312-38Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?

A. Fire sprinkler

B. Fire suppression system

C. Fire alarm system

D. Gaseous fire suppression

Correct Answer: C

An automatic fire alarm system is designed for detecting the unwanted presence of fire by monitoring environmental changes associated with combustion. In general, a fire alarm system is classified as either automatically actuated, manually actuated, or both. Automatic fire alarm systems are intended to notify the building occupants to evacuate in the event of a fire or other emergency, to report the event to an off-premises location in order to summon emergency services, and to prepare the structure and associated systems to control the spread of fire and smoke. Answer option B is incorrect. A fire suppression system is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety. Answer option D is incorrect. Gaseous fire suppression is a term to describe the use of inert gases and chemical agents to extinguish a fire. Answer option A is incorrect. A fire sprinkler is the part of a fire sprinkler system that discharges water when the effects of a fire have been detected, such as when a predetermined temperature has been reached.

QUESTION 2

Which of the following is a symmetric 64-bit block cipher that can support key lengths up to 448 bits?

A. HAVAL

B. BLOWFISH

C. IDEA

D. XOR

Correct Answer: B

QUESTION 3

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail spam

B. E-mail storm

C. E-mail bombing

D. E-mail spoofing

Correct Answer: A

Peter is performing spamming activity. Spam is a term that refers to the unsolicited e-mails sent to a large number of e-mail users. The number of such e-mails is increasing day by day, as most companies now prefer to use e-mails for promoting their products. Because of these unsolicited e-mails, legitimate e-mails take a much longer time to deliver to their destination. The attachments sent through spam may also contain viruses. However, spam can be stopped by implementing spam filters on servers and e-mail clients. Answer option C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient\\'s hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack. Answer option B is incorrect. An e-mail storm is a sudden spike of Reply All messages on an e-mail distribution list, usually caused by a controversial or misdirected message. Such storms start when multiple members of the distribution list reply to the entire list at the same time in response to an instigating message. Other members soon respond, usually adding vitriol to the discussion, asking to be removed from the list, or pleading for the cessation of messages. If enough members reply to these unwanted messages, this triggers a chain reaction of e-mail messages. The sheer load of traffic generated by these storms can render the e-mail servers carrying them inoperative, similar to a DDoS attack. Some e-mail viruses also have the capacity to create e-mail storms, by sending copies of themselves to an infected user\\'s contacts, including distribution lists, infecting the contacts in turn. Answer option D is incorrect. E-mail spoofing is a term used to describe e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path, and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the From field, it actually comes from another source.

QUESTION 4

In which of the following attacks does an attacker successfully insert an intermediary software or program between two communicating hosts?

A. Session hijacking

B. Denial-of-Service

C. Man-in-the-middle

D. Buffer overflow

Correct Answer: C

Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer option B is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as a network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to the network. The effects of a DoS attack are as follows: Saturates network resources Disrupts connections between two computers, thereby preventing communications between services Disrupts services to a specific computer Causes failure to access a Web site Results in an increase in the amount of spam A Denial-of-Service attack is very common on the Internet because it is much easier to accomplish. Most of the DoS attacks rely on the weaknesses in the TCP/IP protocol. Answer option D is incorrect. A buffer-overflow attack is performed when a hacker fills a field, typically an

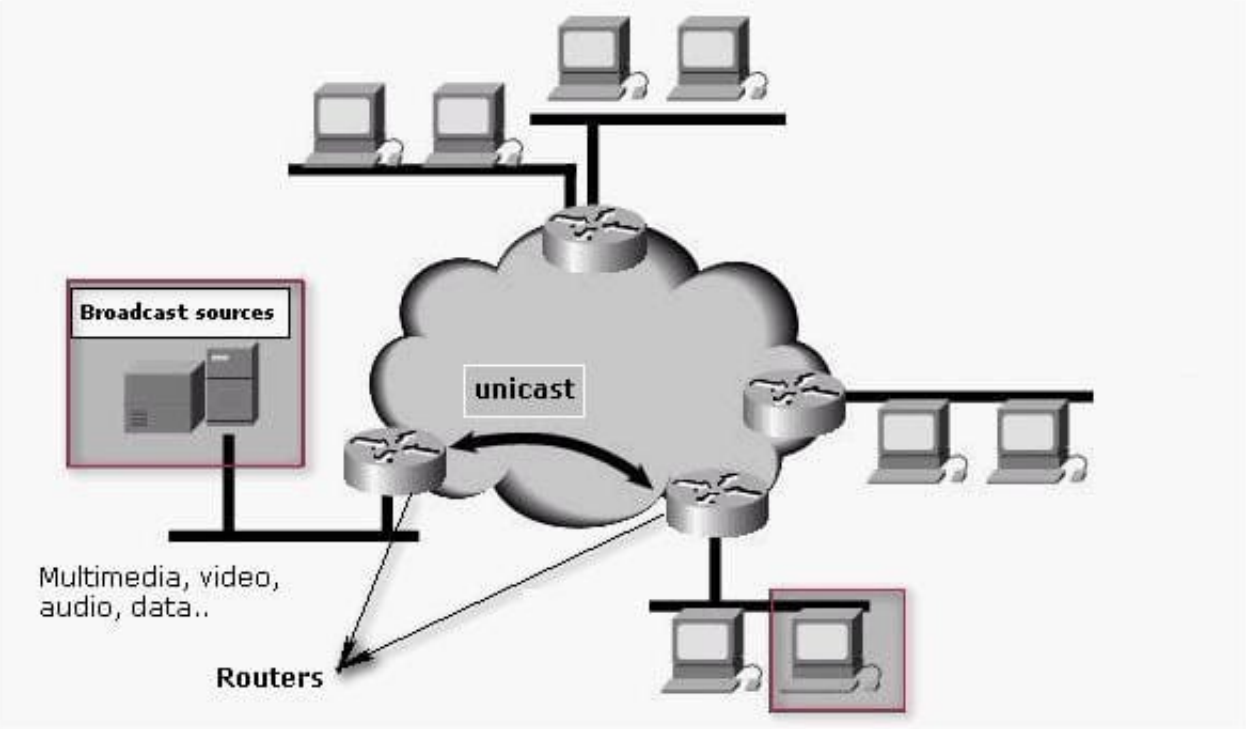
address bar, with more characters than it can accommodate. The excess characters can be run as executable code, effectively giving the hacker control of the computer and overriding any security measures set. There are two main types of buffer overflow attacks: stack-based buffer overflow attack: Stack-based buffer overflow attack uses a memory object known as a stack. The hacker develops the code which reserves a specific amount of space for the stack. If the input of user is longer than the amount of space reserved for it within the stack, then the stack will overflow. heap-based buffer overflow attack: Heap-based overflow attack floods the memory space reserved for the programs. Answer option A is incorrect. Session hijacking refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to Web developers, as the HTTP cookies used to maintain a session on many Web sites can be easily stolen by an attacker using an intermediary computer or with

access to the saved cookies on the victim\\'s computer (see HTTP cookie theft).

TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.

QUESTION 5

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:



What is the IP address of the sender of this email?

A. 209.191.91.180

B. 141.1.1.1

C. 172.16.10.90

D. 216.168.54.25

Correct Answer: D

The IP address of the sender of this email is 216.168.54.25. According to the scenario, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. Once you start to analyze the email header, you get an entry entitled as X-Originating-IP. You know that in Yahoo, the X-Originating-IP is the IP address of the email sender and in this case, the required IP address is 216.168.54.25. Answer options A, C, and B are incorrect. All these are the IP addresses of the Yahoo and Wetpaint servers.