312-38 Q&As

Certified Network Defender (CND)

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

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

QUESTION 1

The _________ mechanism works on the basis of a client-server model.

A. Push-based

B. Host-based

C. Pull-based

D. Network-based

Correct Answer: C

QUESTION 2

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 3

Which field is not included in the TCP header?

A. Acknowledgment number

B. Sequence number

C. Source port

D. Source IP address

Correct Answer: D

QUESTION 4

Which of the following is a presentation layer protocol?

A. TCP

B. RPC

C. BGP

D. LWAPP

Correct Answer: D

QUESTION 5

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. (Choose two.)

A. Using WPA encryption

B. Not broadcasting SSID

C. Using WEP encryption

D. MAC filtering the router

Correct Answer: CA

With either encryption method (WEP or WPA), you can give the password to the customers who need it, and even change it frequently (daily if you like). So this won\\'t be an inconvenience for the customers.