile storage device is faster in reading and writing data.

D. It is computer memory that requires power to maintain the stored information.

ANSWER: C D

Explanation:

Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION NO: 4

You work for a professional computer hacking forensic investigator DataEnet Inc. To explore the e-mail information about an employee of the company. The suspect an employee to use the online e-mail systems such as Hotmail or Yahoo. Which of the following folders on the local computer you are going to check to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. cookies folder

B. Temporary Internet Folder

C. download folder

D. History Folder

ANSWER: A B D

QUESTION NO: 5

Which of the following is the primary international body for fostering cooperative standards for telecommunications equipment and systems?

A. ICANN

B. IEEE

C. NIST

D. CCITT

ANSWER: D

Explanation:

CCITT is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It is now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union). The ITU-T mission is to ensure the efficient and timely production of standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.

Answer option A is incorrect. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.

Answer option B is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas. Answer option C is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is as follows: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NIST had an operating budget for fiscal year 2007 (October 1, 2006-September 30, 2007) of about $843.3 million. NIST's 2009 budget was $992 million, but it also received $610 million as part of the American Recovery and Reinvestment Act. NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates (guest researchers and engineers from American companies and foreign nations) complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at nearly 350 affiliated centers around the country.

QUESTION NO: 6

What is the range for private ports?

A. 49152 through 65535

B. 1024 through 49151

C. Above 65535

D. 0 through 1023

ANSWER: A

QUESTION NO: 7

What is needed for idle scan a closed port the next steps? Each correct answer represents a part of the solution. Choose all that apply.

A. Zombie ignores unsolicited RST, and IP ID remains unchanged.

B. The attacker sends a SYN/ACK zombie.

C. In response to the SYN, the target to send RST.

D. Zombie IP ID will increase by only 1.

E. Zombie IP ID 2 rises.

ANSWER: A B C D

QUESTION NO: 8

How can one identify the baseline for normal traffic?

A. When the SYN flag appears at the beginning and the FIN flag appears at the end of the connection

B. When the RST flag appears at the beginning and the ACK flag appears at the end of the connection

C. When the ACK flag appears at the beginning and the RST flag appears at the end of the connection

D. When the FIN flag appears at the beginning and the SYN flag appears at the end of the connection

ANSWER: A

QUESTION NO: 9

Which of the following are the various methods that a device can use for logging information on a Cisco router? Each correct answer represents a complete solution. Choose all that apply.

A. Buffered logging

B. Syslog logging

C. NTP logging

D. Terminal logging

E. Console logging

F. SNMP logging

ANSWER: A B D E F

Explanation:

There are different methods that a device can use for logging information on a Cisco router:

Terminal logging: In this method, log messages are sent to the VTY session.

Console logging: In this method, log messages are sent directly to the console port.

Buffered logging: In this method, log messages are kept in the RAM on the router. As the buffer fills, the older messages are overwritten by the newer messages. Syslog logging: In this method, log messages are sent to an external syslog server

where they are stored and sorted. SNMP logging: In this method, log messages are sent to an SNMP server in the network. Answer option C is incorrect. This is an invalid option.

QUESTION NO: 10

In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

A. The router does not have a configuration file.

B. There is a need to set operating parameters.

C. The user interrupts the boot sequence.

D. The router does not find a valid operating system image.

ANSWER: C D

Explanation:

The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic tests.

Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup mode when the user switches it on. Setup mode creates an initial configuration. Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

QUESTION NO: 11

Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?

A. Spamming

B. War driving

C. War dialing

D. Warchalking

ANSWER: D

Explanation:

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

Answer option B is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle,

a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Answer option C is incorrect. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.

Answer option A is incorrect. Spamming is the technique of flooding the Internet with a number of copies of the same message. The most widely recognized form of spams are e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.

QUESTION NO: 12

Which of the following types of information can be obtained through network sniffing? (Choose all that apply.)

A. DNS traffic

B. Telnet passwords

C. Programming errors

D. Syslog traffic

ANSWER: A C D

QUESTION NO: 13

Which of the following key features is used by TCP in order to regulate the amount of data sent by a host to another host on the network?

A. Sequence number

B. TCP timestamp

C. Congestion control

D. Flow control

ANSWER: D

Explanation:

Flow control is the process of regulating the amount of data sent by a host to another host on the network. The flow control mechanism controls packet flow so that a sender does not transmit more packets than a receiver can process. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies in the receive window field the amount of additional received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that

amount of data before it must wait for an acknowledgment and window update from the receiving host. Answer option A is incorrect. TCP uses a sequence number for identifying each byte of data.

Answer option B is incorrect. TCP timestamp helps TCP to compute the round-trip time between the sender and receiver.

Answer option C is incorrect. Congestion control concerns controlling traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

QUESTION NO: 14

Which of the following are the valid steps for securing routers? Each correct answer represents a complete solution. Choose all that apply.

A. Use a password that is easy to remember for a router's administrative console.

B. Use a complex password for a router's administrative console.

C. Configure access list entries to prevent unauthorized connections and traffic routing.

D. Keep routers updated with the latest security patches.

ANSWER: B C D

Explanation:

The following are the valid steps for securing routers and devices:

Configure access list entries to prevent unauthorized connections and traffic routing. Use a complex password for a router's administrative console.

Keep routers in locked rooms.

Keep routers updated with the latest security patches.

Use monitoring an equipment to protect routers and devices.

Router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. Router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.

A security patch is a program that eliminates a vulnerability exploited by hackers.

QUESTION NO: 15 - (DRAG DROP)

DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:

	Terms	Description
ASLR	Place Here	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
Hypervisor	Place Here	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
DEP	Place Here	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

ANSWER:

	Terms	Description
ASLR	DEP	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
Hypervisor	ASLR	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
DEP	Hypervisor	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

Explanation:

Following are the terms with their descriptions:

Terms	Description
DEP	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
ASLR	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
Hypervisor	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

QUESTION NO: 16

You are tasked to perform black hat vulnerability assessment for a client. You received official written permission to work with: company site, forum, Linux server with LAMP, where this site hosted. Which vulnerability assessment tool should you consider to use?

A. dnsbrute

B. hping

C. OpenVAS

D. wireshark

ANSWER: C

QUESTION NO: 17

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. The content is stored permanently and even the power supply is switched off.

B. A volatile storage device is faster in reading and writing data.

C. Read only memory (ROM) is an example of volatile memory.

D. It is computer memory that requires power to maintain the stored information.

ANSWER: B D

Explanation:

Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data.

Answer options A and C are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION NO: 18

Which has the following fields IPv6 header is reduced by 1 for each router that sends a packet?

A. None

B. traffic class

C. hop limit

D. Next header

E. Flow label

ANSWER: C

QUESTION NO: 19

Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?

A. Just Enough Administration (EA)

B. User Account Control (UAC)

C. Windows Security Identifier (SID)

D. Credential Guard

ANSWER: A

QUESTION NO: 20

Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.

A. Message replay

B. Identity theft

C. Message modification

D. Message digest

E. Message repudiation

F. Eavesdropping

G. False message

ANSWER: A B C E F G

Explanation:

Following are the common security problems involved in communications and email:

Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.

Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages. These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.

Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.

False message: It the act of constructing messages that appear to be sent by someone else.

Message replay: In a message replay, messages are modified, saved, and re-sent later.

Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.

Answer option D is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.