312-38 Q&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.geekcert.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

Fill in the blank with the appropriate term. A is a block of data that a Web server stores on the client computer.

Correct Answer: cookie

Cookie is a block of data, which a Web server stores on the client computer. If no expiration date is set for the cookie, it expires when the browser closes. If the expiration date is set for a future date, the cookie will be stored on the client\\'s disk after the session ends. If the expiration date is set for a past date, the cookie is deleted.

QUESTION 2

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 3

Heather has been tasked with setting up and implementing VPN tunnels to remote offices. She will most likely be implementing IPsec VPN tunnels to connect the offices. At what layer of the OSI model does an IPsec tunnel function on?

A. They function on the data link layer.

B. They work on the network layer.

C. They function on either the application or the physical layer.

D. They work on the session layer.

Correct Answer: B

QUESTION 4

Which of the following is an intrusion detection system that reads all incoming packets and tries to find suspicious patterns known as signatures or rules?

A. HIDS

B. IPS

C. DMZ

D. NIDS

Correct Answer: D

A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does. Answer option A is incorrect. A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected. Answer option B is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Answer option C is incorrect. 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.

QUESTION 5

Which of the following is a malicious program that looks like a normal program?

A. Impersonation

B. Worm

C. Virus

D. Trojan horse

Correct Answer: D